THESE

présentée pour obtenir le grade de

Docteur de TELECOM ParisTech

Spécialité: Informatique et Réseaux

Giuliana Iapichino

Architecture et Mécanismes pour le Support de la Mobilité dans l'Internet du Futur

Thèse prévue le 12 Juillet 2010 devant le jury composé de:

Rapporteurs	Prof. Khaldoun Al Agha, Université Paris-Sud, France
	Prof. Marcelo Dias Amorim, Université Pierre et Marie Curie, France
Examinateurs	Prof. Raymond Knopp, EURECOM, France
	Dr. Thierry Ernst, INRIA Rocquencourt, France
	Oscar del Rio Herrero, Agence Spatiale Européenne, Pays-Bas
	Cédric Baudoin, Thales Alenia Space, France
Directeur de thèse	Prof. Christian Bonnet, EURECOM, France

TELECOM ParisTech

EURECOM
Sophia Antipolis

THESIS

In Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy
from TELECOM ParisTech

Specialization: Computer Science and Networking

Giuliana Iapichino

Architecture and Mechanisms to Support Mobility in the Future Internet

Defense scheduled on the 12th of July 2010 before a committee composed of:

Reviewers	Prof. Khaldoun Al Agha, Université Paris-Sud, France
	Prof. Marcelo Dias Amorim, Université Pierre et Marie Curie, France
Examiners	Prof. Raymond Knopp, EURECOM, France
	Dr. Thierry Ernst, INRIA Rocquencourt, France
	Oscar del Rio Herrero, European Space Agency, Netherlands
	Cédric Baudoin, Thales Alenia Space, France
Thesis supervisor	Prof. Christian Bonnet, EURECOM, France

To my parents, my sister and Fran.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my advisor Prof. Christian Bonnet for his brilliant supervision and his continual guidance and support throughout my Ph.D. years. Without his technical insight, his advices and on-going encouragement, this thesis would have never been possible. It has been a real pleasure and privilege for me to have Christian as a mentor, on a working and personal points of view.

I would like to acknowledge the European Space Agency (ESA) and Thales Alenia Space (TAS) for the financial support of my work and to specially thank Oscar del Rio and Giovanni Garofalo from ESA, and Cédric Baudoin and Fabrice Arnal from TAS for giving me this unique opportunity and for their support and guidance.

I am very grateful to my colleagues and friends at Eurecom for opening my eyes to different cultures and points of view, I will always keep wonderful memories of these past years together and of my stay in France. Special thanks go to my dearest friends Sara, Ikbal, Randa, Zuleita and Carina for all the time we spend together talking and supporting each other during this experience, I will never forget. Thanks also to my office mate Rizwan and to his family for their kindness and for their help. I want also to thank Daniele, Nghia, Mariam, Philippe, Kostas, Daniel and Erhan for being present in my professional and personal life.

Finally I want to express my deepest gratitude to my parents and my sister Laura for their unconditional love, patience and boundless encouragements. I am especially indebited to Fran for his love, for supporting my choice of moving to France, for believing in me and for all the sacrifices he did to be close to me as much as possible during the course of this thesis.

Abstract

The evolution of Internet and its hosts does not match anymore the current Internet architecture, designed when mobility, multihoming and security were not considered, and based on Internet Protocol (IP) addresses with the double role of host's identity and host's topological location.

A novel mobility architecture for future Internet is proposed in this work based on Host Identity Protocol (HIP) and Proxy Mobile IPv6 (PMIPv6), and mainly on the two principle ideas behind them. The first idea is the concept of *host identity layer* located between network and transport layer. It provides unique cryptographic identifiers for hosts, called *host identifiers*, which are independent of host's current location and network address. The second idea is to create a *locator* which defines the topological location of a host in a way that is routable in the Internet, but has a specific scheme for routing in the local domain to which the host is attached. From these two basic ideas we have defined a unique architecture where each host has:

- an identifier which uniquely identify the host and which is created as the public key of a public/private key pair, bringing built-in security support;
- one or several locators, depending on the fact of having multiple interfaces and being multihomed; locators are used for routing, but they have different topological semantics depending on the network considered, allowing inherent location privacy.

The result is an architecture which not only has the advantages of HIP and PMIPv6 protocols, such as on one side security, global mobility, multihoming and on the other side local mobility and location privacy, but it includes efficient and dynamic mobility and multihoming scheme at local and global level, ad-hoc networking, traffic engineering and addressing scheme.

The work described in this thesis includes also a practical approach to the two main protocols of the architecture. In particular, PMIPv6 has been completely developed on a real test-bed with all the machines running Ubuntu 7.10 with 2.6.22-15-generic Linux kernel and reusing Mobile IPv6 for Linux (MIPL) v.2.0.2. The aim of the implementation has been not only to use it for the architecture, but also to provide to mobile network operators a clear implementation analysis which takes into account all the important recommendations for respecting the standard RFC 5213 and, at the same time, for reducing handover delays. The implementation is fully compliant with the standard and with the directives provided in the standard. For the first time, PMIPv6's implementation issues such as layer 2 attachment and detachment, unicast Router Advertisement messages, default router detection and tunneling have been considered to evaluate their impact on protocol's performances. As regards HIP protocol implementation, the open source Host Identity Protocol for Linux (HIPL) v.1.0.4-48 developed for InfraHIP project by several universities and research groups in Finland has been used. It runs on user-space on Linux kernel, exactly as our PMIPv6 implementation. The two protocol have been combined to test and to prove through experimental results the feasibility of the proposed system architecture.

Finally, this thesis applies the proposed architecture to Public Safety Applications. The problem of supporting mobility at the disaster site to rescue teams equipped with different heterogeneous access technologies and providing interoperability between different agencies and jurisdictions is still under investigation by research communities worldwide. A satellite and wireless mesh network architecture is proposed for emergency mobile communications in which HIP and PMIPv6 represent a secure global and localized mobility solution for the heterogeneous ad hoc mesh network deployed at the disaster site and communicating with the headquarters via satellite. This solution provides also an efficient mechanism of intra and inter-technology handover for Public Safety users equipped with heterogeneous devices at the disaster field and secure end-to-end connections for communications at the disaster area and with the headquarters.

Contents

List of Figures

List of Tables

Acronyms

Here are the acronyms used in this dissertation. They are also defined when they first appear in the text.

3G	Third Generation
3GPP	Third Generation Partnership Project
4G	Fourth Generation
BE	Base Exchange
CoA	Care-of Address
CN	Correspondent Node
EDGE	Enhanced Data rates for GSM Evolution
GMM	Global Mobility Management
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
GTP	GPRS Tunnelling Protocol
HA	Home Agent
HIP	Host Identity Protocol
HIPL	Host Identity Protocol for Linux
HLR	Home Location Register
HoA	Home Address
HNP	Home Network Prefix
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
LMA	Local Mobility Anchor
LMM	Local Mobility Management
LTE	Long Term Evolution
MAG	Mobile Access Gateway
MIH	Media Independent Handover
MIPv6	Mobile IPv6
MIPL	Mobile IPv6 for Linux

MN	Mobile Node
PBA	Proxy Binding Acknowledgement
PBU	Proxy Binding Update
PMIPv6	Proxy Mobile IPv6
RA	Router Advertisement
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

Résumé

Introduction

Les principes de base de l'architecture de l'Internet comprennent l'adressage de bout-en-bout, le routage global et une seule règle pour les adresses IP, qui agissent à la fois comme des localisateurs et des identificateurs de nœuds. Ces principes sont adaptés à des réseaux statiques et hiérarchiques. Cependant, Internet, initialement conçu comme un réseau de recherche, a évolué pour devenir un réseau d'échange d'informations mondial, impliquant une diversité croissante des échanges commerciaux, et des intérêts sociaux, ethniques et gouvernementaux, qui ont conduit à de plus en plus d'exigences contradictoires entre les acteurs en compétition. Ces conflits créent des tensions auxquelles l'architecture de l'Internet tente de résister.

Le succès commercial et l'utilisation généralisée de l'Internet ont conduit à de nouvelles exigences pour l'Internet du futur. Ces exigences comprennent l'interconnexion aux frontières des entreprises, la mobilité, la multi-domiciliation, et la sécurité pour les environnements non sécurisés. Simultanément à cette recherche de nouvelles architectures Internet, la demande pour les réseaux privés et autonomes s'est accrue. Bien qu'ils restent connectés à l'Internet mondial, ces réseaux autonomes offrent des caractéristiques et des capacités locales qui sont indépendantes de l'Internet public. La solution actuelle pour atteindre une plus grande autonomie est appelée Network Address Translators (NAT). Cette méthode, qui est largement utilisée, vise à réutiliser l'espace d'adressage et à découpler le routage des réseaux privés du routage de l'Internet publique. Bien que les capacités du NAT atténuent de multiples problèmes immédiats, les NATs ne sont pas considérés comme une solution "propre".

Les problèmes fondamentaux du protocole IP proviennent de la combinaison de deux fonctionnalités distinctes sur l'adresse IP. L'une est son utilisation comme localisateur, pour exemple comme une adresse qui désigne un emplacement dans la topologie du réseau et spécifie un point de raccordement au réseau. La seconde est celle d'un identificateur qui décrit l'identité du nœud. Le problème avec l'approche NAT est qu'elle fait la traduction entre adresses internes et externes, et avec cela, implicitement la traduction entre les identités associées. Cela provoque la rupture des applications et des protocoles qui échangent des adresses IP, tels que FTP.

Le problème avec l'adressage du point d'attachement au réseau est que la plupart de hôtes ont plus d'une capacité de communication, et avec elle, la possibilité de joindre le réseau par plusieurs interfaces. Cette multi-domiciliation implique que l'hôte se manifeste par plusieurs adresses d'interface, et donc avec des identités multiples.

Le principal objectif de l'intégration de plusieurs technologies d'accès, à la fois avec et sans fil, dans les nouveaux équipements livrés sur le marché, est de fédérer tous les moyens de communication afin de pouvoir accéder à l'Internet de façon ubiquitaire (partout et à tout moment) en l'absence d'une technologie unique déployée universellement. Le flux de trafic peut ainsi être redirigé d'une interface à l'autre suite à la perte de la connectivité ou d'un changement des conditions du réseau dans des milieux d'accès différents. En plus de permettre l'omniprésence de l'accès à l'Internet, l'intégration de plusieurs technologies d'accès permet également l'augmentation de la disponibilité de bande passante et la sélection de la technologie la plus appropriée en fonction du type de flux ou du choix de l'utilisateur (chaque moyen d'accès a des coûts, des performances, une bande passante, un accès, et une fiabilité différents).

Une fois les accès multiples offerts, les utilisateurs peuvent sélectionner les interfaces réseaux les plus appropriées en fonction de l'environnement du réseau, en particulier dans les réseaux sans fil qui sont fluctuantes et moins fiables que les réseaux filaires. L'utilisateur peut aussi sélectionner l'interface la plus appropriée pour le type de communication ou combiner un ensemble d'interfaces pour obtenir une bande passante suffisante.

La nouvelle conception de l'Internet devrait essayer de répondre aux attentes des utilisateurs, conformément aussi aux exigences des deux autres catégories d'acteurs de l'Internet actuel: les opérateurs de réseaux d'accès et les opérateurs d'origine. Les utilisateurs utilisent des hôtes pour lesquels ils désirent une connectivité à Internet efficace, disponible et fiable. Les opérateurs de réseaux d'accès fournissent l'infrastructure que les hôtes ont besoin pour communiquer, collectivement appelés "bord du domaine". Un réseau d'accès peut router des paquets indépendants entre deux hôtes joints, mais pour la connectivité Internet internationale, il doit se connecter à un opérateur d'origine avec son fournisseur. Les fournisseurs forment ensemble un "domaine de base" par lequel les paquets peuvent être échangés entre les réseaux d'extrémités. Les opérateurs de réseaux d'accès sont naturellement enclins à répondre aux attentes des utilisateurs, car ils ont une relation contractuelle directe avec les utilisateurs. Ils ne devraient donc pas dépendre des fonctions d'un opérateur externe pour fournir leur propre connectivité et services de mobilité, tandis que les opérateurs d'accueil devraient se concentrer sur le service à la clientèle et s'appuyer sur les opérateurs d'accès multiples pour offrir à leurs utilisateurs une gestion de la mobilité locale efficace.

Architecture pour la mobilité basée sur HIP et PMIPv6

L'architecture proposée pour la mobilité future de l'Internet est basée sur deux protocoles, HIP et PMIPv6, et principalement sur deux idées principales qui sont à l'origine de ces protocoles. La première idée est le concept de la *couche d'identité* du terminal située entre la couche réseau et la couche transport. Elle fournit des identifiants cryptés uniques pour les terminaux, appelés *host identifiers*, qui sont indépendants de la position et de l'adresse réseau. La deuxième idée consiste à créer un *localisateur* qui définit l'emplacement topologique d'un terminal mobile de manière à ce qu'il soit routable dans l'Internet, mais qui a un régime spécifique pour le routage dans le domaine local auquel l'entité mobile est attachée. A partir de ces deux idées de base, nous avons défini une architecture unifiée où :

- chaque terminal a un identificateur qui l'identifie de façon unique et qui est créé comme la clé publique d'une paire de clés publique/privée, avec prise en charge intégrée de la sécurité;

- un ou plusieurs localisateurs, selon le fait d'être ou non multi-domicilié et d'avoir une ou plusieurs interfaces; les localisateurs sont utilisés pour le routage, mais ils ont des sémantiques topologiques différentes selon le réseau considéré, ce qui permet une confidentialité inhérente de la position.

Le résultat est une architecture qui, non seulement bénéficie des avantages de HIP et de PMIPv6, tels que la sécurité, la mobilité globale, la multi-domiciliation d'un coté et la mobilité locale et la confidentialité de la localisation de l'autre, mais encore comprend une mobilité et une multi-domiciliation efficace et dynamique aux niveaux local et global, réseau ad hoc, ingénierie de trafic et d'adressage.

L'architecture est conçue en gardant à l'esprit les exigences de l'Internet et des opérateurs dans l'avenir. Pour cette raison, nous avons séparés le design en deux parties:

- le cœur de réseau dans lequel sont situés les opérateurs d'origine avec leurs fournisseurs ;
- le réseau de bord où les Local Mobility Domains (LMDs) sont situés. Un LMD est associé à un Access Network Provider (ANP) et à un ou plusieurs Wireless Access Networks (WANs), ayant des technologies d'accès identiques ou différentes.

Le cœur de réseau a des connexions multiples avec le réseau de bord, et est géré par quatre éléments de base:

- le Domain Name Server (DNS), qui a la fonctionnalité de résoudre les Fully Qualified Domain Names (FQDN) avec les host identifiers et les localisateurs correspondants;
- le Rendez-Vous Server (RVS), qui est l'entité qui enregistre des localisateurs associés à un host identifier;
- le Local Mobility Anchor (LMA), qui représente le point d'accès du LMD et le point d'ancrage topologique des hôtes dans le LMD;
- le Mobility Access Gateway (MAG), qui est le routeur d'accès du WAN et gère la signalisation liée à la mobilité pour les hôtes attachés à son lien d'accès.

L'architecture d'ensemble est illustrée dans la Fig. 1.

Schéma pour l'adressage

L'adresse IPv6 (la localisation) configurée par le nœud dans l'architecture pour la mobilité est obtenue par le biais du protocole PMIPv6. Quand un hôte s'attache à un domaine PMIPv6 (à un LMD dans cette architecture), le MAG sur le lien d'accès effectue une procédure d'authentification d'accès avec un serveur de politiques en envoyant l'identificateur du nœud. Le MAG reçoit le profil de l'hôte mobile, qui contient le Home Network Prefix (HNP), l'adresse de LMA et d'autres paramètres de configuration. Ensuite, le MAG envoie au LMA un message Proxy Binding Update (PBU) au nom de l'hôte mobile comprenant l'identificateur de l'hôte, son HNP et l'adresse MAC de

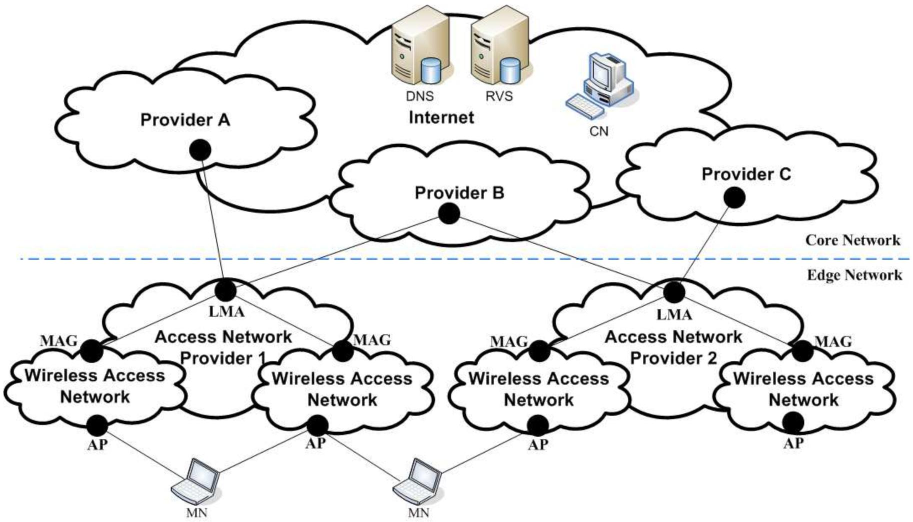

Figure 1: Architecture pour la mobilité.

l'interface utilisée. En acceptant le message, le LMA répond avec un message Proxy Binding Acknowledgement (PBA), et il crée une Binding Cache Entry (BCE) avec l'identifiant de l'hôte, son HNP, le localisateur (créé à partir du HNP et de l'adresse MAC) et l'adresse du MAG. Ensuite, le MAG et le LMA créent un tunnel bi-directionnel IP-dans-IP pour le routage du trafic du nœud mobile. Comme dernière étape, le MAG envoie un message Router Advertisement (RA) au nœud mobile avec le HNP comme préfixe de lien d'accueil. Sur réception de ce message, l'hôte mobile configure son interface en utilisant l'un des modes de configuration d'adresse avec ou sans état. L'hôte mobile termine avec une adresse de son HNP qu'il peut utiliser lors de ses déplacements dans le domaine PMIPv6.

Résolution de nom

La procédure de résolution de nom commence par un FQDN, que les nœuds résoudront via le DNS. Le DNS renvoie l'identifiant de l'hôte mobile et le localisateur de son RVS. Avec ces deux informations, la communication entre pairs peut commencer. Le premier message de l'échange Base Exchange (BE) (I1) envoyé par le nœud correspondant (CN) passe par le RVS qui le redirige vers le localisateur de MN. Une fois que l'hôte mobile a reçu le paquet, il peut répondre au CN directement avec son localisateur. Le reste de l'échange BE (R1, I2, R2), dédié à l'établissement des Associations de Sécurité (SA) peut se faire par communication directe entre pairs.

Sécurité

La nature cryptographique des identificateurs d'accueil est la pierre angulaire de la sécurité de l'architecture HIP ainsi que de notre architecture. Chaque point final génère exactement une paire de clés publiques. La clé publique de la paire de clés fonctionne comme l'identificateur de l'hôte. Chaque hôte conserve la clé privée secrète correspondante et ne la divulgue à personne. L'utilisation de la clé publique comme nom permet de vérifier directement si la partie est effectivement en droit d'utiliser le nom. Un simple protocole d'authentification par clé publique, comme le schéma Diffie-Hellman inclus dans le HIP, est suffisant pour cela. Ceci est accompli avec un échange en quatre messages, composé de messages I1, R1, R2 et I2. Après ces échanges de messages, les deux hôtes savent que l'autre est en effet l'entité qui possède la clé privée qui correspond à son identificateur d'hôte. En outre, l'échange crée une paire d'Associations de Sécurité (SA) IPSec Encapsulated Security Payload (ESP) , une dans chaque direction. Les hôtes utilisent les SAs ESP pour protéger l'intégrité des paquets circulant entre eux.

Confidentialité de la localisation

L'architecture standard HIP ne fournit pas de confidentialité de la localisation, car les informations sur le localisateur contenues dans les messages BE ne sont pas cryptées et peuvent être divulguées par des tiers. En outre, il existe des scénarios dans lesquels même les CN ne devraient pas être au courant de l'emplacement exact de leurs correspondants. Dans l'architecture pour la mobilité proposée, même si le localisateur est divulgué par des pairs ou des tiers, il est configuré de manière à ce qu'il pointe toujours sur le LMA du LMD où l'hôte mobile est situé, mais ne révèle pas la position exacte de l'hôte. Seul le LMA est en mesure de localiser l'hôte et de router les paquets à lui. En particulier, la BCE du LMA contient des entrées pour chaque hôte attaché au LMD, avec le MAG associé correspondant.

Mobilité

Le schéma de mobilité globale et locale de notre architecture est une combinaison de HIP et PMIPv6. En ce qui concerne la mobilité globale, quand l'hôte mobile se déplace d'un LMD à un autre, il obtient par le biais du PMIPv6 une nouvelle HNP (HNP2), qui est utilisée pour créer un nouvel emplacement (localisation 2). Comme dans le standard HIP, l'hôte mobile

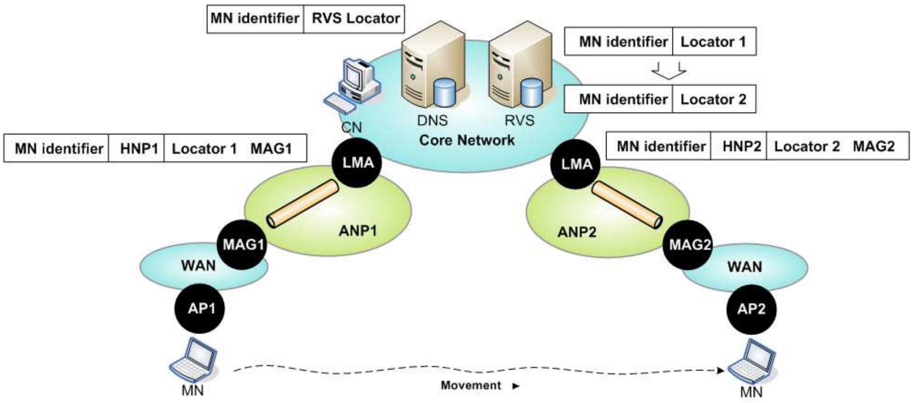

Figure 2: Mobilité globale.

doit mettre à jour le RVS avec son nouvel emplacement comme dans la Fig. 2.

Le cas de la gestion de la mobilité locale suit exactement la procédure PMIPv6. Chaque LMD fournit toujours la même HNP à l'hôte mobile quelle que soit l'interface utilisée, car la HNP est liée à l'identifiant du l'hôte mobile. Le LMA met à jour la BCE avec les informations correctes de localisation et avec le MAG associé à l'identifiant de l'hôte mobile et le HNP, comme le montre la Fig. 3. Dans ce cas, il n'est pas nécessaire pour l'hôte mobile d'actualiser le RVS, car le localisateur enregistré dans le RVS est toujours routable au LMA.

Multi-domiciliation

Au niveau global, la multi-domiciliation consiste en l'enregistrement par l'hôte mobile dans la base de données du RVS de multiples localisateurs (un par LMD) associés au même identifiant, comme illustré sur la Fig. 4.

Au niveau local, c'est le LMA qui tient à jour son BCE en associant les multiples localisateurs à l'identifiant et au HNP du MN. Même si l'hôte mobile est multi-domicilié au niveau local, les entités externes, telles que le RVS et CNS, ne sont pas conscientes de cela, comme illustré dans la Fig. 5.

Réseau ad-hoc

Nous avons également considéré le cas dans lequel, au lieu d'avoir juste un hôte mobile attaché au LMD, il y a un réseau ad-hoc. Les nœuds dans le réseau ad-hoc peuvent partager un identifiant commun, appelé Group Identifier (GI), qui peut être utilisé dans le PBU au lieu de l'identificateur

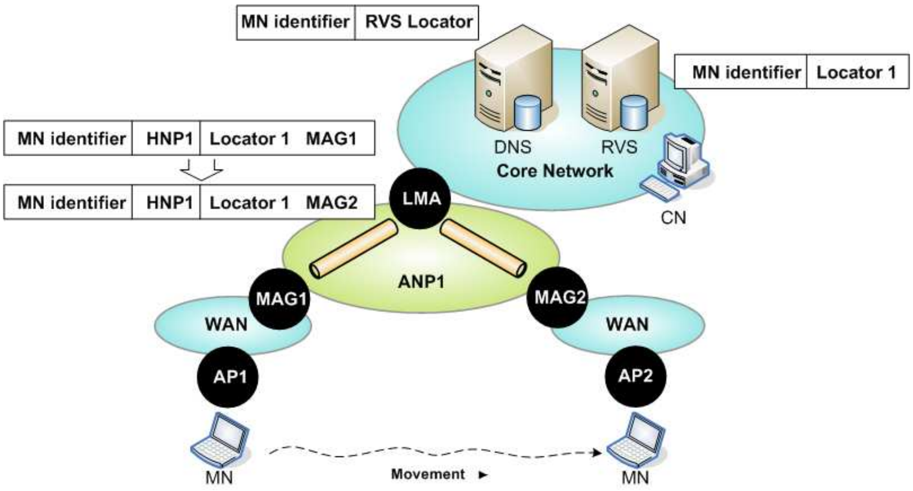

Figure 3: Mobilité locale.

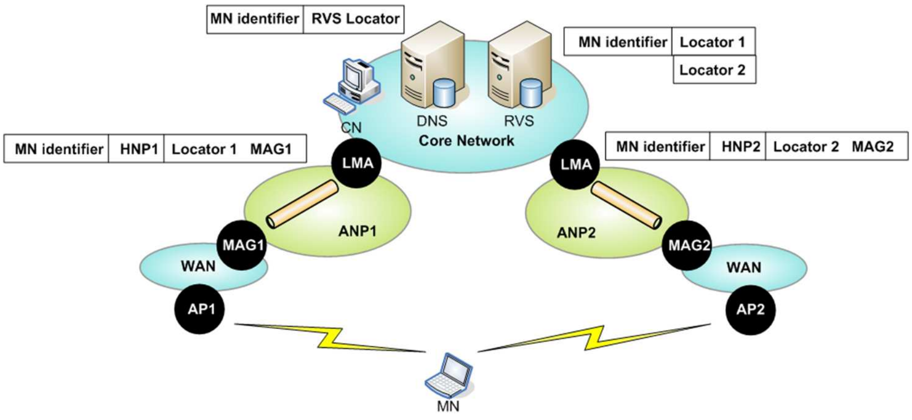

Figure 4: Multi-domiciliation au niveau global.

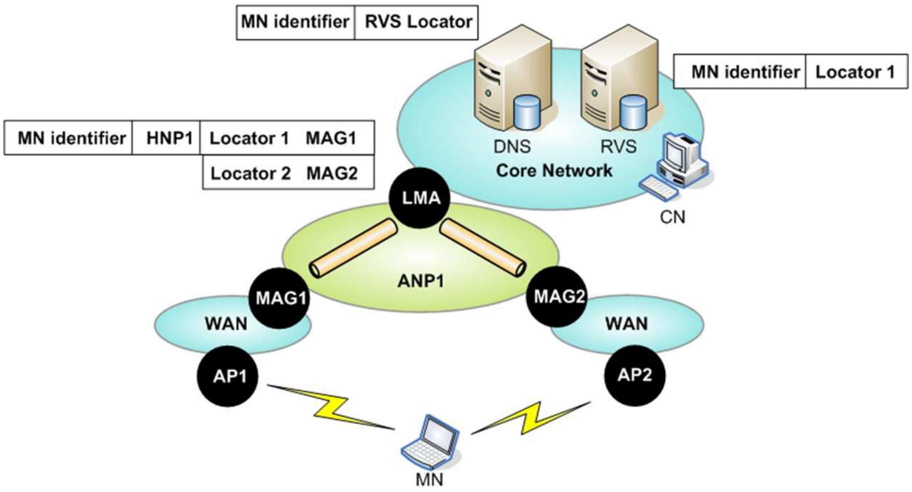

Figure 5: Multi-domiciliation au niveau locale.

d'hôte. La structure de données du BCE maintenu par le LMA, peut être étendue pour le stocker, et contenir le HNP correspondant au GI. De cette façon, le HNP est partagé par tous les nœuds du réseau ad-hoc, qui l'utilisent pour configurer leurs adresses IPv6. Tout le trafic ayant comme adresse de destination une adresse avec cette HNP est routé par le LMA vers le MAG servant le réseau ad-hoc, et ensuite par le MAG vers le réseau ad-hoc, qui se servira de son protocole de routage interne ad-hoc pour livrer le trafic vers l'hôte mobile correct.

Routage

Le routage dans le cœur et dans les réseaux de bord est fait de deux manières différentes. Alors que dans le cœur, il peut être basé sur un protocole standard de routage de l'Internet, le routage dans les LMDs est entièrement basé sur les informations contenues dans la BCE de chaque LMA. Le LMA peut router les paquets pour l'hôte mobile vers le MAG correct en fonction de l'adresse IPv6 destination (Locator) ou, dans le cas où il n'y a pas d'entrée pour elle, vers la HNP.

Ingénierie du trafic

Le LMD peut silencieusement décider de déplacer le trafic de l'hôte mobile d'un WAN à l'autre. Dans notre architecture, ceci est possible grâce à la distinction entre localisateur et identification, et au fait que les SAs sont liées aux identificateurs et non pas aux localisateurs. Même si l'adresse IP de l'interface sur laquelle l'hôte mobile reçoit les paquets est différente de l'adresse de destination des paquets, l'hôte mobile peut accepter le trafic de données dans la mesure où le même HNP est utilisé dans l'adresse de destination. Dans le même temps, l'hôte mobile peut choisir, en fonction des circonstances, de déplacer le trafic d'une interface à une autre, donc d'un WAN à un autre. L'hôte mobile peut exprimer ses préférences dans le message UPDATE, précisant quel flux il souhaite déplacer et de quelle interface à quelle autre.

Implémentation de l'architecture pour la mobilité

Les deux protocoles, PMIPv6 et HIP, ont été implémentés et combinés sur un véritable banc d'essai au laboratoire Eurecom, afin de prouver la faisabilité de l'architecture pour la mobilité proposée.

Implémentation de Proxy Mobile IPv6

PMIPv6 a été entièrement développé sur un test-bed réel avec tous les ordinateurs exécutant Ubuntu 7.10 avec le noyau Linux 2.6.22-15-generic et la réutilisation de Mobile IPv6 pour Linux (MIPL) v.2.0.2. Toutes les briques de base de MIPL sont utilisées de manière efficace comme le montre la Fig. 6.

Dans MIPL, Mobile IPv6 est implémenté en utilisant un système multi threads: un pour la manipulation des messages ICMPv6, un pour le traitement des messages Mobility Header, et un autre pour le traitement des tâches et des événements en temps. Pour développer PMIPv6, nous avons étendu ces éléments et mis en œuvre toutes les procédures nécessaires pour la gestion des messages et des événements. Les messages ICMPv6 et Mobility Header sont analysés par le Handler comme entrées pour le Finite State Machine, qui est le cœur du système. Deux Finite State Machines différentes sont définies pour le LMA et le MAG. Elles sont chargées de prendre des décisions appropriées et de contrôler tous les autres éléments pour fournir un comportement correct du protocole. Le PMIPv6 Binding Cache stocke toutes les informations sur les points d'attachement des hôtes mobiles et est régulièrement mis à jour selon la mobilité des hôtes mobiles.

Comme l'implémentation de PMIPv6 est construite sur MIPL v.2.0.2, il pourrait être, dans l'avenir, facilement intégré dans MIPL, en devenant de plus en plus en ligne avec les normes ainsi que le code source de MIPL.

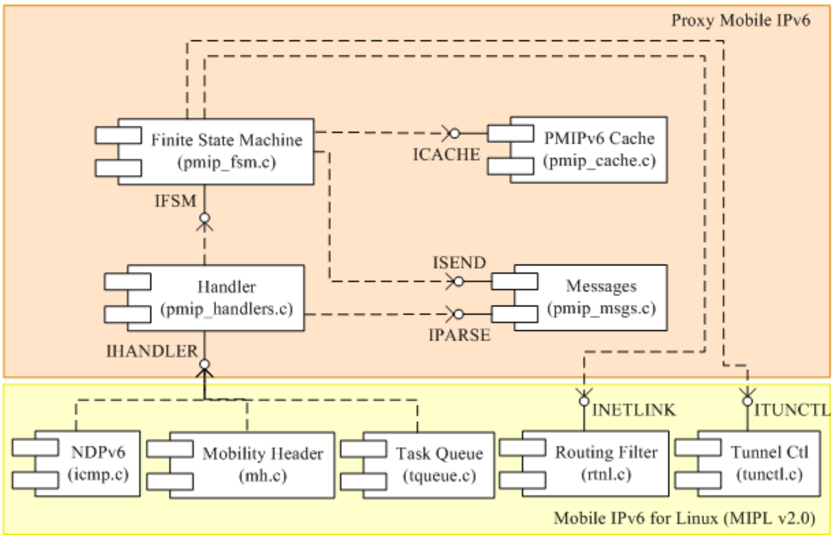

Figure 6: Architecture du software PMIPv6.

La Figure 7 montre la topologie expérimentale de notre test-bed. Un hôte mobile non modifié, qui n'a pas de logiciel spécifique pour la mobilité, utilise son Netgear Wireless Card pour s'attacher à l'un des deux Cisco Aironet 1100 series Access Points (APs), qui supportent les spécifications IEEE 802.11a/g. Chaque AP est directement lié à un MAG. L'implémentation des fonctionnalités de MAG contient des fonctions supplémentaires et des modifications de MIPL pour traiter les messages PBU et PBA et les options de mobilité, et une modification du Router Advertisement daemon (RADVD), qui envoie en unicast des RA avec un HNP spécifique par nœud. Chaque MAG est relié au LMA. Le LMA est configuré comme un HA modifié dans MIPL, qui stocke un unique HNP dans la BCE pour chaque hôte mobile et est capable de gérer les messages PBU et PBA. Enfin, un CN non modifié est relié au LMA. Toutes les entités dans le test-bed exécutent Ubuntu 7.10 avec le noyau Linux 2.6.22-15-generic.

Dans ce travail, nous considérons les contraintes pratiques les plus importantes auxquelles nous ayons été confrontées lors de l'implémentation de la norme PMIPv6 dans un test-bed réel. Elles peuvent être résumées comme suit:

1. **Phases d'attachement et de détachement:** le standard du PMIPv6 ne précise pas toutes les fonctionnalités de ces deux phases, car son but principal est de définir uniquement les éléments et les messages de signalisation à l'intérieur du domaine PMIPv6. Une possibilité

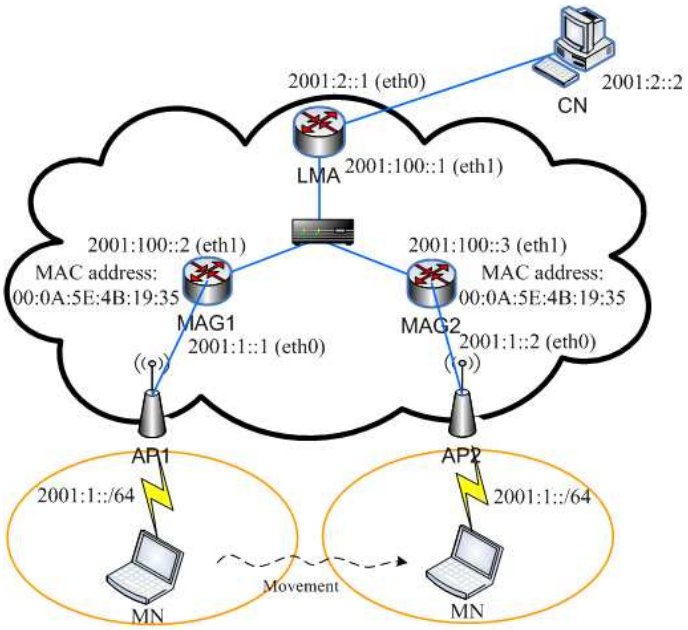

Figure 7: Topologie du test-bed.

est d'utiliser une solution basée sur la couche IP, la seconde consiste à élaborer un mécanisme spécifique de couche de liaison. Nous avons choisi la deuxième option, parce que l'utilisation de déclencheurs situés en couche 2 permet une détection plus rapide de mouvement. Nous avons utilisé les messages Syslog envoyés par les points d'accès Cisco au MAG et contenant les informations de “associate”, “disassociate” et “reassociate” pour détecter les “attachements” et les “détachements” de l'hôte mobile dans le domaine PMIPv6. Dans l'avenir, nous intégrerons notre implémentation de PMIPv6 avec le standard IEEE 802.21 Media Independent Handover (MIH), afin de bénéficier d'un mécanisme de collecte des informations provenant de divers types de liens et de réseaux associés fonctionnant d'une manière opportune et cohérente, et de livrer ces informations à des entités de la couche réseau.

2. **Unicast RA:** comme le HNP est unique par hôte mobile, il doit être envoyé dans un message unicast RA par le MAG à l'hôte mobile spécifique. Nous avons développé et intégré dans le démon de PMIPv6 des MAGs basé sur le démon RADVD une fonctionnalité permettant l'envoi unicast de RA. L'adresse de l'hôte mobile est con-

figurée automatiquement par la fonction IPv6 Stateless Address Auto Configuration.

3. **La configuration de l'adresse de lien local du MAG:** : le MAG est le routeur IPv6 par défaut du nœud mobile sur le lien d'accès. Toutefois, comme l'hôte mobile se déplace d'un lien d'accès à un autre, les MAGs de ces liens respectifs envoyent les messages RA. Si ces RA sont envoyés en utilisant une autre adresse de lien local ou une autre adresse de couche de liaison, le nœud mobile détecte toujours un nouveau routeur par défaut après chaque transfert. Pour résoudre ce problème, le standard exige que tous les MAGs dans le domaine PMIPV6 utilisent la même adresse de lien local et de liaison sur chacun des liens d'accès auxquels le nœud mobile s'attache. Afin de suivre cette importante spécification, nous avons configuré les MAGs avec la même adresse de lien local à l'aide de la commande

   ```
   Macchanger -m newMAC@ interface
   ```

   Cette opération n'a aucun inconvénient sur le réseau et sur la mobilité, car elle n'implique pas l'adresse de lien local sur le côté réseau.

4. **Tunneling:** le tunnel bidirectionnel est utilisé pour le routage des données de trafic depuis et vers le nœud mobile entre le MAG et le LMA. Un tunnel cache la topologie et permet à un nœud mobile d'utiliser l'adresse de son HNP depuis n'importe quel lien d'accès dans le domaine PMIPv6. Un tunnel peut être créé dynamiquement lorsque c'est nécessaire et retiré lorsqu'il n'est pas nécessaire. Toutefois, les implémentations peuvent choisir d'utiliser des tunnels statiques préétablis au lieu de les créer et de les détruire dynamiquement en fonction des besoins. Nous avons mis en place un tunnel statique et partagé entre chaque MAG et le LMA, afin de servir tous les hôtes mobiles attachés au même MAG avec le même tunnel.

L'impact de ces configurations d'implémentation sur les performances PMIPv6 est analysé ci-après.

Résultats expérimentaux

Nous avons testé les performances de handover de notre implémentation PMIPv6 selon la procédure de configuration décrite précédemment et avec la configuration du test-bed illustrée à la Fig. 7. Iperf v.2.0.2 est utilisé pour générer le trafic TCP / UDP. Grâce au logiciel Wireshark v 1.0.1, nous avons analysé le déroulement des tests.

	Different MAC address Scenario 1	Same MAC address Scenario 2
Average	45.72 ms	32.06 ms
Standard Deviation	4.74 ms	5.71 ms

Tableau 1: Latence de handover pour le trafic UDP dans les scenarios 1 et 2.

Comme les points 1 et 2, attachement-détachement dans la couche 2 et unicast RA, représentent des suggestions pratiques sur la façon de mettre en œuvre le protocole, nous avons centré notre analyse sur les points 3 et 4, à savoir l'adresse de lien local du MAG et les tunnels, car ils peuvent avoir un impact sur les performances de PMIPv6.

Nous avons analysé le comportement des différentes implémentations de PMIPv6 selon différentes configurations d'adresses locales de MAG. Dans le premier scénario, nous n'utilisons pas la fonction Macchanger et nous laissons les deux MAGs avec leur propre adresse MAC, tandis que dans le second scénario, nous appliquons la modification comme indiqué dans la Fig. 7. Les figures 8 et 9 illustrent les throughput UDP lorsque le MN effectue un handover de AP1 à AP2 dans les deux scénarios respectifs. Nous pouvons voir que les performances UDP pour le deuxième scénario sont légèrement meilleures par rapport à celles du premier scénario.

Afin de mieux évaluer le temps de latence du handover pour le trafic UDP, nous avons répété l'épreuve 50 fois pour chaque scénario. Les résultats sont présentés sur la Fig. 10 et résumés dans le tableau 1. Dans le cas de la configuration avec une adresse MAC différente, la latence du handover est en moyenne supérieure de 45 ms, tandis que si nous configurons la même adresse MAC dans les deux MAGs, la latence de transfert est en moyenne 32,06 ms.

Les considérations sont différentes lorsque nous analysons les performances du trafic TCP au cours du transfert pour les deux scénarios. Les figures 11 et 12 montrent, dans les graphiques de temps séquence de TCP, la différence importante entre le comportement de la latence de handover dans les scénarios 1 et 2. Avec 50 pistes d'essai, nous obtenons les résultats résumés dans le tableau 2. Ce résultat montre l'importance de configurer la même adresse de lien local pour tous les MAG, en particulier pour le trafic TCP, afin de donner la possibilité au MN de l'utiliser pour le routage pendant la configuration de routeur par défaut.

Enfin, nous avons considéré un troisième scénario dans lequel le tunnel

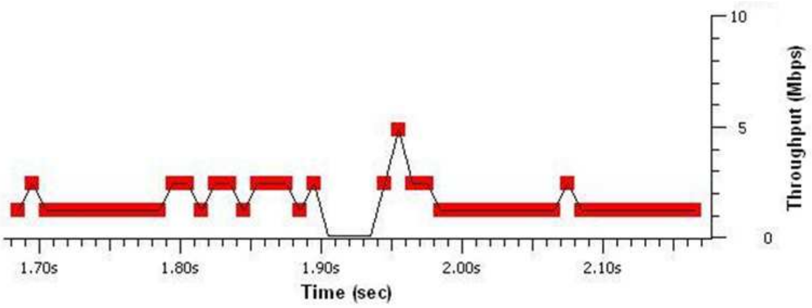

Figure 8: Throughput UDP pendant le handover dans le premier scénario.

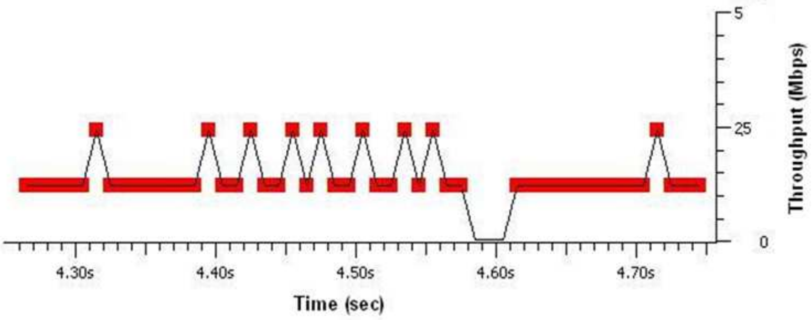

Figure 9: Throughput UDP pendant le handover dans le deuxième scenario.

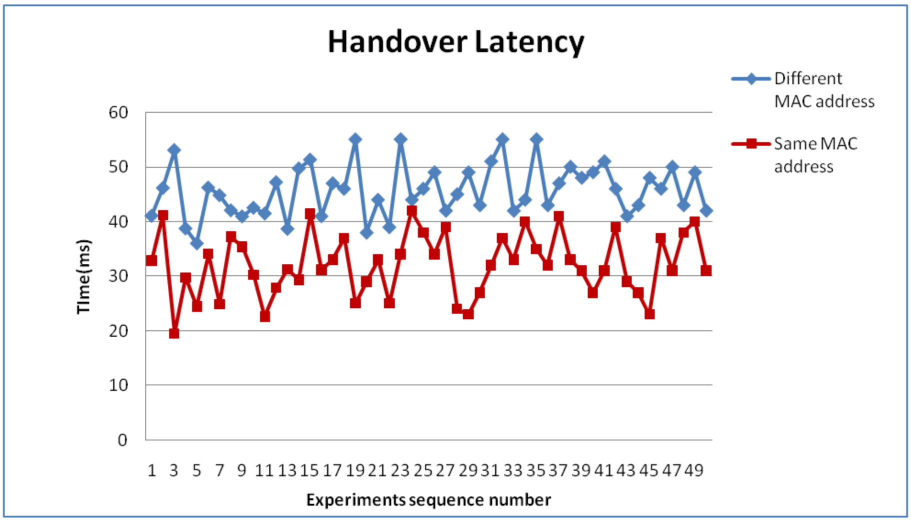

Figure 10: Latence de handover pour le trafic UDP dans les scenarios 1 et 2.

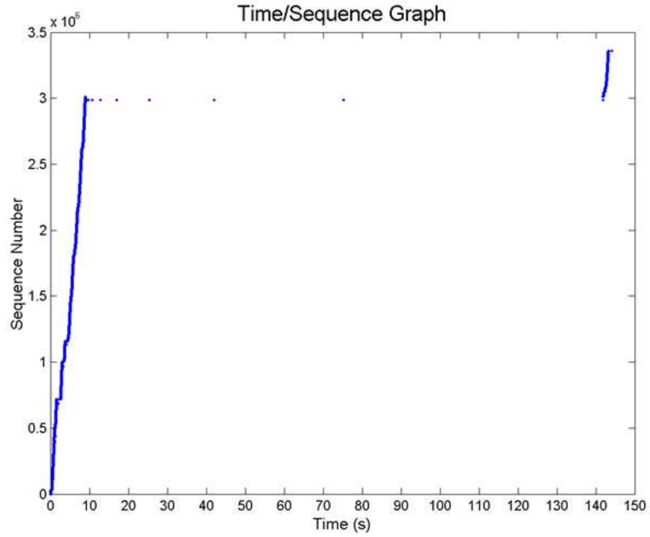

Figure 11: Performance du handover pour TCP dans le scenario 1.

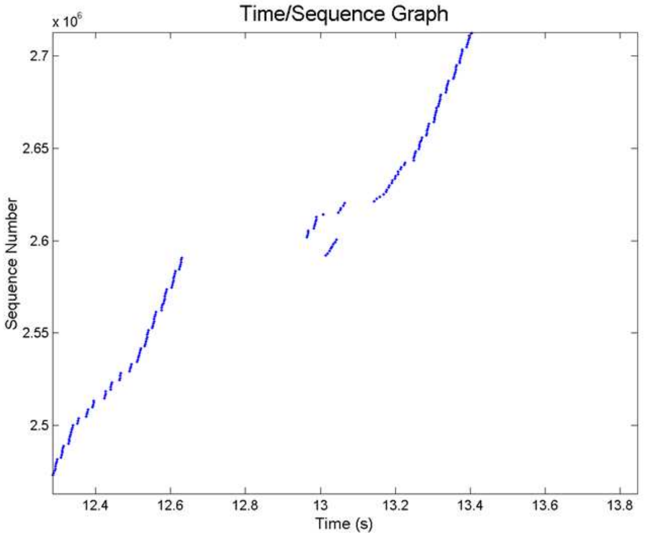

Figure 12: Performance du handover pour TCP dans le scenario 2.

	Different MAC address Scenario 1	Same MAC address Scenario 2
Average	122789.05 ms	67.51 ms
Standard Deviation	164.77 ms	10.23 ms

Tableau 2: Latence de handover pour le trafic TCP dans les scenarios 1 et 2.

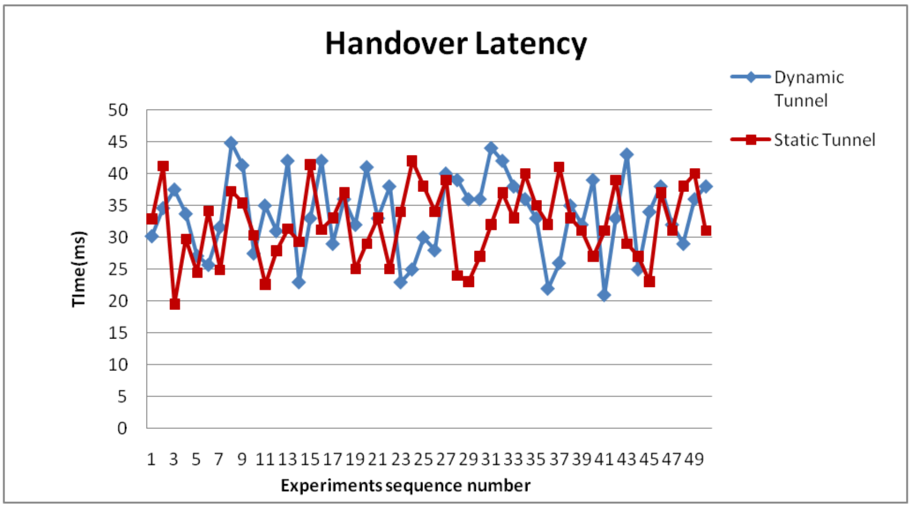

Figure 13: Latence de handover pour le trafic UDP dans les scenarios 2 et 3.

bi-directionnel entre le MAG et le LMA est créé dynamiquement. Nous voulons préciser que le scénario préalablement défini numéro 2 a un tunnel statique. Nous avons comparé la latence de handover pour le trafic UDP entre les scénarios 2 et 3. Comme on peut le voir dans la Fig. 13 et le tableau 3, les performances sont pratiquement identiques, ainsi le délai de création de tunnel peut être considéré comme non pertinent. galement les performances avec le trafic TCP ont fourni des résultats similaires.

Implémentation combinée de PMIPv6 et HIP

Parmi les différents implémentations open source HIP disponibles, nous avons choisi HIPL v.1.0.4-48, l'open source de HIP dans l'espace utilisateur sur le noyau Linux, implémenté dans le cadre du projet InfraHIP par le Helsinki Institute for Information Technology (HIIT) et Helsinki University of Technology (TKK) en Finlande, en collaboration avec des partenaires in-

	Static Tunnel Scenario 2	Dynamic Tunnel Scenario 3
Average	32.06 ms	33.64 ms
Standard Deviation	5.71 ms	6.15 ms

Tableau 3: Latence de handover pour le trafic UDP dans les scenarios 2 et 3.

dustriels comme Nokia, Ericsson, Elisa et les Forces de défense finlandaises. Il représente l'implémentation la plus complète de HIP, en termes également de déploiement des entités d'infrastructure.

Nous avons combiné notre mise en œuvre PMIPv6 avec HIPL dans le test-bed illustré à la figure 7, pour tester les performances de notre architecture pour la mobilité de l'Internet du futur dans le cas de transfert intra-technologie.

Le software PMIPv6 est mis en oeuvre sur le LMA et les MAGs, les entités du domaine local, tandis que le MN et le CN mettent en œuvre le démon HIP respectivement en tant que client et serveur. En outre, afin d'être plus conforme au standard PMIPv6, nous avons également mis en place un serveur RADIUS et un client RADIUS co-localisés au LMA et au MAG respectivement, pour l'authentification du MN et pour stocker ses HNP.

Dans notre scénario basé sur IPv6, le MN se déplace entre AP1 et AP2, et change également de sous-réseau en se déplaçant entre MAG1 et MAG2. Pour faire un scénario réaliste, nous avons exécuté des tests dans lesquels le MN reçoit un flux multimédia (vidéo et audio) du CN, en utilisant le logiciel VideoLAN (VLC). Afin de faire de VLC une application supportant HIP, nous avons spécifié les HIT du MN, au lieu de son adresse IPv6, lors du démarrage du VLC au niveau du serveur. Comme spécifié par HIP, dans les flux multimédia, les paquets UDP sont encapsulés et envoyés en utilisant un mode spécial IPSec ESP appelé End-to- End Tunnel (BEET). Les données vidéo et audio sont encodées en utilisant MP4V et MPGA respectivement. La vidéo et l'audio utilisent la méthode d'encodage Constant Bit Rate (CBR).

Avec ce scénario, nous avons exécuté 50 tests afin de mesurer la latence de handover expérimenté par le MN dans le cas d'un handover intra-technologie . Les mesures de throughput UDP sont extraites du logiciel Wireshark installé dans le MN et faites pendant les déplacements deAP1 vers AP2 tout en recevant les flux multimédia. Dans le même temps, nous avons recueilli

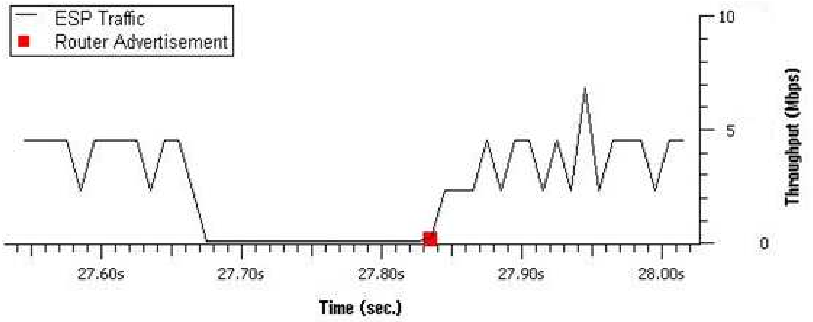

Figure 14: Throughput UDP pendant le handover Intra-technologique.

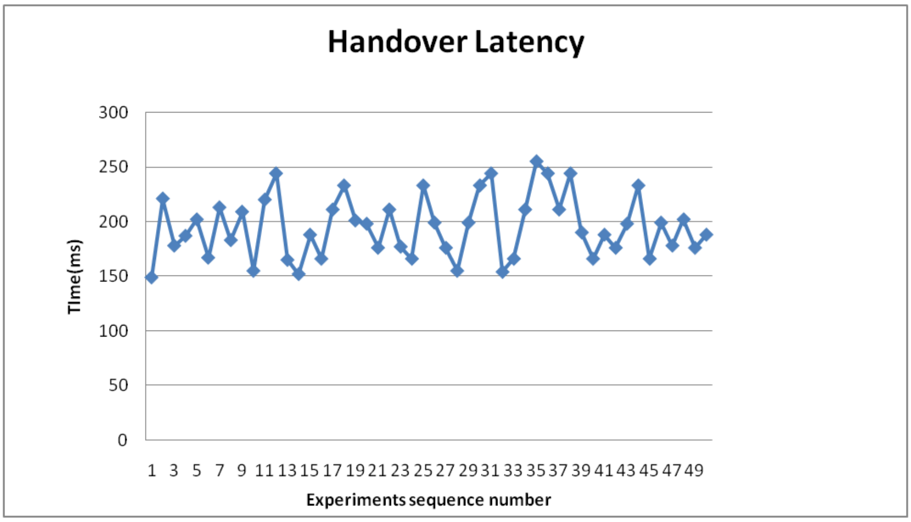

Figure 15: Latence du handover pendant le Handover Intra-technologie.

les traces de MAG2 afin de mesurer le retard correspondant à chaque phase PMIPv6.

De la Fig. 14, nous pouvons voir que le throughput UDP est tout à fait stable et devient nul lors du handover pendant moins de 200 ms. En particulier, nous pouvons remarquer que dès que le MN reçoit le message RA (carré rouge), qui est la dernière étape de la procédure PMIPv6, le MN recommence à recevoir le flux multimédia.

En outre, la Fig. 15 et le tableau 4, où nous avons reporté les durées de handover mesurées pour les 50 tests réalisés, montrent que le processus de handover intra-technologique handoff prend en moyenne moins de 200 ms.

Enfin dans le tableau 5, nous avons reporté la rupture du temps de latence de PMIPv6 en considérant toutes les phases importantes de la procédure

	PMIPv6 - HIP Combination Handover Latency
Average	195.12 ms
Standard Deviation	28.39 ms

Tableau 4: Latence du Handover pour le trafic temps-réel dans le scenario PMIPv6-HIP.

Phases	Average
L2 Attachment - Access Request	1.06 ms
Access Request - Access Accept	1.99 ms
Access Accept - PBU	1.87 ms
PBU - PBA	2.32 ms
PBA - RA	7.21 ms
Total PMIPv6 Latency	16.78 ms

Tableau 5: Latence du handover des Phases PMIPv6.

PMIPv6. Le tableau montre qu'il n'y a pas de différence significative entre les temps de latence des différentes phases de PMIPv6, seul le PBA-RA est plus long en raison de la latence du démon RADVD responsable de l'envoi en unicast du RA.

Il est important de souligner que le temps de latence de PMIPv6 a une contribution très réduite à la latence du handover total indiqué ci-dessus. D'après le tableau 5 nous pouvons voir que, la latence moyenne PMIPv6 mesurée sur 50 tests est de 16,78 ms, tandis que dans le tableau 4, nous avons un retard de transfert global de 195,12 ms. Malheureusement, la phase d'attachement à la couche 2 pour le Wi-Fi est relativement significative et affecte la latence de handover global. Il serait possible d'améliorer les performances de cette phase en incluant dans le déploiement des logiciels PMIPv6-HIP le Media Independent Handover. En outre, MIH aiderait au déploiement du handover inter-technologie, comme son objectif principal est d'améliorer le handover entre technologies réseau hétérogènes. La section suivante fournit des indications et des suggestions.

Applications de sécurité civile

Les situations d'urgence exigent des systèmes de communication à large bande fiables, en mesure de transmettre les informations pertinentes du site de la catastrophe au centre décisionnel, et capables de transmettre les informations des premiers intervenants sur les dangers potentiels ou des décisions. Le facteur clé dans la conception d'un système de communication robuste dédié à l'intervention d'urgence est le développement d'une infrastructure rapidement et facilement déployable, mobile, fournissant des services de voix et données, et disponibles dans les premières 24 heures.

Tenant compte de tous les exigences fonctionnelles et de performances mentionnées ci-dessus, le fait qu'aucun système terrestre et / ou satellitaire existant pour les communications d'urgence n'est en mesure de couvrir toutes ces exigences simultanément, et que les réseaux par satellite sont les meilleurs et les plus fiables pour les communications dans les situations d'urgence pour fournir une connexion à l'infrastructure du réseau intacte, nous proposons une nouvelle architecture système avancée hybride satellite et terrestre basée sur notre proposition de schéma PMIPv6-HIP. L'architecture d'ensemble est illustrée dans la Fig. 16.

Elle fournit à la fois une pleine mobilité dans le site de la catastrophe aux équipes de secours, et une connectivité à large bande à l'intérieur du réseau de la catastrophe et avec les headquarters. L'architecture proposée est rapidement déployable et adaptable dynamiquement aux catastrophes de toute nature et quel que soit l'emplacement. Elle est basée sur IPv6 et est capable de supporter l'interopérabilité avec les terminaux IP appartenant à différents administrateurs et technologies. Comme, généralement, le déploiement d'unités de la sécurité civile fait appel à deux entités, les véhicules et les utilisateurs de la Sécurité Civile, équipés de terminaux satellite et radio, nous avons décidé de les mettre en œuvre dans l'architecture système hybride satellite et terrestre proposée. Il permet aux unités de la Sécurité Civile de se déplacer sur le site de crise, et de communiquer des informations urgentes entre les équipements sur le terrain et des équipements vers l'Internet et les headquarters.

Ce résultat est obtenu en ayant un réseau maillé mobile ad-hoc sur le site de la catastrophe, une infrastructure qui permet à toute entité de joindre facilement les headquarters. Le rôle le plus important et central de l'architecture présentée est joué par les Vehicle Communication Gateways (VCGs). Ils sont dotés de fonctionnalités doubles, comme montré sur la Fig. 17. D'un côté, les VCGs fournissent des communications vehicle-to-infrastructure (V2I) pour maintenir la connectivité Internet avec le site de la catastrophe par le biais des liaisons par satellite: les véhicules S-UMTS opérent dans la bande S/L et les véhicules DVB-RCS fonctionnent en bande Ku/Ka. De l'autre côté, les GCVs sont en mesure d'établir des communications Vehicle-to-Vehicle (V2V), donnant la connectivité aux terminaux mobiles à travers le réseau mobile ad-hoc maillé.

Les VCGs et les routeurs mobiles, qui sont les entités qui composent le réseau maillé ad hoc mobile, peuvent assumer les fonctionnalités de LMAs et de MAGs pour créer un domaine PMIPv6, utilisé comme une infrastructure à la zone de crise, auquel les terminaux mobiles IPv6 non modifiés des différentes équipes de secours peuvent accéder et être aisément gérés. De cette façon, une connectivité sans faille peut être garantie pour les communications à large bande à l'intérieur de la zone sinistrée et avec les headquarters, par des liaisons par satellite.

La combinaison des protocoles PMIPv6 et HIP permet aux équipes de sauvetage de se déplacer facilement et de garder leur connexion tout en se déplaçant d'un routeur mobile à un autre, et d'une technologie d'accès à une autre. Chaque MN dans le réseau ad hoc maillé a un identificateur, utilisé pour établir les connexions de sécurité avec les pairs. Le schéma Diffie-Hellman pour l'échange de clé secrète avec IPSec est utilisé pour la création de SA entre MNs, comme dans le schéma HIP . Une fois que la SA est établie, les modifications de l'adresse IP du MN en raison de la mobilité ne cassent pas la connexion, car la SA est liée aux identificateurs. Afin d'éviter une signalisation inutile de mise à jour par les pairs de la nouvelle localisation comme dans le standard HIP, nous appliquons une solution de micro-mobilité basée sur PMIPv6.

Chaque MN obtient une adresse IP à partir du réseau, qui est routable en dehors du réseau ad hoc maillé, et reste inchangée même si le MN passe derrière les différents routeurs maillés différentes à l'intérieur du domaine. Grace à la gestion de la micromobilité, le réseau est capable de router correctement le trafic vers ne change pas, aucun message de mise à jour n'est nécessaire. Dans le cas où le MN est équipé avec de multiples interfaces et veut passer d'une technologie d'accès à une autre, par exemple, afin d'utiliser une connexion plus fiable, il peut aviser le réseau de son intention et le trafic sera acheminé directement à la nouvelle interface. Pour les communications entre les équipes de secours situées dans le lieu de la catastrophe et les décideurs dans l'headquarters, ce mécanisme est vraiment utile, car il contribue à économiser les ressources et la bande passante par satellite. En outre, il réduit le délai et permet aux équipes de secours de bénéficier de la vision Always Best Connected (ABC), ce qui prouve la robustesse et la fiabilité du système. Le mécanisme est également indépendant de la technologie d'accès, l'interopérabilité des équipements de communication au sein et entre les différents organismes et administrations est donc possible.

En ce qui concerne le réseau satellite, les véhicules S-UMTS permettent des solutions de communication mobiles par bande S/L entre les réseaux

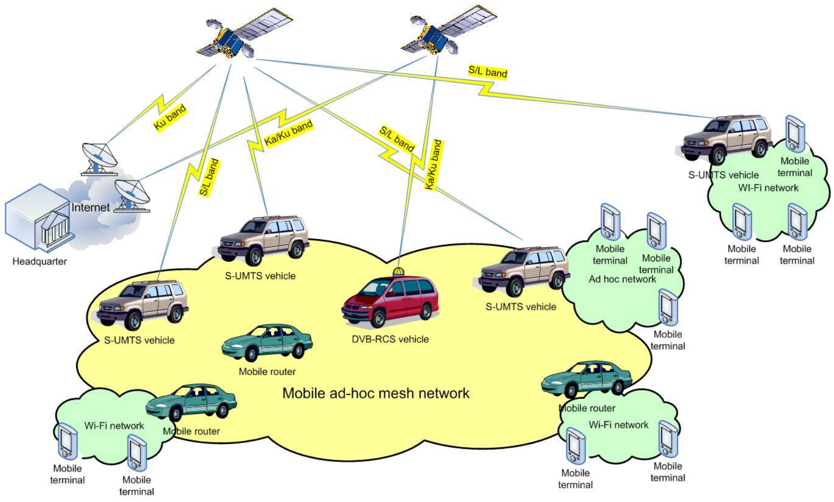

Figure 16: Architecture Hybrid Satellitaire and Terrestre.

maillés mobiles ad-hoc situés sur le terrain de la catastrophe et l'Internet, où le centre de décision fixe et les headquarters sont situés. Les terminaux transportables, comme les véhicules DVB-RCS, qui fonctionnent à l'arrêt ou à très basse vitesse, fournissent les bénéfices de throughput élevé et une utilisation efficace de la bande passante. Enfin, les véhicules S-UMTS peuvent être utilisés pour donner une connectivité externe à des groupes non atteints par le réseau maillé ad-hoc mobile.

Conclusion

Dans cette thèse, nous avons présenté un nouveau paradigme pour l'avenir de l'Internet et des futurs opérateurs de téléphonie mobile. L'architecture proposée a reconnu la tendance actuelle dans les réseaux à un paysage hétérogène des fournisseurs d'accès. Dans ce contexte, il est important de donner aux fournisseurs d'accès la flexibilité de la gestion de la mobilité à l'intérieur de leurs domaines en fonction de leurs besoins et de leurs technologies, sans être conditionné par la façon dont la mobilité est gérée dans d'autres domaines. Pour faire face à ce concept, l'architecture proposée dans cette thèse sépare la gestion de la mobilité en deux niveaux: la mobilité locale selon le schéma PMIPv6 (network-based local mobility management), et la mobilité globale selon le schéma HIP (host-based global mobility management). En conséquence, la gestion de la mobilité dans ces deux niveaux est réalisée de façon entièrement indépendante.

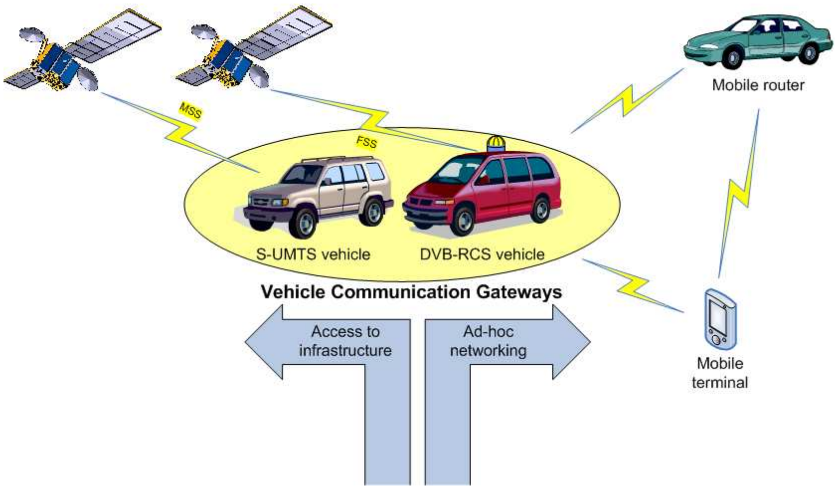

Figure 17: Vehicle Communication Gateways.

Le mécanisme efficace de gestion de la mobilité n'est pas le seul avantage de l'architecture de mobilité proposée. Les principaux éléments de conception ont été le recours à des identifiants cryptographiques utilisés comme interfaces virtuelles pour les hôtes mobiles multi-domiciliés, et à des identificateurs de groupe utilisés pour identifier les nœuds mobiles appartenant au même réseau ad-hoc, les repères spécifiques créés par le biais du home Network Prefixes pour fournir la confidentialité de la localisation, la réduction du temps de latence du handover et les frais généraux de signalisation, et la sécurité de bout en bout basée sur HIP. En conséquence, avec la combinaison de PMIPv6 et HIP, l'architecture est en mesure de supporter la mobilité, la multi-domiciliation, les réseaux hétérogènes, seamless handover, la sécurité, un routage et un schéma d'adressage efficaces, la confidentialité de la localisation et les réseaux ad hoc.

Cette thèse a également examiné les contraintes pratiques auxquelles les futurs opérateurs mobiles devront faire face pour mettre en œuvre l'architecture proposée, en particulier tous les aspects liés à la mise en œuvre de PMIPv6 dans un véritable test-bed, les directives sur HIP ayant été elles déjà largement abordées. Nous avons effectué une étude entièrement empirique basée sur des expériences réelles de PMIPv6. Au vu de nos connaissances, notre travail est le premier à fournir une perspective sur l'implémentation du standard PMIPv6 sous différentes configurations d'implémentation. Le schéma d'allocation de préfixe par MN et l'envoi en unicast de messages AR ont été implémentés, ainsi que la BCE au LMA et le tunnel dynamique bidirectionnel entre le MAG et le LMA. En outre, l'importante fonction de répartition d'une même adresse de lien local à tous les MAG a été respectée. Les résultats expérimentaux montrent que le dernier aspect ne peut pas être omis dans la mise en œuvre, tandis que le fait de mettre en œuvre un tunnel dynamique ou permanent entre MAG et LMA peut être librement décidé car il n'impacte pas les performances de transfert. Nous avons également mis notre implémentation de PMIPv6 en open source dans le site Web d'Eurecom. Il ne nécessite pas de modification dans le noyau standard IPv6.

Enfin, nous avons proposé notre projet HIP-PMIPv6 pour la sécurité civile avec une architecture système composé des réseaux satellitaires et ad hoc maillés. Les équipes de secours dans le lieu de la catastrophe peuvent profiter de la gestion de la mobilité a niveau global et local pour se déplacer dans le réseaux de façon transparente, sans "casser" leurs liens avec les équipes de secours par le biais du réseau ad-hoc maillé, et avec les headquarters grâce au réseau satellitaire . L'architecture du système proposé est facile à déployer, car elle utilise des antennes satellites transportables qui peuvent être montées sur des véhicules, et des gateways et des routeurs dotés des fonctionnalités de LMA et MAG. Les équipes de sauvetage peuvent continuer à utiliser leurs équipements standards, car PMIPv6 ne nécessite pas de modifications de leur noyau, alors qu'une simple mise à jour de l'espace utilisateur est nécessaire pour installer le démon HIP et pour bénéficier de communications sécurisées. L'architecture du système donne également l'occasion aux équipes mobiles de passer d'une technologie d'accès à une autre, par exemple en vue d'utiliser une connexion plus fiable, en informant le réseau de leur intention de router le trafic directement vers la nouvelle interface. Pour les communications entre les équipes de secours situées dans la zone sinistrée et les décideurs situés aux headquarters, ce mécanisme est vraiment utile, car il permet d'économiser des ressources en bande passante par satellite. En outre, il réduit le délai et permet aux équipes de sauvetage de bénéficier d'une vision Always Best Connected, prouvant la robustesse et la fiabilité du système. Le mécanisme est également indépendant de la technologie d'accès, l'interopérabilité des équipements de communication à l'intérieur et entre les différents organismes et administrations est donc possible.

Perspectives futures

La présente thèse a proposé une architecture et des techniques pour supporter la mobilité dans l'Internet du futur. Elles représentent un pas en avant, donnant les directions pour favoriser la mobilité future et pour inciter à l'utilisation d'identificateurs et de localisateurs séparés.

Cependant, il reste des aspects non abordés dans cette thèse.

Les prochaines étapes de ce travail pourraient se pencher sur l'extensibilité et les fonctionnalités de multicast pour l'architecture proposée. Un mécanisme permettant la communication entre LMA et MAG devrait être considéré pour couvrir ces aspects importants. Il pourrait être utile pour l'extension de l'architecture aux réseaux maillés. Cette étude a été partiellement couverte dans notre article de journal, mais nécessite une investigation plus complète et doit être incluse d'une manière efficace dans l'architecture pour la mobilité.

Au point de vue de la mise en œuvre, le intra-technology handover a été entièrement implémenté et testé, tandis que le inter-technology handover, ainsi que la multi-domiciliation, sont encore en phase de mise en œuvre. Une importante valeur ajoutée serait l'intégration de notre implémentation de HIP-PMIPv6 dans le standard IEEE 802.21 MIH. Cela fournirait un mécanisme permettant aux MNs avec multiples interfaces de donner des informations aux MAG sur l'état des différents liens. Les primitives MIH peuvent être utilisées pour aider le MAG à faire face à des scénarios avec multi-technologies, améliorant la circulation et la gestion des flux de nœuds mobiles multi-domiciliés.

Chapter 1

Introduction

1.1 Background

In the early days of Internet, hosts were big and clumsy and remained in fixed locations. This led to the design of the current Internet architecture, which does not match anymore the evolution of Internet and its hosts.

Mobile Communications is now a reality and it is part of our daily lives. Most of the devices that are available today in the market are *mobile* and equipped with *multiple radio interfaces*. Thus, it is reasonable to assume that the mobile devices that attach to the Fourth Generation (4G) networks and Internet in the future will also be equipped with multiple radio interfaces, such as Long Term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMAX), Wi-Fi, etc, and in any combination. These mobile nodes can potentially attach to the network using one or more interfaces and be using all of those interfaces simultaneously for their data sessions. Moreover, it is given that the next generation mobile networks will be true heterogeneous networks. A mobile operator can potentially be managing more than one access technology in their core network. Or, they may have partnership with other operators that support a different access technology than what is supported in the operator's home network. The mobile device capabilities coupled with the availability of heterogeneous network with multiple access technologies requires *seamless mobility support*. Following there are some of the mobility related considerations:

- Roaming in a homogeneous network - a mobile node has the ability to seamlessly roam and change its point of attachment within a single access technology domain, thus the mobile node moving from one base station or router to another using the same interface for its network attachment.

- Roaming in a heterogeneous network - a mobile node has the ability to seamlessly roam between two different access networks, performing inter-technology handoff and moving its IP address configuration and all the IP sessions from one interface to another one.

- Multihoming support - a mobile node has the ability to attach to network using multiple interfaces and is able to use any one or more of its interfaces for network connectivity.

- Flow mobility support - a mobile node has the ability to move the flows between interfaces on a selective basis.

- Local and global mobility management - management of a mobile node's movements between two subnets within the same domain or in two different network domains.

Mobility support is not the only limitation of the current Internet design and it involves also other problematics. The original design of the Transmission Control Protocol (TCP)/IP Internet protocols was created for an environment where the end-users were assumed to be mutually trusting, at least to a minimal degree, and where the network was assumed to be inherently unreliable due to a potential attacker physically destroying routers and links. Since then, the environment has grossly changed as a side effect of the huge success of the Internet, creating a need to design a communication architecture that provides the following functions:

- Ability to operate over all kinds of underlying networks, including adhoc, commercial, and dedicated; this implies the ability to dynamically pay for the services on-line, the ability to hide the real identities of communicating parties from the underlying networks, etc.

- Ability to survive in a partially hostile environment where some of the underlying networks may be only partially co-operating, competing, or even outright antagonistic to each other; this implies the ability to isolate underlying networks from each other, when needed.

- Ability to support application, host, and sub-network level mobility and multi-access as primary design elements and not as extensions.
- Ability to support full location privacy, especially against any transit networks and other third parties.

The goals above can be seen as a new incarnation of the original IP design goal, adapted to the contemporary needs. Nowadays the underlying communication network is more diverse, sometimes even hostile, in addition to being unreliable, and a fraction of users must be assumed to be egregiously selfish or outright malicious. Along with revising the original goals to meet todays needs, it has also become clear that the operational costs of the current network are becoming quite high. Consequently, there is a need for a network that can self-organise, including functions such as infrastructure discovery and the ability to find reasonably functioning communication paths among multiple alternatives.

To fulfil all the aforementioned requirements represents a big challenge for researches worldwide.

1.2 Thesis Motivation

To conjecture the future directions of Internet, one need to start with an ordered list of the fundamental design goals. As Clark argued in a discussion on the design goals for the Internet architecture [1] [2], “It is important to understand that these goals are in order of importance and an entirely different network architecture would result if the order were changed”. What should be in the set of the fundamental design goals for future mobility support in Internet? And how should one order them? To answer these questions, one may take a look at the relatively short history of the Internet itself. What enabled its explosive growth? One can identify a few important enablers, the open access (anyone can connect to Internet at a low cost), open architecture, and distributed management. Of course the success of Internet is fueled by the advancement of computing technologies and innovations in applications, however the open access eased interconnections of all interested parties, the open architecture offered a low threshold to enter for new users and new innovations, and the absence of central control or central authority removed potential constraints on its growth.

Based on these considerations from the Internet history, it is important to put forth the following requirements at the top of the list of the design goals for future mobility support. First, effectively connecting mobile devices to Internet in a secure way should be of the first and foremost importance, above any other desired goals such as guaranteed service quality or ease of accounting. Second, the solutions should be able to support mobility at local and global level for an unlimited number and a large variety of mobile devices equipped with several active interfaces in a cost effective way. Furthermore, increasing numbers of mobile devices will inevitably bring in new mobile applications that we may not envision today, which suggests that it would be best to decouple mobility support from applications above it.

1.3 Contributions and Outline of the Dissertation

Foreword: *This dissertation stems from an European Space Agency (ESA) initiative, called Networking Partnering Initiative (NPI) program [3], which put the basis for the agreement between ESA-ESTEC, the Netherlands, and Thales Alenia Space, France, and EURECOM, France. The conducted research work was fully co-funded by ESA and Thales Alenia Space.*

The present thesis focuses on designing a mobility architecture for future Internet, which is based on Host Identity Protocol (HIP) [4] and Proxy Mobile IPv6 (PMIPv6) [5]. HIP is a new host-based global mobility management protocol which is having more and more success among researchers for future Internet, as it also provides inherent security and multihoming features to heterogeneous mobile networks with multihomed hosts, having a light impact on mobile terminals. On the other side, PMIPv6 is a network-based mobility management protocol which enables IP mobility for a host without requiring its participation in any mobility related signaling. It has been designed with the goal that the network will perform the mobility management on behalf of the client, resulting in a simple client with minimal software requirements. This design choice has been quickly adopted in LTE, Third Generation Partnership Project (3GPP) and WiMAX architectures.

The combination of these two protocols not only creates an efficient mobility and multihoming management scheme for multihomed terminals at local and global level. It also puts the basis for a new Internet architecture that benefits, on one side, of HIP built-in features such as security and efficient Host Identity (HI) namespace, and on the other side, thanks to the particular locators (IPv6 addresses) created through the PMIPv6 scheme, of location privacy, efficient routing and traffic engineering at local level. The mobility and multihoming scheme adopted by the proposed mobility architecture significantly reduce the signaling overhead in the wireless link as well as in the infrastructure, without increasing the complexity on the mobile terminals and networks.

Furthermore a part of the work is dedicated to the implementation of PMIPv6 and to the analysis of the requirements for its real deployment. The protocol is also combined with HIPL, an open source implemetation of HIP, in order to prove the viability of the mobility architecture through experimental results. Thus, the contributions of the thesis are partially of conceptual value and partially of development and analytical value. Finally, we focus also on the contribution that this new mobility architecture can apport to Public Safety Networks and to rescue teams at disaster sites, always affected by mobility and interoperability issues between different agencies and organizations.

We provide below an outline of the dissertation and describe the contributions made in each chapter.

Chapter 2 - Internet Mobility Support

A variety of approaches have been made in various kinds of access networks to create workable mobility solutions for mobile devices. In this introductory chapter there is a brief summary of the fundamental properties and characteristics of supporting mobility in the future Internet, showing that all mobility support designs involve the same three basic components: identifier, IP address and a mapping system in between. We analyse the designs of GPRS, MIPv6, PMIPv6 and HIP and we show that they are simply different realizations of the same three basic components. We restrict our overview on layers 3 and 3.5, as mobility at layer 2 is dependent on one technology and it is not suitable for heterogenous networks, while at layer 4 it is bound to the use of a specific application protocol. The aim of this chapter is also to provide a broad view on mobility management and to show how it is related to other important networking aspects as routing, access control, security and multihoming.

Parts of this chapter's material are contained in:

- G. Iapichino, C. Bonnet, "IPv6 mobility and ad hoc network mobility overview report", Eurecom, Rapport de Recherche, RR-08-217, Sophia Antipolis, France, March 2008.

Chapter 3 - Secure Global and Local Mobility Management

Chapter 3 presents a two-fold contribution for PMIPv6 and HIP. New extensions for PMIPv6 are being planned to allow client to perform inter-technology handoff or to express handoff or flow preferences. The combination of PMIPv6 with HIP described in this chapter represents an important improvement to PMIPv6 for inter-technology handover and multihoming, as it overcomes the current virtual interface solution in proving IP session continuity and simultaneous usage of multiple interfaces for multihomed mobile nodes. On the other side, an efficient micro-mobility solution for HIP is still missing. Current solutions take inspiration from micro-mobility schemes for Mobile IPv6. Having in mind such a different Internet architecture, they do not represent an optimized solution for HIP. PMIPv6 represents an efficient local mobility solution for HIP as it can be applied to any global mobility protocol without adding any host stack software complexity. Their efficient combination provides a secure global and localized mobility management solution for multihomed mobile nodes applicable to any kind of access technology.

Parts of this chapter's material are contained in:

- G. Iapichino and C. Bonnet, "Host Identity Protocol and Proxy Mobile IPv6: a Secure Global and Localized Mobility Management for Multihomed Mobile Nodes", in Proceedings of *IEEE Global Communications Conference* (GLOBECOM 2009), pp. 1-6, Honolulu, Hawaii, USA, December 2009.

- G. Iapichino, C. Bonnet, "Combination of ad hoc mobility with IPv6 mobility mechanisms report", Eurecom, Rapport de Recherche, RR-09-225, Sophia Antipolis, France, January 2009.

Chapter 4 - Mobility Architecture for Future Internet

The current Internet architecture, though hugely successful, faces many difficult challenges as the incorporation of mobile and multihomed terminals and an overall lack of protection against Denial-of-Service attacks and other lacking security mechanisms. Although many of these problems have been widely recognized for some time, a complete and adequate solution is still missing. In this chapter we present a completely new mobility architecture which has native support for future Internet and operators' requirements through an efficient integration of its basis protocols: HIP and PMIPv6. The proposed architecture includes as main features mobility management, multihoming, addressing, name resolution, security, location privacy, ad-hoc networking, routing and traffic engineering.

Parts of this chapter's material are contained in:

- G. Iapichino and C. Bonnet, “A Host Identity Protocol and Proxy Mobile IPv6 based Mobility Architecture for Future Internet”, to be submitted to *IEEE Journal on Wireless Communications.*

- G. Iapichino, C. Bonnet, “Ad hoc network connection continuity for security applications report”, Eurecom, Rapport de Recherche, RR-09-237, Sophia Antipolis, France, November 2009.

Chapter 5 - Implementation and Evaluation

To speed up PMIPv6’s adoption by mobile network operators, we provide in this chapter an implementation analysis of PMIPv6, which takes into account all the important recommendations for respecting the standard and, at the same time, for reducing handover delays. This is the first attempt to study PMIPv6’s implementation issues, analysing each implementation configuration and evaluating different performance metrics. Moreover, PMIPv6 has been integrated with an open source version of HIP realised by research institutes in Finland in order to analyse the feasibility and the performances of the proposed mobility architecture. Finally Media Independent Handover (MIH) software is suggested as future step to add to the test-bed to complete the implementation.

Parts of this chapter’s material are contained in:

- G. Iapichino and C. Bonnet, “Experimental Evaluation of Proxy Mobile IPv6: an Implementation Perspective”, in Proceedings of *IEEE Wireless Communications and Networking Conference* (WCNC 2010), Sydney, Australia, April 2010.

- H.N. Nguyen, C. Bonnet, and G. Iapichino, “Extended Proxy Mobile IPv6 for Scalability and Route Optimization in Heterogeneous Wireless Mesh Networks”, accepted for publication in *International Journal of Ubiquitous Computing*, Serial Publications, to appear in 2010.

Chapter 6 - Public Safety Applications

Emergency Management is an important topic for research community worldwide, especially after recent major disasters. The problem of supporting mobility at the disaster site to rescue teams equipped with different heterogeneous access technologies and providing interoperability between different agencies and jurisdictions is still under investigation. In this chapter we propose to merge the advantages of IPv6 micro-mobility management of

PMIPv6 with macro-mobility management, security, inter-technology handover and multi-homing features of HIP. This new approach applied to our proposed ad-hoc satellite and wireless mesh system architecture for emergency mobile communications can improve mobility, security, reliability and interoperability in Emergency Management domain.

Parts of this chapter's material are contained in:

- G. Iapichino, D. Câmara, C. Bonnet, and F. Filali, "Public Safety Networks", accepted for publication in *Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts*, IGI Global, to appear in 2010.

- G. Iapichino, C. Bonnet, O. Del Rio, C. Baudoin, and I. Buret, "Adhoc Mobility in Satellite-based Networks for Public Safety Applications", in Proceedings of *1st Networking/Partnering Day 2010*, European Space Agency/ESTEC Conference, Noordwijk, The Netherlands, January 2010.

- G. Iapichino, C. Bonnet, O. Del Rio, C. Baudoin, and I. Buret, "Combining Mobility and Heterogeneous Networking for Emergency Management: a PMIPv6 and HIP-based Approach", in Proceedings of *ACM International Workshop on Advanced Topics in Mobile Computing for Emergency Management: Communication and Computing Platforms*, in conjunction with IWCMC 2009, Leipzig, Germany, June 2009.

- G. Iapichino, C. Bonnet, O. Del Rio, C. Baudoin, and I. Buret, "Mobility, Access Heterogeneity and Security for Next Generation Public Safety Communications", in Proceedings of *IEEE Workshop on Next Generation Public Safety Communication Networks and Technologies*, in conjunction with ICC 2009, Dresden, Germany, June 2009.

- G. Iapichino, C. Bonnet, O. Del Rio, C. Baudoin, and I. Buret, "A Mobile Ad-hoc Satellite and Wireless Mesh Networking Approach for Public Safety Communications", in Proceedings of *10th IEEE International Workshop on Signal Processing for Space Communications*, (SPSC 2008), Rhodes, Greece, October 2008.

- G. Iapichino, C. Bonnet, O. Del Rio, C. Baudoin, and I. Buret, "Advanced Hybrid Satellite and Terrestrial System Architecture for Emergency Mobile Communications", in Proceedings of *26th AIAA International Communications Satellite Systems Conference*, (ICSSC 2008), San Diego, USA, June 2008.

- G. Iapichino, C. Bonnet, “Security scenario definition report”, Eurecom, Rapport de Recherche, RR-08-216, Sophia Antipolis, France, March 2008.

Chapter 7 - Conclusions and future directions

This chapter performs an evaluation of the work highlighting the most important aspects and achievements of the thesis. It also points to some future directions for this work and perspectives for research in the fields concerned by this thesis.

Chapter 2

Internet Mobility Support

2.1 Introduction

In the early days of the development of the Internet architecture mobile nodes were not the common network entity that they are today. The most part the entities attached to what became the Internet were large mainframe and minicomputers. Today on the other hand the trend is for relatively more mobile wireless computing devices, not only the laptop for the mobile professional, but also mobile PDAs and phones with data capabilities. As these types of devices increase, and the ways of connecting to the Internet through these types of devices proliferate, mobility will be the common use case and fixed stations will become proportionately less.

This chapter looks at the different existing design systems supporting mobility and provides an overview on the key components of mobility management together with correlated mobility aspects, such as routing, access control, security and multihoming.

2.2 Mobility Support in Different Designs

2.2.1 Basic Components for Mobility Support

Mobility approaches for the Internet have long focused on the need to provide address continuity for mobiles as they move around the network. The natural way to provide mobility seems to be to provide a new IP address for a mobile node at each of its points of attachment as it moves around the Internet, and in particular across a mobility event, when the mobile node has changed from one point of attachment on one subnet to a different point of attachment on another subnet. But many applications require the address to remain stable because they are using the address as an identifier rather than a locator, so there needs to be a mapping between the address that changes naturally as the mobile node moves and the one that remains constant while the application remains active.

These two fundamentally different aspects of addressing highlight a key issue in the use of the IP address. Different layers in the IP stack in a node use the IP address in two fundamentally different ways [6]:

1. To the transport layer, where TCP and User Datagram Protocol (UDP) reside, the IP address serves as a communications identifier used to record the identity of the entity at the other end of a communication.

2. To the network layer, where IP resides, the IP address serves to record the location of the IP node, so that all the routers between the communicating entities know where to forward the packet to get it to the right destination.

When a node is stationary these two functions coincide, but when a node is mobile, the opposite endpoints of the communication need to maintain communication by keeping track of identity which does not change, but deliver packets to the correct location which has changed.

In order to support such fully mobile usage, a mobility scheme must be deployed. It will maintain session continuity between a mobile node and the endpoint with which it is corresponding as the mobile moves from one endpoint to another. Such a mobility scheme will alleviate the difficulties caused by the two uses of the IP address, one as an endpoint identifier and the other as a location marker.

In summary, supporting mobility essentially involves three basic components [7]: a *stable identifier* for a mobile, an *IP address* of the mobile's current location, and a *mapping* between the two. Different mobility support designs have adopted different ways to choose mobile identifiers and different approches to provide mapping between the identifiers and the mobiles current IP addresses [8]. They are analysed hereafter.

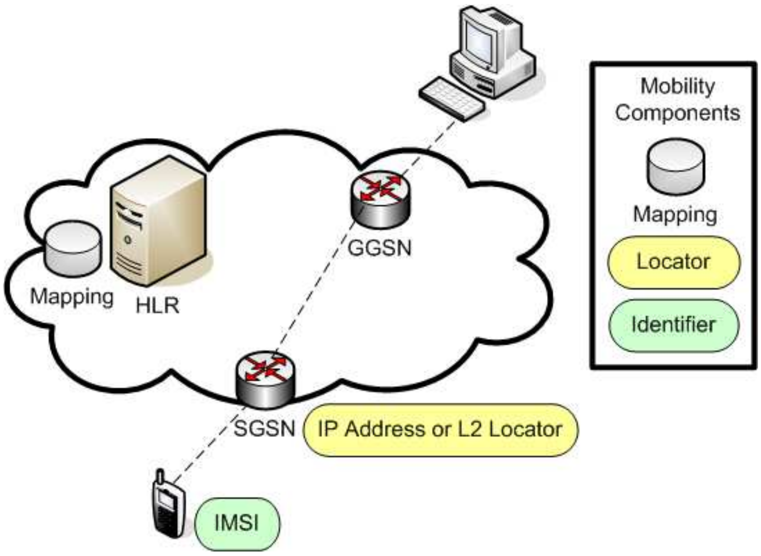

Figure 2.1: Mobility Components in GPRS.

2.2.2 General Packet Radio Service

The 3GPP has developed a set of technology specific protocols for Global System for Mobile communication (GSM) networks called General Packet Radio Service (GPRS) [9]. It has been widely deployed on GSM, Enhanced Data rates for GSM Evolution (EDGE), and Universal Mobile Telecommunications System (UMTS) cellular systems, and an interface is also available for 802.11 Wireless Local Area Network (WLAN). In general, GPRS provides more services than mobility management, and much of the signaling is tied closely to the Signalling System No.7 (SS7)/Mobile Application Part (MAP) protocol used in legacy GSM networks. As such, it is not an Internet protocol even though the GPRS Tunnelling Protocol (GTP) parts of the protocol set use IP for transport. GTP is separated into a control plane protocol (GTP-C) and bearer plane protocol (GTP-U) with the GTP-U providing tunneling. However, when considering only the GTP parts of the protocol, GPRS provides a kind of IP localized mobility management that requires minimal host involvement. From the IP perspective, the mobile node attaches to a single subnet while it moves around a particular GPRS domain.

GPRS does this by establishing overlay routes between the access routers and a mobility anchor router, called a Gateway GPRS Support Node (GGSN) on the Internet side of the access routers (the function that we identify as the access router in the GPRS architecture is called the SGSN, the Serving GPRS Support Node). The GGSN acts as a gateway between the overlay network and an external routed IP network. When a mobile node moves between SGSNs, signaling at the link layer between the mobile node and network is necessary to set up the mobile node on the new link. This signaling triggers a routing update from the SGSN to the GGSN. The signaling causes the GGSN to change the overlay route so that packets to/from the mobile node now go through the new SGSN. From the mobiles point of view nothing has happened at the IP layer and the SGSN is not providing a local subnet for the mobile nodes. The mobile perceives itself as always at home even though the router serving the subnet containing its address may be nowhere near geographically.

The GPRS identification procedure is used to request the mobile to provide specific identification parameters such as the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI). The location of the mobile is represented by the SGSN the mobile is connected to and the GGSN carries out a role equivalent to the Home Agent in Mobile IP. The home service provider keeps the mapping of its number and its location at the Home Location Register (HLR). The GPRS' mobility components are shown in Fig. 2.1.

2.2.3 Mobile IPv6

Mobile IPv6 (MIPv6) [10] specifies a protocol which allows nodes to remain reachable while moving around in the IPv6 Internet. Each Mobile Node (MN) is always identified by its Home Address (HoA), regardless of its current point of attachment to the Internet. A MN is always expected to be addressable at its HoA, whether it is currently attached to its home link or is away from home. The HoA is an IP address assigned to the mobile node within its home subnet prefix on its home link. While a MN is at home, packets addressed to its HoA are routed to the MN's home link, using conventional Internet routing mechanisms.

While a MN is attached to some foreign link away from home, it is also addressable at one or more Care-of Addresses (CoAs). A CoA is an IP address associated with a MN that has the subnet prefix of a particular foreign link. The CoA represents the locator for the MN. The MN can acquire its CoA through conventional IPv6 mechanisms, such as stateless or stateful auto-configuration. As long as the MN stays in this location, packets addressed to this CoA will be routed to the MN. The MN may also accept packets from several CoAs, such as when it is moving but still reachable at the previous link.

The association between a MN's HoA and CoA is known as a "binding" for the MN. While away from home, a MN registers its primary CoA with a router on its home link, requesting this router to function as the Home Agent (HA) for the MN. The MN performs this binding registration by sending a Binding Update (BU) message to the HA. The HA replies to the MN by returning a Binding Acknowledgement (BA) message. The HA represents the entity responsible for the mapping between the HoA and the CoA. Any node communicating with a MN is called a Correspondent Node (CN) of the MN, and may itself be either a stationary node or a mobile node. A MN can provide information about its current location to CNs. This happens through the correspondent registration. As a part of this procedure, a return routability test is performed in order to authorize the establishment of the binding. Figure 2.2 shows the mobility components in MIPv6.

There are two possible modes for communications between the MN and a CN. The first mode, bidirectional tunneling, does not require MIPv6 support from the CN and is available even if the MN has not registered its current binding with the CN. Packets from the CN are routed to the home agent and then tunneled to the MN. Packets to the CN are tunneled from the MN to the HA ("reverse tunneled") and then routed normally from the home network to the CN. In this mode, the HA uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the MN's home address (or home addresses) on the home link. Each intercepted packet is tunneled to the MN's primary CoA. This tunneling is performed using IPv6 encapsulation. With the second mode, that is route optimization, the communication between MN and CN can be direct without going through the HA. This is one of the main advantages of MIPv6 over MIPv4, where route optimization is not possible. Route optimization requires that the MN registers its current binding at the CN. Packets from the CN can be routed directly to the CoA of the MN. When sending a packet to any IPv6 destination, the CN checks its cached bindings for an entry for the packet's destination address. If a cached binding for this destination address is found, the node uses a new type of IPv6 routing header to route the packet to the MN by way of the CoA indicated in this binding.

Figure 2.3 describes the mobility mechanisms in MIPv6.

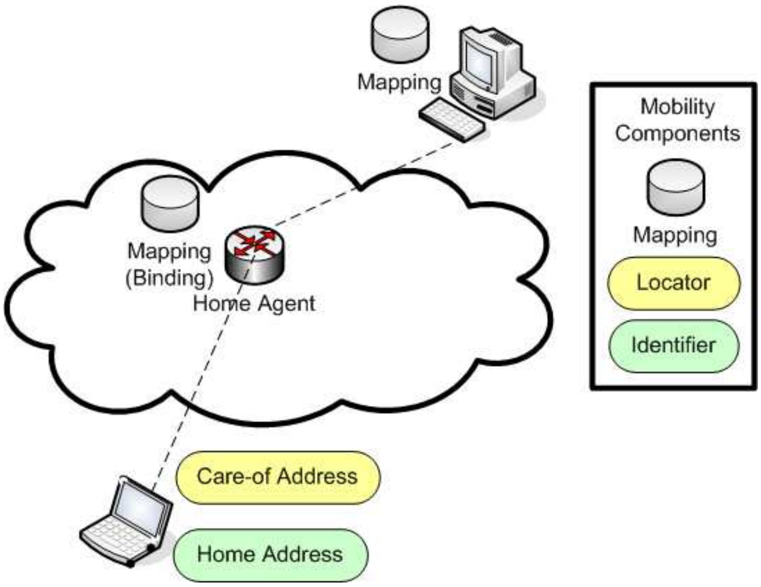

Figure 2.2: Mobility Components in Mobile IPv6.

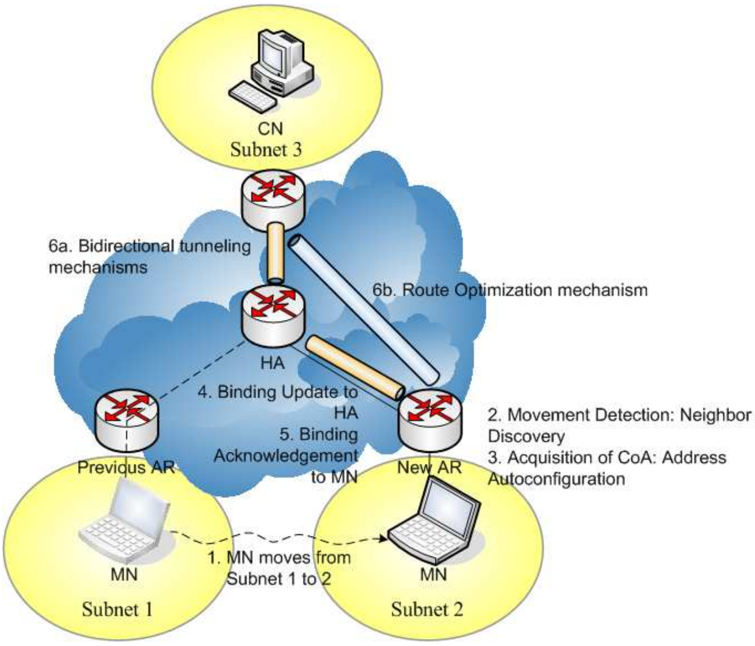
CN
Subnet 3
6a. Bidirectional tunneling mechanisms
6b. Route Optimization mechanism
HA
4. Binding Update to HA
5. Binding Acknowledgement to MN
2. Movement Detection: Neighbor Discovery
3. Acquisition of CoA: Address Autoconfiguration
Previous AR
New AR
MN
1. MN moves from Subnet 1 to 2
MN
Subnet 1
Subnet 2

Figure 2.3: Mobile IPv6 Mechanism.

2.2.4 Proxy Mobile IPv6

3GPP has closely investigated the mobile operator requirements from a service aspect point of view. The requirement to provide handover capability within and between access systems with no perceivable service interruption has been identified. This means that the delay introduced by the mobility management procedure must be minimized. Efficient use of wireless resources is another requirement for mobility management because wireless resources could be a bottleneck. Finally, it is generally desirable to minimize MN involvement in mobility management to improve the battery life of the terminal. Network-based mobility management fulfills very well these requirements, thus Proxy Mobile IPv6 (PMIPv6) [5], an extension of MIPv6 which frees MNs from performing any mobility-related signaling, has been chosen by cellular operators and adopted as the IP mobility protocol for mobility between 3GPP and non-3GPP accesses and as an option for intra-3GPP access mobility.

With PMIPv6 the network takes the responsibility for managing IP mobility on behalf of the MN within a single operators network. Each mobile retains its IPv6 address when it roams within its domain (a network that uses PMIP for mobility support), and thus this address is equivalent to the HoA in MIPv6, i.e. the identifier of the mobile. The core functional entities are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). The LMA is responsible for maintaining the MN's reachability state and is the topological anchor point for the MN's Home Network Prefix (HNP). The MAG is the entity that performs the mobility management on behalf of a MN and it resides on the access link where the MN is anchored. The MAG is responsible for detecting the MN's movements to and from the access link and for initiating binding registrations to the MN's LMA. The IP address of MAG is used to reach the mobile, thus represents the locator for the MN, and LMA is the entity which keeps the mapping between the Home Address of the mobile and the address of serving MAG. Figure 2.4 shows the mobility components in PMIPv6 and Fig. 2.5 its mechanism.

As shown in Fig. 2.6, once a MN enters a Proxy Mobile IPv6 domain and attaches to an access link, the MAG on that access link, after identifying the MN and acquiring its identity, determines if the MN is authorized for the network-based mobility management service. If the network determines that the network-based mobility management service needs to be offered to that mobile node, the network will ensure that the MN using any of the address configuration mechanisms permitted by the network will be able to obtain the address configuration on the connected interface and move

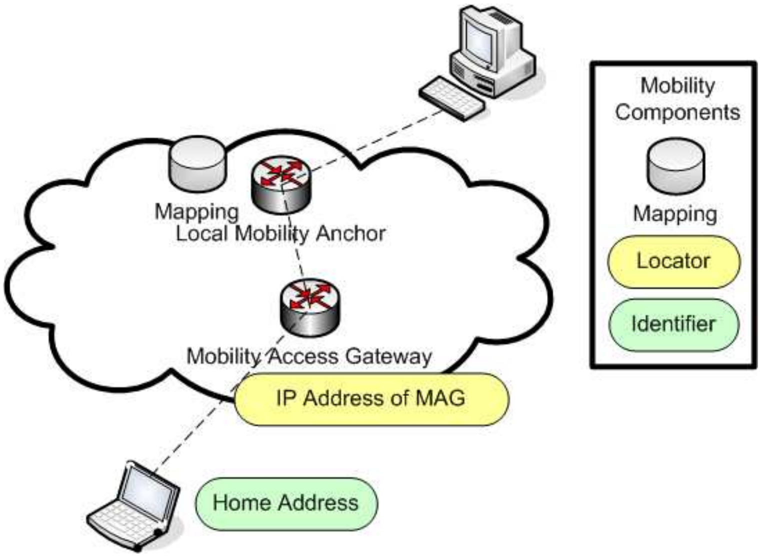

Figure 2.4: Mobility Components in Proxy Mobile IPv6.

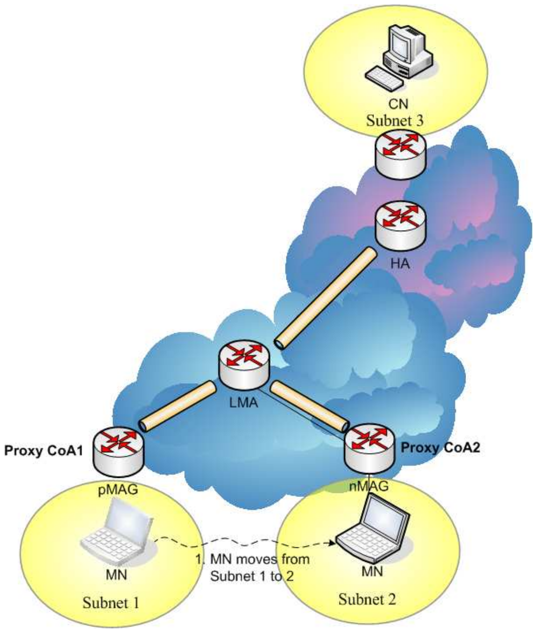

Figure 2.5: Proxy Mobile IPv6 Mechanism.

anywhere in that Proxy Mobile IPv6 domain. The obtained address configuration includes the address(es) from its home network prefix, the default router address on the link and other related configuration parameters. From the perspective of the mobile node, the entire Proxy Mobile IPv6 domain appears as a single link, the network ensures that the mobile node believes it is always on the same link where it obtained its initial address configuration, even after changing its point of attachment in that network.

For updating the LMA about the current location of the MN, the MAG sends to it a Proxy Binding Update (PBU) message. Upon accepting this PBU message, the LMA sends a Proxy Binding Acknowledgement (PBA) message including the MN's HNP. It also creates the Binding Cache entry and sets up its endpoint of the bi-directional tunnel to the MAG.

The MAG on receiving the PBA message sets up its endpoint of the bi-directional tunnel to the LMA and also sets up the data path for the MN's traffic. At this point the MAG has all the required information for emulating the MN's home link. It sends Router Advertisement (RA) messages to the MN on the access link advertising the MN's home network prefix as the hosted on-link-prefix.

The MN on receiving these Router Advertisement messages on the access link attempts to configure its interface either using stateful or stateless address configuration modes, based on the modes that are permitted on that access link. At the end of a successful address configuration procedure, the MN ends up with an address from its home network prefix. Once the address configuration is complete, the MN has a valid address from its home network prefix at the current point of attachment. The serving MAG and the LMA also have proper routing states for handling the traffic sent to and from the MN using an address from its home network prefix.

The LMA, being the topological anchor point for the MN's home network prefix, receives any packets that are sent to the MN by any node in the network and it forwards them to the MAG through the bi-directional tunnel. The MAG on other end of the tunnel, after receiving the packet, removes the outer header and forwards the packet on the access link to the MN. The MAG typically acts as a default router on the access link. It intercepts any packet that the MN sends to any CN and sends them to its LMA through the bi-directional tunnel. The LMA on the other end of the tunnel, after receiving the packet, removes the outer header and routes the packet to the destination.

Figure 2.7 shows the signaling call flow for the MN's handoff from previously attached MAG (pMAG) to the newly attached MAG (nMAG). After obtaining the initial address configuration in the Proxy Mobile IPv6 domain,

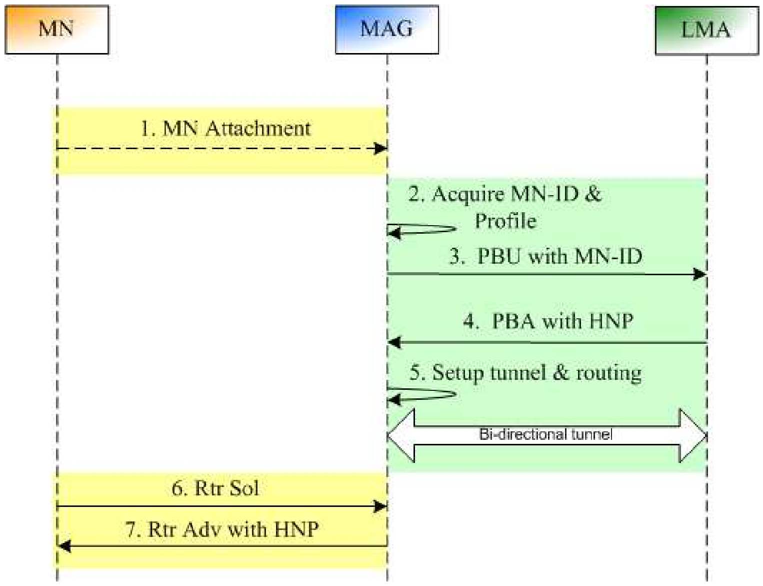

Figure 2.6: Attachment and Registration in Proxy Mobile IPv6.

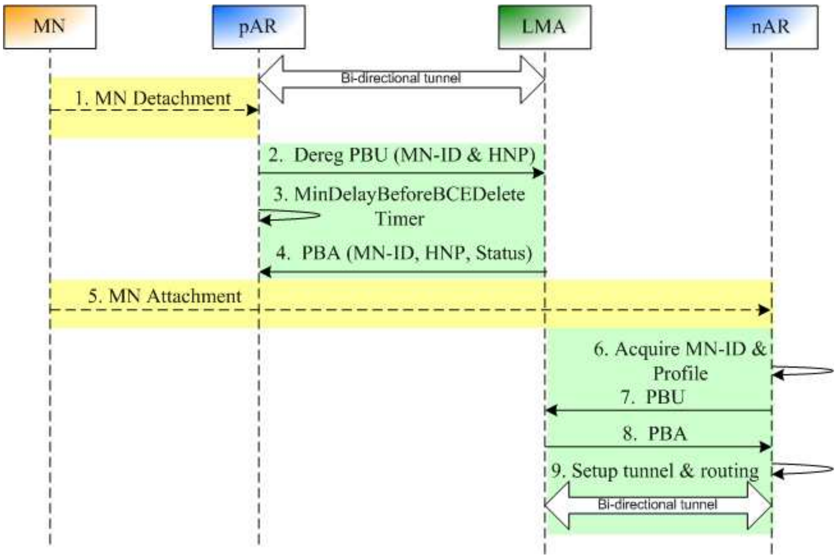
MN
pAR
LMA
nAR
Bi-directional tunnel
1. MN Detachment
2. Dereg PBU (MN-ID & HNP)
3. MinDelayBeforeBCEDelete Timer
4. PBA (MN-ID, HNP, Status)
5. MN Attachment
6. Acquire MN-ID & Profile
7. PBU
8. PBA
9. Setup tunnel & routing
Bi-directional tunnel

Figure 2.7: Handover in Proxy Mobile IPv6.

if the MN changes its point of attachment, the pMAG detects the MN's detachment from the link, signals the LMA and removes the binding and routing state for that MN. The LMA, upon receiving this request, identifies the corresponding mobility session for which the binding update request was received and, once it accepts, the request waits for certain amount of time for allowing the nMAG to update the binding.

The nMAG upon detecting the MN on its access link signals the LMA for updating the binding state. Once that signaling is complete, the MN continues to receive the Router Advertisements containing its home network prefix, making it believe it is still on the same link and it will use the same address configuration on the new access link.

2.2.5 Host Identity Protocol

The Host Identity Protocol [4] puts the mapping in a new layer, the Host Identity layer, just above the IP layer. HIP assigns each host a cryptographic-based identifier which is totally independent from its IP address of the current location. A mobile updates its relative entry in the Domain Name Server (DNS) when moving to a new address. DNS is used to provide the mapping between the identifier and up-to-date IP address for a mobile. Figure 2.8 shows the mobility components in HIP. HIP may also use a dedicated server other than DNS, known as Rendezvous Server (RDV) [11].

HIP separates the locator and identifier roles of IP addresses by introducing a new name space, the Host Identity (HI) name space. In HIP, a Host Identity is a public cryptographic key from a public-private key-pair. A host possessing the corresponding private key can prove the ownership of the public key, i.e. its identity. This separation of the identifiers and locators makes it also simpler and more secure to handle mobility and multi-homing than what is currently possible.

Figure 2.9 shows where the new HIP sublayer is located in the current stack. On the layers above the HIP sublayer, the locator(s) of the host do not need to be known. Only the HI or its 128-bit representation, the Host Identity Tag (HIT), are used. The Host Identity sublayer maintains mappings between identities and locators. When a mobile host changes its location, HIP is used to transfer the information to all peer hosts. The dynamic mapping from the identifier to locators, on other hosts, is modified to contain the new locator information. Upper layers, e.g. applications, can remain unaware of this change; this leads to effective division of labour and provides for backwards compatibility. During the connection initialisation between two HIP hosts, a four-way handshake, called Base Exchange

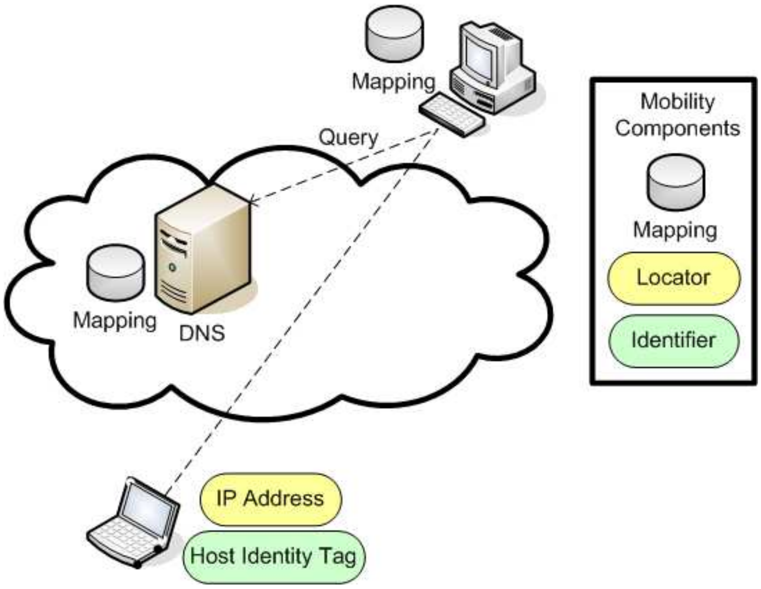

Figure 2.8: Mobility Components in Host Identity Protocol.

(BE), is run between the hosts. During the exchange, the hosts identify each other using public key cryptography and exchange Diffie-Hellman public values. Based on these values, a shared session key is generated. Further, the Diffie-Hellman key is used to generate keying material for other cryptographic operations, such as message integrity and confidentiality. During the Base Exchange, the hosts negotiate what cryptographic protocols to use to protect the signalling and data messages. As of today, the default option is to establish a pair of IPsec Encapsulated Security Payload (ESP) Security Association (SA) between the hosts. The ESP keys are retrieved from the generated Diffie-Hellman key and all further user data traffic is sent as protected with the ESP SAs.

HIP Base Exchange

The Base Exchange is depicted in Fig. 2.10. It consists of four messages, named by letters and numbers. The letters denote the sender of the packet, I for initiator or R for responder. The numbers are simply sequential. Hence, the four messages are named as I1, R1, I2, and R2. The I1 message is a mere trigger. It is used by the initiator to request an R1 message from the responder. By default, any HIP host that receives an I1 packet will blindly

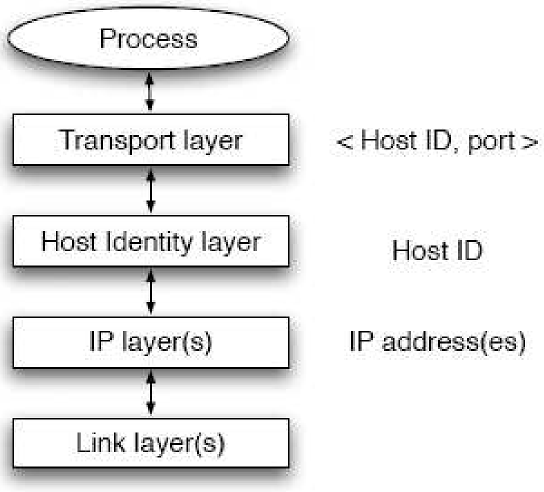

Figure 2.9: Host Identity Protocol Architecture.

reply with an R1 packet; that is, the responder shall not remember the exchange.

Remaining stateless while responding to an I1 with an R1 protects the responder from state-space-exhausting denial-of-service attacks. However, as a side effect it adds flexibility to the architecture. It does not need to be the responder itself that replies to an I1. Hence, if there is some other means by which the initiator may acquire a fresh R1 message, such as a directory look up, it is perfectly fine to skip the I1/R1 exchange. As long as the host responding with an R1 has a supply of fresh R1s from the responder, it can be any node.

The R1 message contains a cryptographic puzzle, a public Diffie-Hellman key, and the responders public Host Identity key. The Diffie-Hellman key in the R1 message allows the initiator to compute the Diffie-Hellman session key. Hence, when constructing the I2 message it already has the session key and can use keys derived from it.

In order to continue with the base exchange, the initiator has to solve the puzzle and supply the solution back to the responder in the I2 message. The purpose of this apparently resource-wasting method is to protect the responder from CPU-exhausting denial-of-service attacks by enforcing the initiator to spend CPU to solve the puzzle. Given the puzzle solution, the responder can, with very little effort, make sure that the puzzle has been recently generated by itself and that is has been, with high probability,

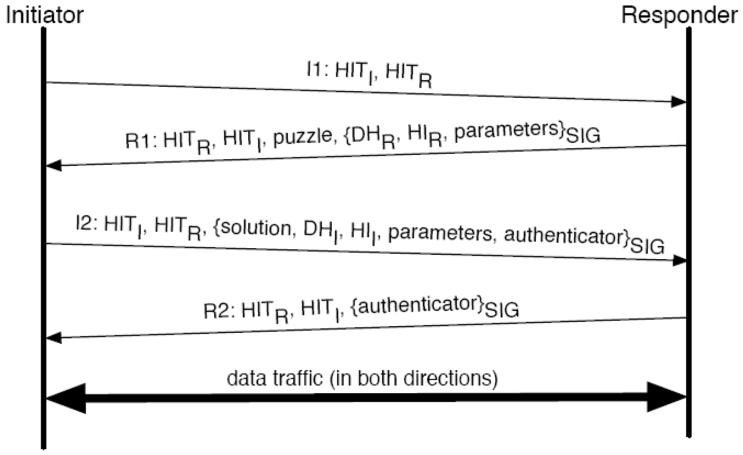
Initiator
Responder
I1: HIT_I, HIT_R
R1: HIT_R, HIT_I, puzzle, $\{DH_R, HI_R, \text{parameters}\}_{SIG}$
I2: HIT_I, HIT_R, $\{\text{solution}, DH_I, HI_I, \text{parameters, authenticator}\}_{SIG}$
R2: HIT_R, HIT_I, $\{\text{authenticator}\}_{SIG}$
data traffic (in both directions)

Figure 2.10: Host Identity Protocol Base Exchange.

solved by the initiator and is not a result of a puzzle posted much earlier or a puzzle generated by someone else. That is, by verifying the puzzle solution the responder knows that, with high probability, the initiator has indeed used quite a lot of CPU to solve the puzzle. This, seemingly, is enough to show the initiator's commitment to the communication, thereby warranting the forthcoming CPU cycles that the responder needs to process the rest of the I2 message. The difficulty of the puzzle can be varied depending on the load of the responder. For example, if the responder suspects an attack, it can post harder puzzles, thereby limiting its load.

The I2 message is the main message in the protocol. Along with the puzzle solution, it contains the initiators public Diffie-Hellman key, the initiators public Host Identity key, optionally encrypted with the Diffie-Hellman key, and an authenticator showing that the I2 message has been recently constructed by the initiator.

Once the responder has verified the puzzle, it confidently can continue to construct the Diffie-Hellman session key, to decrypt the initiators Host Identity public key (if encrypted), and to verify the authenticator. If the verification succeeds, the responder knows that there is out there a host that has access to the private key corresponding to the initiators Host Identity public key, that the host wants to initiate a HIP association with it, and that the two hosts share a Diffie-Hellman session key that no other node knows. Given this information, the responder can consult its policy database to determine if it wants to accept the HIP association or not. If it does, the responder computes an authenticator and sends it as the R2 packet to the initiator.

2.3 Mobility Management

A fundamental component of mobility support, and in particular of IP mobility support, in all the different designs considered above is the mobility management. It consists of two main components: location management and handoff management.

Location management enables the system to track the location of MNs between consecutive communications, discovering their current points of attachment to the system. It includes two major tasks: *location registration* (or *location update*) and *data delivery.* During the first step, the MN periodically notifies the network of its access point, allowing the system to authenticate the MN and to update relevant location databases with its up-to-date location information. The second task consists of determining the serving location directory of the receiving MN and locating its visiting cell/subnet.

Handoff management is the process by which the system maintains a user's connection as the MN continues to move and change its access point to the network. It involves three stages: *initialization*, *new connection generation* and *data flow control.* During initialization, the user, the network agent or changing network conditions identify the need for handoff. In the second stage, the network must find new resources for the handoff connection and perform any additional routing operations. During the final step, the delivery of the data from the old connection path to the new connection path is maintained according to agreed-upon service guarantees.

The handoff process can be intra-system or inter-system. The first type, also called *horizontal handoff*, occurs when the user moves within a service area (or cell) and experiences signal strength deterioration below a certain threshold that results in the transfer of the user's services to new radio channels of appropriate strength at the same base station. The intersystem handoff or *vertical handoff* arises when the user is moving out of the serving network and enters another overlaying network, when it is connected to a particular network but chooses to be handed off to another network for its future service needs, or when it distributes the overall network load among different systems to optimize the performance of each individual network.

Mobility management can be broadly classified into two schemes: Global Mobility Management (GMM) or macro-mobility and Local Mobility Management (LMM) or micro-mobility. Moreover, mobility management protocols can be distinguished between host-based and network-based.

2.3.1 Global vs. Local Mobility Management

Global mobility management is the movement of mobile nodes between two subnets in two different network domains, while local mobility management is the movement of mobile nodes between two subnets within the same domain. On a operator's point of view, global mobility management handles changes between different serving network providers' subnets, i.e. the home network provides a global endpoint identifier and global mobility anchor for the mobile node, while local mobility management handles mobility within the serving operator's network, to avoid requiring the mobile node to signal back to the home operator's network upon every movement between access routers.

It is worthwhile to attempt to make some distinction between local mobility and global mobility based on topological distance in the routing infrastructure. Topological distance between two subnet locations can be characterized by the number of routing hops between the two last hop routers, the routers that deliver packets to a mobile node over a particular access link. When there are few such routing hops, the subnets are "close", and if there are many such routing hops the subnets are topologically "far". Due to artifacts of network deployments, topologically close subnets may often have similar subnet identifiers, often with a subset of their prefixes being shared if the routing for the network is well aggregated. This topological closeness can help differentiate also between localized mobility management and global mobility management.

It is also important to realize that the topological distance between two subnets will often have little or no relationship to the geographical distance between the access routers serving the mobile nodes in the two different networks. A mobile node may see access routers in two different networks over two different kinds of access technologies at the same time. But these two access routers may be topologically very far apart, perhaps in different BGP Autonomous Systems, even though the radio coverage of the two access networks mostly overlap. So if the mobile node "moves" from one of these access networks to the other (detaches itself from one network an attaches itself to another), the mobility event should be considered a global mobility event. It is also important to note that topologically close subnets may cover a wide geographic area and that for a mobile node to move between the two coverage areas would require the mobile itself moving geographically over a long distance. So when thinking about network architecture and mobility management protocols it is important to keep in mind that the important characteristic is topological distance rather than geographical distance because we are dealing with forwarding packets to the correct location over an infrastructure that does not always correlate well with geographical distance. There are deployed examples of very small topological differences covering large (country-sized for example) geographical distance.

MIPv6 and HIP are both global mobility management protocols. They require no special knowledge of local network that a mobile node visits, other than simple IP subnet configuration information, and they utilize a globally reachabile mobility anchor, the home agent and the DNS respectively. Anyway, the layer in which they operate the mapping is different: at network layer for the HA and at Host Identity layer for the DNS, thus bringing to a complete different mobility architecture.

On the other side, GPRS and PMIPv6 are local mobility management protocols. GPRS is localized as it is operating within some part of a service providers network. It combines an IP mobility protocol called GTP with a cellular specific set of protocols for managing mobile nodes within a specific cellular domain. The mobility protocol in GPRS is not wholly separate from the specifics of the cellular network. In PMIPv6 the LMA serves as a local anchor node which maintains the mapping between a mobile node's identity and its current location. It is similar to the HA in MIPv6, but it is only anchoring mobiles in a particular localized domain.

2.3.2 Host vs. Network-based Mobility Management

Global and localized mobility management can be either based within the host, as with MIPv6 and HIP, or in the network, as with GPRS and PMIPv6.

In host-based protocols, the host itself detects the movement at the IP layer and performs the signaling that updates the mapping between the forwarding identifier and the endpoint identifier, wherever that mapping might be maintained. In network-based mobility management protocols within some restricted localized mobility management domain, the network arranges so that the host does not detect any subnet movement when it moves to a new access router, but the access router signals to a mobility anchor on behalf of the mobile that movement has occurred. The host therefore is not required to update the forwarding identifier to endpoint identifier mapping, because the mobility anchor rearranges the overlay routing so that the old address can still be used as a forwarding identifier.

The two approaches have different impact on deployment and performance points of view:

- Host-based network layer approaches require protocol stack modification of the MN in order to support them, causing increased complexity on the MN. Network-based approaches support unmodified MNs, accelerating their practical deployment.
- Host-based approaches imply tunneling overhead as well as significant number of mobility-related signaling message exchanges via wireless links due to the MNs involvement in the mobility signaling. On the other side, with a network-based solution, an efficient use of wireless resources can result in the enhancement of network scalability and handover latency.

For purposes of having a globally deployable, Internet based, easy to use mobility management architecture, a combination of host-based global mobility management and network-based localized mobility management seems to be a good choice.

Host-based global mobility management is necessary because hosts are often aware of multiple potential serving networks and only the host can choose among these multiple networks or detect when it has moved to a new serving network. IP network service providers typically do not have the same kind of tight business links that traditional cellular providers have, so requiring the network to perform this function may require the home network operator to place too much trust in the serving network operator. If the host performs this function, the home network operator maintains a tight, end to end connection with the customer and doesn't require special business and security arrangement with all the possible serving networks to which the mobile node's user might roam.

Network-based localized mobility management allows the serving network to optimize IP handover to remove the long signaling latencies involved in using global mobility management on every move. In addition, because the serving network handles the mobility management within itself, no host to network security is required for mobility management except for movement detection, and that is required in any case for detecting global mobility. Network-based localized mobility management also supports tight integration with radio resource management and traffic engineering, allowing the serving operator to more efficiently manage its network.

2.4 Related Aspects to Mobility Support

2.4.1 Mobility and Routing

Mobility with mapping mechanisms and routing can be strictly interconnected. All the abovementioned protocols provide a mapping between a mobile's stable identifier and its dynamically changing IP address. This allows a mobile node to update only a single binding location about its location change. When the mapping is done at IP layer, the mobility design offer the advantage of hiding the mobility from correspondent nodes throught one level of indirection. When a correpondent node sends packets to an IP address which is a mobile's identifier, the packets will be delivered to the location where the mapping information of the mobile is kept, so that the packets can be delivered to the mobile's current location via either encapsulation or destination address translation. Although this one level of indirection at IP layer makes mobility transparent, it has a potential side effect of introducing non optimal routing: the path taken by the packets via the mapping point can be much longer than the direct path between the correspondent and the mobile's current location. As increasing number of mobile devices are connected to Internet, some mobility solutions, as HIP, have opted to expose mobility to both ends and let them communicate directly. One common approach is to use DNS for the mapping function to keep track of mobile current locations. Mobiles use dynamic DNS updates to keep their DNS servers updated with their current locations, using for example the Rendezvous Server.

An other approach is to support mobility through dynamic routing. In such design, a mobile keeps its IP address regardless of its location changes, thus the IP address can be used both to identify the mobile and to deliver packets to it. As a result, such designs do not require an explicit mapping function. Rather, the routing system must continuously keep track of mobile's movements and reflect their current positions in the network on the routing table, so that at any given moment packets carrying the (stable) receiver's IP address can be delivered to the right place. This is the case of Border Gateway Protocol (BGP) for example. Supporting mobility through dynamic routing is conceptually simple as it does not require a mapping function. It also provide robust and efficient routing, assuming that the routing system can keep up with the mobile movements. However, because the whole network must be informed of every movement of every mobile, this approach is feasible only in small scale networks with a small number of mobiles; it does not scale well in large networks or for large number of mobiles.

An efficient mobile system architecture should consider mobility management central and integrated with the routing architecture, rather than an add on.

2.4.2 Mobility and Access Control

Providing Internet connectivity to a mobile means two things: the mobile is connected to Internet, and it can be reached by any correspondent. The former involves access control, and the latter mobility management. Depending on the system design these two functions can be strictly interconnected or not.

Cellular networks implement both functions in a combined way. First, each cellphone is made uniquely identifiable through its SIM card given by its home service provider. Second, when a cellphone C wanders into the territory of a foreign provider, through a global number database the foreign provider can find C's home service provider. If the latter has contractual relations with the former, then C can be granted network access. Third, when someone makes a call to C, the call is first routed to the home service provider and then redirected to C's current location. Here we note 3 essential pieces in this mobility support design: (1) the unforgeable identity of the cellphone, (2) the global database to find the home provider, and (3) the dual role of the home service provider: not only it performs mobility management for the cellphone, it also keeps the accounting book with foreign providers who grant the mobile device access to the foreign network resources. In other words, the access control and mobility management are bundled together as one service offer.

On the contrary, Internet mobility support concerns only the mobility management, assuming mobiles are already connected to Internet. Today's mobile laptops obtain Internet access as they go. It is up to individual devices and individual networks to decide whether to, and how to, grant network access to visiting mobile devices.

Due to fundamental differences between cellular networks and Internet, the cellular networks' mobility support model is simply not applicable to the Internet. First of all, today's moving hosts in general do not have an unforgeable identity. Although it is technologically feasible to assign each host a cryptographic-based identifier, as the work done by the IETF HIP working group, that is not the common practice for the moment. Thus moving laptops miss a fundamental component to mimic the access model used by cellphones. Second, different from cellular service market where a small number of major providers dominate (who also interconnect), there exist a large number of Internet service providers and most of them do not have direct interconnectivity; contractual relations only exist between topologically interconnected ISPs. Consequently, Internet access control and mobility are not connected. A mobile node obtains Internet access as it goes and receives mobility support from its anchor point.

2.4.3 Mobility and Security

An other important point in the mobility design is the security. Securing mobile movement updates, which may be sent to either Home Agents or DNS servers or other mobile nodes, is an essential requirement and the coordination between security mechanisms (e.g. IPSec) and mobility protocols is of paramount importance. Also the definition of the identifier in the design of the mobility system can add a strong level of security to the system architecture. This represents for example one of the weak points of Mobile IPv6 and its extensions. On the contrary, HIP uses cryptographic host identifiers as an integral part of connectivity, thereby providing automatic identity authentication. Moreover, the separation of identities and locators makes it easier to hide the topological location of communicating parties.

2.4.4 Mobility and Multihoming

Effective mobility support requires a level of indirection to map the mobile entity's stable name to its dynamic and changing location. Effective multihoming support (or support for multi-access / multi-presence) requires a similar kind of indirection, allowing the unique name of a multi-accessible entity to be mapped to the multitude of locations where it is reachable. Within the Internet community, the historical approach to solve these problems has been to consider mobility and multihoming as separate, technical problems, something that just needs to be solved through engineering. The main result of this attitude are Mobile IP protocols, which are architectural based on re-using a single namespace, the IP address space, for both stable host identifiers (Home Addresses) and dynamic locators (Care-of Addresses). While the approach works in basic network topologies, it creates to major drawbacks.

Firstly, it binds the communication sessions (TCP connections and application state) to the home addresses. This, in turn, when combined with the only known scalable solutions to a number of related security problems, creates an undesirable dependency on a constant reachability of the home address. In other words, the mobile host is intrinsically bound to the availability of the home addresses; the home agent becomes a new single point of failure. Secondly, approaches that use names from a single name space for multiple purposes create a number of potential semantic problems. For example, the so-called alias problem relates to the use of multiple names from a single name space to denote same entities in a non-transparent way. In practical terms, when Mobile IP is used, there is no easy way to tell if two IP addresses point to a single host (e.g., due to one being its home address and another one its care-of address) or not, i.e., whether one is merely an alias for the other or an identifier for a genuinely different host. For applications or users that cache previously used IP addresses and reuse them later, aliasing can cause applications to unknowingly connect to different hosts. On the other hand, multi-homing creates the inverse problem, where aliasing (multiple IP addresses pointing to a single host) is the desired outcome but the applications are not aware of it.

As briefly mentioned above, HIP provides an alternative approach to implementing mobility and multi-homing. It explicitly adds a new layer of indirection and a new name space, thereby adding the needed level of indirection to the architecture. Furthermore, the inherent ability to delegate, provided by the cryptographic nature of the Host Identifiers, allows HIP to provide more natural support for other granularities of mobility, such as application or sub-network mobility.

2.5 Conclusions

In this chapter we have presented a high level assessment on the current state of the art and general direction for mobility support in the Internet. MIPv6, GPRS, PMIPv6 and HIP have been described highlighting the basic components of their mobility system designs. Moreover, an accurate description of mobility management, distinguishing between global and local and between host-based and network-based, is provided together with an analysis of the additional aspects that influence Internet mobility support.

Chapter 3

Secure Global and Local Mobility Management

3.1 Introduction

A network-based local mobility management scheme provides an excellent method for a network service provider to provide a high quality user experience for a large number of subscribers through careful management of the network resources, with minimal interaction from the mobile node. At the same time there is a genuine need for subscribers with mobile nodes having multiple points of attachment to be able to select the network that is providing service and the type of service. These two operational needs dovetail nicely with a model that includes both a local mobility management protocol for the single network service and a global mobility management protocol for the multiple network service.

In this chapter we propose a secure global and local mobility management scheme suitable for multihomed mobile nodes. It is based on the host-based GMM scheme of Host Identity Protocol and on the network-based LMM scheme of Proxy Mobile IPv6. It merges the new identifier/locator split architecture proposed by HIP, especially designed for providing security and multihoming to MNs, with the micro-mobility management scheme of PMIPv6, which has been proposed for "unmodified" MNs with future Global Mobility Management protocols. HIP-PMIPv6 combination has double benefits. On one side, it represents an efficient micro-mobility solution for HIP. On the other side, it provides a GMM scheme for PMIPv6, which supports inter-technology handover and multihoming together with security.

3.2 Problem statement

In this section, we provide the motivation for the combination of HIP and PMIPv6 and an overview on the current problems which still need to be solved in both protocols.

3.2.1 ID/locator split and HIP micro-mobility

In the current Internet architecture the IP address is used for describing the topological location of the host, and at the same time, to identify the host. This feature is not efficient in handling mobility, so different schemes have been proposed to enhance current network model's support to mobility.

Among all the GMM schemes at IP layer, Mobile IPv6 [10] is the most known. As described in section 2.2.3, it assigns a new IP address, called CoA, to the mobile node each time it changes its point of attachment to the Internet. A binding between the HoA and the CoA is used by the MN for updating its Home Agent about its new IP address to maintain its reachability. Not only MIPv6 is just by-passing the main problem, but it also has major security flaws and requires important changes in the IP stack of the hosts, which prevent its widespread deployment. A new network architecture that could separate the identifier and the locator role of the traditional IP addresses is needed for the future Internet.

Host Identity Protocol [4], as described in section 2.2.5, is resolving this problem by introducing a Host Identifier for each MN and a new layer between the network and the transport layer. In HIP, the transport layer connections are bound to the Host Identity Tag (HIT), a 128-bit hash of the HI, not anymore to the IP address. HIP represents a new secure GMM protocol that overcomes MIPv6, providing security and inherent multihoming features to heterogeneous mobile networks with multihomed hosts [12], and having light impact on mobile terminals [13]. During BE, MNs create a session key through the Diffie-Hellman scheme, used then in the IPSec Encapsulating Security Payload (ESP) Security Association (SA). With HIP the SAs are bound to HITs, not to IP addresses as the current IPSec defines. Therefore the change of IP address is transparent to applications and SAs remain valid. When a host changes its address during a connection, it can send a HIP UPDATE packet to any HIP enabled correspondent peer. This

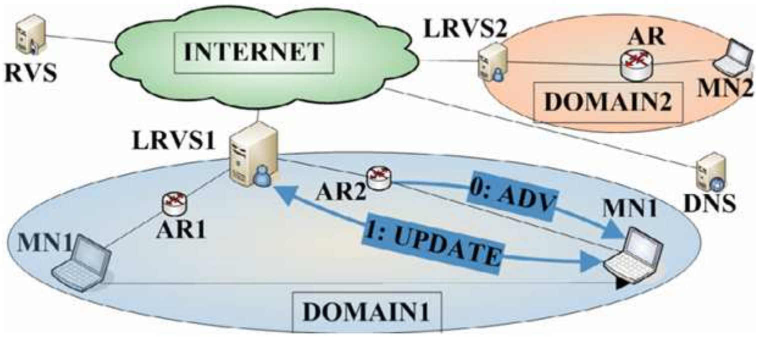

Figure 3.1: Novaczki's Micro-mobility for HIP.

packet contains the current ESP sequence number and Security Parameter Index (SPI) to provide denial-of-service and replay protection, and is authenticated with a HIP signature [12]. Mobility is handled via secure DNS updates just as in end-to-end mobility, but, to avoid frequent DNS updates, HIP introduces a new entity called Rendezvous Server (RVS) [11]. The DNS stores the HIT of the MN together with a stable locator, thus the RVS' IP address, and the RVS is in charge of keeping updated information about MN's current locator. The RVS replaces the role of HA in MIPv6.

Anyway, an efficient micro-mobility solution for HIP is still missing. Current solutions take inspiration from micro-mobility schemes for MIPv6 [14] [15]. Having in mind such a different Internet architecture, they do not represent an optimized solution for HIP.

In [14], Novaczki et al. propose a micro-mobility scheme for HIP similar to HMIPv6. They introduce a new entity, the Local Rendezvous Server (LRVS), which acts as the Mobile Anchor Point (MAP) for HMIPv6. The MN needs to register itself in the RVS and in the LRVS. When the MN moves inside the domain, it needs to notify the LRVS of its new address and not anymore the CN. The scheme is illustrated in Fig. 3.1. The LRVS is in charge of redirecting all HIP-based communication streams into its new address. As a drawback, this scheme is affected by the high number of messages needed to update the LRVS for each MN's movement and by the fact that the LRVS has to be a Security Parameter Index multiplexed Network Address Translator (SPINAT) device [16] to allow the overlay routing based on SPI.

In [15], So and Wang propose a new HIP architecture composed of micro-HIP (mHIP) agents: mHIP gateways and mHIP routers. mHIP agents under the same network domain share a common HIT to represent the whole mHIP domain and can sign messages on behalf of the group. This scheme permits to distribute the load of the LRVS in Novaczki's scheme among mHIP agents and provides a framework in which any type of security scheme can be adopted. As in the LRVS of Novaczki's scheme, a modified SPINAT device has to be implemented in the mHIP agents. In the same way, the MN registers itself in the RVS and in the mHIP gateway, with the difference that the MN registers itself in the RVS with the HIT of the mHIP gateway. This behavior breaks the macro-mobility support of HIP, as changing domain for the MN will imply changing HIT, thus breaking previous sessions.

3.2.2 PMIPv6 inter-technology handover with multihoming

An important point raised in [17] is the fact that wireless IP nodes may support in the future a GMM protocol that is not MIPv6. This has led to the design of a new network-based scheme for LMM, which does not require any additional effort to implement, deploy, or in some cases, even specify in a non-Mobile IPv6 mobile environment: the Proxy Mobile IPv6 protocol [5]. As described in 2.2.4, it is based on the concept that the network provides always the same Home Network Prefix to the MN independently of its point of attachment to the PMIPv6 domain. This mechanism provides the MN with an IPv6 address that is routable outside the PMIPv6 domain and managed by the LMA inside the domain. The configured IPv6 address remains unchanged for every handoff operated with the same interface, thus the mobility is transparent for the MN. Experimental protocols developed in the past for LMM, namely Fast-Handovers for Mobile IPv6 (FMIPv6) [18] and Hierarchical Mobile IPv6 (HMIPv6) [19], are host-based solutions that require host involvement for each handoff similar to, or in addition to, that required by MIPv6 for GMM. PMIPv6 can be applied to any GMM protocol and reduces host stack software complexity, expanding the range of MNs that could be accommodated.

Anyway, PMIPv6, as all the local mobility management protocols, needs to be combined with a global solution. So far, it has been only applied to MIPv6 [20], even if its main added value is to provide micro-mobility to "unmodified" MNs, i.e. non MIPv6 devices. Moreover, at the moment, PMIPv6 is also lacking of specific functionalities for IP session continuity across different network interfaces for multihomed MNs.

Ensuring session continuity to a MN equipped with multiple radio interfaces during inter-technology handoff is an open issue for PMIPv6. The precondition for a MN to move IP sessions from one interface to another is that it is able to configure the same IP address on both interfaces, using the same interface identifier and the same HNP in order to create the same IP address. The fact that there are link layers which do not allow for MAC address negotiation and where the MAC address assigned to the device is authenticated by the certificate and thus cannot be changed, i.e. IEEE 802.16, leads to consider specific functionalities for this issue.

In [21] - [22] the proposed solution is based on Virtual Interface (VI) configuration, that hides the multiple physical interfaces involved in the handover. The address configured by the MN is assigned to the VI, which is the only one visible to the applications as illustrated in Fig. 3.2. This method is efficient when only one interface is active at a time, as the MN maps the VI to the active physical interface. When a handover happens, the MN maps the VI to the new active physical interface. This solution represents the most reasonable one, but it does not cover the case in which the MN is multihomed and uses several interfaces at the same time, as the basic rules of IP networking impose that the same IP address cannot be assigned to more than one interface. Moreover, as highlighted in [23], the MN has to be enhanced with PMIPv6 specific capabilities to be able to notify its willingness of moving IP sessions across interfaces and it has to be aware about the PMIPv6 service availability. Extension to Router Advertisement (RA) and Router Solicitation (RS) messages, e.g. new flags, have been proposed in [24], but they are not sufficient and still an explicit notification from the MN about which IP session coming from which interface should be moved to the new interface is missing.

3.3 Proposed Combination of HIP and PMIPv6

Our scheme represents a novel micro-mobility management solution for HIP and, at the same time, an enhancement for PMIPv6 to support MNs roaming between different network interfaces and multihoming [25] - [26] . The architecture is illustrated in Fig. 3.3.

Before starting to analyze each mobility management phase, some assumptions need to be done for the proposed scheme. As in So's scheme, we suppose that all the entities in the PMIPv6 domain (LMA and MAGs), besides their own HIT, share a common HIT (HIT-domain) to represent the whole PMIPv6 domain. We suppose also that each entity can sign messages on behalf of the domain thanks to Mobility Management Key (MMK). The MN can verify the signature of the group.

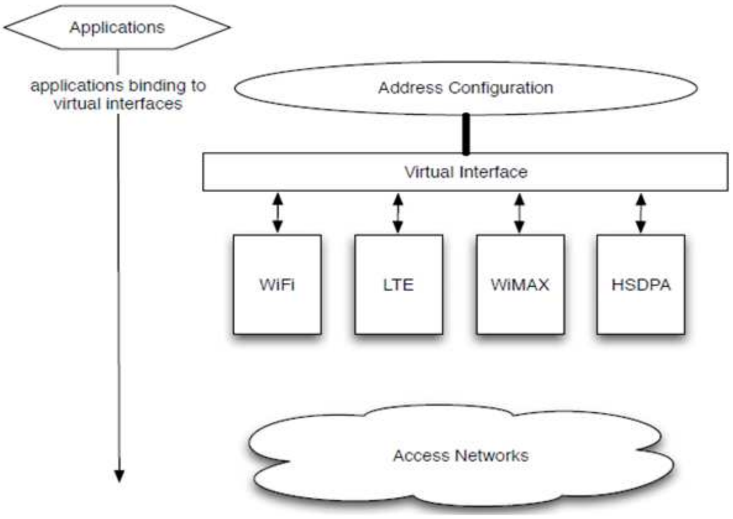

Figure 3.2: Use of Virtual Interface.

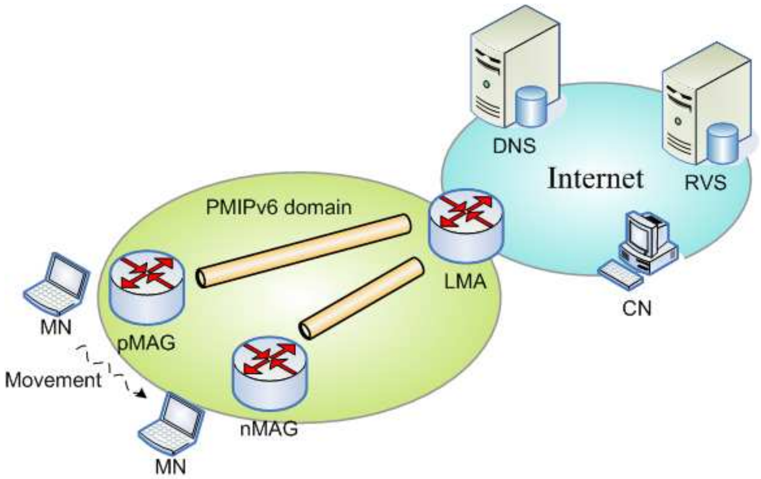

Figure 3.3: Global and Localized Mobility Management Architecture.

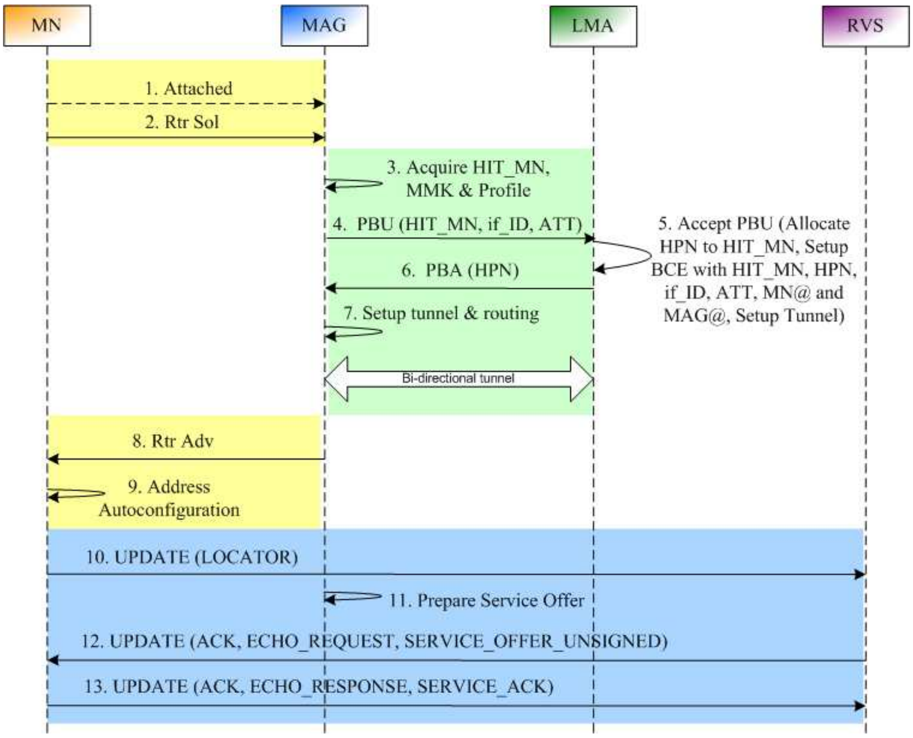
MN
MAG
LMA
RVS
1. Attached
2. Rtr Sol
3. Acquire HIT_MN, MMK & Profile
4. PBU (HIT_MN, if_ID, ATT)
5. Accept PBU (Allocate HPN to HIT_MN, Setup BCE with HIT_MN, HPN, if_ID, ATT, MN@ and MAG@, Setup Tunnel)
6. PBA (HPN)
7. Setup tunnel & routing
Bi-directional tunnel
8. Rtr Adv
9. Address Autoconfiguration
10. UPDATE (LOCATOR)
11. Prepare Service Offer
12. UPDATE (ACK, ECHO_REQUEST, SERVICE_OFFER_UNSIGNED)
13. UPDATE (ACK, ECHO_RESPONSE, SERVICE_ACK)

Figure 3.4: Initialization.

3.3.1 Initialization

We suppose the MN is already registered in the RVS and it enters a PMIPv6 domain. The complete process is illustrated in Fig. 3.4 and described hereafter.

The first part of the initialization phase is based on PMIPv6 prefix allocation [5]. As soon as a MN attaches to a PMIPv6 domain, it will be detected by the serving MAG on the access link. In particular, the link local address in the RS message sent by the MN is used by the MAG to obtain the interface identifier (interface-ID), i.e. the MAC address. A request is sent by the MAG to the Authentication, Authorization and Accounting (AAA) server or to the Local Policy Device with the interface-ID of the MN, in order to receive the authorization to provide the network-based mobility management service to the MN together with the MN identifier (HIT-MN) and profile, and the MMK.

The PMIPv6 procedure starts. The MAG sends a Proxy Binding Update

(PBU) message to the LMA containing the HIT-MN, the interface-ID and the Access Technology Type (ATT). The LMA replies with a Proxy Binding Acknowledgement (PBA) message including the MN's HNP, unique for that specific HIT-MN. A Binding Cache Entry (BCE) is created by the LMA in which it registers the HIT-MN, the HNP, the interface-ID, the ATT, the new MN's IP address created using HNP and interface-ID and the MAG's IP address. LMA and MAG set up their endpoints for creating a bi-directional tunnel between them.

The MAG sends RA messages to the MN on the access link advertising the MN's HNP as the hosted on-link prefix. The MN can configure an IP address for its interface that will never change as long it remains inside the PMIPv6 domain.

Once the environment for micro-mobility management is created, the macro-mobility management procedure will start as in HIP. The new IP address needs to be registered by the MN in the RVS. It is done following the RVS update procedure as defined in [11]. An UPDATE message containing the new LOCATOR is created by the MN and sent to the RVS. Once this message reaches the MAG, it will play the role of service provider for the micro-mobility service offered by PMIPv6 as in [23]. In order to establish a trusted relationship between the MN and the MAG, we use HIP service provision and discovery mechanism as specified in [27]. A SERVICE-OFFER-UNSIGNED (SOU) parameter is added by the MAG to the UPDATE ACK message sent by the RVS. This parameter is not covered by signature in the HIP control packet, so it can be added by HIP-aware middleboxes. The SOU contains three parts: SERVICE-PROPERTIES (SP) for describing the type of service, SERVICE-ID (SID) to identify a specific service and SERVICE-DESCRIPTION (SD) for providing specific service-related information, in our case the MMK and HIT-domain. The MN, that accepts the micro-mobility service, replies with a SERVICE-ACK parameter in the next UPDATE message to RVS. At this point the MMK and HIT-domain will be used by the MN to authenticate the service provider. In alternative to this solution, the PMIPv6 mobility management service can be notified by the MAG in the RA by setting a specific flag, as suggested in [23], but this implies modifications at the standard RA message.

In the case there are on-going sessions with Correspondent Nodes (CNs), the MN needs to send an UPDATE message to each CN with the new LOCATOR and ESP-INFO parameter containing the SPI value assigned to that specific session. As the HIP UPDATE packets are signed but not encrypted, they can be used by LMA for activating the status of the MN's interface adding the SPI value and CN's IP address to the interface-ID in

HIT-MN	HNP	If-ID$_1$	ATT$_1$	IP address$_1$	MAG$_1$	A	CN$_1$	SPI$_1$
		If-ID$_2$	ATT$_2$	IP address$_2$	MAG$_2$	Preliminary		

Table 3.1: Example of Binding Cache Entry per MN at LMA

the BCE. This aspect is explained in details in the next paragraph.

3.3.2 Communication Setup

HIP Base Exchange [4] is required before every HIP-based communication is established. A CN that wants to reach a MN needs to contact the DNS server to get, first, the RVS' IP address for that MN. Then the CN can start the HIP BE with the MN via RVS. The first packet, a HIP I1 message, is forwarded by the RVS directly to the recorded locator of the MN. The peculiarity of PMIPv6 is that the IP addresses generated through the PMIPv6 prefixes are routable outside the PMIPv6 network and always point to the LMA. This feature allows us to avoid using a LRVS in the local network as in [14] and [15]. As soon as I1 reaches the LMA, it is tunneled to the serving MAG and then delivered to the MN. The rest of the BE operates in the standard way, the MN and the CN exchange R1, I2 and R2 packets directly without passing through the RVS.

As HIP BE packets, but also HIP UPDATE packets as seen before, are not encrypted, they can be used by the LMA for updating the BCE. Thus, only HIP control packets are inspected, not data packets. An interface of a MN registered in a "preliminary" (P) status (no active connections) can become "active" (A) as in [28] adding the SPI and CN's IP address information carried in HIP BE or UPDATE packets. Table 3.1 represents an example of BCE at LMA for a MN with two interfaces. When BE or UPDATE processes have finished, there is not anymore HIP overhead in data packets. LMA is not a SPINAT device in our architecture, so routing at LMA for tunneling packets to the correct MAG is done based on the IP addresses of MN and CN.

3.3.3 Intra-technology Handover

The intra-technology handover phase represents the most important contribution of PMIPv6 to micro-mobility management for HIP. As the MN's locator does not change, the process is completely transparent to HIP. This phase is based on PMIPv6 procedure [5] and it is illustrated in Fig. 3.5. When the MN changes its point of attachment, the MAG on the previous

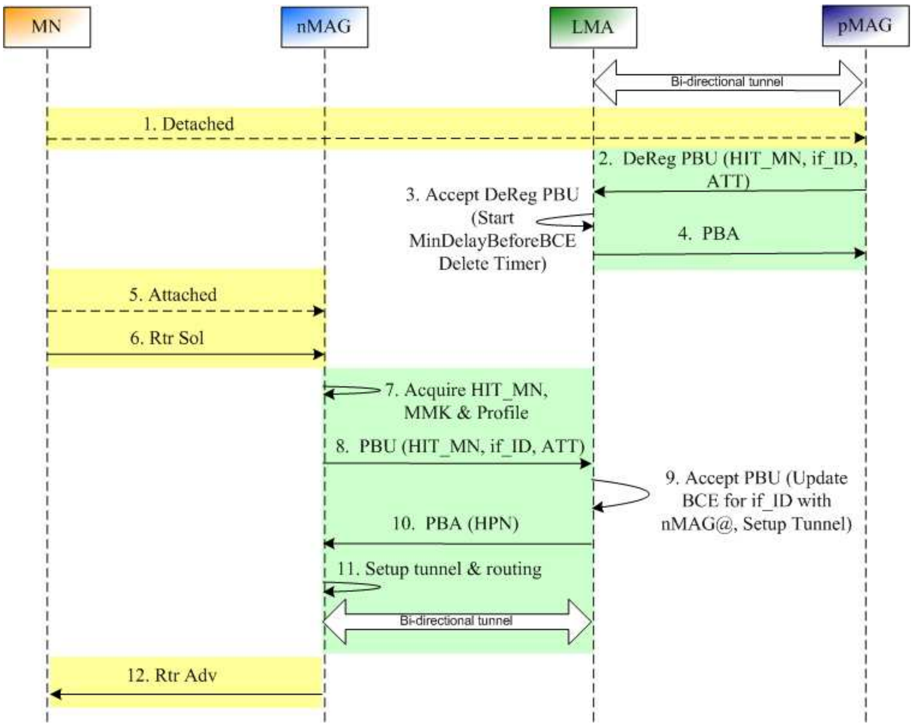
MN
nMAG
LMA
pMAG
Bi-directional tunnel
1. Detached
2. DeReg PBU (HIT_MN, if_ID, ATT)
3. Accept DeReg PBU (Start MinDelayBeforeBCE Delete Timer)
4. PBA
5. Attached
6. Rtr Sol
7. Acquire HIT_MN, MMK & Profile
8. PBU (HIT_MN, if_ID, ATT)
9. Accept PBU (Update BCE for if_ID with nMAG@, Setup Tunnel)
10. PBA (HPN)
11. Setup tunnel & routing
Bi-directional tunnel
12. Rtr Adv

Figure 3.5: Intra-technology Handover.

link (pMAG) detects the MN's detachment from the link. It sends to the LMA a Deregistration PBU with the HIT-MN, interface-ID and ATT. The LMA, upon receiving this request, identifies the corresponding MN and interface for which the request was received. The LMA accepts the request and then it waits for a certain amount of time to allow the MAG on the new link (nMAG) to update the binding. However, if it does not receive any Proxy Binding Update message within a given amount of time, the LMA deletes the interface from the MN entry in the BCE.

With the new attachment, the PMIPv6 prefix allocation procedure starts, as in the initialization process, and terminates with the RA message sent by the nMAG to the MN containing the HNP. The LMA updates the BCE for that interface with the nMAG's IP address. The MN does not detect any change with respect to the layer-3 attachment of its interface, the IP address has not changed. There is no need for UPDATE messages to RVS and CN.

3.3.4 Inter-technology Handover and Multihoming

The multihoming support in PMIPv6 [5] is simply simultaneous connection/attachment support for a multiple interfaced MN. However, there are many scenarios in which the simultaneous "usage" of multiple interfaces for a MN and the possibility of moving a single IP flow from a certain access technology to another one require some enhancement/modification to the current PMIPv6 base protocol. [29] explores the merits and the tradeoffs of the basic principle of two PMIPv6 multihoming models such as the same unique prefix across all the interfaces and per interface unique prefix. Our proposal is based on unique HNP for all interfaces of a MN and on the mobility features of HIP [12] in combination with micro-mobility features provided by PMIPv6. Advantages of this choice are described hereafter.

To illustrate this phase we suppose the MN has an ongoing IP session with a CN and wants to move it to its second interface without disconnecting the first one. When the MN switches on its second interface to configure the IP address, it obtains the same HNP from the network, as the HNP is assigned to MN's identifier, reducing operation complexity at LMA. In this way the MN realizes it is still in the same domain and no UPDATE messages are sent to the RVS, due to the fact that anyway all the IP addresses configured in the PMIPv6 are pointing to the LMA. In order to explicitly notify its willingness to move a particular IP session, the MN has to send to the CN an UPDATE message with the new LOCATOR parameter containing the second interface's IP address. In the UPDATE message it is also present the ESP-INFO parameter containing the values of the old and new SPIs for the SA. In this case, the OLD SPI and NEW SPI parameters both are set to the value of the preexisting incoming SPI; this ESP-INFO does not trigger a rekeying event. The UPDATE packet with the new IP address is intercepted and processed by the nMAG and it is not forwarded to the CN as illustrated in Fig. 3.6.

On one side, the nMAG is handling the UPDATE packet on behalf of the CN, performing address verification by placing a nonce in the ECHO-REQUEST parameter of the UPDATE message sent back to the MN. The MN recognizes the HIT-domain and the MMK in the message and accepts the reply. It completes the readdress by processing the UPDATE ACK and echoing the nonce in an ECHO-RESPONSE.

On the other side, thanks to the information carried in the UPDATE message, the nMAG knows that it is an inter-technology handover and can send to the LMA a PBU message containing Handoff Indicator option set to the value of 2 (handoff between two different interfaces of the MN), the

HIT-MN and the SPI. Based on these parameters the LMA updates the corresponding BCE substituting the pMAG's IP address with the nMAG's one. A PBA is sent by LMA to nMAG.

As highlighted in [29], when applying the same HNP for all interfaces of a MN, there are three different methods for routing using the cache at LMA. We have chosen the address based cache method, thus LMA tunnels the incoming packets from the CN to the correct MAG depending on the IP source and destination addresses in the IP header. With this approach the willingness of the MN of using the new locator and thus the new access technology is respected even if the CN has not been updated and keeps using the previous locator. When packets reach the MAG, they are routed based on the HNP. Moreover, the MN can be configured to accept packets to be received by any interface as long as the destination address matches the HNP regardless of the actual address configured for that interface. For outgoing packets, the CN can still receive them even if they are coming from a different interface of the MN due to the fact that the SA takes into account the MN's identifier and not its locator.

The HIP identifier/locator split principle is based on the same basic idea of the virtual interface (IP session continuity is assured by the fact that applications are linked to the identifier or to the VI, not to the current IP address), but our proposal represents a more complete solution as it can be applied to multihomed MNs using multiple active interfaces.

The multihoming features of our proposed scheme can be summarized as follows. A comparison with the MobiSplit architecture [30], which separates mobility management and multihoming at global and local levels using MIPv6 and NetLMM, can help to better explain multihoming in our scheme. At global level, HIP-PMIPv6 scheme is similar to MobiSplit approach, but instead of using multiple CoAs, one per domain, associated to the same HoA and registered in the HA, in our scheme multiple locators, one per PMIPv6 domain, are associated to the identifier and registered in the RVS. At local level, as in MobiSplit, the external entities to the PMIPv6 domain (RVS, CNs) do not distinguish the situation in which the MN is using one or more interfaces. The MN registers only one locator per PMIPv6 domain. The difference with MobiSplit consists on the fact that the MN is not forced to configure the same locator on each of its active terminal interfaces. As the SAs are linked to the MN's identifier, CNs can receive and process packets having a different source address.

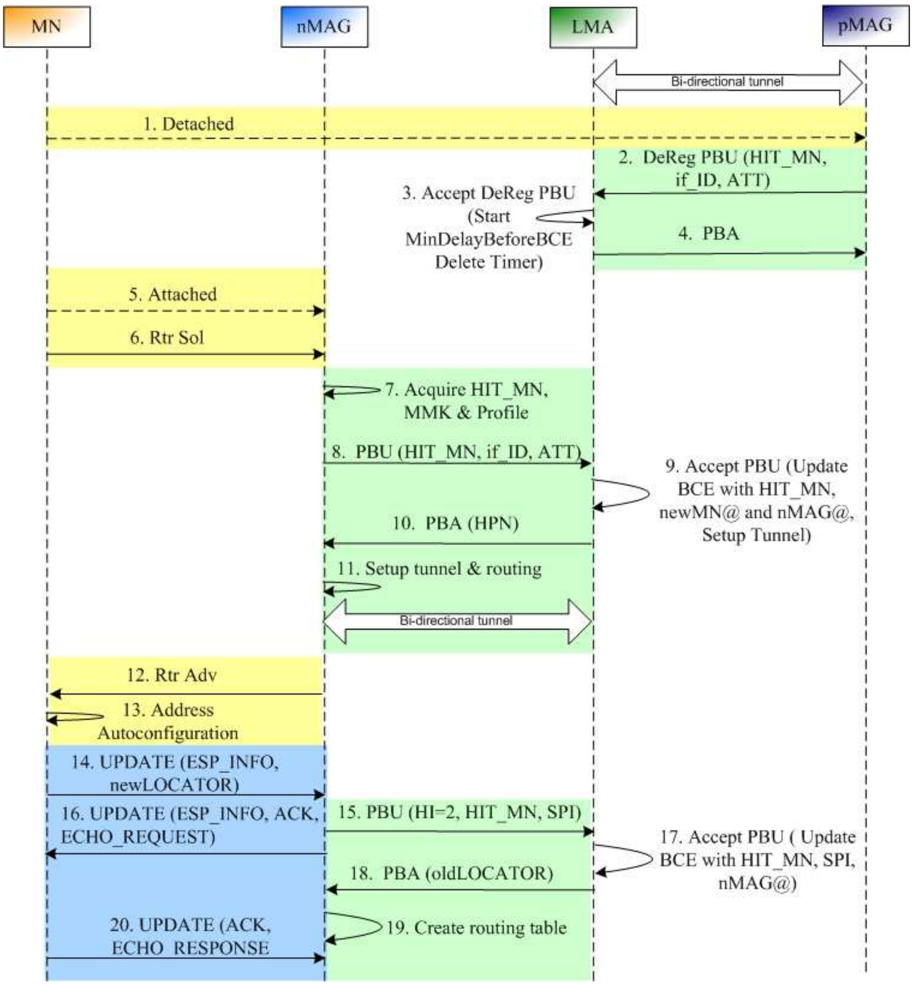
MN
nMAG
LMA
pMAG
Bi-directional tunnel
1. Detached
2. DeReg PBU (HIT_MN, if_ID, ATT)
3. Accept DeReg PBU (Start MinDelayBeforeBCE Delete Timer)
4. PBA
5. Attached
6. Rtr Sol
7. Acquire HIT_MN, MMK & Profile
8. PBU (HIT_MN, if_ID, ATT)
9. Accept PBU (Update BCE with HIT_MN, newMN@ and nMAG@, Setup Tunnel)
10. PBA (HPN)
11. Setup tunnel & routing
Bi-directional tunnel
12. Rtr Adv
13. Address Autoconfiguration
14. UPDATE (ESP_INFO, newLOCATOR)
15. PBU (HI=2, HIT_MN, SPI)
16. UPDATE (ESP_INFO, ACK, ECHO_REQUEST)
17. Accept PBU (Update BCE with HIT_MN, SPI, nMAG@)
18. PBA (oldLOCATOR)
19. Create routing table
20. UPDATE (ACK, ECHO_RESPONSE

Figure 3.6: Inter-technology Handover.

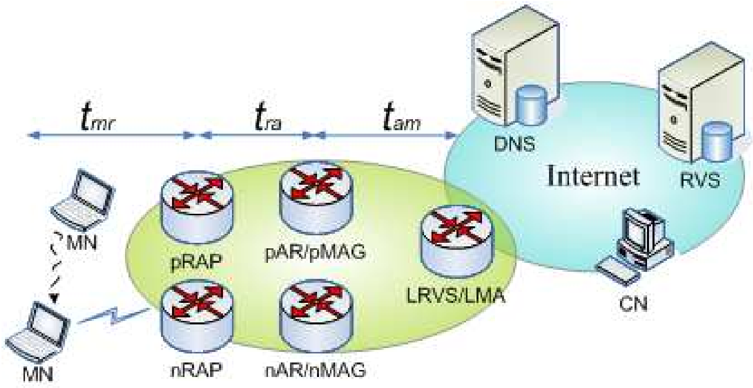

Figure 3.7: Simple Analytical Model for Performance Analysis.

3.4 Handover Latency Analysis

In this section we analyze the handover latency of our HIP-PMIPv6 scheme for the two cases of intra and inter-technology handover between two MAGs belonging to the same PMIPv6 domain. We compare the performances of our scheme with Novaczki's proposal. So's scheme represents an extension to Novaczki's one in a balanced binary tree structure, thus a comparison between our and So's schemes will replicate the analysis between HIP-PMIPv6 and Novaczki's proposal.

We consider the simple analytical model shown in Fig. 3.7, in which the LRVS of Novaczki's proposal is collocated with our LMA and the Access Routers (ARs) with MAGs. Similar to [31] [32], we use the following notations:

- The delay between MN and Radio Access Point (RAP) is t_{mr}, which is the time necessary for a packet to be sent between the MN and the RAP through a wireless link.
- The delay between RAP and AR/MAG is t_{ra}.
- The delay between AR/MAG and the LRVS/LMA is t_{am}.

Handover latency is defined as the time that elapses between the moment in which the L2 handover completes at the RAP and the moment the MN receives the first packet after moving to the new point-of-attachment. It can be expressed as

$$T_{HO} = T_{L2} + T_{MD} + T_{AC} + T_{REG} \tag{3.1}$$

where T_{L2} represents the delay due to layer 2 signaling, T_{MD} the movement detection delay, T_{AC} the address configuration delay and T_{REG} the location registration delay.

In Novaczki's scheme there is no difference between the handover latency for intra and inter-technology handover. It is composed of:

- T_{L2} equivalent to t_{mr};
- T_{MD} calculated considering the delay due to the reception of an unsolicited RA message. Each router that supports mobility is configured with a *MinRtrAdvInterval (MinInt)* and *MaxRtrAdvInterval (MaxInt)*. The mean time between unsolicited RA messages is expressed as *(MinInt + MaxInt)/2* so T_{MD} is half of that, thus *(MinInt + MaxInt)/4*;
- T_{AC} is due to the Duplicate Address Detection (DAD) process and can be expressed as *RD*, where *R* is *RetransTimer* and *D* is the *DuplAddrDetectTransmit*;
- T_{REG} includes the time of the HIP registration update delay from MN to the LRVS (i.e., *3(t_{mr} + t_{ra} + t_{am})*).

In conclusion the handover latency for Novaczki's scheme is

$$\begin{aligned} T_{HO}^{Nov} &= t_{mr} + \frac{MinInt + MaxInt}{4} + RD + 3(t_{mr} + t_{ra} + t_{am}) \\ &= \frac{MinInt + MaxInt}{4} + RD + 4t_{mr} + 3(t_{ra} + t_{am}) \end{aligned} \tag{3.2}$$

In HIP-PMIPv6 approach the handover latency, in the case of intra-technology handover, is composed of:

- T_{L2} equivalent to t_{ra};
- T_{MD} is null as the IP-level movement detection does not occur;
- T_{AC} is null as it occurs only when the MN enters a PMIPv6 domain, then the MN keeps the same address inside the domain;

t_{mr}	t_{ra}	t_{am}	*MinInt*	*MaxInt*	*R*	*D*
10 ms	2 ms	20 ms	30 ms	70 ms	1000 ms	1

Table 3.2: Parameters for the Performance Analysis

- T_{REG} is composed of the sum of the PBU delay between the MAG and the LMA $2t_{am}$ and the packet delivery delay from the MAG to the MN $(t_{mr} + t_{ra})$.

Thus, the handover latency for intra-technology handoff in HIP-PMIPv6 scheme is

$$T_{HO-INTRA}^{HIP-PMIPv6} = t_{ra} + 2t_{am} + t_{mr} + t_{ra} = 2t_{ra} + 2t_{am} + t_{mr} \tag{3.3}$$

In the case of inter-technology handover, the handover latency of HIP-PMIPv6 is the sum of $T_{HO-INTRA}^{HIP-PMIPv6}$ and an additional T_{REG}, due either to the HIP registration update delay (i.e., $3(t_{mr} + t_{ra})$) when the delay between MN and MAG is higher than the one between MAG and LMA or to the PBU delay between MAG and LMA $2t_{am}$ in the other case.

The result is

$$T_{HO-INTER}^{HIP-PMIPv6} = \begin{cases} 4t_{mr} + 5t_{ra} + 2t_{am} & \text{for } 3(t_{mr} + t_{ra}) \geq 2t_{am} \\ t_{mr} + 2t_{ra} + 4t_{am} & \text{for } 3(t_{mr} + t_{ra}) \leq 2t_{am} \end{cases} \tag{3.4}$$

Based on the previous analysis and on the values in Table 3.2 [32], in which it is assumed a low bandwidth wireless link between the MN and the AR, it is possible to show the following numerical results.

Figure 3.8 shows that, in the three considered cases, handover latencies increase with the wireless link delay. The intra-technology HIP-PMIPv6 is the least affected by the distance between MN and RAP as the MN is not involved in mobility-related signaling. Comparing Novaczki's scheme with HIP-PMIPv6 inter-technology, we can see that, even if t_{mr} contributes in the same way to both schemes, Novaczki's proposal is penalized by the fact that the 3-way HIP UPDATE procedure involves the LRVS, and not the MAG as in HIP-PMIPv6 scheme for inter-technology handover, causing higher values of handover latency.

Figure 3.9 evaluates the impact of T_{MD} over the handover latencies of Novaczki's scheme and HIP-PMIPv6 proposal. The advantage of applying

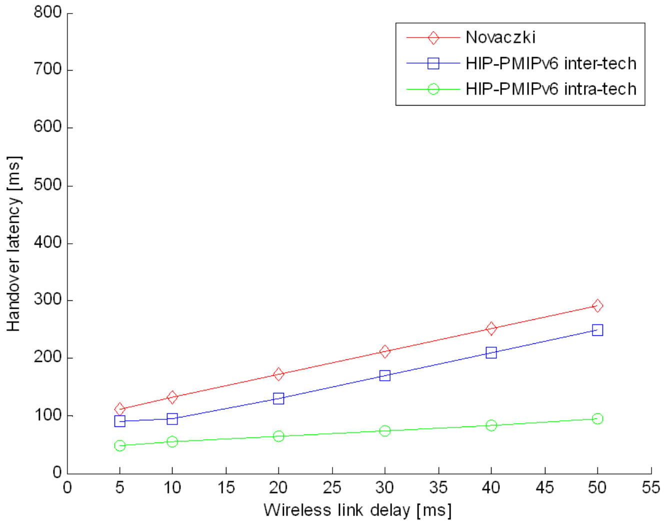

Figure 3.8: Handover Latency vs. Wireless Link Delay.

the per-MN-prefix model in our proposal is used to make the MN believe it is always in its home network, thus no IP-level movement is detected by the MN and T_{MD} has no impact in our proposal. On the contrary, the graph for Novaczki's scheme increase as T_{MD} does.

Finally Fig. 3.10 shows the impact of $(t_{mr} + t_{ra} + t_{am})$ over the handover latency, in particular the impact of t_{am} keeping t_{mr} and t_{ra} constant. The intra-technology HIP-PMIPv6 has again the best performances as it is only affected by PBU and PBA messages delay. As regards inter-technology HIP-PMIPv6 and Novaczki's scheme behaviors, we see that, when the delay between MN and LRVS/LMA reaches 70 ms, our proposal pays the price for having double PBU-PBA messages, reporting higher values of handover latency. Anyway, Fig. 3.10 shows the resulting handover latencies for a scenario in which the MN is single-homed, thus the handover process from one technology to the other one is done by the MN right after the new attachment. Novaczki's scheme does not support multi-homed MNs. On the contrary, our proposal takes into account a scenario in which technology domains can be overlapped and multihomed MNs have the possibility, after having done the new attachment, of moving IP sessions from one interface to the other one, following the Always Best Connected concept. This is possible using the double PBU-PBA messages.

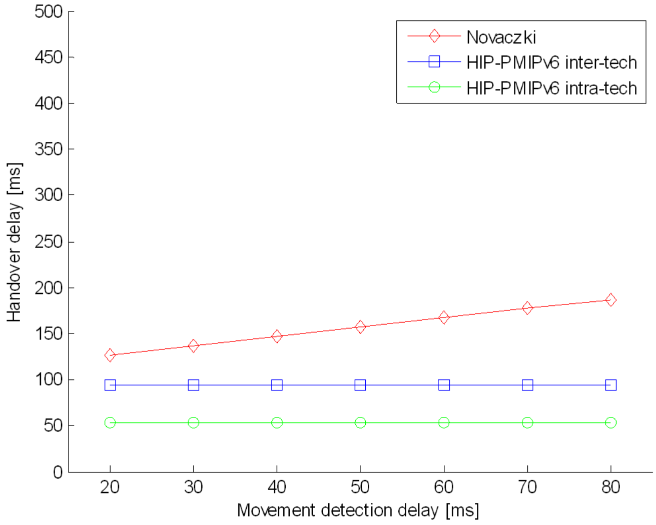

Figure 3.9: Handover Delay vs. Movement Detection Delay.

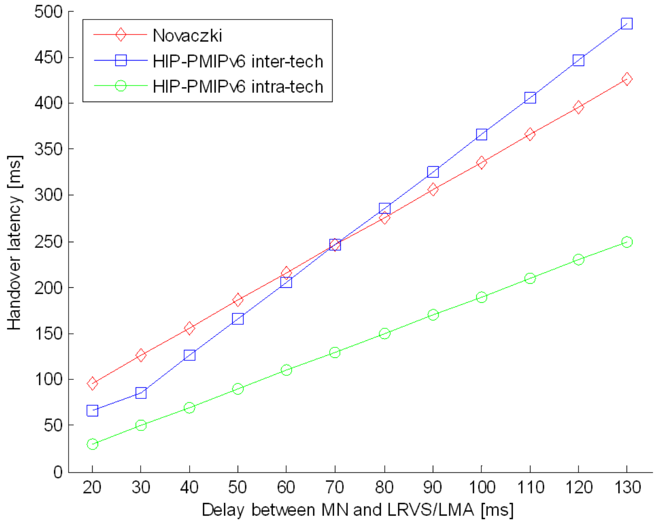

Figure 3.10: Handover Latency vs. Delay between MN-LRVS/LMA.

3.5 Conclusion

In this chapter we have presented a secure global and local mobility management scheme based on HIP and PMIPv6 and applicable to the future Internet, where security, mobility and multihoming are the key aspects. We have demonstrated that our proposal represents an important improvement to PMIPv6 for inter-technology handover and multihoming, as it overcomes the current Virtual Interface solution in providing simultaneous usage of multiple interfaces for multihomed MN. This is achieved through the use of HIT-MN, instead of VI-identifier, as MN-identifier to which applications are linked, because it allows the MN to have several interfaces active at the same time and to move flows among them.

Moreover, we have proved that our scheme represents also a very efficient micro-mobility solution for HIP. Applying PMIPv6 features to HIP, it is possible to have an intra-technology handover process which is completely transparent to HIP MNs thanks to the fact that they do not detect any change to the previous configured IPv6 address. Thus, the necessary signaling messages for the handover are reduced and the performances in terms of handover latency demonstrate the high efficiency of this solution compared to any other previous proposal. Finally, our scheme considers also the case of inter-technology handover and multihoming, merging together PMIPv6 with HIP mobility and multihoming features.

Chapter 4

Mobility Architecture for Future Internet

4.1 Introduction

This chapter presents a novel mobility architecture for future Internet derived from the Host Identity Protocol and the Proxy Mobile IPv6. The proposed architecture not only preserves the best of both protocols, such as the idea of separating a hosts identity from its present topological location in the Internet and the mechanism of network-based mobility management without host involvements, but it combines them in an efficient way. In our architecture the host identifier is used as a virtual interface for multihomed terminals and the group identifier to identify nodes in an ad-hoc network, while the locator is configured such as it provides location privacy and avoids the use of local NATs. The result is a mobility architecture which addresses the requirements of future Internet and operators, as addressing, name resolution, security, location privacy, mobility, multihoming, ad-hoc networking, routing and traffic engineering.

4.2 Problem statement

The basic principles of the original Internet architecture include end-to-end addressing, global routeability and a single address space of IP addresses that act as locators and node identifiers at the same time. These principles are suitable for static and well-managed network hierarchies. However, since the Internet has evolved from a small research network to a worldwide information exchange network, a growing diversity of commercial, social, ethnic, and governmental interests have led to increasingly conflicting requirements among the competing stakeholders. These conflicts create tensions that the original Internet architecture struggles to withstand.

The commercial success and widespread use of the Internet have lead to new requirements for a future Internet, which include internetworking over business boundaries, mobility, multihoming, and security for untrusted environments. Concurrently with this research into new Internet architectures, a demand for private, autonomous networks is growing. Although still connected to the global Internet, these autonomous networks offer local features and capabilities that are independent from the public Internet. The todays solution to achieve more autonomy are Network Address Translators (NAT) [33], which is a popular method for reusing address space and decoupling routing in the private network from routing in the public Internet. Although these capabilities of NATs mitigate many immediate problems, NATs are not a clean solution [34].

The fundamental problems of the Internet Protocol stems from overloading two separate functionalities onto the same bit string of the IP address. One is its use as a locator, i.e., as an address that denotes a location in the topology of the network and specifies a network attachment point (interface). The second one is that of an identifier that describes the identity of a node. The problem with the NAT approach is that it translates between internal and external addresses and with that also implicitly translates between the associated identities. This causes applications and protocols that exchange IP addresses in their payloads, such as FTP, to break.

The problem with addressing a network attachment point is that today most hosts have more than one communication capability, and with it the possibility to attach to the network through several interfaces. This multihoming causes the host to show up with multiple interface addresses, and thus multiple identities.

The main purpose of several access technologies integration, both wired and wireless, in the new equipments shipped on the market now is to federate all means of communications in order to access the Internet ubiquitously (from everywhere and at any time) as no single technology can be expected to be deployed everywhere [35]. Flows may thus be redirected from one interface to the other following the loss of connectivity or change of the network conditions in different access mediums. Besides enabling ubiquitous

Internet access, integrating several access technologies also allows increased bandwidth availability and selection of the the most appropriate technology according to the type of flow or choices of the user, since each access medium has different cost, performance, bandwidth, access range, and reliability.

Once multiple accesses are offered, users may want to select the most appropriate set of network interface(s) depending on the network environment, particularly in wireless networks which are mutable and less reliable than wired networks. Users may also want to select the most appropriate interface per communication type or to combine a set of interfaces to get sufficient bandwidth.

The new design of Internet should try to satisfy users expectations, in accordance also with the requirements of the other two classes of players in the current Internet: access network operators and home operators. Users operate hosts for which they desire efficient, available, and reliable Internet connectivity. Access network operators provide the infrastructure that hosts needs to communicate, collectively called the "edge domain". An access network can indepently route packets between two attached hosts, but for global Internet connectivity, it must connect to a home operator with its provider. Providers jointly form a "core domain" via which packets can be exchanged between edge networks. Access network operators are naturally eager to meet the expectations of users because they have a direct business relationship with the users, thus they should not depend on functions of an external operator to provide their own connectivity and mobility service, while home operators should focus on customer support and rely on multiple access operators to provide their users with efficient local mobility management.

4.3 HIP and PMIPv6 based Mobility Architecture

4.3.1 Assumptions and Principles

The proposed mobility architecture for future Internet is based on two protocols, HIP and PMIPv6, and mainly on the two principle ideas behind them. The first idea is the concept of *host identity layer* located in the middle of network and transport layers. This layer provides unique cryptographic identifiers for hosts, called *host identifiers*, which are independent of the host's current location and network address. The second idea is to create a *locator*, which defines the topological location of a host in a way that it is routable in the Internet, but has a specific scheme for routing in the local domain to which the host is attached [36].

From these two basic ideas we have defined a unique architecture where each host has:

- an identifier which uniquely identify the host and which is created as the public key of a public/private key pair, bringing built-in security support;
- one or several locators, depending on the fact of having multiple interfaces and being multihomed; locators are used for routing, but they have different topological semantics depending on the network considered, allowing inherent location privacy.

The result is an architecture which has the advantages of HIP and PMIPv6 protocols, such as on one side security, global mobility, multihoming and on the other side local mobility and location privacy, together with an efficient and dynamic mobility and multihoming scheme at local and global level.

The architecture is designed keeping in mind the requirements of Internet and operators in the future. For this reason we split the design in two parts:

- the core network in which home operators with their providers are located;
- the edge network where Local Mobility Domains (LMDs) are located. A LMD is associated with an Access Network Provider (ANP) and one or more Wireless Access Networks (WANs), having same or different access technologies.

The core network has multiple connections with the edge network, which are managed by four basic components:

- the Domain Name Server (DNS), which has the functionality of resolving Fully-Qualified Domain Names (FQDNs) with the corresponding host identifiers and locators;
- the Rendezvous Server (RVS) [11], which is the entity registering the locators associated with a host identifier;
- the Local Mobility Anchor (LMA), which represents the access point to the LMD and the topological anchor point for hosts in the LMD;

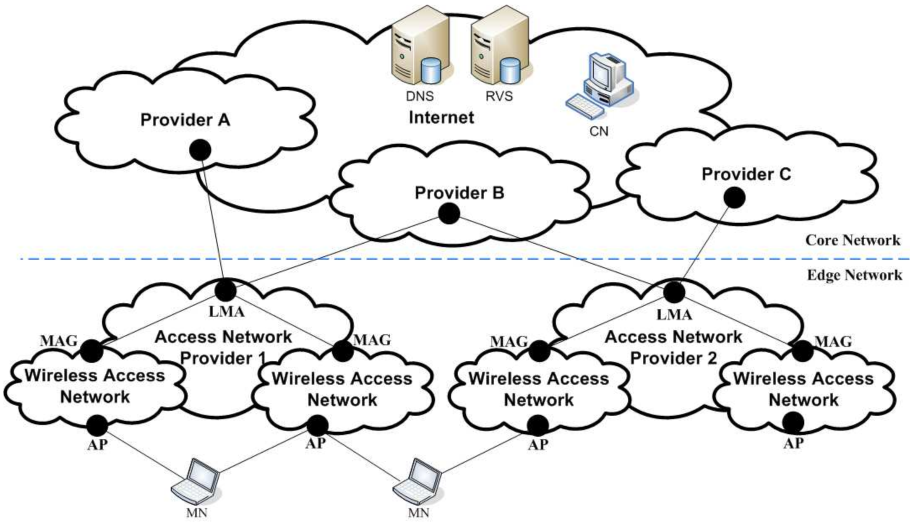

Figure 4.1: Mobility Architecture.

- the Mobility Access Gateway (MAG), which is the access router for the WAN that manages the mobility-related signaling for the MNs attached to its access link.

The overall architecture is illustrated in Fig. 4.1.

4.3.2 Addressing Scheme

The IPv6 address (i.e. the locator) configured by MN in the mobility architecture is obtained through the PMIPv6 mechanism. When a MN attaches to a PMIPv6 domain (a LMD in this architecture), the MAG on that access link performs an access authentication procedure with a policy server sending the MN's identifier. The MAG receives the MN's profile, which contains the Home Network Prefix (HNP), the LMA address and other related configuration parameters. Then, the MAG sends to the LMA a Proxy Binding Update (PBU) message on behalf of the MN including the MN's identifier, its HNP and the used interface's MAC address. Upon accepting the message, the LMA replies with a Proxy Binding Acknowledgement (PBA) message, and it creates a Binding Cache Entry (BCE) with MN's identifier, its HNP, the locator (created from the HNP and the MAC address) and the MAG's address. Then, the MAG and the LMA create an IP-in-IP bidirectional tunnel for routing MN's traffic. As last step, the MAG sends a unicasted Router Advertisement (RA) message to the MN advertising the HNP as the hosted on-link prefix. On receiving this message, the MN configures its interface either using stateful or stateless address configuration modes. Finally the MN ends up with an address from its HNP that it can use while moving in the PMIPv6 domain.

4.3.3 Name Resolution

The name resolution procedure begins with a FQDN, which nodes resolve via the DNS. The DNS returns the identifier of the MN and the locator of its RVS. With these two information, communication between peers can start. The first Base Exchange (BE) message (I1) sent by the Correspondent Node (CN) passes through the RVS which redirects it to the MN's locator. Once the MN receives the packet, it can reply to the CN directly providing its locator. The rest of BE (R1, I2, R2) for establishing the Security Associations (SAs) can occur through direct communication between peers.

4.3.4 Security

The cryptographic nature of the host identifiers is the security cornerstone of HIP architecture as well as of our architecture. Each end-point generates exactly one public key pair. The public key of the key pair functions as the host identifier. The end-point keeps the corresponding private key secret and does not disclose it to anybody. The use of the public key as the name makes it possible to directly check that a party is actually entitled to use the name. A simple public key authentication protocol, such as the Diffie-Hellman scheme included in the HIP BE, is sufficient for that. This is accomplished with a four-way handshake, consisting of messages I1, R1, I2 and R2. After these exchange messages, both communicating hosts know that at the other end-point there indeed is an entity that possesses the private key that corresponds to its host identifier. Additionally, the exchange creates a pair of IPSec Encapsulated Security Payload (ESP) SAs, one in each direction. The hosts use the ESP SAs to protect the integrity of the packets flowing between them.

4.3.5 Location Privacy

Standard HIP architecture does not provide location privacy as the locator information contained in the BE messages are not encrypted and can be disclosed by third parties. Moreover, there are scenarios in which even the correspondent peer should not be aware of the exact location of its peer. In the proposed mobility architecture, even if the locator is disclosed by peers

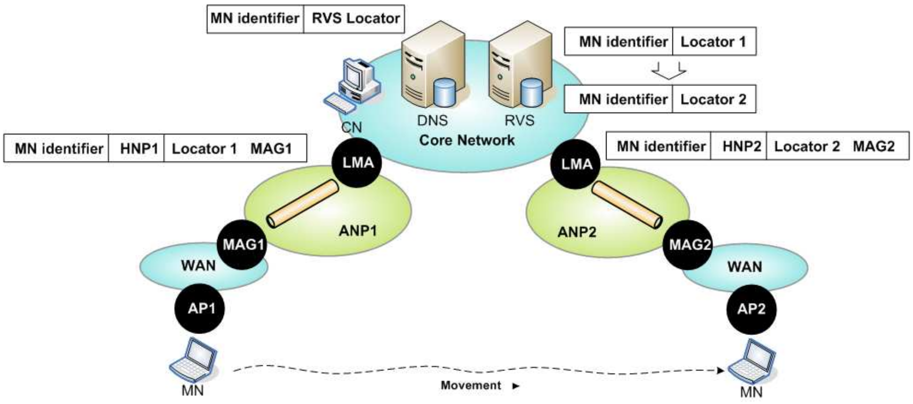

Figure 4.2: Global Mobility.

or on-lookers, it is configured in a way that it always points to the LMA of the LMD where the MN is located, but does not reveal the exact position of the MN. Only the LMA is able to locate the MN and to route packets to it. In particular, the BCE at LMA contains entries for each MN attached to the LMD with the corresponding serving MAG.

4.3.6 Mobility

The global and local mobility scheme of our architecture is a combination of HIP and PMIPv6 schemes. As regards global mobility, when a MN moves from a LMD to another one, it obtains through the PMIPv6 mechanism a new HNP (HNP2), which it is used to create a new locator (Locator 2). As in standard HIP, the MN needs to update the RVS with its new locator as in Fig. 4.2.

The case of local mobility management follows exactly the standard PMIPv6 procedure. Each LMD provides always the same HNP to the MN regardless the used interface, as the HNP is linked to the MN's identifier. The LMA updates the BCE with the correct information of locator and MAG associated with the MN's identifier and HNP as shown in Fig. 4.3. In this case, there is no need for the MN of updating the RVS as the registered locator in the RVS is always routable to the LMA.

4.3.7 Multihoming

At global level, multihoming consists on the registration done by the MN, in the RVS database, of multiple locators, one per LMD, associated to the

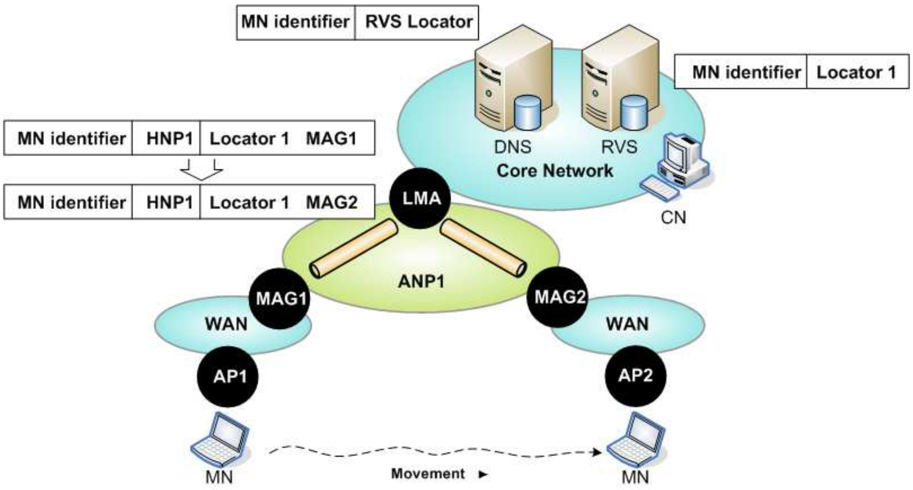
MN identifier | RVS Locator
MN identifier | Locator 1
MN identifier | HNP1 | Locator 1 MAG1
MN identifier | HNP1 | Locator 1 MAG2
DNS
RVS
Core Network
CN
LMA
ANP1
MAG1
MAG2
WAN
WAN
AP1
AP2
MN
Movement
MN

Figure 4.3: Local Mobility.

same identifier.

At local level, it is the LMA that keeps updated its BCE associating multiple locators to the same identifier and HNP. Even if the MN is multihomed at local level, external entities, such as RVS and CNs, are not aware about it.

4.3.8 Ad-hoc Networking

We have considered as well the case in which, instead of having just a MN attached to the LMD, there is an ad-hoc network. As defined in [37], the nodes in the ad-hoc network can share a common identifier, called Group Identifier (GI), which can be used in the PBU instead of the host identifier. The BCE data structure maintained by the LMA, can be extended to store it and have a corresponding HNP for that GI. In this way the HNP is shared by all the nodes of the ad-hoc network which use it to configure their IPv6 addresses. All the traffic having as destination address an address with that particular HNP is routed by the LMA to the serving MAG for the ad-hoc network, and then by the MAG to the ad-hoc network, which will use its internal ad-hoc routing protocol for delivering the traffic to the correct MN.

4.3.9 Routing

Routing in the core and in the edge networks is done in two different ways. While in the core network it can be based on any standard routing protocol of Internet, routing in the LMDs is completely based on information contained in the BCE of each LMA. The LMA can route packets for the MN to the correct MAG based on the destination IPv6 address (locator) or, in case there is no entry for it, on the HNP.

4.3.10 Traffic Engineering

The LMD can silently decide to move the traffic of a MN from one WAN to another. In our architecture, this is possible thanks to locator/identifier split and to the fact that SAs are linked to identifiers and not to locators. Even if the IP address of the interface in which the MN is receiving packets is different from the destination address of the packets, the MN can accept the data traffic as far as the same HNP is used in the destination address.

At the same time, the MN can choose, depending on the circumstances, to move traffic from one interface to another one, thus from one WAN to another one. The MN can express its preferences in the UPDATE message, specifying which flow it wants to move from which interface to which other one.

4.4 Architecture Comparison

The separation of identity and location is fundamental in our mobility architecture and so also in many other proposed architectures including FARA [38], the Layered Naming Architecture [39] and DOA [40], the NAT-based architectures TRIAD [41] and IPNL [42], Host Identity Indirection Infrastructure (Hi3) [43], a combination of HIP and the Internet Indirection Infrastructure (i3) [44] [45], in TurfNet [46] and in the Split Naming/Forwarding Architecture (SNF) [47].

There are also several proposals in the IETF and IRTF that use the idea of locator/identity split. There are host-based proposals like HIP and Site Multihoming by IPv6 Intermediation (SHIM6) [48] and router-based solutions such as LISP [49] and Six/One [50].

The proposals differ for instance in how the identifiers are defined. HIP architecture introduces unstructured cryptographic identifiers and in this sense the work most similar to us. The Layered Naming Architecture and DOA also propose the use of topology-independent endpoint identifiers from a flat namespace while in TRIAD and IPNL domain names (FQDNs) are used as identifiers. Hi3 and i3 do not support internetworking across heterogeneous domains, while TurfNet uses a large number of proxy locators to forward data instead of host identities.

The more incremental solutions Shim6, LISP and Six/One, do not fully separate the identifier and locator functions but use IP addresses (or parts of IP addresses) also as identifiers. LISP divides IP addresses into endpoint identifiers and routing locators. A host is unaware of the latter which is used as transit address when tunnelling between network providers. The tunnels in LISP can in our work instead be implemented with IP-in-IP tunnelling for routing. The "originally from/to" header option in Six/One can be compared to our HIP header, which applies only to control messages in our case.

In sections 3.2 and 3.3 we have already described the difference between this architecture and HIP architecture and PMIPv6 scheme. Here we prefer to restrict the analysis to two specific architectures, MobiSplit [30] and Node-ID Architecture [51], which have several similar mechanisms and scenarios to our proposed architecture, even if significant differences exist.

The Node-ID architecture has as common design elements with our mobility architecture the fact of having independent locator domains, end-to-end security based on Node-IDs and reliance on cryptographic self-managed Node-IDs. The difference consists on the role of Node-ID routers (located in the LMAs in our architecture) , which are the contact locators for local nodes, mapping communications across borders by translating between different locator spaces and connectivity technologies, taking over the role NATs have today. The Node-ID router is similar to the Mobility Anchor Point (MAP) of Hierarchical Mobile IP v6 (HMIPv6) [19], and better to the Local RVS (LRVS) with Security Parameter Index multiplexed Network Address Translator (SPINAT) functionalities as defined in [14], in which local mobility is managed with a host-based scheme. Such mechanism has the drawback of adding complexity to the network and to the terminals and of increasing signaling overhead in the wireless links, compared to the network-based local mobility management proposed in our architecture.

On the other side, MobiSplit uses network-based mobility management mechanism for LMD and is based on the idea of separating mobility management in two levels, local and global, that are managed in completely independent ways. However, MobiSplit does not decouple identifiers from locators and uses MIPv6 as global mobility management protocol. As a consequence, in order to move sessions from one interface to another one, as sessions are linked to the locators, the MN needs to keep the same IP

	Node-ID	MobiSplit	HIP-PMIPv6
Global Mobility	Host-based	Host-based	Host-based
Local Mobility	Host-based	Network-based	Network-based
Multihoming	Local	Global and Local	Global and Local
Ad-hoc Networking	Yes	No	Yes
Security	Yes	No	Yes
Network Complexity	High	Low	Low
Terminal Complexity	Low	High	Low
Signaling Overhead	High	Low	Low

Table 4.1: Architectures Comparison

address while changing interface. This mechanism can bring difficulties from the point of view of the implementation because it is not the normal behavior of IP stack. Moreover, to achieve local multihoming, the same CoA needs to be configured by the MN on each terminal active interface, using for example a virtual interface. This implies that the MN cannot use its interfaces at the same time, as the basic rules of IP networking impose that the same IP address cannot be assigned to more than one interface at time. Compared to MobiSplit, our solution has built-in mechanisms for multihoming thanks to the identifier/locator split and does not implies any modification to the standard IP stack.

Table 4.1 summarizes briefly some characteristics of above described architectures.

4.5 Conclusions

In this chapter we have presented a mobility architecture for future Internet, which is based on HIP and PMIPv6. The combination of these two protocols not only creates an efficient mobility and multihoming management scheme for multihomed terminals and ad-hoc networks at local and global level, but puts also the basis for a new Internet architecture that benefits of HIP built-in features such as security and efficient HI namespace. Moreover, thanks to the particular locators (IPv6 addresses) created through the PMIPv6 scheme, location privacy, efficient routing and traffic engineering at local level are also supported. The mobility and multihoming scheme adopted by this architecture significantly reduces the signaling overhead in the wireless links as well as in the infrastructure without increasing the complexity on networks or on mobile terminals.

Chapter 5

Implementation and Evaluation

5.1 Introduction

In this chapter we analyse PMIPv6 and HIP on an implementation point of view. In particular, we address the practical constrains we have faced when implementing PMIPv6 from the virtualization phase to the real test-bed deployment phase, such as layer 2 attachement and detachment, unicast RA, same MAC address on MAGs and tunnelling. We also present the HIP implementation from InfraHIP Project and MIH implementation from ODTONE project. They can be both combined with PMIPv6 in order to have a complete deployment of the proposed mobility architecture for future Internet.

5.2 Proxy Mobile IPv6 Implementation

5.2.1 PMIPv6 Motivations

As described in section 2.3.1, a global mobility protocol may be necessary when a mobile node moves between two access networks. Mobility between two Access Points (APs) under the same Access Routers (ARs) constitutes intra-link (or Layer 2) mobility, and is typically handled by Layer 2 mobility protocols (if there is only one AP/cell per AR, then intra-link mobility may be lacking). Between these two lies local mobility. Local mobility occurs when a mobile node moves between two APs connected to two different ARs.

Global mobility protocols allow a mobile node to maintain reachability when the MN's globally routable IP address changes. It does this by updating the address mapping between the permanent address and temporary local address at the global mobility anchor point, or even end to end by changing the temporary local address directly at the node with which the mobile node is corresponding. A global mobility management protocol can therefore be used between ARs for handling local mobility. However, there are three well-known problems involved in using a global mobility protocol for every movement between ARs. Briefly, they are:

- Update latency. If the global mobility anchor point and/or correspondent node (for route-optimized traffic) is at some distance from the mobile node's access network, the global mobility update may require a considerable amount of time. During this time, packets continue to be routed to the old temporary local address and are essentially dropped.

- Signaling overhead. The amount of signaling required when a mobile node moves from one last-hop link to another can be quite extensive, including all the signaling required to configure an IP address on the new link and global mobility protocol signaling back into the network for changing the permanent to temporary local address mapping. The signaling volume may negatively impact wireless bandwidth usage and real-time service performance.

- Location privacy. The change in temporary local address as the mobile node moves exposes the mobile node's topological location to correspondents and potentially to eavesdroppers. An attacker that can assemble a mapping between subnet prefixes in the mobile node's access network and geographical locations can determine exactly where the mobile node is located. This can expose the mobile node's user to threats on their location privacy.

These problems suggest that a protocol to localize the management of topologically small movements is preferable to using a global mobility management protocol on each movement to a new link. In addition to these problems, localized mobility management can provide a measure of local control, so mobility management can be tuned for specialized local conditions. Note also that if localized mobility management is provided, it is not strictly required for a mobile node to support a global mobility management protocol since movement within a restricted IP access network can still be accommodated. Without such support, however, a mobile node experiences a disruption in its traffic when it moves beyond the border of the localized mobility management domain.

Existing solutions for localized mobility management fall into two classes:

1. Interoperable IP-level protocols that require changes to the mobile node's IP stack and handle localized mobility management as a service provided to the mobile node by the access network.
2. Link specific or proprietary protocols that handle localized mobility for any mobile node but only for a specific type of link layer, for example, 802.11.

The dedicated localized mobility management IETF protocols for Solution 1 are not yet widely deployed, but work continues on standardization. Some Mobile IPv4 deployments use localized mobility management. For Solution 1, the following are specific problems:

- The host stack software requirement limits broad usage even if the modifications are small. The success of WLAN switches indicates that network operators and users prefer no host stack software modifications. This preference is independent of the lack of widespread Mobile IPv4 deployment, since it is much easier to deploy and use the network.
- Future mobile nodes may choose other global mobility management protocols, such as HIP or MOBIKE [52]. The existing localized mobility management solutions all depend on Mobile IP or derivatives.
- Existing localized mobility management solutions do not support both IPv4 and IPv6.
- Existing host-based localized mobility management solutions require setting up additional security associations with network elements in the access domain.

Market acceptance of WLAN switches has been very large, so Solution 2 is widely deployed and continuing to grow. Solution 2 has the following problems:

- Existing solutions only support WLAN networks with Ethernet backhaul and therefore are not available for advanced cellular networks or picocellular protocols, or other types of wired backhaul.
- Each WLAN switch vendor has its own proprietary protocol that does not interoperate with other vendors' equipment.
- Because the solutions are based on Layer 2 routing, they may not scale up to a metropolitan area or local province, particularly when multiple kinds of link technologies are used in the backbone.

Having an interoperable, standardized localized mobility management protocol that is scalable to topologically large networks, but requires no host stack involvement for localized mobility management is a highly desirable solution [53].

Compared with Solution 1, a network-based solution requires no localized mobility management support on the mobile node and is independent of global mobility management protocol, so it can be used with any or none of the existing global mobility management protocols. The result is a more modular mobility management architecture that better accommodates changing technology and market requirements.

Compared with Solution 2, an IP-level network-based localized mobility management solution works for link protocols other than Ethernet, and for wide area networks.

Having these requirements in mind, IETF NETLMM WG has proposed PMIPv6 [5] as a new network-based mobility protocol for IPv6 nodes which does not require host involvements. It extends MIPv6 [10] signaling and reuses many concepts such as the Home Agent (HA) functionalities.

Anyway, even if there is a strong interest from mobile network operators on PMIPv6, the protocol is still missing a detailed implementation analysis that could speed up its adoption by the mobile network operators. We have implemented PMIPv6, taking into account all the important recommendations for respecting the standard and, at the same time, for reducing handover delays. To the best of our knowledge, this is the first attempt to study PMIPv6's implementation issues, such as Layer 2 attachment and detachment, unicasted Router Advertisement (RA) messages, default router detection and tunneling, and to evaluate their impact on protocol's performances. Our PMIPv6's implementation is developed with all the machines running Ubuntu 7.10 with 2.6.22-15-generic Linux kernel and reusing Mobile IPv6 for Linux (MIPL) v.2.0.2. [54] on a real test-bed for an experimental evaluation of PMIPv6. Analysis of each implementation configuration and evaluation of different performance metrics are provided in the following sections.

5.2.2 PMIPv6 Overview on Implemetation Point of View

Figure 5.1 illustrates the PMIPv6 architecture with the two core functional entities to be implemented:

- LMA: it has similar implementation functionalities as HA in MIPv6. LMA is responsible for maintaining the MN's reachability state and it is the topological anchor point for the MN's HNP. LMA has a cache which includes a Binding Cache Entry (BCE) for each currently registered MN with the MN-Identifier, the MN's HNP, a flag indicating the proxy registration and the interface identifier of the bi-directional tunnel between the LMA and the MAG.
- MAG: it is the entity that performs the mobility management on behalf of the MN and it resides on the access link where the MN is anchored. The MAG is responsible for detecting the MN's movements to and from the access link and for initiating binding registrations to the MN's LMA through PBU-PBA messages. We have enhanced BU and BA messages from MIPv6 to carry the additional information of PBU and PBA. Moreover, the MAG establishes a tunnel with the LMA for enabling the MN to use the address from its HNP and emulates the MN's home network on the access network for each MN. For tunnelling functionalities we have reused MIPv6 tunnelling functions, in our case applied between LMA and MAG instead of between HA and MN as in MIPv6.

The main steps in the PMIPv6 mobility management scheme are described hereafter:

- MN attachment: once a MN enters a PMIPv6 domain and attaches to an access link, the MAG on that access link performs the access authentication procedure implemented with a RADIUS policy server in our case using the MN's profile, which contains the MN-Identifier, the LMA's address and other related configuration parameters;
- Proxy Binding exchange: the MAG sends to the LMA a PBU message on behalf of the MN including the MN-Identifier. Upon accepting the message, the LMA replies with a PBA message including the MN's

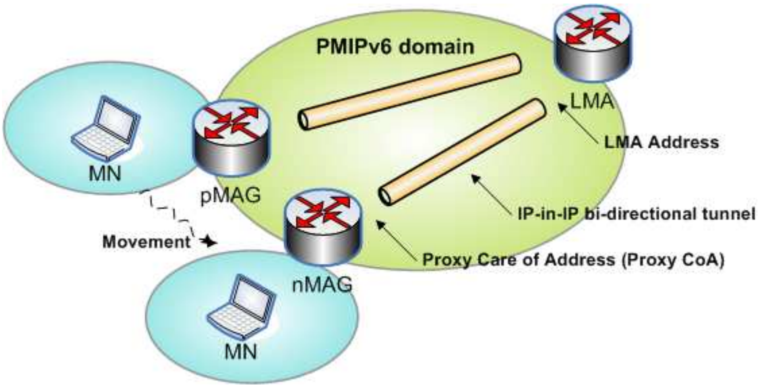
PMIPv6 domain
LMA
LMA Address
MN
pMAG
IP-in-IP bi-directional tunnel
Movement
Proxy Care of Address (Proxy CoA)
nMAG
MN

Figure 5.1: Overview of PMIPv6 Architecture.

HNP. With this procedure the LMA creates a BCE for the MN and a bi-directional tunnel between the LMA and the MAG is set up similarly to MIPv6 tunneling;

- Address Configuration procedure: at this point the MAG has all the required information for emulating the MN's home link. It sends a unicasted RA message, implemented through a modification of RADVD daemon of MIPv6, to the MN on the access link advertising the MN's HNP as the hosted on-link-prefix. On receiving this message, the MN configures its interface either using stateful or stateless address configuration modes. Finally the MN ends up with an address from its HNP, which it can use while moving in the PMIPv6 domain.

The LMA, being the topological anchor point for the MN's HNP, receives all packets sent to the MN by any CN and forwards them to the serving MAG through the bi-directional tunnel. The MAG on other end of the tunnel, after receiving the packet, removes the outer header and forwards the packet on the access link to the MN.

The MAG typically acts as a default router on the access link. It intercepts any packet that the MN sends to any CN and sends them to its LMA through the bi-directional tunnel. The LMA on the other end of the tunnel, after receiving the packet, removes the outer header and routes them to the destination. The functionalities of inner and outer header add and removal are implemented as in the HA of MIPv6.

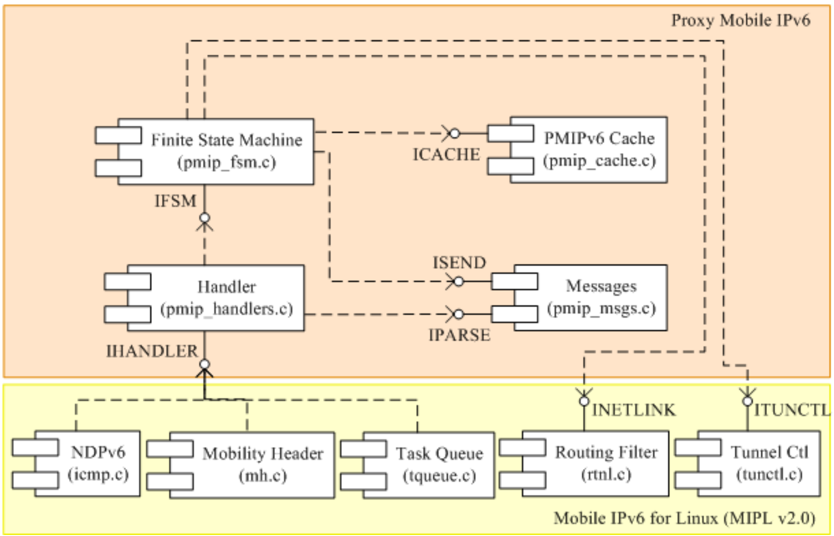

Figure 5.2: PMIPv6 Software Architecture.

5.2.3 Real Implementation of PMIPv6

We have implemented PMIPv6 first under Linux vanilla kernel 2.6.20 and then under 2.6.22-15-generic Linux kernel reusing Mobile IPv6 for Linux (MIPL) v 2.0.2 [54]. All the basic bricks of MIPL are used in an efficient way [55] as shown in Figure 5.2.

In MIPL, Mobile IPv6 is implemented using multi threads: one for handling the ICMPv6 messages, one for handling Mobility Header messages, and another one for handling tasks and time events. To support PMIPv6, we have extended these elements and implemented handlers for all necessary messages and events. ICMPv6 messages and Mobility Header messages are parsed by the Handler as inputs to the Finite State Machine, which is the heart of the system. Two different Finite State Machines are defined for LMA and MAG. They are in charge of making appropriate decisions and controlling all the other elements to provide a correct predefined protocol behavior. The PMIPv6 Binding Cache stores all information about MNs' points of attachment and it is kept up-to-date with the mobility of MNs.

As PMIPv6 implementation is built on top of MIPL version 2.0.2, it could be, in the future, easily integrated in MIPL, growing in line with the standards as well as with MIPL source code.

Virtualization-based Development Process Phase

The first development phase has been realized in a virtualization-based process [56] using a combination of User-mode Linux (UML) [57] - [58] and Network Simulator 2 (Ns-2) Emulation [59], allowing the migration to the real testbed with minor changes.

UML is a Linux kernel which is compiled to run as a virtual machine on a Linux host. The virtual machine, called the guest to distinguish it with the real host machine, can be assigned to a guest root file system and other virtual physical resources different from the host machine. A UML virtual machine requires a guest kernel and a guest root file system. The guest root file system of an UML is stored in a file on the real host machine. The guest root file system is a normal file that can be mounted directly to the host file system. This allows developers to work with the guest file system without the need of turning on the virtual machine. Copy-On-Write is another interesting feature when playing with UML as it allow different virtual machines to run on the same guest root file system and save the disk space by storing the differences in .cow files. Figure 5.3 shows the dependency between different components of UML.

The Ns-2 emulation feature has been used to emulate the wireless environment. It can grab packets from a virtual machine with real IPv6 stack, pass them through a simulated wireless network, and then inject them back into the destination virtual machine. To emulate the wireless transmission and the mobility of the mobile node, we extend the Ns-2 Emulation, allowing the mapping of the virtual machines into Ns-2 wireless nodes.

During this preliminary phase, the topology has been generated by the Virtual Network User-mode Linux (VNUML) [60]. The Linux kernel 2.6.20 has been compiled under User-mode architecture to serve as a guest kernel for virtual machines. The scenario have been defined and automated with Tcl language, which it is a part of Ns-2 Emulation.

Real Test-bed Process Phase

Once we have reached a stable deployment of our code, we have migrated to a real test-bed process phase and to 2.6.22-15-generic Linux kernel. Figure 5.4 shows the experimental topology of our test-bed. An unmodified MN, which does not have any specific software for mobility, uses its Netgear wireless card to attach to one of the two Cisco Aironet 1100 series Access Points (APs), which support IEEE 802.11a/g specifications. Each AP is directly connected with a MAG. The implementation of MAG functionalities

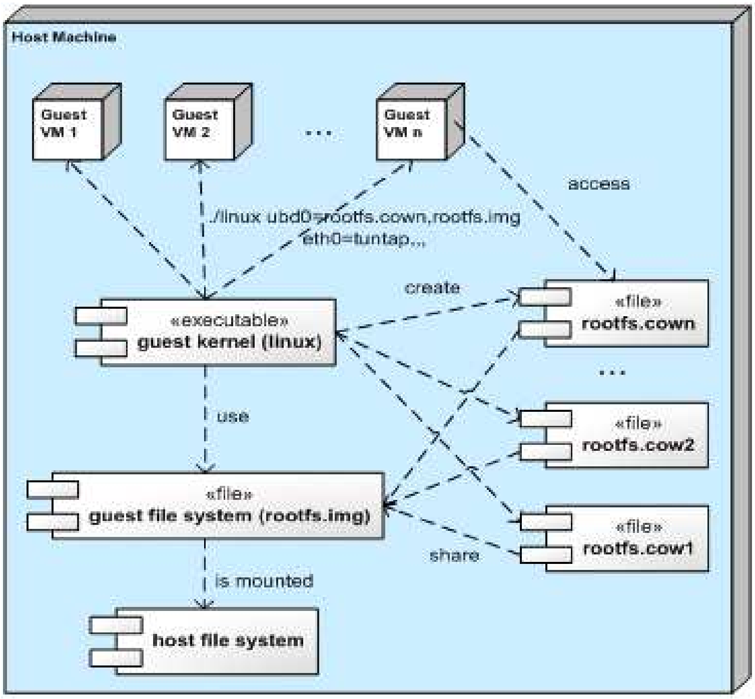

Figure 5.3: Virtualization with User-mode Linux.

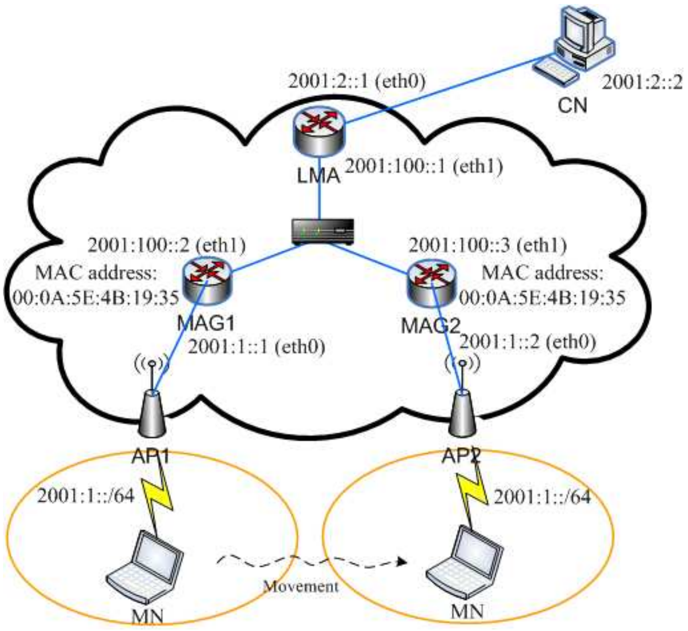

Figure 5.4: Test-bed Topology.

contains additional features and modifications of MIPL to handle PBU and PBA messages and mobility options, and a modified Router Advertisement daemon (RADVD), which unicasts RAs with a specific HNP per MN. Each MAG is connected to the LMA. The LMA is configured as a modified HA in MIPL which stores a unique HNP in the BCE for each MN and it is able to handle PBU and PBA messages. Finally, an unmodified CN is connected to the LMA. All the entities in the test-bed are running Ubuntu 7.10 with 2.6.22-15-generic Linux kernel. More detailed specifications of each device are presented in Table 5.1.

5.2.4 PMIPv6 Implemetation Analysis

Our implementation of PMIPv6 protocol is not the first tentative to provide experimental results on PMIPv6, but it is the only one that analyses the implementation issues of the protocol and gives an implementation perspective. In [61] authors compare PMIPv6 with other local mobility management protocols, but the implementation is using IPv6-in-IPv4 tunnel to emulate the IPv6 network and a network emulator to emulate the network environment. Moreover, no specifications are given to operators for PMIPv6 implementa-

Name	Hardware Configuration
LMA	CPU Pentium 4 2 GHz RAM 512 MB NIC 3com 3C905C-Tx
MAG	CPU Pentium 4 2,66 GHz RAM 1 GB NIC 3com 3C905C-Tx
AP	Cisco Aironet 1100 series AIR-AP 1120 B SERIES
MN	CPU Pentium M 1,6 GHz RAM 512 MB NIC Netgear WAG511 v2
CN	CPU Core 2 Duo 2,6 GHz RAM 4 GB NIC Broadcom BCM5755M
HUB	Dell Power Connect 2716 1 G Ethernet

Table 5.1: Hardware Configuration of Devices

tion. [62] focuses its analysis on the empirical comparison between MIPv6 and PMIPv6, demonstrating the superiority of PMIPv6, but no details are provided for important aspects in the PMIPv6 implementation. Also [63] compares MIPv6 with PMIPV6, with the difference that the measurements have been made over two different access networks, WLAN and HSDPA. Signaling and processing overheads have been analyzed, but no mobility handover analysis is provided. In this work we consider the most important practical constraints that we have faced when implementing the standard PMIPv6 in a real test-bed. They can be summarized as follow:

1. **Attachment and detachment phases:** standard PMIPv6 does not specify any functionality for these two phases as its main purpose is to define only the elements and the signaling messages inside the PMIPv6 domain. As point of reference we have considered [64], in which suggestions on the MN-MAG interface are provided. One possibility is to use an IP layer-based solution, the second one is to develop a specific link-layer mechanism. We have chosen the latest as the use of triggers at layer 2 allows faster movement detection. We have used the Syslog messages sent by the Cisco APs to the MAGs containing

"associate", "disassociate" and "reassociate" information to detect attachments and detachments of the MN from the PMIPv6 domain. As future work, we will integrate our PMIPv6 implementation [65] with the IEEE 802.21 Media Independent Handover (MIH) protocol [66] - [67] in order to benefit of a mechanism to gather information from various link types and associated networks in a timely and consistent manner, and deliver it to network layer entities.

2. **Unicast RA:** as the HNP is unique per MN, it needs to be sent in a unicast RA message by the MAG to the specific MN. We have developed and integrated a functionality in the PMIPv6 daemon for MAGs based on RADVD daemon to unicast RAs. MN's address is auto-configured through IPv6 Stateless Address Auto Configuration.

3. **MAG's link-local address configuration:** as specified in [5], the MAG is the IPv6 default-router for the mobile node on the access link. However, as the MN moves from one access link to another, the serving MAG on those respective links will send the RA messages. If these RAs are sent using a different link-local address or a different link-layer address, the MN will always detect a new default-router after every handoff. For solving this problem, standard PMIPv6 requires all the MAGs in the domain to use the same link-local and link-layer address on any of the access links wherever the MN attaches. In order to follow this important specification we have configured all MAGs with the same link-local address using the command

   ```
   Macchanger -m newMAC@ interface
   ```

   This operation brings no drawbacks on the network and on the mobility as it does not involve the link-local address on the network side.

4. **Tunneling:** bi-directional tunnel is used for routing data traffic to and from the MN between the MAG and the LMA. A tunnel hides the topology and enables a MN to use the address from its HNP from any access link in the PMIPv6 domain. A tunnel may be created dynamically when needed and removed when not needed. However, implementations may choose to use static pre-established tunnels instead of dynamically creating and tearing them down on a need basis. We have implemented a static and shared tunnel between each MAG and the LMA in order to serve all the MNs attached to the same MAG with the same tunnel.

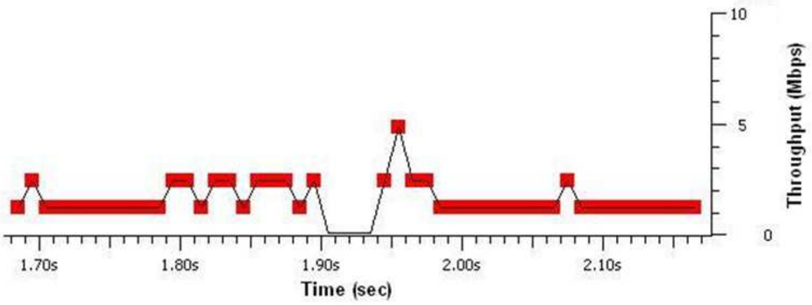

Figure 5.5: UDP Throughput during handover in first scenario.

The impact of these implementation configurations on PMIPv6 performances are analyzed in the following section.

5.2.5 Experimental Results

We have tested the handover performances of our PMIPv6 implementation under the previously described configuration setup and with the test-bed configuration illustrated in Fig. 5.4. Iperf v 2.0.2 [68] is used to generate TCP/UDP traffic. Through Wireshark Software v 1.0.1 [69] we have analyzed the test runs.

As points 1 and 2, layer 2 attachment-detachment and unicast RA, represent practical suggestions on how to implement the protocol, we have focused our analysis on points 3 and 4, MAG's link-local address and tunnelling, which can have an impact on PMIPv6's performance.

First of all, we have analyzed the different behavior of PMIPv6 implementation under different MAG's link local address configurations. In the first scenario we do not use the Macchanger function and we leave the two MAGs with their own MAC addresses, while in the second scenario we apply the modification as shown in Fig. 5.4. Figures 5.5 and 5.6 illustrate the UDP throughput when the MN performs handover from AP1 to AP2 in the respectively two scenarios. We can see that the UDP performances for the second scenario are slightly better than the ones for the first scenario.

To better evaluate the handover latency for UDP traffic we have repeated the test 50 times for each scenario. Results are shown in Fig. 5.7 and summarized in Table 5.2. In the case of different MAC address configuration the handover latency is in average higher than 45 ms, while if we configure the same MAC address in both MAGs the handover latency is in average 32.06 ms.

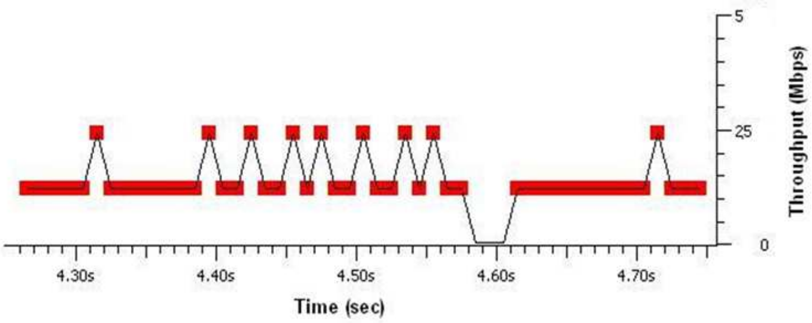

Figure 5.6: UDP Throughput during handover in second scenario.

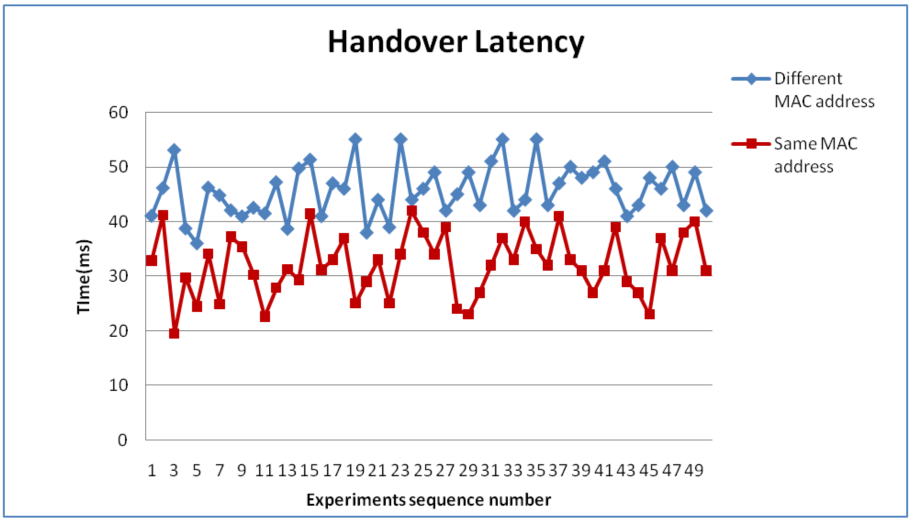

Figure 5.7: Handover Latency for UDP traffic in scenarios 1 and 2.

	Different MAC address Scenario 1	Same MAC address Scenario 2
Average	45.72 ms	32.06 ms
Standard Deviation	4.74 ms	5.71 ms

Table 5.2: Handover Latency for UDP traffic in scenarios 1 and 2

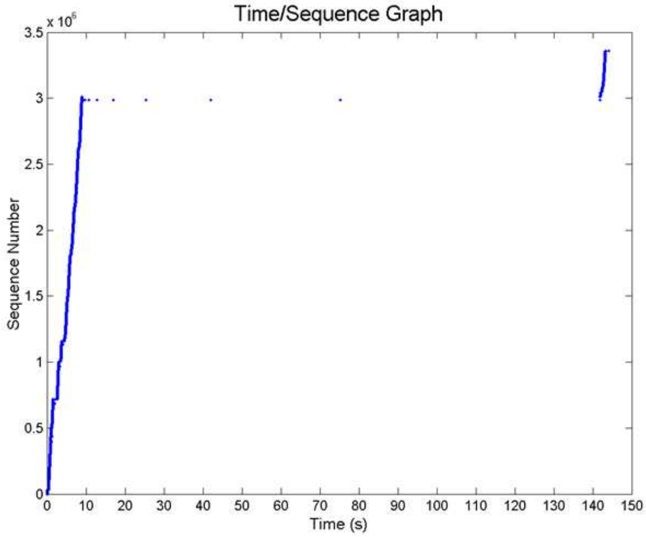

Figure 5.8: Handover Performance for TCP in scenario 1.

	Different MAC address Scenario 1	Same MAC address Scenario 2
Average	122789.05 ms	67.51 ms
Standard Deviation	164.77 ms	10.23 ms

Table 5.3: Handover Latency for TCP traffic in scenarios 1 and 2

Different are the considerations when we analyze the performances of TCP traffic during handover for the two scenarios. Figures 5.8 and 5.9 show, in the time-sequence graphs of TCP, the important difference between the behaviour of handover latency in scenarios 1 and 2. Over 50 test runs we get the results summarized in Table 5.3. This result shows the importance of configuring the same link-local address for all the MAGs, especially for TCP traffic, in order to give the possibility to the MN of using it for routing in the mean-time the default-router is configured.

Finally we have considered a third scenario in which the bi-directional tunnel between MAG and LMA is dynamically created. We want to specify that the previously defined scenario 2 has static tunnel. We have compared the handover latency for UDP traffic between scenarios 2 and 3. As we can see from Fig. 5.10 and Table 5.4 the performances are mainly the same, thus

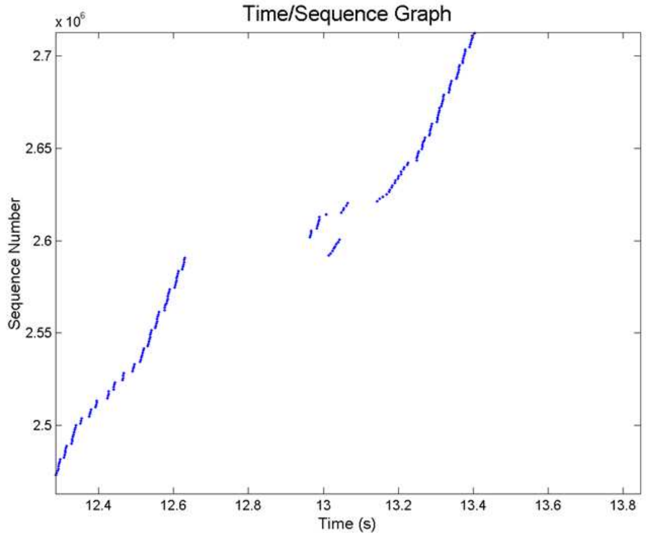

Figure 5.9: Handover Performance for TCP in scenario 2.

	Static Tunnel Scenario 2	Dynamic Tunnel Scenario 3
Average	32.06 ms	33.64 ms
Standard Deviation	5.71 ms	6.15 ms

Table 5.4: Handover Latency for UDP traffic in scenarios 2 and 3

the delay for tunnel creation can be considered irrelevant. Also performances with TCP traffic provide similar results.

5.3 Host Identity Protocol Implementation

5.3.1 Host Stack Implications

HIP is primarily an extension to the TCP/IP stack of Internet hosts. The Host Identity layer is added as a waist between the transport layer and the network layer, as shown in 5.11. There are two primary ways to support HIP on such an end host. The first is to make changes to the kernel implementation to directly support the decoupling of identifier and locator. Although this type of modification has data throughput performance benefits, it is

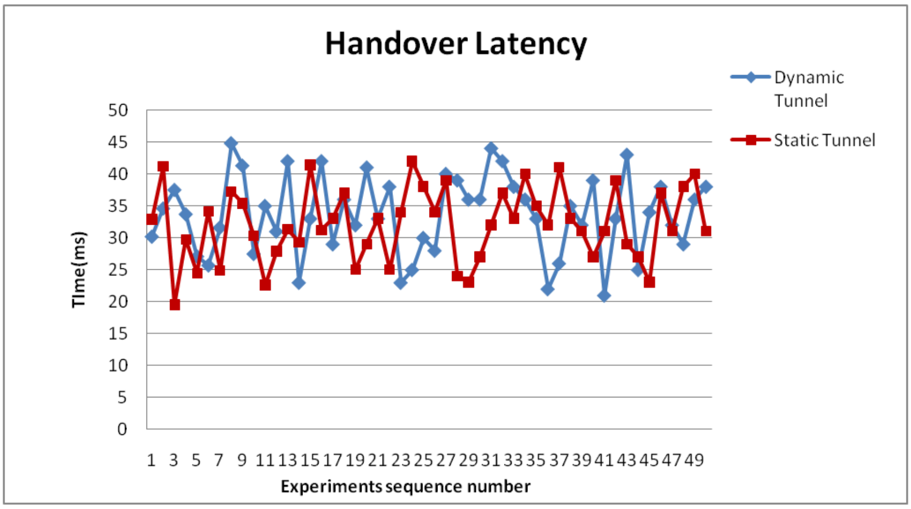

Figure 5.10: Handover Latency for UDP traffic in scenarios 2 and 3.

also the more challenging to deploy. The second approach is to implement all HIP processing in user-space, and configure the kernel to route packets through user-space for HIP processing.

The following public HIP implementations are known and actively maintained:

- HIP4BSD [70] - FreeBSD kernel modifications and user-space keying daemon;
- HIP for Linux (HIPL) [71] - Linux kernel and user-space implementation;
- OpenHIP [72] - User-space keying daemon and packet processing for Linux, Windows XP and Vista, and Apple OS X.

As described in [73], to enable HIP natively in an implementation requires extensions to the key management interface with the security association database (SAD) and security policy database (SPD), changes to the ESP implementation itself to support BEET-mode processing, extensions to the name resolution library, and (in the future) interactions with transport protocols to respond correctly to mobility and multihoming events.

On the other side, HIP can be implemented entirely in user-space, an approach that is essential for supporting HIP on hosts for which operating system modifications are not possible. Even on modifiable operating systems,

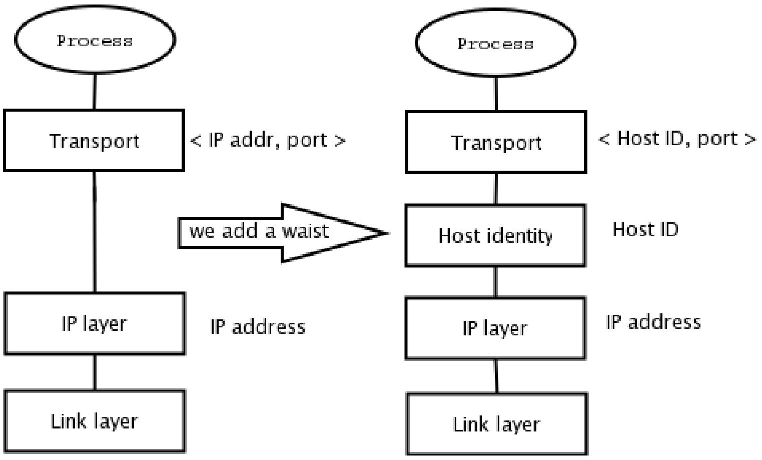

Figure 5.11: Overview of HIP Architecture.

there is often a significant deployment advantage in deploying HIP only as a user-space implementation. All three open source implementations provide user-space implementations including packaging (RPMs, self-extracting installers) typical of application deployment on the target systems.

When HIP is deployed in user-space, some techniques are necessary to identify packets that require HIP processing and divert them to user- space for such processing, and to re-inject them into the stack for further transport protocol processing. A commonly used technique is to deploy a virtual device in the kernel, although operating systems may provide other means for diverting packets to user-space. Routing or packet filtering rules must be applied to divert the right packets to these devices.

As an example, the user-space implementation may install a route that directs all packets with destination addresses corresponding to HITs to such a virtual device. In the user-space daemon, the ESP header and possibly UDP header is applied, an outer IP address replaces the HIT, and the packet is resent to the kernel. In the receive direction, a raw socket bound to ESP or a UDP port number may be used to receive HIP-protected packets. HIP signaling packets themselves may be sent and received by a socket bound to the HIP protocol number or UDP port when UDP encapsulation is used.

Among the three available HIP open source implementations, we have chosen HIPL v.1.0.4-48, the open source of HIP in user-space on Linux kernel, implemented in the frame of InfraHIP project by Helsinki Institute for Information Technology (HIIT) and Helsinki University of Technology (TKK) in Finland in collaboration with industrial partners as Nokia, Er-

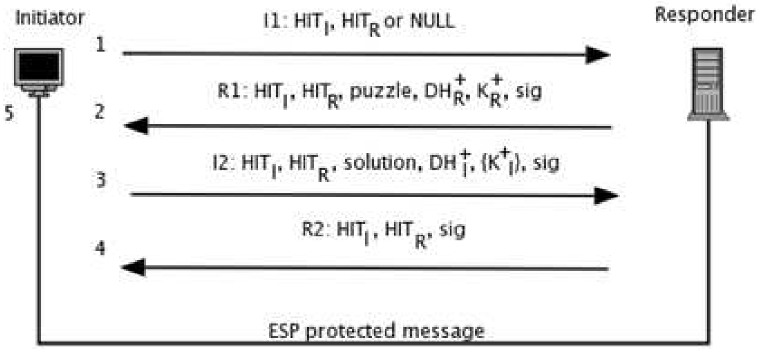
Initiator
Responder
1
I1: HIT_I, HIT_R or NULL
2
R1: HIT_I, HIT_R, puzzle, DH_R^+, K_R^+, sig
3
I2: HIT_I, HIT_R, solution, DH_I^+, (K^+_I), sig
4
R2: HIT_I , HIT_R, sig
5
ESP protected message

Figure 5.12: Message flow in HIP.

icsson, Elisa and Finnish Defence Forces. It represents the most complete implementation of HIP in terms also of infrastructure entities deployment.

5.3.2 HIP Overview on Implemetation Point of View

The Host Identity Protocol (HIP) is composed of two-round-trip, end-to-end Diffie-Hellman key exchange protocol, a mobility exchange and some additional messages. The purpose of the HIP Base Exchange (see Fig. 5.12) is to create assurance that the peers indeed possess private keys corresponding to their host identifiers (public keys). In consequence, the Base Exchange creates a pair of IPSec Encapsulated Security Payload (ESP) Security Associations (SAs), one in each direction.

We can describe this process in following steps:
I → Directory: lookup R
I ← Directory: return R's address and HI/HIT
I1 I → R (Hi, Here is my I1, let's talk with HIP)
R1 R → I (Ok, Here is my R1, handle this HIP cookie)
I2 I → R (Computing, here is my counter I2)
R2 R → I (OK. Let's finish HIP with my R2)
I → R (ESP protected data)
I → I (ESP protected data)
Figure 5.12 shows the process of Base Exchange. First the initiator looks up HI/HIT of the responder from DNS or RVS (Rendezvous Server). Figure 5.13 depicts the procedure for HIP with DNS. On the client side, the

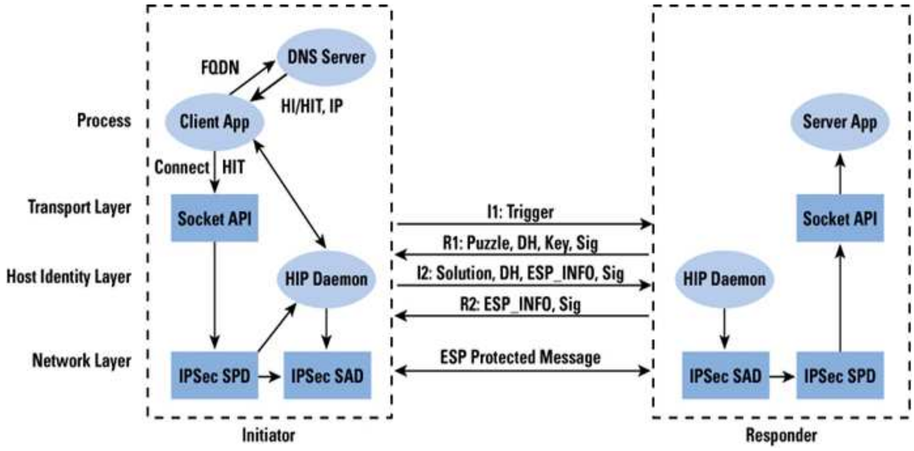

Figure 5.13: HIP Software Architecture.

application sends DNS query to a DNS server. The DNS server replies with HI (FQDN → HI) instead of IP address. In a second step, another lookup is made in the Host Identity layer by the HIP daemon. This time, Host Identities are translated into IP addresses (HI → IP) for network layer delivery.

The transport protocol sends a packet containing server's HI. The Host Identity layer replaces the HI with corresponding IP address of the server. The network layer transmits this packet with an IP header. Accordingly, the 5-tuple socket becomes protocol, source HI, source port, destination HI, destination port from conventional protocol, source IP, source port, destination IP, destination port.

HIP uses a special IPSec ESP mode called Bound End-to-end Tunnel (BEET). The new mode provides limited tunnel mode semantics without the regular tunnel mode overhead.

Mobility

Since the SAs are not bound to IP addresses, the host is able to receive packets that are protected using a HIP-created ESP SA from any address. Thus, a host can change its IP address and continue to send packets to its peers. Figure 5.14 depicts the mobility process. In the beginning, the mobile host is at address 1 and it moves to the address 2 later. During the mobility process, the mobile host is disconnected from the peer host for a brief period of time while it switches from address 1 to address 2. Upon obtaining a new

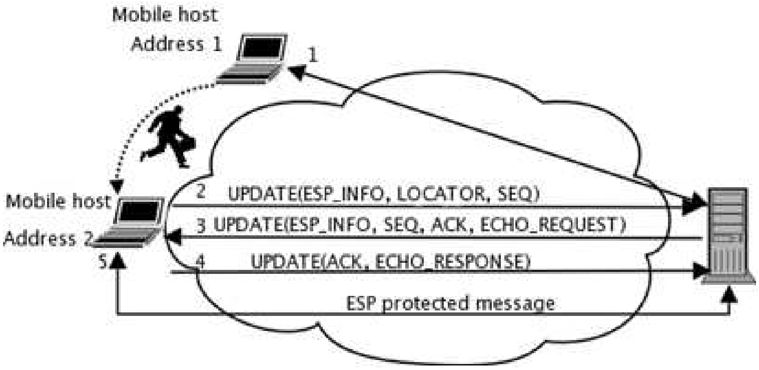
Mobile host
Address 1
1
Mobile host
Address 2
2 UPDATE(ESP_INFO, LOCATOR, SEQ)
3 UPDATE(ESP_INFO, SEQ, ACK, ECHO_REQUEST)
4 UPDATE(ACK, ECHO_RESPONSE)
5
ESP protected message

Figure 5.14: HIP Mobility Scheme.

IP address, the mobile host sends a LOCATOR parameter to the peer host in an UPDATE message. The LOCATOR indicates the new IP address, the SPI associated with new IP address, the address lifetime and whether the new address is a preferred address. The peer host performs an address check and solicits a response from the mobile host. Depending on whether the mobile host has initiated a rekey, and on whether the peer host itself wants to rekey to verify the mobile host's new address, the process can be categorized into three cases:

1. Readdress without rekeying, but with an address check, as in Fig. 5.14;

2. Readdress with a mobile-initiated rekey;

3. Readdress with a peer-initiated rekey.

Multihoming

A host can sometimes have more than one interface. The host may notify the peer host of the additional interfaces by using the LOCATOR parameter. In Fig. 5.15 we assume that the multihoming host has two IP addresses, addr1 and addr2. Further, we assume that addr1 is the preferred address. The multihoming host sends an UPDATE packet including addr1 and addr2 to its peer host. The peer host sends UPDATE packets to each address and updates corresponding SPIs.

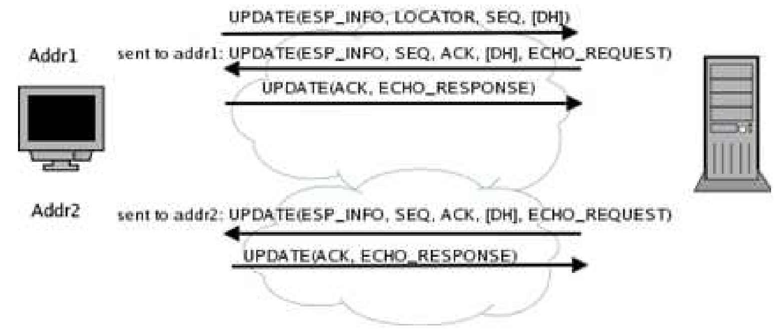
UPDATE(ESP_INFO, LOCATOR, SEQ, [DH])
Addr1
sent to addr1: UPDATE(ESP_INFO, SEQ, ACK, [DH], ECHO_REQUEST)
UPDATE(ACK, ECHO_RESPONSE)
Addr2
sent to addr2: UPDATE(ESP_INFO, SEQ, ACK, [DH], ECHO_REQUEST)
UPDATE(ACK, ECHO_RESPONSE)

Figure 5.15: HIP Multihoming Scheme.

5.4 Combined PMIPv6 and HIP Implementation

We have combined our PMIPv6 implementation with HIPL in the testbed illustrated in Fig. 5.4 for testing the performances of our mobility architecture for future Internet in the case of intra-technology handover.

PMIPv6 software runs on LMA and MAGs, the entities of the local domain, while MN and CN runs HIP daemon as client and server respectively. Moreover, in order to be more compliant with PMIPv6 standard, we have also implemented a RADIUS Server and a RADIUS Client collocated in the LMA and MAG respectively for MN's authentication and for storing its HNP.

In our IPv6-based scenario, the MN moves between AP1 to AP2 and also changes its subnet moving between MAG1 and MAG2. To make a realistic scenario, we have executed tests in which the MN receives a multimedia stream (video and audio) from the CN using the VideoLAN (VLC) software [74]. In order to make VLC a HIP-enabled application, we have just specified the HIT of the MN, instead of its IPv6 address, when starting the VLC at the server side. As specified by HIP, in the multimedia stream, UDP packets are encapsulated and sent using a special IPSec ESP mode called Bound End-to-End Tunnel (BEET). Video and audio data are encoded using MP4V and MPGA respectively. Video and audio use Constant Bit Rate (CBR) encoding method.

With this scenario, we have executed 50 test runs in order to measure the handover latency experienced by the MN in the case of intra-technology handoff. The measurements of UDP throughput are extracted from Wireshark software running in the MN during its movements from AP1 to AP2 while receiving the multimedia stream. At the same time, we have collected

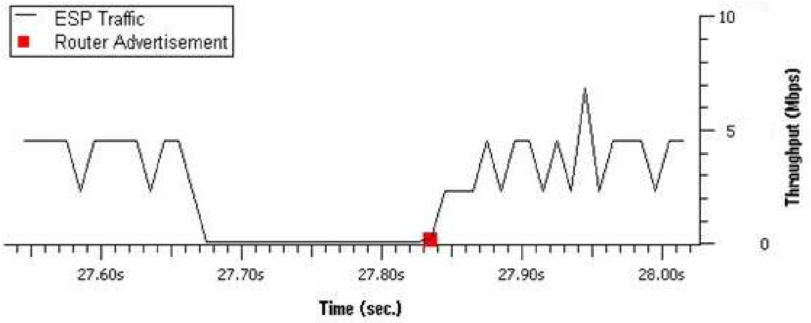

Figure 5.16: UDP Throughput during Intra-technology Handover.

the traces from MAG2 in order to measure the delay corresponding to each PMIPv6 phase.

From Fig. 5.16 we can see that the UDP throughput is quite stable and becomes zero during the handover for less than 200 ms. In particular, we can notice that as soon as the MN receives the RA message (red square), which is the last step of PMIPv6 procedure, the MN starts again receiving the multimedia stream.

Moreover, from Fig. 5.16 and Table 5.5, where we have reported the measured handover latencies for the 50 test runs, we can assess that the handover process for intra-technology handoff takes in average less than 200 ms.

Finally in Table 5.6 we have reported the breakdown of the PMIPv6 latency considering all the important phases of PMIPv6 procedure. The table shows that there is not significant difference between the latency of the different phases of PMIPv6, only the PBA-RA is taking longer due to the latency of RADVD daemon responsible for unicasting the RA.

It is important to point out that the PMIPv6 latency has very reduced contribution to the total handover latency reported above. From Table 5.6 we can see that in average PMIPv6 latency measured over 50 tests is 16.78 ms, while from Table 5.5 we have an overall handover delay of 195.12 ms. Unfortunately the phase of attachment at layer 2 at the Wi-Fi is quite relevant and affects the overall handover latency. It would be possible to improve the performances of this phase including in the PMIPv6-HIP software deployment the Media Independent Handover software. Moreover, MIH will help the deployment of the inter-technology handover as its main goal is to improve handover between heterogeneous network technologies. The following section provides some indications and suggestions.

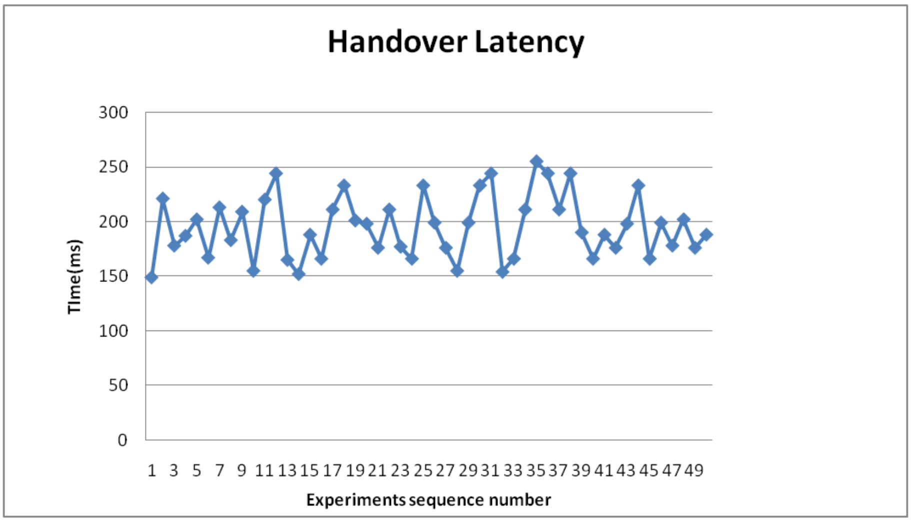

Figure 5.17: Handover Latency during Intra-technology Handover.

	PMIPv6 - HIP Combination Handover Latency
Average	195.12 ms
Standard Deviation	28.39 ms

Table 5.5: Handover Latency for real-time traffic in PMIPv6-HIP scenario

Phases	Average
L2 Attachment - Access Request	1.06 ms
Access Request - Access Accept	1.99 ms
Access Accept - PBU	1.87 ms
PBU - PBA	2.32 ms
PBA - RA	7.21 ms
Total PMIPv6 Latency	16.78 ms

Table 5.6: Handover Latency of PMIPv6 Phases

5.5 Media Independent Handover Implementation

5.5.1 MIH Motivations and Overview

Device manufacturers are integrating more network interfaces into their devices. Many cell phone models now support both Wi-Fi and 3G wireless. Notebook computers are available with built-in support for Wi-Fi, WiMAX, and 3G. As this trend in multi-interface devices continues, operators with multiple networks must facilitate easy access across their multiple technologies through a single device. Supporting seamless roaming and inter-technology handover is a key element to help operators manage and thrive from this heterogeneity.

Operators who have the ability to switch a user's session from one access technology to another can better manage their networks and better accommodate the service requirements of their users. For example, when the quality of an application running on one network is poor, the application can be transferred to another network where there may be less congestion, fewer delays, and higher throughput. Operators also can leverage this ability to manage multiple interfaces to balance traffic loads more appropriately across available networks, improving system performance and capacity.

IEEE 802.21 [66] defines a Media Independent Handover (MIH) framework that can significantly improve handover between heterogeneous network technologies. The standard defines the tools required to exchange information, events, and commands to facilitate handover initiation and handover preparation. IEEE 802.21 does not attempt to standardize the actual handover execution mechanism. Therefore, the MIH framework is equally applicable to systems that employ mobile IP at the IP layer.

IEEE 802.21 is unique within IEEE standards in that it provides interworking within IEEE 802 systems (e.g., IEEE 802.11 and IEEE 802.16e) and between IEEE 802 and non-IEEE 802 systems (e.g. cellular networks). The need for MIH services spanning multiple external networks led to the creation of the IEEE 802.21 WG with a project to create a standard that "defines extensible 802 media access independent mechanisms that enable the optimization of handover between heterogeneous 802 systems and may facilitate handover between 802 systems and cellular systems".

The purpose of IEEE 802.21 is to improve the user experience by providing an MIH functionality that facilitates both mobile-initiated and network-initiated handovers. The specification consists of the following elements:

- MIH Function (MIHF), which encompasses three types of services:

  - The Media Independent Event Service (MIES) detects changes in link layer properties and reports appropriate events from both local and remote interfaces.
  - The Media Independent Command Service (MICS) provides a set of commands for both local and remote MIH users to control link state.
  - The Media Independent Information Service (MIIS) provides information about neighboring networks including their location, properties, and related services.

- Service Access Points (SAPs), which define both media-independent and media-specific interfaces. In particular, the SAPs include:
  - MIH-SAP, a media independent SAP that provides a uniform interface for higher layers to control and monitor different links regardless of access technology.
  - MIH-LINK-SAP, a media specific SAP that provides an interface for the MIHF to control and monitor media specific links. For the MIHF to provide MIES and MICS for a specific link layer, it must implement the MIH-LINK-SAP for that specific link layer.
  - MIH-NET-SAP, a media-dependent SAP that provides transport services over the data plane on the local node, supporting the exchange of MIH information and messages with the remote MIHF.
- MIH users, which are the functional entities that employ MIH services.

The MIHF is a logical entity that provides abstract services to the higher layers through a media independent interface and obtains information from the lower layers through media specific interfaces. MIH services may be either local or remote, with local operation occurring within a protocol stack and remote operation occurring between two MIHF entities. For example, remote communication can occur between an MIHF entity in a mobile node and another MIHF entity located in the network.

The MIH SAPs are defined in terms of primitives in the IEEE 802.21 specification, which provides information about their functionality and parameters. The 802.21 specification does not mandate a specific programming language for representing the primitive and requires implementers of the MIHF to define specific application programming interfaces (APIs) in terms of their chosen programming language.

MIH users are abstractions of the functional entities that employ MIH services, that is, consumers of MIH services. A typical user of MIH services could be a mobility management application that would use these services to optimize handovers, e.g. PMIPv6. MIH users can subscribe with the MIES to be notified when specific events important to the handover decision and process occur.

5.5.2 Real Implementation of MIH

ODTONE [75] stands for Open Dot Twenty ONE and is an open source implementation of a Media Independent Handover Function (MIHF) for the IEEE 802.21 Media Independent Handover Services standard, using C++ APIs. It has been implemented by the Heterogeneous Working Group at Instituto de Telecomunicações (IT) in Aveiro, Portugal.

ODTONE supplies the implementation of a MIHF, supporting its inherent services (Media Independent Event Service (MIES), Media Independent Command Service (MIIS) and Media Independent Command Service (MICS), as well as supporting mechanisms (Capability Discovery, MIHF Registration, Event Registration, etc.).

ODTONE's implementation aims to provide a MIHF that works as a base for user's scenarios, and which enables the users to implement their own MIH-SAP and MIH-LINK-SAP. ODTONE provides a simple and flexible interface for the development of these SAPs, handling MIH Protocol messages and state transitions.

The MIH architecture, shown in Fig. 5.18, features a MIHF supporting the MIES, MICS and MIIS, as well as support logic to manage the MIH Protocol and the interaction with MIH services. These services are made available by the MIH-SAP to users, and allow them to connect to their own technology adapters via the MIH-LINK-SAP.

5.6 Conclusions

This chapter has started with our PMIPv6 implementation on a real-test bed and on the analysis of the practical constrains that need to be taken into account when developing the software. Suggestions on how to implement layer 2 attachement and detachement and unicast RA are provided, together with considerations on the importance of applying the same MAC address on all the MAGs and on using static or dynamic tunnelling. Then HIP software from InfraHIP project has been presented and combined with our PMIPv6 software in order to test intra-technology handover for our proposed

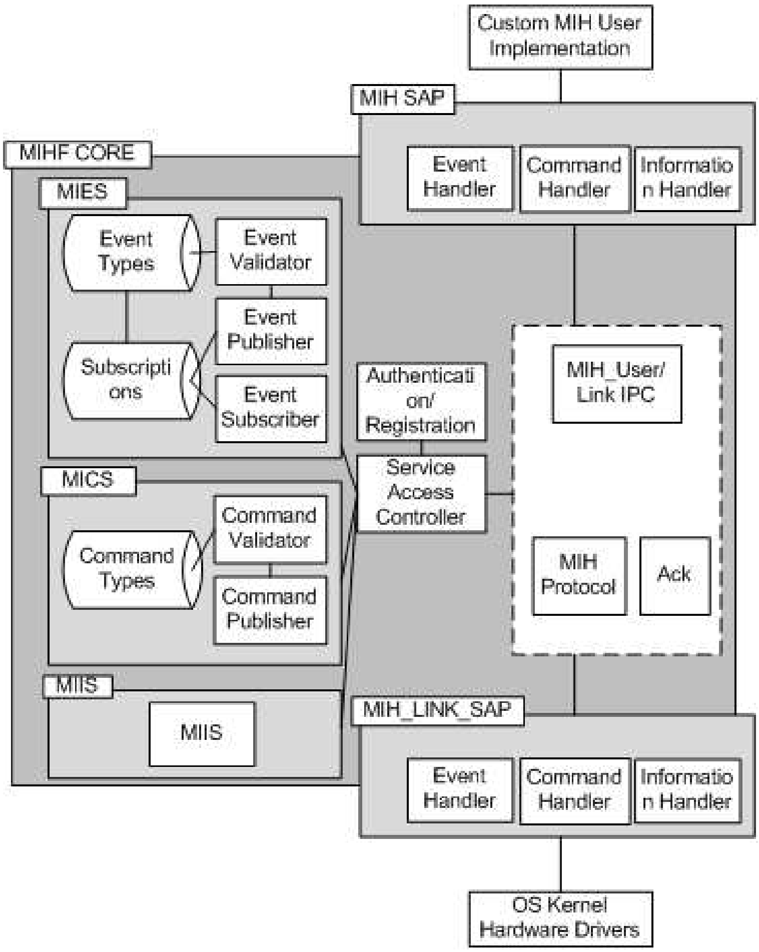

Figure 5.18: MIH software architecture.

mobility architecture. Finally we have concluded the chapter suggesting the MIH software from ODTONE Project to be included into the test-bed to improve layer 2 latency and facilitate the deployment of the inter-technology handover.

Chapter 6

Public Safety Applications

6.1 Introduction

The awareness of the need for effective emergency telecommunication network has raised, especially after recent major disasters. The lesson learned from them and from the interviews to team leaders at first response organizations points out that the use of public communication systems is not sufficient. There are important factors, not considered in public communication systems, which responders faced during rescue operations: mobility, access heterogeneity and security. Mobility and access heterogeneity refer to the ability for Public Safety users to roam between different networks, potentially operated by different agencies and jurisdictions, and the procedures involved in self-organization as device discovery, connection establishment, address allocation, routing and topology management. On the other hand, a common secure system is needed at the disaster site in order to protect sensitive data coming from multiple federal, state and local agencies with different charters and possibly also from military forces, assuring encryption and information privacy.

In this chapter we apply the combination of HIP-PMIPv6 scheme to Public Safety Networks and we propose an advanced hybrid satellite and terrestrial system for emergency mobile communications, that is quickly deployable and dynamically adaptable to disasters of any nature and location, as a potential solution to the above requirements. The overall architecture is IPv6-based and we present and emphasize the important role of Vehicle Communication Gateways (VCGs) in the system. Thanks to the satellite and wireless interfaces, VCGs are able to connect via satellite the disaster area with the headquarters, to create an inter-vehicular mobile ad-hoc mesh network in the emergency field and to provide connectivity to isolated IPv6 cells. Two types of VCGs are envisaged from a satellite interface point of view, S-UMTS vehicles operating in L or S band and nomadic DVB-RCS vehicles operating in Ku or Ka band.

6.2 Emergency Management Phases

Disaster can be defined as the onset of an extreme event causing profound damage or loss as perceived by the afflicted people. Disasters can be of different types: natural disasters, as hurricanes, floods, drought, earthquakes and epidemics, or man-made disasters, as industrial and nuclear accidents, maritime accidents, terrorist attacks. In both cases, human lives are in danger and the terrestrial telecommunication infrastructures may be no longer operational [76]. Moreover, the crisis scenarios are quite complex as frequently terrestrial infrastructure is disrupted, civil protection agencies involved in the recovery operations use different systems, and services supporting emergency preparedness missions must be provided priority treatment over other traffic. In these scenarios, satellite communications networks can play an important role as they provide ubiquitous coverage, instant and flexible hot spot capacity, including broadband services, and a backup for terrestrial networks [77]. Also they can contribute in all the emergency management phases.

Disaster management involves three main phases:

- Preparedness must be to some extent envisaged:
  - Satellite networks must be operational when some disaster occurs.
  - To observe the Earth, to detect hazards at an early stage.
- Crisis from break-out (decision to respond) to immediate disaster aftermath, when lives can still be saved. Crisis is understood as the societys response to an imminent disaster; it must be distinguished from the disaster itself.
- Return to normal situation must be envisaged with provisory networks based on satellite links.

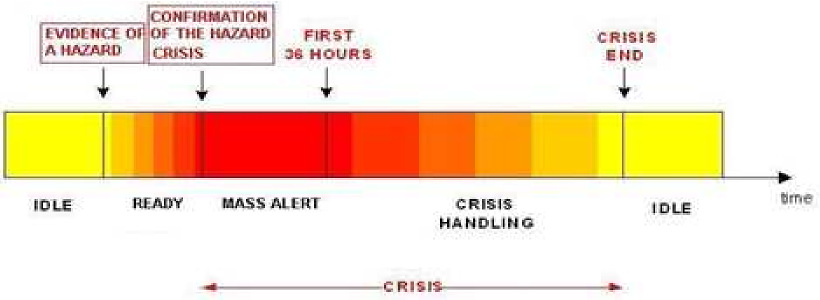

Figure 6.1: Successive Phases of an Emergency Situation.

Figure 6.1 represents the three main phases of a disaster management in a temporal scale underlining each different state.

In this way it is possible to represent all the phases in a state diagram as shown in Fig. 6.2.

6.2.1 Preparedness

The first phase called preparedness involves missions accomplished in normal situation. They are basically of three kinds:

- Observation. The observation system has two main functions:
  - Detection of hazards. Satellite can play a role to that respect by means of observation and scientific satellites. A typical case when satellites can detect hazards prior to any other means is meteorological hazards.

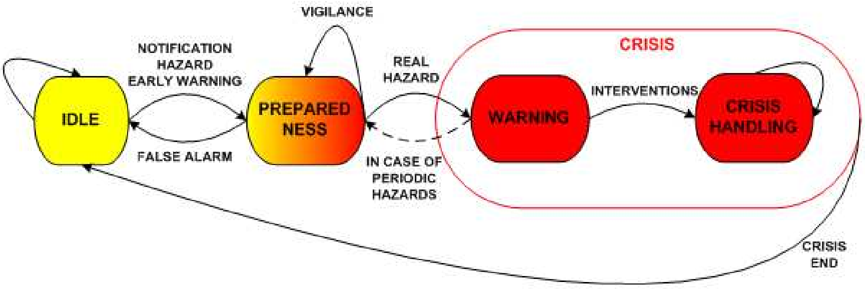

Figure 6.2: Emergency State Diagram.

  - Location of the source of hazards. Satellite is nowadays the best means to provide the geographical coordinates of any object thanks to GPS/Galileo/Glonass constellations. The idea is to have terrestrial sensors coupled with a GPS/Galileo/Glonass sensor.

- Maintenance of the system. An emergency system must be ready to start at any time. To that end, it must be tested at regular time intervals in quiet times from end to end.

- Education of professionals and citizens.

Detection of a hazard

In terms of networks, detection may be considered as the essential function of a feeder link or uplink. Detection of a hazard may be done by several means:

- Emergency call: this is the case where a Citizen is calling a dedicated emergency call centre e.g. dialing 112 in Europe to witness of the break out of a hazard.

- Systematic watch by professionals e.g. helicopters flying over forests in summertime to detect fires.

- Sensors involved in a complex network with machine-to-machine connections. Sensors are useful in places where human being can not go (nuclear reactor) or actually rarely goes (water level sensor upward a river to detect inundations). Satellite is then a relevant solution to connect the sensors to an expertise centre.

6.2.2 Crisis

In a situation of crisis the involved parties can be classified in the following way, taking also into account the degree of mobility they need:

- Local Authority (ies) (LA); *fixed*: the person (or group of persons) in the administrative hierarchy competent to launch a warning to the population and to the Intervention Teams.

- Citizens (Cs); *either mobile or fixed*: non professional people involved in the crisis.

- Intervention Teams (ITs); *mobile*: professionals (civil servants or militaries) in charge of rescuing Citizens in danger, preventing hazard extension or any time critical mission just after the break out of the crisis; in charge of caring injured people once the crisis is over.
- Risk Management Centre (RMC); *fixed*: group of experts and managers in charge of supervising operations. The Risk Management Centre works in close cooperation with Local Authorities.
- Health Centres (HC); *fixed*: infrastructure (e.g. hospital) dedicated to caring injured citizen and backing intervention teams as for this aspect of their mission.

Warning

It is important to manage properly this critical phase as it is the moment where a quick response is the most efficient in terms of lives and goods saved. This means advertising professionals of the incoming hazard.

Warning makes sense if and only if there is a delay between the very break out of the hazard and the damages it could cause which leaves time to people to escape. Warning to the population is always Local Authorities responsibility since they are the only one who can clearly appreciate the danger depending on local circumstances. Deciding that the situation is critical may be taken at governmental, national level. This is the case for examples for earthquakes in all European countries.

In every stage, satellite could be an efficient way to propagate alert. Alert could be a typical mission of a satellite based emergency system.

Crisis Handling

Coordination of Intervention Teams begins when the crisis breaks out. The Local Authorities alert them just before the population and then hand over supervision to the Risk Management Centre. Later on, Intervention Teams still receive instructions from their Local Authorities, from the Risk Management Centre and from the Health Centre. In general, instructions are transmitted through a back-up network made up by a satellite terminal which links the disaster area to terrestrial backbones.

It is worth to create a “cell” surrounding the satellite terminal within which Intervention Teams communicate by terrestrial mobile radio means. It is called an EDECC (Easily Deployable Emergency Communications Cell). It is a very flexible solution based on a lot of radio mobile communication devices that could be packed in a container and transported to the field of operations by helicopter or any other means. In an EDECC, it is possible for example recreate a GSM communication cell by means of a mini Base Transceiver Station linked to a Mobile Switch Centre of any operator. Other technologies are possible too (e.g. WiFi). Intervention Teams return information to Local authorities, to the Risk Management Centre, to Health Centres about the situation and request for help. They use one and the same network for receiving instructions and returning feedback.

6.2.3 Return to Normal Situation

At that point, the crisis is over and the situation has come back to a stable point. The ordinary networks are down and it is necessary to set up a network able to work on a regular basis.

The main functions of the network are the following:

- Coordinating intervention teams and returning feedback from the field which is still necessary at that point.

- As far as possible enabling the same services as before the crisis and offering public access.

The architecture may be the same as the one outlined above with a satellite link but the network should be more stable and powerful.

6.3 Important Factors for Emergency Networks

A flexible communication infrastructure has some specific requirements that need to be considered within the context of emergency response scenarios [78]. They are summarized in the following.

Disaster Categories

Disasters differ from each other depending on their scale, which is crucial to consider in designing an appropriate response/recovery system. This can be defined by the degree of urbanization or the geographic spread. Degree of urbanization is usually determined by the number of people in the affected area, which is very important in disaster handling as the impact of the event changes based on the number of people involved and the breadth of spatial dispersion, both of which impact response and recovery from disasters.

Another key factor, which makes a big difference in the response and recovery stage, is whether the disasters have been predicted or not. Clearly, sudden natural or man-made disasters do not give sufficient warning time. Other disasters may give a longer time window to warn people and take appropriate actions. Thus, if there is advance notification, it is potentially possible to set up a better communication infrastructure and possibly even have a backup technology in place before the disaster occurs.

Specific Technology Requirements

Sometimes depending on the nature of disaster, there are more specific communication needs. For example, telemedicine communication may require interactive real-time communication. Transferring data, audio and video require special bandwidth requirements and high network security. The service needs to be reliable and continuous and work with other different first responder organizations devices if necessary. Users may have different devices such as laptops, palms, or cell phones which may work with different network technologies such as WLAN, WiMAX, WWAN, Satellite, or wired networks. Additionally a communication network needs to be easily configurable and quickly deployable at low cost.

Mobility, Reliability and Scalability

In order to help emergency personnel to concentrate on the tasks, emergency network should be mobile, deployed easily and fast with little human maintenance. Therefore devices must be capable of automatically organizing into a network. Procedures involved in self-organization include device discovery, connection establishment, scheduling, address allocation, routing, and topology management.

The reason for reliability is two-fold. First, in emergency situations each rescue worker must neither be isolated from the command center nor from other team members. Second, mobility is likely to occur frequently in an emergency network. Thus, ability to adapt to network dynamics and harsh situations plays a major role in the design.

Scalability refers to the ability of a system to support large number of parameters without impacting the performance. These parameters include number of nodes, traffic load and mobility aspects. Limited processing and storage capacities of some of the radio devices are also a concern.

Interoperability and Interdependency

Communication technology provides the tool to send data; however when information is sent over different channels or systems, interoperability may not necessarily have been provided. First responder should be equipped with devices capable of using different technology by choosing the appropriate interface card and still working together to form a mesh network and communicate data. Therefore, regardless of what technology each individual might use, they are uniformly connected to the relaying mesh nodes and able to exchange data.

Another factor which needs to be considered in the design of future communication technology is minimizing possible interdependencies in a system. This helps to design a more robust system which is resilient to failures in sub-components of the system.

Multimedia Broadband Services

Communications for the benefit of local rescuers, national authorities or international assistance are mainly to coordinate efforts of field teams and connect teams to remote decision-making centers. In particular, to retrieve monitoring data from the disaster site and to distribute data to local teams or remote expertise centers are important requirements for an emergency communication system. Thus, providing broadband communication capacity during emergency or crisis times is becoming more and more necessary. Concerning services, users basic requirements are voice and data communications with short and long range capabilities, but users require also multimedia communications with large volume of data able to provide the logistics of the situation, medical data, digital map, blueprints or intelligence data.

Knowledge and Training

An important factor to be considered as addressed is the lack of knowledge on exact capabilities of the new technology being deployed and lack of training. The new technology needs to be installed and fully tested in drills and preparation exercises well before it is used in an actual disaster. It is also very important to consider who will be the users of this technology and what level of knowledge and technical background they have. We would like to design future emergency communication tools and public awareness systems to be user friendly with minimal training requirements, yet also secure.

Information Sharing and Data Dissemination

In some disaster scenarios when people have important information, there needs to be a motivation for them to share it across first responder organizations. When the information is provided, there needs to be some mechanism to verify the accuracy of the information provided. Privacy is a factor that needs to be considered in determining who should have access to this information.

Warnings and Alerts

Warning messages should be provided with the consideration that some people may disregard the warnings, therefore even the well-designed warning system must consider human error or resistance.

People may not evacuate to safe areas even if asked or ordered to do so for different reasons such as family, belongings, and pets, or they may not trust the accuracy or source of the warning. They may not take the warning serious if they hear different messages from different sources, or if the source of the warning has not proven to be accurate or reliable in the past. The warning should provide a clear explanation of the nature of the disaster and appropriate actions to be taken.

6.4 Terrestrial and Satellite Systems for Emergency Management

6.4.1 Terrestrial-based solutions

Even though modern telecommunication technology is readily available with modern satellite communication, when faced with a situation of a disaster, rescue forces often rely on very simple communication systems as analogue and digital radio systems described hereafter.

HF, VHF, UHF Equipments

In times of crisis and natural disasters, Amateur radio is often used as a means of emergency communication when wired communication networks, cellular wireless networks and other conventional means of communications fail. High Frequency (HF) designates a range of electromagnetic waves whose frequency is between 3 MHz and 30 MHz. Very High Frequency (VHF) designates a range of electromagnetic waves whose frequency is between 30 MHz and 300 MHz. Ultra high frequency (UHF) designates a range of electromagnetic waves whose frequency is between 300 MHz and 3.0 GHz. Figure 6.3 shows one UHF terminal.

It is the actual most common tool used for communications by rescue teams because it is very easy to use and widely deployed in most of countries. Different rescue organizations can use the same frequency and so can communicate with each another (firemen, police officers). This solution is quite limited because the basic services provided by HF, VHF and UHF communication devices are voice.

Professional Mobile Radio

The Professional Mobile Radio (PMR) is a communication system, which is composed of portable, mobile, base stations and some console radios [79]. The antenna must be mounted in height. The coverage can vary a lot (between 3 and 7 km for point to point, up to 50 km for an extend networks). The PMR system is actually used by a lot of police centers and fire brigades. It is easy to use and to deploy. Many rescue teams are now familiar with these equipments in all the kinds of crises. Some standards have been developed for specific usage and the Trans European Trunked Radio (TETRA) [80] is the most developed. Several manufacturers propose different terminals for the communications, but all these equipments offer interoperability. The user can choose the manufacturer and the product he prefers.

TETRA is an open digital standard defined by the European Telecommunications Standard Institute (ETSI). The purpose of TETRA is to cover the different needs of traditional user organizations such as public safety, transportation, military and government. TETRA is based on a suite of standards that are constantly evolving. It can support the transportation of voice and data in different ways. It is able to operate in direct mode (DMO)

Figure 6.3: UHF Terminal.

by building local radio nets and in standard mode (TMO). TETRA can thus be used as walkie-talkie (DMO) or as cell phones (TMO). Another mode, called “Gateway” allows a TETRA terminal to use a gateway in order to extend the coverage zone.

The different network elements of a typical TETRA architecture makes TETRA fully operational with other infrastructures (PSTN, ISDN and/or PABX, GSM, etc.). TETRA provides excellent voice quality through individual calls (one-to-one) but also through group communication. This technology can be utilized for emergency calls and ensure secure encrypted communications (Figure 4). The Release 2 of TETRA improves the range of the TMO (up to 83 km), introduces new voice codecs and speeds up the transmission of data up to 500 kbps. Thus, the high coverage provided by TETRA, the fast call set-up (less than 1 s), both direct and gateway modes make of TETRA an interesting communication technology. Figure 6.4 shows two TETRA terminals.

6.4.2 Satellite-based solutions

International rescue forces have nowadays started more and more to use satellite communications. After a disaster, even if the terrestrial network is completely out of order, it remains always possible to communicate using the satellite network. Satellite communications are highly survivable, independent of terrestrial infrastructure, able to provide the load sharing and surge capacity solution for larger sites, best for redundancy: they add a layer of path diversity and link availability.

Satellites are the best and most reliable platform for communications in emergency scenarios and perform effectively when:

- Terrestrial infrastructure is damaged, destroyed or overloaded;
- Interconnecting widely distributed networks;

TETRA Hand portable radio

TETRA Mobile radio

Figure 6.4: TETRA Terminals.

- Providing interoperability between disparate systems and networks;
- Providing broadcasting services over very wide area such as a country, region or entire hemisphere;
- Providing connectivity for the “last mile” in cases where fiber networks are simply not available;
- Providing mobile/transportable wideband and narrow-band communications;
- Natural disaster or terrorist attacks occur.

Thus, the benefits of using satellite in emergency communications are:

- *Ubiquitous Coverage:* a group of satellites can cover virtually all of the Earth’s surface;
- *Instant Infrastructure:* satellite services can be offered in area where there is no terrestrial infrastructure and the costs of deploying a fiber or microwave network are prohibitive. It can also support services in areas where exiting infrastructure is outdated, insufficient or damaged.
- *Independent of Terrestrial Infrastructure:* satellite service can provide additional bandwidth to divert traffic from congested areas, provide overflow during peak usage periods, and provide redundancy in the case of terrestrial network outages.
- *Temporary Network Solutions:* for applications such as news gathering, homeland security, or military activities, satellite can often provide the only practical, short-term solution for getting necessary information in and out.
- *Rapid Provisioning of Services:* since satellite solutions can be set up quickly, communications networks and new services can be quickly recovered and reconfigured. In addition, it is possible to expand services electronically without traditional terrestrial networks, achieving a high level of communications rapidly without high budget expenditures.

In times of disaster recovery, solutions provided via satellite are more reliable than communications utilizing land-based connections.

Satellite can provide different connection scenarios and different services as showed in Fig. 6.5 - 6.8 .

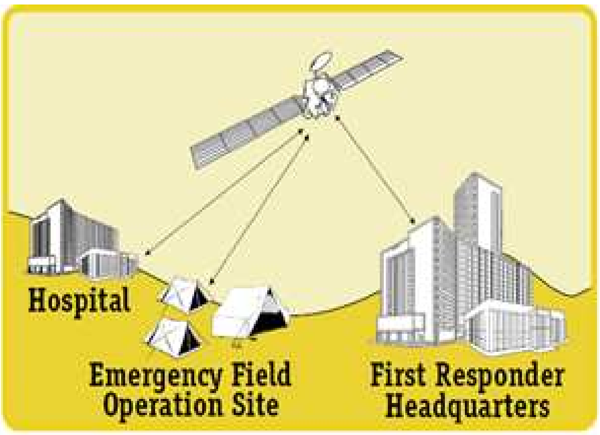

Figure 6.5: Fixed-to-fixed Communications.

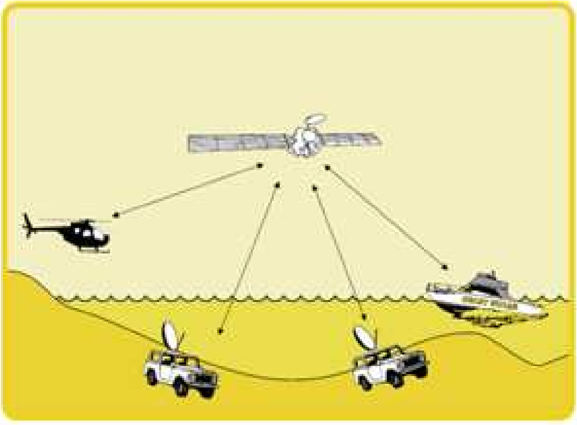

Figure 6.6: Transportable-to-mobile Communications.

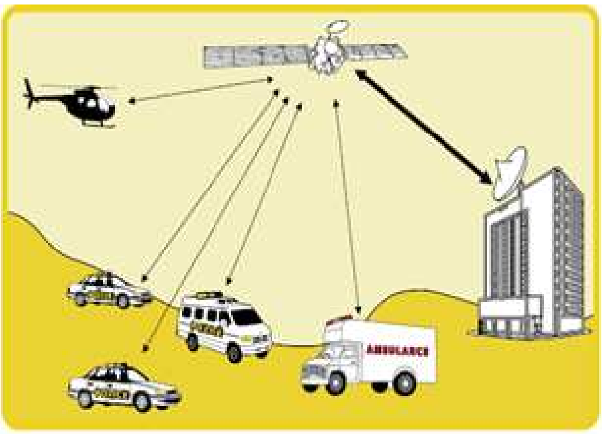

Figure 6.7: Fixed-to-mobile Communications.

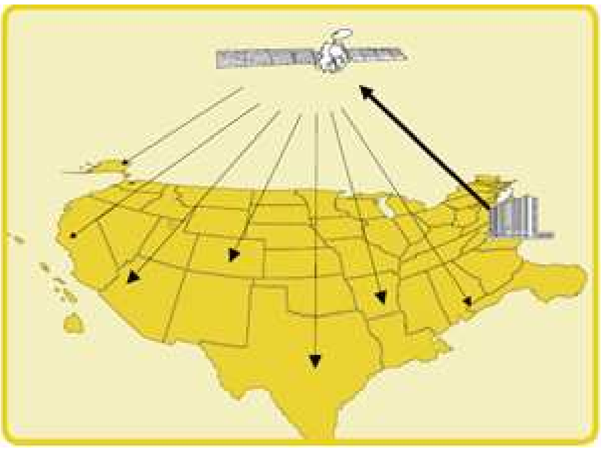

Figure 6.8: Point-to-multipoint Communications.

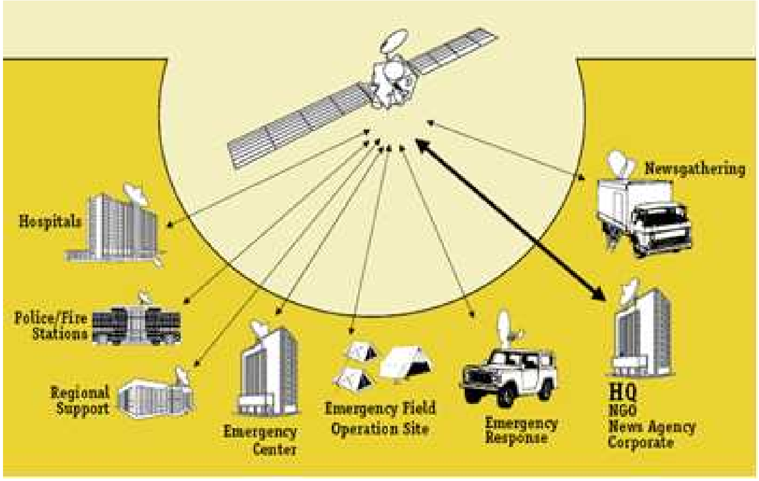

Figure 6.9: Fixed Satellite Services.

Fixed Satellite Services

Fixed Satellite Service (FSS) has traditionally referred to a satellite service that uses terrestrial terminals communicating with satellites in geosynchronous orbit (Fig. 6.9). New technologies allow FSS to communicate with mobile platforms.

Satellite VSAT network: a satellite Very Small Aperture Terminal (VSAT) network consists of a pre-positioned, fixed, or transportable VSAT (Fig. 6.10) that connects to a hub station to provide broadband communications to hospitals, command posts, emergency field operations and other sites. Very small aperture terminal refers to small earth stations, with antennas usually in the 1.2 to 2.4 m range. Small aperture terminals under 0.5 m are referred to Ultra Small Aperture Terminals (USATs). There are also variants of VSATs that are transportable which can be on-the-air within 30 minutes and require no special tools or test equipment for installation. Remote FSS VSAT equipment requires standard AC power for operation, but comes equipped with lightweight, 1 and 2 KW, highly efficient and self-contained power generator equipment for continuous operation, regardless of local power availability.

Internet access and Internet applications (i.e. VoIP) are supported through the remote VSAT back through the FSS provider teleport location which is connected to the PSTN and/or the Internet. A typical VSAT used by a first responder may have full two-way connectivity up to several Mbps for any

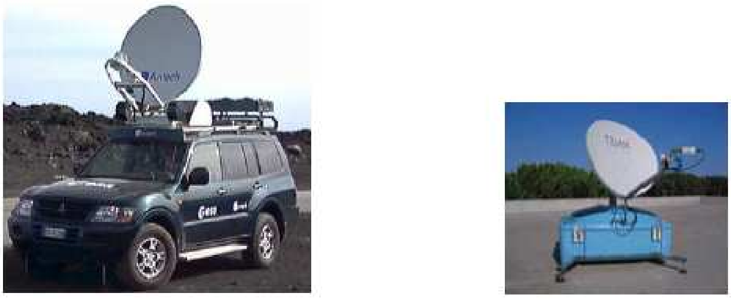

Figure 6.10: ESA Pajero and Temix EasyFlySat terminal.

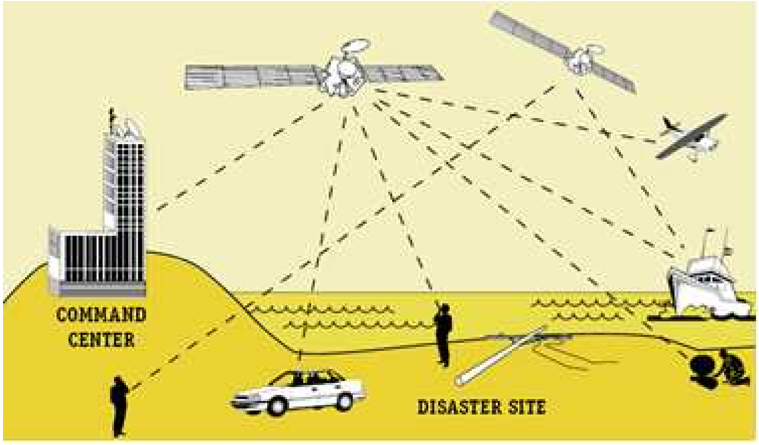

Figure 6.11: Mobile Satellite Services.

desired combination of voice, data, video, and Internet service capability. VSATs are also capable of supporting higher bandwidth requirements of up to 4 Mbps outbound and up to 10 Mbps inbound.

Mobile Satellite Services

Mobile Satellite Service (MSS) uses portable satellite phones and terminals. As shown in Fig. 6.11, MSS terminals may be mounted on a ship, an airplane, truck, or an automobile. MSS terminals may even be carried by an individual. The most promising applications are portable satellite telephones and broadband terminals that enable global service.

Satellite Phones: Several manufacturers offer mobile phones providing different coverage of the earth [81] - [82]. In general, satellite phone is very

Figure 6.12: Satellite Phones.

user friendly; it looks like GSM mobile phone with one telephone number and one mini personal subscriber identity module (SIM)(Fig. 6.12). Satellite phones are water, shock and dust resistant for rugged environment and offer voice and data services with additional capabilities as call forwarding, two-way SMS, one touch dialling, headset/hands-free capability.

The major advantage of this solution is the possibility to phone anywhere, any time, using a satellite link and then the normal public terrestrial phone network.

BGAN System: Broadband Global Area Network (BGAN) from Inmarsat [83] operates in L-band and offers a number of innovative services (3G like) in the arena of mobile multimedia, video and audio multicasting and advanced broadcasting, with three land portable terminal types. Target users are professional mobile users (on-ground, maritime, aeronautical) in any service area worldwide, except Polar Regions. The service is IP-based and allows data transfer speeds up to 492 kbps, streaming up to 256 kbps. The high levels of portability of BGAN terminals (Fig. 6.13), as well as the easiness of use, make BGAN attractive for emergency services. It is also the first mobile communications service to offer guaranteed data rates on demand.

This way, it is relatively easy to plug a laptop on this equipment and to have an Internet access. It is so possible to use IP facilities like Visio conference or other real time applications, with a correct quality thanks to the guaranteed data rate. Currently the solution yet is not very exploited but tends to be developed. Its major advantage is the quasi-total cover of planet thus same that the polar zones and oceans.

Figure 6.13: BGAN Terminal.

Communications On The Move Solution

Communications On The Move (COTM) is the most promising solution for emergency communications. FSS and MSS COTM solutions can provide fully mobile IP data and voice services to vehicles on the move up to 100 km/h (Fig. 6.14). The comprehensive FSS COTM offering includes the terminal, teleport, and satellite capacity to provide high performance COTM IP connectivity.

Typical applications supported:

- Any vehicle can also serve as a mobile command post while in-route and as a fixed command access point for personnel upon arrival at the designated location when local Telco terrestrial and wireless infrastructures are not available.

- A full 10 Mbps downlink channel is delivered via FSS to the vehicle and 512 Kbps uplink channel transmitted from the vehicle to the Internet using IP support for voice, video and data simultaneously.

- Support for 802.11x wireless access allows vehicle to function as wireless hot spot access point for a First Responder convoy while in-route or a fixed hot spot for personnel upon arrival.

6.4.3 Hybrid satellite/terrestrial solutions

Two European projects, TRACKS and Emergesat, have developed hybrid satellite-terrestrial solutions for emergency communications, but both solutions cannot be hand-carried to the disaster site and require either a van or a helicopter respectively.

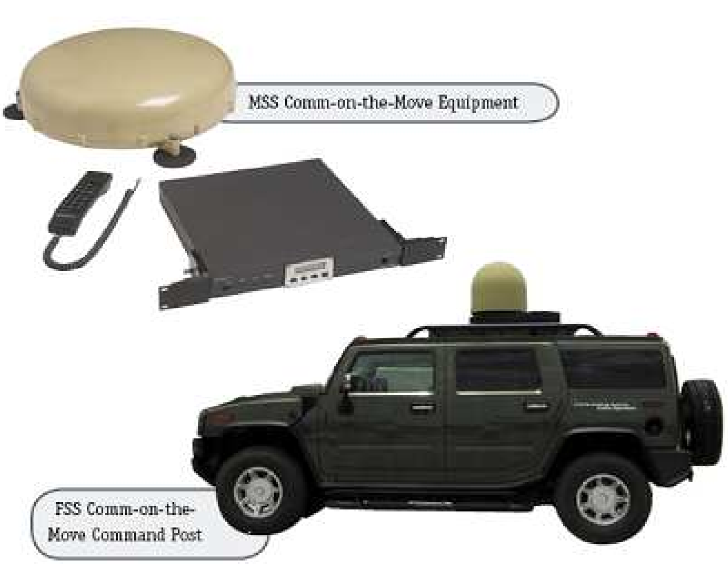
MSS Comm-on-the-Move Equipment
FSS Comm-on-the-Move Command Post

Figure 6.14: COTM Equipments.

TRACKS

In the frame of the ESA-Industry Telecommunications Partnership Program, the project ARTES 4 "TRACKS" [84] deals with the development of the prototype of a van transportable communication station (VSAT terminal, GSM Micro Switch, BSC and BTS, internet access) dedicated to support pre-operational applications (Fig. 6.15). It represents a good candidate telecom solution in case of crisis, when terrestrial communication are damaged or destroyed after a disaster.

TRACKS is first of all a van, which can be driven with a normal driving license. The principal characteristics of the system are the following:

- Quick move on site;
- Link with Internet Network;
- Link with the Public Switched Telephone Network;
- Provide GSM services and Internet access Services.

TRACKS is deployed on the disaster area by local rescue teams. A local command centre can be deployed using the services provided by the van. Thanks to the satellite link, the teams are directly connected to a global command centre, which collect all the information (weather forecast, satellite images) and coordinate the local actions.

TRACKS is composed of several equipments:

- Power generating unit: the van can be autonomous during a period of one or two days. An external 220 VAC power supply can be used too;
- VSAT Terminal;
- On the roof of the VAN, a 1.2 m antenna is used for communications with satellite. Several air interface access schemes have been tested and used in Ku-band, including the SCPC and DVB-RCS. An automatic pointing permits to deploy quickly the antenna;
- a telescopic mast (12 m);
- GSM Equipments (coverage : 1 km);
- Wi-Fi Equipments.

Thanks to the Wi-Fi Equipments, the rescue team on site can use the network developed by TRACKS with the office tools: PC, PDA and laptop. The services are not limited. Some applications like videoconference, telemedicine, cartography can be used thanks the internet access provided by the van.

Different configurations with these equipments have been tested in demonstration or crisis simulation. Compared with handheld solutions or easily portable solution like BGAN, TRACKS has limits inherent to this type of transportable solutions: when the roads are damaged, the van cannot reach immediately the site. A second point is the need to train rescue teams or some specialized people to use this material. Improvements are necessary to make it user-friendlier to be used as "GSM-like" solutions.

EMERGESAT

Emergesat [85] is a system developed by Thales Alenia Space as an initiative funded by the French government in response to needs of responding to humanitarian crises. Flown in locally to a disaster site, Emergesat provides all emergency aid teams, irrespective of nationality, with global information on the crisis situation and assistance with coordination of aid work, and other decision-making aid services. The Emergesat humanitarian aid tool applies the space-based technologies of telecommunications, earth observation and

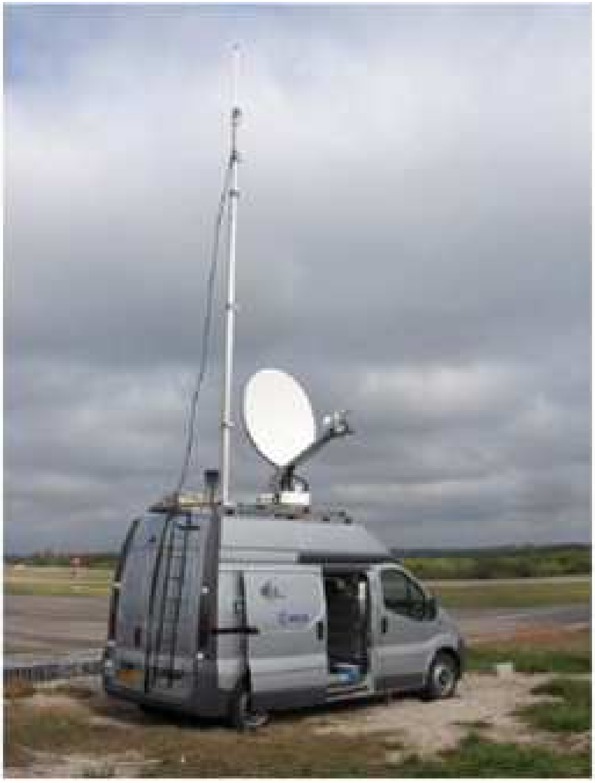

Figure 6.15: TRACKS.

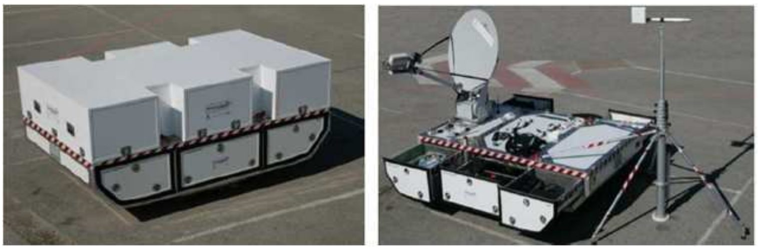

Figure 6.16: Emergesat container before and after installation.

location/navigation satellites. Emergesat is a federating tool, proposed by France and open to partnerships and cooperation arrangements, designed to be at the service of all worldwide.

Emergesat is basically a container as shown in Fig. 6.16, especially designed in its dimensions, weight and the composite materials used in its construction, for transport in the luggage hold of any passenger line aircraft. It has rings for slinging under a helicopter, and is seal-tight under the most extreme weather conditions and totally autonomous in terms of power supply. The basic container incorporates its own communication equipment, and can also be used to transport a complete, autonomous water purification plant or small medical centre.

The container has the following characteristics:

- transportable, adaptable and easy to use;
- rapidly deployable and operational as soon as the relief teams arrive;
- easy to bring in by line aircraft, helicopter and truck, ship, etc.;
- configurable according to the nature of the disaster;
- simple to use, user friendly and multi-lingual;
- all-weather, strong, lightweight, air-conditioned and autonomous;
- weight: 400 kg;
- dimensions: 2 m x 1.5 m x 1.6 m ;
- volume: 4,8 m;

The core of the Emergesat communication system is a satellite transceiver unit, providing for high-rate communication from any point on the globe.

Its automatic dish antenna ensures that the system can be placed in service immediately. A GSM transmission BTS connected to the satellite system makes it possible to set up a complete GSM network. A long-range Wi-Fi network system provides for connection with a large action perimeter. A remote server collects all information required by the rear support bases. A software suite enables the operational teams to keep themselves fully informed about the evolution of the crisis, treatment of victims, civil engineering problems, etc. in real time. This system is fully open to all users. The teams in the field can hook up using a conventional tool (PC, PDA, etc.), and obtain information and decision-making aid services, including cartography, meteorology, languages and dialects, and also access collaborative working tools such as videoconference, messaging, application sharing.

6.5 System Architecture for Emergency Mobile Communications

Emergency situations require reliable communication broadband systems able to transmit relevant information from the disaster site to the decision makers and to send feedback from first responders regarding potential dangers or decision. Key factor in designing a robust communication system with applications to emergency response is the development of a quickly, easily deployable and mobile infrastructure providing voice and data communications, available within the first 24 hours.

Taking into account all above mentioned functional and performance requirements, the fact that no existing terrestrial and/or satellite system for emergency communications is able to cover all those requirements at the same time and that satellite networks are the best and more reliable platform for communications in emergency scenarios for providing a backhaul connection to the intact network infrastructure, we propose a new advanced hybrid satellite and terrestrial system architecture.

It provides, at once, full mobility in the disaster site to rescue teams and broadband connectivity inside the disaster network and with headquarters. The proposed architecture is quickly deployable and dynamically adaptable to disaster of any nature and location. It is IPv6-based and able to support IP interoperability with terminals belonging to different administrators and technologies. As, generally, the deployment of Public Safety units makes use of two entities, vehicles and Public Safety users equipped with satellite and radio terminals, we have decided to implement them in the proposed hybrid satellite and terrestrial system architecture. It allows Public Safety units

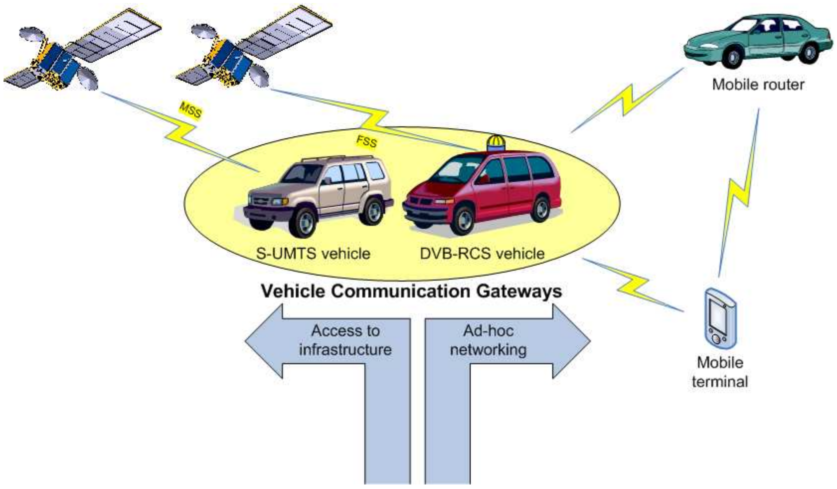

Figure 6.17: Vehicle Communication Gateways.

to move on the crisis site and to communicate urgent information among devices in the field and from devices to Internet and headquarters.

This is achieved by having a mobile ad-hoc mesh network at the disaster site, an infrastructure which enables any entity to easily reach the headquarters. The most important and central role of the presented system architecture is played by Vehicle Communication Gateways (VCGs). They have double functionalities as shown in Fig. 6.17. On one side, VCGs provide vehicle-to-infrastructure (V2I) communications maintaining Internet connectivity with the disaster site through satellite links: S-UMTS vehicles operating in S/L band and DVB-RCS vehicles operating in Ku/Ka band. On the other side, VCGs are able to establish vehicle-to-vehicle (V2V) communications, giving connectivity to mobile terminals through the mobile ad-hoc mesh network.

6.5.1 System Architecture Overview

Disasters are unplanned and unexpected, and they involve loss of lives and infrastructures. The impacted community might receive several days' notice or not all; the disaster may affect a locality or could spread or cascade to affect larger areas. Thus, it is important to design a system architecture that could easily adapt to all different scenarios' configurations and to properly manage the network deployment phases that follow a hazard.

Figure 6.18 presents a general overview of the proposed system architecture for emergency mobile communications [86]. It consists of:

- A space segment which includes two GEO satellites, one MSS and one FSS;
- A terrestrial infrastructure segment which includes two Earth stations connected through the Internet to the headquarters (or operation centers in case of international support), providing the link between the satellite system and satellite terminal segment deployed in the disaster site;
- A terminal segment which includes:
  - A satellite terminal segment composed of:
    - User terminals such as satellite phones that provide direct satellite access to end-users;
    - VCGs that provide satellite access to terrestrial user terminals and mobile routers;
  - A terrestrial terminal segment that includes:
    - End-user terminals such as handhelds, PDAs, PCs;
    - Vehicular terminals that provide access to the terrestrial end-user terminals and are enabled with routing capabilities, they form a mobile ad-hoc mesh network over the crisis area.

Figure 6.19 describes the proposed hybrid satellite and terrestrial system architecture, which has a high level of robustness and fault tolerance together with high reliability and quick deployment. HIP-PMIPv6 scheme is applied to the system architecture.

VCGs and mobile routers, the mesh entities composing the mobile ad-hoc mesh network, can assume LMAs and MAGs functionalities in order to create a PMIPv6 domain, used as an infrastructure at the crisis area, to which IPv6 unmodified mobile terminals coming from different rescue teams can have access and be easily managed. In this way, seamless connectivity can be guaranteed for broadband communications inside the disaster area and with the headquarters via satellite links [87].

The combination of PMIPv6 and HIP protocols helps rescue teams to easily move and keep their connections on while moving under different mobile routers and switching from one access technology to another. Each MN in the ad hoc mesh network has an identifier, used for establishing security connections with peers. Diffie-Hellman scheme for secret key exchange

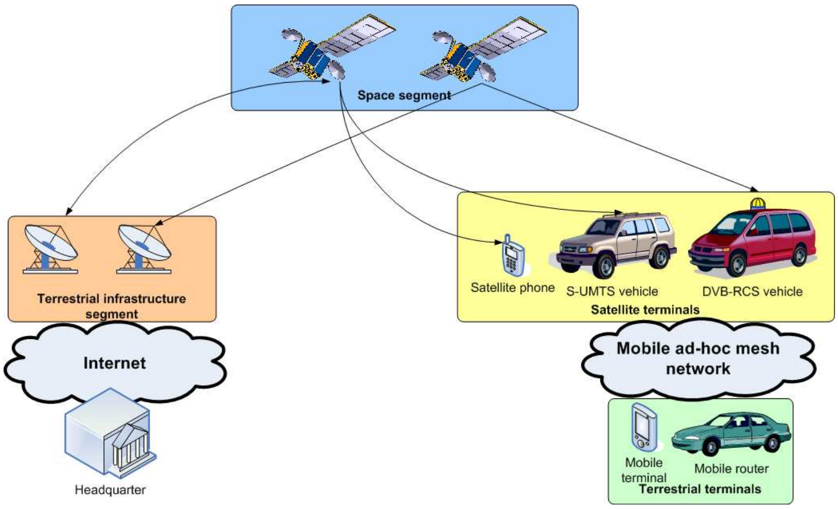

Figure 6.18: General Overview of the System Architecture.

together with IPSec is used for creating the SA between MNs, as in HIP scheme. Once the SA is established, modifications to the IP address of the MN due to the mobility do not break the connection, as the SA is linked to the identifiers. In order to avoid unnecessary signaling for updating the peer about the new locator as in HIP standard, we apply a micro-mobility solution based on PMIPv6 [88].

Each MN obtains an IP address from the network that is routable outside the ad hoc mesh network and remains unchanged even when the MN moves behind different mesh routers inside the domain. Thanks to micro-mobility management, the network is able to route correctly the traffic to the right MN proving seamless handover features. As the IP address does not change, no update messages are needed. In the case the MN is equipped with multiple interfaces and wants to switch from one access technology to another, e.g. in order to use a more reliable connection, it can notify the network with its intention and the traffic will be routed directly to the new interface. For communications between rescue teams located at the disaster area and decision makers at the headquarters, this mechanism is really useful as it helps to save resources and satellite bandwidth. Moreover, it reduces the delay and allows rescue teams to benefit of an Always Best Connected vision, proving robustness and reliability to the system. The mechanism is also independent from the access technology, so interoperability of communication devices within and across different agencies and jurisdictions is

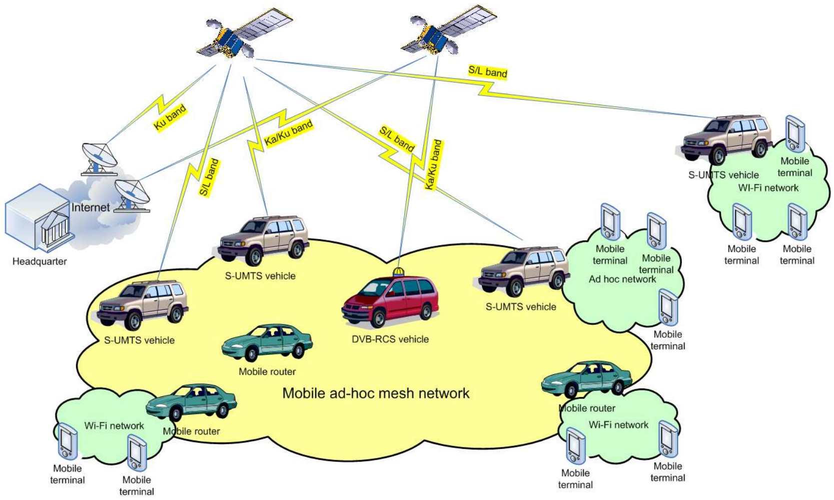

Figure 6.19: Hybrid Satellite and Terrestrial System Architecture.

possible [89].

As regards the satellite network [90], S-UMTS vehicles provide a mobile communications solutions through S/L band between the mobile ad-hoc mesh network at the disaster field and the Internet backbone where the fixed decision center and headquarters are situated. Transportable terminals, like DVB-RCS vehicles, working on-the-pause or at very low speed, provide the benefit of high throughput and efficient bandwidth utilization. Finally, S-UMTS vehicles can be used to give external connectivity to groups not reached by the mobile ad-hoc mesh network.

6.5.2 S-UMTS Vehicles

The use of narrowband, such as L or S band, has encountered such a success in emergency mobile communications that it cannot be ignored in a disaster system scenario definition as it permits mobility and low cost antennas and terminals. Narrow band allows developing mobile terminals which serve as interface between the satellite and any type of terrestrial network access point (e.g. UMTS, Wi-Fi, 2G).

Considering the limited bit rate that can be reached at those frequencies, the leading idea is to dynamically create a distributed gateway between S-UMTS vehicles that are in LOS for the external communications, so the effective bit rate can be higher depending on the number of vehicles used.

As regards the type of L or S band vehicular antenna installed on it,

Category	Parameters	Active Antenna	Ominidirectional Antenna
RF Section Characteristics	Frequency Band	2.1-2.2 GHz	
	Antenna Diameter	0.16 m	0.09 m
	Rx G/T	- 16 dB/K	- 21 dB/K
	Tx EIRP	18.5 dBW	10.5 dBW
	Total Bandwidth	Tx: 5 MHz Rx: 5 MHz	
Downlink	Proposed Air Interface	DVB-S2	
	Modulation and Coding	QPSK 1/2	
	Waveform	TDM	
	Max Data Rate	4 Mbit/s	
Uplink	Proposed Air Interface	S-UMTS	
	Modulation and Coding	QPSK 1/3	
	Waveform	CDMA	
	Spreading Factor	32	64
	Max Data Rate per User	80 Kbit/s	40 Kbit/s

Table 6.1: Specifications of S-UMTS Vehicle

two candidate solutions are presented in this work: active antenna and omnidirectional antenna. Terminal mobility is around 50 Km/h. Technical specifications for the S-band link, described in Table 6.1, have been chosen as baseline to characterize S-UMTS vehicles.

Based on the technical specifications outlined before, an analysis and assessment of system performance in S band has been carried out. The proposed S-UMTS specifications shall be considered as a study case to show capabilities and performance of the system design. The DVB-S2 standard [91] has been assumed as baseline for the Forward link, while the S-UMTS has been assumed for the Return link. A ground station antenna diameter of 8 m, channelization of 5 MHz and satellite effective EIRP/beam of 68 dBW have been taken into account.

Moreover, the following assumptions have been considered:

- C/(N+I) uplink in Forward Link is at least 20 dB.
- C/(N+I) downlink in Return Link is at least 20 dB.

End-to-end link budget results for S-UMTS vehicle in S band are summarized in Table 6.2 and Table 6.3.

Category	Parameters	Active Antenna	Ominidirectional Antenna
Up-link Result	C/(N+I)	20 dB	
Satellite Transmission Characteristics	Transmission Frequency	2.2 GHz	
	Effective EIRP/beam	68 dBW	
Satellite to S-UMTS Vehicle Propagation	Total Attenuation	191.2 dB	
S-UMTS vehicle	G/T	- 16 dB/K	- 21 dB/K
Down-link Results	C/N	22.5 dB	17.5 dB
	C/I	94 dB	
	C/(N+I)	22.5 dB	17.5 dB
Forward Link Results	Total C/(N+I)	18.5 dB	16 dB
TDM	Required C/N at Physical Layer at BER 10^5 in AWGN	1 dB	
	Implementation Losses	0.5 dB	
LOS Margin at Physical Layer wrt AWGN		17 dB	14.5 dB

Table 6.2: Forward Link in S band

Category	Parameters	Active Antenna	Ominidirectional Antenna
S-UMTS Vehicle Transmission Characteristics	Transmission Frequency	2.1 GHz	
	Effective EIRP/beam	18.5 dBW	10.5 dBW
S-UMTS Vehicle to Satellite Propagation	Total Attenuation	190.4 dB	
Satellite	G/T	12 dB/K	12 dB/K
Up-link Results	C/N	3 dB	-5 dB
	C/I	12 dB	
	C/(N+I)	2.5 dB	-5.1 dB
Down Link Results	C/(N+I)	20 dB	
Return Link Results	Total C/(N+I)	2.4 dB	-5.1 dB
CDMA	Required C/(N+I) at Physical Layer at BER 10^5 in AWGN	-12.1 dB	-15.1 dB
	Implementation Losses	0.5 dB	
LOS Margin at Physical Layer wrt AWGN		13.9 dB	9.4 dB

Table 6.3: Return Link in S band

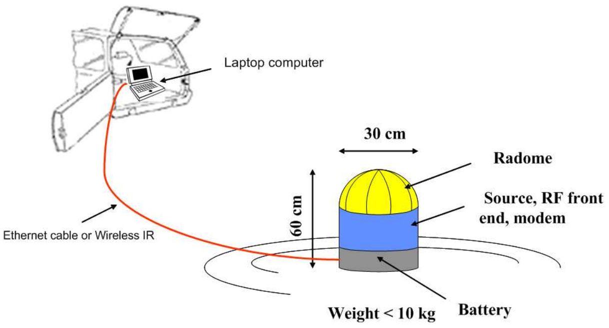

Figure 6.20: Nomadic Terminal in Ka band.

The analysis on the link budgets shows that S-UMTS vehicles with active antenna can reach data rate up to 4 Mbit/s in the Forward Link, and up to 80 Kbit/s in the Return Link. Thanks to CDMA and Spread Aloha access method in the return link, the data rate can reach 800 Kbit/s if at least 10 vehicles are in LOS, transmitting simultaneously as a distributed gateway.

6.5.3 DVB-RCS Vehicles

S or L band provides services as voice and data for emergency communications, but only broadband, as Ku or Ka band, can offer large capacity and high date rate necessary to exchange multimedia data such as medical data, digital map or intelligence data. This frequency band has several advantages. Transportable terminals can benefit of broadband communications, efficient bandwidth utilization and cheap capacity. The terminal mobility spans from fixed to a target speed of 10 Km/h. The available bandwidth is very large and not much occupied and it is possible to use small antennas for terminals as the Ultra-Small Aperture Terminal (USAT) [92] - [93] as illustrated in Fig. 6.20.

Technical specifications for the Ka band link of DVB-RCS vehicle are provided in Table 6.4.

Once again, the proposed DVB-RCS specifications shall be considered as a study case to show capabilities and performance of the system design. The Digital Video Broadcasting via satellite version 2 (DVB-S2) standard has been assumed as baseline for the Forward link, while the DVB-RCS standard [94] has been assumed for the Return link. The idea is to use, in the future, DVB-RCS mobile for the Return Link. Based on the same feeder link assumptions of S-UMTS vehicle, end-to-end link budget calculations have been done for the DVB-RCS vehicle in Ka band. Results are summarized

Category	Parameters	Rain Conditions	Clear sky Conditions
RF Section Characteristics	Frequency Band	20.2 - 30 GHz	
	Antenna Diameter	0.3 m	
	Rx G/T	8 dB/K	
	Tx EIRP	38 dBW	
	Total Bandwidth	Tx: 56 MHz Rx: 56 MHz	
Downlink	Proposed Air Interface	DVB-S2	
	Modulation and Coding	QPSK 1/4	QPSK 1/2
	Waveform	BH-TDM	
	Max Data Rate	8 Mbit/s	25 Mbit/s
Uplink	Proposed Air Interface	DVB-RCS	
	Modulation and Coding	QPSK 1/2	
	Waveform	MF-SDMA	
	Max Data Rate per User	128 Kbit/s	512 Kbit/s

Table 6.4: Specifications of DVB-RCS Vehicle

in Table 6.5 and Table 6.6.

As shown in Table 6.5 and Table 6.6, with a diameter of 30 cm and a satellite EIRP of 58 dBW, the presented DVB-RCS vehicle can receive, on the satellite downlink, data rates up to 25 Mbit/sec in temperate and desert zones and a data rate of 8 Mbit/sec in tropical zone. With a satellite G/T of 19 dB/K thanks to the Space Division Multiple Access (SDMA), it can provide uplink with a data rate up to 512 Kbit/sec in temperate and desert zones and a data rate of 128 Kbit/sec in tropical zone.

6.6 Conclusions

Disasters are often combined with the destruction of the local telecommunication infrastructure, causing severe problems to the rescue operations. In this cases the only possible way to guarantee communications services, is to use satellite to provide a backhaul connection to the decision center. A new system architecture, which is HIP-PMIPv6 based and which can integrate hybrid satellite and wireless terrestrial networks to provide mobile emergency communications, has been presented. The key objectives of the targeted heterogeneous infrastructure are the full mobility of rescue teams and the covering of bi-directional communication needs for voice and data

Category	Parameters	Rain Conditions	Clear sky Conditions
Up-link Result	C/(N+I)	20 dB	
Satellite Transmission Characteristics	Transmission Frequency	20.2 GHz	
	EIRP on Overall Bandwidth	58 dBW	
Satellite to DVB-RCS Vehicle Propagation	Total Attenuation	218.6 dB	213.6 dB
DVB-RCS Vehicle	G/T	7 dB/K	8 dB/K
Down-link Results	C/N	0.15 dB	5.8 dB
	C/I	23.8 dB	
	C/(N+I)	0.13 dB dB	5.8 dB
Forward Link Results	Total C/(N+I)	0.1 dB	5.7 dB
TDM	Required C/N at Physical Layer at BER 10^5 in AWGN	-2.35 dB	1 dB
	Implementation Losses	0.5 dB	
LOS Margin at Physical Layer wrt AWGN		1.95 dB	4.2 dB

Table 6.5: Forward Link in Ka band

Category	Parameters	Rain Conditions	Clear sky Conditions
DVB-RCS Vehicle Transmission Characteristics	Transmission Frequency	30 GHz	
	EIRP per Carrier	38 dBW	
DVB-RCS Vehicle to Satellite Propagation	Total Attenuation	225.5 dB	214.5 dB
Satellite	G/T	19 dB/K	
Up-link Results	C/N	9 dB	14 dB
	C/I	20 dB	
	C/(N+I)	8.6 dB	13 dB
Down Link Results	C/(N+I)	20 dB	
Return Link Results	Total C/(N+I)	8.3 dB	12.2 dB
SDMA	Required C/(N+I) at Physical Layer at BER 10^5 in AWGN	5.7 dB	5.7 dB
	Implementation Losses	0.5 dB	
LOS Margin at Physical Layer wrt AWGN		2.1 dB	6 dB

Table 6.6: Return Link in Ka band

in the first critical hours following an emergency. Two types of VCGs have been envisaged as mobile and transportable backhaul to headquarter via satellite, S-UMTS vehicles operating in S or L band and DVB-RCS vehicles operating in Ku or Ka band.

Results presented in this chapter show that a combined solution composed of S-UMTS vehicles and DVB-RCS vehicles permits to create a universal scenario suitable for all emergency mobile communications. S-UMTS vehicles allow higher mobility in the disaster site so they can be used to extend the coverage of DVB-RCS vehicles in more critical area and to exchange critical data with headquarter taking advantages of a more robust link. On the other side, DVB-RCS vehicles, working on-the-pause or at very low speed, offer high throughput, important aspect as it allows receiving and sending multimedia data to headquarter.

Finally, the proposed system architecture provide an infrastructure in which Public Safety users can use the different technologies of their multihomed devices and be free to move IP sessions from one interface to another one without breaking the already established secure associations, being connected to the always best network available at the disaster site.

Chapter 7

Conclusion

The main subject of this thesis is "mobility" and the design of architecture and techniques that can help render this paramount aspect of networking practically applicable to future Internet. The increasing complexity being perceived in next generation mobile networks, with multi-mode terminals always best connected, with multiple types of network available, both operators and community supported, has brought mobility issues into a central role for the future networks and Internet. The other trend we have observed is that users are becoming more and more detached from their physical devices. While it is true in IP networks today that a user is comprehended by the network as the device it owns, the pervasive component in current research tells a different story. People will not only own multiple devices, from PDAs to laptops, but also interact with public devices which enhance the user's experience depending on hic context and preferences. These devices can be accessed by anyone at anytime, which means that mobility is associated to the person's perceived identity and not to the individual devices he interplays with. The present thesis has attempted to address these problematics.

In this thesis we have presented a new paradigm for future Internet and future mobile operators. The proposed architecture has recognized the current trend in networks to a heterogeneous landscape of access providers. In this environment it is important to give the access providers the flexibility of managing the mobility inside their domains according to their needs, technologies and requirements, without being conditioned by how the mobility is managed in other domains. To cope with this concept, the architecture proposed in this thesis has splitted the mobility management into two levels: the local mobility according to PMIPv6 scheme, thus a network-based local mobility management, and the global mobility according to HIP scheme, thus a host-based global mobility management. As a conseguence, the management of the mobility in these two levels has been kept completely independent. Efficient mobility management mechanism has not been the only advantage of the proposed mobility architecture. The key design elements have been the reliance on cryptographic host identifiers used as virtual interfaces for multihomed mobile hosts and on group identifiers used for identifying mobile nodes belonging to the same ad-hoc network, the specific locators created through Home Network Prefixes for providing location privacy, reduced handover latency and signaling overhead, and the end-to-end security based on HIP. As a consequence, with the combination of PMIPv6 and HIP, the architecture is able to support mobility, multihoming, heterogeneous networking, seamless handover, security, efficient routing and addressing scheme, location privacy and ad-hoc networking.

This dissertation has also considered the practical constrains future mobile operators will face once implementing the proposed architecture. In particular all the aspects related to the implementation of PMIPv6 in a real test-bed, as directives on HIP have been already extensively covered. We have completed an entirely empirical study based on real experiments of PMIPv6. To the best of our knowledge, our work is the first to provide an implementation perspective on the standard PMIPv6 under different implementation configurations. The per-MN-prefix allocation scheme and unicast RAs have been implemented, as well as the BCE at LMA and the dynamic bidirectional tunnel between MAG and LMA. Moreover, the important feature of allocating the same link-local address to all MAGs has been respected. The experimental results show that the latest aspect cannot be omitted in the implementation, while the fact of implementing a dynamic or permanent tunnel between MAG and LMA can be freely decided as it does not impact the handover performances. We have also released our PMIPv6 implementation as open source in Eurecom's website. It does not require any modification in the IPv6 standard kernel.

Finally, we have proposed our HIP-PMIPv6 scheme for Public Safety Networks in a system architecture composed of satellite and ad-hoc mesh networks. Rescue teams at the disaster site can take advantage of the global and local mobility management scheme for seamlessly moving inside the crisis area without breaking their connections with other rescue teams through the ad-hoc mesh network and with their headquarters through the satellite network. The proposed system architecture is easy to deploy as it makes use of transportable satellite antennas that can be mounted on vehicles and of gateways and routers enhanced with LMA and MAG functionalities. Rescue teams can keep using their standard equipments as PMIPv6 does not require any modifications in their kernel, while a simple update at user-space is necessary to install the HIP daemon to benefit of extremely secure communications. The system architecture gives also the opportunity to the mobile teams to switch from one access technology to another, e.g. in order to use a more reliable connection, notifying the network of their intention so that the traffic is routed directly to the new interface. For communications between rescue teams located at the disaster area and decision makers at the headquarters, this mechanism is really useful as it helps to save resources and satellite bandwidth. Moreover, it reduces the delay and allows rescue teams to benefit of an Always Best Connected vision, proving robustness and reliability to the system. The mechanism is also independent from the access technology, so interoperability of communication devices within and across different agencies and jurisdictions is possible.

Future Perspectives

The present dissertation has proposed architecture and techniques to support mobility in the future Internet. They represent a step forward giving some directions for future mobility support and incentivating the use of separated identifiers and locators.

However, there are still some aspects related to the aforementioned mechanisms that have not been addressed in this thesis. The next steps for this work would be considering scalability and multicasting features for the proposed architecture. A mechanism that could allow communication between LMAs and between MAGs should be considered to cover these important aspects. It could be also useful for the extension of the architecture to mesh networks. This study has been partially covered in our journal paper, but it needs further investigation and needs to be included in a efficient way into the mobility architecture.

On the implementation point of view, the intra-technology handover has been fully implemented and tested, while the inter-technology handover, as well as the multihoming, are still on a implementation phase. An important added value would be the integration of our HIP-PMIPv6 implementation with the IEEE 802.21 MIH protocol. It will provide a mechanism to support multi-interfaced MNs giving information to the MAGs on the status of the different links. The MIH primitives can be used to help the MAGs to deal with multi-technology scenarios, improving traffic and flow management for multihomed mobile nodes.

Appendix A

Publications

List of publications during the Ph.D.

1. Giuliana Iapichino, Daniel Câmara, Christian Bonnet, and Fethi Filali, "Public Safety Networks", Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, IGI Global, accepted for publication, to appear in 2010.

2. Huu Nghia Nguyen, Christian Bonnet, and Giuliana Iapichino, "Extended Proxy Mobile IPv6 for Scalability and Route Optimization in Heterogeneous Wireless Mesh Networks", International Journal of Ubiquitous Computing (IJUC), Serial Publications, accepted for publication, to appear in 2010.

3. Giuliana Iapichino, and Christian Bonnet, "Experimental Evaluation of Proxy Mobile IPv6: an Implementation Perspective", Proc. of IEEE Wireless Communications & Networking Conference (WCNC) 2010, Sydney, Australia, April 2010.

4. Giuliana Iapichino, Christian Bonnet, Oscar Del Rio, Cédric Baudoin, and Isabelle Buret, "Ad-hoc Mobility in Satellite-based Networks for Public Safety Applications", Proc. of 1st Networking/Partnering Day 2010, European Space Agency/ESTEC Conference, Noordwijk, The Netherlands, January 2010.

5. Giuliana Iapichino, and Christian Bonnet, "Host Identity Protocol and Proxy Mobile IPv6: a Secure Global and Localized Mobility Management Scheme for Multihomed Mobile Nodes", Proc. of IEEE Global Communications Conference (GLOBECOM 2009), Honolulu, USA, December 2009.

6. Giuliana Iapichino, Christian Bonnet, Oscar Del Rio, Cédric Baudoin, and Isabelle Buret, "Combining Mobility and Heterogeneous Networking for Emergency Management: a PMIPv6 and HIP-based Approach", Proc. of International Workshop on Advanced Topics in Mobile Computing for Emergency Management: Communication and Computing Platforms, in conjunction with ACM IWCMC 2009, Leipzig, Germany, June 2009.

7. Giuliana Iapichino, Christian Bonnet, Oscar Del Rio, Cédric Baudoin, and Isabelle Buret, "Mobility, Access Heterogeneity and Security for Next Generation Public Safety Communications", Proc. of Workshop on Next Generation Public Safety Communication Networks and Technologies, in conjunction with IEEE ICC 2009, Dresden, Germany, June 2009.

8. Giuliana Iapichino, Christian Bonnet, Oscar Del Rio, Cédric Baudoin, and Isabelle Buret, "A Mobile Ad-hoc Satellite and Wireless Mesh Networking Approach for Public Safety Communications", Proc. of 10th IEEE International Workshop on Signal Processing for Space Communications (SPSC 2008), Rhodes, Greece, October 2008.

9. Giuliana Iapichino, Christian Bonnet, Oscar Del Rio, Cédric Baudoin, and Isabelle Buret, "Advanced Hybrid Satellite and Terrestrial System Architecture for Emergency Mobile Communications", Proc. of 26th AIAA International Communications Satellite Systems Conference (ICSSC 2008), San Diego, USA, June 2008.

10. Giuliana Iapichino, and Oscar Del Rio, "QoS Provisioning for Multimedia Services on all-IP Based Hybrid Networks", Proc. of 26th AIAA International Communications Satellite Systems Conference (ICSSC 2008), San Diego, USA, June 2008.

11. Giuliana Iapichino, and Christian Bonnet, "Ad hoc network connection continuity for security applications report", Eurecom, Rapport de Recherche, RR-09-237, Sophia Antipolis, France, November 2009.

12. Giuliana Iapichino, and Christian Bonnet, "Combination of ad hoc mobility with IPv6 mobility mechanisms report", Eurecom, Rapport de Recherche, RR-09-225, Sophia Antipolis, France, January 2009.

13. Giuliana Iapichino, and Christian Bonnet, "IPv6 mobility and ad hoc network mobility overview report", Eurecom, Rapport de Recherche, RR-08-217, Sophia Antipolis, France, March 2008.

14. Giuliana Iapichino, and Christian Bonnet, “Security scenario definition report”, Eurecom, Rapport de Recherche, RR-08-216, Sophia Antipolis, France, March 2008.

Bibliography

[1] D. Clark, "The design philosophy of the darpa internet protocols," in *ACM SIGCOMM*, Stanford, California, United States, 1988, pp. 106 – 114.

[2] D. Clark, L. Chapin, V. Cerf, R. Braden, and R. Hobby, "Towards the future internet architecture," *IETF Informational RFC 1287*, December 1991.

[3] ESA Networking/Partnering Initiative Home Page, http://www.esa.int/esaMI/Technology/SEM4KVWPXPF0.html.

[4] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host identity protocol," *IETF RFC 5201*, April 2008.

[5] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy mobile ipv6," *IETF RFC 5213*, August 2008.

[6] C. Roberts and J. Kempf, "Mobility architecture for the global internet," in *ACM/IEEE International Workshop on Mobility in the Evolving Internet Architecture*, San Francisco, USA, December 2006, pp. 23–28.

[7] L. Zhang, R. Wakikawa, and Z. Zhu, "Support mobility in the global internet," in *ACM International Conference on Mobile Computing and Networking*, Beijing, China, September 2009, pp. 1–6.

[8] G. Iapichino and C. Bonnet, "Ipv6 mobility and ad hoc network mobility overview report," *Eurecom, Rapport de Recherche, RR-09-217*, March 2008.

[9] 3GPP, "General packet radio service (gprs) service description: Stage 2 v.7.1.0," *3GPP TS 23.060*, June 2006.

[10] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in ipv6," *IETF RFC 3775*, June 2004.

[11] J. Laganier and L. Eggert, "Host identity protocol (hip) rendezvous extension," *IETF RFC 5204*, April 2008.

[12] P. Nikander, T. Henderson, C. Vogt, and J. Arkko, "End-host mobility and multihoming with the host identity protocol," *IETF RFC 5206*, April 2008.

[13] A. Khurri, E. Vorobyeva, and A. Gurtov, "Performance of host identity protocol on lightweight hardware," in *ACM MobiArch 2007*, August 2007.

[14] S. Novaczki, L. Bokor, and S. Imre, "Micromobility support in hip: survey and extension of host identity protocol," in *IEEE MELECON 2006*, May 2006, pp. 651–54.

[15] J. Y. H. So and J. Wang, "Micro-hip: a hip-based micro-mobility solution," in *IEEE ICC Workshop 2008*, May 2008, pp. 430–35.

[16] J. Melen, J. Ylitalo, and P. Salmela, "Security parameter index multiplexed network address translation (spinat)," *IETF Internet Draft draft-melen-spinat-01*, July 2008.

[17] J. Kempf, "Problem statement for network-based localized mobility management (netlmm)," *IETF RFC 4830*, April 2007.

[18] R. Koodli, "Fast handovers for mobile ipv6," *IETF RFC 4068*, July 2005.

[19] H. Soliman, C. Castelluccia, K. El Malki, and L. Bellier, "Hierarchical mobile ipv6 mobility management," *IETF RFC 4140*, August 2005.

[20] G. Giaretta, "Interactions between pmipv6 and mipv6: scenarios and related issues," *IETF Internet Draft draft-ietf-netlmm-mip-interactions-02*, February 2009.

[21] R. Wakikawa, S. Kiriyama, and S. Gundavelli, "The use of virtual interface for inter-technology handoffs and multihoming in proxy mobile ipv6," in *Mobiworld 2008*, September 2008.

[22] V. Devarapalli, N. Kant, H. Lim, and C. Vogt, "Multiple interface support with proxy mobile ipv6," *IETF Internet Draft draft-devarapalli-netext-multi-interface-support-00*, March 2009.

[23] D. Damic, "Proxy mobile ipv6 indication and discovery," *IETF Internet Draft draft-damic-6man-pmip6-ind-00*, March 2009.

[24] D. Premec and T. Savolainen, "Inter-technology handover in pmipv6 domain," *IETF Internet Draft draft-premec-netlmm-intertech-handover-01*, March 2009.

[25] G. Iapichino and C. Bonnet, "Host identity protocol and proxy mobile ipv6: a secure global and localized mobility management scheme for multihomed mobile nodes," in *IEEE Global Communications Conference (GLOBECOM 2009)*, Honolulu, USA, December 2009, pp. 1 – 6.

[26] ——, "Combination of ad hoc mobility with ipv6 mobility mechanisms report," *Eurecom, Rapport de Recherche, RR-09-225*, January 2009.

[27] T. Heer, H. Wirtz, and S. Varjonen, "Service identifiers for hip," *IETF Internet Draft draft-heer-hip-service-00*, February 2009.

[28] M. Liebsch and L. Le, "Inter-technology handover for proxy mipv6," *IETF Internet Draft draft-liebsch-netlmm-intertech-proxymip6ho*, February 2009.

[29] M. Jeyatharan, C. Ng, V. Devarapalli, and J. Hirano, "Multiple interfaced mobile nodes in netlmm," *IETF Internet Draft draft-jeyatharan-netlmm-multi-interface-ps-03*, October 2008.

[30] J. Abeille, R. Aguiar, T. Melia, I. Soto, and P. Stupar, "Mobisplit: a scalable approach to emerging mobility networks," in *ACM Mobiarch 2006*, December 2006.

[31] H. Faithi and R. Prasad, "Mobility management for voip in 3g systems: Evaluation of low-latency handoff schemes," in *IEEE Wireless Commununications*, vol. 12, no. 2, April 2005.

[32] K. Kong, W. Lee, Y. Han, M. Shin, and H. You, "Mobility management for all-ip mobile networks: Mobile ipv6 vs. proxy mobile ipv6," in *IEEE Wireless Commununications*, vol. 15, no. 2, April 2008.

[33] P. Srisuresh and M. Holdrege, "Ip network address translator (nat) terminology and considerations," *IETF RFC 2663*, August 1999.

[34] M. Holdrege and P. Srisuresh, "Protocol complications with the ip network address translator," *IETF RFC 3027*, January 2001.

[35] T. Ernst, N. Montavont, R. Wakikawa, C. Ng, and K. Kuladinithi, "Motivations and scenarios for using multiple interfaces and global addresses," *IETF Internet Draft draft-ietf-monami6-multihoming-motivation-scenario-03*, May 2008.

[36] G. Iapichino and C. Bonnet, "Ad hoc network connection continuity for security applications report," *Eurecom, Rapport de Recherche, RR-09-237*, November 2009.

[37] G. Gundavelli, K. Leung, B. Patil, and D. Premec, "Mobile node group identifier option," *Internet Draft draft-gundavelli-netext-mn-groupid-option-01*, June 2009.

[38] D. Clark, R. Braden, A. Falk, and V. Pingali, "Fara: Reorganizing the addressing architecture," in *ACM SIGCOMM Workshop on Future Directions in Network Architecture (FDNA)*, August 2003, pp. 313–321.

[39] H. Balakrishnan, K. Lakshminarayanan, S. Ratnasamy, S. Shenker, I. Stoica, and M. Walfish, "A layered naming architecture for the internet," in *ACM SIGCOMM*, September 2004, pp. 343–352.

[40] M. Walfish, J. Stribling, J. Krohn, H. Balakrishnan, R. Morris, and S. Shenker, "Middleboxes no longer considered harmful," in *Proceedings of the OSDI*, 2004.

[41] D. Cheriton and M. Gritter, "Triad: A scalable deployable nat-based internet architecture," in *Stanford Computer Science Technical Report*, January 2000.

[42] P. Francis and R. Gummadi, "Ipnl: a nat-extended internet architecture," in *ACM SIGCOMM*, 2001.

[43] P. Nikander, J. Arkko, and B. Ohlman, "Host identity indirection infrastructure (hi3)," in *Second Swedish National Computer Networking Workshop (SNCNW)*, November 2004.

[44] I. Stoica, D. Adkins, S. Zhuang, S. Shenker, and S. Surana, "Internet indirection infrastructure," in *ACM SIGCOMM*, August 2002.

[45] D. Adkins, K. Lakshminarayanan, A. Perrig, and I. Stoica, "Towards a more functional and secure network infrastructure," in *Technical Report No. UCB/CSD-03-1242, EECS Department, University of California*, 2003.

[46] S. Schmid, L. Eggert, M. Brunner, and J. Quittek, "Towards autonomous network domains," in *8th IEEE Global Internet Symposium*, March 2005.

[47] A. Jonsson, M. Folke, and B. Ahlgren, "The split naming/forwarding network architecture," in *First Swedish National Computer Networking Workshop (SNCNW)*, September 2003.

[48] E. Nordmark and M. Bagnulo, "Shim6: Level 3 multihoming shim protocol for ipv6," *IETF RFC 5533*, June 2009.

[49] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "Locator/id separation protocol (lisp)," *Internet Draft draft-farinacci-lisp-12*, March 2009.

[50] C. Vogt, "Six/one: A solution for routing and addressing in ipv6," *Internet-draft draft-vogt-rrg-six-one-02*, October 2009.

[51] B. Ahlgren, J. Arkko, L. Eggert, and J. Rajahalme, "A node identity internetworking architecture," in *Proc. of 9th IEEE Global Internet Symposium*, Barcelona, Spain, April 2006.

[52] P. Eronen, "Ikev2 mobility and multihoming protocol (mobike)," *IETF RFC 4555*, June 2006.

[53] J. Kempf, "Goals for network-based localized mobility management (netlmm)," *IETF RFC 4831*, April 2007.

[54] Mobile IPv6 for Linux (MIPL), http://www.mobile-ipv6.org/.

[55] G. Iapichino and C. Bonnet, "Experimental evaluation of proxy mobile ipv6: an implementation perspective," in *IEEE Wireless Communications & Networking Conference (WCNC) 2010*, Sydney, Australia, April 2010.

[56] H. Nguyen, C. Bonnet, and G. Iapichino, "Extended proxy mobile ipv6 for scalability and route optimization in heterogeneous wireless mesh networks," *International Journal of Ubiquitous Computing (IJUC), Serial Publications, accepted for publication*, to appear in 2010.

[57] User Mode Linux Home Page, http://user-mode-linux.sourceforge.net.

[58] H. Nguyen and C. Bonnet, "Practical and unified process for developing the future mobile internet with simultaneous access (misa)," *Eurecom, Rapport de Recherche, RR-08-211*, February 2008.

[59] D. Mahrenholz and S. Ivanov, "Real-time network emulation with ns-2," in *Proceedings of The 8-th IEEE International Symposium on Distributed Simulation and Real Time Applications*, Budapest, Hungary, October 2004.

[60] Virtual Network User Mode Linux Home Page, http://www.dit.upm.es/vnumlwiki/index.php/Main-Page.

[61] J. Guan, H. Zhou, W. Xiao, Z. Yan, Y. Qin, and H. Zhang, "Implementation and analysis of network-based mobility management protocol in wlan environments," in *MobiWorld 2008, in conjunction with Mobility Conference 2008*, Ylan, Taiwan, September 2008.

[62] S. Hyeon, Y. Han, H. Lee, and H. Choi, "Empirical performance evaluation of ietf mobile ipv6 and proxy mobile ipv6," in *Mobility Conference 2008*, Ylan, Taiwan, September 2008.

[63] A. Udugama, M. Iqbal, U. Toseef, C. Goerg, C. Fan, and M. Schlaeger, "Evaluation of a network based mobility management protocol: Pmipv6," in *IEEE VTC 2009*, Barcelona, Spain, April 2009.

[64] J. Laganier, S. Narayanan, and P. McCann, "Interface between a proxy mipv6 mobility access gateway and a mobile node," *IETF Internet Draft draft-ietf-netlmm-mn-ar-if-03*, February 2008.

[65] PMIPv6 Open Source, http://www.openairinterface.org/.

[66] IEEE Standard 802.21-2008, "IEEE Standard for Local and Metropolitan Area Networks, Part 21: Media Indipendent Handover Services", February 2008.

[67] C. Bernardos, A. de la Oliva, J. Zuniga, T. Melia, and S. Das, "Pmipv6 operation with ieee 802.21," *IETF Internet Draft draft-bernardos-netext-pmipv6-mih-01*, October 2009.

[68] Iperf 2.0.2 Download, http://linux.wareseeker.com/download/iperf-2.0.2.rar/333782.

[69] Wireshark Software Home Page, http://www.wireshark.org/.

[70] HIP for inter.net Project Home Page, http://www.hip4inter.net.

[71] Host Identity Protocol for Linux (HIPL), http://infrahip.hiit.fi/.

[72] OpenHIP Project Home Page, http://www.openhip.org.

[73] T. Henderson and A. Gurtov, “Hip experiment report,” *IRTF Internet Draft draft-irtf-hip-experiment-06*, October 2009.

[74] VideoLAN software, http://www.videolan.org.

[75] ODTONE Project Home Page, http://hng.av.it.pt/projects/odtone.

[76] G. Iapichino, D. Câmara, C. Bonnet, and F. Filali, “Public safety networks,” *Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, IGI Global, accepted for publication*, to appear in 2010.

[77] G. Iapichino and C. Bonnet, “Security scenario definition report,” *Eurecom, Rapport de Recherche, RR-09-216*, March 2008.

[78] R. Dilmaghani and R. Rao, “On designing communication networks for emergency situations,” in *International Symposium on Technology and Society (ISTAS ’06)*, June 2006.

[79] Professional Mobile Radio (PMR), http://en.wikipedia.org/wiki/Professional-Mobile-Radio.

[80] Trans European Trunked Radio (TETRA), http://www.tetra-association.com/.

[81] Iridium Satellite Communications, http://www.iridium.com/.

[82] Thuraya, http://www.thuraya.com/.

[83] Inmarsat, http://broadband.inmarsat.com/.

[84] TRACKS, http://telecom.esa.int/telecom/www/object/index-cfm?fobjectid=11550.

[85] Emergesat, http://www.emergesat.org/.

[86] G. Iapichino, C. Bonnet, O. del Rio, C. Baudoin, and I. Buret, “Advanced hybrid satellite and terrestrial system architecture for emergency mobile communications,” in *26th AIAA International Communications Satellite Systems Conference (ICSSC 2008)*, San Diego, USA, June 2008.

[87] ——, “A mobile ad-hoc satellite and wireless mesh networking approach for public safety communications,” in *10th IEEE International Workshop on Signal Processing for Space Communications (SPSC 2008)*, Rhodes, Greece, October 2008.

[88] ——, “Mobility, access heterogeneity and security for next generation public safety communications,” in *Workshop on Next Generation Public Safety Communication Networks and Technologies, in conjunction with IEEE ICC 2009*, Dresden, Germany, June 2009.

[89] ——, “Combining mobility and heterogeneous networking for emergency management: a pmipv6 and hip-based approach,” in *International Workshop on Advanced Topics in Mobile Computing for Emergency Management: Communication and Computing Platforms, in conjunction with ACM IWCMC 2009*, Leipzig, Germany, June 2009.

[90] ——, “Ad-hoc mobility in satellite-based networks for public safety applications,” in *1st Networking/Partnering Day 2010, European Space Agency/ESTEC Conference*, Noordwijk, The Netherlands, January 2010.

[91] ETSI EN 302 307: “Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications”, Version 1.1.2, June 2006.

[92] J. Gayrard and F. Blanc, “Ka-band satellite system for public protection and disaster relief operations,” in *22nd AIAA ICSSC*, Monterey, California, May 2004.

[93] J. Gayrard, I. Buret, and A. Bolea Alamanac, “The role of satellites in broadband wireless access for public protection, disaster relief and gmes missions,” in *13th Ka and Broadband Communications Conference*, Turin, Italy, September 2007.

[94] ETSI EN 301 790: “Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems”, Version 1.4.1, July 2009.