UNIVERSITÉ D'EVRY VAL D'ESSONNE

LABORATOIRE DE RÉSEAUX ET SYSTÈMES MULTIMÉDIA

THESES

Pour l'obtention du grade de :

Docteur en Sciences de l'Université d'Evry – Val d'Essonne

Discipline: Informatique

Par

Mr Vamsi Krishna GONDI

Titre:

SEAMLESS SECURED ROAMING OVER HETEROGENEOUS WIRELESS NETWORKS

Mars 23rd, 2009

Jury

Directeur	M. Nazim AGOULMINE	Professeur (Université d'Evry Val-d'Essonne)
Rapporteurs	M. Mikael SALAUN	Docteur (France Télécom)
	Josef NOLL	Professeur (UNIK, Norvège)
Examinateurs	Hossam AFIFI	Professeur (Telecom & Mgmt SudParis)
	Sasitharan BALASUBRAMANIAM	Docteur (TSSG, Irlande)
	Romain DURAND	Chercheur Director R&D (Transatel)

Acknowledgments

First of all, I would like to express my deepest sense of gratitude to my supervisor, Prof. Nazim AGOULMINE, for his guidance, encouragement and excellent advice throughout my research work.

I am thankful to the members of my thesis committee, Mikael SALAUN, Josef NOLL, Hossam AFIFI, Sasitharan BALASUBRAMANIAM, Romain DURAND for the time and effort that they invested in judging the contents of my thesis.

I am pleased to thank all my colleagues at Networks and Multimedia Systems Research Group (LRSM) for their support and their comradeship; especially to Mehdi Nafa, Elyes Lehtihet, Yacine Ghamri Doudane and Quoc Thinh Nguyen, who worked closely with me in Polymage, SEIMONET and SUMO projects.

Finally, I take this opportunity to express my profound gratitude to my beloved parents and sister for their invaluable love and support throughout the years. I cannot thank you enough for your unwavering support, encouragement, and for always believing in me.

Lastly, I would like to thank my fiancé, for her love, encouragement and patience.

Abstract

The future telecom ecosystem will be composed by a set of heterogeneous wireless and cellular networks and user terminal capable to connect and communicate with any of these networks. This thesis contributes for evolution of convergence of wireless heterogeneous networks and to propose novel mechanisms to support low latency handover at authentication level using network selection, security context management and mobility in future telecom ecosystem to allow ubiquitous access to the Internet and services to any individual on the move. This access should be possible anytime anywhere while ensuring the right level of security to the end users as well to the networks.

One main objective of the thesis is to define seamless secured roaming mechanisms to enable subscribers or users to roam along different access networks indifferent of access technologies, operators and accessing mechanisms. The proposed thesis provides a roaming & interworking solution using intermediary entity, called Roaming Interworking Intermediary (RII), which enable the secure handover across different access systems and different operator domains without service interruption. RII acts like a broker in the RII architecture between home and visited operator networks. RII provides mobility management, context transfer between service providers, security architecture for authentication and associations of users while roaming, network and presence management.

The thesis also defines new mechanisms to enable low latency during handovers and roaming by optimizing and introducing new authentication and mobility models (post handover techniques) in heterogeneous networks. We have provided new methods to solve ever longing issue of user identity and routing of user authentication information from visiting access networks with or without a direct SLA with the home network. We have introduced dynamic authentication model with the proposed RII architecture where a user or subscriber gets authenticated at the visiting network without re-routing authentication information to home networks. The thesis also propose a new mobility mechanisms based on Proxy Mobile IP and extending AAA infrastructure to obtain very low latency during handover in WLAN, WIMAX and 3G networks. Testbeds and comparative studies between proposed and existing models for authentication and mobility are provided.

This thesis also provides novel pre handover techniques in heterogeneous networks to ensure seamless handover during mobility and roaming. This method is a network centric approach where the access networks controls whole procedures of network selection, security, mobility etc… with the help of mobile terminals and visiting networks. Therefore, new models for location prediction based Network selection, security context management for authentications, context based mobility models are proposed in this thesis. New supporting protocols and extensions of existing protocol to achieve seamless handovers are proposed in this work. A full testbed is built with the implementation of the proposed protocols to evaluate the proposed of the efficiency of the proposed mechanisms.

Résumé

Écosystèmes de télécommunications seront composés, dans le futur, de plusieurs réseaux hétérogènes, réseaux sans fil et réseaux cellulaires, et un terminal d'utilisateur qui est capable de se connecter et de se communiquer à travers ces réseaux. Cette thèse contribue pour l'évolution de convergence dans les réseaux hétérogènes sans fil ainsi que de proposer des nouveaux mécanismes afin de permettre de délai bas pendant le « handover » au niveau de l'authentification en utilisant la sélection de réseau, l'administration de sécurité et la mobilité dans les futurs écosystèmes de télécommunications pour permettre un accès ubiquité à Internet et aussi à des services en cas de mobilité. Cet accès doit être disponible tout le temps et partout en assurant le bon niveau de sécurité pour les utilisateurs ainsi que pour les réseaux.

Un objectif principal de cette thèse est de définir des mécanismes pour « seamless secured roaming » afin que les abonnés ou les utilisateurs soient capable de se promener entre différents réseaux d'accès qui implémente des technologies et des mécanismes d'accès similaires. La thèse présentée propose une solution de roaming et interopérabilité en utilisant des entités intermédiaires qu'on appelle « Roaming Interworking Intermediary (RII) ». Ces entités permettent un « handover » sûr à travers des différents systèmes d'accès et différents opérateurs sans interruption de service. RII agit comme un agent dans l'architecture RII entre le réseau d'origine et le réseau d'opérateur visité. RII permet l'administration de la mobilité, le transfert entre les fournisseurs de service, l'architecture de sécurité pour l'authentification et les associations d'utilisateurs en parcourant, aussi l'administration de réseau et de présence.

Cette thèse définit, aussi, des nouveaux mécanismes qui permettent des délais bas pendant les « handovers » et « roaming » en optimisant et présentant des nouveaux modèles d'authentification et de mobilité (post hanover techniques) dans les réseaux hétérogènes. Nous avons présenté de nouvelles méthodes afin de résoudre le problème de longues périodes d'identité d'utilisateur et de routage des informations d'authentification d'utilisateur dans les réseaux d'accès visités avec ou sans SLA direct avec le réseau d'origine. Nous avons développé un modèle d'authentification dynamique en utilisant l'architecture de RII proposé, où un utilisateur ou un abonné est authentifiés au réseau de visite sans besoin de router des informations authentiques aux réseaux d'origine. Cette thèse propose aussi des nouveaux mécanismes de mobilité basés sur « Proxy IP Mobile » et étend l'infrastructure d'AAA pour obtenir des délais très bas pendant le « handover » dans les réseaux WLAN, WIMAX et 3G. Des études comparatives, entre les modèles proposés et existants, concernant l'authentification et la mobilité sont effectuées à travers des plate-forme réelles.

La thèse propose aussi des techniques pré-hanover dans les réseaux hétérogènes pour garantir « seamless handover » pendant la mobilité et le « roaming ». Cette approche est une approche focalisée réseau où les réseaux d’accès contrôlent tous les procédures comme la sélection de réseau, la sécurité, la mobilité etc … avec l'aide des terminaux mobiles et des réseaux de visite. Donc, de nouveaux modèles pour la sélection de réseau basés sur la prédiction, l'administration de sécurité pour les authentifications, et des modèles de mobilité sont proposés dans cette thèse. De nouveaux protocoles et des extensions pour le protocole existant afin d’accomplir le « seamless handover » sont proposés dans ce travail. Une plate-forme réelle et complète était construite avec l'implémentation des protocoles proposés pour évaluer l'efficacité des mécanismes proposés.

List of tables

List of figures

Table of content

Chapter 1. Introduction

With the rapid growth of the Internet, multimodal representation and interactive facilities of multimedia-based services, the current wireless technology is burgeoning in every aspect of human life ranging from home, education, medicine, e-commerce and m-commerce etc... The advent of ubiquitous computing and the proliferation of portable computing devices have raised the importance of mobile and wireless networking. Today, almost every network technology is prepared or even explicitly designed to transport IP-packets. Within this heterogeneous and future-oriented context, users will probably have mobile terminals with several different physical interfaces at their disposal. To meet the ever-increasing consumer demands the mobile networks have evolved from 1G to 4G. Future users are provided with different and diverse services at anytime and anywhere during mobility or stationary with a cost efficiency for operators and as well as users. Wireless networks with the interoperable can integrate with other networks and fixed networks providing seamless mobility and services in the heterogeneous networks. The next generation of mobile networks (4G) should be more open and opportunistic in its radio access network choice. It should incorporate the heterogeneous access networks and connect these to a native IP-backbone.

The main objective of the future networks is to provide users with always best connectivity through available different access networks even the user is on move. There are different interworking scenarios where the users are provided with different services during roaming and handover scenarios. Handover is the mechanisms by which terminal maintains its connectivity with an operator network during mobility while the roaming is the the mechanisms by which a user could still use its services from a foreign operator access network. Today the roaming mechanisms are only in one network, an operator can deploy different technologies and therefore handovers between these technologies must be transparent to users, allowing a simplified and seamless on-the-move experience. Hence this transparent handover should be extended to allow user terminals to maintain their connectivity on the mover between different administrative domains (named roaming). However, this implies much more complex mechanisms than of the handover in a unique administrative domain. In summary, 'seamless mobility is predicated on enabling a user to accomplish his or her tasks without regard to technology, administrative domain, type of media, or device, facilitating freedom of movement while maintaining continuity of applications experience'.

This thesis contributes to the evolution of the convergence between different access technologies and networks and different administrative domains. Also this thesis provides different aspects of handover to improve inter systems roaming and handover to ensure seamless mobility and therefore increasing the user experience. The different solutions that are proposed have been specified, developed and validated through different testbeds and simulations. **The work presented in this thesis is the contribution of the author which is performed for the duration of three years.**

1.1. Motivation

Having emerged for more than 10 years, Internet is now experiencing a migration from narrowband to broadband due to increasing demand on advanced data services such as streaming videos and online gaming. Broadband captures significant interests from both IT and telecommunication industries. An interesting tendency perceived in telecommunication world is the convergence of different technologies. The industry has recognized that in order to maximize the user experience, it is essential to mix different technologies in an optimized way. Mobile networks, wireless networks, broadcasting networks and broadband technologies have converged in a way that allows more diverse and appealing services and applications delivering to customers. The convergence of mobile networks and broadband promotes the emergence of 3G whose maximum speed is up to 2Mbps. The convergence of mobile networks and broadcasting networks generates a whole new domains and different range of applications.

Users require more advanced data services; additionally, they also expect to be connected and communicate anywhere, anytime by means of different technologies and networks. Technology convergence and Seamless Mobility are quite dependent and the core logic behind them is identical, it would be very interesting to explore into this innovative and promising arena. Seamless Mobility will be an ever ongoing and improved process, and it must be achieved step by step due to challenges from both technology and market perspectives. The first seamless mobility application that has been commercial is the Unlicensed Mobile Access (UMA) solution, allowing seamless handover between cellular and WiFi hot-spot for voice call services. However, the UMA technology has some drawbacks. It does not ensure the Quality of Service (QoS) of multi-service bearer and the handover between Universal Mobile Telecommunications Service (UMTS) and WLAN has not been yet supported. This solution is only suitable for home or SOHO (Small Office and Home Office) subscribers due to the access capacity limitations. Though the inter-system mobility has attracted immense research and development efforts from the research community and standardization bodies, the seamless handover does not really happen due to many issues related to the different facets of the inter-system mobility management complexity.

Wireless technologies provide extensible service coverage by using adjacent cells, each one contain a radio transceiver known as point of attachment (PoA) in order to serve the mobile nodes (MN) in their coverage areas. MNs may need to change their PoA to the network while moving in order to keep a suitable radio link quality; this process is called handover, where as this handover is provided in the different operator networks then it's known as roaming, the handover between two access nodes of two different technologies is called Vertical handover. Vertical handover is an issue in heterogeneous networks since each technology has its own mobility management (including security management) solution. The mobile terminal must be capable of adapting the communication parameters (and sometime also the service content) each time it changes access network. The two most considered performance criteria for the handover design are latency and packet loss. Generally, multimedia applications, one of main services in 4G networks, require a short handover latency, low jitter and minimal packet loss. Handover is required to be achieved seamlessly. It means that handover is transparent to user's experience: users do not recognize handover occurrences at the application perception. Technically, it means that the handover interruption delay should be very small (below 50ms) and the packet loss ratio should small enough to not affect the service. Users want to have a continuous and qualified service and they do not care about which access technology they have connected, whether the network belongs to its home operator or not, which security mechanisms are used, etc.

1.2. Seamless Roaming requirements from the users and networks perspectives

Clearly, different requirements have to be fulfilled at various levels of the system to achieve seamless roaming. These requirements form a basis for the operation mode of services in multi access technology networks from the perspective of users as well as operators.

1.2.1. Requirements from user's perspective

User satisfaction is crucial for mobile and wireless network operator's providing the services they want, almost anywhere at any times at a good price and the required quality. On the other hand, user's and network operator security requirements should be fulfilled; This is a basic prerequisite to mobile network operators. Any compromise of security that has an effect on user's assets may finally turn out to be a serious problem for mobile and wireless network operators. Security requirements of future integrated wireless networks can be categorized as terminal security and access network security. The security provided at the mobile station is called terminal security in which mobile terminal is an important asset of user. Secure user's assets are an important part of the goal of security architecture of future systems. This is a task of not only for mobile network operators but also manufactures, regulatory bodies and other participants in future environments.

Due to high competition, the mobile network operator will usually enhance its service provision (capacity, quality, variety, etc. of services) to satisfy its customers, possibly by cooperating with other business partners that can be service providers or other network operators. A future integrated mobile and wireless network will also be more open to 3rd parties that provide services independently. Security mechanisms and services should also be intelligible and easy to use. Besides the direct requirements from users, some requirements which are related to operation side should be considered in system design, too. Security mechanisms should be either transparent to users, or sufficiently usable, i.e. without any difficulty or inconvenience for users. Simple operation is much preferable to users otherwise the mechanism may fail because of user's reluctance to use it. Security mechanisms should not compromise service quality apparently, otherwise business competence will be hindered and more important, the mechanisms may be bypassed. Providing users with a chance to choose between different levels of security through technical configuration may not be a good idea, because inappropriate configurations, which can happen for large number of users, may be exploited by attackers, and normally leads to serious influence on marketing. On the other hand, customer support, like education and consulting are very expensive.

Other than security, the other hindering issues are mobility/roaming and quality of service. Due to availability of numerous access technologies at the user's vicinity that belongs to different operators the users cannot identify at every instance which is the best operated network to access and use the services. There must be an architecture where the network has to configure the terminal to access these networks with a cost effective way. When the users moves from one network to another there will be discontinuity of services, the terminal has to cope with changes when the user moves and has trigger mechanisms where the services has to maintain seamlessly the services when there is mobility or roaming of users. Quality of service is a main issue where the users have to be provided better services without overloading the network and cost. In the future networks the users are provided with numerous services ranging from VoIP to VoD services. At any given instance users must not experience defective services, the networks architecture should be designed in a way that quality is controlled and users are served according to their QoS requirements.

1.2.2. Requirements from network's perspective

Heterogeneous networks means combination of different network technology and possibly opening the mobile network operators' 'managed/controlled' network to the Internet which is not under control of anyone. This, besides the general security requirements for a network, brings several new security issues. Secure attachment and detachment to/from network must be provided. This is to prevent unauthorized user from accessing the network or making use of the connection of a detaching user. Access control to various services or network elements must be provided by the operator. The allowed level extent of access should also be decided. Trust relationship should be built between different networks to which a user might move to. This is applicable to both homogeneous and heterogeneous networks. The network must have good accounting mechanism to charge correctly to users, this is both for the benefit of the user as well as the mobile network operator.

In general the operator should have infrastructure security which prevents tampering of the network and its elements. Denial of service attack is easily possible in wireless medium, although not easy to prevent in current systems, methods should be sought for future systems to prevent such attacks. Changes in wireless medium requires adaptation in physical and MAC (medium access control) layers, this should not compromise security. Rogue base stations are also a threat; to prevent this, the mobile network operator should have mechanisms that will identify such base stations and thus protect the users. Mobile network operators should also watch out against service or content providers making illegal use of the network. Operations and management of security solutions must be possible and relatively simple.

Due to availability of multiple access technologies and different operator networks the networks has to assists the user to identify the best networks at that given instance. This selection of networks has to be dynamic and has to take into account number of issues. The Handover management is another concept come into existence to handle roaming or mobility of users from access networks or technologies. Handover management guides the networks and users to follow procedures and mechanisms to ensure seamless transition of services to users during roaming or mobility. The networks have to design this handover management to ensure all the procedures during roaming and to ensure secured seamless mobility in access networks during handover. When the mobile terminal moves from one access network to another the networks, generally users looses the sessions, mobility mechanisms in network must ensure that these sessions are not lost, these mechanisms must ensure the information after roaming is forwarded to users even if they are in another access networks.

1.2.3. Requirements from service's perspective

In future the number of network operators will increase and thus a service that can be provided is openness towards each other which will create positive perception for users. Having openness brings forward several security requirements, level and building trust relationship being one of them. Service should be provided to the specified set of users (authentication), according to the contractual obligation agreed (authorization) and the usage should be accountable. Rogue service or content providers can appear and methods must be developed to deter them. Secure access to services, from any partner, should be provided. The operator should take care that the service providers are correctly charged or if the service provider is paying the operator then the operator should take care that he bills the service provider correctly. Since cooperation with many other service providers are expected in the future communication and service provision systems, non-repudiation will be much important between operators and service providers to prevent and combat frauds. However, appropriate business models may be more efficient than technology means. The provided services must adapt to different environments and terminals, the services must adapt to availability of bandwidth which is called as content adaptive services some of the examples involved are opera mini browser for mobile terminals.

1.3. Issues to be resolved to achieve seamless roaming

There are several issues which have to be resolved to achieve seamless mobility which are mentioned below. Due to the utilization of multiple access technology for access and operating mechanisms and techniques the complexity multiplies. The following section details brief description of issues that arise integrating different possible heterogeneous wireless access networks.

- *Multi User Mode terminals:* To design a single user terminal that can operate in different wireless networks and overcome the design problems such as device size, cost, power, and backward compatibilities.
- *Handover management:* handover management is a process of initiating and ensuring a seamless and lossless handover of a mobile terminal from a region covered by one base station (BS) to another BS, which may belong to a different access network (AN). Handover procedures involve a set of protocols to notify all related entities of a particular connection of which it has been executed.
- *Networks Discovery:* To discover wireless networks at any instance by processing the signals sent from different wireless technologies using different access protocols.
- *Network Selection:* Every wireless networks has its unique characteristics and roles. Wireless technologies provide extensible service coverage by using adjacent cells, each one containing a radio transceiver known as point of attachment (PoA) in order to serve the mobile nodes (MN) in their coverage areas. MNs may need to change their PoA while moving in order to maintain a suitable radio link quality; this process of choosing an access network is called network selection. The main objective of network selection is to identify different access networks and technologies at any given instance. Depending on SNR/RSS, BSSID, availability of bandwidth in the access networks, SLAs between operators, the NS procedure selects best available access network.
- *Terminal Mobility:* to locate and update the location of mobile terminal in various networks. Also to perform horizontal and vertical handover to obtain seamless mobility.
- *Security*: due to different access technologies, the security mechanisms to access these networks complicates. There is a need for light and dynamic security mechanisms to achieve seamless mobility. There is a need for a security mechanism to reuse keying materials derived in one technology to be used in another technology. Some of the security consideration includes access control on a mobile terminal that can be activated and used only by authorized user, terminal should be protected against virus, and network worms,

etc., and stolen terminals should be blocked to access networks. Security consideration during communications and data privacy includes security of voice and data communications, privacy of location, call setup information, user ID, call pattern, etc. and service usage privacy: unauthorized partners must not know which services are used by any specific user, its usage pattern and volume, etc. Security measures to include at service level involving service availability should be ensured to prevent or mitigate Denial of Service (DoS) attack, security against fraudulent service providers, e-commerce/m-commerce security.

- *Fault tolerance and survivability*: To minimize the failures and their potential impacts in any level of wireless networks.
- *Location and Presence management:* To provide location based services for the end users and maintain presence of the users for other management functions to provide access in the networks.
- *SLA and Network Management:* due to large density of access networks and operators the interworking of these networks, the SLAs between them gets complicated due to peer to peer agreements and managing these procedures does complicate and overload different procedures.
- *Billing:* to collect, manage, and store users accounting information from multiple service providers.
- Quality of Service: Future wireless network service quality will be the collective effect of the performance of all system elements in combination with the user expectations, which determines the degree of satisfaction of the users.. The operator's perspective is characterized by the customer service requirements, the customer perception of QoS, the offered QoS, and the actually delivered QoS. Customer QoS requirements are described on an end-to-end basis in terms of the operator networks service and are expressed in non-technical language. Beneath transmission parameters like data rate, customer requirements will also include availability. Furthermore, they will depend on the customer type, with business customers having the most stringent requirements for service availability and exceptional quality.

  Customer perception describes if and how the customer is satisfied with the received QoS. It is very much dependent on the user expectations rather than on objective parameters. This is a crucial issue for operators particularly when considering service deployment in unlicensed spectrum. Offered QoS is expressed in operator language and indicated on a per service basis. It should equate to the customer QoS requirements and may be mandated in a Service Level Agreement. Offered QoS represents a significant factor in forming the customers' expectations for future networks service quality, especially in the case of new innovative services. In the heterogeneous network environment, such performance indicators must address the access network due to its complexity, heterogeneous nature, lack of robustness (particularly when using unlicensed spectrum) and its role as an intrinsic bottleneck (finite radio spectrum). However, as the access network approaches the reliability of wire-line components, the core network will become a more significant factor in determining the delivered quality of service. From a technical point of view, QoS modeling and QoS signaling would be crucial factors for future systems that integrate heterogeneous network types. Suitable abstractions have to be found for different system layers and they have to be mapped onto each other to fulfill and dynamically adapt to the customer requirements. A multi-layer approach has to be taken for a comprehensive solution here.

1.4. Objective of thesis

The objective of the thesis is to propose new interworking mechanisms for seamless secured roaming in heterogeneous networks. In order to support the seamless mobility from one technology to another and one operator access network to another, the access networks involved should be integrated at the infrastructure level. The interworking between Third Generation Partners Project (3GPP) and Third Generation Partnership Project 2 (3GPP2) networks and WLAN networks has been the topic of much work within 3GPP/3GPP2 standardization bodies, a collaboration between groups of telecommunications associations, to make a globally applicable 3G mobile phone system specification within the scope of the International Telecommunication Union (ITU)'s International Mobile Telecommunications-2000 (IMT-2000) project. The UMA solution mentioned above is also recognized as a 3GPP Generic Access Network (GAN) standard. Since WiMAX is much different from WLAN in terms of radio coverage, QoS, capacity and security, the 3GPP/WiMAX/WLAN interworking needs more research efforts. The interworking architecture of different technologies must minimize changes to the existing infrastructure. Most of the existing mechanisms proposed in the research deals with the technologies dealt with the same operator, for true seamless mobility there is a need for interworking between different access networks operators.

Even though the existing solutions provides mobility in the interworking heterogeneous networks there are number of issues which have to be addressed such as network selection, low latency security handover etc… The handover management is a new issue which guides the mobility of users in access networks has to be defined. One of the objectives of the thesis is to provide access network centric handover management procedures to guide the user terminals to perform handover and roaming. Due to availability of number of access networks available at the user terminal vicinity, and based on user profiles network selection procedures has to be proposed. New mechanisms have to be developed to optimize the handover of users and adapt to different operating scenarios and technologies. In this process new security mechanism has to be proposed so that these can be operated across heterogeneous networks, and also mechanisms involving re-using the keying material generated in one access network into another access network. A new mobility solution has to be proposed which is compatible for all the access networks and providing low latency during handover and roaming. One of the goals of this thesis is to provide unified signaling protocol to provide context transfers from access networks to mobile terminals for mechanisms involving handover. New mechanisms has to be proposed where the access networks communicate each other during the mobility or before the mobility of the users to create the user mobility context and execute during handover to eliminate latency of handover/roaming in access networks. Due to complexity of interworking large number of networks a new management system has to be designed.

1.5. Methodology

The proposed approach is based on the concept of Roaming Intermediary Interworking (RII) platform which supports all combinations of different radio technologies in a multi-operator environment. The RII is expected to support secured roaming and seamless mobility across two independent operator networks. New entities are proposed in access networks called Local RII, Core RII and Global RII for WLAN/WIMAX and cellular networks. These entities support handover and roaming of users in access networks. These entities support different procedures involving network selection, authentication, authorization, mobility management, handover management, QoS and location/presence management. On overall we define total interworking system which handles every single aspect of handover and roaming. For maintaining these large numbers of access networks and operators a global entity involved Global RII does the network management, which creates the context and passes this information to other access networks.

During handover in heterogeneous multi operator networks there are different mechanisms involved which have to be efficiently controlled to achieve secured roaming. Existing security mechanisms provide limited support and latency involved is high. We propose new mechanisms where the context of user is transferred to different networks; later the users are authenticated directly without routing authentication information to home network. Issues of user identity management is the main issue in heterogeneous networks, we propose two methods to resolve this issue one is dynamic assignment of identity to users when they are roaming in other networks, and the other is static where the context is created in the home network, and passed to user terminal these context contains duplicate IDs assigned to user according to the SLA which have to be utilized in the visiting networks. Using these mechanisms we have observed considerable less latency than the other models by validating through tested. A new mobility mechanism is also proposed for heterogeneous networks. In this mechanism the mobility of the users are maintained on the access network side. This mechanism uses mobility context transfer from one access network to another dynamically, when the user terminal initiated authentication. After successful transfer the entities of visiting network and home networks negotiate and establish a session for the user. The protocols involved in the mobility procedures are proposed developed and validated through testbed.

We also propose new mechanisms based on network centric handover management of users in access networks. The general procedure involve in this mechanism is the context of the user is created for different procedures by negotiating with the future visiting networks (pre handover mechanisms). We have proposed new techniques and algorithms involved to achieve this goal. All the procedures involved starting from network selection to presence management is handled using this mechanism. This is the most efficient solution as the whole procedure is involved is maintained by access networks in this way by reducing the processing and data collection from entities in terminal is reduced. And also most of the procedure in handover such as Network selection, security, mobility context and QoS negotiation is performed before the mobile node visits the future network, the overall latency involved is reduced drastically than any other procedures existing solutions. A unified signaling protocol is proposed to transport the context created in different processes involved in the proposed solution. We also proposed a new roaming protocol where the access networks communicate to create, negotiate and transferring the context during handover dynamically. Simulation models and testbeds have to be developed to validate the efficiency of proposed solution through results.

In short, the objective of the thesis is to propose and optimize the inter-system handover and roaming procedures between WLAN, WIMAX and cellular networks, by addressing the aspects of interworking and roaming architecture, network selection, security management, mobility management, QoS, handover management.

1.6. Outline

The picture shown below provides the structure of the proposed thesis which is outlined below.

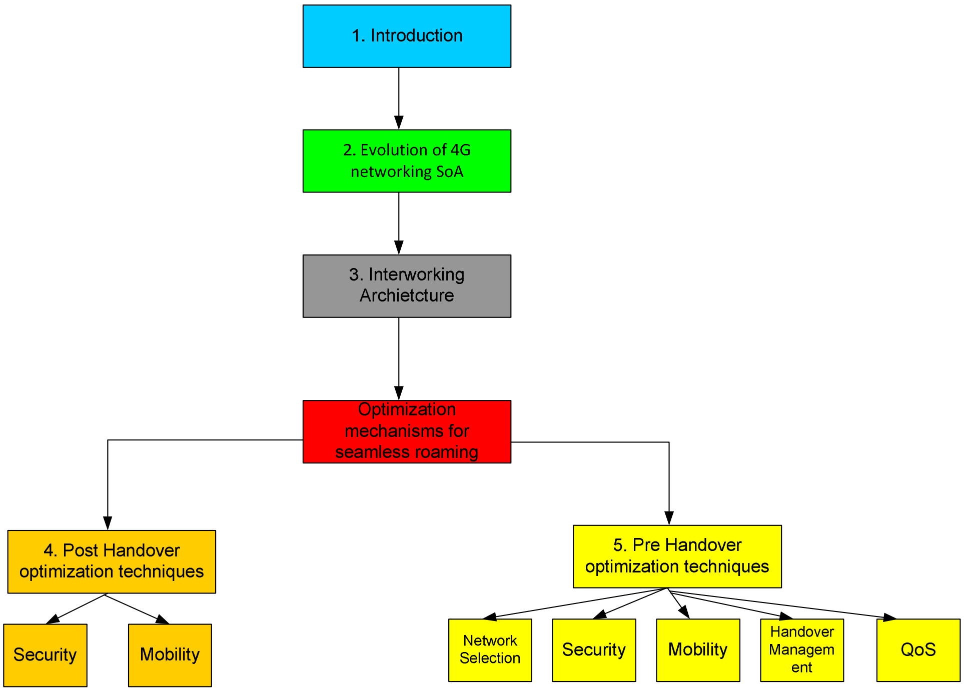

1. Introduction
2. Evolution of 4G networking SoA
3. Interworking Archietcture
Optimization mechanisms for seamless roaming
4. Post Handover optimization techniques
Security
Mobility
5. Pre Handover optimization techniques
Network Selection
Security
Mobility
Handover Managem ent
QoS

Figure 1. Thesis Outline

Chapter 1 **Introduction**: This chapter outlines the problem statement, issues of seamless roaming and interworking, requirements from user, network and service perspective, objective and approaches. This chapter proposes scope of the overall thesis.

Chapter 2 **Evolution of 4G networking and underlying methods for seamless roaming**: This chapter reviews underlying mechanisms for the evolution of wireless and cellular networks. This chapter provides basis for convergence of wireless and cellular networks. We provide information of existing interworking techniques available in the literature and in standardization. This chapter also provides mechanisms for security and mobility for wireless and cellular networks. Overall this chapter concludes the existing research for interworking and seamless roaming and issues which are still to be addressed for seamless roaming.

Chapter 3 **Roaming Intermediary Interworking Architecture RII: This** chapter proposes an interworking system called RII to support interworking in WLAN, WIMAX and cellular networks. This chapter highlights the issues of interworking to be solved that lacks in standard mechanisms, and proposes new interworking architecture RII. Components and mechanisms involved in the architecture are discussed. Issues of security, NS, Mobility etc... are presented. Detailed message exchanges between components are highlighted. Finally testbed has been presented to evaluate the proposed mechanism using WLAN, WIMAX and live 3G network. This chapter also presents location and presence management with the live services in this chapter. To manage and update the components dynamically we have introduced ontology based network management in the RII architecture.

For optimization of handover for seamless roaming we have introduced new mechanisms and techniques, which can be characterized into two parts; post handover techniques and pre handover techniques.

Chapter 4 **Post handover techniques for optimization of handover and roaming**: this chapter proposed new mechanisms for optimizing handover and roaming. It introduces novel mechanisms for security; using this mechanism the authentication delay of users during handover is reduced. Issues of user identity management are discussed in this chapter. Furthermore it proposes new mobility models and extended one model to reduce latency during handover in WLAN, WIMAX and 3G networks. To validate the proposed mechanisms a testbed has been developed and presented in this chapter.

Chapter 5 **Pre handover techniques for optimization of handover and roaming**: this chapter proposes new mechanisms based on network centric handover management of users through operator networks. This solution is based on creating the context for various entities such as NS, Security, mobility, QoS etc.. before the mobile node moves to another network. Various mechanisms involved in this process such as NS are explained in detailed. The proposed algorithms validated through simulations and testbeds using WLAN, WIMAX and 3G networks.

Chapter 6 **Conclusions:** The final chapter provides summary of the thesis, discusses open issues and further research directions.

Annex I: Various WIMAX studies are presented in this section. Performance analysis of WIMAX networks is presented. Multimedia models and analytical models for IPTV on WIMAX is presented here. New mechanisms involved WIMAX networks operating in mesh and integrated with WLAN are presented. Testbeds and results are presented in this section.

Chapter 2. Evolution of 4G networking and underlying methods for seamless roaming

This chapter presents state of the art of evolution of cellular and mobile technologies toward 4G mobile networking. In this chapter we will describe a detailed analysis of cellular and mobile networks. We also provide details of interworking and roaming technologies, and undermining techniques to obtain seamless mobility. These details provided here forms the basis for seamless roaming solutions for heterogeneous networks.

2.1. Evolution of cellular and wireless networks

2.1.1. Roadway for cellular networks

The cellular concept was first used in the AMPS in the United States. As a first generation of cellular systems, AMPS is a FDMA-based analog system. The 2G of cellular systems uses digital technologies. Two interim standards, IS-95 (CDMA-based) and IS-136 (TDMA based), are used in the United States, and TDMA-based GSM is used in European countries. It is clear that the 3G of cellular systems will be CDMA-based. However, the GSM community is developing WCDMA to be backward compatible with GSM while the CDMA community tries to evolve CDMA into CDMA2000.

2.1.1.1. 1G

In the late 1970s and early 1980s, AT&T Bell Laboratories developed the AMPS, which was the first-generation cellular system used in the United States (Rappaport, 2002; Young, 1979). 1G was indeed a major innovation in the telecommunication history. However, it was prone to the problems of quality of transmissions, security and inefficient utilization of the spectrum and capacity of available frequencies.

2.1.1.2. 2G

2G networks currently provides services vast majority of users, it introduces digital circuit switched technology using spectrum more efficient manner than 1G technology. 2G networks consists of IS-54, IS-136, GSM, cdmaone [1].

IS-54: To overcome the limited capacity of AMPS, especially in large cities, D-AMPS (IS-54) was developed in the early 1990s (EIA/TIA, 1990). D-AMPS inherited a lot of features from AMPS. Specifically, in D-AMPS, the same AMPS allocation of frequency spectrum is used, and each channel is still 30 kHz wide. However, in D-AMPS, a 30- kHz channel can be shared by three users through the 2G TDMA digital technology. In a typical D-AMPS cell, some of the 30-kHz channels are assigned for analog AMPS traffic, whereas the others are for digital TDMA traffic. It means that D-AMPS allows a service provider to migrate from the first-generation analog technology to the 2G digital technology on a gradual basis.

IS-136: another prominent TDMA-based cellular system in the United States, is built on D-AMPS. Whereas DAMPS provides dual-mode operations (both analog and digital), IS-136 provide pure digital operations. All the 30- kHz channels are shared by three users via TDMA digital technology. In addition, unlike D-AMPS, IS-136 also uses the digital control channels. IS-136 was initially developed on the 800-MHz cellular spectrum. It can be adopted onto the 1900-MHz PCS spectrum.

GSM: was first developed for Europe in the 900-MHz band (GSM 900), then expanded to the 1800-MHz band (1710–1880 MHz), which is named DCS 1800, and later renamed to GSM 1800. GSM uses the TDMA digital technology. The allocated spectrum is divided into multiple channels of 200 kHz using FDMA, and each 200-kHz channel is shared by as many as eight users using TDMA. The North America version of GSM is called PCS 1900 because of its use of the 1900-MHz PCS spectrum. One feature of GSM worth mentioning is the SIM card that can be inserted into a cellular phone to provide the owner's identity information.

CdmaOne: refers to the original ITU IS-95 using Code Division Multiple Access (CDMA) that was first standardized in 1993. Today, there are two versions of IS-95, called IS-95A and IS-95B. IS-95A employs FDD with a channel bandwidth of 1.25-MHz for each direction, and supports data speeds of up to 14.4Kbps. IS-95B can support data speeds of up to 115 Kbps by bundling up to eight channels. Due to its supportable data speeds, IS-95B is categorized as a 2.5G technology.

2.1.1.3. 2.5G

2.5G provides enhanced data services coupled with 2G networks. General Packet Radio Service (GPRS) is a 2.5G technology providing enhanced services for GSM and IS-136 users. GPRS utilizes packet switched technology providing data rates of up to 172 kbps. Enhanced Data rates for Global Evolution (EDGE), Enhanced GPRS (EGPRS), or IMT Single Carrier (IMT-SC) is a 2.75G backwards-compatible digital mobile phone technology that allows improved data transmission rates of 384kbps. By using EDGE, operators can handle three times more subscribers than with GPRS, triple their data rate per subscriber, or add extra capacity to their voice communications.

2.1.1.4. 3G

3G is the third generation of mobile phone standards and technology [2], it enables network operators to offer users a wider range of more advanced services while achieving greater network capacity through improved spectral efficiency. There is a range of technologies for 3G, all based around CDMA, including UMTS (with both FDD and TDD variants), CDMA2000 and Time Division - Synchronous Code Division Multiple Access (TD-SCDMA).

Universal Mobile Telecommunications System (UMTS) is one of the third-generation (3G) technology uses Wideband Code Division Multiple Access (WCDMA) as the underlying air interface. The user data rate under real conditions can come closer to 384 kbps, to improve the performance of 3G UMTS, two standards High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA), jointly known as HSPA, have been developed. HSPA is usually referred to as a 3.5G technology.

HSDPA [3] is a packet-based data service feature of the WCDMA standard that provides improved downlink data rates. The theoretical peak rate is 14.4Mbps, but the realistic end-user experience is initially likely to be 1.8Mbps or possibly up to 3.6Mbps.

HSUPA delivers substantial improvements in uplink data rates and QoS as well. The HSUPA standard enables users to transmit data upstream at a speed of 5.8Mbps.

CDMA2000, direct successor to 2G CdmaOne, represents an entire family of technologies, including CDMA2000 1xRTT (Radio Transmission Technology), CDMA2000 EVDO (Evolution-Data Optimized), and CDMA2000 EV-DV (Evolution- Data and Voice), standardized by 3GPP2. CDMA2000 is the 3G technology chosen by most CDMA mobile network operators.

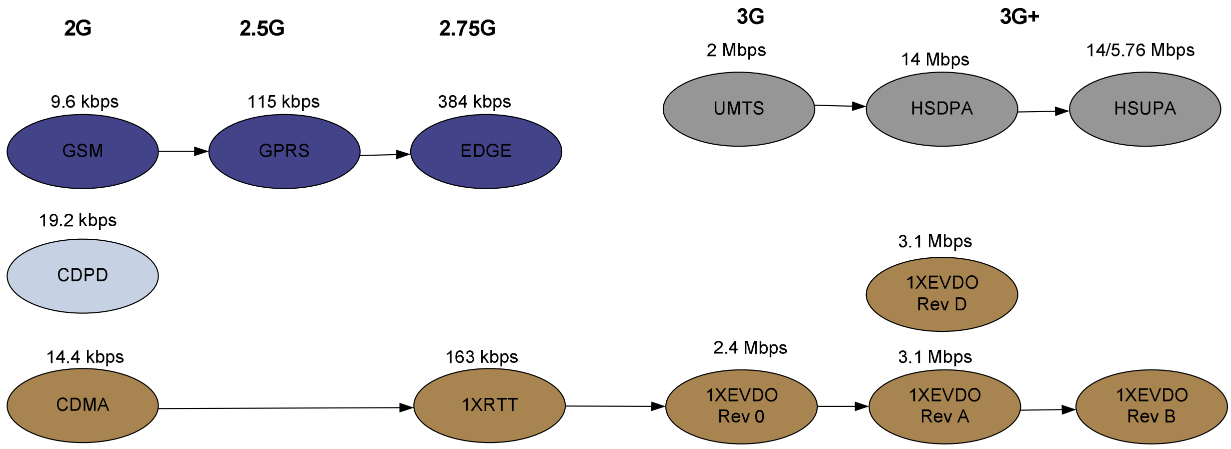


Figure 2. Evolution of Cellular Networks

2.1.2. Pre 4G

Long Term Evolution (LTE) and Ultra-Mobile Broadband (UMB) are intended to be a so-called fourth-generation technology. These technologies use a high bandwidth, low latency, underlying TCP/IP network with high level services such as voice built on top. While no 4G networks have been deployed yet, the much greater amount of bandwidth, and much lower latencies, should enable the use of various application types that have previously been impossible, while continuing to deliver high quality (or higher quality) voice services. The improved bandwidths of the network provided by more efficient technologies may also result in networks with better capacity.

LTE: 3GPP Long-Term Evolution is the next version of the 3GPP-based radio standard [4]. LTE is designed to provide higher data-rate (over 100 Mbps for downlink, and over 50 Mbps for uplink for every 20 MHz of spectrum), lower-latency and packet-optimized system compared to 3G. To this end, LTE uses Orthogonal Frequency Division Multiple Access (OFDMA) for the downlink and Single Carrier Frequency Division Multiple Access (SC-FDMA) for the uplink and employs Multiple-Input Multiple-Output (MIMO) with up to four antennas per station. 3GPP has recently reported LTE's peak theoretical downlink throughput rates of up to 326 Mbps in 2x20 MHz with 4x4 MIMO configuration. LTE is designed to be all-IP and to support mobility and service continuity between heterogeneous access networks.

UMB: 3GPP2 Ultra Mobile Broadband is the successor to CDMA2000 EV-DO, formerly known as EV-DO Revision C [5] UMB also incorporates OFDMA, MIMO and Space Division Multiple Access (SDMA) advanced antenna techniques to provide even greater capacity, coverage, and QoS. UMB can support peak download speeds as high as 280 Mbps in a mobile environment and over 75 Mbps for upstream transmission (with 4x4 MIMO configuration).

2.2. Wireless technologies evolution

2.2.1. WLAN

The popular family of standards for wireless LAN environments IEEE 802.11 [6] has changed the face of networking, providing flexibility, connectivity and (limited) mobility for nomadic users and has eased low-cost deployments not available through conventional wired solutions:

- Enterprises deploy WLANs to reduce the cost of cabling and provide a rapid response to changes in demand and to share Internet connections, printers and peripherals and create backup connectivity solutions while remaining highly scalable and flexible.

- Nomadic workers use public WLAN networks in remote corporate sites to connect to the corporate network or to Internet.
- Home users use a WLAN network to share a broadband Internet connection among multiple PCs without installing cabling throughout the home.
- Operators exploit WLAN for nomadic use.

The family of standards keeps evolving in order to meet users needs.

Initially the IEEE 802.11 standard was developed to provide up to 2Mbps in the 2,4GHz band. The need for higher throughput has become a key issue in all sectors of the telecom industry and as a result the IEEE 802.11a [7] and IEEE802.11b [8] standards were developed. The former supplies 54Mbps in the 5GHz licensed band. The latter runs in the 2,4 GHz unlicensed band but it provides a lower maximum throughput, up to 11 Mbps, which may not be enough for some user requirements.

By the time IEEE 802.11b standard was firmly established, the IEEE 802.11g [9] standard had been made available, to offer the same throughput as IEEE 802.11a but in the same band as, and ensuring backwards compatibility with IEEE 802.11b. One of the main differences between the IEEE 802.11b and the IEEE 802.11g standards is that the first one uses single carrier transmission whereas the second employs OFDM multi carrier transmission, what makes it more resistant to multi-path propagation. A summary of the IEEE 802.11 standards family is given below.

- 802.11: ratified in 1999 to operate in the 2,4GHz band with maximum data rates of 2Mbps. It includes data rates of 1 and 2Mbps, depending on the distance to the user and channel conditions, using Direct Sequence Spread Spectrum (DSSS) and Frequency Hoping Spread Spectrum (FHSS) MAC, and Differential Binary Phase Shift Keying (DBPSK), Differential Quadrature Phase Shift Keying (DQPSK) and Gaussian Frequency Shift Keying (GFSK) modulations.
- 802.11b: ratified in July 1999, 802.11b extends the original IEEE 802.11 Direct Sequence Spread Spectrum standard allowing the use of short physical preambles to operate up to 11Mbps in the 2,4GHz unlicensed band using Complementary Code Keying (CCK) modulation. Four data rates, 1, 2, 5,5 and 11Mbps, are specified on up to three non-overlapping channels, and the lowest two rates are also allowed on up to thirteen overlapping channels. **Status:** Final Approval: September 1999.
- 802.11a: ratified at the same time as the IEEE 802.11b, the IEEE 802.11a standard operates in the 5GHz licensed band. It was designed for higher bandwidth applications than those provided by IEEE 802.11b. It includes data rates of 6, 9, 12, 18, 24, 36, 48, 54Mbps using orthogonal frequency division multiplexing (OFDM) modulation on up to 12 discrete channels.

- 802.11g: in July 1999, the 802.11g subcommittee was charged with the task of providing throughput in excess of 20Mbps in the 2,4GHz band, maintaining compatibility with IEEE 802.11b. The resulting standard was ratified in June 2003. It provides optional data rates of up to 54Mbps, and backwards compatibility with 802.11b devices to protect investments in today's WLAN installations. It specifies OFDM (the same technology used in 802.11a but in the same spectrum as 802.11b) and CCK as mandatory modulation schemes with 24Mbps as the maximum mandatory data rate. It also provides optional higher data rates of 36, 48 and 54Mbps. 802.11g is also limited to the same three non-overlapping channels as 802.11b.

2.2.2. WIMAX

IEEE 802.16 [10] is a technology that provides broadband wireless access. WIMAX (Worldwide Interoperability for Microwave Access), the user-friendly name associated with the IEEE 802.16 standard, is an emerging wireless communication system that can provide broadband access with large-scale coverage. WIMAX is a disruptive technological breakthrough in the telecommunications sector, and will deliver personal broadband to enable users to access the Web, make telephone calls, watch videos and play music. In October 2007, WIMAX was approved as a 3G International Mobile Telecommunications (IMT)-2000 standard. This places WIMAX technology on equal footing with the legacy 3G technologies. It raises opportunities for global deployment of WIMAX, especially within 2.5-2.69GHz band, to deliver cost-effective broadband services to both rural and urban market demand. IEEE 802.16-2004, is a wireless metropolitan-area network (MAN) technology that provides interoperable, carrier-class broadband wireless connectivity to fixed, portable, and nomadic users for the last mile. It provides up to 30 miles of service area, allows users to get broadband connectivity without the need for a direct line of sight to the base station, and provides total data rates of up to 75 Mbps, enough bandwidth to support simultaneously hundreds of businesses and homes with a single base station. WIMAX has a basis in well-defined standards and industry interoperability right from the start. To support a profitable business model, operators and service providers need to sustain a mix of high-revenue business customers and high-volume residential subscribers. 802.16a helps meet this requirement by supporting differentiated service levels. The 802.16 specification also includes robust security features and the Quality of Service needed to support services that require low latency, such as voice and video.

By using a robust modulation scheme, IEEE 802.16 delivers high throughput at long ranges with a high level of spectral efficiency that is also tolerant for signal reflections. Dynamic adaptive modulation allows the base station to tradeoff throughput for range. For example, if the base station cannot establish a robust link to a distant subscriber using the highest order modulation scheme, 64 QAM (Quadrature Amplitude Modulation), the modulation order is reduced to 16 QAM or QPSK (Quadrature Phase Shift Keying), which reduces throughput and increases effective range.

The newer version of IEEE 802.16 is the IEEE 802.16e, also known as Mobile WIMAX. It is intended to enable a single base station to support both fixed and mobile BWA (Broadband Wireless Access). It aims to fill the gap between high data rate wireless local area networks (WLAN) and high mobility cellular wide area networks (WAN). It can be considered as the extension of the MAC and PHY of 802.16a. In order to couple with different channel conditions, this standard employs a scalable OFDMA system, which can scale the Fast Fourier Transform (FFT) size, depending on the channel conditions. The IEEE 802.16e standard also extends the FEC of the previous standard with an optional Convolutional Turbo Code (CTC). As IEEE 802.16e adds mobility, it must cope with two problems not faced by the previous standards: Power Saving and Handoff. Even though the industry is still waiting for mobile WIMAX certified products and the first 802.16e roll-out, the IEEE keeps working on new 802.16 amendments. Two most relevant amendments in progress are 802.16j (Multihop Relay) and 802.16m (Advanced Air Interface). The goal of 802.16m is to achieve data rates up to 1Gbps for fixed users and 100Mbps for mobile users. It aims to improve the capacity and performance of Multimedia Broadcast Multicast Service (MBMS) and Voice over IP (VoIP). The driver behind 802.16m will be MIMO antenna technology on top of an OFDM - based radio system. The 802.16m is comparable with the LTE or UMB in terms of technology, capacity and services. It is expected that the WIMAX 2.0 based on 802.16m will be ready at the end of 2009. Comparisons of 802.16 variations are presented in table 1.1.

	802.16	802.16a	802.16-2004	802.16e
Spectrum	10 to 66 GHz	<11GHz	10-66 GHz and<11GHz	<6GHz
Channel conditions	Line of sight only	Non line of sight	Non line of sight and Line of sight	Non line of sight
Bit Rate	120Mbps	75 Mbps	120Mbps	15 Mbps
Mobility	Fixed	Fixed	fixed	Mobile
Channel bandwidth	25 MHz or 28 MHz	1.25-20MHz	25 MHz or 28 MHz	1.25-20MHz
Typical cell radius	1 to 3 miles	3 to 5 miles	25 miles	1 to 3 miles

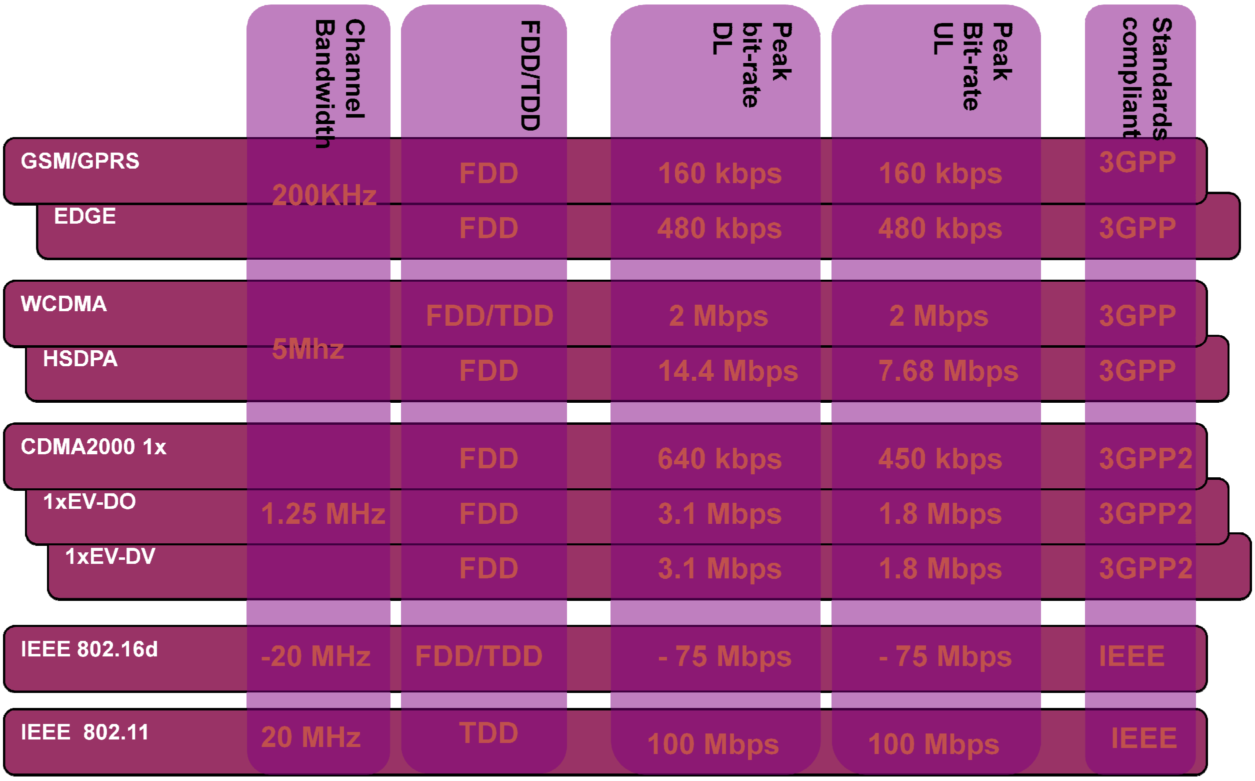
Table 1 IEEE802.16 variations comparison table

2.2.3. Broadband networks (IEEE 802.20)

IEEE 802.20 Mobile Broadband Wireless Access (MBWA) [11] is standard for broadband solution for vehicular mobility up to 250 km/h. The 802.20 standard was being positioned as an alternative to 3G cellular services since it can support high-speed handover and wireless network access. It is likely to be defined for operation below 3.5GHz to deliver peak user data rates in excess of 4Mbps and 1.2Mbps in the downlink and uplink respectively. At this point in time, the standard seems to be suspended owing to lack of consensus on technology and issues with the standardization process.

2.2.4. IEEE 802.22

IEEE 802.22 Wireless Regional Area Network (WRAN) [12] is a standard based on cognitive radio PHY/MAC/air interface utilizing white spaces (channels that are not already used) in the allocated TV frequency spectrum. IEEE 802.22 working group was formed in 2004, nothing has yet been specified regarding the particular functionalities of the PHY/MAC layers. 802.22 specifies that the network should operate in a point to multipoint basis (P2MP). The system will be formed by base stations (BS, above mentioned as Access Points, AP's) and customer-premises equipments (CPE). Figure 3 shows comparative study of Broadband and cellular networks.



	Channel Bandwidth	FDD/TDD	Peak bit-rate DL	Peak Bit-rate UL	Standards compliant
GSM/GPRS	200KHz	FDD	160 kbps	160 kbps	3GPP
EDGE		FDD	480 kbps	480 kbps	3GPP
WCDMA	5Mhz	FDD/TDD	2 Mbps	2 Mbps	3GPP
HSDPA		FDD	14.4 Mbps	7.68 Mbps	3GPP
CDMA2000 1x	1.25 MHz	FDD	640 kbps	450 kbps	3GPP2
1xEV-DO		FDD	3.1 Mbps	1.8 Mbps	3GPP2
1xEV-DV		FDD	3.1 Mbps	1.8 Mbps	3GPP2
IEEE 802.16d	-20 MHz	FDD/TDD	- 75 Mbps	- 75 Mbps	IEEE
IEEE 802.11	20 MHz	TDD	100 Mbps	100 Mbps	IEEE

Figure 3. Comparative study of Broadband and cellular networks.

2.3. 4G networks

2.3.1. Motivations for 4G networking

3G performance not sufficient to meet needs of future high-performance applications like multi-media, full-motion video, wireless teleconferencing. 3G is based on primarily a wide-area concept. We need hybrid networks that utilize both wireless LAN (hot spot) concept and cell or base-station wide area network design. There are multiple standards for 3G making it difficult to roam and interoperate across networks. There is a need for network technology that extends 3G capacity by an order of magnitude and also global mobility and service portability solutions to achieve seamless mobility. This solution has to provide wider bandwidth to provide different services efficiently. This future network must provide services in digital packet network that utilizes IP in its fullest form with converged voice and data capability. The solution has to utilize upmost frequencies available efficiently.

Lower Price Points Only Slightly Higher than Alternatives: The business visionaries should do some economic modeling before they start 4G hype on the same lines as 3G hype. They should understand that 4G data applications like streaming video must compete with very low cost wireline applications. The users would pay only a delta premium (not a multiple) for most wireless applications.

More Coordination Among Spectrum Regulators Around the World: Spectrum regulation bodies must get involved in guiding the researchers by indicating which frequency band might be used for 4G. Standardization of wireless networks in terms of modulation techniques, switching schemes and roaming is an absolute necessity for 4G.

A Voice-independent Business Justification Thinking: Business development and technology executives should not bias their business models by using voice channels as economic determinant for data applications.

Integration Across Different Network Topologies: Network architects must base their architecture on hybrid network concepts that integrates wireless wide area networks, wireless LANS (IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.15 and IEEE 802.16, Bluetooth with fiber-based Internet backbone. Broadband wireless networks must be a part of this integrated network architecture.

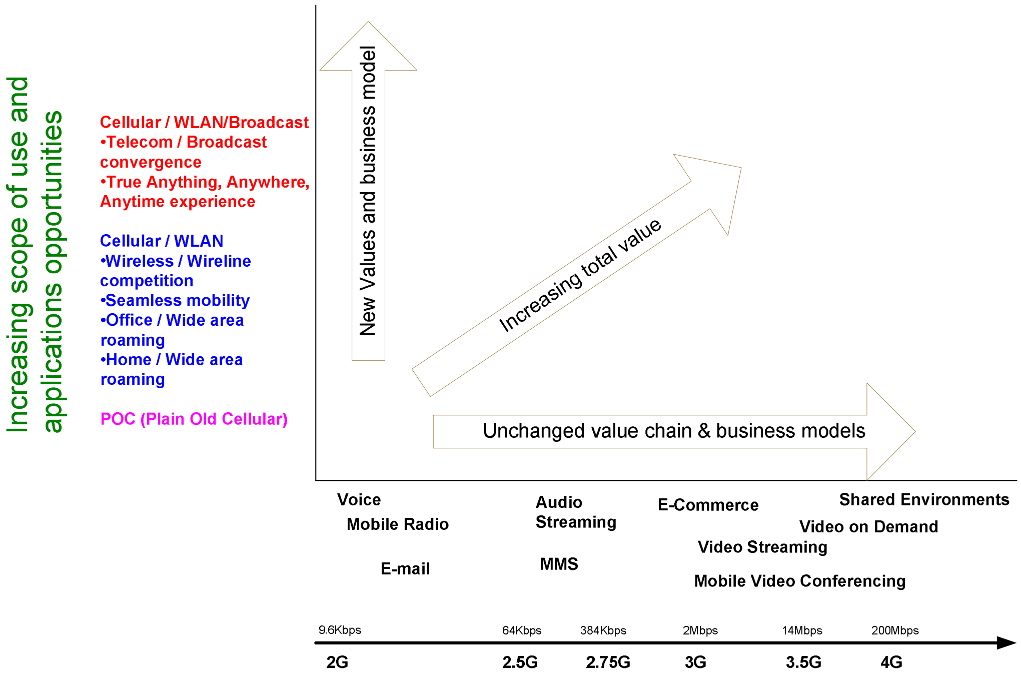

Increasing scope of use and applications opportunities
Cellular / WLAN/Broadcast
•Telecom / Broadcast convergence
•True Anything, Anywhere, Anytime experience
Cellular / WLAN
•Wireless / Wireline competition
•Seamless mobility
•Office / Wide area roaming
•Home / Wide area roaming
POC (Plain Old Cellular)
New Values and business model
Increasing total value
Unchanged value chain & business models
Voice
Mobile Radio
E-mail
Audio Streaming
MMS
E-Commerce
Video Streaming
Mobile Video Conferencing
Shared Environments
Video on Demand
9.6Kbps
64Kbps
384Kbps
2Mbps
14Mbps
200Mbps
2G
2.5G
2.75G
3G
3.5G
4G

Figure 4. Business model in the evolution of 4G networking

2.3.2. 4G networking

Unlike 1G, 2G and 3G, 4G is not a set of formally agreed end-to-end standards developed in the traditional top-down way that the telecommunications industry has used for years [13]. Third generation (3G) mobile networks have given emphasis on the development of a new network standard and hardware such as IMT2000, and the strategy to dynamically allocate frequency spectrum. The major hindrance for the introduction of 3G is the development of new technologies, and how to take away all frequencies from all countries and put them in a common pool. These problems are the main causes for the delay in the development of 3G networks. In spite of these, 3G can provide 2Mbps into a limited coverage area, that is, up to the macro (urban) cells. To solve these problems and to provide high speed transmission and wider coverage, fourth generation mobile networks have been targeted to develop as IP-core heterogeneous networks. It is expected to be commercially launched by around 2010. There are a number of characteristics of 4G networks from users', operators', and service providers' point of views. It is now widely accepted that 4G is a vision of an all-IP based, heterogeneous mobile broadband networks with multiple air interfaces, converged fixed-mobile networks, and multiple devices with multi-mode capabilities. 4G will provide end-users with an Always Best Connected (ABC) facility, low latency and high QoS broadband experience. The ABC means a seamless service provisioning across a multitude of wireless access systems and an optimum service delivery via the most appropriate available network. 4G will be a convergence platform providing clear advantages in terms of coverage, bandwidth and power consumption. 4G will ensure the seamless mobility and global roaming among various access technologies such as cellular networks, WiFi, WIMAX, satellite, Digital Video Broadcasting - Handheld (DVB-H).

4G services will be end-to-end QoS, high security, available at anytime, anywhere with seamless mobility, affordable cost, one billing, and fully personalized. 4G is about convergence, convergence of networks, of technologies, of applications and of services, to offer a personalized and pervasive network to the users. Convergence is heading towards an advent of a really exciting and disruptive concept of 4G. The 4G network will be an umbrella of multitude of technologies.

	3G (including 2.5G, sub3G)	**4G**
Major Requirement Driving Architecture	Predominantly voice driven and data was always add on	Converged data and voice over IP
Network Architecture	Wide area cell-based	Hybrid - Integration of Wireless LAN (WiFi, Bluetooth) and wide area
Speeds	384 Kbps to 2 Mbps	20 to 100 Mbps in mobile mode
Frequency Band	Dependent on country or continent (1800-2400 MHz)	Higher frequency bands (2-8 GHz)
Bandwidth	5-20 MHz	100 MHz (or more)
Switching Design Basis	Circuit and Packet	All digital with packetized voice
Access Technologies	W-CDMA, 1xRTT, Edge	OFDM and MC-CDMA (Multi Carrier CDMA)
Forward Error Correction	Convolution rate 1/2, 1/3	Concatenated coding scheme
Component Design	Optimized antenna design, multi-band adapters	Smarter Antennas, software multiband and wideband radios
IP	A number of air link protocols, including IP 5.0	All IP (IP6.0)

Table 2 Comparisons of 4G and 3G networking

2.4. Interworking in 4G networks

Approach

Interworking, integration and convergence are terms expressing the need for combining the advantages of diverse network technologies in order to get the best service for minimum investment from the network. The interworking in heterogeneous networks needs to consider the integration of the access networks, the integration of the control and the management planes (QoS, Mobility, AAA, Security), the reconfigurability of the system and the terminals, and the adaptability of the network and services. In this context the convergence to all IP is an important issue. There are two main approaches are possible for interworking of access networks; loosed coupled architectures and tight coupled architecture.

2.4.1. Loose coupled architecture

Loose coupling [14] [15] [16] offers a common interface for the exchange of information between the networks to guarantee service continuity. The two access networks have nothing in common, but the core networks are connected together. Loose coupling refers to the Layer 3 (IP) interconnection. WLAN and UMTS are assumed to be in different IP address domains, resulting in obtaining a new IP address as the mobile crosses the boundary. It requires hence the change of IP address when the mobile moves from one network to another. The heterogeneity of different access networks is then managed and hidden by Mobile IP.

This approach separates completely the data path in WLAN and UMTS networks. The WLAN data are consequently never injected into the UMTS core network. Two architectures are independent and can belong to two different operators. If both access technologies are deployed by a single operator the Packet Data Protocol (PDG) may interface directly to the Gateway GPRS Support Node (GGSN) for signaling. Otherwise, the signalling will be transported through the IP network.

The key component for the mobility management of this architecture is the Mobile IP. The Foreign Agents (FA) are located in the GGSN, PDG and the Home Agent (HA) is located in the PDN/Internet and manages the FA of all WLAN and UMTS network. When the mobile moves across the networks its home address is maintained. The major drawbacks of this architecture are the handover latency and the packet loss due to Mobile IP. To overcome this problem, many extensions of Mobile IP have been proposed such as: pre-registration handover, post-registration handover, fast handover, multiple CoA registration, etc.

2.4.1.1. *Intra-3GPP network mobility solution*

Another approach is to manage mobility in the 3GPP core network. The use of TTG *(Tunnel Termination Gateway)* and a subset of GGSN functions to implement the PDG functions of WLAN is presented in Figure 5.

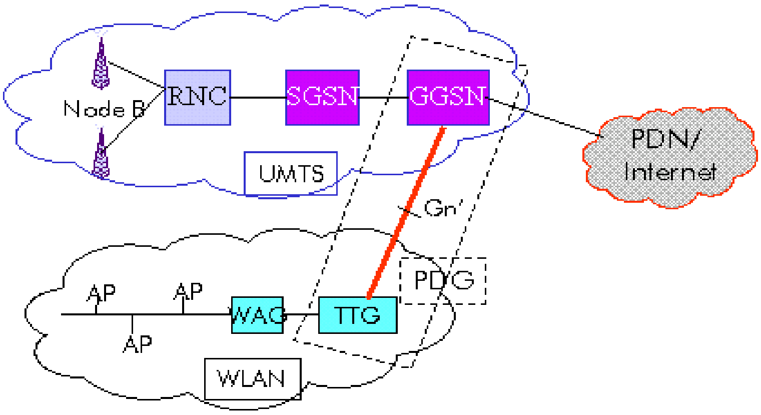


Figure 5. PDG implementation reusing GGSN functionality

In the research studies, the TTG is usually called as SGSN' (SGSN emulator) [17]. The functionality of SGSN' shall cover all aspects of PDG that are not covered by the GGSN. The SGSN' acts as the SGSN in terms of GTP tunnel establishment. It also acts as the WLAN mobile's proxy for the reason of transparency to the WLAN mobile. In this scheme the end-to-end tunnel (e.g. IPSec) from UE to PDG is terminated at SGSN' and a GTP tunnel is established between the SGSN' and GGSN.

2.4.2. Tight coupled architecture

In the tight coupling scheme, the WLAN is connected directly to the UMTS core network. The WLAN may be embedded in the UMTS network at different common integration point. The tight coupling is also considered as UMTS-based solution since the UMTS control protocols are reused in the WLAN and the data traffic is routed via the UMTS core network to the outer entities [18]. Generally speaking, in the tight coupling scheme, two radio access networks are interconnected using layer 2 functions. The handover neither involves the change of IP address nor the AAA policies since the mobile remains in the same subnet.

Recently, the UMA technology, which provides the interworking between WLAN and GSM/GPRS without service interruption, has been standardized in 3GPP. The common integration point of UMA technology is SGSN. This interworking solution [19] [20] has been the most considered solution in the WLAN-3GPP interworking research study. An interworking reference model is represented in Figure 6. In this architecture, an IWU (interworking unit) acts as an RNC emulator. Its main function is to provide a standardized interface to the UMTS core network and hide the WLAN particularities. It should provide numerous functions, such as data encapsulation; voice transcoding between mobile and PCM voice (if IWU is connected to MSC in the circuit-switch domain); signalling transfer; security gateway functions (to terminate secure remote access tunnels from the mobile); paging; handover control; etc.

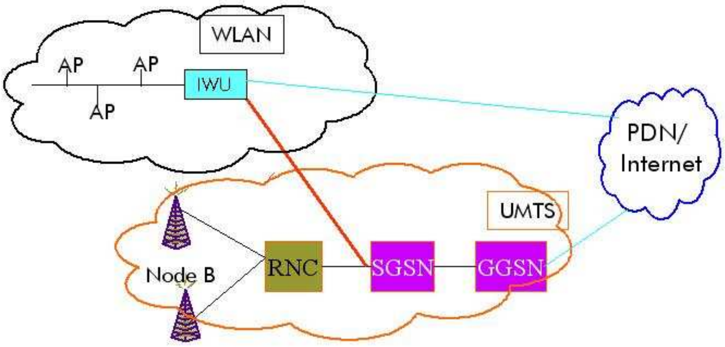


Figure 6. 3GPP – UMTS tight coupling interworking architecture

In this approach, all the layer 3 protocols remain unchanged. The UMTS SM (Session management) and GMM handle the session management and mobility management. The mobile cannot access the Internet directly through WLAN. The handover procedure should be the same as inter-RNCs handover in UMTS. To support mobility the SGSN needs to maintain the Packet Data Protocol (PDP) context, mobility management contexts and sequence number of the packets.

2.4.3. Interworking through 3GPP

2.4.3.1. UMA Release 6 [21]

UMA (Unlicensed Mobile Access) technology is designed to enable Fixed-Mobile convergence in an access network. It is currently endorsed by the 3GPP [20] under the name of GAN (Generic Access network) (In the remaining of this paper, we use UMA and GAN interchangeably). The GAN architecture and functional components are shown in Figure 7. A major feature of GAN is to offer call continuity from a GAN capable terminal between a local area network (UWB or 802.11) terminating at the fixed access and the GSM infrastructure. Data services are also supported but are limited in throughput since interconnection to the PSCN (packet-switched core network) is performed using the 3GPP-defined Gb interface. An important evolution of GAN will be to enrich user experience for data services as intended in 3GPP feasibility study on Enhanced GAN [TR 43.902]. The Gb interface is then replaced by the Gn interface to allow the Enhanced GANC entity interconnecting directly with the GGSN entity. No change on the Circuit-switched domain is required.

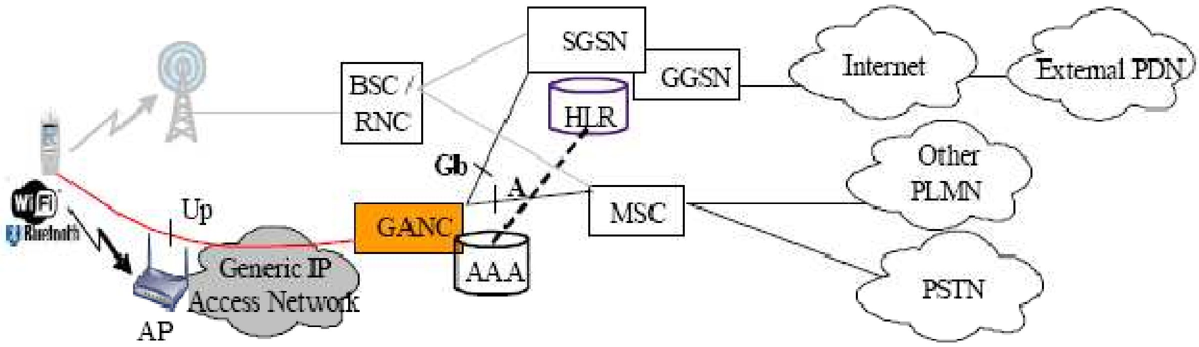


Figure 7. GAN Architecture and Functional Components

In the GAN architecture, an IPSec tunnel is established on the Up Interface between the GAN terminal and the GANC (GAN Controller). This flow tunneling is a strong security requirement that allows conveying both signalling and user data flows (GSM/GPRS signalling and user plane flows are piggy-backed into GAN-specific protocols and the IPSec tunnel) over an access network (named "generic IP Access Network") that is not supposed to be under the control of the mobile operator. The newly defined GANC entity reuses already 3GPP defined interfaces namely Gb and A interfaces to interconnect respectively to the Packet Switched

Core Network and Circuit Switched Core Network. Note that the AAA server is used to authenticate the GAN terminal when it sets up the secure tunnel. Figure 1.5 presents the architecture of GAN and its positioning with respect to the GSM/GPRS architecture.

2.4.3.2. I-WLAN interworking Architecture

In the 3GPP Release 6 specifications that aim at providing access to mobile operator services from a WLAN Access Network, I-WLAN introduces three main components to achieve the 3G/WLAN convergence : a WAG (Wireless Access Gateway), a PDG (Packet Data Gateway) and a AAA Server as shown in Figure 1.6. The UE (User Equipment) is typically dual-mode capable, under the WLAN coverage, it is capable to connect to the WLAN AN (Access Network) using Wi-Fi (as an example of radio technology) before attachment to the I-WLAN infrastructure and when outside this WLAN coverage, it can connect to the UMTS operator network. Data coming from UEs through fixed Access Networks (named Generic IP Access Network in the figure below) are aggregated at WAG, which is further connected to PDG. In roaming case, the visited WAG is also able to route packets towards the home domain of the operator to which the user has subscribed. The PDG in the I-WLAN architecture works as a gateway towards either the external Packet Data Networks (PDNs) or the operator service infrastructure, as shown in Figure 1.6. PDG also interacts with the AAA server to perform service-level authorization, authentication and accounting. When entering into the coverage area of WLAN AN, the UE triggers its attachment procedure with the I-WLAN infrastructure and thus an IPSec (IP Security) tunnel is established between the UE and the PDG. Packet Switched (PS) domain signalling and user plane data are carried into this secure tunnel over Wu interface.

2.4.3.3. I-WLAN Evolution: Release 7 [22]

Work on I-WLAN Release 7 (R7) started in January 2005 with the aim of defining an evolved UMTS architecture. On the core network side, a new work item called "System Architecture Evolution (SAE)" was defined. In this evolved UMTS architecture, it is expected that IP-based services will be provided through various access technologies. A mechanism to support seamless mobility between heterogeneous access networks is needed for future network evolution. To this end, I-WLAN is included in the SAE to ensure a smooth migration path from the R6 I-WLAN work to a generic multi-access solution. Apart from seamless mobility across heterogeneous RATs, I-WLAN R7 also supports access to IMS and private networks from I-WLAN, LoCation Service (LCS) for I-WLAN in order to enlarge the scope of location-services deployed for GSM/UMTS. Some enhancements to support QoS on the WLAN Access Network are also in the scope of studies.

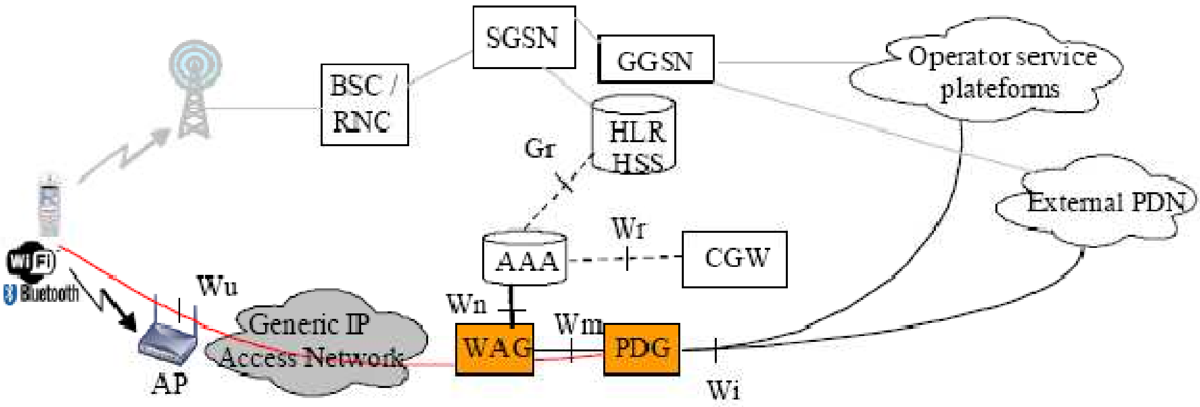


Figure 8. I-WLAN R6 Architecture and Functional Components

2.4.4. SSCAN

The Seamless Converged Communications Across Networks (SCCAN) [23] is an industry standard led by Motorola, Avaya and Proxim. SCCAN supports an emerging open specification for technologies that enable seamless converged communications. By incorporating the most popular Session Initiation Protocol (SIP) of the IETF as a control protocol, SCCAN's specifications aim at the convergence of Wi-Fi technology with cellular networks for voice, video and data services. SCCAN provides an enterprise solution which offers seamless interoperability between Wi-Fi enabled enterprise networks and cellular wide area networks.

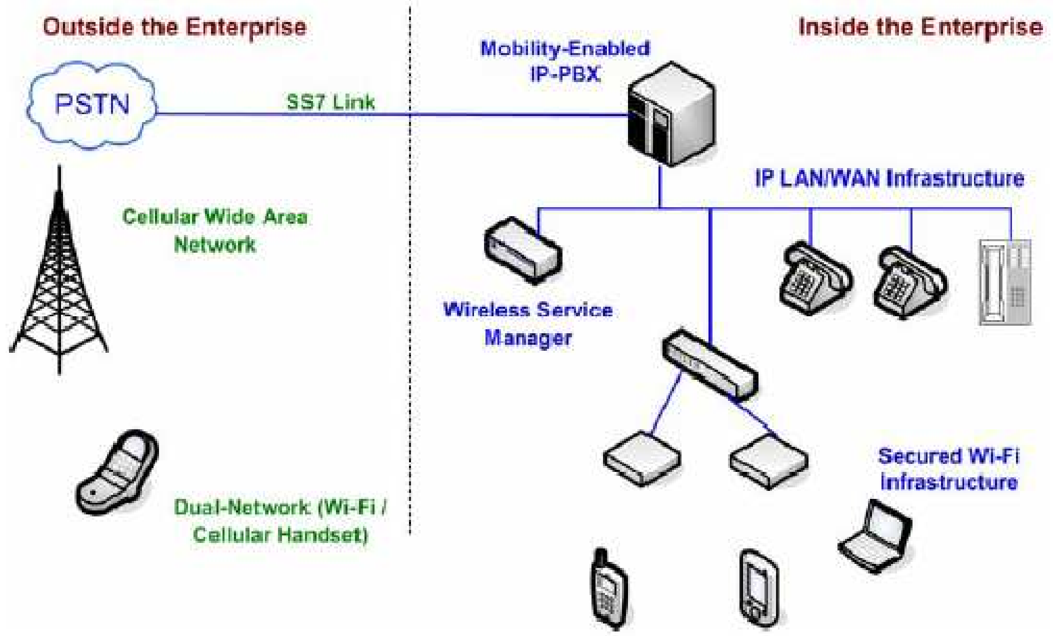

Outside the Enterprise
Inside the Enterprise
Mobility-Enabled IP-PBX
PSTN
SS7 Link
IP LAN/WAN Infrastructure
Cellular Wide Area Network
Wireless Service Manager
Secured Wi-Fi Infrastructure
Dual-Network (Wi-Fi / Cellular Handset)

Figure 9. SCCAN Enterprise Solution Architecture

SCCAN splits the functionality among dual-mode (Wi-Fi/Cellular) handset, mobility-enabled IP Private Branch Exchange (PBX) and WLAN gateway, as shown in Figure 9. While entering the office premises, the user's session switches from the cellular network to the Wi-Fi network. In order to ensure this functionality in the core network, the PBX has an SS7

(Signalling System 7) link to the wireless carrier so that the location registration and call control can be performed on session switching. SCCAN may present some advantages to set up customized business offers. However, from deployment perspective, this type of solutions presents significant constraints to interconnect with the mobile infrastructure since it requires the deployment of interconnection links between IP-PBX and PSTN peering nodes.

2.4.5. MIH IEEE 802.21

The IEEE 802.21 Working Group (WG) defines Media Independent Handover (MIH) in order to offer seamless convergence across heterogeneous networks [24]. MIH defines a framework to support information exchange that facilitates mobility decisions, as well as a set of functional components to execute those decisions. MIH shields link-layer heterogeneity and provides a unified interface to upper-layer applications in order to support transparent service continuity. The handover scenarios considered in 802.21 WG include wired as well as wireless technologies – the complete IEEE 802 group of technologies and 3GPP/3GPP2 access network standards.

The MIH framework provides methods and procedures to gather useful information from the mobile terminal and the network infrastructure in order to facilitate handover between heterogeneous access networks. MIH provides network discovery procedures which help the mobile terminal to determine which networks are available in its current neighborhood. Mobile terminal selects the most appropriate network with the help of the gathered information such as link type and quality, application class, network policy, user profile and power constraints.

2.4.5.1. MIH Architecture

MIHF (Media Independent Handover Function) lies in the heart of the MIH architecture and provides an intermediary or a unified interface between the lower-layer heterogeneous access networks and higher-layer components. MIH provides generic access-technology independent primitives called Service Access Points (SAPs). SAPs are APIs (Application Programming Interfaces) through which the MIHF can communicate with the upper and lower layers entities.

The MIHF facilitates three services namely Media Independent Event Service (MIES), Media Independent Command Service (MICS) and Media Independent Information Service (MIIS).

- Signalling state changes at lower layers.
- Control by higher layers.
- Provision of information regarding the neighbouring networks and their capabilities, respectively.

2.4.6. ETSI TI SPAN

Telecoms & **I**nternet converged **S**ervices & **P**rotocols for **A**dvanced **N**etworks (**TISPAN**) is a standardization body of ETSI, specialized in fixed networks and Internet convergence. [http://portal.etsi.org/tispan]. All current specifications can be found in [25].

TISPAN's release 1 architecture is based upon the 3GPP IP Multimedia Subsystem release 6 architecture. However, TISPAN has adopted a more generalized model able to address a wider variety of network and service requirements. This overall architecture is based upon the concept of cooperating subsystems sharing common components. The subsystem-oriented architecture enables the addition of new subsystems over time to cover new demands and service classes. It also ensures that the network resources, applications, and user equipment (mostly inherited from IMS where possible) are common to all subsystems, hence ensures user, terminal and service mobility to the fullest extent possible, including mobility across administrative boundaries. The role of TISPAN is to standardize converged networks using IMS as its core architecture. This means adding the ability for fixed network access to interface to IMS and also requesting 3GPP to enhance the IMS specification on wireless specific topics. With the objective of moving existing PSTN functionality onto an IP core, IMS is now being focused on to provide PSTN emulation.

PSTN emulation services provide a definition of what must be provided as a minimum, for example malicious call trace. Multimedia must be also allowed to provide additional enhancements to the service.

The location of the Network Attachment Subsystem (NASS) in the overall TISPAN architecture is presented in [26].

Comparisons between different Interworking Mechanisms

	GAN/UMA	I-WLAN	SCCAN	ETSI TISPAN	802.21(MIH)
Handset Network Connection	Unlicensed radio + 3GPP cellular stack (when under GAN/UMA coverage)	Unlicensed radio (when under I-WLAN coverage)	Enterprise WLAN + cellular stack	Fixed + 3GPP + WLAN/WIMAX	802.xx +cellular stack
Standardization Body	3GPP	3GPP	SCCAN Forum	ETSI	IEEE
Mobility Performance	++ Circuit-switched and Packet-switched	+Under study and applicable to Packet-Switched	++Circuit-switched and Packet-switched	++ Under study and applicable Packet-switched services	++Under study and applicable to Packet-Switched

	services	services only	services		services and Circuit-switched
Security	+	+	+	+	+
Network complexity for deployment	+ network impacts reduced	++ network impacts reduced	-- needs for interconnection with mobile network	-- needs for interconnection with mobile network	+ network impacts reduced
Handset Impact	- new handset required	- new handset required	- new handset required	- new handset required	- new handset required
Billing	+ supported	+ supported	- not supported	+ supported	-- Out of scope

+ supported, - not supported

Table 3. Comparisons between interworking mechanisms

2.4.7. 3GPP LTE evolution architecture

The main objective of 3G LTE architecture is to provide a higher data-rate, lower-latency and packet-optimized system that supports multiple RANs. In order to meet the requirements on high data rates with large transmission bandwidth and flexible spectrum allocation, OFDM and MIMO techniques have been chosen for Evolved-RAN [27]. The logical high level architecture of the evolved 3G is illustrated in Figure 10. The intra-LTE access system mobility is managed by two entities: Mobility Management Entity (MME) and User Plane Entity (UPE). The MME manages user contexts such as permanent and temporary identities, mobility states, location areas and user security parameters. The corresponding 2G/3G MME is SGSN. The UPE manages IP bearer service parameters and routing information. It is also responsible for triggering the paging when downlink data arrive for users. The corresponding 2G/3G UPE is the SGSN or SGSN+GGSN. The 3GPP Anchor is a functional entity that anchors the user plane to support mobility between 2G/3G and LTE access systems. The SAE Anchor manages the user plane to support mobility between 3GPP and non-3GPP access systems. The 3GPP anchor can be co-located with the MME/UPE or SAE Anchor or both.

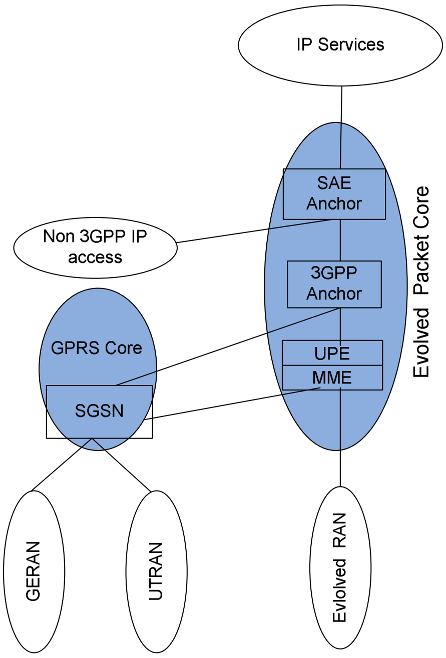


Figure 10. 3GPP LTE evolution architecture

2.5. Handover and roaming mechanisms

2.5.1. Handover Management

The handover management involves three phases: 1) neighboring cell discovery and measurement, 2) network selection and handover decision, and 3) handover execution.

2.5.1.1. Cell discovery & Measurement

The role of cell discovery and measurement is to identify the need for handover. This phase includes the following steps:

- Neighboring cell discovery: It is a preliminary step to be considered before carrying out the signal strength measurement. The MS can learn about its neighbors by scanning different channels or via the provisioning information from its current Base Station (BS).

- Signal strength measurement: The MS should synchronize in frequency and in time with its neighboring cells before it measures their radio link quality. The signal strength is averaged over time so that fluctuations due to radio propagation can be eliminated. Besides the measurement taken by the MS, the network makes itself the measurements such as the uplink quality, Bit Error Rate (BER) of the received data, etc.

- Reporting of measurement result: After the measurement, the MS sends measurement results to the network periodically or based on trigger events.

- Information gathering: Besides the physical link quality related parameters, in heterogeneous environments, the MS is required to collect other information like the terminal capabilities, service experiences status, context information, etc. to assist the vertical handover decision.

2.5.1.2. Network selection and Handover decision

This phase is responsible for determining when and how to perform the handover. We can divide this phase into different steps:

- Network selection triggering (including handover initiation triggering): Network selection is triggered taking as input the measurement results.

- Network selection: Network selection is the process of choosing the best access network among the multiple available ones. In heterogeneous environments, the MS must evaluate different criteria of each available network before selecting the best one. The selected access network must be commonly agreed between the user preferences and the network policy including the roaming agreement.

- Handover initiation: If the network selection results in change of access node, the handover initiation must follow right after. If the access technology of the selected access node is different from the serving access technology, a vertical handover is executed.

- Pre-notification to all recommended target BSs: The network selection gives a list of recommended BSs in the preferred networks order. In this case, the network may query the recommended BSs to check whether they can support the imminent handover from the MS. During this phase, certain pre-registration information of the MS will be relayed to the recommended target BSs for handover preparation purpose. At the end of this phase, the network can decide which target access network to select and send its decision to the MS. Another option is that the network eliminates the undesirable BSs among the recommended ones and then sends back the list of desirable recommended BSs to the MS. Here, the target access network is selected by the MS. Such a pre-notication handover only exists if the MS and the network cooperate together during the network selection and handover decision phase. Otherwise, the MS or the network can decide solely the target access node.

2.5.1.3. Handover execution

The handover execution includes the connection establishment, the resources release and the invocation of proper security services.

- Authentication: Once the target access network is selected and the handover decision is launched, the MS must use appropriate user credentials to authenticate with the target network and get valid encryption keys for communication sessions.
- Execution: Once the best access network is selected, and the re-authentication is successfully achieved, the communication session will be continued on the new radio

interface through a new routing path. The change of routing path must be noted to the Corresponding Node (CN) or the content provider.

2.5.2. Security in Wireless and cellular networks

2.5.2.1. Security solutions for today's 802.11 WLAN

To combat the weaknesses of standard 802.11 security, organizations such as the Institute of Electrical and Electronic Engineers (IEEE), the Wi-Fi Alliance, Cisco Systems and Fortress Technologies have introduced enhanced wireless security solutions developed around standards based technologies.

The IEEE's 802.1X Port Based Network Access Control standard provides strong authentication and network access control for 802.11 networks. Ratified in June 2004, the IEEE 802.11i enhanced wireless security standard introduces strong authentication and data encryption mechanisms and will become the new security standard for 802.11 networks. In late 2002, the Wi-Fi Alliance introduced Wi-Fi Protected Access version 1 (WPA v1), a subset of the 802.11i standard.

a. IEEE 802.1X Port Based Network Access Control:

802.1X [28] is a standard that provides a means to authenticate and authorize devices for network access. 802.1X has three components that combine to deliver a strong authentication solution: the Supplicant, Authenticator and Authentication Server (AS). The wireless terminal is the supplicant and the access point is the authenticator. The most common type of AS is RADIUS (Remote Authentication Dial-In User Service) [29] - typically a stand-alone software package installed on a standard PC platform. Authentication requests occur during system initialization and are initiated by wireless terminals or access points, after the terminal has associated to the access point. Various authentication methods such as digital certificates, smart cards and one-time passwords can be used to provide credential information for authentication. Of course, without successful authentication, network access is denied.

Figure 11 illustrates the IEEE 802.1X setup. The supplicant sends its authentication credentials to the AS via the authenticator. The AS confirms the supplicant's credentials and directs the authenticator to allow supplicant access to the network. The access point communicates with the wireless terminal and submits the terminal credential information to a suitable AS to determine correct authorization.

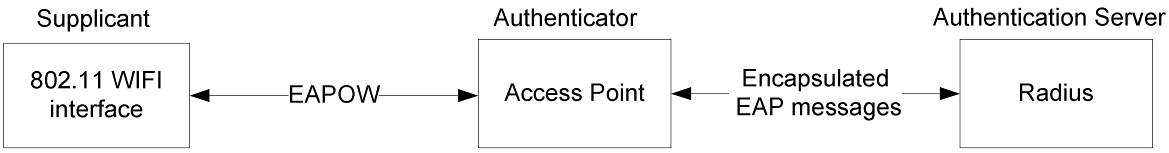


Figure 11. IEEE 802.1x setup

Extensible Authentication Protocol (EAP):

The 802.1X authentication process uses the Extensible Authentication Protocol (EAP) [30]RFC 2284 to pass authentication information between the supplicant and the AS. EAP effectively creates a session with the AS for the terminal to forward its credentials. If the EAP version supports mutual authentication, then the AS provides its credentials to the wireless terminal within the same session. The EAP session allows a wireless terminal limited access to the network for terminal authentication purposes only. Once authentication is complete, the session is terminated and the wireless terminal is granted access. EAP is a general protocol and is 'extensible' in that it supports multiple authentication mechanisms. 802.1X supports such EAP types as Message Digest 5 (MD-5) [31], Transport Layer Security (TLS) [32] [33], and Protected Extensible Authentication Protocol (PEAP) [34].

The authentication dialog between the terminal and authentication server is carried in EAP frames. The encapsulated form of EAP, known as EAP over LAN (EAPOL) and EAP over Wireless (EAPOW), is used for all communication between the supplicant and authenticator. The access point acts as an EAP proxy between the terminal and AS, accepting EAPOL packets from the terminal and forwarding them to the AS over a protocol such as RADIUS. In turn, the access point forwards all AS EAP packets over EAPOL to the wireless terminal.

EAP TLS [32]

EAP-TLS (Transport Level Security) provides strong security by requiring both client and authentication server to be identified and validated through the use of PKI certificates. EAP-TLS provides mutual authentication between the client and the authentication server and is very secure. EAP messages are protected from eavesdropping by a TLS tunnel between the client and the authentication server. The major drawback of EAP-TLS is requirement for PKI certificates on both the clients and the authentication servers - making roll out and maintenance much more complex. EAP-TLS is best suited for installations with existing PKI certificate infrastructures. Wireless 802.1X authentication schemes will typically support EAP-TLS to protect the EAP message exchange. Unlike wired networks, wireless networks send their packets over open air making it much easier to capture and intercept unprotected packets.

EAP SIM:

EAP SIM [35] is a mechanism which specified for authentication session key distribution using global system for mobile communications using subscriber identity module (SIM). GSM authentication mechanism is based on challenge-response. The A3/A8 authentication and key derivation algorithms that run on the SIM can be given a 128-bit random number (RAND) as a challenge. The SIM runs operator-specific algorithms, which take the RAND and a secret key Ki stored on the SIM as input, and produce a 32-bit response (SRES) and a 64-bit long key Kc as output. The Kc key is originally intended to be used as an encryption key over the air interface, but in this protocol it is used for deriving keying material and not directly used. The 64 bit cipher key (Kc) that is derived is not strong enough for data networks where stronger and longer keys are required. Hence in EAP-SIM, several RAND challenges are used for generating several 64-bit Kc keys, which are combined to constitute stronger keying material. In EAP-SIM the client issues a random number NONCE_MT to the network, in order to contribute to key derivation, and to prevent replays of EAP-SIM requests from previous exchanges. The NONCE_MT can be conceived as the client's challenge to the network. EAP-SIM also extends the combined RAND challenges and other messages with a message authentication code in order to provide message integrity protection along with mutual authentication.

The Authentication mechanism of EAP SIM is shown in Figure 12.

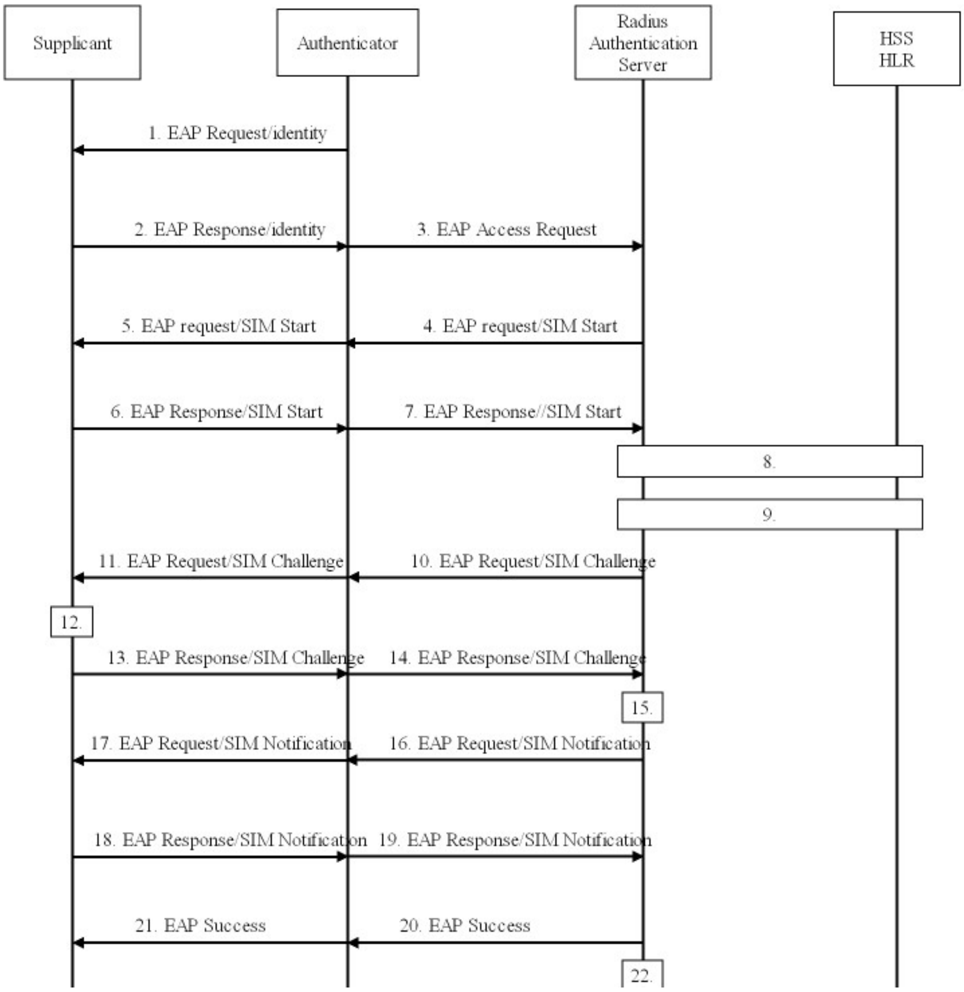

Supplicant
Authenticator
Radius Authentication Server
HSS HLR
1. EAP Request/identity
2. EAP Response/identity
3. EAP Access Request
5. EAP request/SIM Start
4. EAP request/SIM Start
6. EAP Response/SIM Start
7. EAP Response//SIM Start
8.
9.
11. EAP Request/SIM Challenge
10. EAP Request/SIM Challenge
12.
13. EAP Response/SIM Challenge
14. EAP Response/SIM Challenge
15.
17. EAP Request/SIM Notification
16. EAP Request/SIM Notification
18. EAP Response/SIM Notification
19. EAP Response/SIM Notification
21. EAP Success
20. EAP Success
22.

Figure 12 EAP SIM message exchanges

Wi-Fi Protected Access (WPA):

Realizing there was a need for a strong wireless security solution to fill the security gap until the ratification of the 802.11i standard, the Wi-Fi Alliance teamed up with the IEEE and in late 2002 introduced Wi-Fi Protected Access version 1 (WPA v1). WPA v1 is a subset of 802.11i security with many of the same data encryption and authentication components. WPA v1 certification of 802.11 hardware began in February 2003 and became mandatory for Wi-Fi certification at the end of 2003.

WPA v1 utilizes TKIP to provide strong data encryption, and offers two device authentication and key management methods. In enterprise environments with a centralized AS, user authentication is based on 802.1X and mutual authentication based EAP. In home or office environments where a centralized authentication server or EAP framework is not available, user authentication is based on a 'Pre-Shared Key' method (PSK). With Pre-Shared Key authentication, the home or office user manually enters a password (Master Key) in the Access Point or Wireless Router and enters the same password in each client device that accesses the wireless network. The manually configured WPA password (Master Key) automatically starts the TKIP data encryption process.

WPA v1 addresses security requirements for AP-based 802.11 networks only. The Wi-Fi Alliance has adopted the full 802.11i security standard as WPA v2, featuring security requirements for AP-based and ad-hoc (peer-to-peer) 802.11 infrastructures.

2.5.2.2. Security Solutions for WIMAX

The security architecture of 802.16 is divided into two layers; the first layer is to provide encapsulation for the data access across the 802.16 networks. The second is a key management protocol PKM providing secure distribution of keying data between the BS and terminal. PKM supports both mutual authentication and unilateral authentication. The key management protocol uses EAP or X.509 digital certificates together with RSA or a sequence starting with RSA and followed by EAP. It uses strong encryption algorithms to perform key exchanges between the BS and terminal. It supports re-authentications, reauthorizations and key refresh.

PKM protocol establishes a shared secret Authorization Key between the BS and terminal. A BS authenticates a client terminal during the initial authorization exchange. Each terminal presents its credentials, which will be a unique X.509 digital certificate issued by the terminal manufacturer in the case of RSA authentication or an operator-specified credential in case of EAP-based authentication.

PKM RSA authentication

The PKM RSA authentication protocol uses X.509 digital certificates, the RSA public key encryption algorithm that binds public RSA encryption keys to MAC addresses of SSs.

A BS authenticates a client SS during the initial authorization exchange. Each MS carries a unique X.509 digital certificate issued by the SS s manufacturer. The digital certificate contains the SS s Public Key and SS MAC address. When requesting an AK, an SS presents its digital certificate to the BS. The BS verifies the digital certificate, and then uses the verified Public Key to encrypt an AK, which the BS then sends back to the requesting SS.

All SSs using RSA authentication shall have factory-installed RSA private/public key pairs or provide an internal algorithm to generate such key pairs dynamically. If an SS relies on an internal algorithm to generate its RSA key pair, the SS shall generate the key pair prior to its first AK exchange. All SSs with factory-installed RSA key pairs shall also have factory-installed X.509 certificates. All SSs that rely on internal algorithms to generate an RSA key pair shall support a mechanism for installing a manufacturer - issued X.509 certificate following key generation.

PKM EAP authentication

PKM EAP Authentication uses Extensible Authentication Protocol in conjunction with an operator-selected EAP Method (e.g. EAP-TLS). The EAP method will use a particular kind of credential — such as an X.509 certificate in the case of EAP-TLS, or a Subscriber Identity Module in the case of EAP-SIM.

The particular credentials and EAP methods that are to be used are outside of the scope of this specification. Use of an EAP method not meeting these criteria may lead to security vulnerabilities. During re-authentication, the EAP transfer messages are protected with an HMAC/CMAC tuple. The BS and MS must discard unprotected EAP transfer messages or EAP transfer messages with invalid HMAC/CMAC digests during re-authentication.

2.5.2.3. GSM Security

SIM CARD: The IMSI – International Mobile Subscriber Identity – a unique number for every subscriber in the world. It includes information about the home network of the subscriber and the country of issue. The Ki – the root encryption key. This is a randomly generated 128-bit number allocated to a particular subscriber that seeds the generation of all keys and challenges used in the GSM system. The Ki is highly protected, and is only known in the SIM and the network's AuC (Authentication Centre). The phone itself never learns of the Ki, and simply feeds the SIM the information it needs to know to perform the authentication or generate ciphering keys. When a user is subscribed to a network for the first time a subscriber authentication key (Ki) is assigned in addition to the IMSI (stored in SIM).On the network side, this key Ki is stored in the AuC of the HPLMN.

The GSM authentication procedure is based on the algorithm A3 which is implemented both at MS and MNO sides. When needed for each MS, the BSS/MSC/VLR requests security related information from the HLR/AuC corresponding to the MS. This includes an array of pairs of corresponding RAND and SRES (or XRES). The pairs are stored in the VLR as part of the security related information. These pairs are obtained by applying algorithm A3 on each RAND and the key Ki [TS 43.020].

A signed response (SRES) originated by MS is compared by the MSC/VLR against the corresponding AuC generated expected response (XRES) value in order to validate the subscriber identity. i.e if both the values agree, the authentication is successful [TS 43.020]. The AuC generated (RAND, XRES) vector (an array of pairs of RAND,XRES) is passed to whichever network requires them so that a challenge/response process for subscriber identity authentication can take place when the subscriber intends to access services, e.g. MO call.

Authentication During data services

General authentication procedure during data services is handled in similar way as in GSM authentication and Figure 13 illustrates the process.

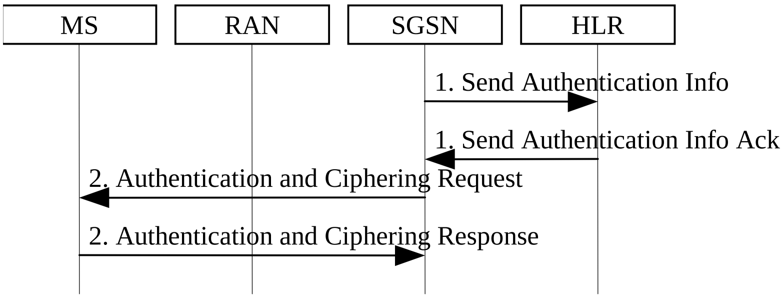

MS
RAN
SGSN
HLR
1. Send Authentication Info
1. Send Authentication Info Ack
2. Authentication and Ciphering Request
2. Authentication and Ciphering Response

Figure 13. General authentication procedure –during data services

Non-transparent access uses an additional PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) based MS authentication for data services. During the PDP context activation process a RADIUS request is built by the GPRS PLMN toward the RADIUS server associated with the APN.

AKA

UMTS AKA is based on the assumption that the Authentication Center (AuC) of the user's home environment and the user's USIM share a user specific secret key K, certain message authentication functions *f1, f2* and certain key generating functions *f3, f4, f5.*

f1 – is used to generate the authentication token (MAC) which has a similar purpose to SRES in GSM, but is used to authenticate the network to the mobile (i.e. the mobile tests if the network has knowledge of the root key K. It’s inputs are RAND (128-bit), K (128-bit), the sequence number SQN (48-bit) and AMF

f2 – is used to generate the XRES, similar to the SRES but 128-bits long. Inputs are K and RAND

f3 – Used to generate the 128-bit ciphering key CK. Inputs are K and RAND.

f4 – used to generate the 128-bit integrity key IK. Inputs are K and RAND. The IK is used to ‘sign’ radio control messages, discussed later.

f5 – used to generate the 128-bit authentication key AK (48-bit) , which is used to encrypt (XORed with) the Sequence number SQN when it is sent to the mobile station.

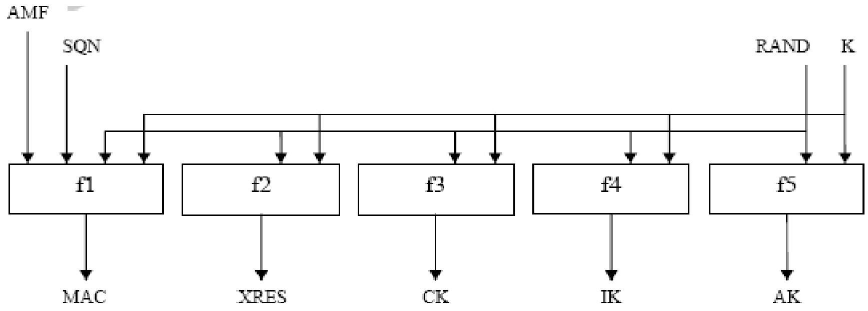


Figure 14. Message authentication functions in AKA

The UMTS AKA consists basically of two phases:

Generation of Authentication Vectors: After receiving an authentication data request from an SN, the HE/AuC generates an array of *n* authentication*5* vectors, each consisting of the following five components: A random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. This array of *n* authentication vectors is then sent to the requesting SN.

Authentication and Key Agreement: In an authentication exchange the SN, resp. one of its corresponding network entities, namely Visitor’s Location Register (VLR) or Serving GPRS Support Node (SGSN), selects the next (the *i*-th, where *1 i n*) authentication vector from the ordered array and sends RAND(*i*), AUTN(*i*) to the user. The USIM checks whether AUTN(*i*) can be accepted, i.e. whether AUTN(*i*) constitutes a valid authentication token, and if so, produces a response RES(*i*) which is sent back to the SN, which compares RES(*i*) to XRES(*i*). The USIM now also computes CK and IK which are subsequently used for ciphering and integrity protection on the air interface.

Authentication Signaling in the Access Networks

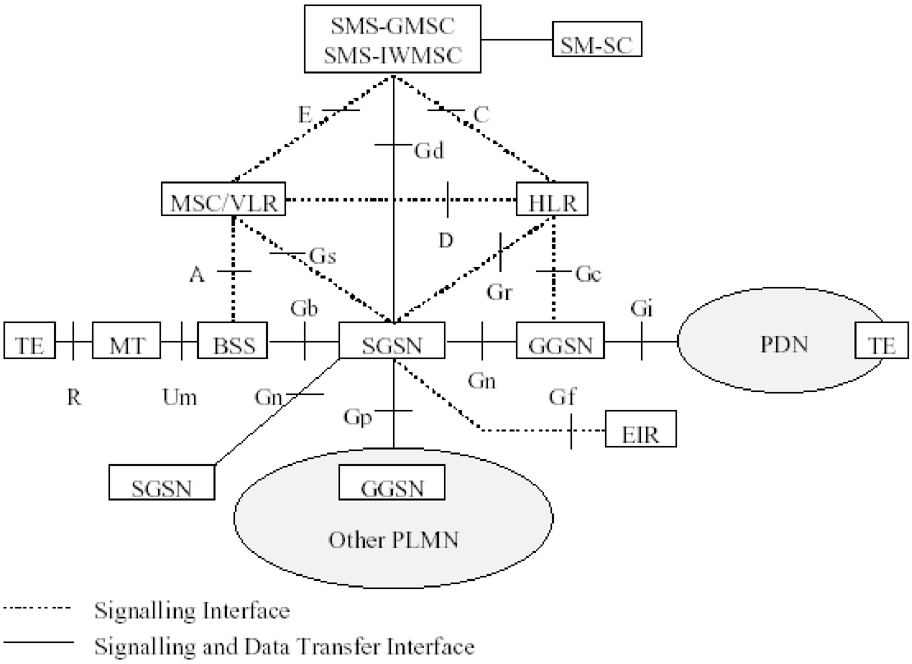


Figure 15. GPRS logical architecture [IR.33]

As specified in IR.33 recommendations GPRS roaming has two basic scenarios;

- MS connects via VSGSN and HGGSN
- MS connects via VSGSN and VGGSN

During the registration of the MS to the visited network, GPRS attach process to the VSGSN shall take place. The VSGSN communicates with the HLR in HPLMN (inter network SS7 links, Gp interface).This validates the user’s roaming mobile services. Once attached user can perform PDP context activation procedure.

When MS connecting via VSGSN to HGGSN, there are several requirements to be satisfied. There has to be SGSN-HLR interactions via Gr interface using Inter network links. Also inter network DNS exchange mechanism has to be in place. Moreover, inter PLMN backbone connectivity via border gateways and an address management plan should also be involved in the architecture. Figure 16 illustrates this scenario.

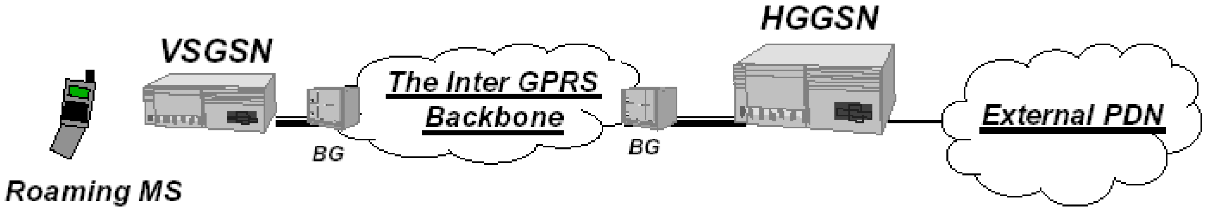


Figure 16. VSGSN and HGGSN using Inter PLMN Backbone

The second scenario typically requires being transparent i.e. with non-authenticated network access-point access. Therefore this approach is generally deployed by the MNOs.

Furthermore, there is no data and signalling exchanges across Inter PLMN backbone as Intra PLMN backbone is used to establish context. This scenario is shown in Figure 17.

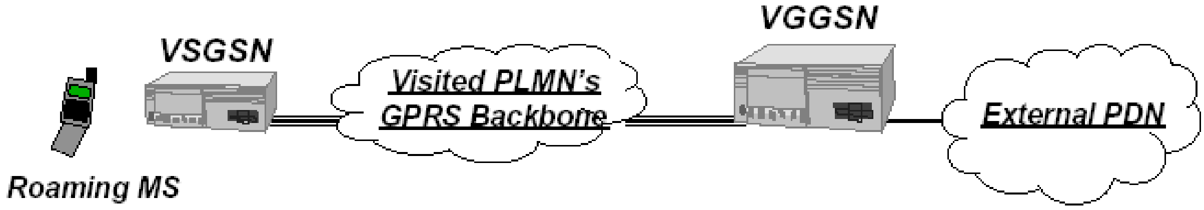


Figure 17. VSGSN and VGGSN using VPLMN Intra GPRS Backbone

2.5.3. Mobility management

IP version 4 assumes that a node's IP address uniquely identifies the node's point of attachment to the Internet. Therefore, a node must be located on the network indicated by its IP address in order to receive datagram's destined to it, otherwise datagram's destined to the node would be undeliverable. For a node to change its point of attachment without losing its ability to communicate, currently one of the two following mechanisms must typically be employed:

- The node must change its IP address whenever it changes its point of attachment.
- Host-specific routes must be propagated throughout much of the Internet routing fabric.

Both of these alternatives are often unacceptable. The first makes it impossible for a node to maintain transport and higher-layer connections when the node changes location. The second has obvious and severe scaling problems, especially relevant considering the explosive growth in of portable devices connected to internet.

2.5.3.1. Mobility at Layer 2

The mobility at this point appears at the link layer of the technology specific. Here at the time of the mobility the IP address of the device point of attachment remains the same even though the mobile moves from one point if attachment to another. Some of the link layer mechanisms are discussed in some of the WGs and specification bodies with the mobility at the layer 2.

- IEEE 802.11f [36]is the draft standard of wi-fi technology to provide mobility support at link layer.
- IEEE 802.16e is the draft wok for adding mobility support to the already existing 802.16-2004 standard for BWA (Broadband Wireless Access)
- IEEE 802.20 is the draft work of MBWA (Mobile Broadband Wireless Access)
- IEEE 802.21 is the draft work of the Media Independent Handover

2.5.3.2. Mobility at layer 3

In the heterogeneous networks, the mobility management at layer 3 can be broadly categorized into two types: macro-mobility and micro-mobility. The mobility between the different administrative domains is referred to macro mobility since it will be global and independent of underlying mechanisms such as routing protocols, link layer access technologies, and security architectures. On the other hand, the term micro mobility refers to the movement of mobile between different subnets belonging to single domain. Note that, one administrative domain may include different access technologies, such as 2G, 3G, WLAN, WIMAX…of one service provider.

a. MIPV4

The Internet Engineering Task Force (IETF) has proposed Mobile IP [37] as an interface between the mobile node home network and foreign network. Mobile IP is a standard that allows a user with a mobile device, whose IP address is associated with a particular network, to stay connected when moving to a network with a different IP subnet addresses. When a user leaves its network (i.e. when its device enters the domain of a foreign network) the foreign network uses the Mobile IP to inform the home network of a Care-of-Address (CoA) to which all packets for the user's device should be sent. By doing so, Mobile IP keeps track of the location of a mobile and delivers packets to its current location.

The Mobile IPv4 enables the mobile terminal to maintain its IPv4 address and the transport layer connection while the mobile changes the access points (During Handoff). It can provide a transparent movement for the transport and upper layer. Mobile IPv6 allows a mobile node to move from one wireless access point or base station with no disruption in network connectivity.

In Mobile IPv4, the Messages from the Internet are always sent to the permanent address assigned to the mobile node. Routing of messages from the home network to the current location of the mobile is accomplished throughout the use of two IP addresses per mobile, a home address for identification and a CoA for routing. The home address does not change regardless where mobile resides, even though the CoA changes according to the connected network. A Home Agent (HA), located in each home network, maintains a database in which the mobiles home address reside. Whenever the mobile node moves to a foreign network, it establishes an association with a Foreign Agent (FA), which is located in the visited foreign network. The Mobile Node registers to the HA through FA.

Home Agent and Foreign Agents send agent advertisement periodically within their respective network domains. After receiving the agent advertisement, the mobile nodes distinguish whether it is in its home network or in a foreign network. When the mobile node is at home network it basically works like natural with normal routing technique. When the mobile moves to foreign network it obtains a CoA by soliciting or listening to the agent advertisements. The mobile node registers its CoA to home agent through foreign agent. Data sent to the home address of the mobile node is then intercepted by the home agent and are tunnelled to the care of address of the mobile node. Once received at the tunnel end point, the Foreign Agent, the data are finally delivered to the mobile node.

Hence, Mobile IP is mainly based of three steps: agent discovery, registration and tunnelling.

Agent Discovery is the process by which Mobile Node determines its new attached points or its IP address when it moves from one place to another place. Through this method Mobile Node performs several procedures. It determines whether it is connected to its Home network or to a Foreign network thanks to the agent advertisements. It detects whether it has changed network or stay connected to present network and finally obtains care of address when it changes the network through the Dynamic Host Configuration Protocol (DHCP) [38] or manual configuration.

Registration is the method performed when Mobile Node connects or disconnects to a foreign network with the home agent. This process is also involved in finding the services offered by the foreign agent and informing the home agent. In this process, it can do re-registration when certain time-values expire. Registration includes two steps, registration-request and registration-reply between the mobile node and home agent. This process also involves deregistration with the home agent when the mobile node returns to its home network.

Tunnelling is the process by which Mobile IP relays the datagram's from the home agent to the mobile node when this latter is connected to a foreign network. The tunnelling is realised with the help of the care-of-address.

Figure 18 summarizes the typical Mobile IP scenario.

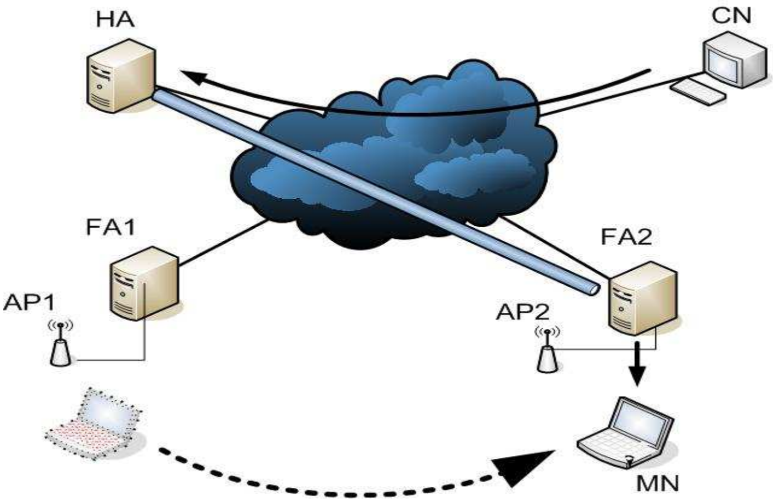


Figure 18. Mobile IPv4 Scenario

The transparent mobility support of Mobile IP is important for long-lived connection-oriented traffic or for incoming traffic initiated by correspondent hosts. However, this transparent mobility support does not come without cost. In the absence of route optimization for Mobile IP, packets destined to a mobile host are delivered to its home network and then forwarded to the mobile host's current care-of-address in the network it is visiting. If a mobile host is far away from home but relatively close to its correspondent host, the path traversed by these packets is significantly longer than the path travelled if the mobile host and the correspondent host talk to each other directly. The extra path length not only increases latency but also generates extra load on the Internet. It even increases load on the home agent, potentially contributing to a communication bottleneck if the home agent is serving many mobile hosts simultaneously.

b. MIPv6

Mobile IPv6 [39] includes many features for streamlining mobility support that are missing in Mobile IPv4. The Mobile IPv6 can support node's mobility in the network layer without the need of FA. Then, the main components of MIPv6 operation are the HA, home address, CoA, mobile/correspondent node. Each mobile is identified by its home address. The HA is a router supporting the mobility services in the home network. Based on the Home Agent Address Discovery protocol the mobile can discover it's HA at the first entry in the network.

If the mobile is at home network, a conventional mechanism is used to route the packets to the mobile. When the mobile moves to another network, it gets a new CoA. The mobile then sends to its HA about its new CoA. An association between the home address and its CoA is established. This association is named *binding.* The HA will then transfer all the packets addressed to mobile to its new location. The Mobile Node also sends Binding Updates messages to its Correspondent Nodes to inform them about its current Care-of Address. This later will allow establishing Route Optimization between both peers avoiding the use of triangular routing as in MIPv4.

Handover procedure with Mobile IPv6

When the mobile changes its point of attachment to the Internet, it will perform the MIPv6 handover process. The handover process is performed according to the following steps:

- **Movement Detection**: In general, the mobile is responsible for movement detection. The mobile is considered to move out of the current network if the current access router is no longer reachable or the new different access router is available.
- **Router Discovery:** This is achieved by receiving the router advertisement periodically sent by the access router. The mobile can also solicit the access router to send the router advertisement. Usually, the mobile sends the router solicitation if it discovers that its current access router is unreachable.

- **Address Configuration:** The mobile must configure itself its IPv6 address used in the new network. Note that the information in the router advertisement is required for configuring the new CoA. This CoA may be obtained either by *Stateful or Stateless Address Autoconfiguration.* The stateless mechanism which configures the CoA with the prefix discovery provides less the delay in comparison with the stateful mechanism.
- **Duplicate Address Detection (DAD):** The mobile should perform the DAD to ensure that its configured addresses are likely to be unique on the link. The mobile cannot begin to use this new CoA until it executes successfully the DAD procedure. However the DAD may add more delay in the overall handover latency.
- **Registration of new CoA:** Once the mobile detects that it has moved to another network, obtained new CoA and checked the validity of this CoA, it should notify its HA of its new location. From the moment when the mobile loses the connectivity with its access router to the moment when the mobile informs the HA its new location, all the packet addressed to it will be lost.
- **Binding update completion:** This step refers to the mobile informing all its correspondent nodes its new location and that the mobile is reachable at its new CoA.

A typical Mobile IPv6 scenario is shown in Figure 19.

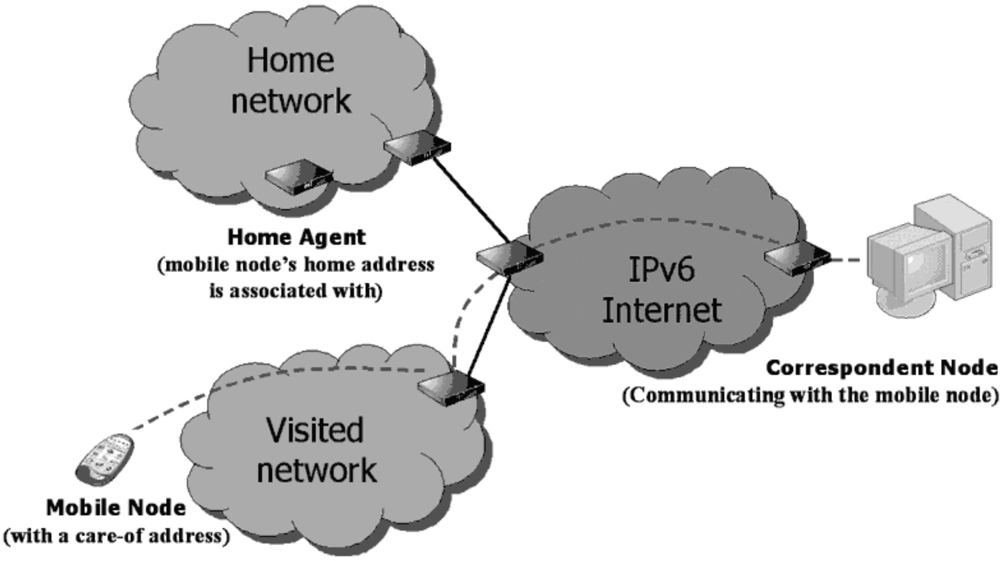


Figure 19. Mobile IPv6 Scenario.

c. Network Based Mobility

The solutions presented above require deep interoperation with the MN. This means that in order to initiate mobility registration, MN needs be able to communicate via the access point in the current network. A safe decision for the network administrator is the MN is authenticated in order to actually be granted connection with the local network. In fact, allowing "unauthorized" mobile device sending information causes security problems and difficulty for the management. An interesting approach is of Intra-domain Multicast-base Mobility (M&M) using Mobility Proxy. Actually, the use of proxy in M&M is not considered as a best choice of the solution, but rather algorithmic mapping. Using multicast address as the CoA of MN, the solution can speed up the handoff phase and keep the packet loss low. This solution may prove efficient with future network, rather than with the actual network, due to its high demand for the support of the multicast address allocation. Nevertheless, the Mobility Proxy shows a potential way to deal with the connection permission of the MN. Instead of letting the MN do the registration with the HA, now an agent, Mobile Proxy does it on the behalf of the MN. The mechanism procedures as follow: when arriving at a new domain, MN communicates with the Access Router (AR), which performs necessary authentication and security measures. The later then sends a request message to the Mobile Proxy (MP). Upon receiving the information from the AR, MP registers with the HA using MIP.

2.5.3.3. Macro Mobility

When the mobile user moves between the different subnets or different domains, its IP address will be changed. In order to maintain the reach ability, the mobile node should have a mechanism to inform quickly its correspondent node of its new address or it should have a permanent IP address seen by its correspondent node. Mobile IP is proposed to solve the problem of node mobility by redirecting packets for the mobile node to its current location. In the following we discuss two optional mechanisms that may be added to Mobile IP in order to improve its performances.

In order to save the energy consumption of the mobile node, IP paging is proposed as extension of Mobile IP. Under the Mobile IP paging, the mobile may be inactive for a period of time. The mobile does not register its location when moving during idle time if it is still in the paging area. This latter is defined by several subnets. The packets destined to the mobile will be buffered at the paging initiator which is responsible for locating the mobile by sending out the IP paging messages within the paging area. When the current location of the mobile is known, the paging initiator will forward the packets to it.

The triangular routing is one of the significant limitations which may cause latency and bottleneck in the network. Furthermore, the packets already sent to old CoA and in flight are lost. The signalling overhead associated with location update may be very high and the signalling delay may be long since the distance between the visited network and home network may be large. The first problem is solved by route optimization which consists of using direct route between the mobile and correspondent node to bypass the home agent. The route optimization also addresses the second problem: the new foreign agent notifies the previous foreign agent about the movement so that the previous foreign agent forwards the packets to the new one.

a. Hierarchical MIPv6

Since the handover delay in MIPv6 limits the real time applications, many researches have been done to suggest the solution for this problem. Among these solutions, Hierarchical MIPv6 (HMIPv6) [40] was designed so as to minimize the signaling quantity to the correspondent node and the HA. This is achieved by allowing the mobile to locally register with a domain. The global Internet will be then divided into the regions named local mobility zone. These zones form the independent subnet domains. Each domain is connected to the Internet via the mobility anchor point (MAP) which behaves like the anchor point for the mobile (see Figure 20). The MAP acts as a local HA which receives all the packets on behalf of the mobile node it is serving and will encapsulate and forward them to the mobile node's current address. When the mobile moves inside the local MAP domain, the mobile only needs to register the new location with the MAP. Therefore, only Regional CoA needs to be registered with the HA and correspondent nodes. The handover is thus hidden at the HA and the correspondent nodes if the mobile moves in the same local MAP domain.

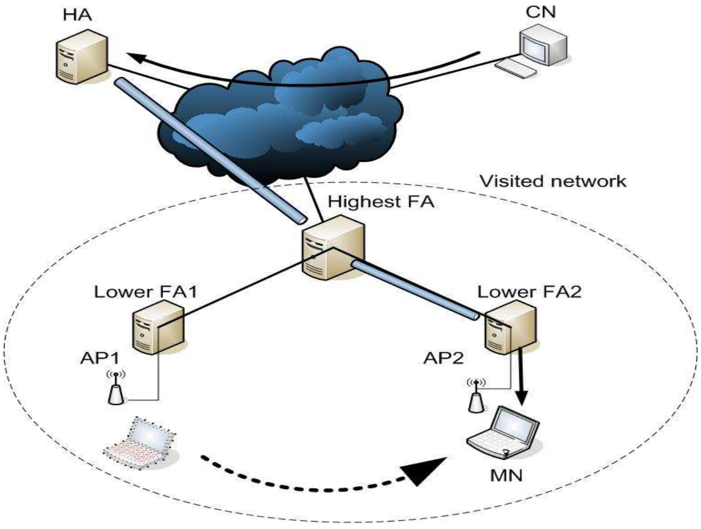


Figure 20. HMIP Architecture

b. Fast handover MIPv6 (FMIPv6)

The fast handover MIPv6 (FMIPv6) [41] is an extension of MIPv6 that allows the mobile to configure a new CoA before it moves to the new network and thus can use it immediately once connecting to the new network. Moreover, the FMIPv6 can reduce the latency involved during the mobile's binding update procedure by providing a bi-directional tunnel between the old and the new access router while the binding update procedures are being performed.

When the mobile detects one or more access routers (AR), it will send a PtSolPr (Router Solicitation for Proxy) message to current access router to request the information about its neighboring networks. The triggers for sending PtSolPr can originate from the link-specific events, e.g., a better signal strength from the new access router. The current AR will then inform the mobile of the neighboring link information (link-layer address, prefixes for configuring a new CoA). The mobile node sends a FBU (Fast Binding Update) including the prospective new CoA (NCoA) to the current access router which then communicates with the target access router to check if this NCoA is not currently used. The mobile will establish a binding between the previous CoA (PCoA) and NCoA and tunnel any packets addressed to PCoA to NCoA. The new AR buffers the packets until the mobile arrives on its link and then delivers them to the mobile. Once attached to new link, the mobile still uses the bi-directional tunnel and sends packet with PCoA as source address until it has completed the MIPv6 binding update procedure.

2.5.3.4. Micro mobility

To enhance the Mobile IP, the so-called micro mobility protocols have been developed for seamless handover within a same administrative domain. The micro mobility solutions aim to reduce the signalling load and delay to the home network during movement within one domain. We can distinguish two kinds of approaches: tunnel driven proposals and routing table driven proposals.

The tunnel based solutions consist of using the local and hierarchical registration. Among the different solutions, the Hierarchical mobile IP (HMIP) was standardized by IETF. The intra-domain mobility management protocol (IDMP) [42] is also a tunnel based micro-mobility protocol which is considered as a two-level hierarchical approach of the Mobile IP architecture.

The routing-based approaches consist of maintaining host-specific routes in the routers to forward packets. The host-specific routes will be updated based on the host mobility information. Cellular IP [43] and HAWAII [44] (Handoff Aware Wireless Access Internet Infrastructure) are the routing based protocols which are proposed to extend the IETF standard.

Each of these proposed solutions concentrates on a particular set of issues related to mobility management within a single administrative domain. In the following descriptions, we first explain the set of issues motivating the corresponding micro mobility management solution. Then, we present how the underlying protocol resolves them

a. IDMP

IDMP is a two-level hierarchical approach of the Mobile IP architecture. The first hierarchy consists of different mobility domains. The second consists of different IP subnets. Therefore, it localizes the intra-domain location update messages. In the IDMP architecture, the MA (Mobility Agent) is responsible for the mobility management within a domain and the SA (Subnet Agent) handles the mobility within a subnet.

Fast Handoff procedure in IDMP is based on triggers available at layer 2 indicating a change in the network. When a mobile node is moving from one base station to another, to minimize the service disruption during handoff, IDMP requires either MN or the base station to generate movement imminent message to the MA. Upon receiving this message the MA multicast all the packets to the entire set of neighboring base stations. All these base station buffers the incoming packets thus minimizing the packet loss during handoff transition. When the MN subsequently performs a subnet-level configuration (using IDMP) with base stations, can immediately forward all such buffered packets over the wireless interface, without waiting for the MA to receive the corresponding Intra-domain Location Update.

b. Cellular IP

Cellular IP is one of the protocols that provide micro mobility management. In Mobile IP various phases and network components are required for managing mobility. Cellular IP system [45] consists of a number of components to allow access, paging and mobility management. The concept behind CIP is the same as mobility management of voice terminals in GSM and IS–41 related air interfaces. Its objective is to allow the idle mobile stations to have discontinuous transmissions. Thus, the main idea behind CIP is that as long as nodes can be traced in larger paging area, they don't have to register every move during passivity.

All the mobile nodes in the access network registers to the *gateway router*. The gateway router is connected to several base stations on one end and connects to Internet on the other end. The visiting mobile node registers to the gateway and uses its IP address as its care-of-address. All the packets destined to the mobile node first reach the gateway from which they are routed through the base stations to their respective IP address (mobile node).

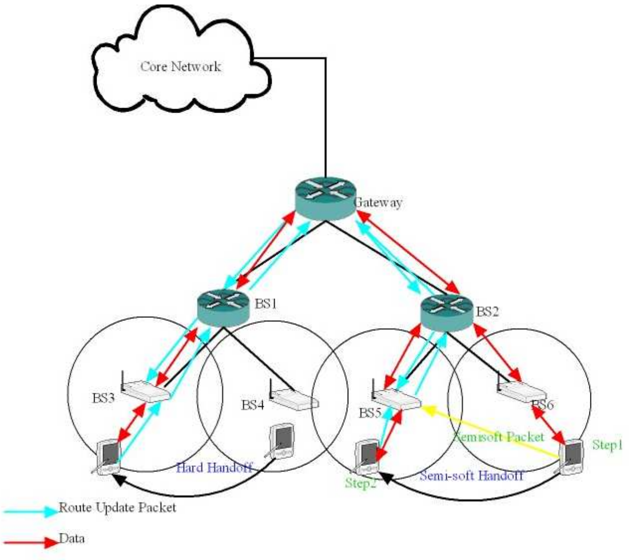


Figure 21. Cellular IP architecture Hard Handoff and Semi-soft Handoff

Hard Handoff: Hard handoff is initiated by the mobile node by sending a route update packet to the other base station. This packet is carried to gateway through that base station thus creating a route for the downlink from the gateway to mobile node. By the neighbour hop address the new base station uses the same link for the uplink also. The next packet to mobile node is routed through the new link or through the old link. A timer keeps the route state active until next route update or timeout.

Semisoft Handoff: in this case, the coexistence of the two routes for a short time is explored. Before sending the route update packet, the mobile node sends a semi soft packet to the new base station. In this packet a request to delay the further incoming packets at the gateway may be included. The route update will trigger a handoff and transmit any delay packets.

c. HAWAII

HAWAII (Handoff Aware Wireless Access Internet Infrastructure) [46] is also a domain based approach for supporting mobility. HAWAII uses specialized path setup which installs host based forwarding entities in specific routers to support intra domain micro mobility and to use default Mobile IP for inter domain macro mobility. Mobile IP provides good framework for macro mobility for users. When Mobile IP is used for micro mobility support it results in high control over head due to frequent notifications to the HA and high latency and disruption during handoff. The goals of HAWAII are:

1. Achieve good performance by reducing update traffic to home agent and the corresponding nodes.
2. Provide intrinsic support for QoS in mobility management.
3. Enhance Reliability.

HAWAII operates entirely in the wireless access network. Mobile hosts run Mobile IP with some extensions including NAI (Network Access Identifier) and route optimization.

Hawaii operation is explained in Figure 22, where Mobile Node obtains co-located care of address, using Dynamic Host Configuration Protocol (DHCP), when connecting to base station located in a foreign domain. It then registers with Home Agent. At the time of handover, Mobile Node keeps the CCoA, and the new base station answers registration request and updates routers. In this process MN views base station as a Foreign Agent.

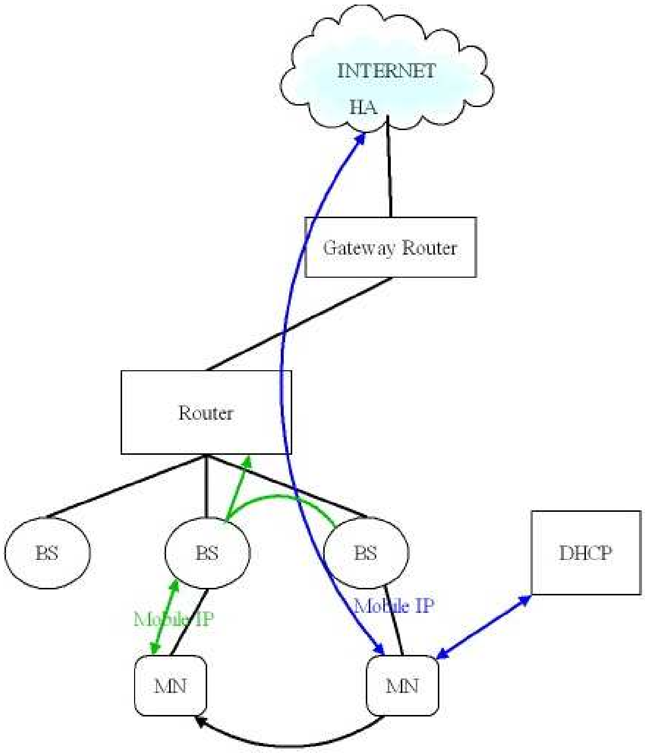


Figure 22. Hawaii Operation

2.5.3.5. MOBIKE

MOBIKE [47](IKEv2 Mobility and Multihoming) is a mobility and multihoming extension to the Internet Key Exchange version 2 (IKEv2) protocol [48]. So we need to present briefly the IKE protocol.

MOBIKE works on a simple approach where the party initiates the IKE_SA i.e.. The client in the remote VPN connection is responsible for deciding which address pairs to be used and collect this information if needed for deciding it. The remote gateway informs what address initiator has but doesn't update the IPsec SA's until it receives message from the initiator to do. Decision at the initiator is normally done by IKEv2 while contacting the responder. MOBIKE has the support for the NAT and stateful packet filters. When the addresses used for IPsec are changed MOBIKE can enable or disable NAT traversal in MOBIKE.

MOBIKE defines five different exchanges. These exchanges are described in the following:

- **Signalling support:** applications that wish to use MOBIKE for a particular IKE_SA must include MOBIKE_SUPPORTED notification in the IKE_AUTH exchange in the payload.
- **Additional Addresses:** both initiator and responder may include one or more additional addresses in the IKE_AUTH exchange. Recipient receives this address but doesnt do anything until it receives any additional messages. The Initiator and Responder maintain these addresses for future procedures.

- **Changing Addresses in IPsec SAs:** As explained above the initiator decides which address it want to use. Any change in the address is sent from initiator to responder by using UPDATE_SA_ADDRESS.

Change in the addresses result to some IKE exchanges between the peers.

- **Updating the additional addresses:** The changes of addresses between peers are done by INFORMATIONAL exchanges request message that contains address payloads or NO_ADDITIONAL_ADDRESSES payload.
- **Return Routability Check:** both peers can verify that the other peer can receive packets at the claimed address. This can be done before updating the IPsec SAs, or continuously at the time of connection.

2.5.3.6. Management through upper layer

Mobility support has also been considered at layers above IP (upper layers). For instance, the TCP migrate extension adds mobility support to TCP sessions. Specifically, it implements extensions to the TCP protocol, so that TCP sessions can continue without interrupt when an endpoint changes point of attachment. Similarly, Mobile SCTP [49] [50] builds upon the features of the SCTP transport protocol to offer transport layer mobility. Seamless mobility is inherent in SCTP and is accomplished through the multihoming support feature of SCTP and some of its extensions (Dynamic Address Reconfiguration).

SIP [51] is a protocol for signalling and session controlling which has been defined to support the multimedia applications. While comparing SIP with other similar protocols as H. 323 and H. 248, SIP is the most used protocol. In fact, SIP provides such a simplicity that leads to network services fast conception and deployment.

Moreover, SIP defines *multimedia calls, presence and instant messaging services* in its specification (multimedia calls in the version 5 of the specification, and presence and instant messaging in version 6). These features enforce the SIP position as the most interesting protocol for signalling and session controlling. It was adopted, in November 2002, as a *3GPP* signalling protocol and is, now, a permanent element of *IMS* architecture.

SIP was originally developed by the *Multiparty Multimedia SessIon Control* (MMUSIC) working group. Then, a SIP-dedicated IETF working group was created (the IETF SIP working group). This working group proposes a new standard for SIP. This standard does not make a break with the features provided by [52]. Indeed, [53] focuses on the same version 2.0 of SIP which is yet used. However, it adds better clarifications and definitions of the SIP mechanisms. In fact, the new standard corrects, first, the errors of the previous standard. Second, it provides more reliability for the *provisional replies* [54] [55] and more precision for the *SIP server localization* [56]. Finally, it introduces the *events notification* (*DMTF Tonality*)

[57] and *the support of TCP* for SIP. Note that UDP remains the adequate transport protocol for SIP, in spite of the TCP support, due to latency problems.

Within IP networks, SIP allows not only telephony services management but also many other services among them the visio-conference and instant messaging. As an example, *Microsoft* adopts SIP for some of its provided services such as instant messaging, presence and transferring data.

The SIP protocol presents a simple and flexible architecture that is moreover scalable. SIP affords also the localisation of terminals, the ability of users to engage in communications andcapacities of devices. However, the main role of SIP is to set-up sessions or associations between two (or occasionally more) Internet users. The session can be established between two Internet users or two systems addressable with *Uniform Resource Identifier* (URI). The sessions that are initiated with SIP can be used to exchange various types of media. Specifically, SIP sessions are commonly used for handling voice media over packet networks.

SIP is a client/server-oriented protocol with two types of messages: *requests* and *responses*. Messages are encoded in textual format using a structure similar to the *Hyper Text Transfer Protocol* (HTTP). The *Session Description Protocol* (SDP), with a mechanism of *Offer/Answer*, is used to open media canals and has to be modified to support IPv6.

2.5.4. Handover triggering mechanisms

- Horizontal vs. vertical handover: During the handover process, the Mobile Node (MN)'s point of attachment changes from one access node to another one. In horizontal handover, the MN moves within a single access technology whereas in vertical handover, the access technology changes.

- Make-before-break vs. break-before-make handover: In make-before-break handover, the connection with the new target access node is established before releasing the connection with the old one. Conversely, in break-before-make handover, the old connection is terminated before the new one with the new target access node is established.

- Hard vs. soft handover: A hard handover is one in which the connection in the serving cell is released and only then the connection in the target cell is engaged. A hard handover is also known as a break-before-make handover. A soft handover is one in which the connection in the serving cell is retained and used for a while in parallel with the connection in the target cell. This handover is called a make-before-break handover.

- Layer-2 vs. Layer-3 mobility: The layer-2 (L2) mobility refers to the case where the MN roams among dierent access nodes while the point of attachment to IP network remains the same. Otherwise, the layer-3 (L3) mobility involves the change of IP addresses.

- Global vs. local mobility: The global mobility protocol handles mobility across access systems by associating the global IP address with the new local IP address at a fixed global mobility anchor. The mobility within one access system is managed by a local mobility management protocol.

2.6. Summary

A clear trend is emerging in the form of fixed and mobile telephony convergence, access technology convergence, service convergence, multi-standard device convergence, etc. Interworking of heterogeneous networks is inevitable for the sake of user service continuity taking advantages of each network. In this chapter, we have addressed a global view of the mobile network evolution from the first generation towards the next future generation which is likely to be characterized by the interworking of heterogeneous access networks. We have proposed different interworking architectures issues surrounding them in this chapter. Issues of mobility management are still at novice stage there are number of issues that has to be resolved to obtain seamless mobility. Issues of security, mobility management, network selection are to be addressed properly for heterogeneous networks as the operating parameters surrounding these networks differs. Obtaining seamless mobility is the main criteria which have to be addressed by these mechanisms. In the following chapters we will provide solutions on interworking in access networks, mobility management, low latency during roaming and handover.

Chapter 3. Seamless Roaming Architecture

The increase in the usage of different access technologies lead to a need for new mechanisms to manage interworking and roaming between different network technologies. To provide secure and seamless roaming capability for mobile users across different access network domains, belonging to the same or different operators, we propose a roaming & interworking solution using intermediary entity, called Roaming Interworking Intermediary (RII). A generic RII-based interworking and roaming architecture between WIMAX, 3GPP (third Generation Partnership Project) and WLAN networks is presented. This chapter describes the operational practices, technical architectures, authentications and mobility mechanisms to enable a subscriber of one operator to roam securely into the access networks of another operator. A test-bed has been setup, using WIMAX, Wi-Fi equipments and real operational cellular network, to demonstrate and evaluate the proposed solutions. The robustness, feasibility and efficiency of the proposed architecture are proven through different user scenarios and services.

3.1. Introduction

Real-world interworking/roaming can encompass a large number of possible scenarios and network configurations. In general, a roaming agreement is required to allow subscribers of one operator to gain access to networks of other operators. The agreement deals with technical and commercial aspects related to the roaming procedure, particularly how costs and earnings are divided. Regardless of roaming relationship, the interworking between cellular and WIMAX/WLAN networks can be categorized into two main approaches: tight-coupling and loose-coupling [58]. Initial work on the interworking between WIMAX and 3GPP networks has been done by the WIMAX Forum in [59]. In fact, the 3GPP-WLAN interworking models proposed in [21] have been reused for the 3GPP-WIMAX interworking. Other than previous proposed model there are different interworking models proposed for seamless secured roaming in heterogeneous networks. The current 3G LTE architecture aims at developing an evolved 3GPP radio access and core networks to enhance the system performance. For the inter-system mobility management, the 3GPP cares much about the interworking between 2G/3G and 3G LTE while the interworking between 3GPP and non-3GPP access systems has not been adequately addressed. There must be an intelligent interworking architecture to support these technologies and mechanisms to provide seamless and transparent services to end users.

On the road to design the roaming between different networks, a third party roaming intermediary has been introduced [60] [61] [62] [63]. The intermediary can enable roaming between two networks without any direct agreements between operators of these networks. While the number of hotspot operators has been rapidly increased, the roaming capability without direct agreement becomes crucial. Besides the roaming intermediaries among hotspot operators, the roaming broker facilitating the roaming between mobile and hotspot operators is also proposed [63]. It is responsible for providing the information of user's home services to the visited domain, taking care of the dynamical relationship and determining signalling and accounting procedures. Unlike a broker, clearinghouse [61] does not resale the WLAN access, instead provides a trusted intermediary for implementing roaming agreements. Most of the current solutions are proprietary ones. Furthermore, several crucial issues for handover and roaming such as network selection, handover, security, mobility, QoS and network management between the home and visited networks has not been addressed in any of the above solutions. In other words, they could not maintain on-going communication sessions while users roam between home and visited networks. In our work, we aim to extend the roaming intermediary concept to deal with not only the roaming but also the interworking issue, called Roaming Interworking Intermediary (RII). Importantly, the proposed RII will enable the secure handover across different access systems and different operator domains without service interruption. The proposed RII architecture is based on LTE and compatible with the mechanisms mentioned above with minor modifications.

RII acts like a broker in the RII architecture between home and visited operator networks. RII provides mobility management, context transfer between service providers, security architecture for authentication and associations of users while roaming, and presence management. In RII network providers need not to have SLAs with each others, instead they provide roaming for foreign users with the help of RII architecture. This architecture have a local RII in WLAN and WIMAX network operators architecture and core RII in 3GPP architecture, which provides the location management for the users, maintaining presence of the users while accessing different networks, assisting users during authentications and handovers. A terminal is equipped with a Configuration Manager (CM) to assist handovers, Network Selection, and enforcing security mechanisms according to the selected access networks.

Using RII architecture we have managed to achieve secure authentication and re-authentication during roaming and handover procedures. The proposed authentication procedure using RII provides low latency and compatible for the existing interworking architectures and procedures. While an RII architecture greatly simplify service delivery for nomadic users, the complexity of managing and exchanging profiles, SLAs and configurations between heterogeneous networks and the RII becomes very complex for network administrators and systems integrators. The operator’s management models encompass a set of profiles (User, Content, Context, Configs, etc.) which must be aligned with the RII to allow interoperability. The user and operators are managed in an efficient manner using network management tool proposed for this specific architecture. Arguably, the first step toward simplifying data integration is to choose a single, yet powerful language in order to maintain a coherent knowledge base. This language, or specification, will then be translated into platform specific formats. Our investigations resulted in the choice of the W3C Web Ontology Language (OWL) [64] as the RII specification language. Using Protégé [65], a tool for manipulating OWL-based ontologies, we have designed a set of concepts and properties based on our previous work in [66]. Also, to reduce the visual complexity of designing the system and to enable a fast prototyping and deployment of our broker, we have developed a tool for loading and manipulating ontologies. This tool implements our platform transformation pattern and automatically generates specific configuration files from the ontology instances (individuals). These configurations are then deployed in different areas of the access network. Section 2 of this chapter presents generic intermediatory architecture RII, section 3 provides different functionalities of RII architecture. Section 4 and 5 provides interworking models and interworking through WLAN, WIMAX and 3G networks. Section 6 provides detailed testbed implementation and results of proposed architecture. Section provides information on network management issues solved and tools proposed using RII architecture. Comparisons of other architectures and proposed architecture are provided in section 8 and conclusion in final section.

3.2. Proposed RII Architecture

Novel RII entity facilitate interworking/roaming among different access technologies and to enable the intersystem handover with uninterrupted services. The major difference between existing solutions and our proposed one is that both roaming and handover aspects are addressed. The proposed architecture will take into consideration different contractual relationships between operators. If the operators have a close Service Level Agreement (SLA), the roaming can be done directly between two involved networks. In this case, the RII will ease the roaming management and enhance the service continuity. On the other hand, if the operators have no agreement, the roaming will be handled with help of the RII. The interworking & roaming architecture among the 3GPP, WIMAX and WLAN networks is illustrated in Figure 23.

This architecture contains a global roaming intermediatory called Global RII which acts as a mediating network between access networks. As shown in the figure the each operator architecture has local roaming intermediatories. They are interconnected to the global roaming intermediatory called Global RII. A mobile network operator (MNO) can deploy WLAN and WIMAX access network as an extension of its existing 3GPP network to best use its existing infrastructure and to best serve its clients. For each non 3GPP access network, the operator uses one local RII to connect to its core RII in order to manage handover and roaming. The MNO can also interwork with other WLAN/WIMAX operators in tight-coupling scenarios if they have a SLA between them or in loose-coupling scenarios with the help of Global RII.

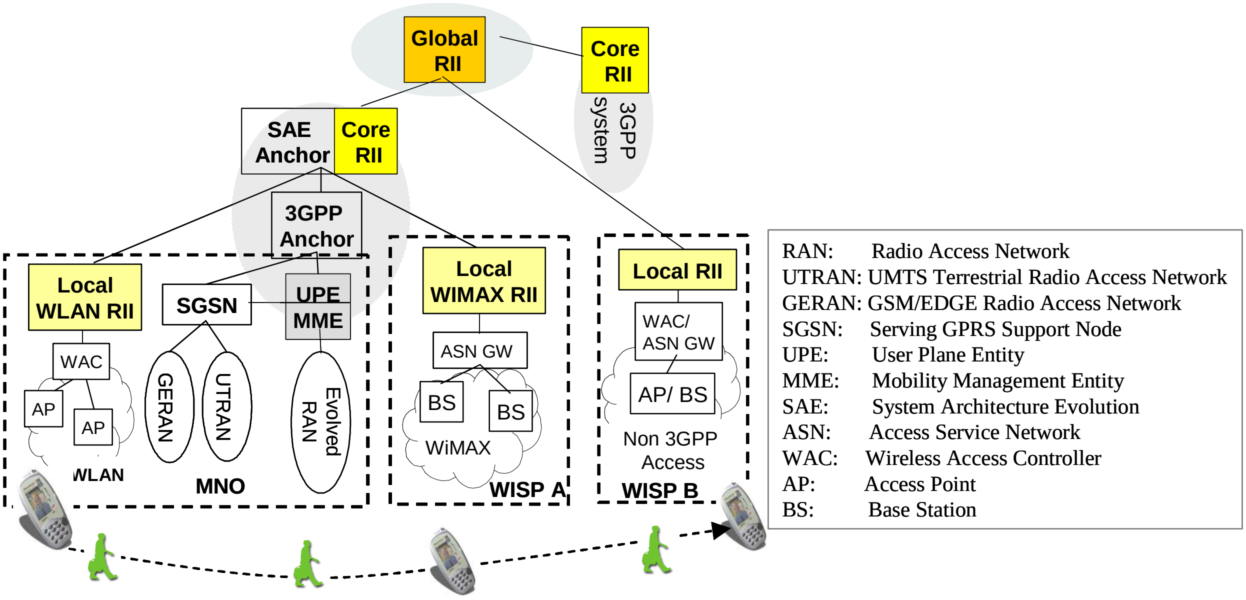

Global RII
Core RII
3GPP system
SAE Anchor
Core RII
3GPP Anchor
Local WLAN RII
SGSN
UPE MME
WAC
AP
AP
WLAN
GERAN
UTRAN
Evolved RAN
MNO
Local WIMAX RII
ASN GW
BS
BS
WiMAX
WISP A
Local RII
WAC/ ASN GW
AP/ BS
Non 3GPP Access
WISP B
RAN: Radio Access Network
UTRAN: UMTS Terrestrial Radio Access Network
GERAN: GSM/EDGE Radio Access Network
SGSN: Serving GPRS Support Node
UPE: User Plane Entity
MME: Mobility Management Entity
SAE: System Architecture Evolution
ASN: Access Service Network
WAC: Wireless Access Controller
AP: Access Point
BS: Base Station

Figure 23. RII architecture for WLAN, WIMAX and 3GPP networks

The architecture is consistent with the 3GPP Long Term Evolution architecture studied within 3GPP standard body. The mobility management for different interworking/roaming scenarios is achieved with help of different types of RII. The Global RII functions as a third party that interconnects the different local RII and core RII in case there's no agreement between the operators. The operators will be interested in using the Global RII to support the roaming to the networks of other operators as a value-added service feature for their subscribers. The Global RII handles the security (e.g., authentication, authorization, accounting…) the mobility management, the presence management and the network selection for intersystem mobility. One of the main aim of Roaming Intermediary is to provide security with low latency, we introduce a concept of unified authentications and authorization during roaming in the architecture. For low latency during handover we introduce security context transfer. Handover initiation and network selection is also supported in this architecture.

3.2.1. Global RII

Global RII works as a mediating network between different operators networks. The main role of the Global RII is to provide services for security, billing, handover management, presence for the users of the network operators while they are roaming along different administrative domains. It provides security context of the user to visiting network. Handover initiation of the users arrives to the Global RII for the target network from a home network, then Global RII sends the request and receives handover initiation from the target network, after receiving the initiation it sends the success to initiate network for a possible handover.

After handover process it does security context transfer to the home network from the target network. After authentication of the user in the target network Global RII starts accounting the user terminal and does the billing of the roaming service. The subsystems of Global RII are presence management (geo information system mapping), authentication management, mobility management, accounting unit, operators information unit (SLAs, policy manager), and context transfer.

Location Management is the subsystem of RII, it is equipped with GIS mappings of the network coverage areas in cells. If there are any queries from operators networks about the available networks in a particular area this section answers to them providing information in the coverage networks. If there is no information available in this section, it forwards the queries to all the other operators RII and gets the feedback to answer the queries.

Authentication Unit provides the authentication support for the access networks and subscribers. In this process the global RII issues the temporary username and passwords for the access networks. These details are provided to the users by their access networks to the subscribers, when a subscriber trying to access the foreign networks the details provided by home networks are used to access the networks. The visiting networks then forward details to the global RII, which checks the username from assigned database of the networks and forwards the authentication details to the home network of the subscriber for authentication, or the global RII does the authenticate the user and does the accounting and forwards the session details to their home networks depending on the SLA between the home and visiting networks with the global RII.

Accounting Unit deals with accounting of the roaming services used by the operators in the other networks for their users.

Handover Unit is used for handover decisions, support for the users in the access networks.

Mobility Management unit provides mobility support at IP layer for mobile terminals, the unit acts as upper FA or HA for registering mobile terminals and providing IP support when the mobile is roaming or interworking through different access networks.

Service Providers Unit, SLA and policy management of the operators and operator subscribers are handled here.

Presence management unit, provides presence of the user in access networks for different services, it is an add on functionality to provide efficient services such as VoIP during mobility etc… in the architecture

3.2.2. Local RII

Local RII provides support for authentication of the users, mobility management, location update, GIS mapping, network coverage information, users database in the operator access networks. The local RI contains Location Management unit, Authentication unit, Mobility management unit, Context transfer unit for communication between other RIIs and with global RII for queries.

Authentication Unit is the one in which users are authenticated in this system, local RII receives the request for authentications and re-authentications; the terminal is authenticated according to access ecurity mechanisms for the authentication. For a request of authentications from other networks, keys which are generated at the startup of terminal are sent to the other RIIs and global RII with the help of context transfer in Local RII to make authentications with low latency. This mechanism assigns the temporary usernames and associated keys to the subscribers allocated by the Global RII, this unit later authenticates the subscriber with the help of the Global RII. The subscriber terminals are assigned to use Global RII as NAI when accessing the foreign network.

Location Management is the unit in which locations of the users are maintained, and GIS information with the corresponding access coverage are maintained also. If there are any queries from terminals with its present location the location manager finds the availability of networks and responds to terminal.

Handover Management Unit, terminals are assisted during handover and roaming to choose the best network according to the policy of the user, QoS, cost, SLAs with the other operators taking into consideration.

Mobility Management, in this process the mobility of user is managed by this unit at the IP layer. In this process the FA or HA sends router advertisements, whenever mobile terminal after authentication receives this advertisements it sends a router solicitation to HA/FA. After receiving the request HA/FA register mobile device

3.2.3. Core RII

Provide the interworking or roaming services for the operators that would like to provide the interworking or roaming services as value-added to their subscribers. The Core RII is responsible for providing the provisioning information such as preferable access network, undesirable access network, charging information of each access network, etc…to the mobile terminal. The Core RII receives the handover request from mobile terminal including the list of potential inter-system cell candidates from the RNC (ASN GW/ WAC) and carries out the handover preparation for the target access network. The Core RII will perform the network selection to eliminate the undesirable target IDs. The Core RII will retrieve the routing information to reach the target RII by consulting the presence database and DNS server and then sends the handover preparation request to target RII. The target core RII is responsible for notifying the imminent handover to UTRAN and allocating the re-configuration radio setup information to the UE via the serving RII. The Core RII will create the security credentials for the UE and transfer the security context and user context to the target RII and UE for fast re-authentication. The core RII then update the user plane routing information and the presence information once the handover completes.

3.2.4. Mobile terminal

Communication Manager is provided in the mobile terminal, which assists the user terminal to access the operator networks in secured manner. CM is equipped with L2 and L3 mobility management, location management, Network Selection, client for connecting the roaming server of the home network. The logical diagram and information flow between different units of CM is shown in Figure 24. The CM on the terminal provides constant information exchanges between the Local RII or Core RII in the home network for the location update, NS, Authentication and re-authentication.

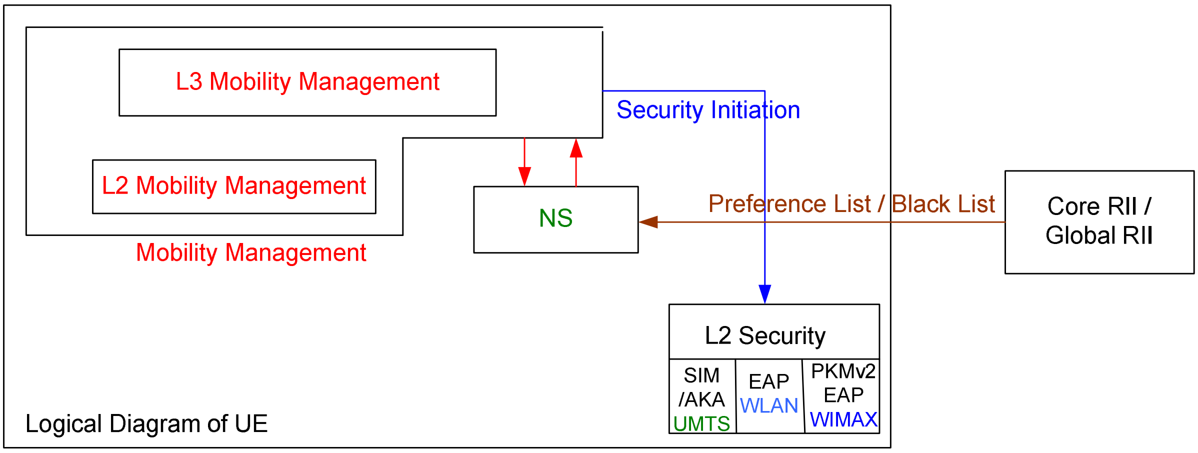


Figure 24. Logical Diagram of UE

3.2.5. Functionalities of RII architecture

RII consists of six different components: network selection, security management, handover management, mobility management, Qos and presence management, performing functionalities for seamless roaming across different service provider networks. Within an RII entity, the HM is a centralized component that interworks with five other components as illustrated in Figure 25. In the global interworking and roaming architecture, the coordination between two interconnected RIIs is shown in

Figure 26. We can distinguish six kinds of information exchanged between RIIs: provisioning information exchange between with the NS components, security context between the SM components, handover trigger and management between HM, radio and resource allocation management between QoS manager, mobility and binding between MM and presence and location management between PS. The details of such coordination will be presented with the handover procedure. Here we will describe the functionalities of these six components.

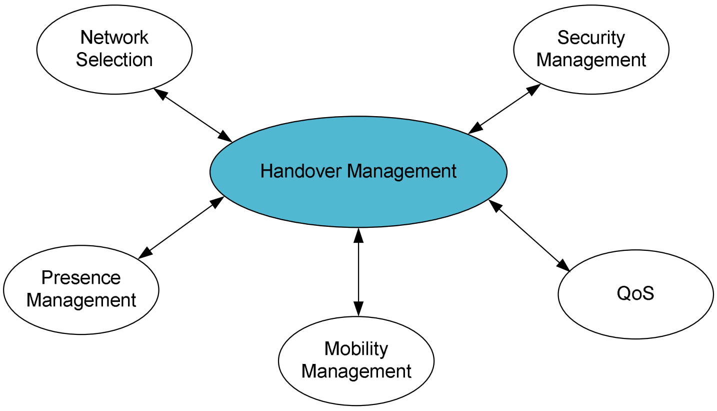


Figure 25. RII functional components

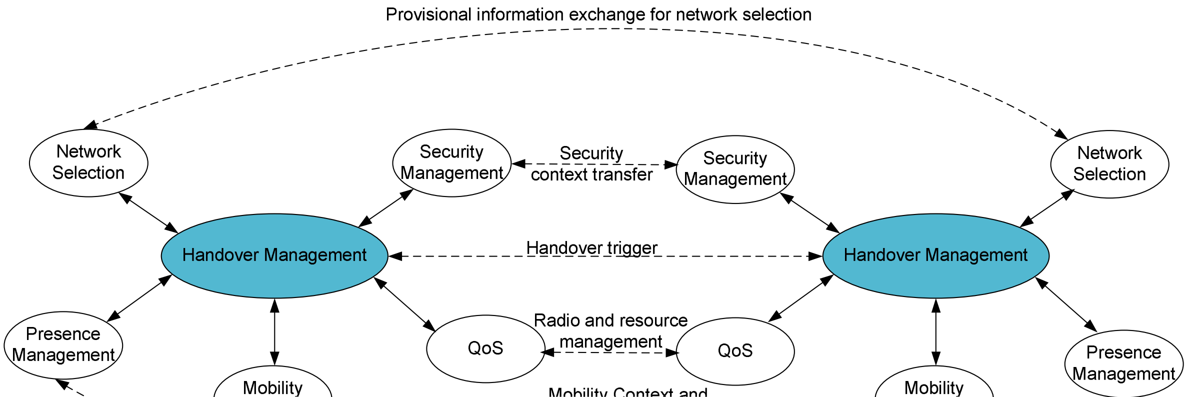


Figure 26. Two interconnected RII Components

3.2.5.1. Network Selection

In this process mobile terminal does network selection for accessing different networks at any given time and location. We have identified two different methods to achieve network selection: Client based and network based selection. Network Selection involves collecting available information from surrounding access networks. The information gathering is performed by terminal, when it is powered on or when it moves across different radio access networks. This procedure allows to determine a generic set of parameters describing access networks and devices (type of access network technology, access network operator, QoS support, cost, remaining battery capacity...). In addition, the information related to the QoS status of the current running applications, the mobile terminal's velocity and the cell coverage radius is also collected.

Physical access networks measurement: The access network characteristics identify the available access networks and their radio link quality. Such information is measured by the physical radio interfaces periodically or when an event occurs. Different link indication parameters like RSS, SNR, SINR can be monitored.

Terminal capabilities: The terminal capabilities information is related to multimode capacity, available radio interfaces and remaining battery. It can influence the network selection and handover management.

Service degradation: The service degradation information is related to the trade-off between the application's QoS requirements and the quality of the current connection. It can be measured through Real-time Transport Control Protocol (RTCP) reports for instance. The combination of service degradation and radio link quality allows describing more accurately the quality of the current connection than the fluctuating physical-layer information only.

Terminal's velocity: The terminal's movement velocity is also an important factor for mobility management in heterogeneous environments. The velocity estimation in mobile cellular systems can be achieved using the Doppler spread in the received signal envelope [67], the eigen-matrix pencil method [68], the time-frequency characteristics of the received signal [69] or the Global Positioning System (GPS)-assisted method [70].

User profiles: contain the user's identities for different access networks and subscribed services, user preferences, and mobility policy repository. In the context of the terminal-controlled mobility management, we are first interested in user preferences, which is a rating relationship among the parameters considered in network selection. Each preference has a relative weight that users assign to each criterion depending on their requirements. User preferences should be adequately configured for different contexts which are characterized by currently connected access node, terminal's velocity and running applications class. As user preferences influence the network selection and handover management process, future terminals will have to provide users with the facilities (e.g., Graphical User Interface dedicated to user preferences configuration) to specify and alter their preferences in an easy manner. Additionally, the terminal can maintain the mobility policy database that contains a black list of access network operators with whom the user has had a bad experience. The black list will be updated through feedback from handover execution failure and bad QoS as perceived by the application. The users can manually pre-specify the black list and remove a specific access network from this list.

Interface management: Based on the gathered information, the interface management will decide to turn on, stand by or turn off one or more radio interfaces to optimize the power consumption. Interface management becomes thus a constraint for network selection.

Local Database: The mobile terminal contains local database contains details of previous connected networks and access networks information provided by the home access network. The information of available access networks are informed to the mobile time during initial registration or through updating profiles through home access networks local or core RIIs. The local and core RIIs coordinate with each other and with global RII to exchange and maintain access networks information.

SLA: The mobile terminal contains the SLAs information of home operators and visiting operator's. Home local RII negotiate SLAs with other access networks RIIs and Global RII, while mobile terminal performing network selection it takes SLAs into consideration, the access network which have direct SLAs with the visiting network with the home networks given higher preference than the access networks which have indirect SLAs through global RII.

After identifying the network selection criteria, the user preferences configuration and interface management, network selection triggering conditions are addressed. Triggering network selection depends on the gathered information and the interface management. In network selection procedure the gathered information is processed and access network with proper SLA associated with the mobile terminal with good SNR ratio and required QoS satisfied is selected. Whenever the access network doesn't provide any service, the network selection procedure is triggered. The whole procedure is performed on the mobile terminal with static context transfer information exchange with the home networks RIIs. We also created a new procedure where the network selection procedure is performed with the help of home and visiting network dynamically and efficient manner. In this process the mobile terminal does the context transfer before disconnecting to present network with the home network. The location of mobile terminal is identified through GPS and the future location of mobile terminal is predicted, using GIS information system the location is mapped to the available access network, home RII of mobile terminal negotiates with the available visiting networks and provides the information to mobile terminal, we have developed new techniques and extended existing mechanisms to provide this support, full details are mentioned in chapter 5. Using this procedure the NS latency is also reduced and performance of the architecture is increased. Once the network is selected through NS procedure, it forwards the information to the handover management procedures.

3.2.5.2. Handover management

The handover management is responsible for preparing the handover by triggering the network selection, routing the handover preparation request based on the information from the different components, checking the QoS support in candidate target access networks and assigning the connection setup information for an imminent handover terminal. Also handover management procedure does communicate with other access networks RIIs for preparing and managing other handover procedure to prepare the visiting network to accept the mobile terminals. It makes the handover decision and notifies the handover to the data plane anchor for handover execution preparation.

3.2.6. Security Management

The SM is responsible for handling authentication, authorization and billing issues for intersystem roaming users. The SM encompasses the Authentication, Authorization and Accounting (AAA) functionalities. In addition, the SM can manage and communicate the user's security context (i.e., authentication identity, user identity, certificates, authorization and encryption keys) for roaming and vertical handover preparation. It is in charge of authenticating and authorizing users based on the subscriber profile retrieved from the Home Location Register (HLR) or from security context transferred by users serving/home network. The SM in the global RII plays the role of a mediator for roaming contract establishment and context transfer between serving and target access networks to optimize handover latency caused by re-authentication procedures.

RII architecture provides high level security architecture where the access networks are independent from any other access network, where as Global RII mediating with all the networks reduces the complexity of routing, security with every individual operator networks, configurations and maintenance tends to ease. The user identities and certificates are generated and then they are distributed to various components of RII architecture and users. Whenever the users are attempting to access network, the local and core RII of networks coupled with Global RII provides assistance for authentications. The Global RII and Local RIIs are configured so that the NAI of the access networks can be identified at any given instance.

3.2.6.1. Mobility management

The proposed architecture allows users to roam among different access systems while maintaining on-going communication sessions. When a UE moves within WLAN/WIMAX systems, the handover will be managed by the WAC/ASN GW and the local RII. Similarly, the handover within 3GPP access systems is managed by the SGSN/MME and the core RII. When the handover occurs between two different access technologies or two different operator domains, the procedure will depend on their contractual relationship. Hence, the hierarchical mobility concept becomes a crucial tool for handover management. Using client based or network based mobility management to achieve mobility in multi operator networks.

Client mobile IP provides mobility from mobile terminal support with the access network. The local RIIs and core RII are equipped with foreign agents (FA) and Home agents (HA). When the mobile terminal is authenticated through RII, the HA/FA sends a router advertisement to the mobile terminal and sends a router solicitation to FA, listening to the reply HA/FA checks the data and does the binding registration and establishes the tunnel for mobility management. The mechanisms also supports during roaming and multi homing scenarios, and heterogeneous networks. The AAA functionalities inside mobile IP also add extra functionalities to support roaming scenario. Hierarchical RII-based mobility management is represented in Figure 5.6. If the handover occurs between two indirectly interconnected access networks, handover signaling will go through intermediaries. For example, if the handover occurs between access network (4) and (5) (case 1), the core RII (1) will play the role of a mediator. If the handover occurs between two access systems that have no direct roaming agreement, case 2 in Figure 27 for instance, the handover is achieved with help of the global RII. The service continuity during roaming between two operators that have no existing agreement is one of the relevant advantages of our proposed solution.

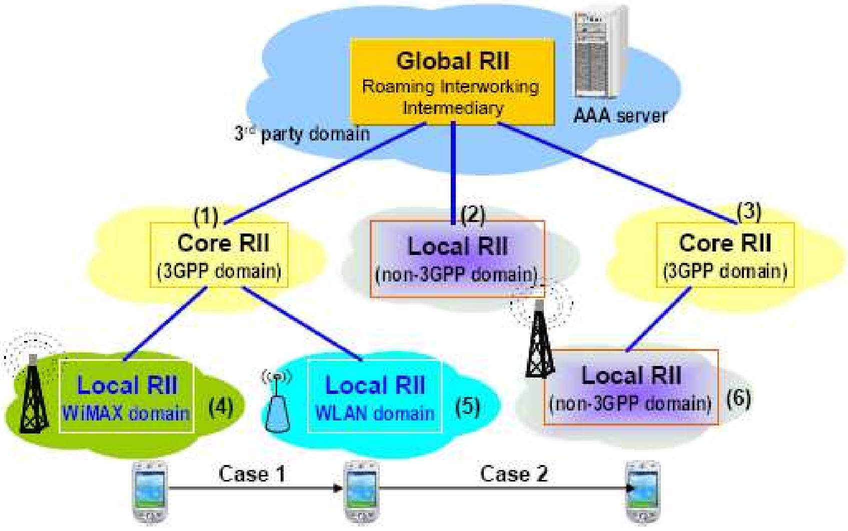


Figure 27. Mobility management in RII architecture.

Proxy mobile IP based on network mobility management, in this process the mobility is provided by network entities instead of mobile client. The functionalities of FA have been modified to support network based mobility. In this process the mobile client keep its home address in the foreign domain. Using PMIP seamless mobility is achieved using RII architecture and its components, more details of PMIP is explained in detailed in chapter 4.

3.2.6.2. QoS Management

The main functionality of this process is to provide resource management and ensuring better QoS for mobile terminals during roaming in RII architecture. The local, core and global RII provides resource allocation when the mobile terminal initiates handover. The local and core RIIs negotiate with network entities such as APs and BS for resources and bandwidth availability for ensuring better QoS when the mobile terminal performs handover. The local and core RII communicates with mobile terminal requesting its services and required bandwidth after performing handover, mobile terminal does respond with appropriate reply. Using network selection results the local and core RII checks for resources at the access networks, if the enough resources are not available the mobile terminal and local/core RIIs are advised to use another networks, if the required resources are sufficient the access network allocate the resources before the mobile terminals move to visiting networks.

3.2.6.3. Presence Management

The PM stores and manages the presence information of users which describes how to reach them. The presence information specifies the serving access network, the serving RII and the location of users. Whenever a user roams to a different access network, at the end of the handover procedure, the user's presence information is updated in the RIIs involved. The paging mechanism is included in the PM to wake up standby users. The PM may also provide functionalities of a presence server.

3.2.7. Interworking models

Different interworking scenarios are studied through this architecture. In this process wireless internet service providers like WLAN, Network Access providers like WIMAX, and mobile network providers interwork with this architecture. In some cases where mobile network providers want to provide services in WLAN and WIMAX networks, operator can deploy directly in his architecture or can have direct SLA's between the operators (Tight Coupling Architecture). In some cases when there are no direct agreement between the operator and mobile network provider they use the intermediate network through this architecture to provide service to its users (Loose Coupled Architecture).

3.2.7.1. Tight coupled architecture

This scenario corresponds to the case where the mobile network operator (MNO) would like to deploy the WIMAX access network or WLAN access network as an extension to their existing infrastructure. As show in

Figure 28 the mobile network operator deploys a WLAN network in his architecture and has direct SLA with different operators. In this architecture all the other Local RII communicate with the Core RII for authentication of the users, network selection, handovers and mobility management when they are directly coupled with the mobile network or if they have a direct SLA with the serving network.

3.2.7.2. Loose coupled architecture

In this scenario a mobile operator does not have direct SLA agreement with the other wireless ISP providers and Network Access providers. In this case the Global RII acts as a mediating network to provide services to the users along different service providers. To maintain low delays during roaming security context transfer and mobility management is introduced in this architecture. As shown in this Figure 29 different service providers interconnect with the Global RII.

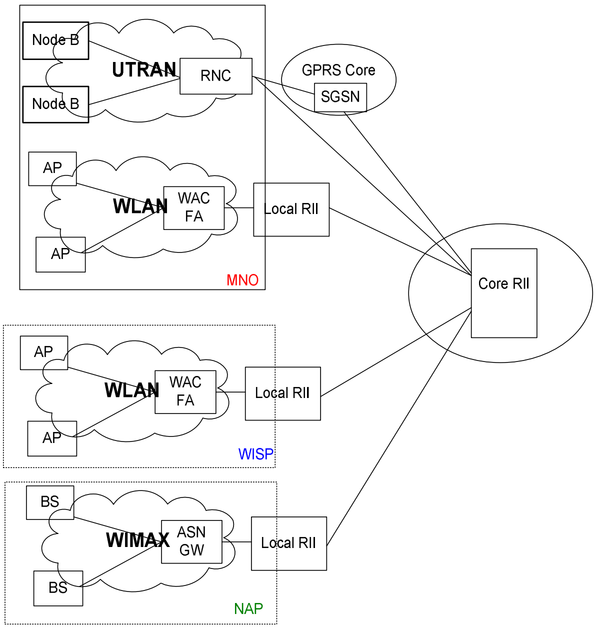


Figure 28. Tight coupling Architecture

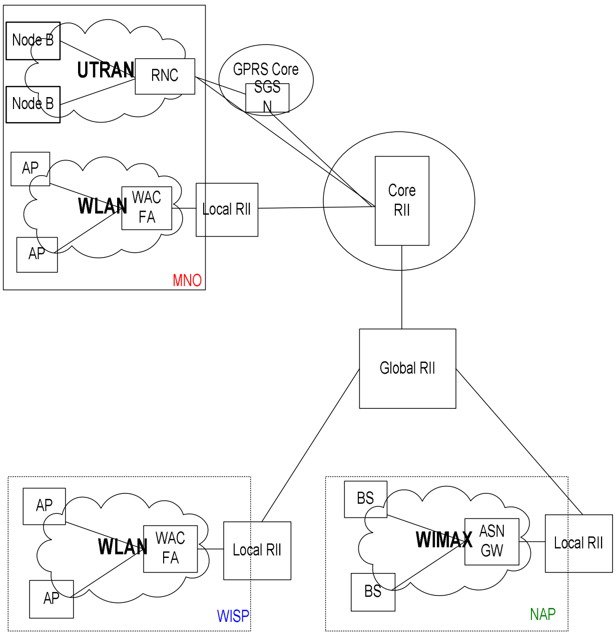


Figure 29. Loose coupling Architecture

3.3. Interworking through WLAN, WIMAX and 3G networks

The proposed architecture allows users to roam among different access networks while maintaining on-going communication sessions: the roaming and mobility management should be done simultaneously. The hierarchical mobility concept (i.e. localized and global mobility management) is used in our proposed architecture. If the handover occurs between two indirectly interconnected access networks, the handover signalling will go through intermediaries. If the handover occurs between two access networks that have no direct roaming agreement, one wireless operator and other the roaming and handover is achieved with help of the global RII. Note that the service continuity during roaming between two operators that have no existing agreement is one of the key challenge of our proposed solution. A generic signalling exchange is illustrated in Figure 30.

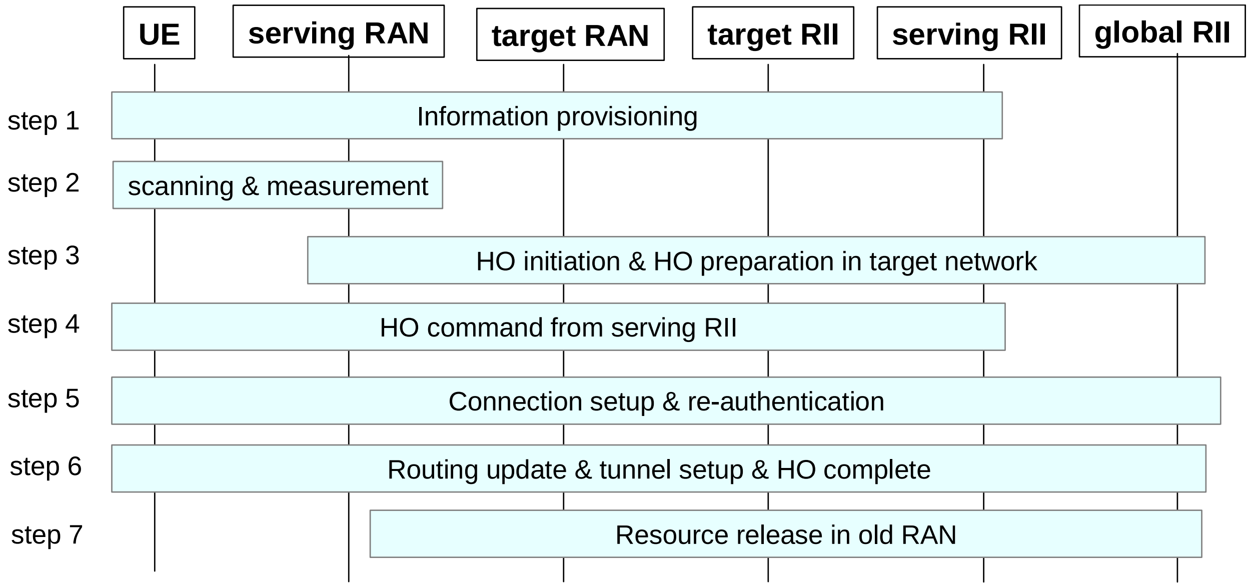

UE
serving RAN
target RAN
target RII
serving RII
global RII
step 1
Information provisioning
step 2
scanning & measurement
step 3
HO initiation & HO preparation in target network
step 4
HO command from serving RII
step 5
Connection setup & re-authentication
step 6
Routing update & tunnel setup & HO complete
step 7
Resource release in old RAN

Figure 30. Generic handover & roaming signalling exchanges

Step 1	During the communication on the serving RAN, the UE receives the provisioning information (e.g., neighbouring cells information, preferable access network list…) from the NS component of the serving/home RII.
Step 2	The UE measures the link quality of serving cell and neighbouring cells and sends measurement reports to the network either periodically or event-based.
Step 3	Once the vertical handover is initiated, the serving RAN will perform the handover preparation: checking whether candidate target access networks can support the imminent handover and performing the resource reservation in advance. The handover preparation request will be routed to the indicated target RAN via the global RII if needed.
Step 4	The serving RII sends the UE a handover command including recommended target cells associated with the connection setup information. The UE selects the most suitable cell among the recommended ones and sends a handover indication to notify its choice to the serving RII for handover execution preparation.
Step 5	The UE performs attachment and re-authentication with the target RAN. If the security context transfer mechanism is used, the target RII authenticates the UE without need to communicate with its home network.
Step 6	Once the connection to the target RAN is successfully achieved, the UE sends the MIP registration to the HA to update the data plane path. The data tunnel will be then established to route packets to the UE.
Step 7	After the handover completion is notified, the resources in the old access network will be released and the presence information will be updated in the RIIs involved.

Table 4. Generic inter-operator domain handover steps description

3.3.1. Interworking Scenarios using RII architecture (tight coupling architecture)

These scenarios correspond to the case where the mobile network operator (MNO) would like to deploy the WIMAX access network or WLAN access network as an extension to their existing infrastructure (tight coupling architecture). In this case, the ASN GW and WAC will emulate the role of the RNC. Besides, the scenario corresponds to the case where a mobile network operator interworks with a WLAN Internet Service Provider or a WIMAX Network Access Provider. Concerning to WIMAX deployment, the Access network (ASN) and the Core service network (CSN) may belong to two different owners. The owner who provides ASN is called Network Access Provider (NAP). One ASN may be shared by several Network Service Providers (NSPs). Thus, an ASN may be shared between CSN and 3GPP core network. Otherwise, the MNO can interwork with a “NAP+NSP” (NAP and NSP belongs to single owner). This scenario refers to the tight-coupling inter-working within the same administrative domain.

Handover between UTRAN and WLAN/WIMAX is performed as a forward handover i.e. the resources and address allocation are prepared in the target network before the UE is ordered by the source network to change to the target access network. The handover preparation is carried out by the core RI and local WLAN/WIMAX RI. Some enhancements such as security context transfer and packet forwarding functionality are used to reduce the interruption time during the handover.

The message sequence chart in Figure 31 and Figure 32 illustrates the high level procedures for the handover solution.

3.3.1.1. Handover from UTRAN to WLAN AN

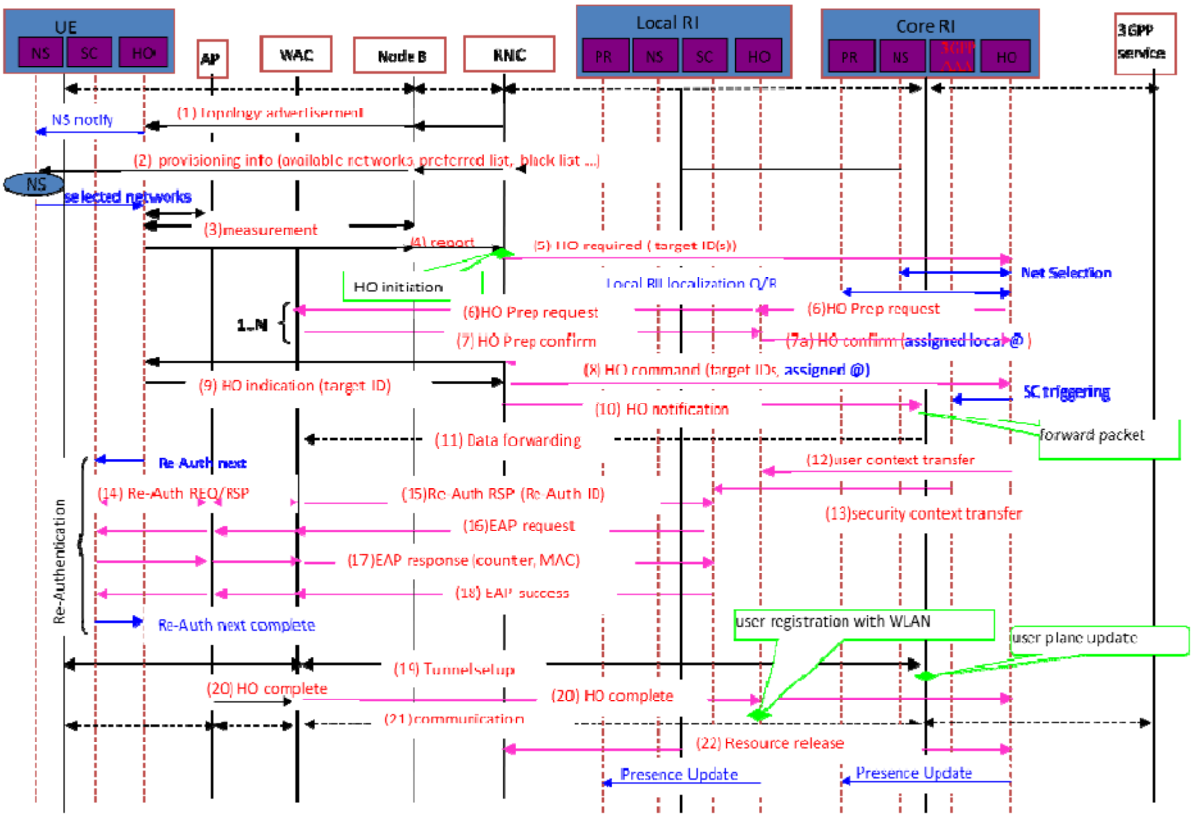


Figure 31. Handover from UTRAN to WLAN Access Network

1) During the communication, the RNC sends topology advertisement (or measurement control message) to the UE to indicate the radio information of the neighboring cells on which the UE can measure the radio link quality. The message includes the information which allows the UE to quickly synchronize with the neighbouring cells and to measure the signal strength.

2) The network selection component in Core RI sends the provisioning information to the UE which may include the preferable access network list, the undesirable access network list, the charging information of certain access networks, etc. for the purpose of network selection in UE.

- Selected network: Based on the topology advertisement and provisioning information, the UE will filter the available access networks for measurement purpose. The NS component in UE will notify the MM component the selected neighboring cells for measurement.

3) The UE performs the measurement procedure on neighboring UMTS cells as well as the intersystem measurement on the neighboring WIMAX and WLAN cells.

4) The UE sends the measurement report to the RNC. The UE can report the signal of WLAN or WIMAX to a false maximum value to indicate its preference for handover to this cell.

5) Based on the measurement report, the RNC decides whether or not to trigger horizontal or vertical handover. If RNC decides to trigger vertical handover to one among the inter-system cells reported in previous step, it will send a HO required message including these potential target IDs and the required QoS of the current running application to the Core RI.

- Network selection: The Core RI may make the network selection to eliminate the undesirable target IDs based on its policy and its preference. It will select the target IDs in the preference order as follow: the target access network deployed by the same operator (scenario 1), the target access networks which have a tight-coupling interworking (scenario 2), and the target access networks that can be reached via inter-AS RI (scenario 3).

- RI localization query/response: The Core RI will learn the address of the target RI by consulting its presence database.

6) The Core RI sends HO preparation request to the local WLAN RI if there exist the WLAN target IDs deployed by MNO in target ID list. The local WLAN RI in turn sends this preparation message to the WAC that controls the indicated target IDs.

7) The WAC sends back the HO confirm to the local WLAN RI if the WAC can reserve the required resource for the handover. 7a) the local WLAN RI then adds the local assigned IP address to the HO confirm message sending to Core RI. This local address IP is used by the UE to establish the IP connection in WLAN access network. By doing this, the UE avoids the IP address allocation (e.g., by DHCP) while attaching to the target WLAN access network.

8) The Core RI sends the HO command message to the UE including the recommended target IDs and information allowing establishing the connection in target access network. Note that the Core RI may select the target cell, and send the "strict" HO command that includes only one selected target cell for handover.

9) If the UE can select the target cell from the recommended list, the UE should send the HO indication including its choice of target cell to the RNC and then to the Core RI.

- Security triggering: Upon receiving the HO indication from the UE or after sending a strict HO command, the MM component in RI will notify the SC component to transfer the security context to the local WLAN RI.

10) Upon receiving the HO indication from UE or after receiving a strict HO command from the Core RI, the RNC sends HO notification to the UPE for the traffic redirection purpose.

11) The UPE stops sending the packets to the UE via SGSN and starts to forward the packets to the WAC that controls the target cell. The WAC address can be retrieved by DNS request from the target ID. The WAC then buffers the packets and waits for the UE attachment. It is optional that the UPE can duplicate and buffer the packets in case the UE cannot attach to the WLAN (i.e. handover failure) and return back to the UMTS connection.

12) The RI sends the user mobility context to the local WLAN RI.

13) The RI sends the user security context to the local WLAN RI for fast re-authentication.

14-15-16-17-18) the re-authentication procedure between the UE and the local WLAN RI using EAP is performed.

- Re-authentication next and re-authentication next complete: are used to by MM component in UE to initiate the re-authentication procedure on SC component and by SC component to indicate MM the success of the re-authentication respectively.

19) A tunnel is then established between the UE and WAC and between WAC and UPE using IKEv2 protocol. Regarding the intra-WLAN mobility, a new IPSec tunnel must be reconfigured each time the UE changes its Point of Attachment. To speed up this kind of IPSec tunnel relocation, we can use the MOBIKE mechanism proposed by the IETF MOBIKE WG.

20) The HO complete is sent from the target AP to the WAC, from WAC to the local WLAN RI and then from local WLAN RI to Core RI.

21) Communication is exchanged via the WLAN access network

22) Resource is released in UTRAN network side and the Presence updates the local WLAN RI and Core RI will update the presence information of the UE.

3.3.1.2. Handover from WLAN AN to UTRAN

1) The network selection component in local WLAN RI sends the provisioning information to the UE for the purpose of network selection in UE.

2) During the communication, the UE may discover the available access networks of other operators by scanning their advertisement messages.

- Selected network: Based on the discovered information and provisioning information, the UE will select the preferable available access networks for the measurement purpose.

3) The UE performs the measurement procedure on neighboring WLAN cells as well as the intersystem measurement on the neighboring WIMAX and UMTS cells.

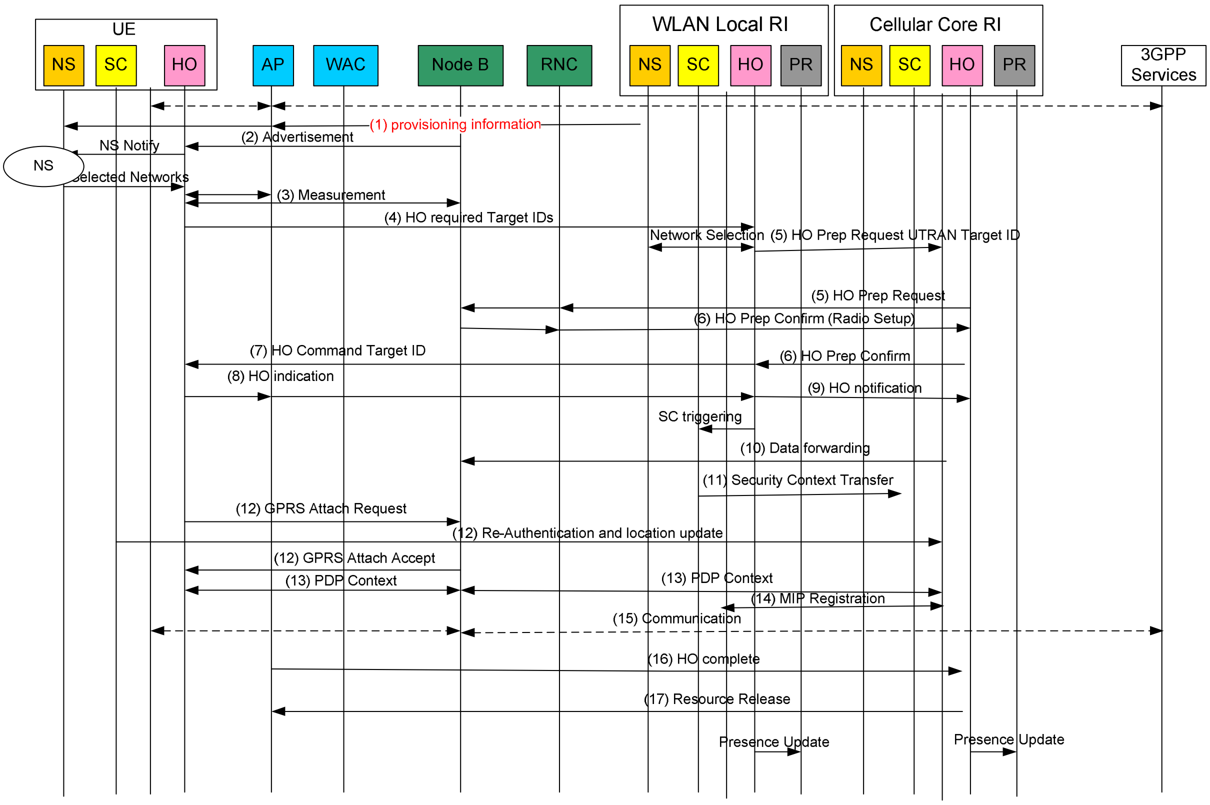


Figure 32. Handover from WLAN Access Network to UTRAN

4) Based on the measurement results, the UE decides whether or not to start a horizontal or a vertical handover. If a vertical handover is decided, a HO required message including the potential target IDs and the required QoS of the current running applications is sent to the local WLAN RI.

- Network selection: The local WLAN RI may make the network selection to eliminate the undesirable target IDs based on its policy and its preference.

- RI localization query/response: The local WLAN RI will learn the address of the target RI by consulting its presence database. In this case, the core RI is the destination since the WLAN ISP has no direct roaming relation with the MNO deployed target UMTS candidate cells.

5) The local WLAN RI sends HO preparation request to the Core RI. The Core RI then sends this preparation message to the RNC that controls the indicated target IDs to allocate the required resource.

6) The RNC sends back the HO confirm to the core RI if the RNC can reserve the required resource for the handover. The core RI adds the reconfiguration information for radio setup to the HO confirm message sending to local WLAN RI.

7) The local WLAN RI sends the HO command message to the UE including the recommended target IDs and the associated pre-configuration reference number.

8) The UE sends the HO indication including its choice of target cell to the WAC and then to the local WLAN RI.

- Security triggering: Upon receiving the HO indication from the UE, the MM component in local WLAN RI will notify the SC component to transfer the security context to the core RI.

9) Upon receiving the HO indication from UE, the WAC sends HO notification to the Data Anchor for the traffic redirection purpose.

10) The Data Anchor stops sending the packets to the UE via the WAC and starts to forward the packets to the SGSN or RNC via UPE that controls the target cell. The UPE will serve as a FA for the handover solution. The SGSN and RNC addresses can be retrieved by DNS request from the target ID. The SGSN or RNC then buffers the packets and waits for the UE attachment.

11) The RI sends the user mobility and security context to the core RI.

12) The UE performs the GPRS attachment procedure in UTRAN network to setup the connection with the target Node B. The GPRS attachment consists of accessing the SGSN, authenticating with the AAA server in Core RI and updating the location.

13) The UE performs then the PDP context activation to establish the data tunnel between RNC and SGSN and between SGSN and UPE.

14) The UPE performs the MIP registration with the Data Anchor.

15) Communication is exchanged via UTRAN network.

16) The HO complete is sent from Node B to the RNC, from RNC to the Core RI and from the Core RI to local WLAN RI.

17) Resource is released in UTRAN network side and the Presence updates the local WLAN RI and Core RI will update the presence information of the UE.

3.3.2. Interworking Scenarios using RII architecture (loose coupling architecture)

This scenario describes the roaming between MNO and different WIMAX/WLAN operator. Only the subscribers (whatever 3GPP, WIMAX or WLAN) that would like to use inter-AS roaming service are connected to Data Anchor point implemented in global RI. The handover preparation is carried out by the core RI and local WLAN RI via Global RI. The message sequence chart in Figure 33 and Figure 34 illustrates the high level procedures for the handover solution. The Data Anchor is considered as data plane anchor for this interworking scenario.

3.3.2.1. Handover from UTRAN to WLAN AN

1) The network selection component in the Core RI sends the provisioning for the purpose of network selection in UE.

2) During the communication, the UE can discover the available access networks of other operators by scanning their advertisement message.

- Selected network: Based on the discovered information and provisioning information, the UE will select the preferable available access networks for the measurement purpose.

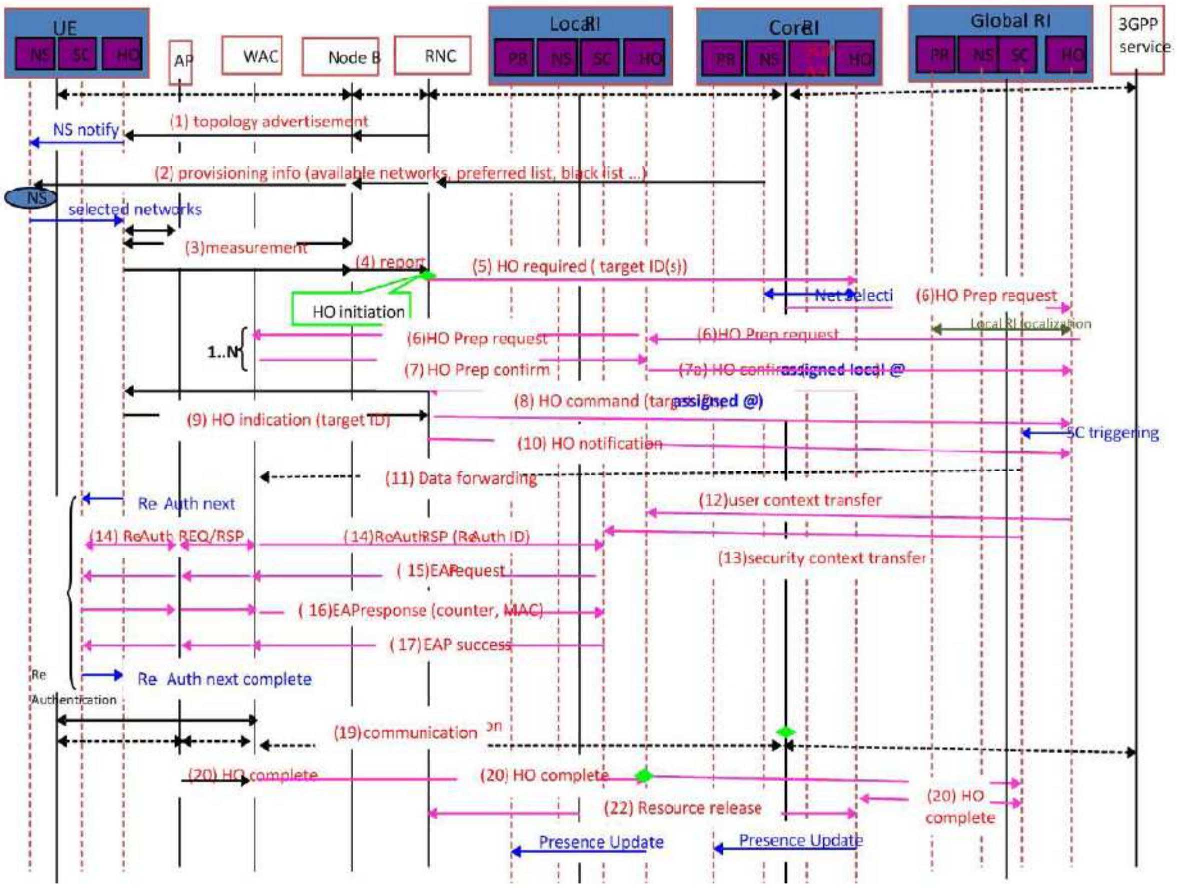


Figure 33.Handover from UTRAN to WLAN AN

3) The UE performs the measurement procedure on neighboring UMTS cells as well as the intersystem measurement on the neighboring WIMAX and WLAN cells.

4) The UE sends the measurement report to the RNC. The UE can report the signal of WLAN or WIMAX to a false maximum value to indicate its preference for handover to this cell.

5) Based on the measurement report, the RNC decides whether or not to make horizontal or vertical handover. If RNC decides to make vertical handover, it will send a HO required message including the potential target IDs and the required QoS of the current running application to the Core RI.

- Network selection: The Core RI may make the network selection to eliminate the undesirable target IDs based on its policy and its preference.

- RI localization query/response: The Core RI will learn the address of the target RI by consulting its presence database. In this case, the Core RI must communicate to global RI to reach the target access network.

6) The Core RI sends HO preparation request to the global RI, which in turn routes the HO preparation message to the local WLAN RI. The local WLAN RI in turn sends this preparation message to the WAC that controls the indicated target IDs.

- RI localization query/response: The global RI will learn the address of the target local WLAN RI by consulting its presence database.

7) The WAC sends back the HO confirm to the local WLAN RI if the WAC can reserve the required resource for the handover. The local WLAN RI then adds the local assigned IP address into the HO confirm message, which is used by the UE to establish the IP connection in WLAN access network. The HO confirm is returned to global RI and then to the Core RI.

8) The Core RI sends the HO command message to the UE including the recommended target IDs associated with the local assigned IP address and information allowing establishing the connection in target access network. Note that the Core RI may select the target cell, and send the "strict" HO command that includes only one selected target cell for handover.

9) The UE should send the HO indication including its selected target cell to the RNC and then to the Core RI.

- Security triggering: Upon receiving the HO indication from the UE or after sending a strict HO command, the MM component in RI will notify the SC component to transfer the security context to the local WLAN RI via Inter-AS RI.

10) Upon receiving the HO indication from UE or after sending a strict HO command, the Core RI sends HO notification to the Data Anchor for the traffic redirection purpose.

11) The Data Anchor stops sending the packets to the UE via UPE and starts to forward the packets to the WAC. The WAC address can be retrieved by DNS request from the target ID. The WAC then buffers the packets and waits for the UE attachment. It is optional that the Data Anchor can duplicate and buffer the packets just in case the UE cannot attach to the WLAN (i.e. handover failure) and return back to the UMTS connection.

12) The RI sends the user mobility context to the local WLAN RI via the Inter-AS RI.

13) The RI sends the user security context to the local WLAN RI via the global RI for fast re-authentication.

14-15-16-17) the re-authentication procedure between the UE and the local WLAN RI using EAP is performed.

- Re-authentication next and re-authentication next complete: are used to by MM component in UE to initiate the re-authentication procedure on SC component and by SC component to indicate MM the success of the re-authentication respectively.

18) The MIP registration is performed between the UE and the WAC that plays the role of an FA, between the FA and the local HA implemented in local WLAN RI and between the local HA and Data Anchor Point. The MIP registration between WAC (FA) and Data Anchor can be done before data forwarding step to shorten the connection setup step.

19) Communication is exchanged via the WLAN access network

20) The HO complete is sent from the target AP to the WAC, from WAC to the local WLAN RI, from local WLAN RI to global RI and then from global RI to the core RI.

21) Resource is released in UTRAN network side and the Presence updates the local WLAN RI and Core RI will update the presence information of the UE.

3.3.2.2. Handover from WLAN AN to UTRAN

1) The network selection component in local WLAN RI sends the provisioning information to the UE for the purpose of network selection in UE.

2) During the communication, the UE may discover the available access networks of other operators by scanning their advertisement message.

- Selected network: Based on the discovered information and provisioning information, the UE will select the preferable available access networks for the measurement purpose.

3) The UE performs the measurement procedure on neighboring WLAN cells as well as the intersystem measurement on the neighboring WIMAX and UMTS cells.

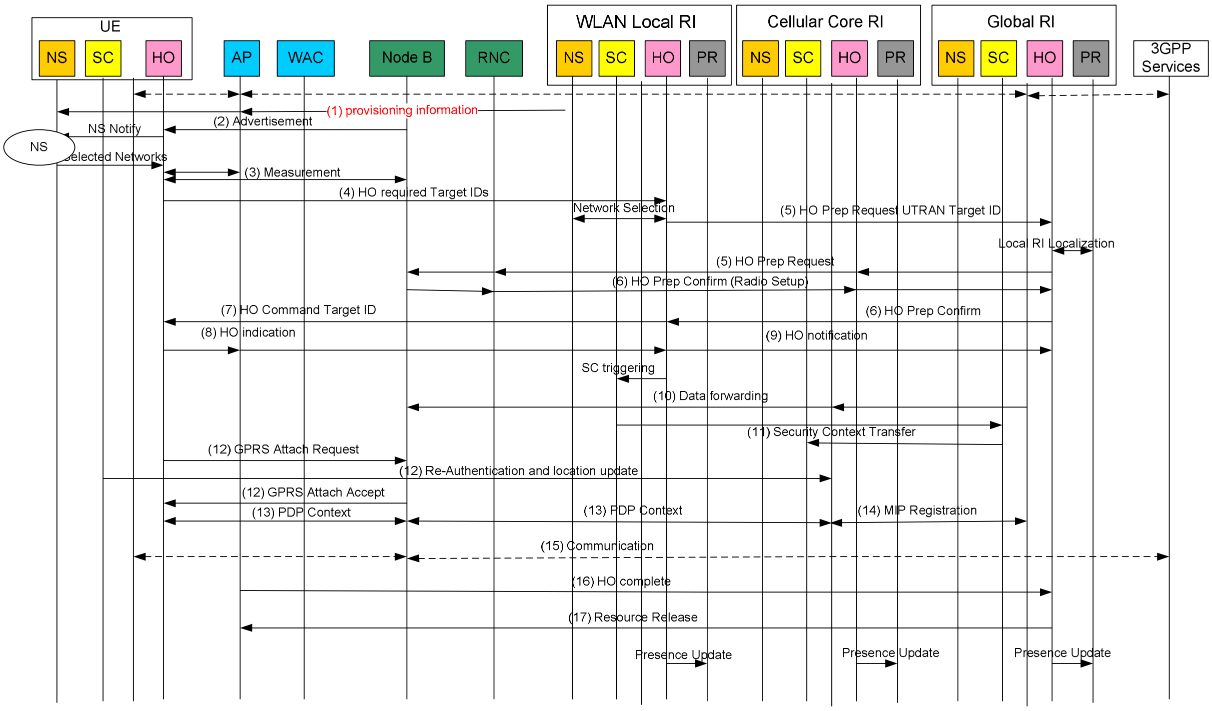


Figure 34. Handover from WLAN AN to UTRAN

4) Based on the measurement results, the UE decides whether or not to make horizontal or vertical handover. If a vertical handover is decided, a HO required message including the potential target IDs and the required QoS of the current running application is sent to the local WLAN RI.

- Network selection: The local WLAN RI may make the network selection to eliminate the undesirable target IDs based on its policy and its preference.

- RI localization query/response: The local WLAN RI will learn the address of the target RI by consulting its presence database. In this case, the Inter-AS RI is the destination since the WLAN ISP has no direct roaming relation with the MNO deployed target UMTS candidate cells.

5) The local WLAN RI sends HO preparation request to the Inter-AS RI which in turn sends it to the Core RI. The Core RI then sends this preparation message to the RNC that controls the indicated target IDs to allocate the required resource.

- RI localization query/response: The global RI will learn the address of the target core RI by consulting its presence database.

6) The RNC sends back the HO confirm to the core RI if the RNC can reserve the required resource for the handover. The core RI adds the reconfiguration information for radio setup to the HO confirm message sending to local WLAN RI via global RI.

7) The local WLAN RI sends the HO command message to the UE including the recommended target IDs and the associated pre-configuration reference number.

8) The UE sends the HO indication including its choice of target cell to the WAC and then to the local WLAN RI.

- Security triggering: Upon receiving the HO indication from the UE, the MM component in local WLAN RI will notify the SC component to transfer the security context to the core RI.

9) Upon receiving the HO indication from UE, the WAC sends HO notification to the Data Anchor for the traffic redirection purpose.

10) The Data Anchor stops sending the packets to the UE via the WAC and starts to forward the packets to the SGSN or RNC via UPE that controls the target cell. The UPE will serve as a FA for the handover solution. The SGSN and RNC addresses can be retrieved by DNS request from the target ID. The SGSN or RNC then buffers the packets and waits for the UE attachment.

11) The RI sends the user mobility and security context to the core RI via the global RI.

12) The UE performs the GPRS attachment procedure in UTRAN network to setup the connection with the target Node B. The GPRS attachment consists of accessing to SGSN, authenticating with the AAA server in Core RI and updating the location.

13) The UE performs then the PDP context activation to establish the data tunnel between RNC and SGSN and between SGSN and UPE.

14) The UPE performs the MIP registration with the Data Anchor.

15) Communication is exchanged via UTRAN network.

16) The HO complete is sent from Node B to the RNC, from RNC to the Core RI and from the Core RI to the global RI and then from global RI to local WLAN RI.

17) Resource is released in UTRAN network side and the Presence updates the local WLAN RI and Core RI will update the presence information of the UE.

3.4. Testbed implementation and Results

3.4.1. Introduction

The main objective of this section is to present the mechanisms we have proposed and the implemented testbed. In this section we explain how the proposed solution have been tested for seamless roaming using RII architecturet. For demonstrating the capabilities of the architecture, we have built a testbed using 3GPP, WLAN and WIMAX Networks. The reference architecture of the architecture is presented in Figure 35. The local RII, core RII and Global RII have been implemented on different servers and connected through high speed IP links. The functionalities of security, mobility, network selection, handover management and presence have been developed and integrated in the RII architecture. In the next sections we will describe the details of the implemented architecture, testbed equipment and different interworking scenarios that are tested. We also used different scenarios taking into consideration of requirements and constraints of those scenarios and also ensuring these requirements are satisfied by RII architecture.

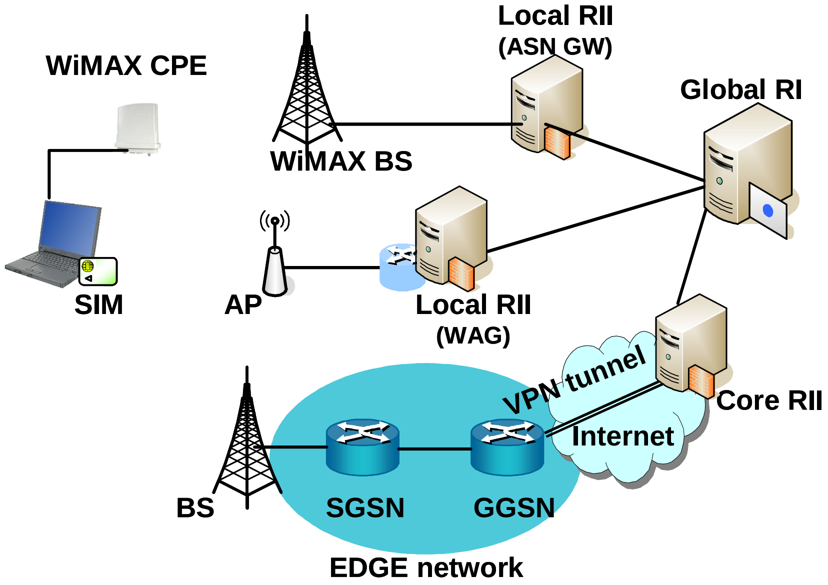


Figure 35. Implementation of RII architecture

3.4.2. Testbed Scenarios and Services

In this section we will detail the different scenarios of user roaming and services accessing. According to the different scenarios of user profiles requirements for seamless roaming are estimated. The aim of the proposed testbed is to show the global behavior of the system to support seamless secure interworking between different administrative domains using RII architecture, satisfy all the requirements and obtain seamless roaming using RII architecture. We have described two scenarios: one is User roaming in WLAN, WIMAX and 3G networks and second is user roaming accessing VoIP and video on demand services.

3.4.3. Testbed description

Testbed Overview

Our multi-interface user terminal used is DELL Latitude-410 equipped with Option GLOBETROTTER 7.2 ready MAX data card for EDGE access and integrated Wi-Fi interface for WLAN access. For the WIMAX access network, the terminal connects to the WIMAX CPE. In our testbed, the global RII assigns the temporary identities for its connected access networks. The access network will communicate such an identity to its subscribers for roaming purpose. The Extensible Authentication Protocol (EAP) is used for authentication signalling within the network entities. When the users roam to a visiting network, they will include the assigned temporary identity as its home network identity and the Network Access Identity (NAI) of the global RII within an EAP-Identity/Response message. Based on this information, the visiting networks check if the NAI in the EAP-Identity/Response belongs to their administrative domain. Accordingly, the user authentication request will be handled locally or will be forwarded to the global RII. The global RII holds a database that makes it possible to retrieve the user home network. The authentication requests are then routed to the home networks to complete the authentication procedure.

For mobility management, we have implemented client-based mobility management using hierarchical MIP. The HA is located in the local RII of the home network. The global RII contains the upper FA, and the local/core RII in each network domain contains the lower FA. Whenever the UE moves to the visiting network, the lower FA receives the registration request. The FA in the local RII forwards the request to the upper FA in the global RII. Next, the upper FA sends the registration to the HA on the home local RII. When the UE moves to another visiting network later, it only needs to update the MIP registration with the upper FA instead of registering again with the HA.

3.4.3.1. Cellular Networks

The following section describes the general GPRS network architecture of MNOs and the connectivity architecture of Transatel which assisted to deploy this architecture by providing cellular access to the testbed. Transatel connects to multiple MNOs in Europe which allows it to offer a range of mobile services as an MVNO(/E) in the region. Subscribers connecting to Transatel use “netgprs.com” as the APN. In the GPRS backbone, an APN gives a reference to a GGSN which is used to create the logical connection between UE and an external PDN. An APN consists a network identifier and an operator identifier of which the former is a mandatory part. The network identifier defines to which external network the GGSN is connected e.g. netgprs.com.

The complete APN can be of the format “<network id>.mnc<MNC>.mcc<MCC>.gprs” where mnc<MNC>.mcc<MCC>.gprs corresponds to the optional operator identifier. MNC and MCC are the components of IMSI defining the mobile network code and the mobile country code respectively. Generally internet domain names (or internal domain names) are used in order to guarantee the uniqueness of the APN network identifier. APN resolution is handled by the DNS servers located at the core IP network of the MNO. When a UE initiates a “PDP context activation” SGSN uses the APN to query the DNS in order to acquire the IP address (es) of the GGSN(s) that connects to Transatel.

The

Figure 36 depicts the network integration architecture of Transatel with partner MNO networks.

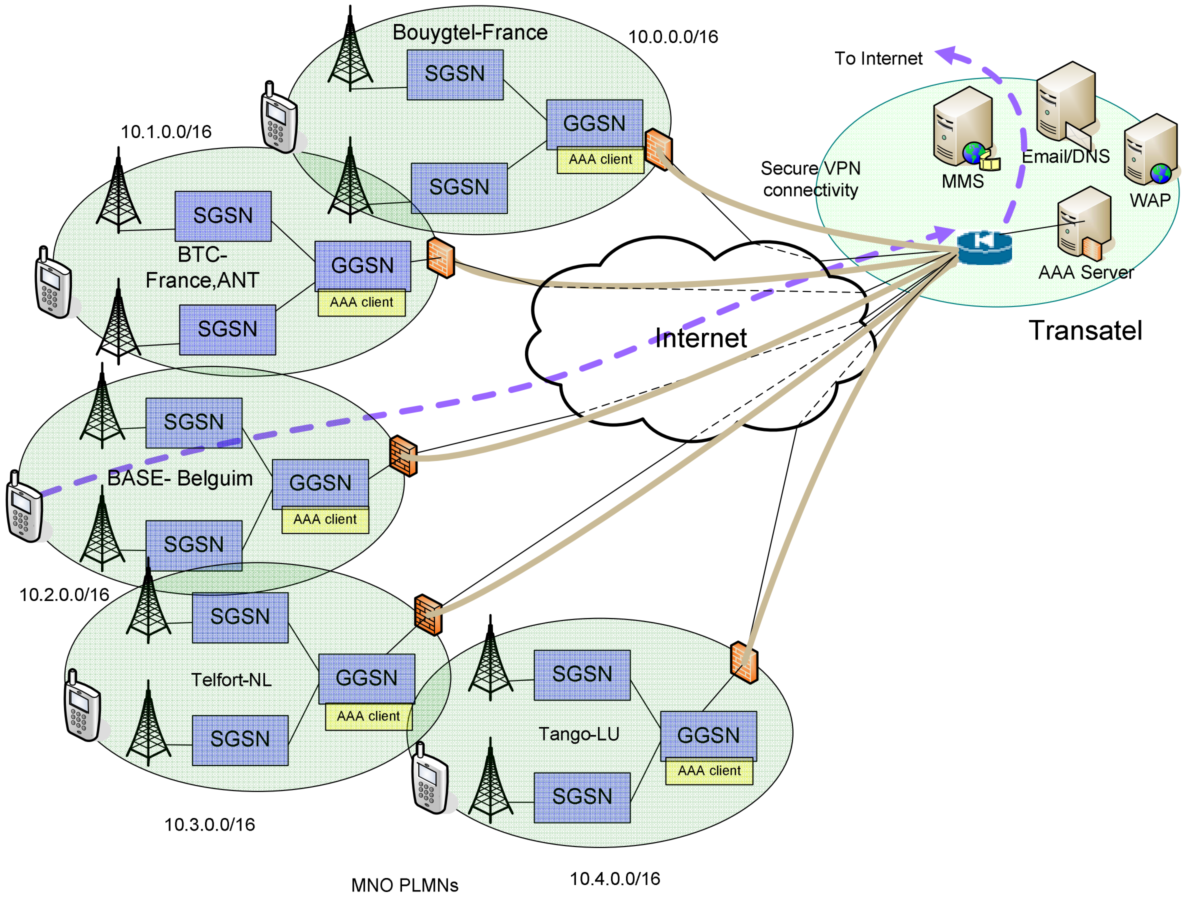


Figure 36. Transatel data network architecture

Access to MNO GPRS backbone is via a secure VPN established between the two networks i.e. a gateway-to-gateway type VPN network connecting two trusted networks. IP address assignment of UE is handled by Transatel. At present, Transatel adopts a dynamic addressing scheme based on the private address space. The IP address allocation is done by a RADIUS server located at the Transatel core network. An AAA client incorporated with the MNO side of the network permits this assignment of Transatel managed IP addresses. Once an IP address is assigned, UE shall connect to the (Transatel) ISP network in order to access Transatel provided data services e.g. WAP, Internet.

Figure 37 shows the protocol stack for the communication between the UE and Transatel IP backbone performed over the Internet via a secure VPN.

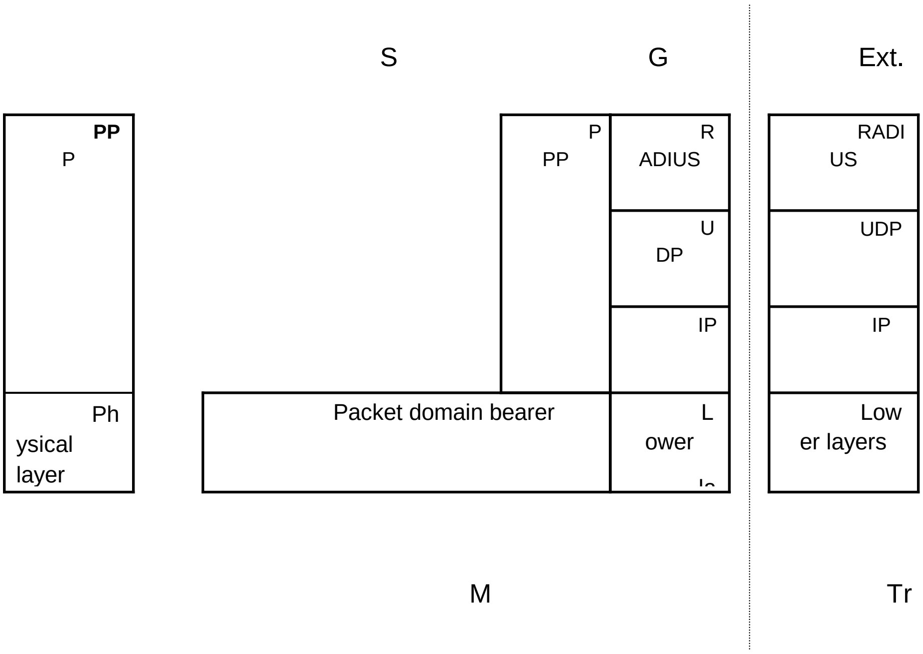


Figure 37. Protocol stack for IP based connectivity between UE and Transatel

A secure IPSec VPN connectivity has been established between LRSM testbed and Transatel GPRS network. This section gives an overview of the general Transatel AAA implementation followed by the AAA routing of information from AAA of Transatel to AAA of core RI based in our testbed.

Complying with the 3GPP specifications [TS 29.061], Transatel provides AAA services in its proprietary infrastructure. The RADIUS (AAA) client function resides in the GGSN. When the GGSN receives a "Create PDP Context" request message the RADIUS client function sends the authentication information to the authentication server, which is identified during the APN provisioning. The authentication server checks for chosen credentials in order to authenticate and subsequently authorize the client. The Calling-Station ID (MSISDN) is generally accepted to be a reliable AAA attribute as it is network originated and this can be used together with username/password (PAP based) pair during the authentication and authorization processes.

As a part of the AAA process Radius accounting functionality also relies on the client originated information. AAA server stores this information which shall eventually be used for charging, etc. These attribute/value pairs indicate the format of actual content of the RADIUS messages exchanged between the GGSN and the AAA server. A detailed description of the common and most of the vendor specific attributes e.g. 3GPP-IMSI, can be found in [TS 29.061].

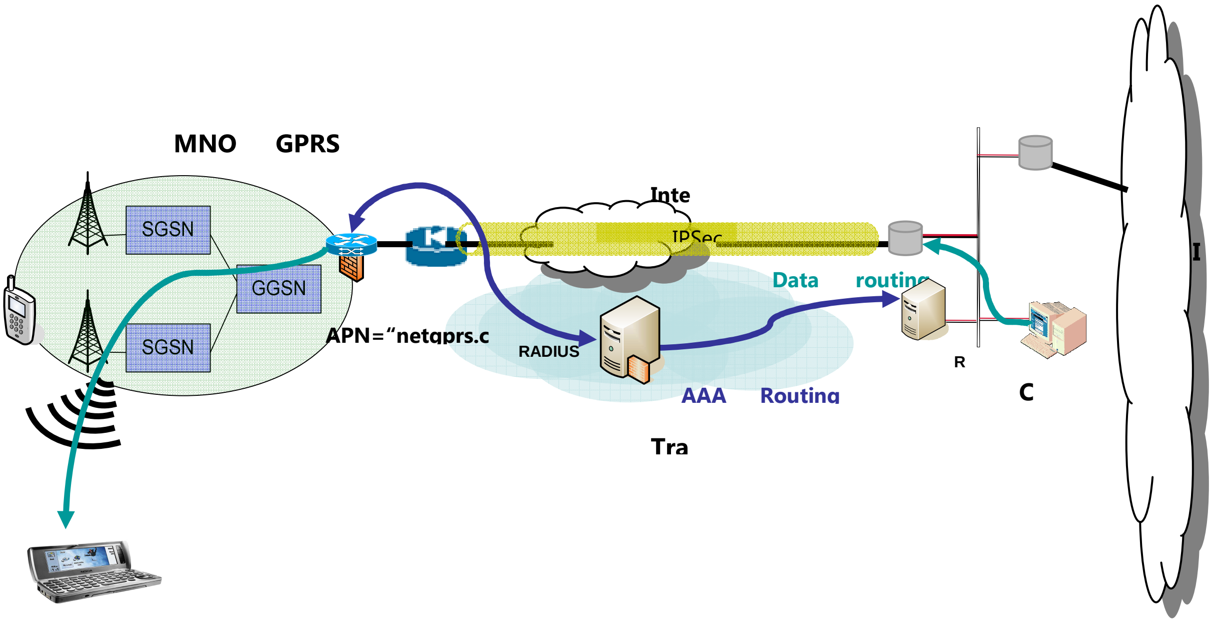


Figure 38. Secured VPN between transatel GPRS network to testbed

IP address allocation is by the Radius server hence it is required to specify the DNS IP addresses in addition to the MS assigned IP. This information is contained in the AAA response. They are as follows; Framed-IP-Address (MS assigned IP address), Primary-DNS-Server, Secondary-DNS-Server, 3GPP-Primary-DNS-Server and 3GPP-Secondary-DNS-Server. When specifying DNS servers the 3GPP format described above is mandatory with respect to certain MNO configurations e.g. BASE

As a part of the integration process AAA of Transatel shall act as an AAA proxy to the AAA of core RI based in our testbed. When a GGSN receives a Create PDP Context Request message for then Transatel APN (netgprs.com), the GGSN sends a RADIUS Access-Request to the AAA server at Transatel. The users shall be identified based on the MSISDN assigned thus the corresponding messages can be relayed through the AAA server of Transatel. The AAA proxy functionality is accordance with realm authentication mechanism. The authentication realm is defined using realm portion of the Network Access Identifier. This is the realm that is passed as part of the User-Name attribute (user@realm).

Once handed over the access requests by the Transatel AAA server the Core RI AAA server authenticates and authorizes the user. The IP address allocation shall also be handled by the Core RI. This has to be in accordance with GGSN IP address plan and to be discussed further. Details on specific Radius attributes of interest are also to be discussed further.

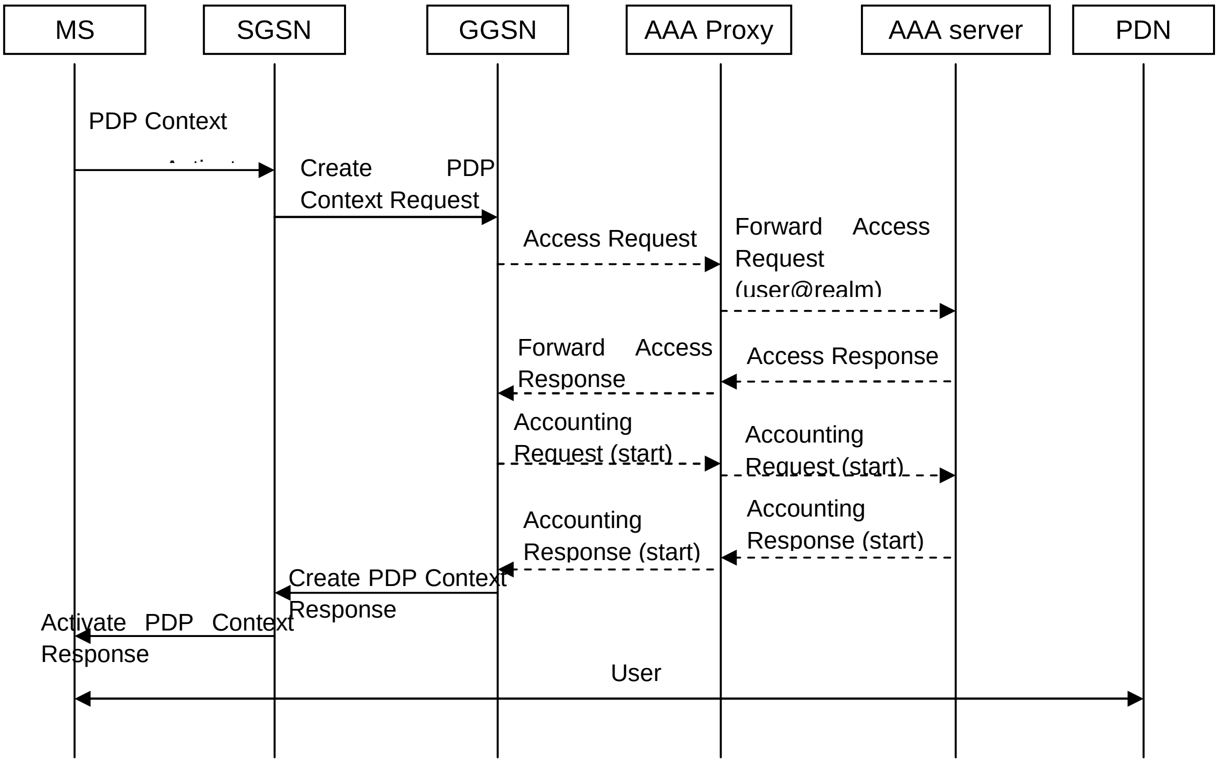

MS
SGSN
GGSN
AAA Proxy
AAA server
PDN
PDP Context
Create PDP Context Request
Access Request
Forward Access Request (user@realm)
Forward Access Response
Access Response
Accounting Request (start)
Accounting Request (start)
Accounting Response (start)
Accounting Response (start)
Create PDP Context Response
Activate PDP Context Response
User

Figure 39. RADIUS message flow for PDP type IP

3.4.3.2. WLAN Network (WISP Operator)

In the testbed we have used different access points and mechanisms. We used different kinds of access points; one is Linksys WRT 64G, the second is Netgear WP11 access points and linux box equipped with Netgear WG311T PCI adapter. We have chosen these specific devices for advanced functionalities.

The Linksys WRT64G provides 802.11g and 802.11b (2.4GHz) Standards standard interface for wireless communications. Provides Wireless Security with Wi-Fi Protected Access (WPA) and Wireless MAC Address Filtering. The linux box is configured using a PCI adapter from Netgear WG311T Atheros chip set. We configured the linux box using Hostapd. Hostapd is a user space daemon for access point and authentication servers. It implements IEEE 802.11 access point management, IEEE 802.1X/WPA/WPA2/EAP Authenticators, RADIUS client, EAP server, and RADIUS authentication server. The current version supports Linux (Host AP, madwifi, Prism54 drivers) and FreeBSD (net80211).

The WISP operator access networks contain information of the users database, their respective security credentials, policies to access the networks. The security mechanisms used in this WISP operator include EAP TLS, and radius server contains details of all the authorized users, SLA agreements between the different WISP Networks and proxies are configured in the radius server. WISP access network contains the Hostap [71] as the access point where the IEEE 802.1X with the EAP TLS and NAI extensions are been implemented. A local AAA server is installed; in this case we used freeradius [72] as our AAA server. Mobility is maintained using dynamics mobile IP [73] in the architecture. On the other hand the client is equipped with WPA supplicant [73] for the authentication over the access networks; it supports the EAP security mechanisms. The client is equipped with the dynamic mobile IP client to register to the FA or the HA when there is a mobility of the client. When a user attempts to access the network, the users are identified and security mechanisms are initiated and the authentication is been done. When the user authorized to the WISP network it initiates the mobile IP and registers to the HA (Home Agent) on the WISP network.

3.4.3.3. WIMAX Access Network

For providing services in WIMAX networks we used Infinet Wireless Pre WIMAX based on IEEE 802.16d specification. We used a BS and CPE model, where the operator has the control of the BS and the user does have control of CPE. We have configured IDU-5000-RJ In door unit (IDU) and R5000-M/ R5000-S outdoor unit (ODU).We operated the equipment at the frequency range of 5.4 Ghz. Due to pre WIMAX equipment utilization we have introduced some new mechanism for authentication and access mechanisms.

The WIMAX network contains a BS and the local RI. This Local RI acts as a authentication server between the clients connected to the access networks. In this particular scenario a CPE get connected to BS, and clients connects to the router of the CPE through Ethernet. When CPE starts authenticating to the BS, it send the information of the shared key to the BS along with the MAC address to the BS. The BS check into the query and authenticates the CPE, if ever there is no information available of the CPE in the BS database it proxies the request to the RAPS server resided in the RI of the architecture which acts as a AAA server. When CPE associates with BS, UE initiates the layer two tunneling mechanisms to the other end with a gateway of BS and starts authentication to the user network using EAP TTLS over wired and gets authenticated to the WIMAX network.

The WIMAX network contains a BS and the WAG network. This WAG acts as a authentication server i.e.. AAA between the clients connected to the access networks. In this particular scenario a CPE get connected to BS, and clients connects to the router of the CPE through Ethernet. When CPE starts authenticating to the BS, it sends the information of the shared key to the BS along with the MAC address to the BS. The BS checks the query and authenticates the CPE, if ever there is no information available of the CPE in the BS database it proxies the request to the RAPS server residing in the RI of the architecture which acts as a AAA server. After that the client connected to the CPE, client starts authentication to the user network using EAP over wired and gets authenticated to the WIMAX network with the AAA server.

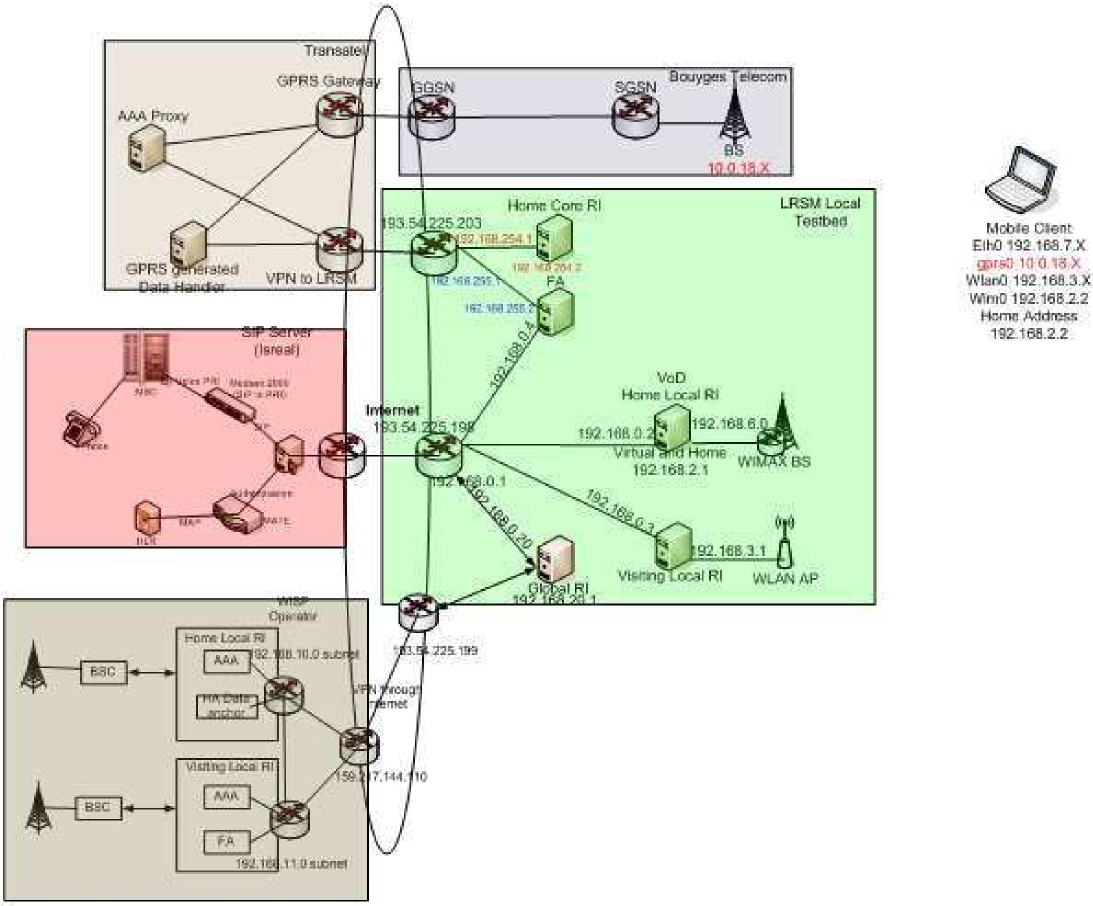


Figure 40. Integrated WLAN, WIMAX, cellular network in our testbed

3.4.3.4. SIP Server Architecture:

The SIP client is connected to the SIP server through SBC (Session Border Controller). The SIP testbed contains the media gateway (MGW) for handling the VoIP media, the SMS server for handling SMS-to-SIP, the presence server, which is described in the above (at the presence section), which controls the service and routes the VoIP calls according to the presence (either to the mobile device or to the SIP client, if available and preferable).

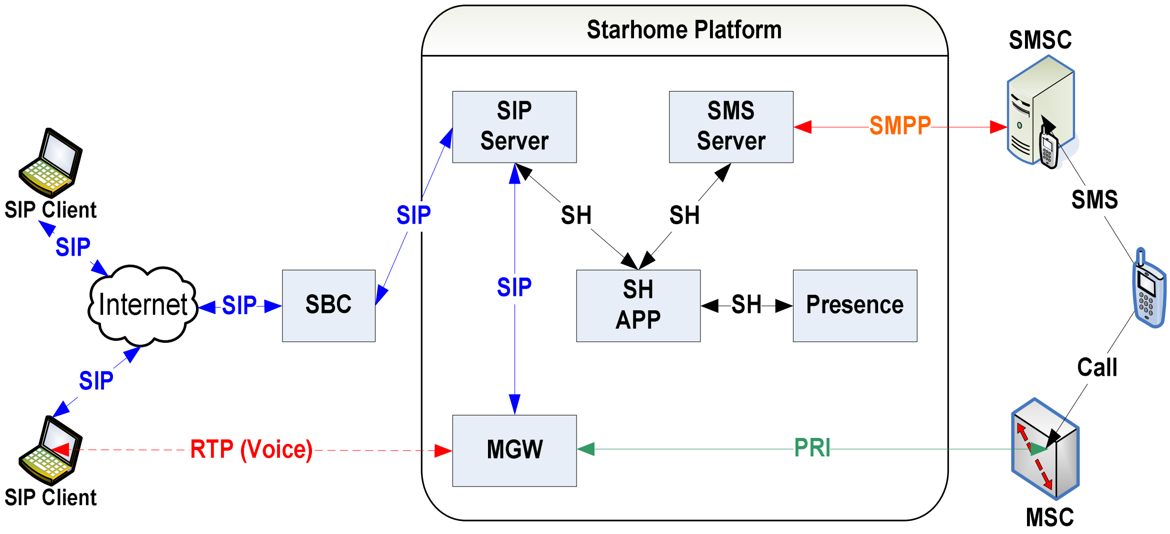


Figure 41. SIP Architecture based

3.4.4. Testing

In this scenario user client moves from WLAN and WIMAX networks. Client is equipped with a WLAN card and Ethernet connected to the router of the CPE. When the client connects to the home network i.e.. WLAN network it authenticates to the access networks and registers to the HA of the home network. When the client connects to the Ethernet, it initiates the network, it establishes the tunnel with the gateway of the BS network, starts authenticating with AAA server of the WIMAX network, and then registers itself with the FA on the WIMAX network which relays the information to the HA for mobile IP and continues the session in the WIMAX network. The whole scenario is replicated as shown in Figure 42.

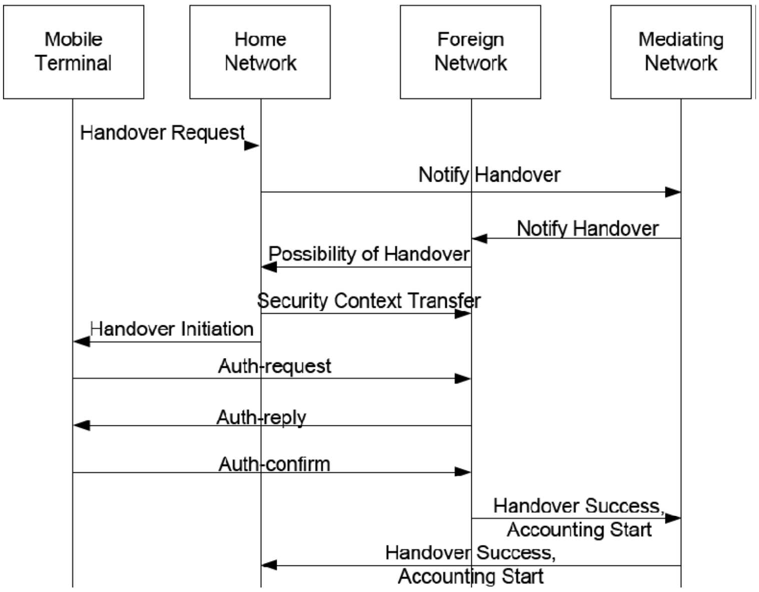


Figure 42. Message exchange user roaming in WLAN and WIMAX

The Figure 43 shown below provides information of message exchanges between different components of the RII architecture where a user roams from cellular, WLAN and WIMAX networks.

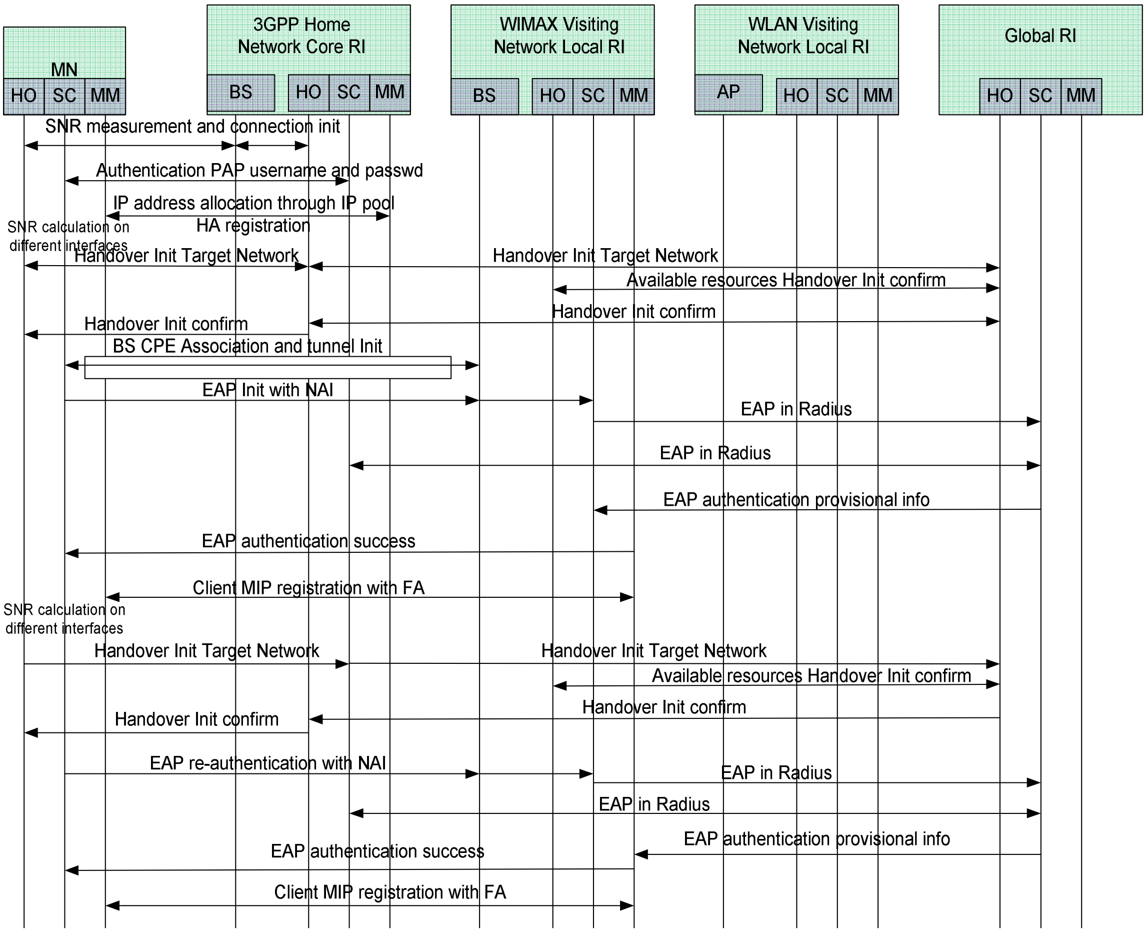

MN
HO SC MM
3GPP Home Network Core RI
BS HO SC MM
WIMAX Visiting Network Local RI
BS HO SC MM
WLAN Visiting Network Local RI
AP HO SC MM
Global RI
HO SC MM
SNR measurement and connection init
Authentication PAP username and passwd
IP address allocation through IP pool
HA registration
SNR calculation on different interfaces
Handover Init Target Network
Handover Init Target Network
Available resources Handover Init confirm
Handover Init confirm
Handover Init confirm
BS CPE Association and tunnel Init
EAP Init with NAI
EAP in Radius
EAP in Radius
EAP authentication provisional info
EAP authentication success
Client MIP registration with FA
SNR calculation on different interfaces
Handover Init Target Network
Handover Init Target Network
Available resources Handover Init confirm
Handover Init confirm
Handover Init confirm
EAP re-authentication with NAI
EAP in Radius
EAP in Radius
EAP authentication provisional info
EAP authentication success
Client MIP registration with FA

Figure 43. Message flow between different components

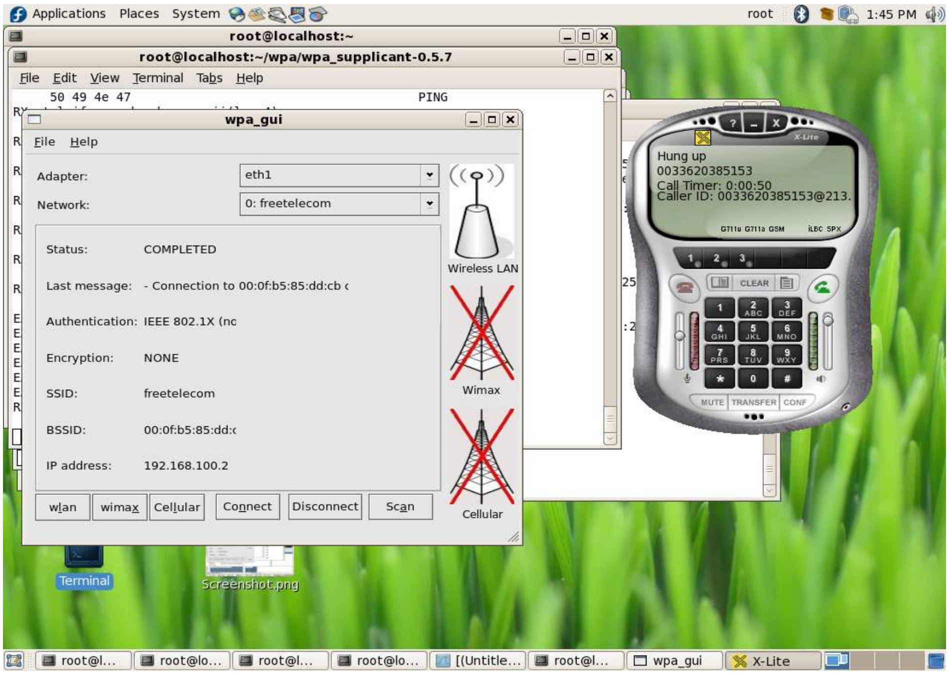
As described previously, the UE in our testbed roams between WIMAX, WLAN and EDGE networks. We do not consider the UE movement and the network selection within our testbed. So, the handover initiation is done manually. The three considered access networks belong to three different operators. Hence the handover and roaming is achieved with the help of the global RII. We have repeated many inter-system inter-operator handovers where the UE is running a VoIP or video on demand application. The average handover latency is given in Table 5.

	WIMAX – WLAN	WIMAX - EDGE	EDGE – WLAN	WLAN – WLAN
Handover latency	1s	3s	1s	4s

Table 5. Handover latency results

This handover latency includes the security, mobility and roaming delay to carry out the whole necessary signalling exchanges. The overall handover latency for the roaming between WIMAX and EDGE is around 3 seconds whereas the latency for roaming between WIMAX to WLAN is around 1 second. When the UE roams from the home WLAN network to the visiting WLAN network using the global RII, the latency is observed around 4 seconds. The handover latency differs for different roaming scenarios. In fact, the signalling messages for authentication and mobility management required in different access networks are different. The high latency of the WLAN-WLAN roaming is due to the fact that the WLAN horizontal handover using only one radio interface necessitates a Wi-Fi scanning and association phase which takes a lot of time.

It should be noted that the handover latency given here is not the handover interruption time. The inter-system handover using two interfaces can be managed in such a way that the communication on the serving RAN is only released when the communication on the target RAN is already started. Furthermore, the handover latency is expected to be significantly reduced once the security context transfer is implemented. After all, the capability of maintaining the communication session while the user roams to a foreign network having no roaming agreement with its home network is a disruptive result in the roaming management.



```
 50 49 4e 47                                   PING
```

Adapter: eth1

Network: 0: freetelecom

Status: COMPLETED

Last message: - Connection to 00:0f:b5:85:dd:cb c

Authentication: IEEE 802.1X (nc

Encryption: NONE

SSID: freetelecom

BSSID: 00:0f:b5:85:dd:c

IP address: 192.168.100.2

Hung up
0033620385153
Call Timer: 0:00:50
Caller ID: 0033620385153@213.
G711u G711a GSM iLBC SPX

Figure 44. Screenshot of UE equipped with WLAN, WIMAX and Cellular network

3.5. SLA and Network Management

While an RII architecture greatly simplify service delivery for nomadic users, the complexity of managing and exchanging profiles, SLAs and configurations between heterogeneous networks and the RII becomes very complex for network administrators and systems' integrators. The operators' management models encompass a set of profiles (User, Content, Context, Configs, etc.) which must be aligned with the Roaming Intermediatory to allow interoperability. Arguably, the first step toward simplifying data integration is to choose a single, yet powerful language in order to maintain a coherent knowledge base. This language, or specification, will then be translated into platform specific formats.

Investigations resulted in the choice of the W3C Web Ontology Language (OWL) as the RII specification language. Also, to reduce the visual complexity of designing the system and to enable a fast prototyping and deployment of our broker, we have developed a tool for loading and manipulating ontologies. This tool implements our platform' transformation pattern and automatically generates specific configuration files from the ontology instances (individuals). These configurations are then deployed in different areas of the access network.

3.5.1. Policy Management

The methodology of policy-based network management was developed within the IETF in the context of the Integrated Services model, where it was proposed to use a policy framework for the management of admission control to reservations of network resources. The approach however is independent of the particular service model and soon it was recognized that it can equally be applied in a Differentiated Services environment and provides help in the application of IPsec. Moreover, it can be applied favourably to other more general management problems. Unfortunately, there is no generic IETF policy framework architecture fully agreed upon and specified. But the key functional blocks seem to be commonly recognized: policy management application, policy repository, policy decision point (PDP) and policy enforcement point (PEP), as shown in Figure 45.

The policy management application provides the interface to the network administrator to create and deploy policies, store them in the repository and monitor the status of the policy-managed environment. This application performs a simple validation that checks for potential policy conflicts. The policy repository is a storage that is used for policy retrieval performed by the policy decision points. Access to the database is accomplished by a repository access protocol. The policy decision point is the point where policy decisions are made. It performs the functions of retrieving and interpreting policies, detecting policy conflicts, receiving policy decision requests from PEPs, and returning policy decisions to them. Triggers to evaluate one or more policy rules can be events, polling, and explicit system component requests. Please note that the IETF policy framework does not include triggers explicitly. Only conditions (including timer conditions) are included.

However, for an implementation of the framework, triggers are a common choice. The PDP makes policy decisions based on policy conditions that are formed of boolean expressions that may refer to network element attributes. If a condition is evaluated to be true, the according action is executed, which typically (re)configures target elements to enforce the policy. If it is necessary it will translate policy rules into more specific parameters that the PEP could understand. A PDP may control multiple PEPs but each PEP is controlled by one PDP. The PEP is the target entity that hosts the network elements where policy decisions are actually enforced. It is the target of a policy action being executed when the rule condition evaluates to true. The separation of PEP and PDP (and also of the policy repository) is a logical one based on functionality, and not necessarily a physical separation. PEP and PDP may be combined and co-located.

The IETF framework suggests LDAP as the protocol for repository access and COPS/COPS-PR as the protocol for policy decision transfer. Other mechanisms such as HTTP, FTP, or SNMP may be used as well. However, no protocols are suggested for the communication between the policy management application and the PDPs or among cooperating PDPs. In general, no implementation details such as distribution, platform, protocols or language are prescribed. The applicability of a policy can be specified by assigning a role to it. The concept of role is central to the design of the entire policy framework. A role is a type of attribute that is used to select one or more policies for a set of entities and/or components from among a much larger set of available policies. The idea behind roles is simple. A policy administrator assigns each resource one or more roles, and then specifies the policies for each of these roles. The policy framework is then responsible for configuring each of the resources associated with a role in such a way that it behaves according to the policies specified for that role.

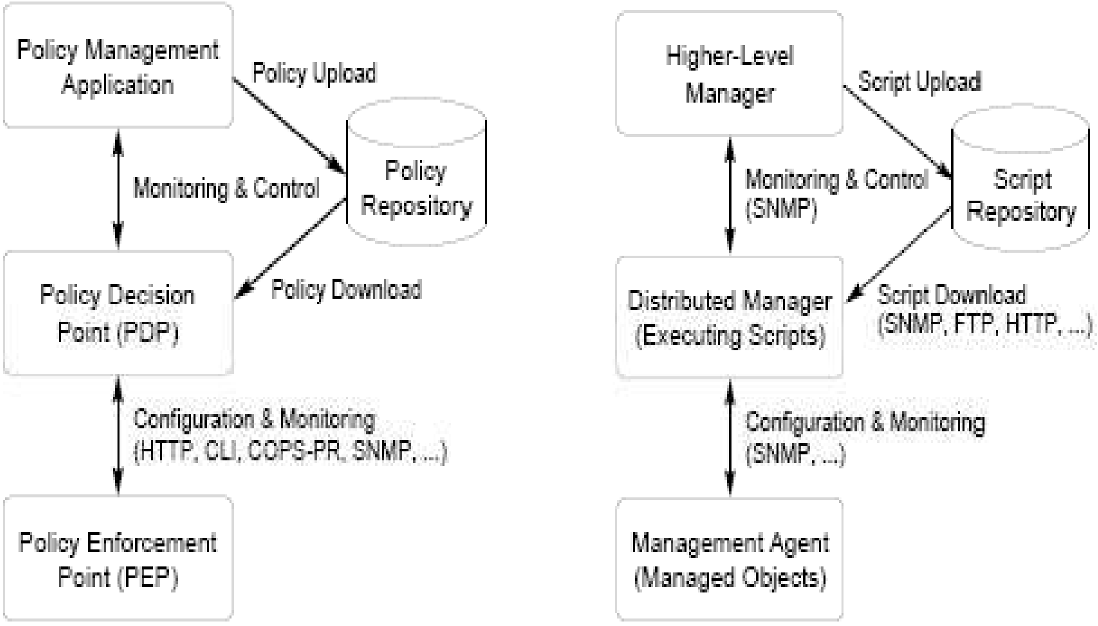

Policy Management Application
Policy Upload
Policy Repository
Monitoring & Control
Policy Decision Point (PDP)
Policy Download
Configuration & Monitoring (HTTP, CLI, COPS-PR, SNMP, ...)
Policy Enforcement Point (PEP)
Higher-Level Manager
Script Upload
Script Repository
Monitoring & Control (SNMP)
Distributed Manager (Executing Scripts)
Script Download (SNMP, FTP, HTTP, ...)
Configuration & Monitoring (SNMP, ...)
Management Agent (Managed Objects)

Figure 45. Architectures of the IETF policy framework and of distributed management by delegation.

3.5.2. User Policy Management

As mentioned above the policy management and enforcements are defined generally using PDP and PEP. The general policies are defined at the time of creating the SLAs, and generating the rules. In the RII architecture the policy rules are defined for the user subscribers and based on the pre defined SLA agreement, the user policies are enforced at the different levels of the architecture. These generated policies are stored in the repository of the Local RI or core RI of the user home network. Using the policy decision in the local RI or core RI the rules are setup at the different enforcement points providing access and different types of services.

Let us suppose a User gets a subscription to an access networks as provided by in his contract he aggress for different services. These are then stored in the repository using the policy management application entry. At this level the subscriber services and permissions are transferred to the different enforcements points of the architecture. Whenever the user tries to access the different types of services the enforcements points check the permissions and provide services according to the policy defined by the policy manager and decision points. At this level in RII architecture the user access management and different services are managed using the Local RI and Core RI using the Inter AS-RI of the architecture.

3.5.3. Network operator management

Using the policy management different entities of the access networks are managed. In this architecture the addition of new access networks changing permissions for the existing access networks and permissions are managed using this. In the RII architecture the different enforcement points are defined and the decision point does create rules for management. The policies are edited or created using a tool at the different levels. In this case we designed using an XML based entry for the policy creation and edition in the access networks. As shown in Figure 46 different PEP and PDP and creation or edition of rules in the RII architecture for the User and Access networks management.

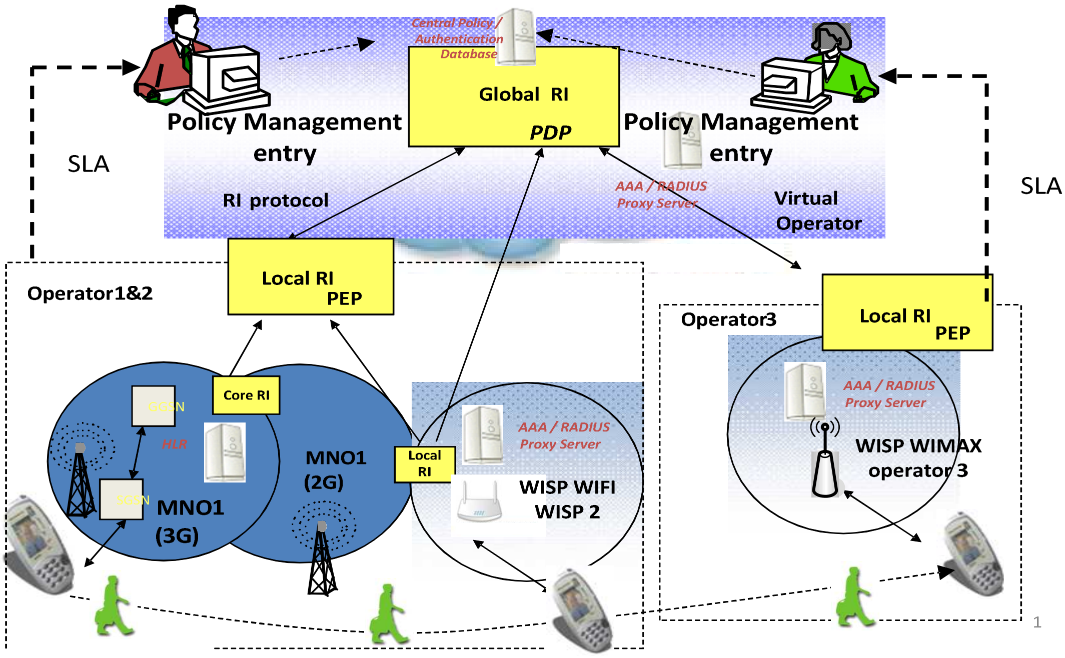


Figure 46. policy management in RII architecture

3.5.4. SLA Management

Service Level Management provides for continual identification, monitoring and review of the levels of services specified in the Service Level Agreements (SLAs). Service Level Management ensures that arrangements are in place with Provider and external entities in the form of Operational Level Agreements (OLAs) and Underpinning Contracts (UCs). The process involves assessing the impact of change upon service quality and SLAs. The service level management process is in close relation with the operational processes to control their activities. The central role of Service Level Management makes it the natural place for metrics to be established and monitored against a benchmark. Service Level Management is the primary interface with the customer (as opposed to the user, who is serviced by the Service Desk). Service Level Management is responsible for ensuring that the agreed services are delivered when and where they are supposed to be liaising with Availability Management, Capacity Management, Incident Management and Problem Management to ensure that the required levels and quality of service are achieved within the resources agreed with Financial Management producing and maintaining a different Service ensuring that appropriate Service Continuity plans. The Service Level Manager relies on all the other areas of the Service Delivery process to provide the necessary support which ensures the agreed services are provided in a cost effective, secure and efficient manner.

Service level management is provided in the RII architecture ensuring ubiquitous services for the subscribers in the RII architecture. As mentioned in the previous documents of this work package the main of the RII architecture is to provide an Peer – Peer SLA agreement is provided by the access networks and the inter AS-RI. There is no need to manage different SLAs with the other access networks providing easy management of the SLA and handling, creating and modifying in the architecture. The created SLA are stored in a centralized database of the RI which are accessible to different entities of the architecture. Authentication and access management does manage these issues after accessing the database.

3.5.5. Database Management

In this section we will describe the user and SLA database of the operators associated with the global RI.

3.5.5.1. User Database

User subscribers database contains details of the user and its SLA between the access networks. These details can be available on the RII according to the SLA of the RII and the access networks. In this particular case we have modified some AAA to provide a temporary user name in the RII and distribute among the access networks. The access networks then distribute these details to its users and suggest use these temporary user IDs when they are accessing visiting networks. The users use these IDs with NAI of the RII, visiting network then forwards the authentication and access request to the RII. RII checks its database for the user IDs which it has distributed to the access networks and forwards the authentication request to that particular access networks. After receiving the authentication request the home access network check the details and does the authentication of the user.

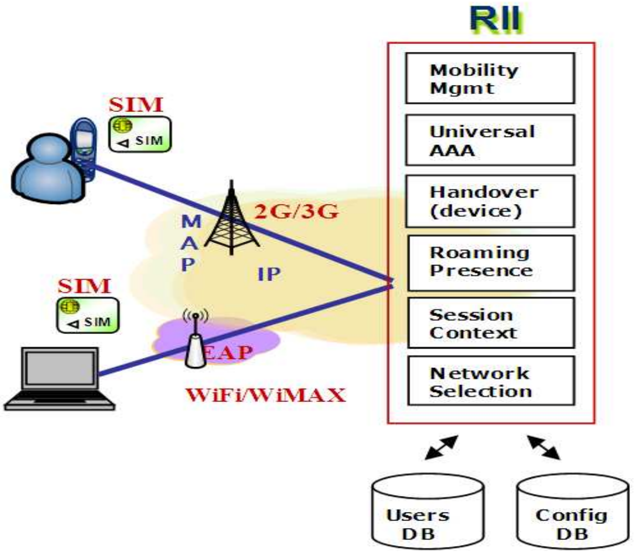


Figure 47. RII architecture using User DB and Config DB

3.5.5.2. Operator SLA database in the RII architecture

The operators SLAs are maintained in the RII at any given instance, the RII architecture can access this information to configure and providing services to the operators. Later in this deliverable we have provided details of maintaining the configurations and SLA between the operators using the network management tool kit developed using protégé.

3.5.6. Network Management tools

3.5.6.1. Ontology

An ontology defines the common words and concepts (the meaning) used to describe and represent an area of knowledge. An ontology is an engineering product consisting of “a specific vocabulary used to describe [a part of] reality, plus a set of explicit assumptions regarding the intended meaning of that vocabulary—in other words, the specification of a conceptualization. Ontology is a data model that represents a set of concepts within a domain and the relationships between those concepts. It is used to reason about the objects within that domain. Ontologies are used in artificial intelligence, the Semantic Web, software engineering, biomedical informatics and information architecture as a form of knowledge representation about the world or some part of it.

- Individuals: the basic or "ground level" objects
- Classes: sets, collections, or types of objects
- Attributes: properties, features, characteristics, or parameters that objects can have and share
- Relations: ways that objects can be related to one another
- Events: the changing of attributes or relations
- Elements: Contemporary ontologies share many structural similarities, regardless of the language in which they are expressed. As mentioned above, most ontologies describe individuals (instances), classes (concepts), attributes, and relations. In this section each of these components is discussed in turn.
- Individuals (instances): are the basic, "ground level" components of an ontology. The individuals in an ontology may include concrete objects such as people, animals, tables, automobiles, molecules, and planets, as well as abstract individuals such as numbers and words. Strictly speaking, an ontology need not include any individuals, but one of the general purposes of an ontology is to provide a means of classifying individuals, even if those individuals are not explicitly part of the ontology.
- Classes (concepts): are abstract groups, sets, or collections of objects. They may contain individuals, other classes, or a combination of both.
- Attributes: Objects in the ontology can be described by assigning attributes to them. Each attribute has at least a name and a value, and is used to store information that is specific to the object it is attached to.
- Relationships: An important use of attributes is to describe the relationships (also known as relations) between objects in the ontology. Typically a relation is an attribute whose value is another object in the ontology.

- Ontology languages: An ontology language is a formal language used to encode the ontology. There are a number of such languages for ontologies, both proprietary and standards-based:

OWL is a language for making ontological statements, developed as a follow-on from RDF and RDFS, as well as earlier ontology language projects including OIL, DAML and DAML+OIL. OWL is intended to be used over the World Wide Web, and all its elements (classes, properties and individuals) are defined as RDF resources, and identified by URIs. KIF is a syntax for first-order logic that is based on S-expressions. The Cyc project has its own ontology language called CycL, based on first-order predicate calculus with some higher-order extensions. Rule Interchange Format (RIF) and F-Logic combine ontologies and rules. In order to work with Ontology Languages, there is some useful technologies like Ontology Editor (to create ontologies using one of these languages), Ontology DBMS (to store and to query an ontology) and Ontology Warehouse (to integrate and to explore a set of related ontologies).

3.5.6.2. Protégé based network management tools in RII architecture

Ontologies start to be widely used in network management mainly because of their powerful semantic and inherent integration capabilities. Also, a strong community support is provided by active user forums (HP Jena, Stanford Protégé, etc.). Arguably, using an ontology language for unifying the syntax and the semantic of the architecture artifacts promise to greatly simplify the task of integrating heterogeneous operators' service delivery platforms. Based on our previous work [16], we have developed, using a bottom-up approach, a minimalist ontology for our scenario. Figure 48 outlines the extensible ontology framework used in this paper. We started by designing an ontology that capture the network characteristics and the operators service level agreements in the heterogeneous networks. The SLA's and Operators information are abstracted and entered into the system using a tool, and using this information integration is maintained at different layers of management between the operators.

After, we have used Protégé for creating instances compliant to our specifications as shown in Figure 49. Then, in order to accelerate the deployment of network configurations, we have developed a tool that load the instance ontology, manage it and generate different configurations files for the platform. The transformations of ontology instances into configurations files implement a transformation pattern that corresponds to our platform. Indeed, if the platform or the operators network artefacts changes, the ontology-based tool can easily be adapted.

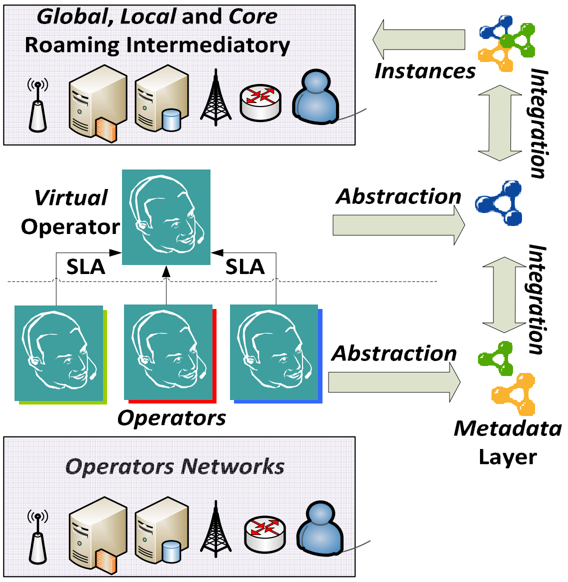


Figure 48. Bottom up Approach for Metadata

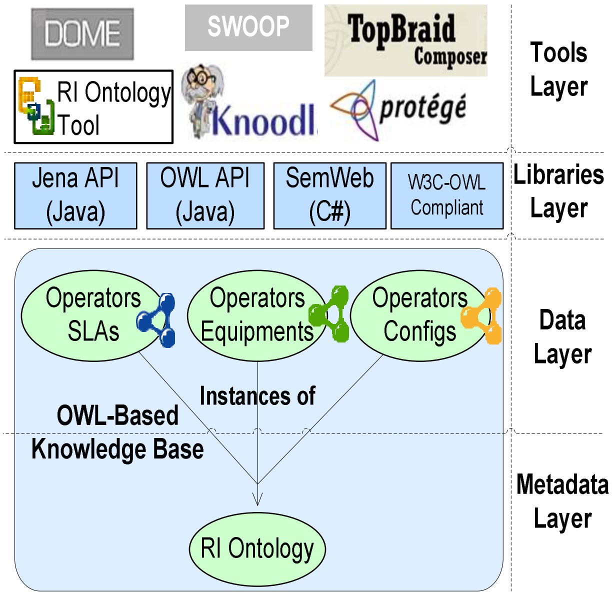
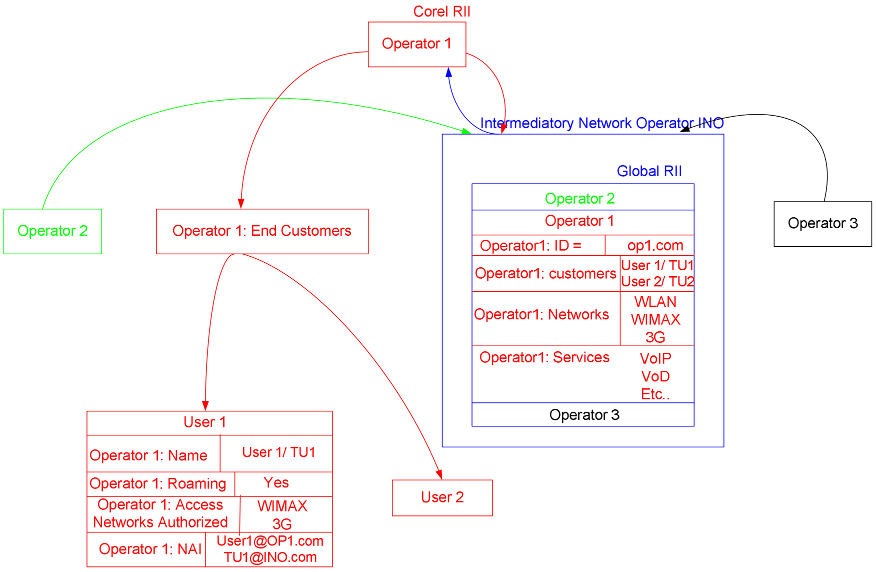


Figure 49. RI Ontology Framework

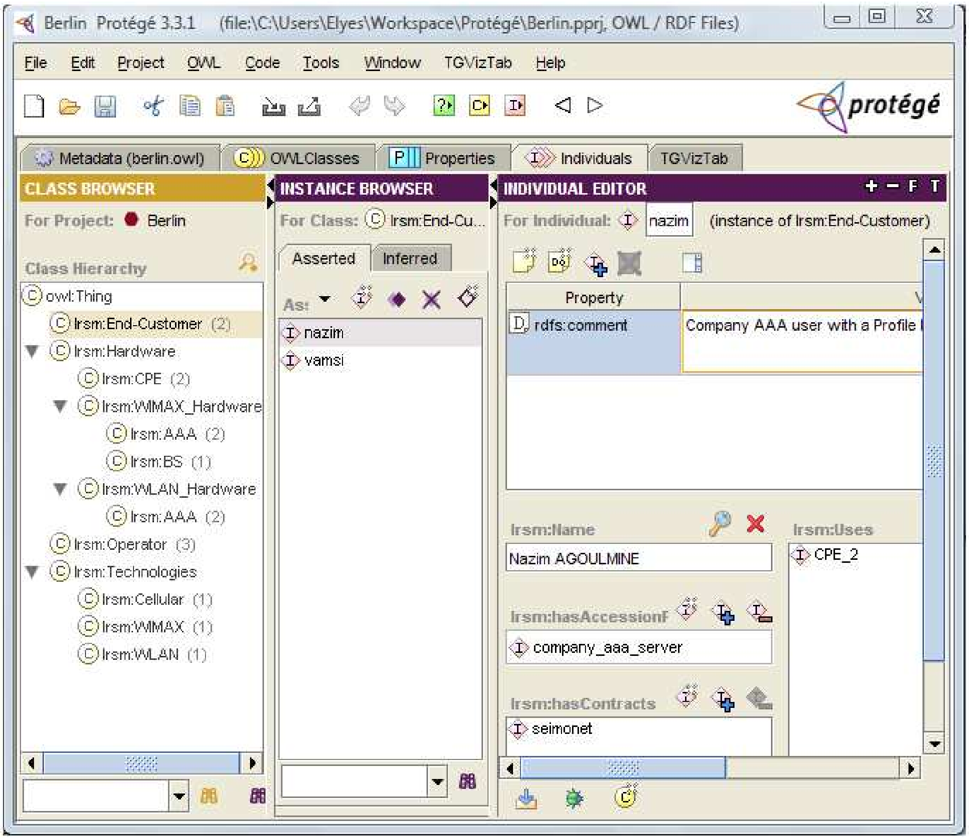
The following Figure 50 gives a brief overview of the ontology instance schema. In this example we have deployed different operators and their users and access technologies. These operator networks contains core RIIs and Local RIIs which are inter connected with the Global RII of the network. In this example operator 1 contains several users, these users details are stored in a database and can be accessed by Core RII of the network, using protégé based tool these information can be retrieved at any given instance. This information can be passed according to SLA of the operator and Global RII, based on the user SLA, the services offered and the access networks authorization can be maintained through this information even the user is roaming in visiting networks. The screenshot of management tools is shown in Figure 51 and Figure 52.


CoreI RII
Operator 1
Intermediatory Network Operator INO
Global RII
Operator 2
Operator 1: End Customers
Operator 3
User 2

Operator 2	
Operator 1	
Operator1: ID =	op1.com
Operator1: customers	User 1/ TU1 User 2/ TU2
Operator1: Networks	WLAN WIMAX 3G
Operator1: Services	VoIP VoD Etc..
Operator 3	

User 1	
Operator 1: Name	User 1/ TU1
Operator 1: Roaming	Yes
Operator 1: Access Networks Authorized	WIMAX 3G
Operator 1: NAI	User1@OP1.com TU1@INO.com

Figure 50. Overview of the resulting ontology



For Individual: nazim (instance of lrsm:End-Customer)

rdfs:comment Company AAA user with a Profile

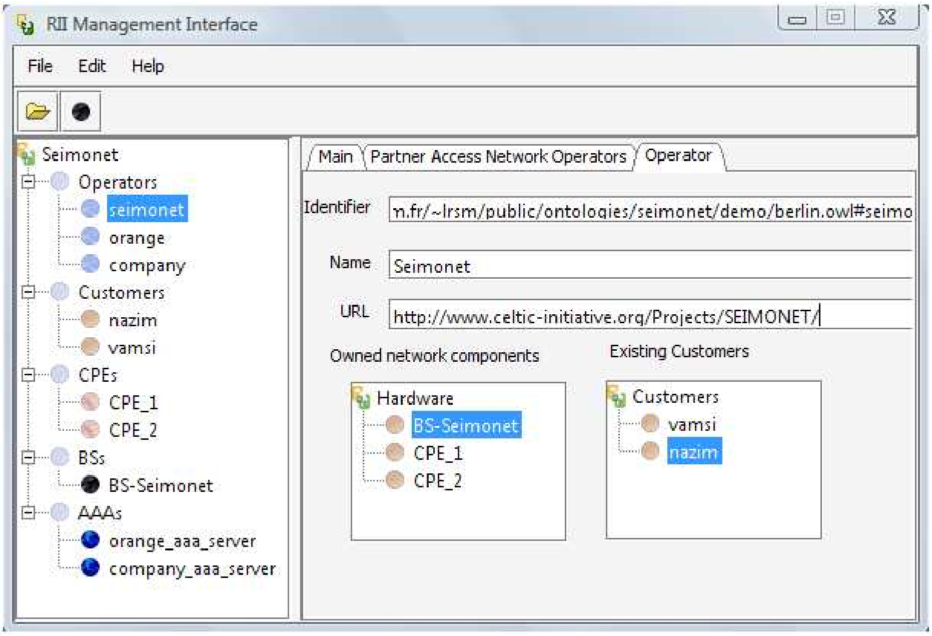
lrsm:Name Nazim AGOULMINE

lrsm:Uses CPE_2

lrsm:hasAccessionF company_aaa_server

lrsm:hasContracts seimonet

Figure 51 : screenshot of ontology tool developed



Identifier n.fr/~lrsm/public/ontologies/seimonet/demo/berlin.owl#seimo

Name Seimonet

URL http://www.celtic-initiative.org/Projects/SEIMONET/

Figure 52. Screen shot of RII management interface.

3.6. Comparisons

We have compared our approach to different approaches available in the literature. Existing architectures such as MobyDick [71], SeQoMo [72], FCAR [73], W-SKE [74], SeaSoS[80] taken into consideration. Table 6 shown below compares other existing architecture with the proposed architecture in this chapter.

Approach	Mobility Support	QoS signaling	Security	Key exchange
MobyDick	MIPv6; HMIPv6	Implicit session signalling	COPS/Diamter	No
SeQoMo	HMIPv6	QoS cond handoff	Diamter	No
FCAR	MIPv4	Changed RSVP	no	No
W-SKE	no	no	EAP+Radius	Yes
SeaSoS	MPIv4/6	Changed RSVP	EAP any AAA	Yes
RII	Any Mobility protocols, Proxy based MIPv4/6	Dedicated protocols for signaling with components as well as operator networks	Any AAA, EAP, AKA, SIM	Yes

Table 6. Comparisons of architectures for different entities.

3.7. Summary

We have presented a novel RII entity which offers a flexible means for interworking/roaming among different access systems. The proposed solution allows users to freely and securely move across different access systems without need of pre-existing subscription. The advantage of the RII architecture for roaming between WIMAX, cellular and Wi-Fi networks has been demonstrated via a testbed implementation. The solution is feasible and economical since it does not require much change in the existing network infrastructure. Indeed, the WIMAX/cellular operator that wants to benefit from such interworking and roaming facilities only needs to add the local/core RII functionalities in its access gateway by software upgrading. The virtual operators have much interest to implement the global RII to provide third party roaming services. With the adoption of proposed RII architecture, the network availability will be widely extended. Firstly, the users will have great interest since it can connect to any access networks. Secondly, the network infrastructure utilization will increase, which will give opportunities to operators to improve their profitability. In our future work, we will extend our RI ontology to align the test-bed artifacts with industry standards (IETF, DMTF, TMF, etc.).

Chapter 4. Post handover techniques for optimization of handover and roaming

Even though interworking architectures provides mobility and roaming in heterogeneous networks the latency during this procedure is very large. This latency is phenomenal and provides disruptive services to the users. There is a need to optimize the mechanisms involved in handover and roaming to obtain seamless mobility. We have identified two methods to obtain this objective one is post handover and the other is pre handover technique. In the post handover techniques at the time of handover the mechanisms involved does the optimization. In this chapter we discuss two mechanisms involving security and mobility.

The security optimization is one of the main challenges hindering the seamless roaming capabilities. With the introduction of multiple access technologies, different security mechanisms involved for authentication complicates the concept of seamless roaming. Re using the keying material involved in one security mechanisms to another is the main approach we are following, as this removes the whole procedure of generating keying material, messages involved during this keying is minimal. This keying material can be handled efficiently by home operator of user and introducing new techniques to use generated IDs and keys in another technology access or in the visiting operator networks. We achieved this goal by utilizing RII architecture and introducing new protocols for context transfer. In this process the home operator generates the keys and re-authentication IDs and dynamically transfers to users as well as visiting operator networks by security context management. Once this procedure is performed the user terminal utilizes this data and does the authentication in the visiting network itself without re-routing authentication data to home network. In this chapter we have proposed mechanisms to utilize this process in WLAN, WIMAX networks keys generated in cellular networks by RII architecture.

Mobility access through IPv4 and IPv6 provides seamless services for user terminals across different access networks. To provide seamless continuity during mobility of users from one operator access network to another, and one technology to another, will be provided by different mechanisms. The proposed mechanisms provide mobility, with special requirements and access mechanisms. Client Mobile IP (CMIP) is a popular solution for mobility, but there are limitations and so it cannot provide a total mobility solution. Proxy Mobile IP (PMIP) is a mobility mechanism which aims at ensuring mobility management of user terminals in different access networks. This method provides network based mobility management without any client interaction. By this method, overhead signaling and latency during handover and roaming is reduced. In this proposed mechanism, mobile nodes do not need to have support for mobility, but instead access networks provide mobility for user terminals. Even though proxy mobile IPv4 provides mobility management, there are some issues that have to be resolved for network controlled mobility management. In this architecture we propose new mechanisms, using proxy mobile IP and AAA with new mobility extensions to provide low latency handover support in heterogeneous networks. We propose new protocol formats and algorithms, and interactions between different components of architecture in heterogeneous networks. We have developed a testbed using WLAN, WIMAX, 3G access networks, and have demonstrated capabilities of resulting solutions. Comparison has been made out with the results and existing mobility solutions to prove efficiency. The issues of IPv6 migration in the architecture have been discussed.

4.1. Security Authentication

This section provided details of security access mechanisms involved authentication of user terminals in access networks. The authentication mechanisms differ from one access technology to another and one operator to another. Generally the authentication is performed by home access networks through the visiting access networks. The whole procedure generated latency as the authentication information is routed through the home and visiting networks for every single exchange of information. The user identity is static in general procedures and the use of identity in visiting networks and technology is provided statically. User identity management is one of the main issues which have to be addressed in heterogeneous networks. Maintaining the identity is crucial for future converged networks as the user credentials differ from one technology to another differs.

Using RII architecture we have addressed this issue. We have approached two ways to solve ever longing issue of user identity and routing of user authentication information from visiting access networks with or without a direct SLA with the home network.

4.1.1. Authentication using Global RI user identity.

In this method the Users are informed to use NAI of the home access network when they are in vicinity of local networks, and use NAI of Global RI when they are in the visiting network using the same user ID. When the user terminal is at home network the local RII and AAA server of the access network identify the authentication request from the user which is relayed by a NAS or AP. After identifying the NAI of the user access request, the AAA server of Local RII does initiate the authentication. Once authentication is done the user terminal is provided the access. If ever the user terminal is in the visiting network, the terminal sends authentication request to NAS or AP with the NAI of the global RI with its own user ID. Once the local RII of the visiting network identifies the global RII NAI it proxies the authentication request to the Global RII. Once the global RII identifies the user ID which it belongs to a network, it forwards the authentication to the local RII with the stripped user ID. Once authentication request is received by the home Local RII, it checks local database and authenticates the user according to its security credentials. The whole process mechanism is sown in Figure 53

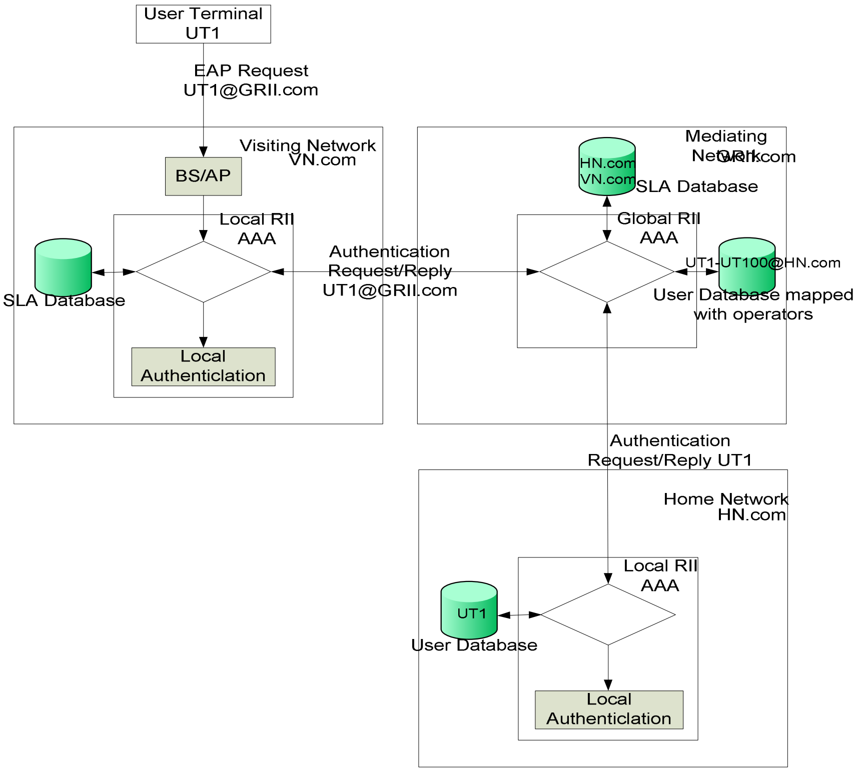


Figure 53. Authentication flow using Global RII

4.1.2. Authentication using temporary user identity allocated by home access networks.

In this method the global RII creates the temporary user IDs and distribute them among the network operators. Network operators based on the SLA with its users they distribute the user IDs to its subscribers. Once the Access networks receive this temporary user IDs, they distribute to users and map with their permanent user IDs (the main objective is to maintain high privacy of the subscribers by not relaying their user details but instead using a temporary and a trusted source to translate the credentials.). Once the visiting network identifies the authentication request from a user with NAI of global RII it forwards the authentication request to global RII AAA server. Once the AAA server of global RII receives the authentication request from a temporary user ID, it checks the database for access network for which it has assigned this temporary ID before. After identifying the access network the AAA server proxies request to home network of the user. With the temporary user ID, from authentication request the AAA server authenticates user and provides services. The whole process is mentioned in Figure 54.

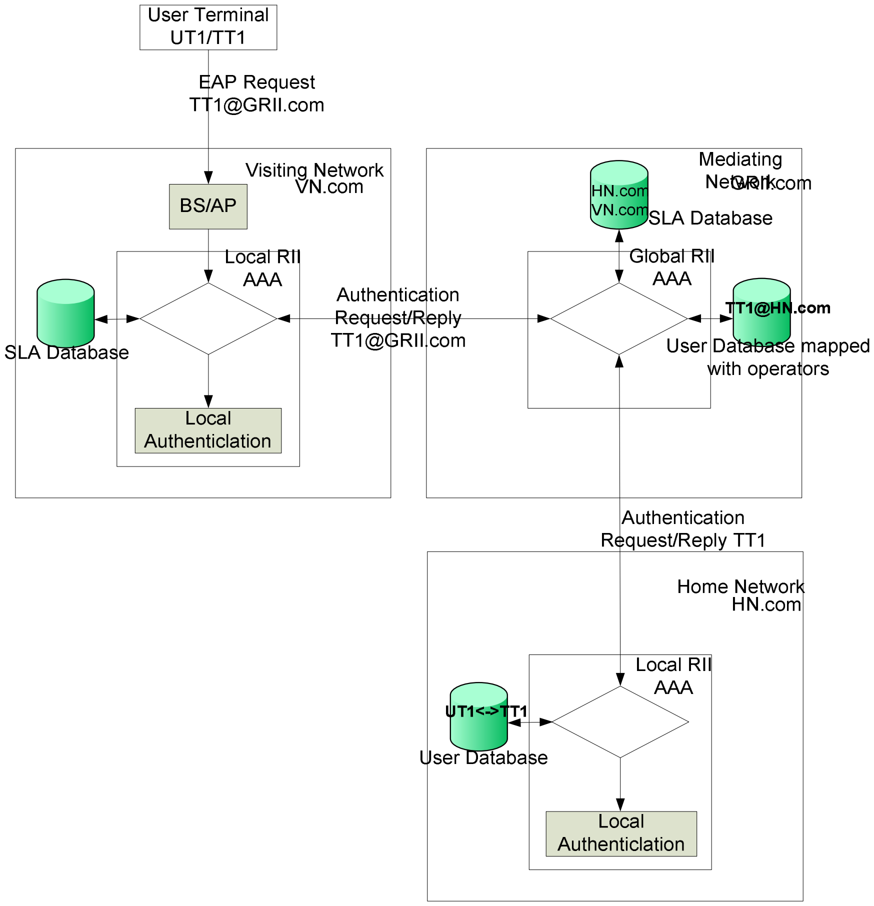
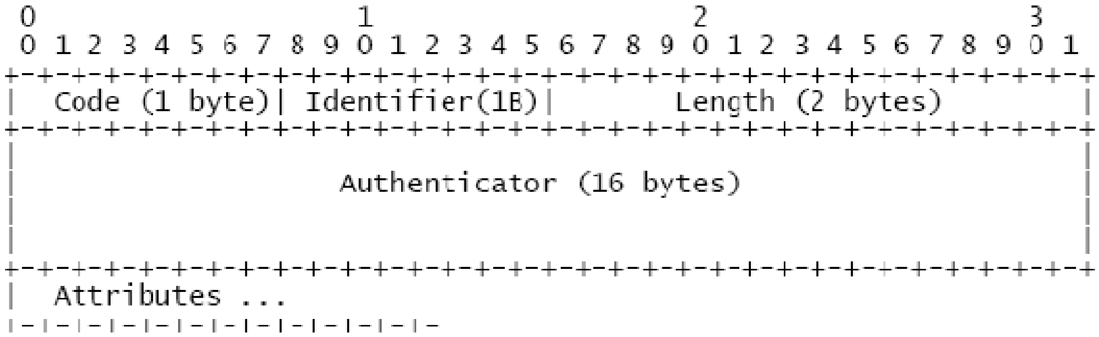


Figure 54. Authentication flow using temporary IDs and Global RII

4.1.3. Radius Roaming Extensions for security context transfer for authentications.

For supporting the methods proposed in the architecture we are proposing new roaming extensions for AAA server. In this process the home RI of access networks and global RI prepares the security context and transfers to the visiting network through AAA server. We have chosen AAA server as it is readily deployable in wireless and cellular networks, modifying with the new extensions is easily done instead of deploying new protocols. The following section provides the protocol formats used for security context transfer using radius protocol.

The home Radius server builds SC Request message from the Access.



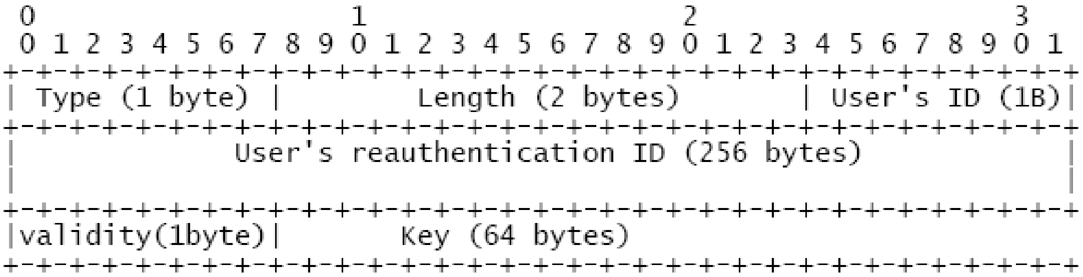
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Code (1 byte)| Identifier(1B)|      Length (2 bytes)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                   Authenticator (16 bytes)                    |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
|-|-|-|-|-|-|-|-|-|-|-|-|-|-
```

Code = (1 byte) SC_Request = TBD (IANA consideration)

Identifier: (1 byte) number to match the Request/Reply.

Length: (2 bytes) length of the message, including Code, Identifier, Length, Authenticator, Attributes.

Authenticator: The Authenticator field is 16 bytes. The most significant octet is transmitted first. This value is used to authenticate the reply from the RADIUS server, and is used in the password hiding algorithm.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type (1 byte) |       Length (2 bytes)        | User's ID (1B)|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              User's reauthentication ID (256 bytes)           |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|validity(1byte)|       Key (64 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type (1 byte) = SC_Request_Attribute = TBD (IANA consideration)

Length (2 bytes) = Length of the message User's reauthentication ID: (256 bytes) home radius server assign this id and forwards this to the visiting networks radius server and as well as to client.

Validity (1 byte) = the valid time of the key and the re authentication id.

Key (64 bytes) = temporary key which is derived in the home radius server the visiting radius server reply to the home radius server with SC Accept message.

Code = SC_Accept = TBD (IANA consideration)

If there is any failure in the packet or the details of SC configuration on the visiting server, it sends the failure to the home radius server.

Code = SC_Reject = TBD (IANA consideration)

4.2. Mobility management

The mobility management in the access networks is provided by the mobile IP for the seamless continuity of the services during handover and roaming. The traditionally user terminal does require a mobile node enabled with a client mobile IP, in some cases the devices can't be enabled with mobile IP, in this case mobility must be provided without changing the software configuration of the devices and provide mobility from access network side. By this method controlling the mobility of the user terminal can be more efficient.

The Proxy Mobile IP [79] solution based on Mobile IP approach; handles mobility management inside access networks. Therefore network entities will require more capability than in the standard Mobile IP. The Foreign Agent is no longer capable to handle the mobility management in this new scenario, so we need to enhance its capabilities with the Mobility Proxy mechanism. This new entity called Mobile Proxy Agent replaces Foreign Agent in the visiting network. It also handles mobility registration with the Home Agent. This change is most significant since the Mobile Node now lies outside the mobility registration procedure. In fact, Mobile Node is not aware of its movement, access networks deceives the host to believe that it is stationary in its Home Network. Since the Mobile Node does not need either movement detection or agent registration, the agent advertisements are no longer necessary.

There are some of the requirements and features to be satisfied for PMIP to provide mobility management:

- Support Unmodified Hosts: As noted above, the protocol supports mobility to nodes that doesn't have capability of mobility.
- Airlink consumption: Mobility-related signaling over the air-link is eliminated. Considering that Network Address Translation (NAT) is ubiquitous in IPv4 networks, a mobile node needs to send keep alive at short intervals to properly maintain NAT states. This can be performed by the MPA in the network which does not consume any air-link bandwidth. The Agent Advertisement is also eliminated in the protocol.
- Support the Heterogeneous Wireless Link Network: One aspect is how to adopt the scheme to an access technology. Since Proxy Mobile IPv4 is based on a heterogeneous mobility protocol, it can be used for any type of access network.
- The other aspect is how to support mobility across different access technologies. As long as the MPA can use the same NAI to identify the MN for various access networks, roaming between them is possible.
- Support the IPv4 and IPv6: As IPv6 increases in popularity, the host will likely be dual stack.

Even though the PMIP provides mobility solutions, there are many issues of user identity, mobility context of users from a home network to the visiting network, the assignment of home address to a user terminal in a visiting network, identification of the user terminal's mobility, and identification of MPA and HA. In this paper, we propose a new mechanism with proxy mobile IPv4, as a mobility solution in networks. In this mechanism during mobile node access authentication, MPA exchanges registration messages with the HA (Home Agent) to set up a suitable routing and tunneling for packets from/to the MN. In this method, the authentication request of the mobile node is passed through the NAS or AP of visiting network, this is then passed to the AAA (Authentication Authorization and Accounting) server, and the authentication server checks the realm and does start authentication procedure at the time of initialing authorizing module of the mobile terminal. It also initiates the mobility extension module, where the AAA server initiates MPA of the access network, which also informs the AAA server of the home network with information on the mobility extensions and request of the mobility parameters of the user terminal. The home AAA server interacts with the HA and collects mobile node parameters, as well as sending back details as a reply request to the visiting AAA server. After the mobility context transfer, the MPA conducts a mobility registration to the HA for that particular mobile node. Later in this paper, we will provide more details of the interaction between different components of the architecture, packet formats, and sequence of message exchanges during a mobility session of a user mobile node during handover.

4.2.1. Proposed new solution for PMIP with integrated AAA architecture of the 3GPP and Wireless networks

4.2.1.1. Overview of the solution

In this new mechanism, mobility registration of a user terminal is performed by visiting access networks and a home access network. The user terminal does general authentication by visiting access networks with the help of an EAP (Extensive Authentication Protocol) mechanism. The visiting access networks receive the authentication request from a user terminal through the NAS or AP of the network. The AAA server of visiting network and home networks are modified so that they can communicate with the HA and MPA of their respective networks. New mobility extensions are developed in AAA server to support mobility management, which adds to its present services. These extensions provide mobility context transfer from home access networks, registering the user terminal for mobility at the time of authentication. The visiting network initiates authentication and the mobility extension method whenever it receives a request from the NAS or AP of the access network. During initiation of mobility extensions, the AAA mobility extension process collects data when NAS/AP requests authentication. The AAA mobility process sends mobility user details request to the home network and the AAA server of the terminal, with newly specified attributes of proxy mobile IP. The Home AAA server does receive a request for the mobility user details request as well as the authentication. The home AAA server distinguishes a proxy mobile IP packet from other codes and attributes of the received packet. If the packets need to be a proxy from an intermediate AAA server, then that server adds the proxy attribute to the received packet and sends it to the destination AAA server. If ever the user terminal belongs to the current network, then the AAA server sends a mobility registration request to HA.

After receiving the request for mobility user details packet from the visiting AAA server, the home AAA server investigates any information available in the packet and collects user identity from the request packet. After processing the request, the mobility extension method prepares user detail request packet to the HA of the access network. This packet contains details of user id and parameters. The HA receives a request, and with a user ID of request it extract the information of its SID, keys, home address and home agent address from the database of the HA. The HA then sends back a reply to the AAA of home network with the above mentioned data. The AAA server receives a reply and processes the information, and sends back a reply message to the visiting AAA server. The visiting AAA server receives a reply from home server and processes it, storing the data of the user in a temporary database. After processing the reply message, the AAA server sends a mobility registration request to the MPA associated with that particular NAS or AP. This request contains the details about user ID, SPI, keys, home address and home agent address. When the MPA receives the packet it starts the mobility registration of a user with details from the AAA server.

MPA initiates a mobility registration request of a user terminal with HA using details provided by visiting AAA server. Registration involves the user SPI and the shared key mechanisms with the key available from the AAA server to the MPA. After successful registration of the user with the HA, the MPA will modify the DHCP server configuration with the user terminal's details. These modifications contain details of MAC address and home address of the user in the DHCP server. After successful authentication of the user terminal it initiates a DHCP request for an IP address. The AP/NAS of the visiting network forwards the request to the DHCP server. With the MAC address of the user terminal modified, the DHCP server sends a reply to user's terminal with its home address. The user terminal receives the reply and configures the IP address to the home address. Necessary modification has to be done by the visiting network to accommodate the terminal with the ARP, etc. When the user terminal is in it home domain, the HA registers the terminal and sends the modified DHCP request to the DHCP server and acknowledges the home AAA server of successful registration of a user terminal. The Proxy Mobile IP with the AAA server mobility architecture is shown in Figure 55.

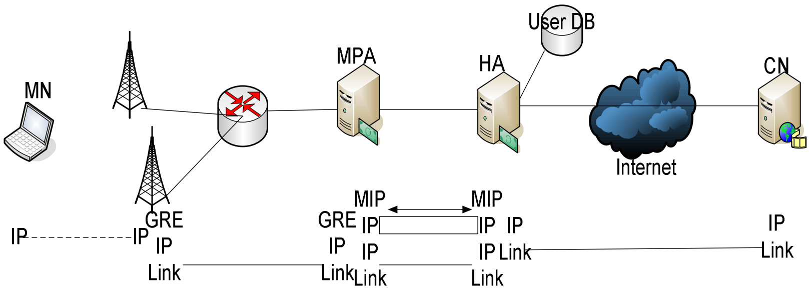


Figure 55. Proxy Mobile IP Architecture

4.2.1.2. AAA mobility extensions for PMIP integrated architecture

In this section we describe the detailed architecture of AAA with mobility extensions to provide mobility management during user mobility in different access networks and technology. In this process, the existing AAA architecture is modified to accommodate proxy mobile IP. In general, authentication information of users is passed through the authenticator, and then this information is passed through the NAS or AP of the access networks. An AAA server authenticates the access networks for the AP or NAS initially, and then processes the user authentication request depending on the realm of the user. In this new method, the mobility management of a user can be initiated during the authentication process. In this process, due to parallel operation of authentication and mobility management, the overall latency of a user during the handover and initial access can be reduced.

When there is an authentication request for a user terminal from an NAS or AP, the AAA server initiate authentication module and mobility modules, and processes the user's details by identifying the NAI of the user terminal request. From the NAS or AP request information, such as MAC address of user terminal, NAS details are processed for further procedures. The AAA is modified, with new attributes and codes being added for supporting the PMIP modules. As mentioned previously in the proposed solution section with new extensions, the AAA of the home network can communicate with a visiting network, and can provide mobility context management. With these mobility extensions, the AAA server can communicate with the MPA and HA of the access networks.

On the other side, the visiting AAA server communicates with the home network AAA server, after receiving an authentication request using the mobility extensions, with user information being available from the authentication request from the user's terminal. The visiting server sends a mobility user details request using ID and NAI of the authentication request to the home AAA server. When the home network receives a request packet, the AAA server processes the information of the user from request. It then sends a request to the HA with the new mobility extension, requesting details of the user. After receiving the request packet and processing user details from its internal database, the HA sends back a reply packet with home address, key, SPI and home agent address to the home AAA server. The home AAA server sends back a reply to the visiting AAA server with user details as the reply. After receiving this reply from the home AAA server, the visiting AAA server processes the information of the user and sends a request for mobility registration request with new attributes to the MPA. The MPA receives the user terminal data, sent by the visiting AAA server, and temporarily stores it in a local database. The MPA, with available user information, starts registering with the HA. After registration request and reply message exchange with HA, the MPA sends reply of success or the failure of mobility registration of user to visiting AAA server. Figure 56 describes the AAA mobility architecture.

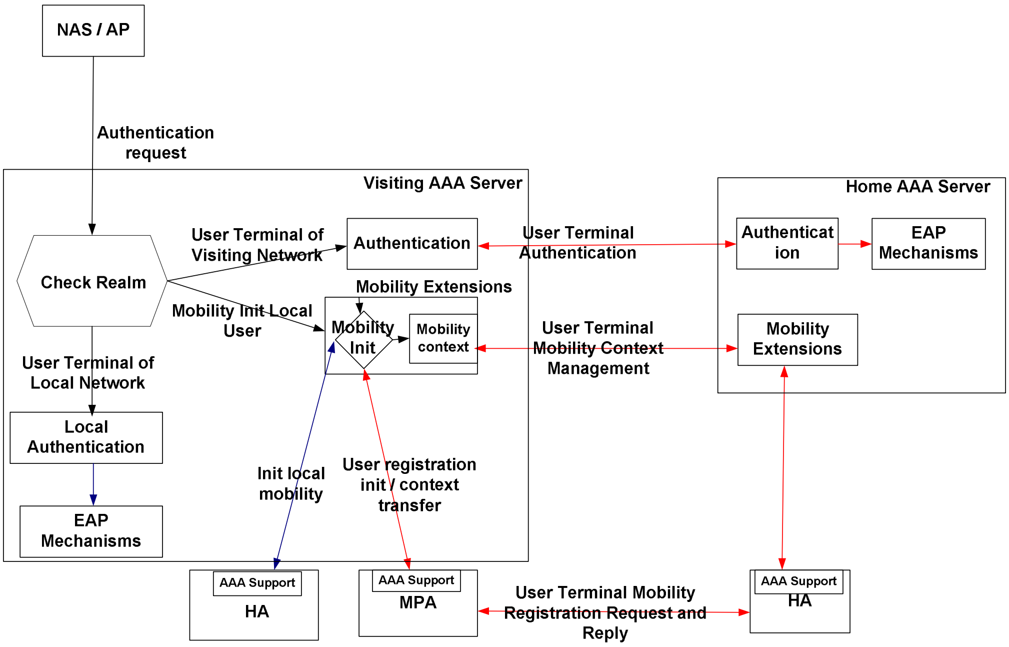


Figure 56. AAA architecture with new mobility extensions and PMIP

4.2.1.3. *PMIP operation with new mobility extensions in MPA and HA*

MPA exchanges registration messages with the HA to set up a proper routing and tunneling packets from/to MN. The MN broadcasts messages containing an MN's Network Access Identifier (NAI) to request authentication/authorization, and the AP transfers the request to the local AAA server (visiting AAA). If the MN is away from home, it is clear that the MN is out of the local authentication database. However, the local AAA server can use the NAI to identify the MN's Home Network, and then the authentication/authorization, along with mobility user details, will request a message to be transferred by the visiting AAA to the home AAA Server (AAAH) in the Home Network.

Along with the authenticating validation, the AAAH searches for information of the MN stored in the HA, containing MN's HA, NAI, and SPI. If the MN is back to its Home Network, then the local AAA server sends a message to the HA to deregister the MN instead of searching for the data. The MN's information will be transferred to the visiting AAA, which will deliver it to the MPA with the AP's MAC address included. Triggered by the AAA server, the MPA exchanges messages with the HA to demand Mobility Registration and Tunneling. Formats of the Mobile IPv4 Registration Request (MIPv4 RRQ – sent by the MPA) and the Mobile IPv4 Registration Reply (MIPv4 RRP – sent back by the HA) are specified in section 4.2.2.

After successful registration, the MPA sends a message to inform the DHCP server about the MN's arrival. It forces the DHCP server to update the configuration file with the Mobile Node information. Finally, the MPA informs the AAA visiting about the successful registration. The Authentication Accept message is sent to the NAS, granting network access to the MN. After authentication success, the MN sends a Binding DHCPDISCOVER to request the IP address. This message is formatted as described by the DHCP protocol (the CIADDR field is filled with the MN's IP). By searching for information of the Mobile Node, in the configuration, the DHCP server replies with a DHCPOFFER message in which the YIADDR field is filled with the MN's Home Address and the default gateway address, being the MPA's. Next, the MN and DHCP server exchange the DHCPREQUEST and DHCPREPLY to complete this procedure. The MN is then ready to connect to the network with its Home Address.

4.2.2. Components interactions with the new extensions proposed in the architecture

4.2.2.1. Mobility Registration

The MN broadcasts messages containing MN's Network Access Identifier (NAI) to request authentication/authorization (Step 1 in Figure 57). The AP transfers the request to the local AAA server (visiting AAA server). If the MN is away from home, it is clear that the MN is out of the local authentication database; however, the local AAA server can use the NAI to identify the MN's Home Network. Along authentication/authorization, visiting AAA server sends mobility user details request message to AAA Server (AAAH) in the Home Network (Step 2).

Alongside with the authentication, the AAAH searches for the information of the MN stored in the HA (Step 3), containing MN's HA, NAI, and SPI. If the MN is back to its Home Network: the local AAA server sends a message to HA to deregister the MN instead of searching for the data. The MN's information will be transferred to the visiting AAA (Step 4), After successful user details request and reply AAA of visiting network sends a mobility registration request to MPA with the AP's MAC address included (Step 5).

Triggered by visiting AAA server (Step 5), the MPA exchanges messages with the HA to demand for the Mobility Registration and Tunneling (Step 6). The formats of the Mobile IPv4

Registration Request (MIPv4 RRQ – sent by the MPA) and the Mobile IPv4 Registration Reply (MIPv4 RRP – sent back by the HA)

After successful registration, MPA sends a message to inform DHCP about the MN's arrival (Step 7). It forces the DHCP server to update the configuration file with the Mobile Node information. Finally, the MPA informs the visiting AAA about the registration successful. The Authentication Accept message is sent to the NAS granting network access to the MN (Step 8).

After the authentication success, the MN sends a Binding DHCPDISCOVER to request for the IP address. This message is formatted as described by the DHCP protocol (the CIADDR field is filled with the MN's IP). By searching the information of the Mobile Node in the configuration, the DHCP server replies with a DHCPOFFER message in which the YIADDR field is filled with the MN's Home Address and the default gateway address is MPA's. Next, the MN and DHCP server exchange the DHCPREQUEST and DHCPREPLY to complete this procedure. The MN is then ready to connect to the network with its Home Address (Step 9).

4.2.2.2. Registration Revocation

After having received Mobility Registration Request (Step 6 in the Figure 57), the HA sends a message to the old MPA of the last visited network to which the MN was connected in order to erase the entry of the MN in that network (including the Mobility Registration database of the old MPA and the DHCP configuration) (Figure 58). Remark that the Mobility Registration Database in the HA is modified and the MobileIPv4RRP is sent regardless to the reception of the Registration Revocation Reply (this message can be undelivered due to congestion, disconnection of the network, etc).

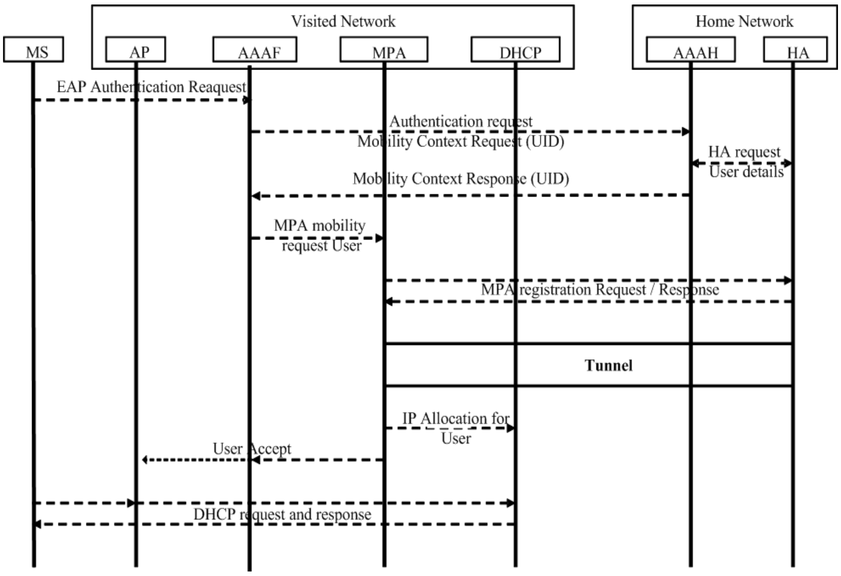


Figure 57. Sequence diagram for new mechanisms with PMIP

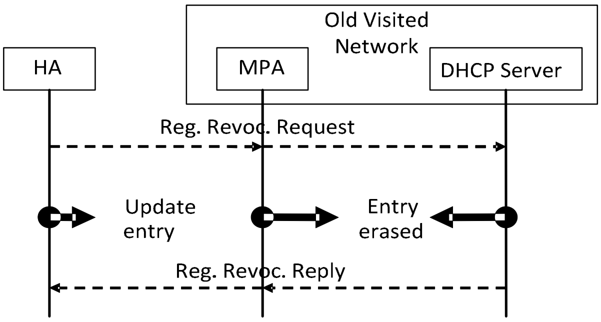


Figure 58. Registration Revocation

4.2.2.3. *ARP, Proxy ARP and Gratuitous ARP*

The use of ARP [80] requires special rules for correct operations when wireless or mobile nodes are involved. The requirements specified in this section apply to all home networks in which ARP is used for address resolution.

In addition to the normal use of ARP for resolving a target node's link-layer address from its IP address, we distinguish two special uses of ARP:

- A Proxy ARP [81] is an ARP Reply sent by one node on behalf of another node which is either unable or unwilling to answer its own ARP Requests. The sender of a Proxy ARP reverses the Sender and Target Protocol Address fields of the request, but supplies some configured link-layer address (generally, its own) in the Sender Hardware Address field. The node receiving the reply will associate this link-layer address with the IP address of the original target node, causing it to transmit future datagram for this target node to the node possessing the link-layer address associated.
- A Gratuitous ARP is an ARP packet sent by a node in order to spontaneously cause other nodes to update an entry in their ARP cache. A gratuitous ARP may use either an ARP Request or an ARP Reply packet. In either case, the ARP Sender Protocol Address and ARP Target Protocol Address are both set to the IP address of the cache entry to be updated, and the ARP Sender Hardware Address is set to the link-layer address to which this cache entry should be updated. When using an ARP Reply packet, the Target Hardware Address is also set to the link-layer address to which this cache entry should be updated (this field is not used in an ARP Request packet).

4.2.2.4. *Back to home network*

As the MN returns to its Home Network, this information is revealed to home AAA server (AAAH) by receiving a Access Request from a NAS, home AAA server will sends a HA Registration Revocation Request to HA which erases the MN entry in its Mobility Registration Database and sends an MIPv4 Registration Revocation to the MPA on the last network that MN has visited. Recall that the Mobility Request message makes the AAAH send a HA

Consultation message in order to get information of the MN, while the Access Request makes the AAAH send a HA Registration Revocation to erase the MN's mobility registration entry.

4.2.3. PMIP with the new extensions in different user terminal mobility scenarios

In this section we will explain in detail of mobility movements of the users in various scenarios. We also provides mechanisms to ensure fast handover mechanisms are provided when the mobile is moving in same domain, different domains and access technologies. The solution we proposed handles the multi homing scenario where a user terminal is provided with the different interfaces and access technologies later in this section. The mobility of the user in different scenarios is depicted in Figure 59.

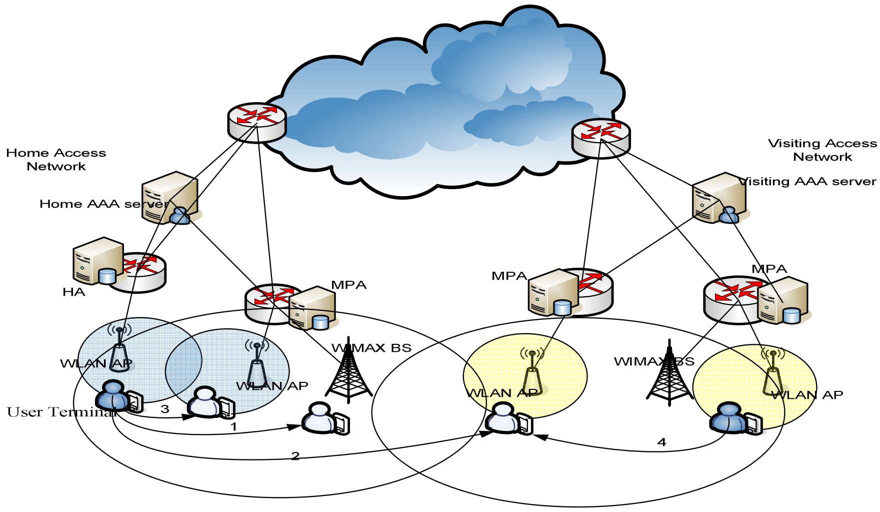


Figure 59. User mobility scenario in different administrative and technology domains

1. User Terminal mobility in the inter-access technology (Macro Mobility).
2. User Terminal mobility from one network operator to another operator network (Macro Mobility intra-access).
3. User Terminal mobility in the same access technology in the home operator network.
4. User Terminal mobility in the visiting networks in the same access technology.

4.2.4. Macro Mobility

In this scenario the user mobile does move from one administrative domain to different administrative domains (one operator to another operator) and from technology to another technology (WLAN<->WIMAX<->3G<-> WLAN).

4.2.4.1. *User mobility from one technology to another access technology*

In this scenario mobile node maintains multiple network interfaces for connecting to access networks. The selection of best suited network is performed according to the SLA, desired QoS and other factors which is out of this chapter context. In this process mobile node initiates access network initially and establishes a session with the access network. During initial authentication procedures, access networks also create mobility context of user and registers user in HA of access network. When user terminal detects availability of access networks on other interface it initiates new interface and starts performing authentication. After listening to the NAS request for authentication of user, visiting access AAA server collects user details from NAS requests and sends authentication and mobility user details request in parallel. Home AAA server after listening to mobility user details request does reply with required details of user with SPI, HA details and home address of the user to visiting AAA server as a reply. After collecting details, visiting AAA sends registration request to MPA of network where NAS or AP resided. The MPA starts the registration of user terminal with HA and caches route in DB of MPA. Once the tunnel is established between HA and MPA, HA updates new route for to and fro communication with user terminal. Figure 60Figure 4.8 provides detail message sequence involved during the procedure.

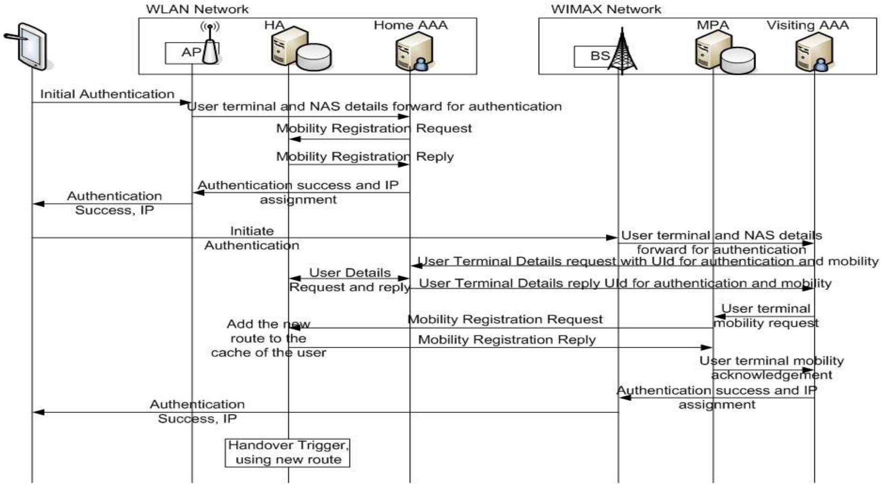

WLAN Network
AP
HA
Home AAA
WIMAX Network
BS
MPA
Visiting AAA
Initial Authentication
User terminal and NAS details forward for authentication
Mobility Registration Request
Mobility Registration Reply
Authentication success and IP assignment
Authentication Success, IP
Initiate Authentication
User terminal and NAS details forward for authentication
User Terminal Details request with UId for authentication and mobility
User Details Request and reply
User Terminal Details reply UId for authentication and mobility
User terminal mobility request
Mobility Registration Request
Add the new route to the cache of the user
Mobility Registration Reply
User terminal mobility acknowledgement
Authentication success and IP assignment
Authentication Success, IP
Handover Trigger, using new route

Figure 60. Message exchange between components of architecture during multi technology scenario

4.2.4.2. *User terminal roaming from one operator network to another.*

In this procedure user terminal connects to an access network and performs authentication to the access network. Access network does register terminal to a HA and provides the IP address to the user terminal. When user terminal does identify different operator network it tries to connect that network by initiating the authentication or re-authentication procedures. When NAS or AP receives the request for authentication, it forwards the details to AAA server. Visiting AAA server does initiate mobility user details request to home network AAA server by identifying the NAI of the user ID for authentication. Upon receiving request home AAA server collects data associated to user ID from request and reply message to HA and sends back reply to visiting AAA server. Visiting AAA server sends mobility registration request to MPA of network associated to the NAS or AP with collected details from home AAA server. MPA does registration with HA using details from AAA server, and sends acknowledgement to AAA server. After authenticating user terminal and upon receiving the reply from MPA, visiting AAA server send success with the IP address of the user terminal sent by the home AAA server to NAS/AP. The message exchange is shown in Figure 61.

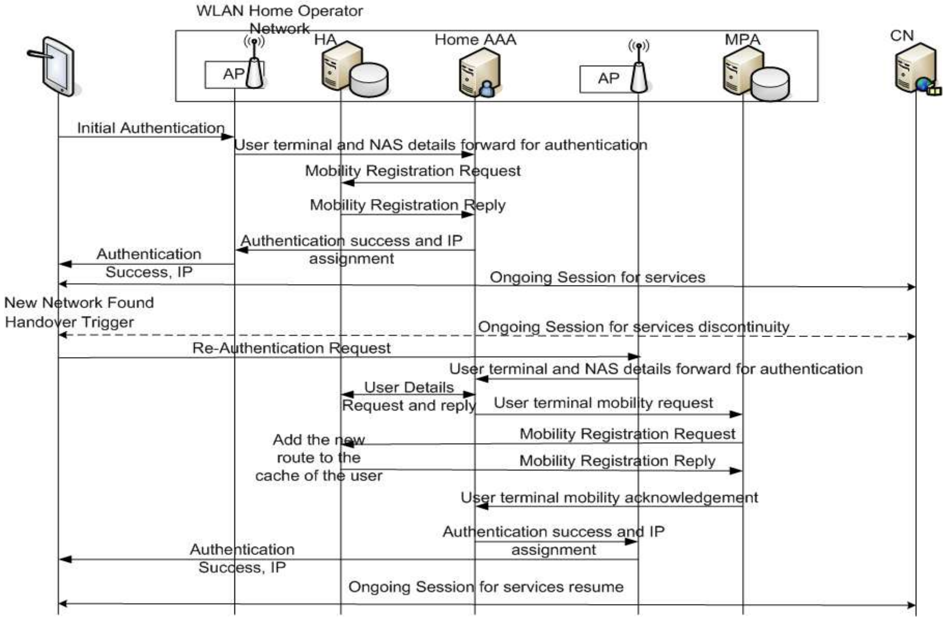

WLAN Home Operator Network
AP
HA
Home AAA
AP
MPA
CN
Initial Authentication
User terminal and NAS details forward for authentication
Mobility Registration Request
Mobility Registration Reply
Authentication success and IP assignment
Authentication Success, IP
Ongoing Session for services
New Network Found Handover Trigger
Ongoing Session for services discontinuity
Re-Authentication Request
User terminal and NAS details forward for authentication
User Details Request and reply
User terminal mobility request
Mobility Registration Request
Add the new route to the cache of the user
Mobility Registration Reply
User terminal mobility acknowledgement
Authentication success and IP assignment
Authentication Success, IP
Ongoing Session for services resume

Figure 61. Message exchange between components of architecture during roaming scenario

4.2.5. Micro Mobility

In this scenario mobility is performed in same administrative domain and same access technology, we have observed two sub scenarios where the proposed architecture addresses this issue.

4.2.5.1. User terminal mobility in home administrative domain on same access technology

In this scenario access network has multiple APs, and user terminal moves from one AP to another AP. During initial authentication of user, AAA server does authenticate user and assists HA for mobility registration of user terminal. When user terminal senses other APs of access network and triggers the handover with re-authentication procedure, upon receiving request from new AP, the AAA server sends a mobility registration request to MPA associated with AP. MPA and HA does the mobility registration of the user terminal and sends acknowledgement to AAA server. Upon successfully authentication and registering terminal in

HA, it provides access and home IP address of user terminal to AP for providing access to user terminal. The message exchange is shown inFigure 62.

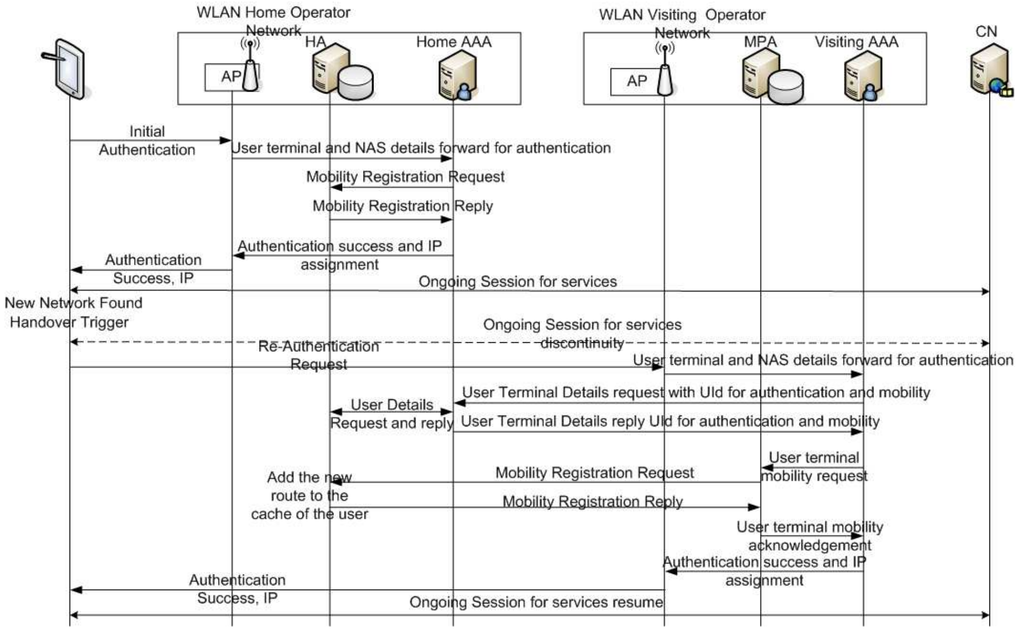

WLAN Home Operator Network
AP
HA
Home AAA
WLAN Visiting Operator Network
AP
MPA
Visiting AAA
CN
Initial Authentication
User terminal and NAS details forward for authentication
Mobility Registration Request
Mobility Registration Reply
Authentication success and IP assignment
Authentication Success, IP
Ongoing Session for services
New Network Found Handover Trigger
Ongoing Session for services discontinuity
Re-Authentication Request
User terminal and NAS details forward for authentication
User Terminal Details request with UId for authentication and mobility
User Details Request and reply
User Terminal Details reply UId for authentication and mobility
User terminal mobility request
Mobility Registration Request
Add the new route to the cache of the user
Mobility Registration Reply
User terminal mobility acknowledgement
Authentication success and IP assignment
Authentication Success, IP
Ongoing Session for services resume

Figure 62. Message exchange between components of architecture during handover scenario in home administrative domain

4.2.5.2. User terminal mobility in visiting administrative domain on same access technology

In this scenario a user terminal moves on same interface from one AP to another in visiting operator network. The user terminal is authenticated and registered in HA with the help of home AAA and visiting AAA servers. When user terminal identifies new AP it triggers the handover and does re-authentication procedures. Upon receiving request from new AP visiting AAA identifies user from previous registration and sends mobility registration request to new MPA with previous details. MPA does register the user terminal with HA and sends acknowledgement to visiting AAA server to complete handover procedure, the whole procedure is shown in message sequence inFigure 63.

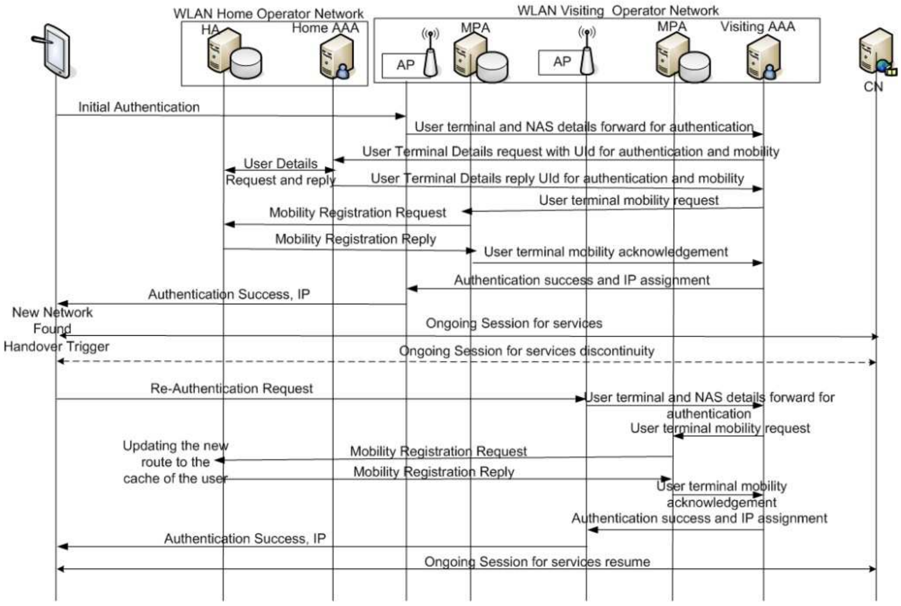

WLAN Home Operator Network
HA
Home AAA
WLAN Visiting Operator Network
AP
MPA
AP
MPA
Visiting AAA
CN
Initial Authentication
User terminal and NAS details forward for authentication
User Terminal Details request with UId for authentication and mobility
User Details
Request and reply
User Terminal Details reply UId for authentication and mobility
User terminal mobility request
Mobility Registration Request
Mobility Registration Reply
User terminal mobility acknowledgement
Authentication success and IP assignment
Authentication Success, IP
New Network
Found
Ongoing Session for services
Handover Trigger
Ongoing Session for services discontinuity
Re-Authentication Request
User terminal and NAS details forward for
authentication
User terminal mobility request
Updating the new
route to the
cache of the user
Mobility Registration Request
Mobility Registration Reply
User terminal mobility
acknowledgement
Authentication success and IP assignment
Authentication Success, IP
Ongoing Session for services resume

Figure 63. Message exchange between components of architecture during handover scenario in Visiting administrative domain

4.2.6. Enhancing the proposed solution using network selection procedure for seamless mobility.

To enhance proposed architecture we used network selection procedures combined with this architecture to use context management between the networks. Using this process access networks can create mobility context even before user terminal does initiate access to visiting network. In this process user terminal can communicates with home network using present connected network and negotiate best suitable network to connect during handover. After selecting best suitable network with the assistance of terminal, home network initiate context transfer and creating mobility context with the future visiting network. Using AAA mobility extensions proposed in this architecture AAA of home network sends a mobility registration request to visiting AAA server with UID of the terminal and mobility context details in the request. After receiving request from home AAA server, visiting AAA server collects data and sends a registration request to MPA of visiting network. After receiving request for mobility registration MPA collects user details and initiates registration request to HA of home access network. After successful registration user details of new route are cached in HA and MPA and a tunnel is established between them. When user or home AAA server does the handover triggering, HA does update route upon receiving the RU (route update) request from home AAA server. In this way maintaining multiple tunnels with future visiting networks of user and triggering with the help of home AAA server seamless mobility is achieved.

The whole message exchange sequence diagram is shown inFigure 64. During implementation of this procedure in a testbed we observed zero latency for multi homing handover and for horizontal handover we obtained small latency delay due to re-authentication procedure.

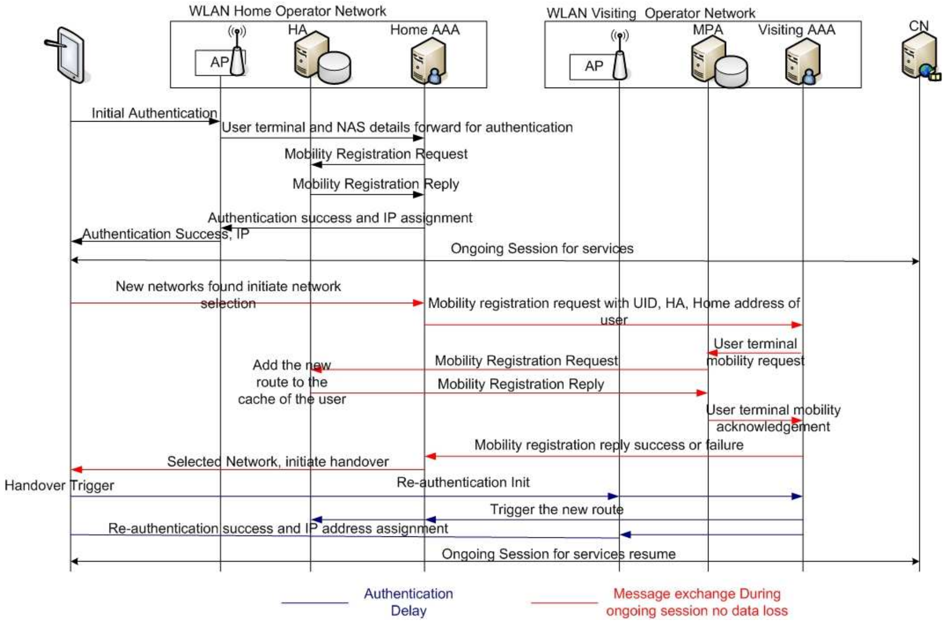

WLAN Home Operator Network
AP
HA
Home AAA
WLAN Visiting Operator Network
AP
MPA
Visiting AAA
CN
Initial Authentication
User terminal and NAS details forward for authentication
Mobility Registration Request
Mobility Registration Reply
Authentication success and IP assignment
Authentication Success, IP
Ongoing Session for services
New networks found initiate network selection
Mobility registration request with UID, HA, Home address of user
User terminal mobility request
Add the new route to the cache of the user
Mobility Registration Request
Mobility Registration Reply
User terminal mobility acknowledgement
Mobility registration reply success or failure
Selected Network, initiate handover
Handover Trigger
Re-authentication Init
Trigger the new route
Re-authentication success and IP address assignment
Ongoing Session for services resume
Authentication Delay
Message exchange During ongoing session no data loss

Figure 64. Enhanced architecture using network selection procedures for seamless mobility

4.2.7. New PMIP and AAA mobility extension development and Testbed setup

4.2.7.1. PMIP and AAA software architecture

To implement proposed architecture we developed AAA server and PMIP in house using existing open source software. We have developed software architecture to implement mobility extensions for AAA server. In this architecture AAA server can receive a request from NAS or from another AAA server. From NAS it can receive authentication request and from AAA server it can receive mobility user detail request. Upon receiving mobility registration request, extensions model respond with the reply of user details. Software architecture of AAA as shown in Figure 65, the AAA server can send requests and reply accordingly to incoming requests with the different components. For implementing the PMIP we used dynamics mobile IP architecture and modified to our requirements. We converted FA to an MPA, modified HA and MPA to accept any requests from AAA server and sending reply accordingly. In this architecture MPA can perform registration requests to HA upon request from AAA server and sends acknowledgement as success or failure. New packet formats and codes are added in MPA and HA to implement the proposed architecture.

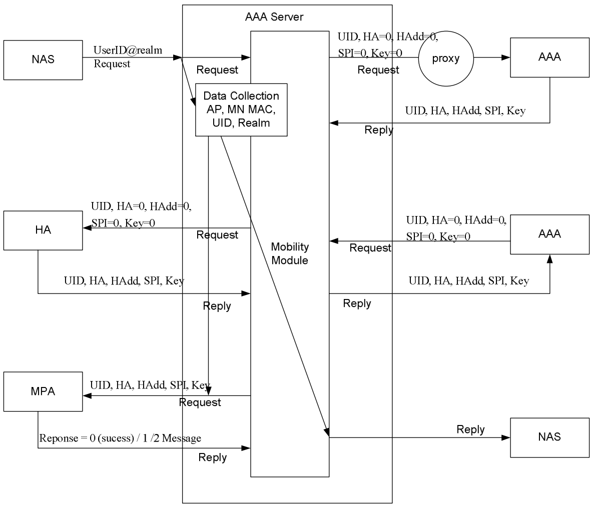


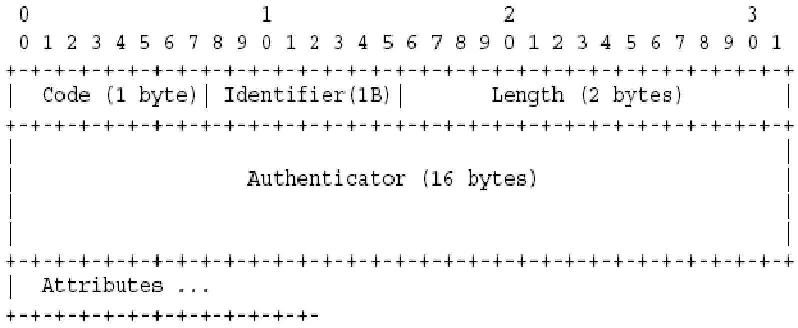
Figure 65. AAA server software architecture with new mobility extension module

4.2.7.2. *AAA Mobility extension and PMIP packet formats*

We have developed new AAA mobility extensions and new codes and packet formats for developing and demonstrating the capabilities of new mechanisms proposed in this architecture. The AAA server builds Mobility User Detail Request message from Access Request or EAP Request from the NAS or AP. Remark that intermediate AAA servers just pass through this step, adding Proxy Attribute and forwarding the Request.

AAA Mobility User detail Request format:

Note: the codes and the attributes in this document are taken as reference these can be changed according to the IANA consideration; in this case we used available values for developing the prototype, we can change this values if there are any issues.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Code (1 byte)| Identifier(1B)|       Length (2 bytes)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                    Authenticator (16 bytes)                   |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

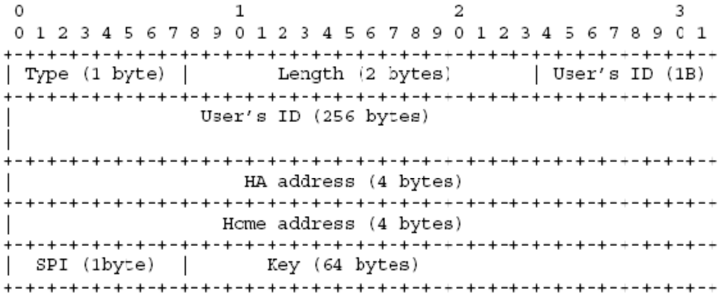
Code: (1 byte) Mobility_User_Detail_Request = 60.

Identifier: (1 byte) number to match the Request/Reply.

Length: (2 bytes) length of the message, including Code, Identifier, Length, Authenticator, Attributes. In the case that there is only mobility attribute, length = 350

Authenticator: The Authenticator field is 16 bytes. The most significant octet is transmitted first. This value is used to authenticate the reply from the RADIUS server, and is used in the password hiding algorithm.

Attributes: Mobility Attribute:



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--
| Type (1 byte) |        Length (2 bytes)       | User’s ID (1B)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--
|                 User’s ID (256 bytes)
|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--
|                     HA address (4 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--
|                   Hcme address (4 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--
|  SPI (1byte)  |       Key (64 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--
```

Type = (1 byte) Mobility_Request_Attribute = 193.

Length (2 bytes) = Length of the message = 332.

User’s ID: (256 bytes) extracted from the name of the user (ex: userID@realm).

HA address: (4 bytes) Home Agent’s IP address, filled with Zeros.

Home Address: (4 bytes) Mobile Node’s Home Address, filled with Zeros.

SPI: 1 byte, filled with Zeros.

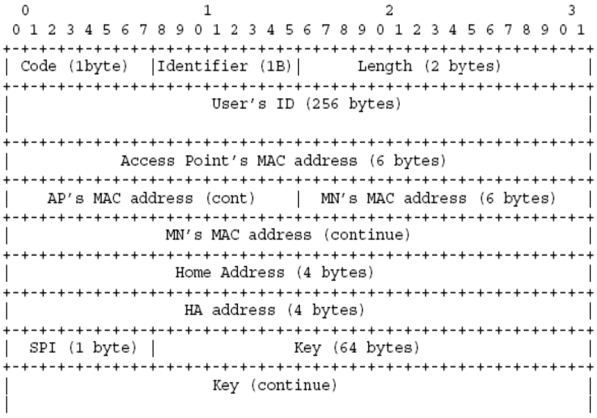
Key: (64 bytes) public key of the HA, filled with Zeros.

The AAAH will reply with a Mobility Response.

HA/MPA consultation

If AAA home server receives Mobility user detail request from a visiting server, the AAAH sends message to HA to fill the information required in the Mobility Request Attribute (fields that are filled with Zeros). Remark that the AAAH sends the HA Consultation message only by being triggered by the Mobility user detail Request; the Access Request forces the AAAH to deregister the MN.

H1: Create a message from AAAH to the HA demanding for the necessary information:



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Code (1byte)  |Identifier (1B)|      Length (2 bytes)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      User’s ID (256 bytes)                    |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Access Point’s MAC address (6 bytes)                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    AP’s MAC address (cont)    |  MN’s MAC address (6 bytes)   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                MN’s MAC address (continue)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Home Address (4 bytes)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  HA address (4 bytes)                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  SPI (1 byte) |               Key (64 bytes)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Key (continue)                           |
|                                                               |
```

Code (1 byte) = HA_Consultation_Request = 63.

Identifier: (1 byte) number to match Request/Response.

Length (2 bytes) = total length of the message = 343

AP and MN's MAC address: These fields are practically used in the message from AAA to MPA. In the message from AAA to HA, these fields are filled with Zeros, and the HA just ignores it. But these fields SHOULD appear in the HA Consultation Message to identify the format of messages AAA-HA and AAA-MPA. It is very useful since the HA and MPA in the same network are usually installed in the same server. This identification simplifies the treatment of message in the HA/MPA server.

Other fields are copied from the Mobility Attribute of the authentication request.

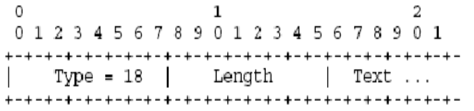
- H2: HA looks for the required information in its database, save the AP and MAC address fields. If the information can't be found (this may be due to the modification of the administrator), HA will pass this phase, so that the message will be left Zeros. That allows the AAAH to detect the failure.

- H3: HA sends back the reply to the AAA after filling the request's required fields and setting Code = HA_Consultation_Response = 64.

- H4: The AAAH replies the visiting AAA with a Mobility user detail Response, which is either an Accept or Reject message. The format of these messages is as same as the request, with different code and attributes:

If the message from HA is not filled with Zeros (successful verification), the AAAH reply to the AAAF with Mobility Accept message which is copied from the Mobility Request whose the Attributes filled by the data retrieved from HA. The Code field for this message is: Code = Mobility_Accept = 61.

If the data from HA is filled with Zeros, the AAAH MUST reply the visiting AAA with a Mobility user detail Reject message, with Code = Mobility user Reject = 62. The Mobility Reject message doesn't contain the Mobility_Attribute, and may include Reply-Massage Attribute which contains the error message shown to the user [82]:



```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|     Type = 18 |    Length     |  Text ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Type: 18 for Reply-Message.

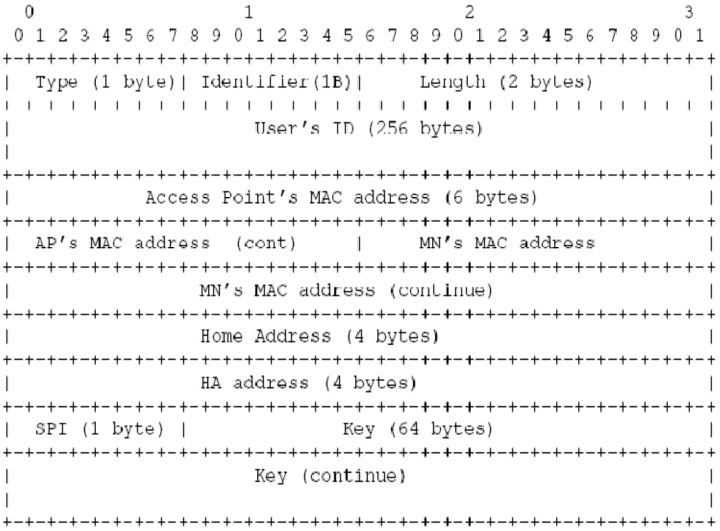
Length: length of the attribute, including Type and Length field.

Text: The Text field is one or more octets, and its contents are implementation dependent. It is intended to be human readable, and MUST NOT affect operation of the protocol. If the registration failed, this field is filled with the message extracted from the MPA Mobility Registration Reply.

Mobility Registration

After receiving the Mobility Accept message, the visiting AAA makes MPA handle the Mobility Registration procedure. The MPA exchanges messages with HA and DHCP server, then informs visiting AAA about the result (success or failure). The Mobility registration Reject causes the AAAF to send the Reject message to the NAS and terminate the whole procedure.

- MR1: Visiting AAA sends a MPA Mobility Registration Request message to MPA: the format is as same as HA Consultation message:



```
  0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Type (1 byte)| Identifier(1B)|     Length (2 bytes)          |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|                       User's ID (256 bytes)                   |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Access Point's MAC address (6 bytes)               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  AP's MAC address  (cont)     |     MN's MAC address          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 MN's MAC address (continue)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Home Address (4 bytes)                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 HA address (4 bytes)                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  SPI (1 byte) |              Key (64 bytes)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Key (continue)                          |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type (1 byte) = MPA_Mobility_Registration_Request = 65.

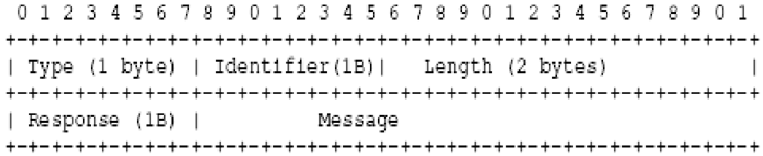
Identifier: (1 byte) number to match Request/Response.

Length (2 bytes) = total length of the message = 343.

Other fields save AP and MN's MAC address are copied from the Mobility Attributes of the Registration Response.

- MR6: MPA Mobility Registration Reply to visiting AAA:

The MPA sends back the reply to the AAA after successful communication with the DHCP server, or if it detects any error (registration unsuccessful, DHCP server refusal to register the Mobile Node, or requests cannot reach the destination). In this latter the MPA sends a reject message to the AAA server (reply with response = 1 or 2).



```
  0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type (1 byte) | Identifier(1B)|   Length (2 bytes)            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Response (1B) |          Message
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type = MPA_Mobility_Registration_Reply = 66

Response = 0 if successful, = 1 if unsuccessful with message, = 2 if unsuccessful without message.

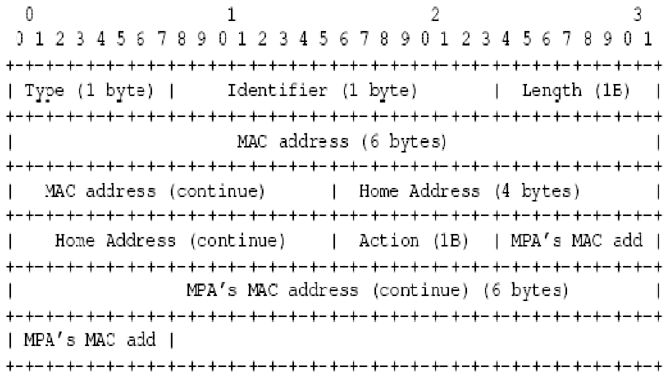
In the unsuccessful case (Response != 0), AAA will sends an Access_Reject message to the NAS. Otherwise, if the Response Code = 1, the text in the Message field can be used in the Reply-Message Attribute in the Mobility Registration Reject message.

- MR2: Registration

For the convenience of use of Client Mobile (Mobile IPv4) and Proxy Mobile IP simultaneously, the MPA and HA should use the Mobility Registration Request as specified as in RFC3344.

HA reply with Mobility Registration Reply, formatted as specified in RFC3344.

MR4: MPA sends DHCP Mobility Registration Request to DHCP server:



```
  0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type (1 byte) |     Identifier (1 byte)       |  Length (1B)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     MAC address (6 bytes)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   MAC address (continue)      |  Home Address (4 bytes)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Home Address (continue)    |  Action (1B)  | MPA's MAC add |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               MPA's MAC address (continue) (6 bytes)          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| MPA's MAC add |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type = DHCP_Mobility_Registration = 67

Identifier: match Request/Response

Length = 21: length of the message, including the Type and Identifier fields

MAC address: MN's MAC address

Home Address = MN's Home Address.

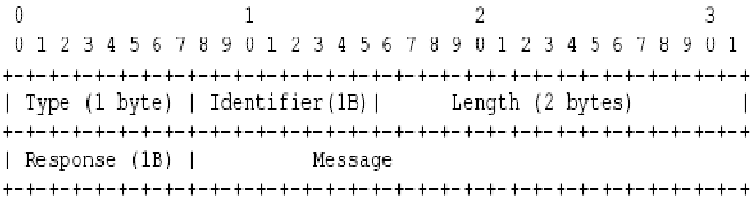
Action: (1 byte) = 0 - binding update: the DHCP server updates its configuration file with the MN's new entry:

MN's MAC address --- MN's IP address --- Default Gateway = MPA's MAC address

If Action = 1 - remove entry: cause the DHCP server to remove the MN's entry in its configuration file. This action is used in the Registration Revocation Procedure. As receiving the message from the MPA, the DHCP server updates its configuration with the information supplied by the MPA. Since then, as soon as the DHCP server receives the (Binding) DHCPDSICOVER message from the MN, it will exchange the messages with the MN granting the MN keep its Home Address; also indicates the MPA as MN's default gateway.

MR5: DHCP Mobility Registration Reply to MPA

The message is formatted as same as the reply from MPA to AAA



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type (1 byte) | Identifier(1B)|      Length (2 bytes)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Response (1B) |          Message
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type = DHCP_Mobility_Registration_Reply = 68

Length = length of the message including the Type and Identifier fields

Response Code = 0: accept, = 1 reject with message, = 2 reject without message.

If the response Code is other than 0, the MPA MUST response with the AAA with MPA Mobility Registration Reply whose Response and Message fields copied from DHCP Mobility Registration Reply message.

Message: this message will be used in the response from MPA to AAA.

4.2.8. Testbed Setup

This section describes testbed setup for implementing solutions proposed in this architecture. As mentioned earlier we have developed mobility extensions for AAA server using Freeradius [72], and PMIP using parts of Dynamics mobile IP [73] with our implementation. The proposed testbed composed of 3GPP, WLAN and WIMAX Networks. We used Infinet's preWIMAX equipment, operating at the frequency of 5.4 GHZ for WIMAX network, WLAN access consists of Linksys WRT54 and Cisco Aironet AP350. The 3GPP network used in this case is EDGE network operated by the French network operator Bouyges Telecom courtesy of MVNO Transatel. The user terminal used in the testbed is DELL Latitude410 using Centrino for wireless with option GT 7.2 ready MAX data card for 3GPP access. Most of our testing for different scenario we have used WIMAX and WLAN due to complexity of EDGE network as we have limited control of the production network provided by MVNO Transatel for us. To validate the solution we used basic testing like vertical handover where the client is equipped with multiple interfaces to validate the solution for multi homing scenarios. As we mentioned earlier horizontal handover is limited for EDGE in our case because of the control of the access network.

The implemented scenario is shown in Figure 66. We have deployed a VPN with cellular network where authentication and data is routed through the cellular network to local testbed. The user terminal is configured with AT commands using PAP for authentication. When user terminal dials for connection, authentication information of user terminal is routed through GGSN to the local authentication in the testbed, the modified AAA server does the authentication and assigns the address using IP pool mechanism, and in parallel mobility context is created for MPA and HA using AAA server.

We have deployed EAP authentication mechanism for authentication in WLAN and WIMAX networks. A user terminal tries to connect access networks using WPA supplicant [20], it is configured with user id with NAI and security mechanisms essential for EAP TLS mechanisms. Once the authentication is initiated in access networks, APs and BS sends authentication request to AAA servers, and AAA initiates authentication and mobility context for user terminal. A GUI is developed on terminal to maintain interfaces and control access management along different access networks.

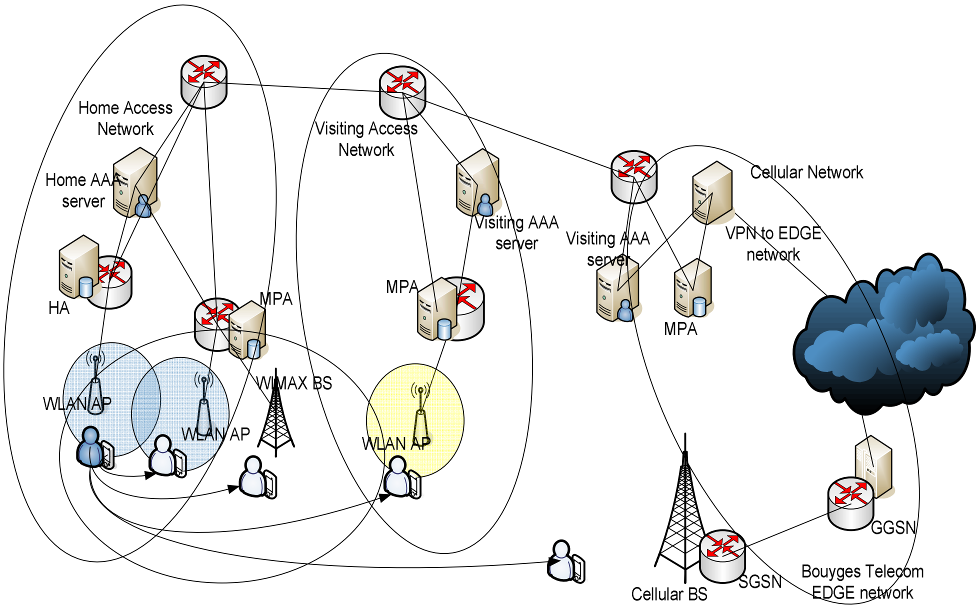


Figure 66 Testbed setup using WLAN, WIMAX and 3G networks

4.2.9. Results

As mentioned in architecture the AAA server does authentication and mobility in parallel when there is a request from the user terminal in testbed. Using this testbed we have achieved mobility of user with low latency and seamless mobility in some scenarios. Multi homing, horizontal handover and roaming is performed efficiently using this mechanism. Various scenarios of mobility as mentioned in section 4.2.3 has been tested using this testbed. Deployment and extending to the new access networks and operator is very efficient as the modifications are made at network side without any client conscious. The modifications on the network side can be made with additional patches with existing deployments. For testing purposes we have used experimental codes and attribute value pairs these can be extended to the vendor specific or using IANA status can be standardized.

We have observed an overall latency of the user terminal involved during roaming from one network to another on the same technology is around 2.4 sec for WLAN, 3.6 seconds for WIMAX, and 16 seconds for 3G networks, due to re-authentication and mobility management. In 3G networks we have observed high latency due to delay of routing messages from bouyges telecom network to our testbed. For multi homing scenario we observed latency of 18 milliseconds as we have implemented multiple interface scenarios, where a user terminal connects to multiple networks and the management of the mobility is performed by triggering route update message in HA of the user terminal. In the next paragraph we have attached a log of our radius servers in home and visiting networks where the whole procedure is depicted. For more details about logs, ethereal results refer to [83].

4.2.10. Comparisons with existing mobility models and issues of IPv6 migration

4.2.10.1. Comparison with existing mobility models

In this section different mobility protocols are compared with the available results and support for access networks with experimental results and simulation results. As we mentioned in last section we have built testbed to perform mobility in different interworking scenarios of mobility using mobility protocols. We take the following result of CMIP, HMIP and PMIP from the testbed, and the result of HAWAII and Cellular IP from other sources [84]. The Table 7 shows the different performance results for mobility protocols.

Protocols	Support for		Handover latency		Access Networks Support	Security
	Macro mobility	Micro mobility	Marco mobility	Micro mobility		
CMIP	++	--	700ms *	Non	WLAN/ WIMAX	+
HMIP	-	++	No	138ms *	WLAN/WIMAX	-
HAWAII	-	++	No	150ms *	WLAN/WIMAX	-
Cellular IP	-	+	No	300ms *	WLAN/WIMAX/Cellular Mobile Network	+
PMIP	++	++	133ms *	70ms ***	WLAN/WIMAX/Cellular Mobile Network	++

Legend: ++ Strong advantage; + Advantage; - Drawback; -- Strong drawback; * not include network selection and authentication, ** include authentication and manual network selection latency, *** include re-authentication

Table 7. Comparisons of mobility protocols with PMIP

In the test for CMIP and HMIP, we take the result from mobility registration procedure only. Macro-mobility handoff time is counted from moment that MN starts to the end of the handoff; and micro-mobility handoff time is counted from the moment that we switch network connection (changing access point). In fact, using manual switch is little different from real-time test in which the MN starts handoff if it moves out of the first access point's cover, since in the later case's handoff time depends largely on network scanning and selecting software used in the MN. We can observe that the CMIP has very high macro-mobility latency, which dues to Agent Discovery phase. We admit that the testbed is so simple as compared to the architecture implemented HAWAII and Cellular IP that the different networks are adjacent, and therefore cannot have a proper comparison among these protocols. The test is purely on latency issue, we don't count on packet loss and robustness. However, the result is persuading enough to prove the advantage of PMIP.

Proxy Mobile IP is advantageous over other mobility protocols over security, since the information is exchanged among the network entities with authenticated mechanism. More precisely, the advantage of PMIP over other protocols comes from the fact that the information exchanged in registration procedure can be generated for each session, i.e., HA can generate necessary information used for each registration session. Hence, outside AAA authentication, no key is actually stored for mobility registration.

The proposed mechanism for mobility management in this paper is compatible and interoperable with the existing converging networks. We have studied different interworking methods to implement our solution for completing the seamless converging puzzle at the mobility management layer. We interrogated different interworking mechanisms such as Seamless Converged Communications Across Networks (SCCAN), Unlicensed Mobile Access (UMA), Interworking- Wireless LAN (I-WLAN), Media Independent Handover (MIH) IEEE 802.21. The proposed solution can be adapted in these mechanisms to provide seamless services at the mobility layer.

4.2.10.2. Issues of IPv6 migrations

Due to low IP address space available for ever increasing terminals there is a need of IPv6 in the near future to deliver the services. NETLMM is an IETF working group working in PMIPv6 [85] [86], Specification of PMIPv6 is still in the infancy stage, there are several issues which has to be addressed to obtain the mobility solution. Issues of Mobile IPv6 and PMIPv6 interactions, AAA support for PMIP, MPA discovery in the access networks, handover and route optimizations, Path Management and Failure Detection, Inter access handover support and multi homing scenario handover are still open in the WG. Using AAA mobility extensions and PMIPv6 supporting AAA extensions as proposed in the architecture, issues mentioned above are solved. As part of our future work we are developing dual stack PMIPv4 and PMIPv6 for mobility support in heterogeneous networks.

4.3. Summary

Post handover techniques are intended to reduce latency during roaming and handover in heterogeneous networks. As a part of this we have proposed security authentication and mobility management to optimize handover and roaming. Extending existing infrastructure such as AAA in this case is more efficient than proposing new protocols and infrastructure. As a part of it security and mobility extensions are proposed. Using the security mechanisms we estimated the latency obtained in this method is far less than any conventional methods available in the literature. The authentication keying material created dynamically, by this way the theft presentational and security vulnerabilities are reduced. The mechanisms presented are applicable to WLAN, WIMAX and cellular networks and utilizing with RII architecture the solution provides the flexibility to operate in any interworking scenarios of roaming and handover.

Proxy Mobile IP is a development of Mobile IP, where the registration is processed by the network entities. Hence, the Mobile Node does not require a Mobile IP stack to roam over the network without losing its IP address, so this can be applied to unchanged devices. Using this proposed mechanism, authentication and mobility management of users during the access is performed in parallel; in this way, latency during the authentication and re-authentication is reduced. In this mechanism, using context management the control of users can be maintained according to the access networks. Fast and seamless handover is achieved in various deployment and mobility scenarios using these mechanisms. Extending and upgrading existing networks can be performed efficiently, as no new hardware is added to the existing architectures. Multi homing scenarios, different interworking architectures of WLAN, WIMAX and 3G are addressed using the proposed mechanisms.

Chapter 5. Pre handover techniques for seamless roaming during handover and roaming in Heterogeneous networks

The main objective of this chapter is to propose new mechanisms to ensure seamless mobility in future telecom eco systems. In this context, the main problems that are to be solve are the seamless selection and association to a network at initialization, the user movement detection and communication degradation, the seamless discovery and selection of alternative network and finally the seamless handover to the an alternative network to support the user seamless service delivery during mobility. Mechanisms which are involved in the process of roaming and handover are Network Selection (NS), handover management (HO) security management (SC), mobility management (MM), Quality of service (QoS), presence management (PM). Issues of Seamless Secured authentication and secured roaming are the issues still to be resolved. Even using high optimized techniques during roaming cannot ensure seamless mobility during roaming. We propose new techniques where the mobile node does create the roaming and handover context with the help of access networks before handover initiation; this procedure is called pre handover mechanisms. These pre handover techniques create context for every single aspect involving roaming between access networks. In this process we have developed a unified signalling protocol, which is used to transport different context created between users and access networks and between access networks.

5.1. Introduction

The current network selection, security management, handover procedures, mobility management procedures are limited and provide seamless roaming mechanisms with little efficiency operating passively with very limited resources. The proposed mechanisms don't have any clarifications on issues of QoS, SLAs using for network selection which play an important role during authentication and service adaptation for data after network selection procedures [87]. The issues of user mobile node mobility are not discussed efficiently in the previously proposed network selections procedure. There is a need for new network selection procedures and security mechanisms to adapt for heterogeneous networks using WLAN, WIMAX and 3G networks, where a user moves across these networks using services efficiently. From the network operator's perspective, network selection and low latency handovers for different services adapted for the users is the biggest challenge, as it involves the resource management, proper network planning involved existing networks and new technologies adding onto existing one. Involvement of multiple operator networks in the areas of operation complicates NS and SC for heterogeneous networks. The ultimate goal of providing low cost efficient services for users is compromised without network selection and security procedures. In this process there is a need for mechanisms where the user mobility and access mechanisms has to be controlled from the network side as the amount of resources available at operator network are far superior than in the mobile terminals and also the knowledge of operation involves high technical expertise which most subscribers lack.. Taking all the above mentioned problems into consideration, we are proposing network selection and security procedures for authentication involved mobile terminal with the network assistance. Using network assistance, the several issues such as coverage of multiple access technologies can be determined precisely, future location of mobile terminal before disconnecting the current connected network, allocation of resources even before mobile terminal roam/handover to future network, SLAs with visiting networks as well as current user profiles.

In this chapter we are proposing enhanced as well as novel mechanisms at various levels of access networks, to develop a network assisted or aided network selection, security context management, handover management and mobility management i.e. user terminal during mobility in heterogeneous networks will be assisted by the networks to achieve in an efficient manner their handover so that it is transparent to the user. In this process we have identified two scenarios; one is user accessing initially, and the other is when the user is performing handover or roaming. In the initial method, with the available profile of access network the mobile terminal performs network selection and authentications, the profiles are update regularly by access network. In the second, process mobile terminal is assisted by access network i.e.. The access network does the network selection and security management, ask mobile terminal to trigger handover on the selected network with the context transfer from home network. The mobile terminal communicates regularly with home access network providing information of required bandwidth, current location from GPS, battery status, available interfaces and scanned networks with corresponding SNR for network selection and keying information for authentications. We have defined two mechanisms for authentication and re-authentication. During initial authentication using available security information from the user profiles provided by the home network, mobile terminal does the authentication after successful network selection. In the other process the mobile terminal does the context transfer with the home network for security information for re-authentication which are derived from the network selection of the future network. The home network identifies the future visiting network for the mobile terminal and does the keying procedure and transfers them to visiting network and mobile terminal. With the new context information mobile terminal does the fast re authentication with the visiting network without routing authentication information to home network, in this way, the latency for authentication is reduced and performed efficiently.

Handover management procedure involved allocation of resources in access networks and controlling different mechanisms to ensure seamless mobility. In this process the HO mechanisms initiate and control NS, SC, MM and QoS. When the mobile terminal tries to roam or to handover, it sends a HO initiate request to access networks, the home access network takes over the request and initiates other procedures for seamless roaming. The other procedures involved are mobility management. When the mobile terminal moves from one network to another, the session is lost as the IP connectivity is lost. The mobility management ensures that the session is not lost during the handover. Even though existing mechanisms ensure mobility, the latency during this procedure is large. In our proposed solution mobility context is created before the handover in access network, the entities which are already deployed are modified, we used Client based mobility protocol and Proxy based mobility protocol.

In this process we have identified different mechanisms to assist for context transfers from access networks and mobile terminal. The most suitable is EAP coupled with AAA as a solution. EAP is generally widely used in wireless networks, and due to its pass through behavior for accessing networks at layer 2, no modifications is required at access points level in access networks. In this paper we are proposing to extend EAP with a new method called handover with NS, SC etc… as subtypes to provide communication channel between access network and user terminal. This new method collects data available in the user terminal including available networks in the vicinity and sends them to the network using the proposed extension of EAP to be assisted in the mobility. While in the case of cellular networks there is no need for context transfer mechanisms as this is been achieved using special dedicated GTP sessions by access networks and mobile terminals.

On the other hand, the operator access networks are widely supported by AAA to provide authentication and access support such as billing, profile maintenance of users etc.. The AAA server can be modified by adding new modules with the existing support to provide seamless mobility support. In our architecture we propose to add new modules such as network selection, security, mobility, QoS and presence in AAA to support handover management. These modules can be used as add-ons so that the operators can use according to their convenience. Also using these modules we can provide context management for access networks to provision the information of users for low latency handover. In network selection procedure the home AAA server of mobile terminal receives a request through EAP NS, HO, AAA provides the support for its request and chooses best available network by negotiating with the future visiting network of mobile terminal.

The proposed mechanism also evaluates at each time the position of mobile terminal and its mobility pattern to estimate the future location of user at any given instance. We propose to use a GIS (Geographic Information Server) system to identify the available networks in the vicinity of the user terminal. Based on the information in the context, the mobility pattern and a set of information provided by the user terminal and future visiting networks, the network selection mechanisms on access network AAA server determine the best target network for handover for mobile terminal.

5.2. Network Selection Management

5.2.1. Location identification

The User Location identification aims to locate the user terminal in the ecosystem. If the user is connected to an UMTS network, the Cell ID and Observed time difference can be used. The cell ID based positioning method is the most trivial indication of the user location, and does not require specific functionality in the UMTS network. It is however not very accurate, because the average size of radio cells in UMTS can vary from 800 meters radius in dense urban areas to about 6 kilometres in rural areas. With additional measurements it is sometimes possible to achieve a higher accuracy [87]. The Observed Time Difference of Arrival (OTDOA) method uses the observed time differences between the mobile terminal and nearest base stations. The measurements of different base stations are used to triangulate the location. The accuracy of the OTDOA positioning method varies depending on the actual location of the terminal within the cell. Especially if a terminal is close to one of the base stations, it may be difficult to "hear" the two other base stations needed for the triangulation. The accuracy is approximately between 50 and 200 meters. The GPS method requires the mobile terminal is equipped with a GPS receiver. The accuracy is approximately of 50 meters in a dense urban environment and a few meters in an open environment. Determining the location of an end-user in a WLAN network can be achieved using a triangulation method similar to UMTS triangulation method described above. A common method is based on signal strengths to multiple (more than three) Access Points, which can be obtained from both the AP itself and the client device.

5.2.2. GIS model

A Geographic Information Server maintains information about the coverage of operators' networks. The geographical area of the location is divided into different cells covering the operators' networks range. In this process the location of BS (Base Station) or AP and their ranges are mapped to these cells. This server can therefore identify at any given time the available access networks at a particular location. The GIS is also capable of predicting the location of the mobile terminal during mobility. For that it is necessary to provide it with information such as user terminal mobility, speed of the terminal, present location and previous locations within the stipulated time constant using Gauss-Markov model. The defined prediction model is presented in the following section.

The GIS is used whenever a mobile terminal is requesting support for network selection during mobility. The mobile terminal sends a request with the current data available from its GPS to the network. The network forwards the request to GIS server to (1) predict the future location of mobile terminals, (2) map this geographic location to available networks database in the vicinity; (3) select the available networks that conform to the selection criteria (user right, QoS, cost, etc) (4) sends a reply to the mobile terminal.

5.2.3. User Mobility Prediction Model

Several Mobility models [89] have been proposed in the literature. Among them, the Random Walk Mobility Model and the Random Waypoint Mobility Model are the two most common mobility model used by researchers. The current speed and direction of a mobile station is independent of its past speed and direction. This characteristic can generate unrealistic movements such as sudden stops and sharp turns. To fix this discrepancy, we use in this work the Gauss-Markov Mobility Model. This model is designed to adapt various levels of randomness using one tuning parameter. At a given instance the mobile terminal for a fixed interval of time 'n', the movement occurs by updating its speed and direction. The value of speed, location and direction at the n'th instance can be based on n-1st instance and equation show n below.

$$s_n = \alpha s_{n-1} + (1-\alpha)\bar{s} + \sqrt{(1-\alpha^2)}s_{x_{n-1}}$$

$$d_n = \alpha d_{n-1} + (1-\alpha)\bar{d} + \sqrt{(1-\alpha^2)}d_{x_{n-1}}$$

Where Sn and dn are the speed and direction of the mobile terminal at nth instance, α, where 0 ≤ α ≤ 1 , is the tuning parameter used to vary the randomness ; ¯s and ¯d are constants representing the mean value of speed and direction as n→∞; and sn−1 and dn−1 are random variables from a Gaussian distribution. Totally random values are obtained by setting α = 0 and linear motion is obtained by setting α = 1. Intermediate levels of randomness are obtained by varying the value of α between 0 and 1. At each time interval, the next location is calculated based on the current location, speed, and direction of movement. Specifically, at time interval n, a mobile station's position is given by the equations.

$$x_n = x_{n-1} + s_{n-1}\cos d_{n-1}$$

$$y_n = y_{n-1} + s_{n-1}\sin d_{n-1}$$

Where (xn, yn) and (xn−1, yn−1) are the x and y coordinates of the mobile station's position at the nth and n-1st time intervals, respectively, and sn−1 and dn−1 are the speed and direction of the mobile station, respectively, at the n-1st time interval.

$$x_{p_k} = x_c + \frac{x_c - x_p}{P} \times k, (0 < k < P)$$

$$y_{p_k} = y_c + \frac{y_c - y_p}{P} \times k, (0 < k < P)$$

The location prediction is used to determine the geographical location of some mobile station at a particular instant of time tp. These predictions are performed based on two times updates location information of the mobile stations. From its recent history (i.e. from recent updates), the mobile station can calculate an expected location for any particular instant. Let the previous location of the mobile station at time of checking tp be (xp, yp). And the current location of the mobile station at time of checking tc be (xc, yc). The update period of mobile station's location information is P = tc − tp. Then, expected location (xe, ye) is given by the equations.

If the location prediction scheme did not exist, uplink request mobile in time tc < t < tc+p would use the routing decision in time tc. As we increase the location update period P, the difference between the real location and the predicted location will also become larger. Therefore, we can shorten difference between the real location and predicted location by using a linear prediction scheme. The error between real location and predicted location will decrease as the location information server divide time intervals t_c < t < tc+p more precisely.

5.2.4. Network Selection Algorithm

During the handover procedure, the user terminal needs to select the most appropriate access network of the same or a different technology. However, as the terminal is blind of the global situation in its neighborhood, we propose that in any situation the terminal collaborate with the network to be assisted in this procedure. The network selection service in the network assists the mobile terminal in its hand over ensuring it to select the best target network depending on the available bandwidth, QoS as well as the cost, for instance when the user is browsing (low bit rate) and VoIP and video on demand services (high bit rate). Once the localization of the mobile terminal evaluated and the set of networks that are operated in the vicinity of that localization, the home access network of mobile terminal performs the network selection with the help of visiting networks. The local database on the mobile terminal is stored with the required information from home network. These details contain available access networks, SLAs, roaming agreements between other operators, cost of communication for using different access technologies. At any given instance the mobile terminal can access this information for decision making. The mobile terminal has the capability to access and initiate different interfaces available such as WLAN, WIMAX and 3G to collect details of networks availability its RSS and SNR.

Initial network selection procedure involves scanning all the network interfaces available on the mobile terminal. Once the wireless interfaces are identified, interfaces are probed for available access networks in the vicinity of mobile terminal. We have identified two working scenarios for network selection procedure, one is when the mobile terminal does initial access and other is when performing handover or roaming. In the initial access the information is collected from the interfaces and previous connected networks. The current location of mobile terminal identified by GPS is provided in the extension of the EAP request to the access network.

The new extension for EAP to support the HO allows the mobile terminal to request assistance during mobility to its home network. In this method the handover method is subdivided in several methods, NS is one such sub method. On the other side the AAA is also extended so that it recognizes handover and NS as sub methods. When required, the mobile terminal sends a request to the home network, to identify access networks in its future localization. It provides the current and previous GPS locations info and available access networks at that moment. Due to pass through behavior and already existing support for EAP and AAA in wireless networks we use new extensions instead of creating new protocols for context transfer. On the cellular networks the mobile terminal uses GTP session dedicated to the mobile terminal to send the information request to the server in the access networks. When the AAA server receives the request, it communicates first with the GIS to identify the following location of the mobile terminal as well as the available networks at that location (and therefore their corresponding AAA). Then, it communicates with the other access networks AAA using radius roaming extensions [90] to retrieve information relates to the QoS in the target network, access policy and cost.

5.2.5. Network selection procedure in mobile terminal

Network selection engine in the mobile terminal is the core of the procedure, where it collects details from different entities of mobile terminal. It collects required QoS, expected cost of communication, available networks and their respective SNRs, location of mobile terminal and previous associated networks at that location and networks availability from the database provided by home operator network, SLAs and profiles. With the scanned networks and high value SNR networks are prioritized, from the previous connected networks are again prioritized with the context transferred information of networks availability from home network with the new protocols, later the networks belongs to home operators are given more priority than the visiting operator networks. These prioritized networks are sent to next procedures such as handover or authentication use. If ever the access networks are not available are out of range, the NS procedure is performed again. The flow charts are mentioned in figure 1 and 2.

Network Selection during Initial Access: In this process the mobile terminal initiates the network selection procedure, after initiation the mobile terminal starts the network scan. During the network scan the device probes the different devices available and scans the available networks. The client terminal processes the information from devices and processes the SSIDs of the networks. And the terminal initiates the location based process such as GPS, and available home network from the local database. With all the available networks gathered from different processes, policy of the user, the client selects the best suitable network. The client can initiates the NAI of the home network or depending on the selected network it can initiate the mediating network. The whole process is shown in Figure 67.

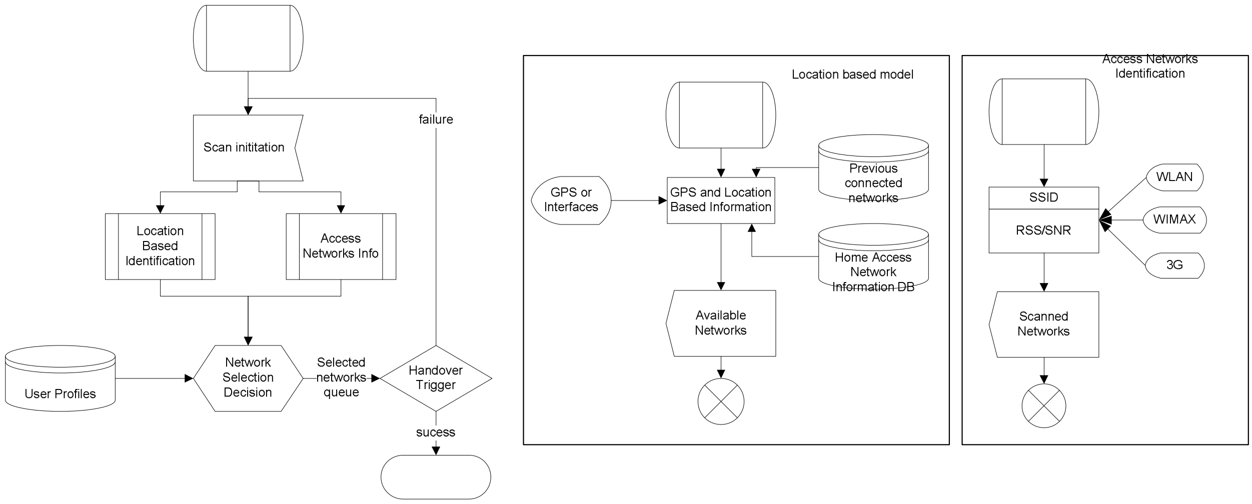


Figure 67. Network selection procedure during initial access in mobile terminal

Network Selection during Handover or Roaming: In this process the mobile terminal constantly monitors the SNR and availability of bandwidth of the connected network. When the threshold of the required SNR and bandwidth are below the required par for services, the mobile terminal initiates the network selection procedure. As in the initial process in this procedure GPS is triggered and current location between different time intervals are identified and sent to home access network through EAP extensions. Mobile terminal also probes the available network interfaces for scanned SSIDs and their respective SNRs, this information is also passed to home access network. Once the data sent is processed on the home network, after selecting best available network, home AAA server sends a response with best suitable network. The process mechanism is shown in Figure 68.

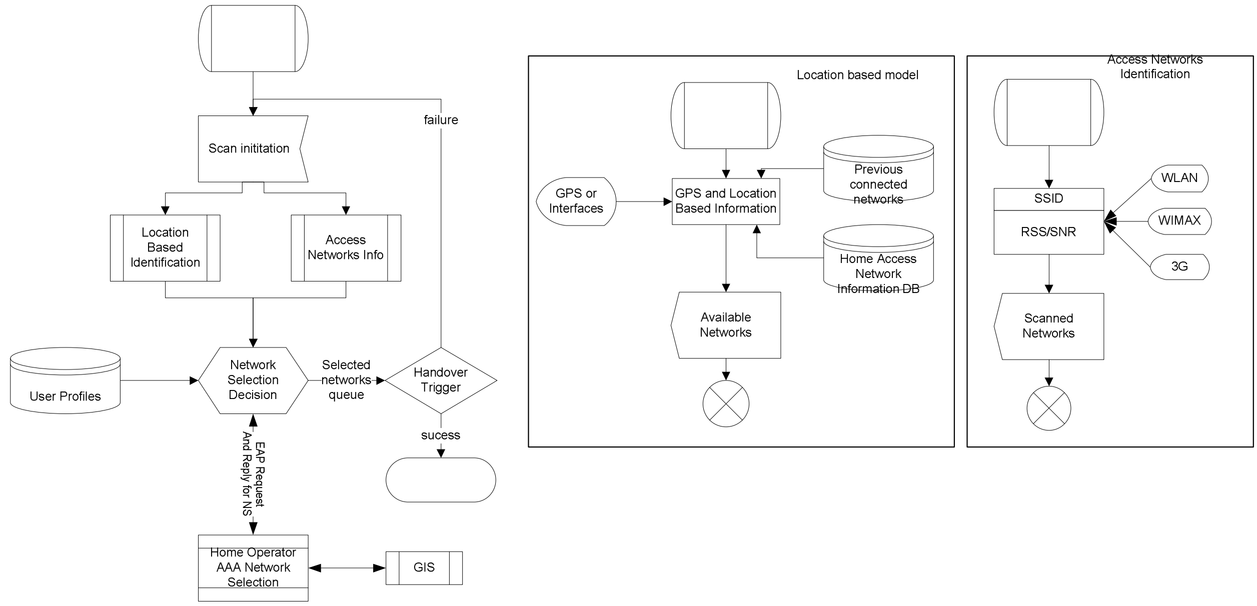

Scan inititation
failure
Location Based Identification
Access Networks Info
User Profiles
Network Selection Decision
Selected networks queue
Handover Trigger
sucess
EAP Request And Reply for NS
Home Operator AAA Network Selection
GIS
Location based model
Previous connected networks
GPS or Interfaces
GPS and Location Based Information
Home Access Network Information DB
Available Networks
Access Networks Identification
WLAN
SSID
WIMAX
RSS/SNR
3G
Scanned Networks

Figure 68. Network selection procedure during handover or roaming in mobile terminal

5.2.6. Network selection procedure in Access networks

As shown in Figure 69 the EAP NS on the client communicates with the home AAA server with the target network IDs, home AAA differentiates with the Local networks, networks which have direct SLA agreement or have with the RII mediating network. According to the type of network home AAA process the information in different manner. If the home network has an indirect SLA, through the RII server, home AAA server sends a radius NS extensions request to the RII server, RII server process the information and adds the request to the database with the stripped user ID and the access network. With the available target lists the AAA of RII sends a NS request to AAA of the visiting network. Visiting network process the available information and sends the available target ID as a reply to the RII. If ever the request fails, it sends NS failure as code value of the packet. If ever the visiting network has a direct SLA the home network communicates with the visiting network directly. In this case it sends a user without any stripped ID of the user, after checking the available resources the visiting network sends a reply with a NS extension of AAA.

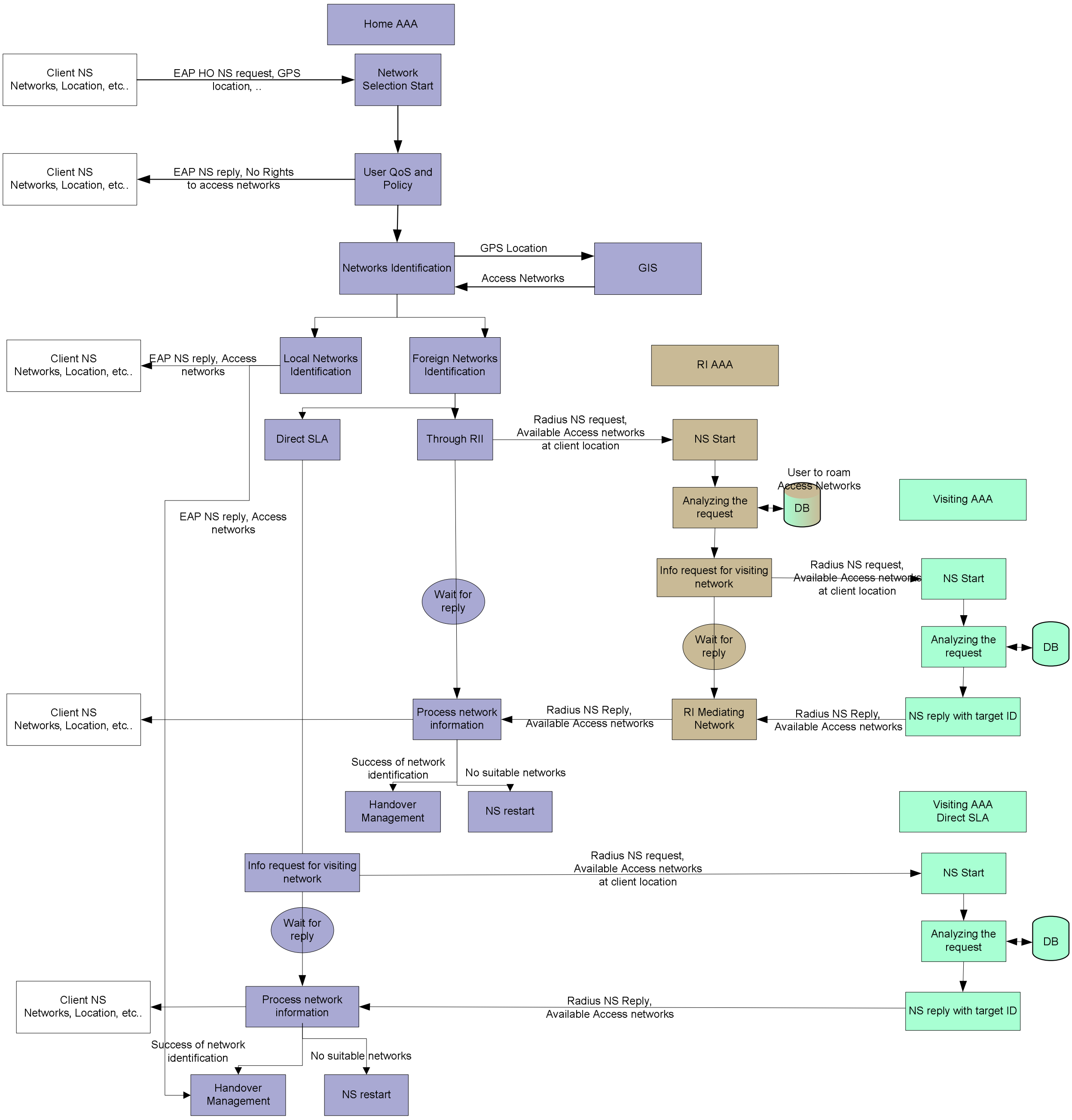

Home AAA
Client NS Networks, Location, etc..
EAP HO NS request, GPS location, ..
Network Selection Start
Client NS Networks, Location, etc..
EAP NS reply, No Rights to access networks
User QoS and Policy
Networks Identification
GPS Location
Access Networks
GIS
Client NS Networks, Location, etc..
EAP NS reply, Access networks
Local Networks Identification
Foreign Networks Identification
RI AAA
Direct SLA
Through RII
Radius NS request, Available Access networks at client location
NS Start
User to roam Access Networks
Analyzing the request
DB
Visiting AAA
EAP NS reply, Access networks
Info request for visiting network
Radius NS request, Available Access networks at client location
NS Start
Wait for reply
Wait for reply
Analyzing the request
DB
Client NS Networks, Location, etc..
Process network information
Radius NS Reply, Available Access networks
RI Mediating Network
Radius NS Reply, Available Access networks
NS reply with target ID
Success of network identification
No suitable networks
Handover Management
NS restart
Visiting AAA Direct SLA
Info request for visiting network
Radius NS request, Available Access networks at client location
NS Start
Wait for reply
Analyzing the request
DB
Client NS Networks, Location, etc..
Process network information
Radius NS Reply, Available Access networks
NS reply with target ID
Success of network identification
No suitable networks
Handover Management
NS restart

Figure 69. Network selection procedure in access networks.

5.3. Security Management

5.3.1. Security context mechanisms

The role of this process in mobile terminal is to identify the network and get authenticated or re-authenticated to the different access networks. Security mechanism can be obtained by EAP and implementing EAP methods of EAP-SIM/AKA and EAP-TLS on wireless networks and SIM or AKA based in cellular networks. On the other hand access network have a capability to authenticate the user's using these mechanisms. Whenever there is requests for authentication from the user Radius, server of the access networks uses specific EAP methods and creates the security credentials and authenticate the users. Using the network selection procedure, the home access network and mobile terminal identifies the future visiting access network. Later home network creates the re-authentication credentials like Re-id, duplicate certificates and keys according to the selected network and they are sent to the MT and to the target access network using security context transfer using radius roaming extensions. We used security context transfer to reduce latency delay during re-authentications by using context transfer of security to target network, while the MT tries to authenticate at the target network without reaching to the home network for re-authentications, by this way latency can be reduced. In this section we deal with authentication and re-authentication of the client terminal with the help of security context management and process involved in the access networks.

5.3.2. Authentication procedures in mobile terminal

5.3.2.1. During initial access:

With the access network, ID and with the specific NAI the user id is strapped. The network interface is initiated and the security mechanism on that interface is started, the client uses the strapped user ID with NAI to access with the access network security mechanisms in this case we used EAP with TLS or SIM for the authentication. After successful authentication mobility management is processed. If ever the authentication fails the network selection is processed again. Figure 70 describes the security management during initial access.

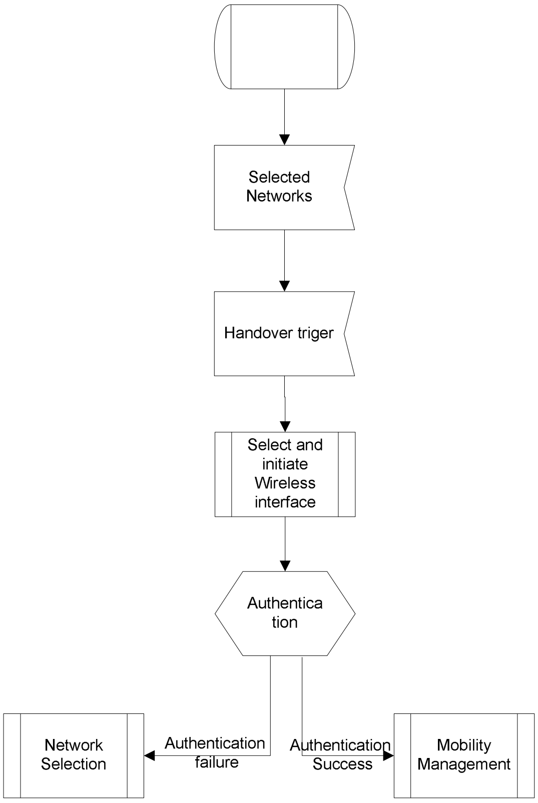


Figure 70. Security Management during initial access

5.3.2.2. SC management during handover in mobile terminal:

After the security context management is started the client terminal contacts the home network server. Home radius server provides the re-authentication ID and duplicates keys to the client. After the client receiving the security IDs and keys it informs interface security management. After handover decision the interface initiates the security authentication with the provided keys, if the re-authentication is successful it initiates the mobility management if ever the authentication fails it initiates the network selection again.

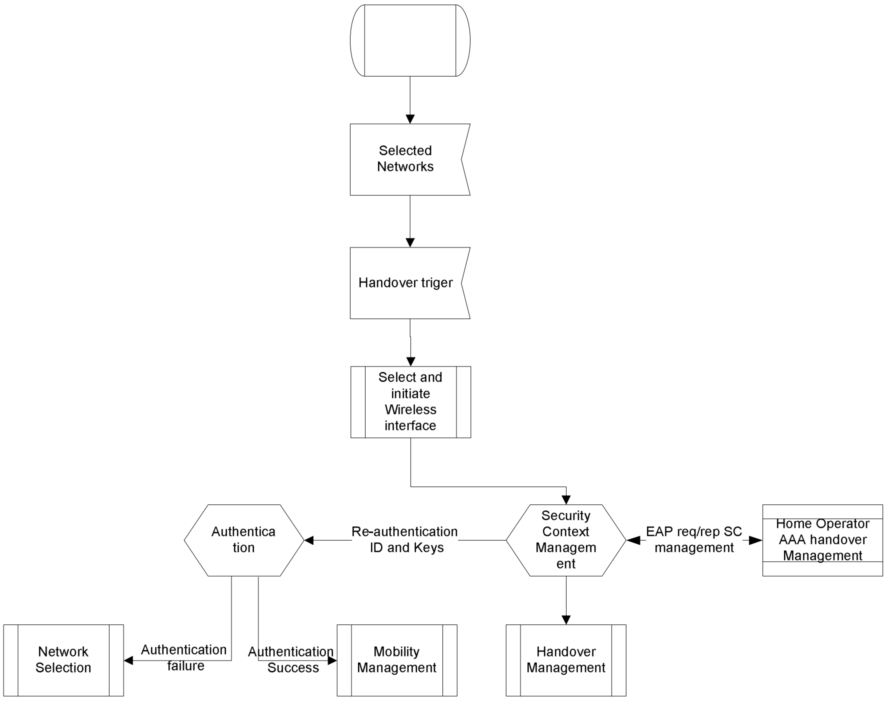

Selected Networks
Handover triger
Select and initiate Wireless interface
Authentica tion
Re-authentication ID and Keys
Security Context Managem ent
EAP req/rep SC management
Home Operator AAA handover Management
Network Selection
Authentication failure
Authentication Success
Mobility Management
Handover Management

Figure 71. Security Management during re-authentication.

5.3.3. Authentication procedures in access networks

For providing low latency during handover, access networks are proposed to use network selection procedures and keying mechanisms with context transfer is proposed. As mentioned in section 5.2, the access networks identify the future network and its capabilities, using this information access network derive keys and re-authentication id which are suitable with the future visiting networks. Once this is achieved, visiting network must have the capability of configuring in the local network for the context information dynamically and must authenticate the users directly without routing the information for authentication way back to home network of the users. Achieving this low latency at authentication level is performed during handover and roaming scenarios. Issues of SLAs are also solved as the information is passed on request and reply dynamically without any static information. Figure 72 describes the procedure involved in access networks during security context transfer.

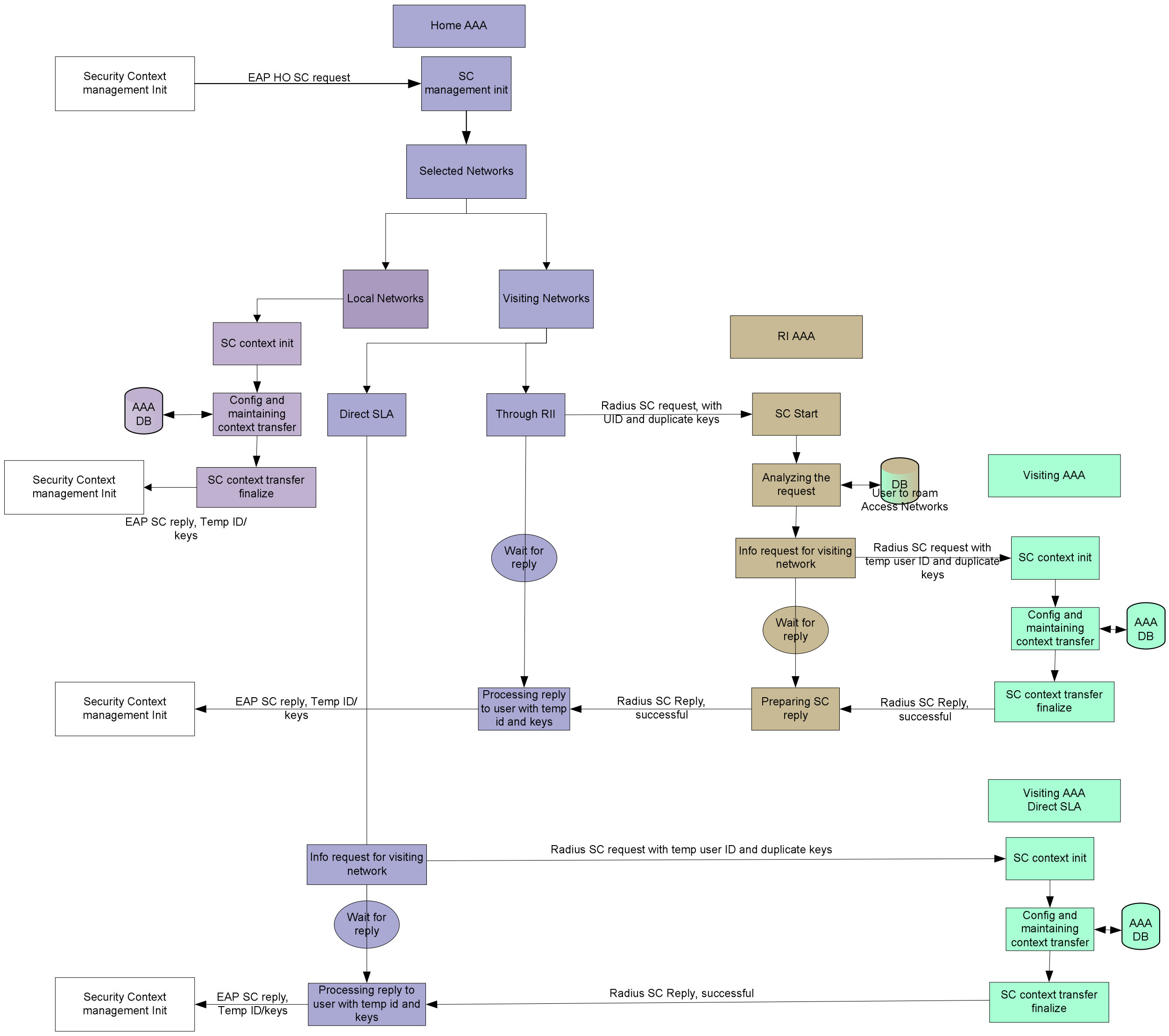

Home AAA
Security Context management Init
EAP HO SC request
SC management init
Selected Networks
Local Networks
Visiting Networks
SC context init
RI AAA
AAA DB
Config and maintaining context transfer
Direct SLA
Through RII
Radius SC request, with UID and duplicate keys
SC Start
Security Context management Init
SC context transfer finalize
Analyzing the request
DB
User to roam Access Networks
Visiting AAA
EAP SC reply, Temp ID/ keys
Wait for reply
Info request for visiting network
Radius SC request with temp user ID and duplicate keys
SC context init
Wait for reply
Config and maintaining context transfer
AAA DB
Security Context management Init
EAP SC reply, Temp ID/ keys
Processing reply to user with temp id and keys
Radius SC Reply, successful
Preparing SC reply
Radius SC Reply, successful
SC context transfer finalize
Visiting AAA Direct SLA
Info request for visiting network
Radius SC request with temp user ID and duplicate keys
SC context init
Wait for reply
Config and maintaining context transfer
AAA DB
Security Context management Init
EAP SC reply, Temp ID/keys
Processing reply to user with temp id and keys
Radius SC Reply, successful
SC context transfer finalize

Figure 72. SC management in access networks.

5.3.4. Message exchanges between different components

This section provides information on message exchange between different components of the architecture proposed in this paper. Figure 73 provides the detailed message sequence diagram. As mentioned earlier, mobile terminal does the initial network selection with the available resources and performs authentication and access the networks. Once the mobile terminal is provided with access NS procedure terminal communicates the context transfer with home access network. . During an ongoing communication, mobile terminal initiates EAP HO NS and sends a request to AP or BS, and then AP forwards the request to AAA of the access network. Checking the realm of the user with NS request, AAA server forwards the request to home AAA server of the user or process locally. When the local network has an indirect SLA with the operator, it forwards the request through RII mediating network. Once the home AAA server receives the request for NS it processes the data inside the request, checks GPS locations and scan the SSIDs. The AAA server sends a request to GIS server with the available information; GIS server does the mobility prediction of the user and maps the location and collects the available networks information and forwards to home AAA server.

After checking the available access networks belongs to local or visiting networks (direct or indirect SLA), AAA sends a radius NS request to that access networks AAA. After receiving request, visiting networks check available resources of the AP or BS and responds with available networks as a response to home network. If ever the operators doesn't have direct SLAs they use RII mediating network for network selection. Once the network selection is performed the home access networks AAA sends EAP response to mobile terminal with the available access networks suitable at current and predicted location. Once NS is performed in the access networks, they initiate authentication for the mobile terminal and visiting networks. In this process the EAP HO SC initiated by the mobile terminal which is relayed to home network. The home network does the keying and sends radius roaming extensions security request with the keying material to the future visiting network. Once the home AAA server receives reply from visiting AAA server, it sends EAP response with keys and ID to mobile terminal. Once NS, security and mobility context are initiated, mobile terminal does initiate handover, using this procedure latency for handover is reduced drastically and whole process is controlled at every single step of handover making this architecture robust and secured.

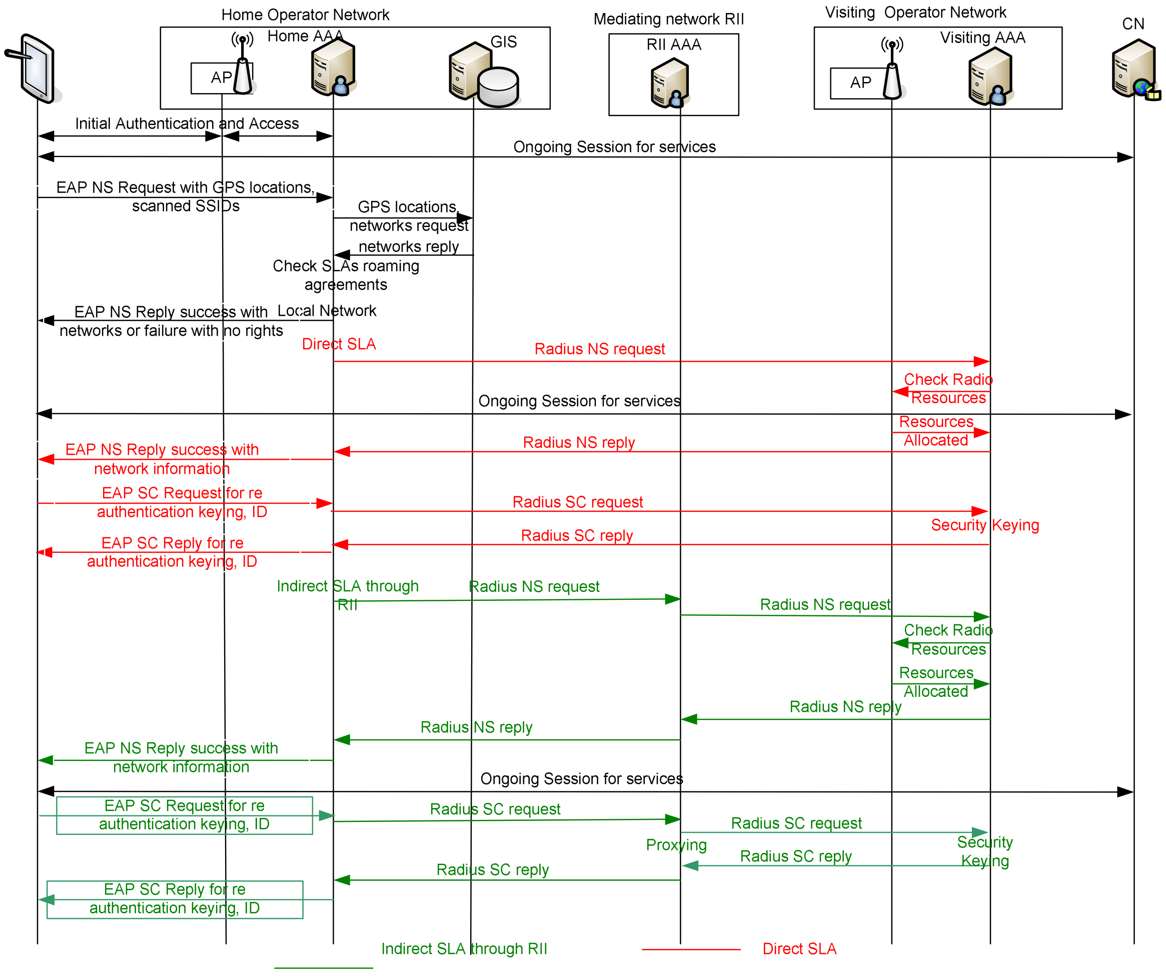

Home Operator Network
Home AAA
GIS
AP
Mediating network RII
RII AAA
Visiting Operator Network
Visiting AAA
AP
CN
Initial Authentication and Access
Ongoing Session for services
EAP NS Request with GPS locations, scanned SSIDs
GPS locations networks request
networks reply
Check SLAs roaming agreements
EAP NS Reply success with Local Network networks or failure with no rights
Direct SLA
Radius NS request
Check Radio Resources
Ongoing Session for services
Resources Allocated
EAP NS Reply success with network information
Radius NS reply
EAP SC Request for re authentication keying, ID
Radius SC request
Security Keying
EAP SC Reply for re authentication keying, ID
Radius SC reply
Indirect SLA through RII
Radius NS request
Radius NS request
Check Radio Resources
Resources Allocated
Radius NS reply
Radius NS reply
EAP NS Reply success with network information
Ongoing Session for services
EAP SC Request for re authentication keying, ID
Radius SC request
Radius SC request
Proxying
Security Keying
Radius SC reply
Radius SC reply
EAP SC Reply for re authentication keying, ID
Indirect SLA through RII
Direct SLA

Figure 73. Message sequence exchange between components using proposed mechanism

5.4. HO Management

Handover management in this architecture, initiates network selection, does the required measurements on the network interfaces for network selection. HO on the mobile terminal does the measurements and initiates the network selection and informs the access network about the selected target network from the NS process for a possible handover or roaming. On the other hand HO on the access network prepares the network for handovers and communicates with other networks. After identifying the selected target network from the home network, the home network sends the handover initiation to the HO of the mobile terminal for initiating the handover to the target network. After handover initiation messages from the home network, HO on mobile terminal initiates the security (SC) management on the mobile terminal for authentication and re-authentication on the target network. This procedure involves the decision after gathering the information from all the other procedures of security and mobility. As mentioned earlier, the mobile terminal performs two methods one at initial authentication and the other during the re-authentication.

5.4.1. HO management during initial access in mobile terminal:

After receiving the selected network from NS, the handover initiation function initiates the SC and MM and waits until all the other procedures are completed and then does the handover trigger and does the initial connection on the selected interface with the selected network, the process mechanisms is shown in Figure 74.

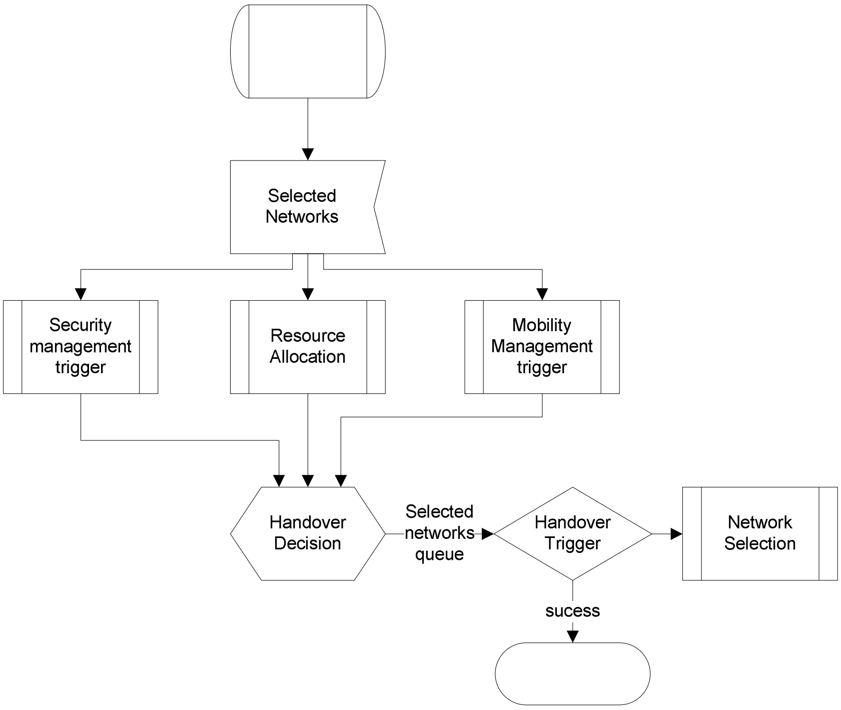


Figure 74. HO management during initial access in mobile terminal.

5.4.2. HO management during handover in mobile terminal:

With the selected network the client terminal does start the handover mechanism, the handover function calls home network for confirming the selected network to handover. After receiving the reply from the server the decision is made and triggers the handover procedure with SC and MM, the procedure involved is shown in Figure 75.

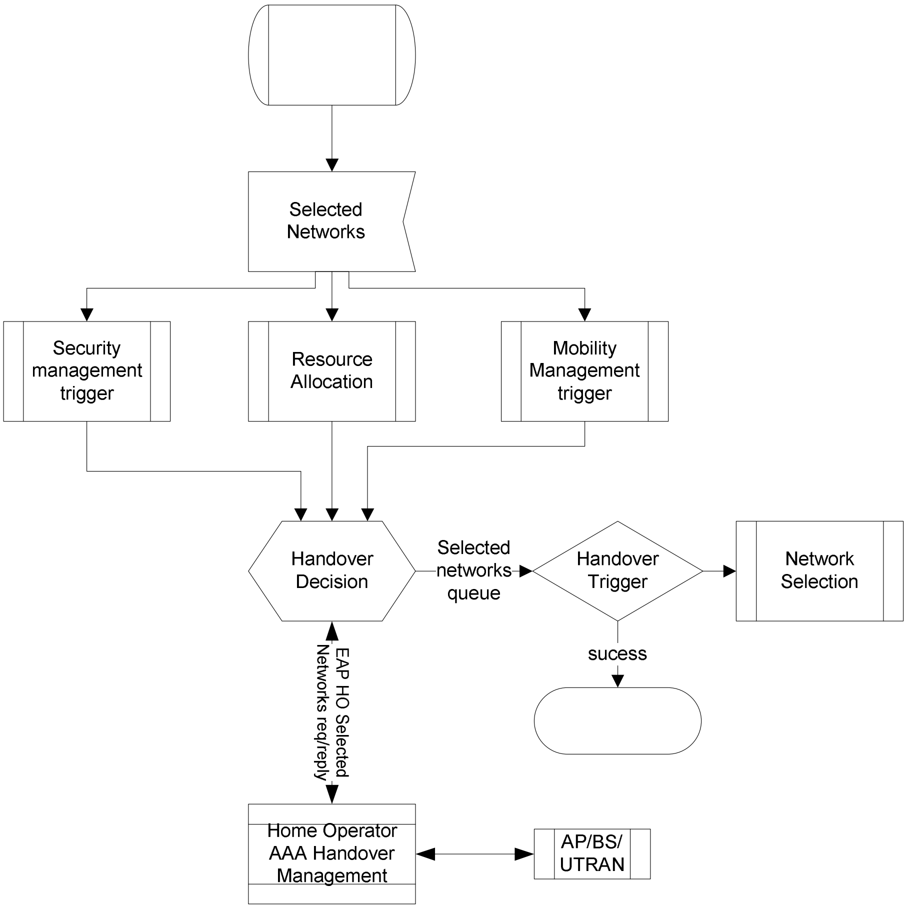


Figure 75. HO management during pre handover in mobile terminal.

5.4.3. HO management in Access networks

In this process, when the client sends the HO initiation request for the target ID, the home radius server sends the request to the visiting radius server for HO initiation. Visiting Radius checks for the available resources for that target ID and sends accept or reject as a reply to the home radius server, the whole process mechanism is shown in Figure 76.

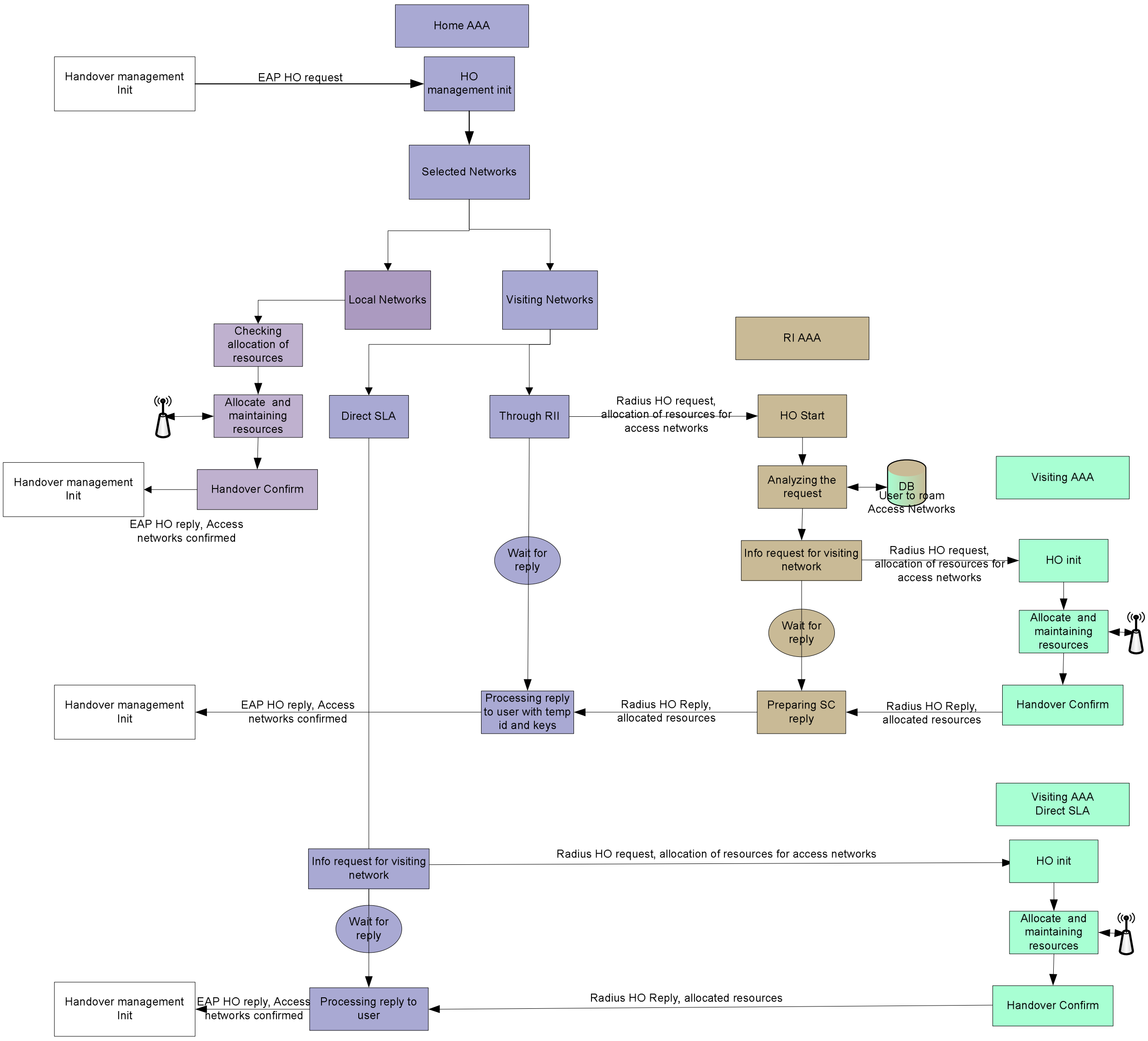

Home AAA
Handover management Init
EAP HO request
HO management init
Selected Networks
Local Networks
Visiting Networks
Checking allocation of resources
Allocate and maintaining resources
Direct SLA
Through RII
Radius HO request, allocation of resources for access networks
RI AAA
HO Start
Handover management Init
Handover Confirm
EAP HO reply, Access networks confirmed
Analyzing the request
DB
User to roam Access Networks
Visiting AAA
Wait for reply
Info request for visiting network
Radius HO request, allocation of resources for access networks
HO init
Wait for reply
Allocate and maintaining resources
Handover management Init
EAP HO reply, Access networks confirmed
Processing reply to user with temp id and keys
Radius HO Reply, allocated resources
Preparing SC reply
Radius HO Reply, allocated resources
Handover Confirm
Visiting AAA Direct SLA
Info request for visiting network
Radius HO request, allocation of resources for access networks
HO init
Wait for reply
Allocate and maintaining resources
Handover management Init
EAP HO reply, Access networks confirmed
Processing reply to user
Radius HO Reply, allocated resources
Handover Confirm

Figure 76. HO management in access networks.

5.5. Mobility Management

This section deals with the mobility management during initial access and handover or roaming. In this process mobility context for the users is created with the help of access networks. This context is created even before the mobile performs handover. The context is initiated on the terminal as well as network entities as the mobile performs handover. The main background procedure involved during mobility is done before initiation the overall latency is reduced. We have identified two mobility mechanisms; client based mobility protocol and proxy based mobility protocol. The procedures involved in mobile terminal and access networks are mentioned below.

5.5.1. MM during initial access in mobile terminal:

In this process mobility management is started when the security and handover is performed. After receiving information of IP from DHCP, mobile IP functions are initiated. During initial access general mobility procedures take place, the process mechanisms are shown in Figure 77.

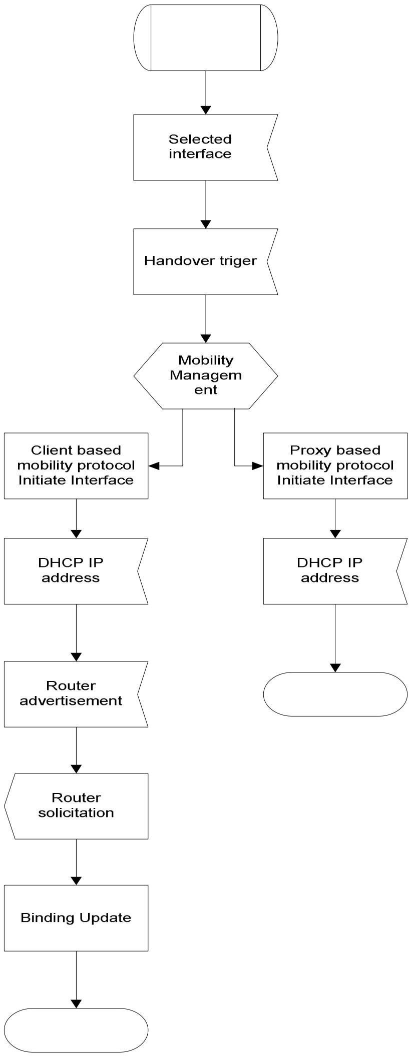


Figure 77. MM procedure during initial access in mobile terminal.

5.5.2. MM during handover and roaming in mobile terminal:

Mobility management sends the home network the information regarding which type of mobility mechanisms are to be implemented, the home network assists according to the visiting network information and replies to the client whether to use Proxy MIP or Client MIP. Other information such as keys etc.. are transferred to the client, the process mechanisms is shown in Figure 78.

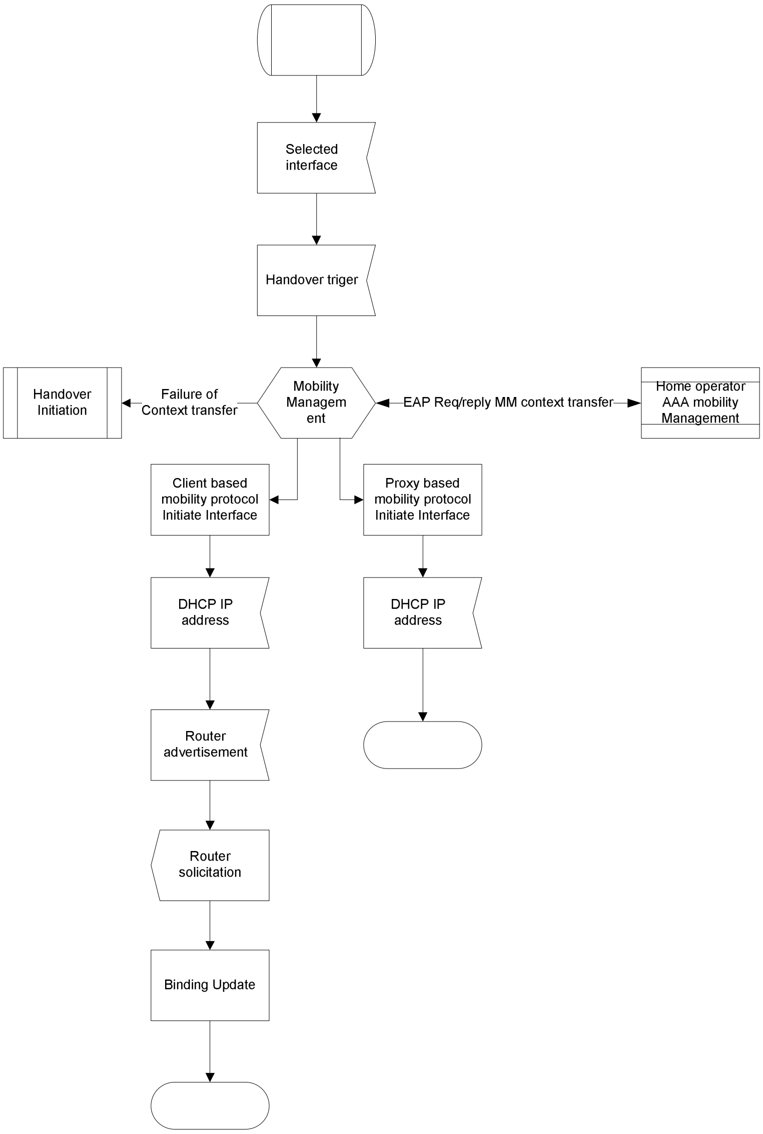

Selected interface
Handover triger
Mobility Managem ent
Failure of Context transfer
Handover Initiation
EAP Req/reply MM context transfer
Home operator AAA mobility Management
Client based mobility protocol Initiate Interface
Proxy based mobility protocol Initiate Interface
DHCP IP address
DHCP IP address
Router advertisement
Router solicitation
Binding Update

Figure 78. Process mechanisms involved in MM during handover and roaming in mobile terminal.

5.5.3. MM access networks:

The client can do register with the home network before it does the handover with this proposed mechanism. The client or the network can choose which type of mobility management can be employed. In the following section we have proposed two new mechanisms where a client establishes a mobility management even before the client roams and access in different network.

5.5.3.1. Client Mobile IP

In this method the visiting network sends the IP address and COCA after receiving a request from the home network. The home agent registers for the request and the COCA from the visiting network, sends the BU and the tunnel information is sent to the client. The whole procedure is shown in figure 79.

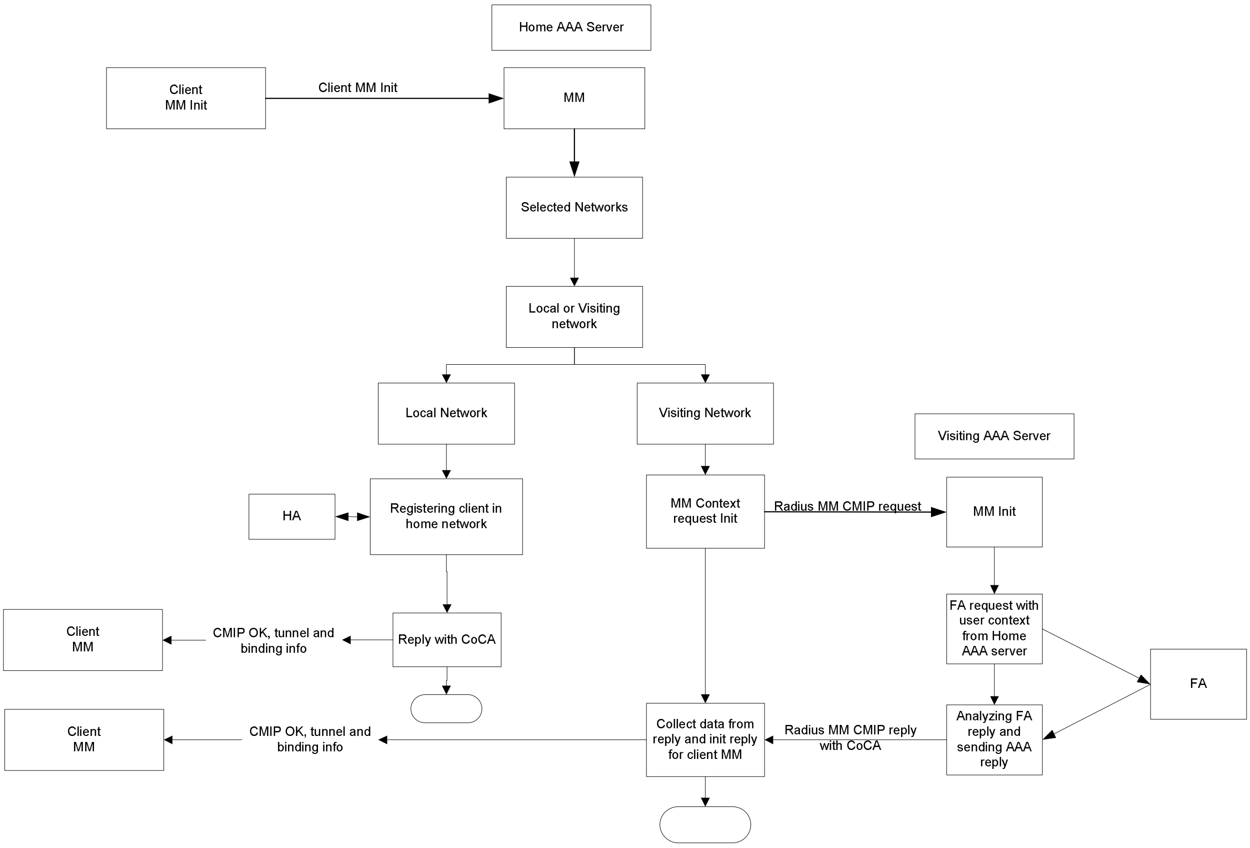

Home AAA Server
Client MM Init
Client MM Init
MM
Selected Networks
Local or Visiting network
Local Network
Visiting Network
Visiting AAA Server
HA
Registering client in home network
MM Context request Init
Radius MM CMIP request
MM Init
FA request with user context from Home AAA server
Client MM
CMIP OK, tunnel and binding info
Reply with CoCA
FA
Client MM
CMIP OK, tunnel and binding info
Collect data from reply and init reply for client MM
Radius MM CMIP reply with CoCA
Analyzing FA reply and sending AAA reply

Figure 79. Client based mobility protocol mechanism in access networks.

5.5.3.2. Proxy Mobile IP

As mentioned in chapter 4, we propose a new mobility solution based on proxy mobile IP. In this process the access networks communicate and processes the mobility information before the client moves to another network as shown in figure 80.

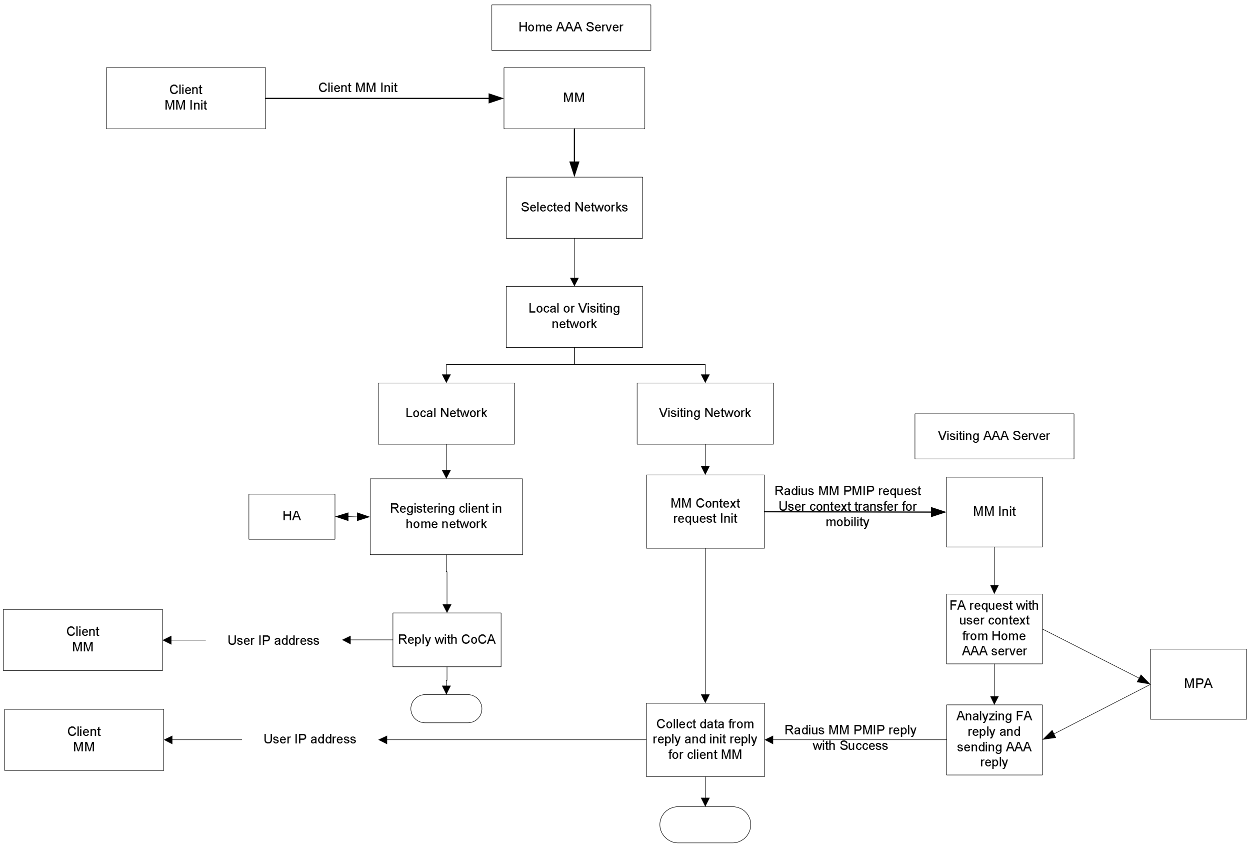

Home AAA Server
Client MM Init
Client MM Init
MM
Selected Networks
Local or Visiting network
Local Network
Visiting Network
Visiting AAA Server
HA
Registering client in home network
MM Context request Init
Radius MM PMIP request User context transfer for mobility
MM Init
FA request with user context from Home AAA server
Client MM
User IP address
Reply with CoCA
MPA
Client MM
User IP address
Collect data from reply and init reply for client MM
Radius MM PMIP reply with Success
Analyzing FA reply and sending AAA reply

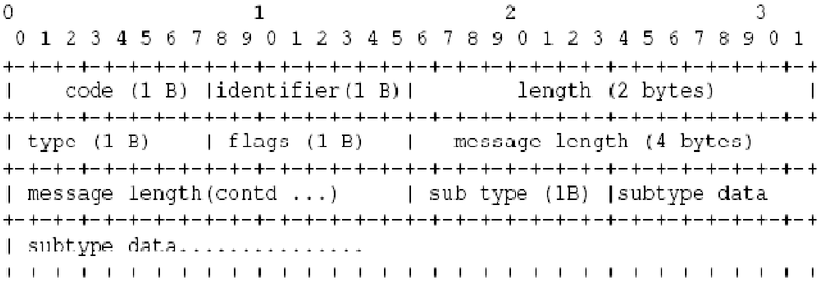
Figure 80. Proxy based mobility protocol mechanism in access networks.

5.6. QoS and Presence Management

This section deals with quality of service and resource allocation in access networks during handover and roaming. During initialization of handover management, QoS management in access networks gathers the information of allocated resources and the required amount of resources for services for user terminals. Collected information is processed using this mechanism and required bandwidth, the cost of communications is calculated. Based on the user required service this process allocates sufficient amount of resource in access network. Using this mechanism precious radio resources are not accumulated by unwanted mobile terminals. On the other hand, presence management is the process of locating the mobile terminals in access networks. This is an essential mechanism in future telecom systems as there will be a number of access technologies which are operated by different access networks. The routing of information in access networks is controlled by updating the location of the mobile terminal in the presence server location in access networks and controlled by AAA servers. When the mobile terminal does the handover or initiates the handover procedures the present server is updated by radius roaming extensions by sending its new location, this information can be accessed by any number of services, for example the VoIP call from outside to mobile terminal utilizes the present server to locate and page the mobile in access networks.

5.7. EAP Handover Extensions

The proposed protocol is to transport information for handover and roaming support for a client in different access networks to its home network dedicated server. In this process the NAS and the radius server of the visiting network routes the packets from the client to the home radius server. The client and radius server are equipped to access and process the information between them through an API and EAP HO. The proposed EAP handover method supports different functionalities of Network selection, Handover Management, security context management, mobility management and presence management.



```
0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    code (1 B) |identifier(1 B)|        length (2 bytes)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| type (1 B)    | flags (1 B)   |   message length (4 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| message length(contd ...)     | sub type (1B) |subtype data
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| subtype data...............
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
```

As mentioned in the above packet format, the packet contains fields of code, identifier, length of the packet, its type, flags for controlling, message length if in the case the packet is supporting the fragmentation, and the main important is the subtype method which is the mechanisms involved like the NS or SC etc.., and the subtype main data.

Code: The Code field is one octet and identifies the Type of EAP packet.

EAP HO Codes are assigned as follows:

1	Request
2	Response
3	Success
4	Failure

Since EAP only defines Codes 1-4, EAP packets with other codes MUST be silently discarded by both authenticators and peers.

Identifier: The Identifier field is one octet and aids in matching Responses with Requests.

Length: The Length field is two octets and indicates the length, in octets, of the EAP packet including the Code, Identifier, Length, and Data fields. Octets outside the range of the Length field should be treated as Data Link Layer padding and MUST be ignore upon reception. A message with the Length field set to a value larger than the number of received octets MUST be silently discarded.

Type: the type of EAP HO is not yet identified by the IETF for the experimental purposes we are using 255 as our data field.

Flags: the flags for the packet in the proposed mechanisms is shown below.

0 1 2 3 4 5 6 7

L M S R R R R

L is for length inclusion

M is for More Fragments, this is included on the entire packet but it is excluded in the last packet.

S is for EAP HO Start

R is for Reserved for future inclusions

Message Length: the message length field is of size 4 octets contains the information of the total length of the message in the packet.

Subtype: subtype field of 1 octet, it contains details of which type of sub information the packet is carrying. This is specified by an API from libraries to the EAP engine.

0 1 2 3 4 5 6 7

NS HO SC PM CM PR QoS

NS field is used in case the packet is carrying the NS information from the client and server.

HO field is for Handover Management

SC is for security context management

PM is proxy mobile IP management

CM is Client mobile IP management

PR is for presence management for the routing and session management

QoS is for quality of service

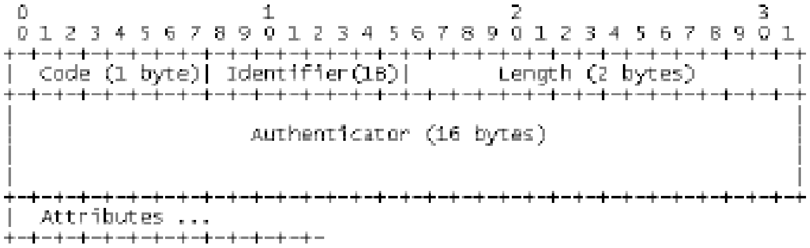
Subtype Data: this data is the information which the packet is transporting from the client and server and vice versa.

5.8. Radius Roaming extensions

5.8.1. AAA NS extension

In this section we explain details of the extended functionalities of AAA with the NS with a new attribute valued pairs and codes.

The AAA server builds NS Request message from the Access.



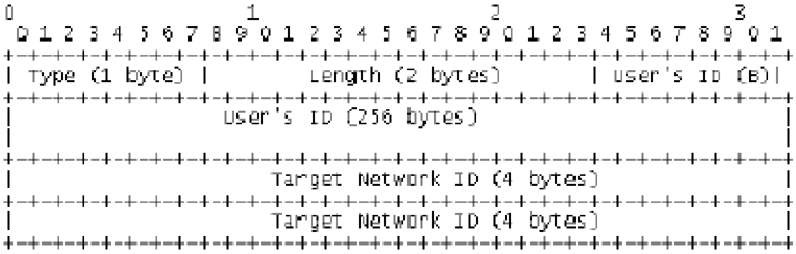
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Code (1 byte)| Identifier(1B)|       Length (2 bytes)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                   Authenticator (16 bytes)                    |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Code = (1 byte) Network_Selection_Request = 60.

Identifier: (1 byte) number to match the Request/Reply.

Length: (2 bytes) length of the message, including Code, Identifier, Length, Authenticator, Attributes. In case there is only mobility attribute, length = 350

Authenticator: The Authenticator field is 16 bytes. The most significant octet is transmitted first. This value is used to authenticate the reply from the RADIUS server, and is used in the password hiding algorithm.



```
0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type (1 byte) |        Length (2 bytes)       | User's ID (B)|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 User's ID (256 bytes)                         |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Target Network ID (4 bytes)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Target Network ID (4 bytes)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Attributes: Network selection Attribute

Type = (1 byte) NS_Request_Attribute = 193.

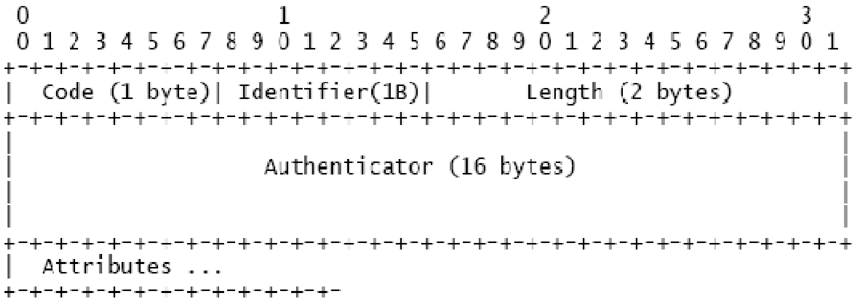
Length (2 bytes) = Length of the message = 267.

User's ID: (256 bytes) extracted from the name of the user (ex: userID@realm), whenever there is a request from the RI server to the visiting server for request RI server translates the User ID to a temporary UID with realm as mediating network.

Target Network ID: contains details of target network BS or AP ID of around 4 bytes, the request can be sent around multiple target IDs to the authenticator in this case another AAA server, if ever there are no multiple entries the field will be empty.

5.8.2. AAA SC extensions

The home Radius server builds SC Request message from the Access.



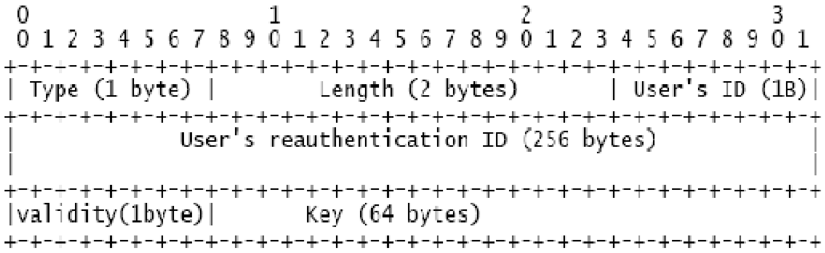
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Code (1 byte)| Identifier(1B)|       Length (2 bytes)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                   Authenticator (16 bytes)                    |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Code = (1 byte) SC_Request = TBD (IANA consideration)

Identifier: (1 byte) number to match the Request/Reply.

Length: (2 bytes) length of the message, including Code, Identifier, Length, Authenticator, Attributes.

Authenticator: The Authenticator field is 16 bytes. The most significant octet is transmitted first. This value is used to authenticate the reply from the RADIUS server, and is used in the password hiding algorithm.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type (1 byte) |        Length (2 bytes)       | User's ID (1B)|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            User's reauthentication ID (256 bytes)             |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|validity(1byte)|      Key (64 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type (1 byte) = SC_Request_Attribute = TBD (IANA consideration)

Length (2 bytes) = Length of the message

User's reauthentication ID: (256 bytes) home radius server assign this id and forwards this to the visiting networks radius server and as well as to client.

Validity (1 byte) = the valid time of the key and the re authentication id.

Key (64 bytes) = temporary key which is derived in the home radius server the visiting radius server reply to the home radius server with SC Accept message.

Code = SC_Accept = TBD (IANA consideration)

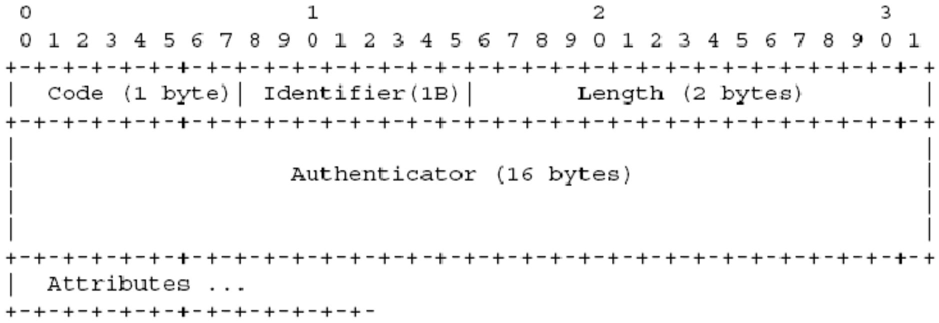
If there is any failure in the packet or the details of SC configuration on the visiting server, it sends the faliure to the home radius server.

Code = SC_Reject = TBD (IANA consideration)

5.8.3. Radius HO extension:

In this section we explain details of the extended functionalities of Radius with the HO with a new attribute valued pairs and codes.

The home Radius server builds HO Request message from the Access.



```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |  Code (1 byte)| Identifier(1B)|       Length (2 bytes)        |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 |                  Authenticator (16 bytes)                     |
 |                                                               |
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |  Attributes ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-
```

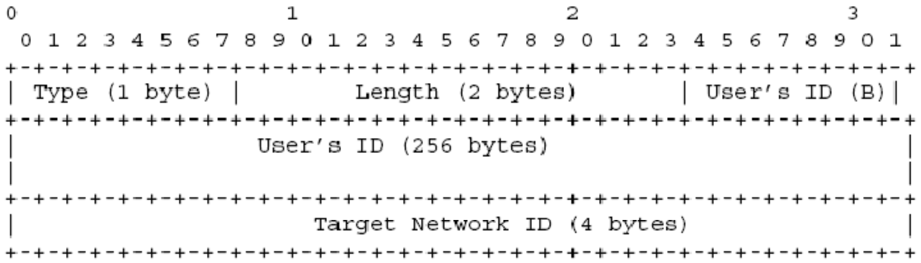
Code = (1 byte) Handover_init_Request = TBD (IANA consideration)

Identifier: (1 byte) number to match the Request/Reply.

Length: (2 bytes) length of the message, including Code, Identifier, Length, Authenticator and attributes.

Authenticator: The Authenticator field is 16 bytes. The most significant octet is transmitted first. This value is used to authenticate the reply from the RADIUS server, and is used in the password hiding algorithm.

Attributes: Handover Initiation Attribute



```
0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type (1 byte) |        Length (2 bytes)       | User's ID (B)|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 User's ID (256 bytes)                         |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Target Network ID (4 bytes)               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type = (1 byte) HO_Request_Attribute = TBD (IANA consideration)

Length (2 bytes) = Length of the message

User's ID: (256 bytes) extracted from the name of the user (ex: userID@realm).

Target Network ID: contains details of target network BS or AP ID of around 4 bytes.

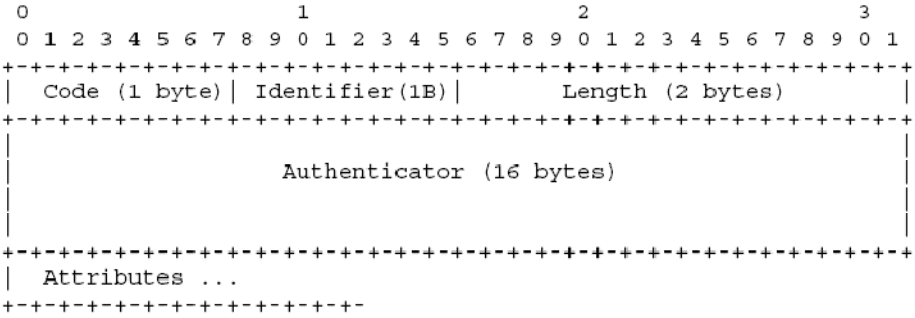
The visiting radius server reply to the home radius server with handover initiation Accept message.

Code = HO_Accept = TBD (IANA consideration)

If there is failure in retrieving and processing the data the visiting radius server must reply the home radius server with a HO initiation Reject message.

Code = HO_Reject = TBD (IANA consideration)

5.8.4. Mobility Request format:



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Code (1 byte)| Identifier(1B)|       Length (2 bytes)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                   Authenticator (16 bytes)                    |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

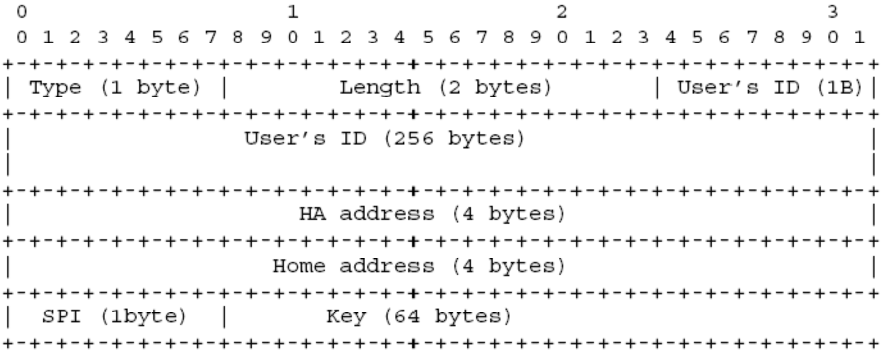
Code = (1 byte) Mobility_Request = TBD (IANA consideration)

Identifier: (1 byte) number to match the Request/Reply.

Length: (2 bytes) length of the message, including Code, Identifier, Length, Authenticator, Attributes. In the case that there is only mobility attribute, length = 350

Authenticator: The Authenticator field is 16 bytes. The most significant octet is transmitted first. This value is used to authenticate the reply from the RADIUS server, and is used in the password hiding algorithm.

Attributes: Mobility Attribute



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type (1 byte) |        Length (2 bytes)       | User's ID (1B)|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 User's ID (256 bytes)                         |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     HA address (4 bytes)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Home address (4 bytes)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  SPI (1byte)  |       Key (64 bytes)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type = (1 byte) Mobility_Request_Attribute = TBD (IANA consideration)

Length (2 bytes) = Length of the message = 332.

User's ID: (256 bytes) extracted from the name of the user (ex: userID@realm).

HA address: (4 bytes) Home Agent's IP address, filled with Zeros.

Home Address: (4 bytes) Mobile Node's Home Address, filled with Zeros.

SPI: 1 byte, filled with Zeros.

Key: (64 bytes) public key of the HA, filled with Zeros.

The visiting radius server reply to the home radius server with Mobility Accept message, the Code field for this message is:

Mobility_Accept = TBD (IANA consideration)

If there is any faliure in retreiving and processing the data the visiting radius server must reply the home radius server with a Mobility Reject message, with Code

Mobility_Reject = TBD (IANA consideration)

5.9. TESTBED

We built a testbed to demonstrate the capabilities of the proposed solutions using WLAN, WIMAX and cellular networks. The implemented architecture is shown in Figure 81. Our multi-interface user terminal used is DELL Latitude-410 equipped with Option GLOBETROTTER 7.2 ready MAX data card for EDGE access and integrated Wi-Fi interface for WLAN access. For the WIMAX access network, the terminal connects to the WIMAX CPE. The client is equipped with WPA supplicant with modified new EAP HO extensions for authentication and context transfer, mobility management using modified Dynamics mobile IP for CMIP and our PMIP solution, and a GUI for manual network selection of access networks. On the other side access networks are also modified to provide pre handover context and configuration of networks dynamically. Testbed setup of user client is shown in Figure 82.

5.9.1. WIMAX network domain

The WIMAX network domain in the testbed is composed of Infinet's pre-WIMAX equipments, operating at the frequency of 5.4 GHz. The user terminal connects to the router of the CPE through Ethernet and the CPE connects to the WIMAX BS via the air interface. The WIMAX network contains a BS and access components to provide access to users. Freeradius is used as AAA server which is resided in access network with the modified roaming extensions to support NS, SC, HO and MM. HO management algorithm is developed and deployed in freeradius server. PMIP MPA and HA/FA server is deployed to support mobility management.

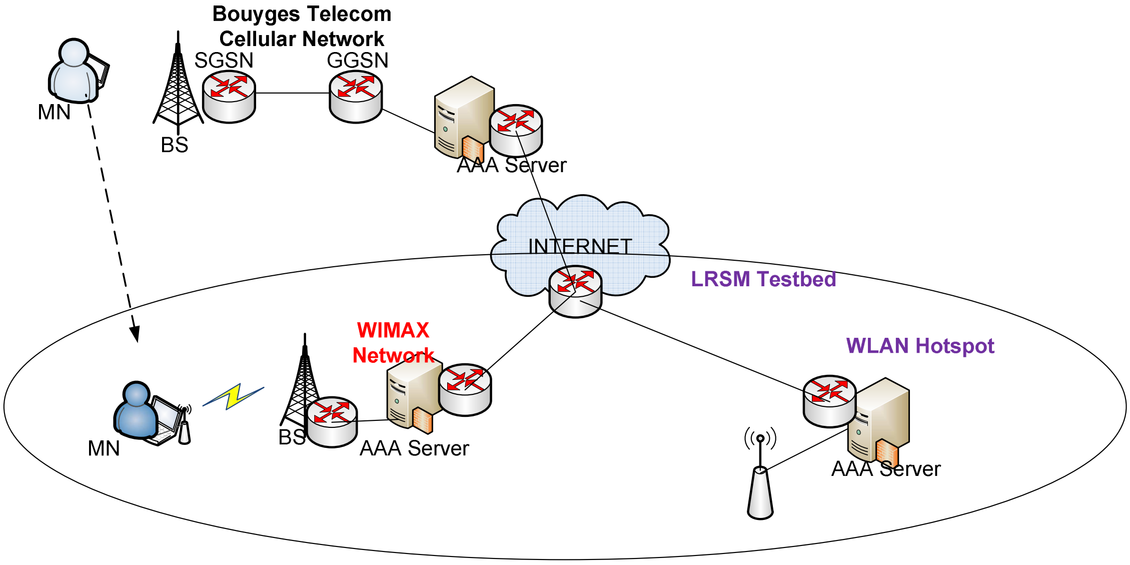


Figure 81. Testbed architecture

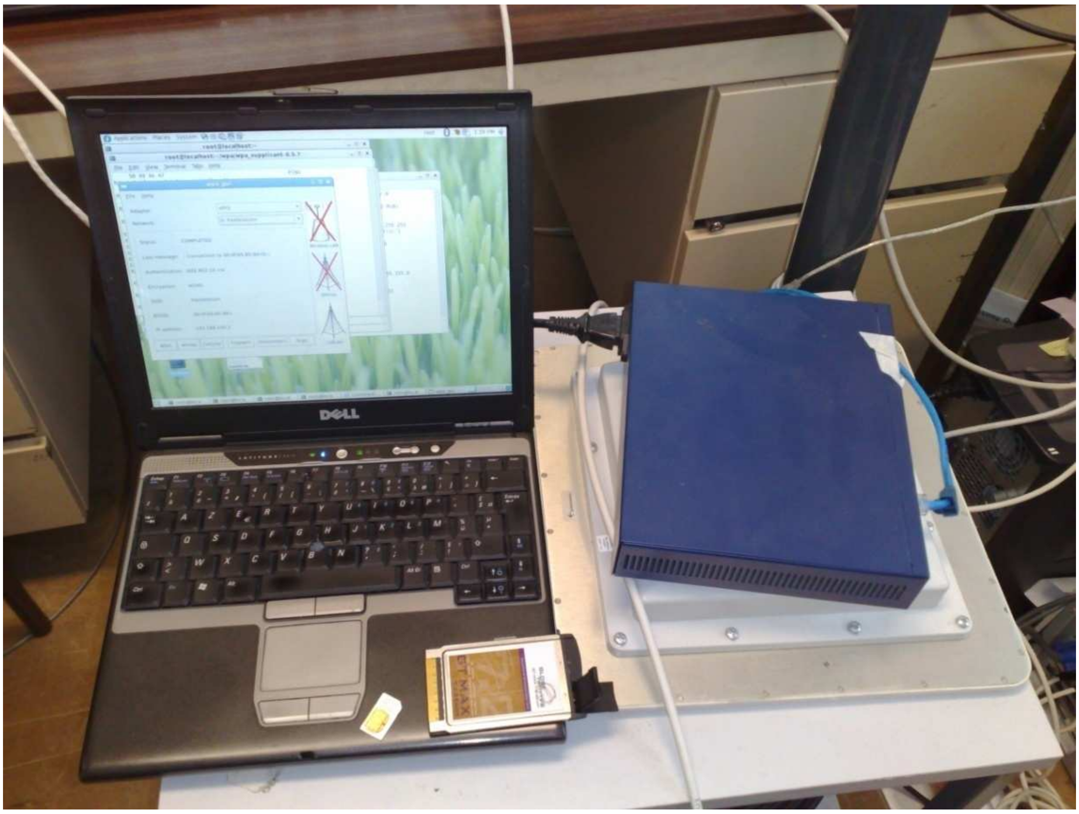


Figure 82. User terminal with a GUI with WIMAX CPE and EDGE Datacard with SIM

5.9.2. WLAN network domain

The WLAN network consists of Wi-Fi APs (Linksys WRT54 and Cisco Aironet AP350) connected directly to a WLAN Access Gateway (WAG) which is co-located inside the local WLAN RII. We also use the Host AP (device drivers for Linux) [14] which allow a WLAN card to perform all the functions of an AP.

5.9.3. EDGE network domain

The cellular network used in our testbed is the EDGE network operated by the French network operator Bouyges Telecom courtesy of MVNO Transatel. When the user accesses the operational EDGE network, the signalling messages will be forwarded to the testbed located in our premises. Authentication and access control is maintained in our testbed using AAA server specifically modified to support this functionality. Instead of using a GTP tunnel as mentioned earlier we have deployed an Ethernet tunnel over IP interface provided by the AAA server to provide context transfer while it is accessing cellular network, due to limited access to the GGSN and SGSN of bouyges telecom network. On the Ethernet interface we used EAP with modified HO extensions to support handover from cellular network to another network and for context management.

5.9.4. Methodology

We have developed EAP HO and Radius roaming extensions to support pre handover support for network selection and authentication. In this process we have performed manual selection as we don't have any proper GIS system to work on. We statistically plotted the access networks availability on a graph and with the localized GPS the mobile terminal identifies the location and through EAP NS forwards to AAA server. AAA server through mobility prediction model identifies the future network and with NAI details forwards to mobile terminal. For utilizing EAP and modifying we use WPA SUPPLICANT, once mobile terminal receives this information the configuration file is updated dynamically, then the client initiates EAP HO SC mechanism by sending a request to home AAA server. The AAA server initiates a duplicate id and a key and sends a roaming request to visiting AAA server, once visiting AAA server receives, freeradius server configures this information on the configuration files and if it is successful it sends a reply as a success to home AAA server. Home AAA server sends reply with the security details to mobile terminal. The mobile terminal configures the details from the reply and initiates handover and mobility management. Once the security management is performed in the access networks mobility management procedures are initiated, in this process AAA of home access network creates the mobility registration request and sends to visiting AAA server and HA of home network. After receiving a request from home AAA server, visiting network AAA identifies the MPA/FA and sends a registration request with the user context details from home AAA server request. MPA/FA register with HA of home network, after successful registration both HA and MPA does initiate the tunnel and wait for AAA server request of tunnel update. With all the process mechanisms are initiated and configured AAA of home network sends HO initiation message to client, after listening to this reply mobile terminal does start roaming/handover. Using context details we have achieved seamless handover in vertical scenarios where as in horizontal handover we have achieved low latency averaged around 30ms which includes network selection, authentications, mobility management in access networks.

5.10. Summary

The chapter proposes new network selection, security management, handover management, mobility management procedures using access networks consent. The proposed mechanism supports WLAN, WIMAX and 3G networks. Using the mobility prediction model coupled with GIS information system the access networks at future location of mobile terminal. Using pre handover mechanisms with EAP HO and AAA extensions proposed in this paper the home access networks negotiate with visiting access networks and networks entities to allocate and reserve resources for accommodating mobile terminals enabling the solution proposed is efficient. Using these mechanisms the mobile terminal mobility can be handled efficiently in any access networks.

Chapter 6. Conclusions

Mobile technologies are dominating the modern communication world. As foreseen by many researchers and analysts, the next generation wireless mobile communications (4G) will be based on the heterogeneous underlying infrastructure integrating different wireless access technologies. Future mobile users need to enjoy seamless mobility and ubiquitous access to services in an always best connected mode. We underlined some critical issues that appear in the context of future 4G heterogeneous mobile networks and this thesis than concentrates on the issues related to the heterogeneous network access in the presented open 4G environment. These include convergence of heterogeneous networks, network detection and discovery, roaming service access control, security access, mobility management and user QoS over different link technologies.

In this context, the inter-system roaming architectures play an important role to achieve the goal of seamless mobility. We have designed an open and flexible interworking architecture using an intermediate entity called Roaming Intermediatory Interworking (RII). The proposed RII enables the secure handover across different access systems and different operator domains without service interruption and with no intervention of the user. From the user's point of view, our approach guarantees a stable transparent seamless roaming service environment. The proposed solution allows users to freely and securely move across different access systems without need of pre-existing subscription. From the operator's point of view, our system uses the best available resources and providing cost effective services efficiently. The solution is feasible and economical since it does not require much change in the existing network infrastructure. Indeed, the WISP/WIMAX/cellular operator that wants to benefit from such interworking and roaming facilities only needs to add the local/core RII functionalities in its access gateway, physicially connect its network to the RII and establish an SLA (Service Level Agreement) with the RII operator to take benefit of this service. One of the main aim of Roaming Intermediary architecture is to provide security authentication and re-authentications, different security access mechanisms are proposed in this thesis to achieve this with low latency. Handover mechanisms are proposed to ensure different processes involved such as Network detection and Selection during roaming are performed efficiently. We validated our architecture by developing a testbed and its components using WLAN, WIMAX and 3G networks. Comparisons with other existing architectures revealed the efficiency of our architecture supporting every aspect involving roaming and handover than other systems. Due to complexity of maintaining large number of access networks involving different access technology in the future converged networks, we have proposed different network management techniques to ease the integrating and updating access networks and technologies.

The other contribution of the thesis was to optimize and propose novel techniques to obtain seamless roaming in converged networks. We categorized this into two parts, one is post handover trigger optimization and the other is pre handover optimizations. Post handover techniques enhance the performance of the approach (i.e. reduce latency) of the roaming and handover of a mobile terminal in heterogeneous networks.

We introduced new techniques in security authentication and mobility access. With the introduction of multiple access technologies, different security mechanisms involved for authentication complicates the concept of seamless roaming. User identity management is one of the main issues which have to be addressed in heterogeneous networks. Maintaining the identity is crucial for future converged networks as the user credentials differ from one technology to another differs. We have approached two ways to solve ever longing issue of user identity and routing of user authentication information from visiting access networks with or without a direct SLA with the home network. The first method proposes dynamic assignment of user credentials derived from home networks to the users by security context management and the other procedure involves a mediating entity providing identity to users, mediating networks maintaining this identity dynamically with visiting networks. The authentication mechanisms differ from one access technology to another and one operator to another. Authentication is performed by home access networks through the visiting access networks, this procedure generates high latency as the authentication information is routed through the home and visiting networks for every single exchange of information. Re using the keying material involved in one security mechanisms to another is the main approach we are following, as this removes the whole procedure of generating keying material, messages involved during this keying is minimal. The authentication keying material created and transferred to visiting access networks dynamically, in this way the theft presentational and security vulnerabilities are reduced. The mechanisms presented are applicable to WLAN, WIMAX and cellular networks.

We also propose new mobility model using PMIP and AAA as a mobility solution for future networks. In this mechanism the mobility is managed through the network entities, mobility of user is triggered when there is a request for access from mobile terminal to the access networks. Authentication and mobility access are performed in parallel and once the authentication is successful the mobility registration is granted to user terminal to provide access. Fast and seamless handover is achieved in various deployment and mobility scenarios using these mechanisms. Extending and upgrading existing networks can be performed efficiently, as no new hardware is added to the existing architectures. Multi homing scenarios, different interworking architectures of WLAN, WIMAX and 3G are addressed using this mechanism and validated using developed testbed involving WLAN, WIMAX and cellular networks.

Using highly optimized techniques for roaming and handover cannot ensure seamless mobility. We are proposing enhanced as well as novel mechanisms at various levels of access networks, for network assisted or aided network selection, security management, handover management and mobility management in heterogeneous networks. When a mobile terminal is connected to an access network and is on move the SNR of the connected network is constantly monitored, if ever the required threshold is less than the current SNR the terminal does the handover. The user terminal gathers information on its inner capabilities, surrounding networks, active sessions, global position and the user preferences. This real-time information is gathered by the terminal and provides context transfer to the service platform or network entities. By predicting the user mobility pattern using GIS and provisioning information from user terminal, availability of resources the network does select the suitable network and sends it user terminal. In addition to the access network discovery, the transfer of user's mobility and security contexts from the serving network to the target network, network entities and the mobile terminal is performed. Once this information is transferred the network entities creates the user context and prepares for handover, after receiving selected network and handover trigger initiation from access network, user terminal trigger the handover with context details from other procedures. By utilizing optimized procedures at every stage of handover the overall latency and control of procedures are obtained. We also introduced new EAP method to perform these functionalities, and Radius roaming extensions on the network side. We developed a testbed with minimal functionalities to validate Security management and Mobility management using WLAN and WIMAX networks proposed.

6.1.1. Future Work

Seamless Secured Roaming and handover in heterogeneous networks is a complex problem comprising of a large number of challenging issues. Regarding the aspects addressed in this thesis, there are still many possible research areas that the future work may take.

In heterogeneous networks, the users will be always best connected (ABC) through the best access network using the best available device. The network operator has to satisfy ABC property for users (or aid users to get ABC property) and has to maintain the best possible utility out of its investment. From the network operators' perspective, the operators need environment which fulfills the requirements for "Always Best Managed" (ABM) infrastructures, networks, and services. An intelligent network selection and an autonomous handover management are required to achieve ABC and ABM simultaneously. The autonomous handover and roaming management in heterogeneous networks becomes one of future research directions towards seamless mobility. One of the other research directions towards the seamless roaming is the radio resource management (RRM). In an open access heterogeneous networks, two independent operators battle to get user connections (by allocating an appropriate resource amount to each user) to maximize their resource utilization and their revenue knowing that users have liberty to select the access network of highest utility level (according to preferences of each user). Although we provided initial input for this concept by utilizing pre handover QoS resource allocation, there are number of issues that have to be addressed to provide end to end efficient services.

Dynamic Spectrum Access (DSA) or cognitive radio a network is a new network paradigm which addresses the limited available spectrum and the inefficiency in the spectrum usage. The cognitive radio techniques allow users to select the best available channel for the communication. The users can switch from one spectrum hole to another to maintain the connectivity, which is known as spectrum handover. The purpose of spectrum mobility management, including best channel selection and spectrum handover, is to make sure that such transitions are seamless and as soon as possible such that the applications running on cognitive radio users perceive minimum performance degradation during a spectrum handover. One of our future works includes adapting our secured roaming architecture to these spectrum handover operations to maintain the seamless service delivery and also study the techniques that are to be included for delivering seamless services such as mobility, security managements.

We are also looking into possibility of standardization of some of our work presented in this thesis. As an initial step we have contributed and presented some of our protocols in IETF working groups and Forums.

References

[1] W. Webb, *The Future Wireless Communications*. John Wiley & Sons, 2007.

[2] 3GPP TS 21.101, "Technical Specifications and Technical Reports for a UTRAN-based 3GPP system".

[3] 3GPP TS 25.308, "High Speed Downlink Packet Access (HSDPA)".

[4] 3GPP TS 36.201, "Evolved Universal Terrestrial Radio Access (E-UTRA); Long Term Evolution (LTE) physical layer".

[5] C. S.-0. 3GPP2, "Signaling Conformance Specification for Ultra Mobile Broadband Air Interface".

[6] IEEE, "IEEE Std 802.11™-1999: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications".

[7] IEEE, "IEEE Std 802.11a™-1999: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band".

[8] IEEE, "IEEE Std 802.11b™-1999: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band".

[9] IEEE, "IEEE Std 802.11g™-2003 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band".

[10] J. G. Andrews and A. Ghosh, *Fundamentals of WIMAX: Understanding Broadband Wireless Networking*. NJ, USA: Prentice Hall PTR, 2007.

[11] I. 802.20, "Mobile Broadband Wireless Access (MBWA) http://www.ieee802.org/20/".

[12] IEEE802.22-06/0069r2, "PHY/MAC Specification for IEEE 802.22".

[13] A. V. 2. N. 1. Anritsu News, Ed., *What Exactly is 4G? Sorting Out the 4G Stew.* 2007.

[14] S.-L. Tsao and C.-C. Lin, "Design and evaluation of UMTS-WLAN interworking strategies," in *Vehicular Technology Conference*, 24-28 Sept. 2002, pp. Page(s):777-781vol26th.

[15] M. Dillinger and S. Buljore, *Reconfigurable systems in a heterogeneous environment.* John Wiley & Son, Ltd, 2003.

[16] y.-H. Choi, O. Song, and D.-H. Cho, "A seamless handoff scheme for UMTS-WLAN interworking", Global Telecommunications Conference," in *GLOBECOM '04*, 29 Nov.-3

Dec. 2004 , pp. 1559-1564Vol3.

[17] V. Varma, et al., "Mobility Management in Integrated UMTS/WLAN Networks," in *IEEE ICC 2003*, Anchorage, Alaska, USA , May 2003.

[18] M. Jaseemuddin, "An Architecture for Integrating UMTS and 802.11 WLAN Networks," in *Eighth IEEE International Symposium on Computers and Communications*, 2003, p. 716.

[19] A. K. Salkintzis, C. Fors, and R. Pazhyannur, "WLAN-GPRS integration for next-generation mobile data networks," in *Wireless Communications, Volume 9, Issue 5*, Oct. 2002, p. 112–124.

[20] S. Parkvall, "Long-term 3G Evolution – Radio Access," Ericsson Research Report.

[21] T22.234.. 3GPP, "3GPP Technical Specification: Group Services and Systems Aspects - Requirements on 3GPP System to WLAN Interworking (Release 6)," pp. 2005-2006.

[22] T.22.234 3GPP, "3GPP Technical Specification: Group Services and Systems Aspects - Requirements on 3GPP System to WLAN Interworking (Release 7)," 2006.

[23] "The SCCAN Forum (www.sccan.org)".

[24] L. Vollero and F. Cacace, "Managing mobility and adaptation in upcoming 802.21 enabled devices," in *Proceedings of the 4th international workshop on wireless mobile applications and services on WLAN hotspots (collocated with MOBICOM 2006)*, Los Angeles, CA, USA, September 2006.

[25] "ETSI TI-SPAN general link specifications: http://portal.etsi.org/docbox/TISPAN/Open/," in .

[26] ETSI E20v1 0 "NGN Funcional Architecture; Network Attachment Subsystem Release 1," in .

[27] TS23.882 v1.6.1 TR., "3GPP System Architecture Evolution: report on technical options and Conclusions," in , 2006.

[28] IEEE, "Local and Metropolitan Area Networks: Port-Based Network Access Control," in *IEEE Standard 802.1X*, September 2001.

[29] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS) ," in *RFC 2865*, June 2000.

[30] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," IETF RFC 2284, March 1998.

[31] B.S. Aboba, and H. Levkowetz, "Extensible Authentication Protocol (EAP) Key Management Framework," IETF RFC, October 2005.

[32] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol," IETF RFC 2716, October 1999.

[33] P. Funk and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-

TTLS)," IETF RFC Work in Progress, August 2004.

[34] Palekar and et. al, "Protected EAP Protocol (PEAP)," IETF RFC, July 2004.

[35] H. Haverinen and J. Salowey, "EAP SIM Authentication," IETF RFC 4186, January 2006.

[36] IEEE. 802.11F, "IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation.".

[37] C. Perkins, "IP Mobility Support," IETF RFC 2002, October 1996.

[38] R. Droms, "Dynamic Host Configuration Protocol, ," IETF RFC 2131, March 1997.

[39] Johnson. D, and Arikko. J, "Mobility Support in IPv6," IETF RFC 3775, June 2004.

[40] H Soliman and et al, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," IETF RFC 4140, August 2005.

[41] R Kodali, "Fast Handovers for Mobile IPv6," IETF RFC 4068, July 2005.

[42] A Mishra, "IDMP-based Fast Handoffs and Paging in IP-based 4G Mobile Networks," *IEEE Commun. Mag*, pp. 138-145, 2002.

[43] A.T Campbell et.al, "Design, Implementation, and evaluation of Cellular IP," *IEEE Pers. Commun*, pp. 42-49, Aug. 2000.

[44] R Ramjee. et. al, "HAWAII : A domain –based Approach for supporting mobility in Wide-Area Wireless Network," *IEEE/ACM Trans. Net*, vol. 10, no. 3, p. 396–410, Jun. 2002.

[45] A. katouin, "cellular IP report," in *3G Mobile Technologies conference Publication No 471*, pp. 129-132.

[46] R Ramjee. e. al, "IP Micro Mobility Support using HAWAII," IETF RFC, 25 June 1999.

[47] P Eronen, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)," MOBIKE Working Group, October 7, 2005.

[48] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol," IETF RFC 2407, September 23, 2004.

[49] R.Stewart and et. al, " Stream Control Transmission Protocol," IETF RFC 2960, October 2000.

[50] L. Ong, "An Introduction to the Stream Control Transmission Protocol (SCTP)," IETF RFC 3286, May 2002.

[51] N.Parameshwar and et. al, "Advanced SIP series: SIP and 3GPP Operations," Award Solutions Inc, Nov. 2001.

[52] H.Schulzrinne, " SIP: Session Initiation Protocol," IETF RFC 2543, March 1999.

[53] J.Rosenberg and al, "SIP: Session Initiation Protocol," IETF RFC 3261, Jun. 2002.

[54] J. Rosenberg and H. Schulzrinne, "Reliability of Provisional Response in Session Initiation Protocol," IETF RFC 3262, Jun. 2002.

[55] Masinter and et.al , "Uniform Resource Identifiers (URI): Generic Syntax," IETF RFC 2396, Aug. 1998..

[56] J. Rosenberg, "Session Initiation Protocol (SIP): Locating SIP Servers," IETF RFC 3263, Jun. 2002.

[57] A. B Roach, " Session Initiation Protocol (SIP)-Specific Event Notification," IETF RFC 3265, Jun. 2002.

[58] AK. Salkintzis and et. al, "WLAN-GPRS integration for next-generation mobile data networks," *IEEE Wireless Communications*, p. 112—124, 2002.

[59] WIMAX. Forum, "WIMAX Forum Network Architecture Stage 2," January, 2008 .

[60] Intel, "Public WLAN hotspot deployment and interworking," Intel Technology Journal, 2003," Intel Technology Journal, 2003.

[61] B. Anton and al, "Best current practices for wireless internet service provider roaming," WiFi Alliance, 2003.

[62] Akyildiz, M. S, and X. J, "A ubiquitous mobile communication architecture for next generation heterogeneous wireless systems," *IEEE Radio Communications*, p. 29–36, Jun. 2005.

[63] WeRoam, "Wireless LAN roaming brokers and the role they play between WISPs and providers," *white paper*, Jan. 2005.

[64] OWL Web Ontology. [Online]. http://www.w3.org/

[65] Stanford Protégé. [Online]. http://protege.stanford.edu/

[66] T.R Grber, " A translation approach to portable ontologies. , 5(2):, .," Knowledge Acquisition, 1993.

[67] S Mohanty, "VEPSD: a novel velocity estimation algorithm for next-generation wireless systems," *IEEE Transactions on Wireless Communications*, vol. 4, p. 2655to2660, Nov. 2005.

[68] M Turkboylari andG Stuber, "Eigen-matrix pencil method-based velocity estimation for mobile cellular radio systems," in *IEEE International Conference on Communications (ICC)*, New Orleans, USA, 2000.

[69] A. G, Senadji B, and B. B, "Velocity estimation in cellular systems based on the time-frequencycharacteristics of the received signal," in , Malaysia, 2001, p. SixthInternationalSymosiumonSignalProcessinganditsAlications.

[70] J. How, and et.al, "GPS Estimation Algorithms for Precise Velocity, Slip and Race-Track Position Measurements," Society of Automotive Engineers (02MSEC-93), Technical report, 2002.

[71] Host AP . [Online]. http://hostap.epitest.fi/

[72] Freeradius. [Online]. http://freeradius.org/

[73] Dynamics mobile IP. [Online]. http://dynamics.sourceforge.net/

[74] WPA Supplicant. [Online]. http://hostap.epitest.fi/wpa_supplicant/

[75] V. Marques, R.L. Aguiar, and et al, "An IP-based QoS Architecture for 4G Operator Scenarios," in *IEEE Wireless Communications*, June 2003, pp. 54-62.

[76] X. Fu, T. Chen, A. Festag, H. Karl, G. Schaefer, and C. Fan, "QoS-Enabled Mobility Support for IP-based Networks," in *IPCN'2003*, Dec. 2003.

[77] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller, "Architecture for Mobility and QoS Support in All-IP Wireless Networks," *IEEE JSAC*, pp. 691-705, May 2004.

[78] L. Salgarelli and e. al, "Emerging Authentication and Key Distribution in Wireless IP Networks," *IEEE Wireless Communications*, pp. 52-61, Dec. 2003.

[79] Leung K., Dommety G., Yegani P, Chowdhury K, "Mobility Management using Proxy Mobile IPv4," IETF RFC, January 2007.

[80] Plummer D."Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware," IETF RFC 826, November 1982.

[81] Postel. J, "Multi-LAN Address Resolution", , ," IETF RFC 925, October 1984.

[82] Adoba. B, "IANA Considerations for RADIUS," IETF RFC 2869, July 2003.

[83] Detailed results and logs of testbed implementations. [Online]. http://193.54.225.196/pmip

[84] Vollero. L and Cacace. F, "Managing mobility and adaptation in upcoming 802.21 enabled devices," in *4th international workshop on wireless mobile applications and services on WLAN hotspots*, Los Angeles, CA, USA, September 2006.

[85] Arikko. J and e. al, "Mobility Support in IPv6," IETF RFC 3775, May 2003.

[86] Network-based Localized Mobility Management. [Online]. http://www.ietf.org/html.charters/netlmm-charter.html

[87] Arikko. J and e. all, "Network Discovery and Selection Problem," IETF RFC draft-ietf-eap-netsel-problem-04, May 25, 2006.

[88] Z. Yilin, "Standardization of Mobile Phone Positioning for 3G Systems," *IEEE Communications Magazine*, Jul. 2002.

[89] Liang. B and Haas. Z, "Predictive distance-based mobility management for PCS networks," in *IEEE Computer and Communications Societies(INFOCOM)*, March 1999.

[90] V. K. Gondi and N. Agoulmine, "Radius Roaming Extensions," IETF RFC proposal draft-gondi-radext-radius-roaming-01, march 2008.

[91] E. Gregori and et.al "Mesh networks: commodity multihop ad hoc networks," *IEEE Communications Magazine*, vol. 43, no. 3, pp. 123-131, Mar. 2005.

[92] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Communications Magazine*, vol. 43, no. 9, pp. S23-S30, Sep. 2005 .

[93] Balali. K and e. al, "Performance evaluation of hybrid wireless network architecture for rural communication," in *ICPWC*, 2005.

[94] O.I Hillestad and et.al, "Delivery of on - demand video services in rural areas via ieee802.16 broadband wireless access networks," in *2nd ACM Workshop on Wireless Multimedia Networking and Performance Modeling (WMuNeP´06),*, 2006.

[95] C.Cicconneti, L. Lenzini. Unknown, M. E, and E. C, "Qality of service support in IEEE802.16 networks," *IEEE Network* , vol. 20, no. 2, p. 50–55, 2006.

[96] Sullivan. G.J and e. al, "Advanced video coding for generic audio visual services : Itu-trec. h.264 and iso/iec 14496-10 (mpeg-4 part10) avc," Tech.Rep, 2003.

[97] Sullivan.G.J and et.al, "Video compression-from concepts to the h.264/avc standard," *IEEE Networks*, vol. 93, p. 18–31, 2005.

[98] T.Sikora, "Mpeg digital video-coding standards," *IEEE Signal Processing Magazine*, vol. 14, no. 5, pp. 82-100, 1997.

[99] M. V and e. al, "An IP-based QoS Architecture for 4G Operator Scenarios," in *IEEE Wireless.*

[100] "Yilin Zhao, ”Standardization of Mobile Phone Positioning for 3G Systems”, ," Jul. 2002.

[101] Rhee and Injong, "Error control techniques for interactive low bit rate video transmission over the internet," vol. 28, no. 4, pp. 290-301, Oct. 1998.

Annex A. WIMAX Study

The main aim of the chapter is to discuss WIMAX operating and deployment scenarios studies, this chapter also defines security and mobility architecture for WIMAX networks. Due to the mobility of the users as well as the networks some of the key issues like security and mobility management are not addressed properly due to non availability of infrastructure to handle authentications, mobility management in the access networks. To provide services in a isolated areas, and to cover large areas the ideal solution is provided by the cellular networks, but the bandwidth, cost of communication and the availability for different services are limited by the cellular networks. For this purpose we propose to integrate WIMAX (IEEE 802.16) based networks working in a mesh configuration with WLAN (IEEE 802.11) as a solution to provide different services. By this method a centralized system is proposed to process authentication and mobility management in the network for the users as well as access networks. In the proposed architecture, a master node acts as a gateway for mesh and slave nodes. The gateway has an AAA server which acts as an authentication and accounting server for the mesh nodes. WLAN are interconnected to mesh nodes and slave nodes and the users use WLAN as an access network. The user authenticates to the network using EAP or a onetime password method to access the services in the network. We also proposed mobility management in the architecture where users roams along different access networks in an efficient manner. We evaluated the architecture using a testbed, we calculated the time of authentications and re-authentications during roaming, delay at the user level while networks are in mobile mode.

Also in this chapter we show experimental results of video streaming over IEEE 802.16 networks, returned from testbed measurements, which is done in the framework of an interactive urban IP Television using Wireless Broadband Networks (Polymage). We focus on the quantification of the throughput parameter related to multiple video streaming session received in parallel on a terminal and study its behavior under 802.16 channel frequency variations and deployment architectures. The main aim of this study is to evaluate the most critical properties while streaming video by tuning 802.16 equipments parameters to be ready for the deployment of a real urban wireless network for TV broadcasting. We studied different deployment scenarios of WIMAX deployments; WIMAX BS and multiple CPE model, WIMAX in a MESH formation and the final is WIMAX BS with Multiple CPEs interconnected with the

WLAN APs. We provide the different results through the parameters variation from the deployed scenarios in this paper.

A.1. Introduction

With shared data rates up to 75 Mbps, a single area of an 802.16a base station provides sufficient bandwidth to cover a large area. To support a profitable business model, operators and service providers need to sustain a mix of high-revenue business customers and high-volume residential subscribers. 802.16a helps meet this requirement by supporting differentiated service levels. The 802.16 specification also includes robust security features and the Quality of Service needed to support services that require low latency, such as voice and video.

By using a robust modulation scheme, IEEE 802.16 delivers high throughput at long ranges with a high level of spectral efficiency that is also tolerant for signal reflections. Dynamic adaptive modulation allows the base station to tradeoff throughput for range. For example, if the base station cannot establish a robust link to a distant subscriber using the highest order modulation scheme, 64 QAM (Quadrature Amplitude Modulation), the modulation order is reduced to 16 QAM or QPSK (Quadrature Phase Shift Keying), which reduces throughput and increases effective range.

In this chapter we identified different parameters of WIMAX in various scenarios of WIMAX deployments to obtain best effort service for the video on demand services Through this deployment we have obtained the average throughput, packet loss of the video services at different operated frequencies, modulation mechanisms, physical bit rate and power level at CPE and BS.

A.2. Background of WIMAX and Wireless Mesh Networking

WIMAX aims at serving the broadband services in a metropolitan areas using Mesh networking [91]. Mesh networks are built by a set of nodes interconnected by wireless links, nodes can send the data to other nodes directly or by using intermediate nodes until data reaches to the final gateway. It is gaining significant attention as a possible way for cash strapped Internet service providers (ISPs), carriers, and others to roll out robust and reliable wireless broadband service access in a way that needs minimal up-front investments [92] [93] [94]. With the capability of self-organization and self configuration, WMNs can be deployed incrementally, one node at a time, as needed. As more nodes are installed, the reliability and connectivity for the users increase accordingly. Wireless mesh networks will help the users to be always-on-line anywhere anytime. With the gateway/bridge functionalities in mesh networks enable the integration of mesh networks with various existing wireless networks such as cellular, wireless sensor, wireless-fidelity (Wi-Fi), worldwide inter-operability for microwave access (WIMAX), WiMedia networks.

A.3. Architecture

This section provides details of WIMAX access networks and their security and mobility architectures, WLAN networks and their security access and mobility management, WIMAX mesh networks, methodologies in security and mobility in the proposed architecture. This section also defines the proposed architecture WIMAX mesh network as a infrastructure backbone with WLAN and its security and mobility management to provide services for users.

A.3.1. Security in WIMAX Access Networks

The security architecture of 802.16 is divided into two layers; the first layer is to provide encapsulation for the data access across the 802.16 networks. The second is a key management protocol PKM providing secure distribution of keying data between the BS and terminal. PKM supports both mutual authentication and unilateral authentication. The key management protocol uses EAP or X.509 digital certificates together with RSA or a sequence starting with RSA and followed by EAP. PKM EAP uses Extensible Authentication Protocol with an operator selected a specific EAP method like EAP − TLS, EAP − SIM. As in the WLAN the WIMAX subscribers use EAP NAI for identification extension and Network selection to authenticate over the WIMAX networks.

A.3.2. Security in WLAN Access network

The IEEE's 802.1X is a Port Based Network Access Control standard provides strong authentication and network access control for 802.11 networks. Various authentication methods such as digital certificates, smart cards and one-time passwords can be used to provide credential information for authentication. The most common type of Authentication Server is RADIUS (Remote Authentication Dial-In User Service). EAP is a general protocol and is 'extensible' in that it supports multiple authentication mechanisms. 802.1X supports such EAP types as Message Digest 5 (MD-5), Transport Layer Security (TLS), and Protected Extensible Authentication Protocol (PEAP), EAP SIM, EAP – AKA.

A.3.3. WIMAX Mesh Network

WIMAX mesh networks are based on IEEE 802.16 standard (2004) which provides fast and efficient deployment of WIMAX in a mesh network. The standard provides information of scheduling schemas, routing in the mesh nodes. In the proposed architecture different WIMAX nodes form a mesh network in a secured manner and perform the routing using minimum multihop algorithm and the network advertises the gateway once the node is connected to the mesh node [91]. In the proposed solution the security mechanisms are deployed using public authentication or private authentication schemas using AAA server. Once the new WIMAX node identifies the network, is starts the authentication mechanisms and register in the local database of the gateway. Once establishing the network it establishes the connection between the different nodes, and then evaluates the possible minimal route and the cost of communication on the whole to identify the best possible routes. The mesh node continuously does the procedure in case of topological changes or link conditions to ensure the route is optimal from the node to the gateway. The mesh nodes can switch to alternative routes in case the active routes tend to get worse.

A.3.4. Security and mobility management for mobile wireless network using Integrated WIMAX Mesh Network with WLAN Networks

To provide services in mobile wireless networks the main requirements are to provide better bandwidth and connectivity. These issues can be solved using WIMAX as an infrastructure for the WLAN networks. In this traditional method a CPE is connected to a BS. If the CPE moves to long distance the connectivity is lost. Or in some cases these networks are isolated, to provide services a BS must be installed at the places where networks are in range. This provides more complexity and requires infrastructure. Instead these networks can form a mesh and forwards the information to a specific fixed gateway. Even though this is a very efficient manner there are still some complex issues like the identification and authentication of the mesh nodes, mobility of the mesh nodes, authentication of users who would like to use the services, billing. Using a two layer security mechanisms, by maintaining centralize data base of the networks as well as users the above mentioned complexities are solved. By including the mobility management and self healing capacity of mesh nodes, they work in a mobile environment. Even the users can roam with the security and mobility management proposed here in the following sections of the paper.

In the architecture the WIMAX mesh networks contains mesh nodes which acts as routers. The mesh nodes in the network form, mesh of self-configuring, self-healing links among themselves, with gateway functionality mesh nodes are connected to the Internet. Infrastructure mechanisms enable integration of WMNs with existing wireless networks, through gateway/bridge functionalities in mesh nodes. As shown in figure 1 WIMAX nodes forms a mesh network and the routers on the nodes are integrated with the WLAN networks. One of the node in the network is fixed and acts as a gateway to the internet. Nodes authentication and user authentications are also passed through the gateway AAA server. All the other node are configured as mobiles and WLAN networks are connected at the end point of the network. Due to self configurable nature of WIMAX mesh networks all the data and control messages are passed through the Master node which acts as a gateway.

In this particular scenario we observed two cases one is when the user roams in the WLAN networks in the inter or the intra mesh node and the second is whole network roams to another location, i.e.. connected in the different group or to another node. First scenario is explained detailed in the next section, in the second scenario of network mobility, mesh node connects to another node transparently. The user connected to the network doesn't know the network mobility but the users can observe small latency and packet loss. After the mesh node performs roaming all the data are redirected through the new mesh node or from the new gateway of mesh network.

The mobility of the users in this architecture is provided by the Client Mobile IP or Proxy Mobile IP. The mesh nodes are maintained dynamically in this architecture due to the robustness of the WIMAX mesh architecture. The FA and HA of the mobility management are located at the mesh nodes and master nodes to provide mobility for the users in the presented architecture.

A.3.5. Network Operator and User perspectives

In the architecture users connected doesn't have any interaction with infrastructure of the network. The user authenticate to the access networks, when the users start roaming from one network to another network in the same node the user terminal performs the reauthentication and starts registering to the Home Agent through the foreign agent, continues the session. Wide range of applications like accessing internet, VoIP, Video On Demand and location based services can be introduced by the network operator with this architecture.

A.4. Testbed – Setup, Results

The proposed testbed is composed of Infinet's pre-WIMAX equipment, operating at the frequency rate of 5.4 GHZ. WLAN access consists of Linksys WRT54 and Cisco Aironet AP350. The user terminal used in the testbed is DELL Latitude410 using centrino for wireless. In this section we give brief description about the implementing the proposed solution using WLAN and WIMAX networks, the implemented architecture is shown in Figure 83.

A.4.1. Testbed Setup

As proposed in the architecture part, we have built testbed using WIMAX working in the mesh networks, and WLAN networks connected to different mesh nodes. We initially built a WIMAX mesh network using one of the node as master and all the nodes working as mesh. We installed a gateway at the master node. We configured the mesh nodes so that they can identify and connect to the mesh network when they are range with the other nodes. The nodes calculates the best route to the gateway once it connects to the network. Before connecting to the network the mesh node is authenticated by using private key, this key differs from one node to the other node. The private keys and corresponding MAC addresses of the nodes are maintained at gateway of the network. Once the mesh node is in range of the mesh network it authenticates through the master node to a AAA server which maintains the database of the nodes.

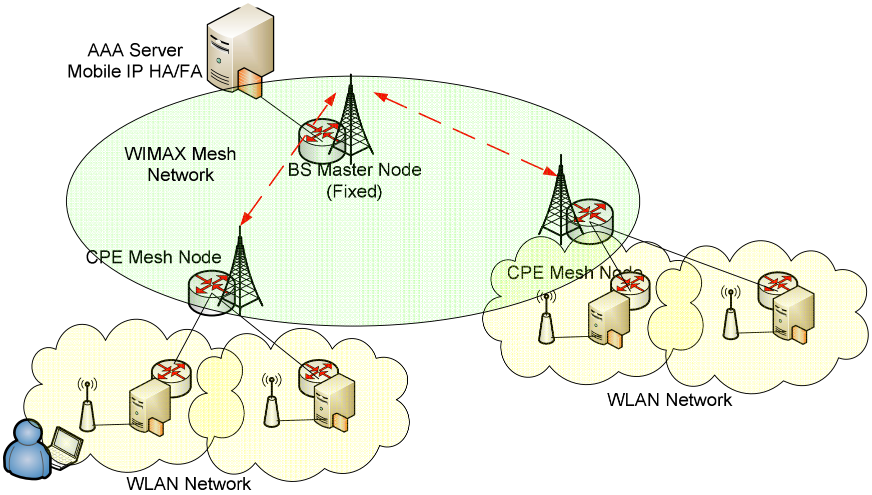


Figure 83. Testbed setup using WLAN and WIMAX

WLAN are connected to the mesh nodes. For the testing purpose we setup 3 access networks using a Linksys AP, and with two other computers acting as a access point using hostap. We also setup the mobility agents in the WLAN networks and at the gateway level. The core AAA server is resided at the other end of the gateway node. Whenever there is any request for authentication, authentication messages are routed to AAA server, after checking with the identity of the subscriber AAA sends granting access to authenticator resided in the WLAN network. Mobility is maintained using dynamics mobile IP in the architecture. On the other hand the client is equipped with WPA supplicant for the authentication over the access networks, it supports the EAP security mechanisms. The client is equipped with the dynamic mobile IP client to register to the FA or the HA when there is a mobility of the client. When a user attempt to access the network, the users are been identified and security mechanisms are initiated and the authentication is been done. After user authorize to the WLAN network UE initiates the mobile IP and registers to the HA (Home Agent) on the WISP network.

For the testing scenario we identified two main scenarios, the first is when the user moves and the second is when the network moves. For the first scenario the user is connected to a WLAN network and authenticates and establishes the mobility registration. And after user starts move from that network the network selection on the mobile terminal of the user identifies the network and start re-authenticating to the access networks. Once it is authenticated its sends the registration request to the HA for the mobility with the help of the FA on WLAN. In the second scenario the user stay connected to WLAN, while the mesh node moves to another topological network or nodes, the mesh node automatically authenticates to the system and establishes the routes and the tunnel with the Master node and gateway. In this scenario user experiences some delay and packet loss.

A.4.2. Results

After setting up testbed and performing some tests, we also calculated different parameters using the testbed in different scenario as shown in the previous section. Total amount of delay is around 6 seconds during initial access to the system from the user which includes network selection, security authentication and registering to the home agent. During the reauthentication the delay is around 4 seconds (NS and reauthentication factor we considered). The delay a user experienced when the network roams is around 2 to 3 seconds.

A.5. Case Study – applicability

We did a case study of the proposed architecture to implement in the realistic scenario. We have chosen French rail network TGV as an ideal contender to implement the proposed solution. The rail network consists around 250 stations which are the ideal to operate as a base station operating as a master nodes, the 400 trains which operated along a network of 1540 kms can be operated with mesh nodes, with a potential users around 1.2 billion per year. On the overall the trains operated and stations form a mesh network. The different compartments in the trains are equipped with WLAN access points which are connected to the WIMAX mesh node. With the proposed architecture a user can connect to the WLAN using onetime password which a user receives from a train ticket or can have a yearly or monthly subscription with SSL certificates, in a secured manner. With proposed solution implemented in the trains the user can access the network in the train while train is moving. He can move from one compartment to another without service interruption, or he can change trains or use the train stations in a seamless manner. With this implementation different types of services can be implemented like VoD, VoIP, location based services, browsing internet etc…, the whole scenario is depicted in Figure 84.

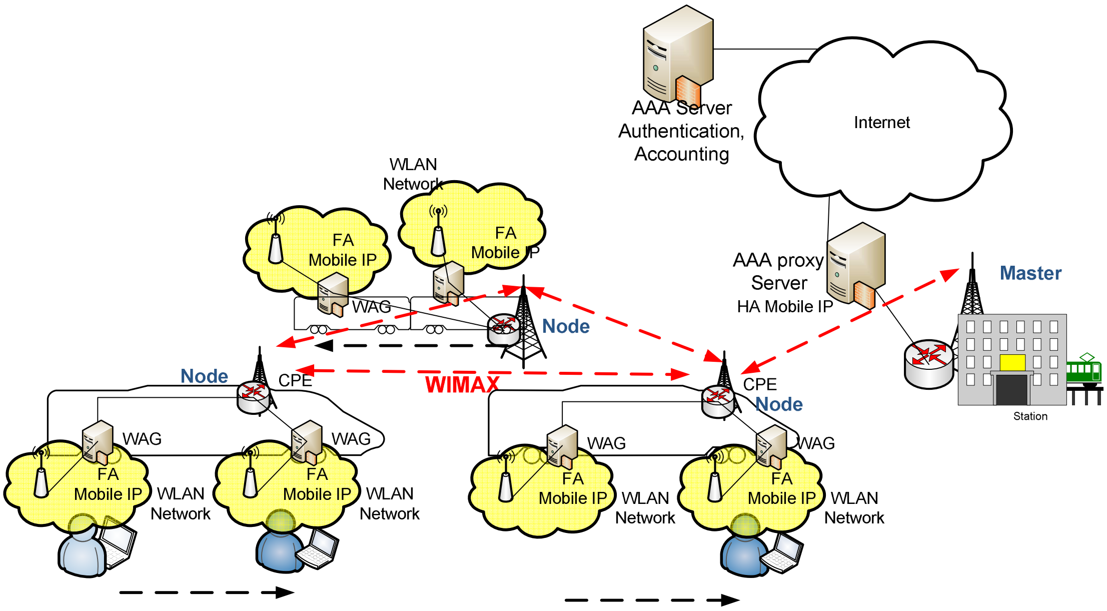


Figure 84. Applicability Scenario of the proposed architecture in the French Rail Network TGV conclusion and future works

A.6. Video on demand using WIMAX networks

In recent years, multimedia streaming over 4G heterogeneous networks is attracting research community and industries. Various multimedia applications (information, entertainment, surveillance, health care, IPTV, Video on Demand), are spread in traditional wired Internet now. To operate these applications in wireless domain some of the key issues like high level availability of bandwidth to run the application, low latency, QoS provisioning must be addressed properly, to cope with high bandwidth requirement of video in both real time and video on demand streaming applications.

Recently, a new concept has appeared, known as urban or municipal TVs using media streaming methods that initiate new ways to establish community communication especially in isolated areas, targeting people who share the same interest information exchange and communication. Instead of using the traditional way communicating using wired network technologies, in this scenario wireless broadband is used as a technology to broadcast content to the users inside a cluster (i.e a rural area). The development of home and handheld devices allowing more facilities to integrate different wireless network interfaces to offer many services that still restricted to fixed network for nowadays users.

Deployment cost of wired networks is very high compared to the Wireless one, especially when it concerns rural and low density areas. The traditional wireless networks uses Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard (loosely termed Wi-Fi), which supports bandwidth speeds up to 11 Mbps (IEEE 802.11b) or 54 Mbps (IEEE 802.11a and 802.11g)-to patch the last-mile gaps. With Wi-Fi technology, mobile users may stay connected via a standards-based connection; WISPs can offer broadband services to geographically challenged areas such as rural towns. In the meantime, Wi-Fi, with a mesh network topology, is more advantageous in both cost-effectiveness and flexibility than its wired counterparts. WISPs use this technology to cover large areas and extend the reach of the local-area network (LAN) for indoor and outdoor applications. Even though, WLAN considered as a cost effective solution for the broadband in this paper, we are proposing in the framework of this an urban TV project POLYMAGE (Figure 85), is to use new wireless technologies and precisely IEEE 802.16 to ensure many services around interactive multimedia streaming and build what a participative urban television. .

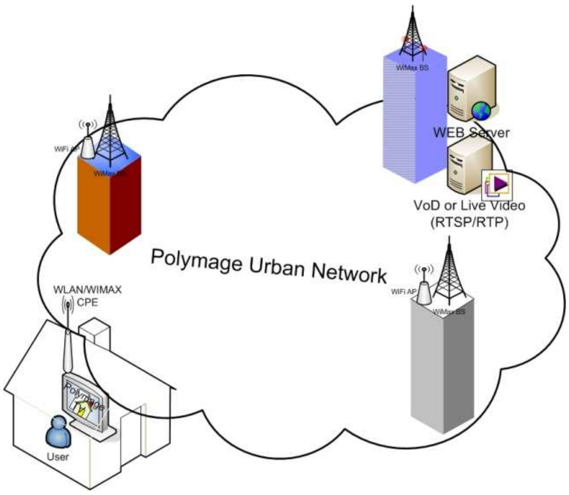


Figure 85. POLYMAGE: Urban TV Project

A.7. Multimedia streaming parameters

In [94] a simulation study of delivery of streaming video on-demand via IEEE 802.16 based technologies is described. The authors used NCTUns on which they added the IEEE 802.16 simulation model; This simulation study proved that IEEE 802.16 can support up to 9/10 simultaneous users streaming typical streaming using H.264/AVC Scalable Video Coding (SVC) and a buffer-based congestion control algorithm in an adaptive video streaming solution. Cicconetti et al [95] evaluate the performance of the 802.16 for two cases - the first based on residential users and second case is on SME users. They focus on the system behavior regarding delay sensitive applications and report useful results which show its ability for various load configurations. In our case we use the WIMAX link for streaming, via multiple video sessions, between the BS and CPE which will redistribute to other networks, essentially over WLAN sub networks.

While one part of the community wants to understand the real capabilities of 802.16 technologies, other researchers are focusing on improvements of the capabilities of video compression methods. The development of H.264/AVC [96] marked an important milestone in this field. The standard employs advanced inter- and intra-prediction techniques such as the use of multiple frames and adaptive block sizes for more efficient motion compensation, and context-adaptive entropy coding. It also includes a considerable amount of error resilience tools to allow for efficient transmission and improved quality in error-prone environments. H.264/AVC was specifically designed for delivery over packet-switched networks, and has been reported to give over 50% gains in coding efficiency compared to MPEG-2. For this reason we adopted it for our experiments.

In the recent past multimedia streaming services development (TVoIP, triple play, interactivity abilities etc) knew a considerable growth among the internet community. TV channels are now able to broadcast on the Internet using video streams, in addition to the Video on Demand services that are available under different forms.

In the wireless realm, media streaming knows some problems like interruption due to the variation of different parameters of the wireless link itself, which results in packet losses and then significant degradation of served media quality. So all optimization to be down for such consideration will be on the wireless network side by tuning the parameters to provide better quality where the User Datagram Protocol (UDP) is used for carrying the media streams. For the reason that it doesn't require any acknowledgement messages moreover when an application level error correction is used.

Multimedia contents such as video are usually enormous in size and stored using servers in the core network. Since the network becomes a bottleneck for the transmission of such amount of data, encoding norms like MPEG-2 and MPEG-4 [97] are used to compress the data, making video transmission lighter. In spite of such encodings, the end-to-end performance still suffers from the unreliable wireless links. Retransmissions and forward error correction schemes have been proposed to shield the effects of the loss medium [98]. Even with such techniques, it is difficult to achieve high data rates (100 Mbps).

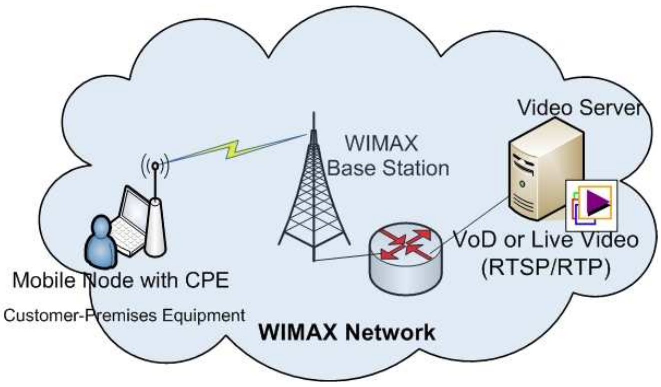


Figure 86. WIMAX Architecture

We built a tesbed to demonstrate the multimedia streaming over WIMAX network. For media streaming we used VideoLan software as a streaming server and client. The proposed test-bed composed of Infinet's pre-WIMAX equipment, working on different parameters settings to measure each time the throughput of multimedia content in the access network. We used two dell computers, with windows XP OS, connected respectively to WIMAX BS and CPE and proceed to different parameters tuning on the equipment during the ongoing video sessions. The videos are streamed from the server at 1024 Kbps using MPEG-4 AVC format encapsulated in TS (Transport Stream) we took this relatively high bit rate to have a significant measurement of the throughput.

A.8. Settings

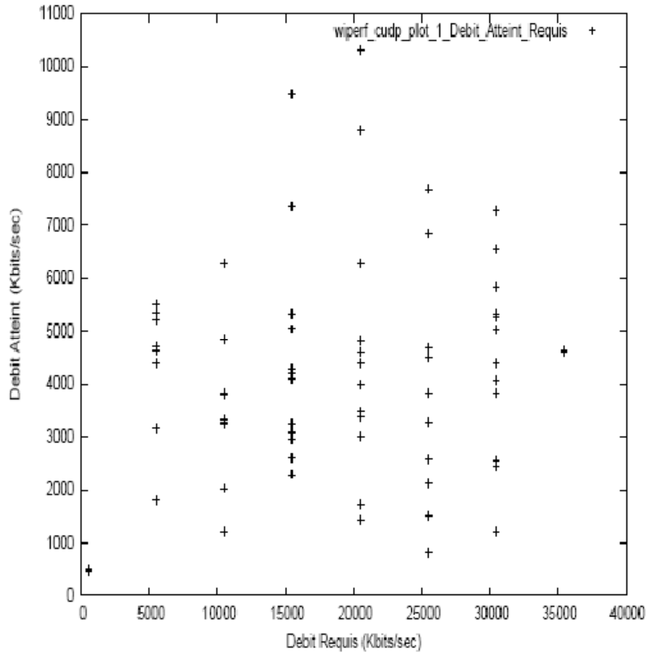
As mentioned earlier we have deployed the WIMAX mesh network in the local testbed. This contains a master, mesh and slave nodes, the users are connected at the different nodes, in this setup the user client is connected to a slave node and the VoD server is resided at the master gateway. In this scenario the slave node configure itself while moving in the network and use the VoD services. We also deployed the integrated WLAN and WIMAX, the total throughput at the user client in this scenario is obtained and presented in the results section.

A.9. Results

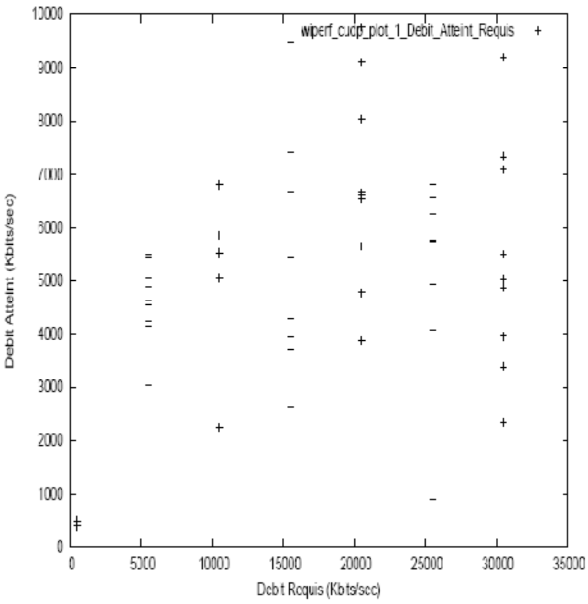
We have deployed different WIMAX deployment scenarios, using different operation parameters we have calculated throughput with different window sizes. Using Wiperf we have obtained results as shown in figure below. Using different QoS operating parameters in a BS for different CPEs the throughput is calculated.

Point à multipoint without priority

CPE 1

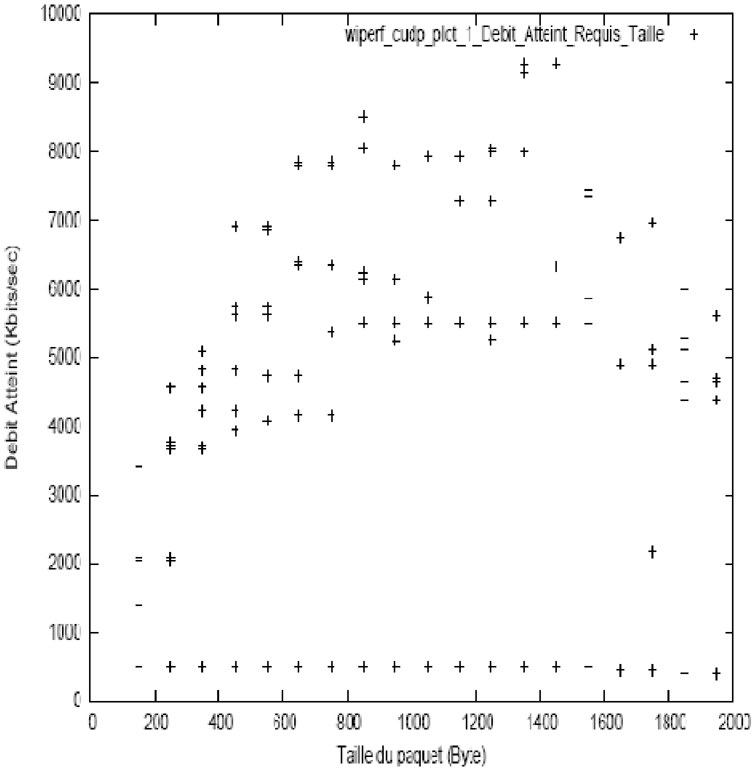


CPE 2

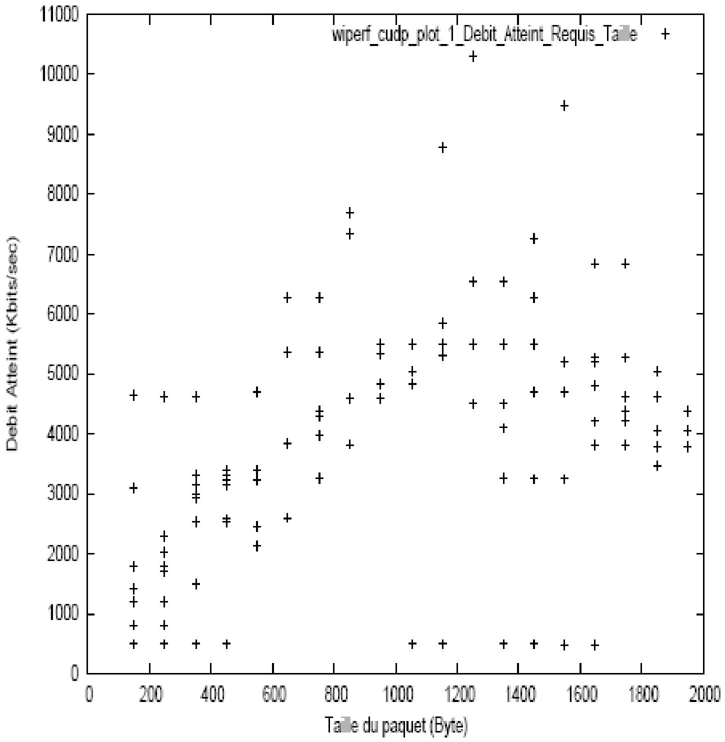


Point to multipoint avec with priority

CPE1 low priority



CPE2 high priority



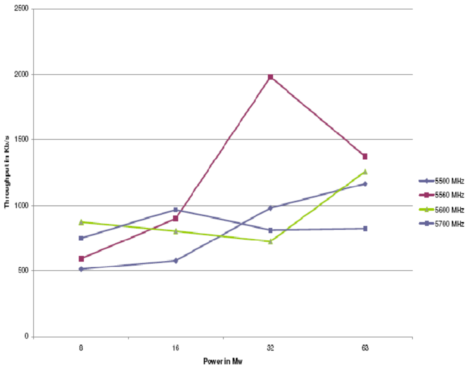


Figure 87. CPE throughput

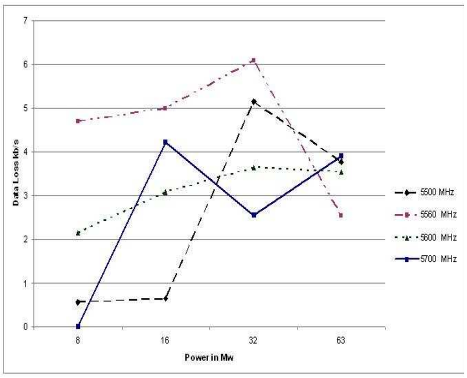


Figure 88. data loss vs power variable frequency

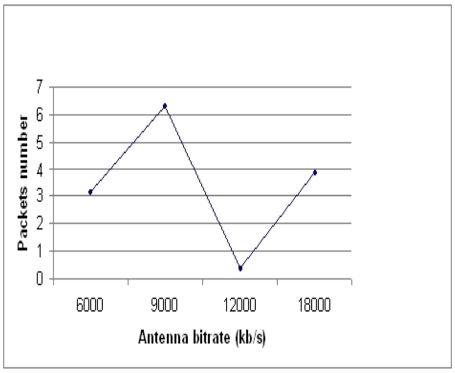


Figure 89. avg packet loss

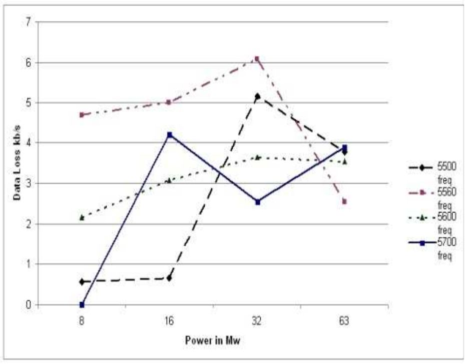


Figure 90. power and variable freq vs packet loss

The measurements are performed when a terminal with a CPE connects to a BS and starts a video session. By varying the frequency of operation and the power level between the CPE and BS we calculated the throughput and quantity of the lost data. Figure 87 shows the graph of the throughput between the CPE and BS at different Frequencies. We have measured at 5500, 5560, 5600 and 5700 Mhz frequencies and power level is about 8, 16, and 32, 63Mw on both CPE and BS. Through the results we observe that throughput varies on a single frequency with different power levels, and on the same power level at different frequency ranges throughput of the video also varied. We also observed at the frequency range of 5560 at the power level of 32 the throughput is at maximum around 2M. We also measured the quantity of the data lost in each power level and for every range of frequency. The values are illustrated in a graph as shown in Figure 88. We observed that there is less data loss for low power level and in the smallest frequencies.

In Figure 89 we measured the number of packets sent per second from the BS to the CPE and we calculated average lost packets between CPE and BS, we can observe that with this video bit rate and in this type of antenna the best bit rate is 12000 kbps. With which ten streams can theoretically be held with a 1024 video bitrate without any buffering. The tests of parallel video streaming sessions prove that WIMAX equipment can carry up to ten video streaming sessions. Figure 90 depicts the available bandwidth after adding gradually 3, 6 and 10 streams to the channel. The allowable remaining bandwidth, measured on the base station, is able to hold more streams, but due to a processor limit caused by video application we succeeded to prove it for 10 parallel streams. Taking the standard parameters and without any optimization mechanisms. From the streaming quality side we observed no loss on the received video as it is shown in Figure 90 then we cans say that up to ten streams there is no need for error correction mechanisms. But for a realistic deployment it is considered mandatory to implement this kind of correction mechanisms.

In Figure 91 the throughput of the video in the normal condition in traditional WIMAX deployment scenario is shown with the time. In the Figure 92 the WIMAX CPE is provided the highest priority than the other deployed CPEs the throughput is shown. In Figure 93 the throughput for CPE with the minimal priority is shown.

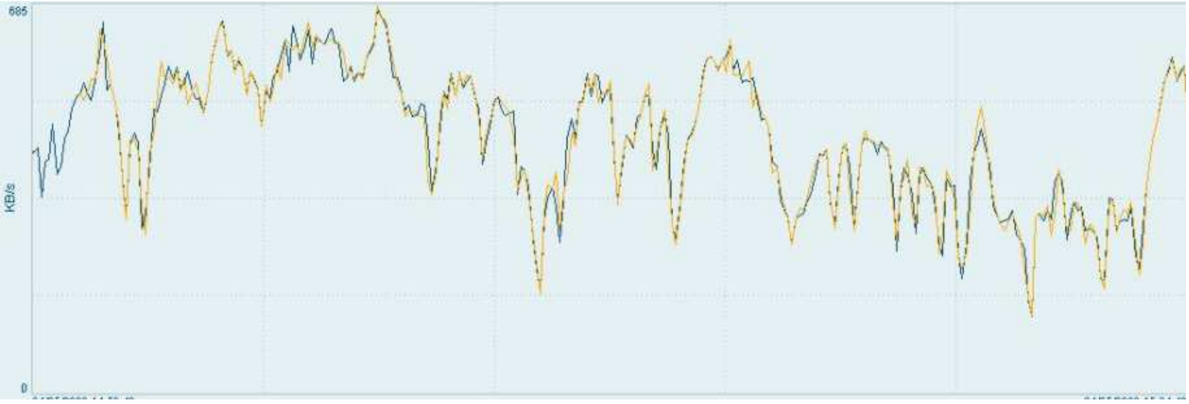


Figure 91. CPE through put in the normal conditions

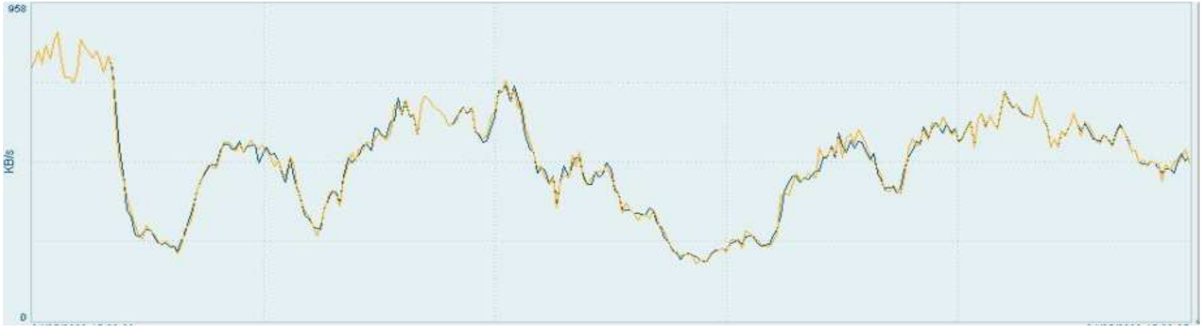


Figure 92. CPE through put with the highest priority

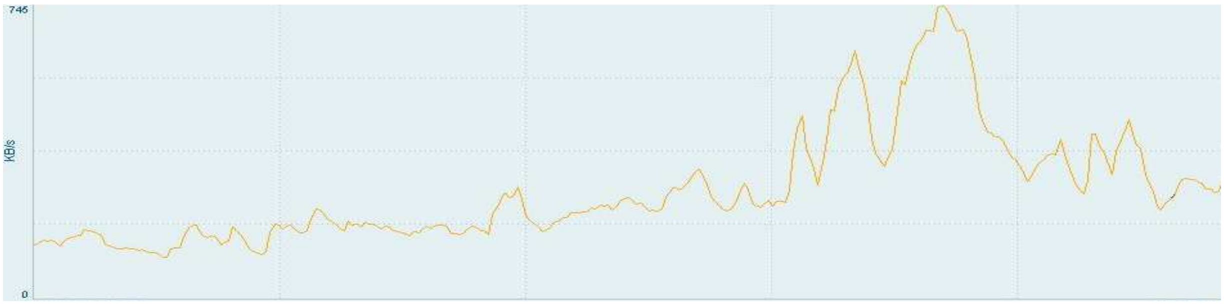


Figure 93. CPE throughput with the low priority

We also obtained the throughput of the client in the mesh deployment scenario as shown in Figure 94, and the integrated multiple WLAN and WIMAX deployment client throughput is shown in Figure 95.

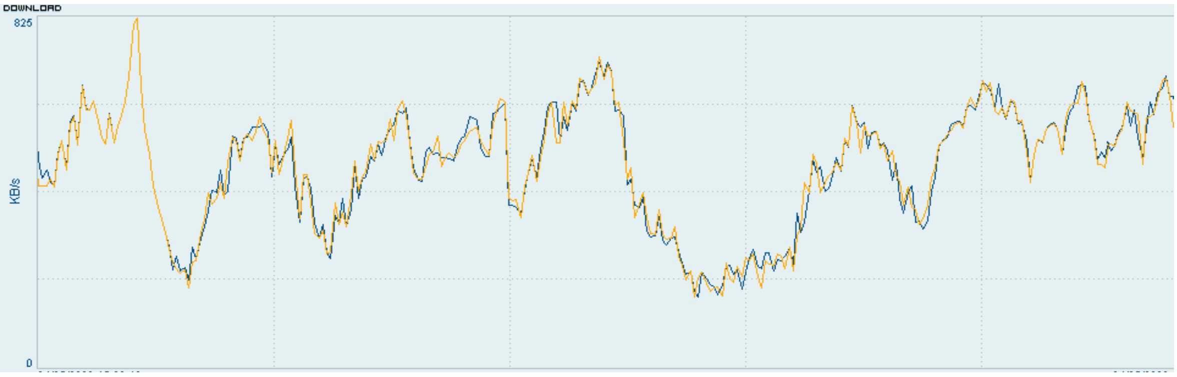


Figure 94. Mesh Node throughput in the WIMAX mesh network deployment

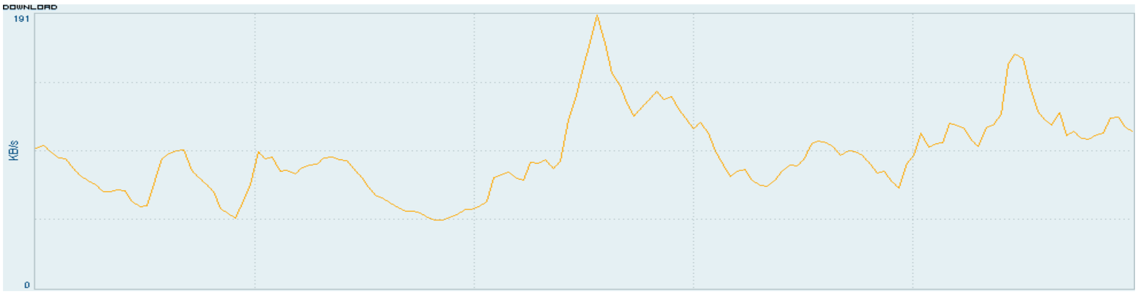


Figure 95. Client throughput connected to WLAN APs in integrated deployment scenario.

A.10. Summary

With the above proposed solution broadband access is achieved in isolated wireless networks. Using two layer security mechanisms proposed architecture is robust and efficient manner. With the centralized architecture network nodes or the users are maintained efficiently. With the above architecture a user can access services VoIP, Video on demand and internet browsing services with high data rates. A user can roam along different access networks with small latency. With the self healing capacity of mesh nodes and gateway mechanisms the nodes in the mesh network perform efficiently with little delay. Even though the proposed solution is efficient and tested using a testbed some of the issues like the load, QoS are not studied in the architecture. To make the proposed architecture robust and reliable we are studying some of the issues like QoS, very large amount of deploying networks, efficiency.

In this chapter, we studied experimentally streaming media possibilities over WIMAX and tuned different parameters present in the 802.16 equipment from both CPE and BS side. We conducted measurement experiments to appreciate the quality of packets reception and throughput on the CPE side. Measurements results demonstrate the effectiveness of the WIMAX parameters variation influence on the video packets delivery on the client side. We also studied different scenario deployments of WIMAX for the urban deployments.

Annex B. Abbreviations

3GPP Third Generation Partners Project

3GPP2 Third Generation Partnership Project 2

AAA Authentication, Authorization and Accounting

ABC Always Best Connected

AHP Analytic Hierarchy Process

AMPS Advanced Mobile Phone System

AP Access Point

APN Access Point Name

AR Access Router

ASN Access Service Network

ASN GW Access Service Network Gateway

BER Bit Error Rate

BPSK Binary Phase-Shift Keying

BS Base Station

BSC Base Station Controller

CBC Cell Broadcast Center

CDMA Code Division Multiple Access

CIP Cellular IP

CoA Care of Address

CN Corresponding Node

CPICH Common Pilot Channel

CRRM Common Radio Resource Management

CSN Connectivity Services Network

D-AMPS Digital Advanced Mobile Phone System

DHCP Dynamic Host Configuration Protocol

DNS Domain Name Server

DSL Digital Subscriber Line

DSSS Direct Sequence Spread Spectrum

DVB-H Digital Video Broadcasting - Handheld

EAP Extensible Authentication Protocol

EDGE Enhanced Data rates for GSM Evolution

FA Foreign Agent

FDD Frequency Division Duplex

FHSS Frequency Hopping Spread Spectrum

GAN Generic Access Network

GANC Generic Access Network Controller

GERAN GSM / EDGE Radio Access Network

GGSN Gateway GPRS Support Node

GSM Global System for Mobile communication

GPRS General Packet Radio Service

GMM GPRS Mobility Management

GSA Global mobile Suppliers Association

GTP GPRS Tunnelling Protocol

FIFO First In First Out

FTTH Fiber To The Home

HA Home Agent

HAWAII HandoAware Wireless Access Internet Infrastructure

HDTV High Definition TV

HIP Host Identity Protocol

HMIP Hierarchical MIP

HLR Home Location Register

HO Handover

HSDPA High Speed Downlink Packet Access

HSUPA High Speed Uplink Packet Access

HSS Home Subscriber Server

IDMP Intra-Domain Mobility Management Protocol

IETF Internet Engineering Task Force

IP Internet Protocol

IPSec IP Security

IMT-2000 International Mobile Telecommunications-2000

ITU International Telecommunication Union

ITU-R Radio Communication Sector of the International Telecommunication Union

IWU InterWorking Unit

LMA Local Mobility Anchor

LMDS Local Multipoint Distribution System

LTE Long Term Evolution

MAC Media Access Control

MAG Mobile Access Gateway

MAP Mobility Anchor Point

MBMS Multimedia Broadcast Multicast Service

MIH Media Independent Handover

MIP Mobile Internet Protocol

MIMO Multiple-Input Multiple-Output

MMDS Multichannel Multipoint Distribution Services

MME Mobility Management Entity

MN Mobile Node

MNO Mobile Network Operator

MOBIKE IKEv2 Mobility and Multihoming

MS Mobile Subscriber

MSC Mobile Switching Center

MVNO Mobile Virtual Network Operator

NMT Nordic Mobile Telephone

OCS Online Charging System

OFDM Orthogonal Frequency Division Multiplexing

OFDMA Orthogonal Frequency Division Multiple Access

PDG Packet Data Gateway

PDN Packet Data Network

PDP Packet Data Protocol

PLMN Public Land Mobile Network

QoS Quality of Service

QPSK Quadrature Phase-Shift Keying

RAN Radio Access Network

RAT Radio Access Technology

RII Roaming Interworking Intermediary

RLS Recursive Least Square

RNC Radio Network Controller

RRC Radio Resource Control

RRM Radio Resource Management

RSS Received Signal Strength

RTP Real-time Transport Protocol

RTT Radio Transmission Technology

SAE System Architecture Evolution

SCTP Stream Control Transmission Protocol

SDMA Space Division Multiple Access

SGSN Serving GPRS Support Node

SIM Subscriber Identity Module

SINR Signal to Inference plus Noise Ratio

SIP Session Initiation Protocol

SLA Service Level Agreement

SM Session Management

SNR Signal-to-Noise Ratio

SOFDMA Scalable Orthogonal Frequency Division Multiple Access

SS Subscriber Station

TACS Total Access Communication System

TCP Transmission Control Protocol

TDD Time Division Duplex

TDMA Time Division Multiple Access

TTG Tunnel Termination Gateway

UDP User Datagram Protocol

UE User Equipment

UMA Unlicensed Mobile Access

UMB Ultra-Mobile Broadband

UMTS Universal Mobile Telecommunications Service

UPE User Plane Entity

UTRA UMTS Terrestrial Radio Access

UTRAN UMTS Terrestrial Radio Access Network

VoD Video on Demand

VoIP Voice over IP

VLC VideoLAN client

VPN Virtual Private Network

WAC Wireless Access Controller

WAG Wireless Access Gateway

WCDMA Wideband Code Division Multiple Access

WIMAX Worldwide Interoperability for Microwave Access

WISP Wireless Internet Service Provider

WLAN Wireless Local Area Network

WMAN Wireless Metropolitan Area Network

Annex C. Publications

C.1. Journals

Vamsi Krishna Gondi, Nazim Agoulmine, "Users and Network management for Secure Interworking & Roaming in WIMAX, 3G and Wi-Fi networks using RII Architecture", The European Journal for the Informatics Professional, special issue on Network Management, Vol. IX, issue no. 6 (December 2008), ISSN 1684-5285

C.2. Book Chapters

Vamsi Krishna Gondi, Nazim Agoulmine, "Secure Interworking & Roaming of WIMAX with 3G and Wi-Fi", IN-TECH, WIMAX New Developments, ISBN978-953-7619 (Publication July 2009)

C.3. Conferences and Workshops

- Vamsi Krishna Gondi, Nazim Agoulmine, "Mobility Management over heterogeneous networks in multi operator access networks using RII architecture", May 2006, HPOVUA, Nice, France.
- Vamsi Krishna Gondi, Nazim Agoulmine, "Secured Roaming over WLAN and WIMAX networks", IEEE IM BCN, May 2007, Munich, Germany.
- Vamsi Krishna Gondi, Nazim Agoulmine, "Ontology-based Network Management in Seamless Roaming Architectures", IEEE Noms BCN 2008, El Salvador, Brazil
- Vamsi Krishna Gondi, Nazim Agoulmine, "Novel mobility solution using PMIP and Radius mobility extensions", IEEE Noms BCN 2008, El Salvador, Brazil
- Vamsi Krishna Gondi, Mehdi Nafaa, Nazim Agoulmine, "Multimedia Streaming in IPTV over 802.16 Experiments: Tesbed Measurements", 1st International Conference on "M4D": Mobile communication technology For Development, 11-12 December, 2008, Karlstad, Sweden.

C.4. Short papers and Posters

- Vamsi Krishna Gondi, Nazim Agoulmine, “Security and Mobility architecture for isolated wireless networks using WIMAX as an Infrastructure”, IEEE IM 2009

- Vamsi Krishna Gondi, Nazim Agoulmine, "Secure Interworking & Roaming Testbed for WIMAX with 3G and Wi-Fi", IEEE IM 2009

C.5. IETF RFC Proposals

- Mobility Management using AAA mobility extensions and Proxy Mobile IPv4, draft-gondi-netlmm-pmip-aaam-00 RFC proposal, IETF NETLMM WG.
- Radius Mobility Extensions, draft-gondi-radext-radius-mobility-00 IETF RFC proposal IETF RADEXT WG in progress.
- Roaming Extensions for radius server draft-gondi-radext-radius-roaming-01, IETF RFC proposal IETF RADEXT WG in progress.
- Handover method using EAP, draft-gondi-hokey-neweap-handover-method-00, IETF RFC proposal, IETF HOKEY WG in progress.

C.6. Project Deliverables

Seimonet (Secure interworking of mobile & wireless networks) is a collaborative research project within the European Celtic programme

- D6.1: State of the art; interworking requirements for mobility, Technical Deliverable Report D6.1, project Celtic SEIMONET 2, 2006.
- D6.2: Seamless interworking mobility architecture solution description, Technical Deliverable Report D6.2, project Celtic SEIMONET, 2007.
- D6.3: Software mobility detailed design document, Technical Deliverable Report D6.3, project Celtic SEIMONET, 2007.
- D7.1 Security and Policy/SA Definition, To identify the technical standards, functional and operational requirements for various access networks, Technical Deliverable Report D7.1, project Celtic SEIMONET, 2007.
- D7.2 Security and Policy/SA Definition, Establish security architecture including AAA, secure user traffic management; signalling gateway, Technical Deliverable Report D7.2, project Celtic SEIMONET, 2007.
- D7.3 Security and Policy/SA Definition, Architecture and Scenario document, Technical Deliverable Report D7.3, project Celtic SEIMONET, 2007.
- D7.4 Security and Policy/SA Definition, Interworking architectures policy, user and network management, databases, Technical Deliverable Report D7.4, project Celtic SEIMONET, 2008.
- D8.1 Integration and Testing, Integration Plan Document, Technical Deliverable Report D8.1, project Celtic SEIMONET, 2007.
- D8.2 Integration and Testing, Integrated architecture detailed Document (Software and WPs Integration) , Technical Deliverable Report D6.3, project Celtic SEIMONET, 2007.

- D8.3 Integration and Testing, Test Execution (Software and Test Report), Technical Deliverable Report D6.3, project Celtic SEIMONET, 2008.

SUMO (Service Ubiquity in Mobile and Wireless Realm) is a collaborative research project within the European ITEA programme.

- D1.1 Identifying different operational scenarios and Business Enablers, Technical Deliverable Report D1.1, project ITEA SUMO, 2006.
- D1.2 SUMO system requirements and basic functional architecture, Technical Deliverable Report D1.2, project ITEA SUMO, 2007.
- D2.1 State of the art; functional and operational requirements, Technical Deliverable Report D2.1, project ITEA SUMO3, 2007.
- D2.2 Seamless service delivery architecture, Technical Deliverable Report D2.2, project ITEA SUMO, 2007.
- D5.1 Technical Demonstrator identify different implementation scenarios and technical requirements, Technical Deliverable Report D5.1, project ITEA SUMO, 2007.

Polymage (French National Project)

Study of Audio and Video deployment and scenarios of deployments using wireless heterogeneous networks, Technical Report, Ploymage.

C.7. Under Review

- Vamsi Krishna Gondi, Nazim Agoulmine "Low Latency Handover Using Security Context Transfer For Heterogeneous Wireless and Cellular Networks", Wiley's Security and Communication Networks Journal, Special Issue on Security in Mobile Wireless Networks
- Vamsi Krishna Gondi, Nazim Agoulmine, "Access Networks Aided Network Selection procedures For Heterogeneous Wireless and Cellular Networks", IEEE WOWMOM 2009.
- Vamsi Krishna Gondi, Nazim Agoulmine, "A novel Mobility solution based on PMIP using AAA mobility extensions in heterogeneous networks", Elsevier, Computers and Electrical Engineering, Special issue on: Emerging Wireless Networks.
- Vamsi Krishna Gondi, Nazim Agoulmine, Mehdi Nafaa "Novel network selection procedures for heterogeneous networking", IEEE IM BCN 2009.
- Vamsi Krishna Gondi, Nazim Agoulmine, Khanh-Toan TRAN "Comparisons of Mobility protocols for Next generation wireless networks", IEEE IM BCN 2009.