Global mobility approach with Mobile IP in "All IP" networks

L. Morand[#], S. Tessier [*]

[#]France Telecom R&D
38-40, rue du General Leclerc, 92794 Issy Moulineaux Cedex 9, France
[*]T-Nova Deutsche Telekom Innovationsgesellschaft mbH, Berkom
Glosarer Ufer 35, 10589 Berlin, Germany

Abstract- **The purpose of the document is to describe how the EURESCOM project P1013 FIT-MIP evaluates the use of Mobile IP in an IP core network, acting as a mobility management protocol federating heterogeneous access network technologies such as PSTN, WLAN or GPRS. The aim is to provide a wide IP environment with an always-on access to IP applications (VoIP, VPN, mobile Internet, etc.), Mobile IP functionalities enabling seamless mobility through the various networks.**

Keywords: Mobile IP, GPRS, WLAN, inter-access mobility

List of Acronyms:

3GPP	3rd Generation Project Partnership
AAA	Authentication, Authorization and Accounting
CN	Correspondent Node
CoA	Care-of-Address
CoCoA	Co-located Care-of-Address
DHCP	Dynamic Host Configuration Protocol
FA	Foreign Agent
FACoA	Foreign Agent Care-of-Address
FN	Foreign Network
GPRS	General Packet Radio Service
HA	Home Agent
HN	Home Network
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunications Union
LAN	Local Area Network
MIPv4/v6	Mobile IP version 4/version 6
MN	Mobile Node
PC	Personal Computer
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTT	Round Trip Time
SIP	Session Initiation Protocol
TCP	Transport Control Protocol
UMTS	Universal Mobile Telecommunication System
UTRAN	UMTS Terrestrial Radio Access Network
VoIP	Voice over IP
WLAN	Wireless Local Area Network

I. INTRODUCTION

Currently there are several ongoing efforts to define mobile network architectures that would enable fully IP based service offering i.e. data, voice and multimedia services would be provisioned over an IP bearer. Such network architectures are referred as "All IP" networks.

As advances are being made towards this goal in the different standardization areas (IETF, 3GPP, 3GPP2, ITU), it is become now obvious that the core network of the next generation mobile system will be pure IP-based, leading to an eventual network convergence between the various telecommunication systems. This concept should allow the deployment of a unified backbone federating different access technologies e.g. narrow/broad-band, fixed/wireless, and public/private access networks.

A critical point here is to offer to the user an always-on access to IP-based services from any suitable access point regardless of the types of fixed or mobile networks and the terminal used. Besides a common session control mechanism, where the Session Initiation Protocol (SIP) seems to be generally designated, the major requirement remains the provision of a mobility management scheme enabling a seamless roaming between various access technologies to the IP core network.

As it is exposed in the first FIT-MIT Project Report [1] [2], in that network context the IP mobility providing by the routing protocol Mobile IP [3] does appear as the potential key solution. Handling the terminal mobility at the IP layer, Mobile IP provides indeed two fundamental intrinsic proprieties in an IP environment. The first one is to make the mobility transparent for the applications running over IP, which are generally based on the assumption that the terminal is fixed. The second propriety is that Mobile IP such a pure IP-based protocol is able to be deployed in any network where the IP connectivity is ensured, whatever the underlying protocols and technologies used. In that sense, the access to a Mobile IP based core network can be either wired (PSTN, ISDN, xDSL, Ethernet LAN, etc.) or wireless (WLAN, GSM, GPRS, UMTS, etc.)

Initially developed for the Internet world, Mobile IP can therefore be considered as the expecting federating protocol for a global mobility management approach enabling:

- A smooth integration of all existing and future means of access to an "All IP" core network,
- And a seamless roaming between heterogeneous access networks.

The main functions of this protocol are briefly introduced in the following section.

II. OVERVIEW OF MOBILE IP

The IETF solution for enabling the IP mobility is to use two IP addresses, a permanent address – the home address – assigned to the IP node and acting as the endpoint identifier, and a temporary address – the care-of address (CoA) – giving

the current location of the node. The approach here is to maintain the same IP address −the so-called home address− wherever the terminal is located, so that it will always have a unique identifier. In this situation, it becomes the responsibility of the Mobile IP protocol [3] to track the location of the mobile terminal in a meaningful way (topologically significant) in order to deliver any packet to it wherever it moves.

The mobility functions needed by the mobile node (MN) are administered at the network level (IP layer) by two mobility functions implemented in IP routers: the Home Agent function (HA) in the home network and (eventually) the Foreign Agent function (FA) in a foreign network. Arrived in any foreign network, the mobile node must firstly acquire a new care-of address (CoA). This CoA can be allocated either by a Foreign Agent present in the sub-network (Foreign Agent care-of address – FACoA), or by any alternative mechanism such as the Dynamic Host Configuration Protocol (DHCP), referred then as a co-located care-of address (CoCoA). Once the address obtained, the mobile node updates the Home Agent with its CoA.

Datagrams sent by a correspondent node to the mobile node's home address are then intercepted by the mobile node's HA and tunnelled to the current mobile node's CoA. The tunnel endpoint is either the FA (in case of FACoA) or the mobile node itself (for a CoCoA). In the reverse path, datagrams sent by the mobile node are usually delivered to the correspondent node using standard IP routing mechanisms, with the mobile node's home address as IP source address.

The traditional IP routing between a mobile node and a correspondent node is depicted in Fig. 1.
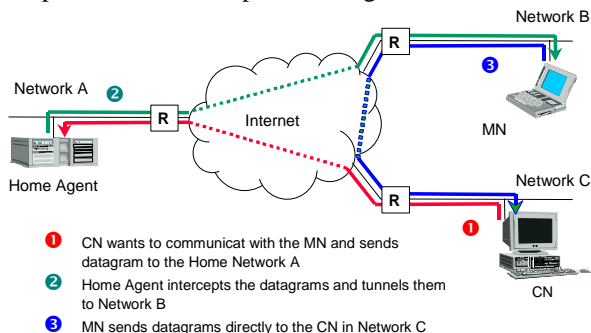

❶ CN wants to communicat with the MN and sends datagram to the Home Network A

❷ Home Agent intercepts the datagrams and tunnels them to Network B

❸ MN sends datagrams directly to the CN in Network C

Fig. 1. Mobile IP Routing

III.   REFERENCE MODEL

To handle the mobility in the wired (core/access) networks, the second FIT-MIT Project Report [4] concludes that Mobile IPv4 is a good candidate to become a federating protocol for different access networks. However, when used inside cellular systems, Mobile IP reaches rapidly its limits: it is not sufficient to handle efficiently (i.e. seamlessly) handovers, in particular for time-stringent applications such as VoIP (Voice over IP).

Two solutions could address the problem:

- Extend Mobile IP with intrinsic micro-mobility management capabilities. It is the way chosen in the current definition of Mobile IP version 6 [5];

- Keep Mobile IP in its original form – Mobile IPv4 – and use specific protocols in the cellular access networks, in a transparent way for Mobile IP.

In a short-term view, protocol stability and product availability for IPv4 lead to consider the second alternative as the easiest way for the introduction of Mobile IP in mobile networks.

Considering a generic IP architecture in which various access networks are interconnected through the global Internet, we apply on the Mobile IP *philosophy*. For this purpose, the Home (core) network is defined as any IP network containing a Home Agent-enabled router. A specific router placed in the access network border ensures the continuity of the Mobile IP dialogue between the mobile node and the Home Agent. So it has to provide Mobile IP Foreign Agent functionality. This particular router, which will be called a Gateway Foreign Agent (GFA), introduces a hierarchy in the mobility management: macro-mobility management above the GFA (inside the core network), and micro-mobility management under the GFA (inside the access network).

The separation between the mobility management in the core and the access networks confines the micro-mobility specificity (if any) in the access network and keeps Mobile IP as the common mobility protocol between different access networks. From the core network point of view, there is no difference between wired and wireless access networks.

In roaming case, Mobile IP functionality is not sufficient to guarantee the user identity and to handle access rights. For this purpose, AAA protocols e.g. RADIUS or Diameter are used for authentication, authorisation, and accounting relationships between different administrative domains [6].

To summarize the different entities and protocols involved in mobility management and roaming procedures in an all-IP architecture, we first propose the following figure (Fig. 2). It establishes a parallel between the different possible network configurations and the different roaming cases.
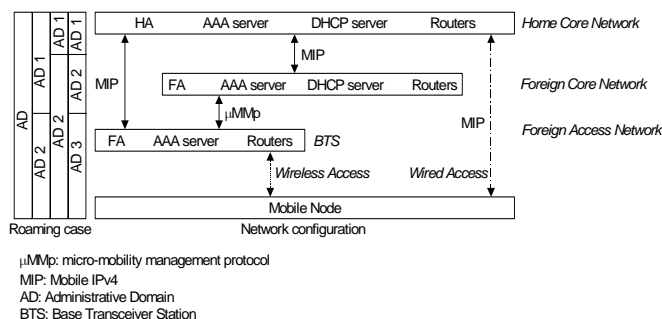
Fig. 2. FIT-MIP Reference Model

μMMp: micro-mobility management protocol
MIP: Mobile IPv4
AD: Administrative Domain
BTS: Base Transceiver Station

IV. FIT-MIP GLOBAL SYSTEM ARCHITECTURE

The first aim of the FIT-MIP project was to study the feasibility of building a global system based on an IP-based core network that can provide mobile users with existing and new IP services in various access networks (whether wired or wireless).

In order to provide to the user a large mobility environment including home, office, street or public area, the following access networks were considered by the project team:

1) GPRS Release 99 network [7], with the large radio coverage offered by GSM or UMTS in urban/sub-urban area;
2) LAN access, widespread in the corporate environment;
3) WLAN access, being able to be used in either office or any public area (hotel, airport, etc.)
4) PSTN/ISDN access with PPP connections generally used at home.

Pooling infrastructures and equipment provided by several European project partners, the FIT-MIP project testbed has been intended to realize a global telecommunication system based on the reference architecture introduced in the previous chapter.

The overall network architecture is depicted in Fig. 3.

The main points covered by this architecture are the following:

- Mobile IPv4 is the mobility management protocol in the core network. It is used to handle IP mobility between two access networks (wired or wireless).
- Micro-mobility management is an intra-access network issue. For instance, the GMM (GPRS Mobility Management) protocol will be used in a GPRS network or a specific solution such as Cellular IP [10] in a WLAN access. However, any solution must be transparent to Mobile IP and the IP core network.
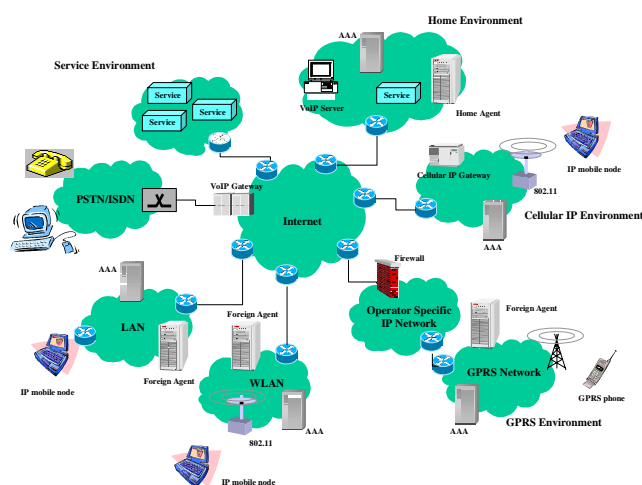

Fig. 3. FIT-MIP Global System Architecture

- A Gateway Foreign Agent (GFA) ensures the continuity of the mobile IP dialogue between the Home Agent and the mobile node.
- The mobile node's care-of address registered in the Home Agent should be the GFA IP address.
- The mobile node may acquire its co-located care-of address in the visited network using the DHCP server (instead of using the GFA IP address). However, it should be enforced to register through the GFA in this architecture.
- AAA servers may be used (in roaming situation) in order to authenticate the user during Mobile IP registration phase and to create roaming relationships between two administrative domains.

Given that reference architecture, a set of test scenarios has been elaborated by the project team. This portfolio considers several test objectives (handover, roaming, personal mobility etc.), different access networks (LAN, WLAN, GPRS, PPP over ISDN, UTRAN (UMTS Terrestrial Radio Access Network), etc.) and various factors of testing (basic functionality, services, performance/conformance of mobility protocol and version, interoperability with other protocols, scalability, security etc.). Criteria of selection are based on relevance and current access technology availability.

With test cases achieved during the second part of the project, either within local sites (hosted by France Telecom, Deutsche Telekom, Telenor and Telefonica) or through interconnected platforms, an analysis of results allowed to judge the pertinence of such architecture and to identify the needed improvements for a future deployment [8].

Among other test cases, a particular attention was given to the roaming scenario between WLAN and GPRS networks, highlighting the inter-technology access specificity and promising to be a major driving application in a short-term context for a corporate use.

V. HANDOVER BETWEEN WLAN-GPRS

The *Inter-technology Mobility* is a key challenge for future communication systems and foreseen to be one of the understandings of the 4th Generation (4G) system concept.

In order to evaluate the relevance of Mobile IP for inter-technology handoff (as stated in the FIT-MIP project) it is necessary to appraise its impact on the upper layers (especially TCP –Transport Control Protocol) and QoS mechanisms.

This was studied through a test campaign on successive handovers between WLAN and GPRS for a corporate access to Intranet in which we assume:

- A local Intranet access through WLAN (preferred in corporate environment);
- A global Intranet access through GPRS;
- End user terminals are Lap-tops;
- The switching between link layers is controlled by the Handover controller.

The Mobile terminal – a laptop connected to a GPRS terminal via an Infrared link – can switch automatically between WLAN and GPRS and vice versa based on the signal strength of WLAN. The implicit assumption here is that a link change implies an IP sub-net change. The Handover Controller is in charge of this operation. It bases its decision on link layer information that it gets from the different devices (laptop and GPRS phone).

The handover controller performs the following functions:

- Decision on which link to use.
- On/Off link switching
- Routing table control
- MIP operations control (partly)
- Ethernet device addresses allocation

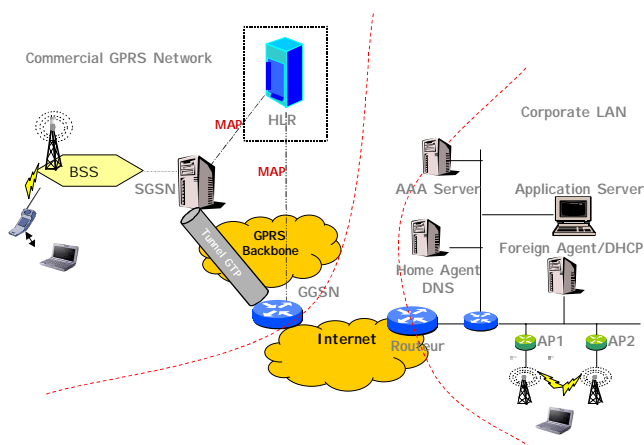The test platform is described in the following figure:

Fig. 4. GPRS-WLAN platform for Handover Tests

Using an existing commercial mobile operator network, the co-located mode is used in GPRS, as the support of the Foreign Agent mode is not available in the existing system based on the release 97 specifications. In the GPRS network, it is the GGSN that assigns to the mobile node the IP address, statically or dynamically.

In the three following sub-chapters we differentiate the performance results achieved in the tests themselves. These results highlight the TCP limitations, the time critical sessions and layer 2 issues.

A. Inter-access handoffs

The handoff time is calculated as the time for recovering the IP connectivity (IP packets can be routed to the proper IP address). In our case this is the time needed for the completion of the Mobile IP registration. Given the low load in the Home Agent the handover time is close to the round trip time (RTT).

- *From WLAN to GPRS*: When the registration is done through WLAN the handoff time is equal to the round trip time of WLAN. Which is dependant on the signal to noise ratio (C/N). At low C/N a RTT of 40 ms were experienced. When the registration is done through GPRS the handoff time is the round trip time of GPRS. It is about 1.5 seconds but with high variations.

- *From GPRS to WLAN*: Here the key measure is the WLAN signal detection time. Indeed the Mobile IP registration under WLAN is very quick thus the handover time is in the order of milliseconds (see above). The important measure is the average time for discovering the WLAN coverage. With our algorithm the average detection time is half of the monitoring period. Higher monitoring period leads to higher detection time but lower battery consumption.

A better algorithm could decrease the monitoring period when some low level WLAN signal is detected or when knowing that the terminal is close from a source of WLAN (thanks to some possible broadcast info on the GPRS cell about neighbouring WLAN coverage).

The MIP registration time (sending the MIP registration request and receiving the MIP registration reply) is lower bounded by the round trip time of the current link. Thus using the link that has the lowest RTT is preferable in order to minimise the handoff latency. WLAN even for bad radio conditions provides a higher throughput than GPRS. It is so beneficial to send the registration request from the WLAN network.

B. TCP behaviour

For the data transmission control, the TCP layer tries to converge its sending window towards the bandwidth-delay ratio. When this ratio changes significantly it takes some time before the sending window converges towards the new optimum. This leads to low utility or clogging of the link.

Additionally the time out value for retransmissions is based on the current Round Trip Time (RTT). When changing between link layer technologies the RTT changes and it takes some time before TCP understands the new value. This leads to unnecessary retransmissions due to early time outs or, inversely, long waiting times before retransmissions. These two aspects have cumulative effect that can be disastrous for the overall TCP performance and the Quality of Service as it is seen from the user point of view when moving from a WLAN to a GPRS network.

Performances can be improved by optimal setting of the TCP parameters and the parameters of the switching algorithm used by the Handover Controller (Threshold). Nevertheless this leads to a high level of engineering complexity and conflicts may arise if several ongoing TCP connections exist, even more in the case of simultaneous TCP and UDP connections are active at the same time. Modifications to TCP or on the fly changing of TCP parameters when handover between link technologies occurs seem a better way of tackling the problem.

VI. CONCLUSIONS

Mobile IP addresses mobility at the IP layer. When switching between IP sub-nets IP connectivity is regained through the use of Mobile IP. From our experience from the test bed and the use of Mobile IP for handovers we understand that Mobile IP is not sufficient for efficiently handling seamless handovers between sub-nets. Additional functionality and enhancements to Mobile IP and to other layers are required.

- *Mobile IP and the network layer*: Mobile IP as such suffers from slow handover performance. This is not adequate for many applications. Integration of Local Mobility Management (e.g. Hierarchical Mobile IPv6 [9]) solutions has proven beneficial to remedy this flaw.

- *Mobile IP and lower layers*: For supporting handoffs between links of different characteristics (e.g. WLAN and GPRS) additional functions at the link layer are required. Among others, algorithms to decide when to switch and the switching itself require considerable efforts. Interactions between Link Layer and Mobile IP have proven beneficial in providing faster handover.

- *Mobile IP and upper layers*: Mobile IP shields IP mobility to upper layers. Thus the transport layer and the application layer are not aware of the users IP mobility. That considerably reduces the complexity required at upper layers for supporting handovers between IP sub-nets. Nevertheless, for efficient handovers between heterogeneous networks, enhancements to upper layers are needed. For handovers between WLAN to GPRS for instance, TCP needs to become aware of handovers to perform well. For real time or streaming applications the session characteristics need to be modified after the switching between the two access networks

A general conclusion could be derived from those results: the strict layered architecture is not well suited for seamless inter-access handovers. High performance handovers require higher interaction between layers as well as new functions for handling optimally these interactions.

The results of the different test scenarios prove that the benefits of Mobile IP are nevertheless obvious in a global mobility system:

- It stands for the necessary bridge linking heterogeneous networks to form a widespread environment of IP connectivity,

- It will allow an always-on access to ISP services (VoIP, VPN, mobile Internet, etc.) and to Intranet networks.

Mobile IP still remains the promising cornerstone to provide the universal mobility in the next generation IP based telecommunication systems.

REFERENCES

[1] EURESCOM Project P1013-FIT-MIP, "First steps towards UMTS: Mobile IP services, an European tesbed", http://www.eurescom.de/public/projects/P900-series/p1013/P1013.htm, work in progress

[2] FIT-MIP Project Results, Deliverable 1: "Definition of Terminology for Mobile IP/Definition of IP services in the Mobility Context", September 2000

[3] C. Perkins, ed., "IP mobility support for IPv4", IETF RFC 2002, October 1996

[4] FIT-MIP Project Results, Deliverable 2: "Reference architecture and test specifications for a Mobile IP-based core network", March 2001

[5] David B. Johnson, C. Perkins, "Mobility Support in IPv6", IETF Internet Draft, July 2001

[6] S. Glass et al., "Mobile IP Authentication, Authorization, and Accounting Requirements", IETF RFC 2977, October 2000

[7] 3G TS 23.060: "General Packet Radio Service (GPRS) Service description; Stage 2", March 2000

[8] FIT-MIP Project Results, Deliverable 3: "Architectures and requirements to provide and test mobile IP services. Practical tests and demonstrations. Conclusions", September 2001

[9] Soliman, Castelluccia, El-Malki, Bellier, "Hierarchical MIPv6 mobility management", IETF Internet Draft, February 2001

[10] A. Campbell, "Cellular IP", IETF Internet Draft, January 2000