Mobile IP and Wide Area Wireless Data

Thomas F. La Porta
Bell Labs – Lucent Technologies,
Room 4F-519,
101 Crawfords Corner Road,
Holmdel, NJ 07733, USA
E-mail: tlp@lucent.com

Luca Salgarelli
Bell Labs – Lucent Technologies,
Room 4E-622,
101 Crawfords Corner Road,
Holmdel, NJ 07733, USA
E-mail: lsalgarelli@lucent.com

Gerard T. Foster
Lucent Technologies,
Q-100 Stonehill Green
(Quadrant 1+3),
Swindon, WI, United Kingdom
E-mail: gerryfoster@lucent.com

***Abstract* – In this paper we present techniques for allowing Mobile IP to interwork with wide area cellular networks. As an example, we illustrate a network consisting of a GSM General Packet Radio Service (GPRS) air interface and a Mobile IP backbone network. The advantage of such a solution is that the backbone network may easily be used to support integrated wireless and wired data transfer, and the leveraging of standard data networking protocols and equipment will reduce the cost of wireless data networks. We present issues and suggested solutions for mobility management functions, such as detecting changes in points of attachment to a network, micromobility, roaming, and paging, and security functions, such as authentication and ciphering. We show which elements of each network, GSM and Mobile IP, may be re-used, combined, or eliminated to provide a single, unified network.**

I. Introduction

To date, wide area wireless data services have not been growing at nearly the rate of their wired counterparts. The reasons include the lack of bandwidth on the wireless interface, the form factor of wireless devices, and the cost of wireless services. However, emerging services and research activities are currently addressing these limitations.

New standards, such as General Packet Radio Service (GPRS) [1] and Enhanced Data Rates for GSM Evolution (EDGE) [2], are being developed to allow wireless packet access at hundreds of kilobits per second, and several types of new wireless and portable devices are becoming widely available. The one remaining hurdle to successful wireless data services is cost.

One way to keep the cost of wireless packet data networks low is to re-use infrastructure from existing packet networks and adhere to well accepted data networking standards. This will allow integrated wireless/wireline packet data networks, and allow applications to work on both types of networks. In addition, advances made in packet technology can be applied to wireless networks directly.

In this paper, we discuss using the IETF Mobile IP 1 [3] as a networking protocol to provide wide area wireless packet data services. The use of Mobile IP meets the goals stated above of allowing the re-use of existing packet infrastructure for integrated wireless/wireline data, and adhering to a widely accepted data networking standard. Also, as IP telephony and quality of service (QoS) standards are finalized and deployed, they may be applied to a network based on Mobile IP. This will allow voice applications to be supported by this network.

To follow this approach, Mobile IP must be made to interwork with cellular networks. Cellular networks have infrastructure in place to perform mobility management, accounting, and security functions. Current cellular networks use several types of air interfaces including GSM [4] and IS-136 [5] which use Time Division Multiple Access (TDMA) to arbitrate network access, or IS-95 [6] which uses Code Division Multiple Access (CDMA). Future networks, referred to as third generation (3G) networks [7], will use some form of wide-band CMDA.

In this paper we discuss issues and possible solutions for using Mobile IP as a backbone network for cellular packet wireless data. We use GSM as an illustrative example of a cellular network. The remainder of the paper is organized as follows: in Section II we provide a background on Mobile IP and GSM; in Section III we discuss aspects of mobility management and in Section IV we discuss aspects of security. In Section V we provide concluding comments.

II. Background on Mobile IP and GSM

In this section we provide brief overviews of Mobile IP and GSM.

A. *Mobile IP*

Fig. 1 shows a generic Mobile IP network. The mobile device attaches to a network through a router that terminates a radio interface[1]. Inside the network there are two mobility agents: a *home agent* and a *foreign agent*. Each mobile node has two addresses assigned to it: a home address that corresponds to its home network, and a *care-of address* that corresponds to the network to which it is currently attached.

When a mobile device attaches to a network, it receives a care-of address from the serving network. This is often the address of an interface on the foreign agent serving the mobile device. The mobile device then registers this address with its home agent. Mobile security associations are required between the mobile device and its home agent. In addition, further security associations may exist between the mobile device and the foreign agent, and the foreign and home agents.

When packets are sent to the mobile device by a corresponding host, they are addressed to the home address of the mobile node. These packets are routed through the Internet as normal IP packets until they reach the home network of the

[1] In general, the radio interface may be on a different entity than the router, but for the purposes of our discussion they are the same.

0-7803-5669-1/$10.00 (c) 1998 IEEE

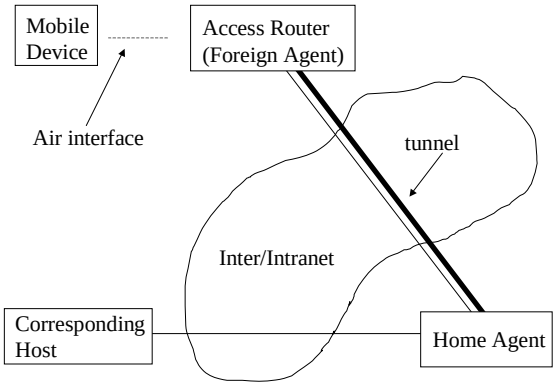

Fig. 1. Mobile IP Network.

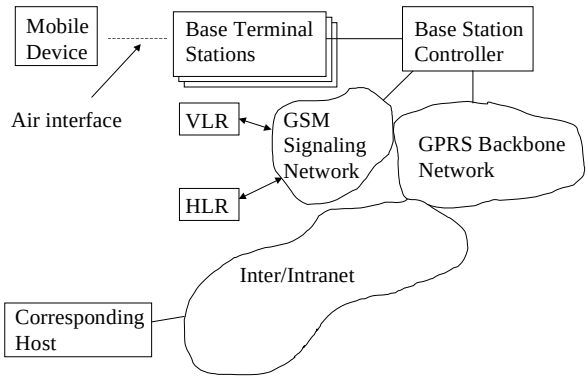

Fig. 2. GSM Network.

mobile device. In the home network, the home agent of the mobile device intercepts these packets. The home agent encapsulates these packets inside packets that are addressed to the care-of address of the mobile device. These packets are then routed on the Internet as normal IP packets until they reach the foreign agent corresponding to the mobile device. In this way packets are *tunneled* through the network.

The foreign agent decapsulates the original IP packets and forwards them to the mobile device. Packets sent from the mobile device may be treated as normal IP packets. When a mobile device moves between points of attachment on a network and changes foreign agent, it receives a new care-of address, and re-registers with its home agent. In this way, mobility management is performed.

Mobile IP also defines mechanisms allowing mobile devices to perform their own decapsulation functions, by means of a co-located care-of address. In addition, the IETF is working on an extension to Mobile IP called route optimization [8], allowing the home agent to inform corresponding hosts about the current care-of address of mobile devices. Route optimization also allows packets to be forwarded from an old foreign agent to a new foreign agent, enabling smoother handoffs.

B. GSM

Fig. 2 shows the structure of a typical GSM network. The mobile device attaches to the network over an air interface that is terminated on a Base Terminal Station (BTS). Several BTS' attach to the backbone network through a Base Station Controller (BSC).

GSM networks use a two-level hierarchy of databases to manage mobility and assist with security. The *Visitor Location Register* (VLR) is a database located in the area serving the mobile device. It maintains a temporary profile for the mobile device. The *Home Location Register* (HLR) is located in the home network of the mobile device and has a permanent copy of the profile for the mobile device, and a pointer to its current VLR.

When a user moves between areas covered by different VLRs, it registers its new VLR with its HLR. In addition, the HLR interacts with an *Authentication Center* and the VLR to authenticate the mobile device before it is allowed to receive service.

One possible packet air interface to use with a GSM network is GPRS. In a GPRS network, the BTS terminates the radio interface, Media Access Control (MAC), and Radio Link Control[2] (RLC) protocols. GPRS re-uses the GSM VLR/HLR databases for roaming and security. In addition to an air interface, GPRS also defines a backbone network as shown in Fig. 2. For our purposes, we will focus on the air interface and interaction with the GSM VLR and HLR.

Fig. 3 shows the reference system we use in the remainder of the paper. It includes the BTS, BSC, and HLR of a GSM network, and the mobility agents of Mobile IP. The BTS terminates the radio interface, RLC and MAC protocols. In our system, we use the BSC as the access router; the interface of the BSC with the BTS is a bridge over any link layer protocol, and the interface between the BSC and the wired network is a true IP router. Because this is the IP element closest to the mobile device, it is the ideal location for the foreign agent. The remainder of the core network adheres to Mobile IP.

III. MOBILITY MANAGEMENT

In this section we discuss how the mobility management procedures of Mobile IP may work in a GSM network. We consider four issues with mobility management: detecting a change in network attachment, micromobility, paging, and roaming. We defer discussion of security issues until Section IV.

A. Change In Network Attachment

Mobile IP defines two methods for determining that a change in network attachment has occurred, thus triggering procedures to obtain a new care-of address and re-register with a home agent.

[2] To simplify, we have combined several GPRS protocols that perform complimentary functions into a single RLC protocol.

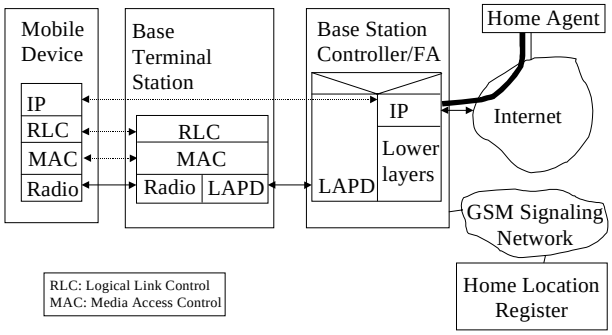

Fig. 3. Reference system.

In the first, foreign agents broadcast *Foreign Agent Advertisements*, which are received by the mobile devices on the same subnet as the foreign agent. These advertisements include the care-of addresses supported by the foreign agent. Through a set of well-defined rules, a mobile device can deduce when it is no longer in contact with its existing foreign agent and must therefore register with a new foreign agent.

In the second method, when a mobile device senses a change in link level attachment to a network, it searches for a suitable foreign agent on the new subnet, or over the air interface, by sending *Foreign Agent Solicitation* messages to which any receiving foreign agent may reply.

The agent advertisement is convenient when a broadcast channel is present. All cellular air interfaces have broadcast channels defined. However, they are of limited capacity and support only standard messages[3]. Unless a change is effected in the standards, these channels cannot be used to broadcast agent advertisements. A possible solution is to have the mobile device acquire a link level connection to the network, and then have the foreign agent multicast agent advertisements to all connected users. This technique simulates a broadcast network. The drawback of this approach is the overhead of multicasting the agent advertisements.

Alternatively, when a mobile device determines it has changed base stations by virtue of the standard broadcast channels, it may send an agent solicitation message on the link. This will be received by the foreign agent which may then reply with a care-of address. This technique is simple and does not require updates to any standards. Also, it will work with any air interface.

B. Micromobility

Once a change in network attachment is detected, a handoff (known as a *mobility update* in GPRS) must occur for the mobile device to continue to receive data. To do this, routing tables, or their equivalents, must be updated in the network.

[3] In this context, with "*standard messages*" we refer to signaling messages defined by the standardization bodies relevant to a given cellular system, e.g. the *European Telecommunications Standards Institute* for GSM.

In a pure Mobile IP network, all mobility may be handled at the IP level. In a cellular network, as shown in Fig. 3, mobility between two BTS' on a common BSC cannot be handled at the IP level because the BTS' are not assigned IP addresses and are not IP routers. In a BSC, a mapping exists between the IP address of the mobile device, the link layer connection to the BTS and the air interface connection with the mobile device. To perform a handoff requires mapping packets arriving at the FA to a different outgoing link to a BTS.

Therefore, there are two levels at which handoffs must be handled. At the lowest level, link level mobility is provided; above this, IP level mobility is provided.

C. Paging

In Mobile IP networks, because the network is IP end-to-end, a mobile device is always reachable. If the device moves to a different point in the network, its care-of IP address changes, and it re-registers.

In a cellular network, registrations from a mobile device do not typically occur upon each move unless a logical boundary or some pre-defined level in the network hierarchy is crossed. Therefore, there are periods when the exact location of a mobile device is unknown beyond a certain level in the network. This is done purposefully so that mobile devices may enter a standby mode to conserve power and do not have to re-register with the network frequently. When a device must be located, and its location is not precisely known, the network pages over the air interface for the device. When the device responds, its exact location is determined, routing tables are updated, and packets are delivered.

One simple solution to interworking paging in a cellular network is to place the FA at the BSC as shown in Fig. 3. When the mobile device moves between BSCs, it receives a new care-of address and registers. In this way, the network can always route packets to the current BSC serving the mobile device. When packets arrive at the BSC, if it does not have a current mapping for the device, the BSC pages the mobile device to locate its current BTS. When the device responds, the BSC updates its tables, and forwards packets to the mobile device. This requires that the BSC queue packets for the mobile device while the paging procedure is executing.

An alternative solution is for the BSC to broadcast packets for the mobile device to all of its BTS' if it does not know the exact BTS serving the mobile device. When the mobile device receives the first packet, it will respond and allow the BSC to update its tables and unicast subsequent packets. This eliminates the need for queuing at the BSC, but increases the air interface usage.

D. Roaming

In a cellular network, when a mobile device moves between logical registration areas, it registers with its VLR and HLR. This allows the mobile device to be located by other corresponding users. To locate a mobile device, the HLR is queried, which in turn queries the VLR, which responds with

the location of the mobile device. The logical registration areas may cover several BSCs.

The HLR is assigned based on the GSM address of the mobile device. It is not a router, and does not receive or process user data. As discussed in Section IV, it plays a key role in authenticating the mobile device.

In a Mobile IP network, similar functions are managed by interactions between the FA and HA. The FA replaces the functionality of a VLR; it receives local registration messages, and if a new mobile registers, it contacts the home agent to register the mobile device. The HA, like the HLR, knows the foreign agent currently serving the mobile device. Unlike the HLR, the HA receives all data packets destined to the mobile device and can forward them directly to the correct FA. Therefore, for data routing functions, the HA may replace the HLR. However, as we discuss in Section IV, the HLR is also used to perform additional security functions in GSM.

IV. Security

There are two aspects to security in a wireless system: authenticating users and approving them for service, and encrypting user information and signaling to prevent eavesdropping.

A. Authentication

In a GSM network, a mobile device and its HLR share a secret key. When a mobile device registers with a VLR for the first time, the VLR contacts the HLR to request authentication information for the user. The HLR replies with a set of random numbers and their corresponding signatures computed using the secret key of the mobile. The VLR can then challenge the mobile with one of the random numbers. The mobile uses its secret key to compute the signature of the random number, and sends the result back to the VLR. The VLR authenticates the mobile by matching its reply with the signature loaded by the HLR. While the HLR and the mobile device share a permanent security association (the secret key), the VLR and the mobile device share a temporary security association (the set of random numbers and their associated signatures).

In a Mobile IP system, each mobile device shares a secret key with its home agent. Optionally, a mobile can share a different secret key with each foreign agent, and each foreign agent can share another key with the home agent. Each registration message and the associated reply contain a set of authentication extensions, computed by signing the message with the relevant secret key. For example, the home agent can authenticate a message coming from a mobile by computing the signature of the message with the key it shares with the mobile, and comparing the result with the signature contained in the authentication extension.

One of the issues associated with this authentication technique is the burden in distributing the set of authentication keys. Ongoing work in the IETF [9] proposes using three sets of short-lived authentication keys that would be distributed to the HA, FA, and mobile by an Authentication, Authorization, and Accounting (AAA) server. In this case the AAA server, similar to an HLR, would share the permanent secret key with the mobile, while the three set of temporary keys would be used for authentication between mobile and FA, FA and HA, and mobile and HA. As with GSM, the mobile would hold a permanent security association with the AAA server, while temporary security associations would exist between the mobile, the foreign agent, and the home agent.

One option for using Mobile IP in a cellular network is to retain both authentication procedures. The HLR/VLR would authenticate based on the GSM address of the device, and the AAA/HA/FA would authenticate based on the IP address of the device. The drawback of this approach is the extra overhead.

A second option is to have the HLR act as the AAA server. In this case, the permanent secret key shared between the HLR and the mobile device would be the same for the Mobile IP and GSM authentication. To implement this approach, the HLR would have to be augmented with an IP interface so that it could distribute to HAs and FAs the set of short-lived keys used for Mobile IP authentication. For example, a FA acting as a VLR would receive from the HLR a set of temporary authentication keys, derived from the mobile's secret key and a set of random numbers. The set of authentication keys could then be used to perform Mobile IP authentication between the mobile device and the FA using standard authentication extensions.

B. Ciphering

In GSM, along with the random numbers and corresponding signatures, the HLR loads the VLR with a series of temporary ciphering keys that may be used by the mobile device. These ciphering keys may be computed only using the mobile's secret key over the random numbers. Therefore, when ciphering is to be enabled, the VLR sends the mobile device one of the random values it received from the HLR along with the ciphering algorithm selected by the HLR. The mobile device computes the ciphering key from its secret key and the random number and uses it for ciphering both user data and signaling on the session.

Although Mobile IP does not provide any encryption service *per se*, the IETF is defining a mechanism to enable the use of IPSec [10] ciphering tunnels with Mobile IP [11]. For example, while Mobile IP tunnels provide basic IP connectivity to the mobile, the establishment of IPSec tunnels between the mobile and the HA would enable the ciphering of the data. Mechanisms are being defined for establishing IPSec tunnels between mobile and HA, FA and HA, or mobile and FA. As in GSM, the keys used for ciphering are different from the keys used for authentication. Ciphering keys are distributed to the interested parties by means of standard IPSec procedures during the setup of the tunnel.

In the case of Mobile IP in cellular networks, the GSM and IPSec ciphering systems could be applied independently from each other, using two different sets of ciphering keys. This approach could be expensive, both because of the burden in maintaining two separate sets of ciphering keys, and because

of the overhead of the two encryption systems running in parallel.

An alternative approach would be to use the same set of temporary ciphering keys distributed by the HLR to activate IPSec tunnels, and to selectively enable one encryption mechanism or the other in different parts of the network. For example, where the air interface provides a limited bandwidth, GSM encryption could be used between the mobile device and the foreign agent, while an IPSec tunnel would serve the purpose between the FA and the HA. On the other hand, if the mobile decided to enable IPSec encryption with its home agent, GSM encryption on user data should be disabled.

V. Summary

In this paper we presented several issues and possible solutions for interworking Mobile IP with cellular networks. This is desirable so that Internet-based technology can be applied to mobile wireless networks allowing wireless/wireline integration and reducing network costs.

We examined four areas associated with mobility management. *To detect a change in network attachment*, we propose using a combination of standard GSM and Mobile IP techniques. We use GSM broadcast channels to detect attachment, and Mobile IP methods for contacting a FA. Likewise, to manage *micromobility*, we propose a combination of techniques. GSM link level handoffs are used for fine-grained mobility, and IP level handoffs are used for larger scale mobility. This two-level hierarchy also lends itself to supporting *paging procedures* so that inactive mobile devices may remain attached to the network in a passive manner thus conserving battery power. We suggest tracking mobile devices at the granularity of their serving IP router, and paging to determine their link level attachment. For *roaming*, we suggest using Mobile IP HAs to track the location of Mobile IP devices.

We also examined two areas associated with security. For user *authentication*, we proposed using the GSM HLR as a AAA server so that common secret keys may be used for GSM authentication and Mobile IP authentication. Similarly, for *ciphering*, we proposed to use a common set of temporary ciphering keys for both GSM and IPSec, and to selectively enable the two ciphering systems to avoid concurrent operation.

The above proposals require minimal modification to the core GSM and Mobile IP procedures, and allow a re-use of most existing infrastructure.

References

[1] Digital Cellular Telecommunication System, General Packet Radio Service (GSM 02.60, version 6.1), ETSI, 1997.

[2] Digital Cellular Telecommunication System, Enhanced Data Rates for GSM Evolution - Project Plan and Open Issues for EDGE (GSM 10.59, version 1.6), ETSI, 1997.

[3] C. E. Perkins, “IP Mobility Support,” IETF RFC 2002, October 1996.

[4] Digital Cellular Telecommunication System, Network Architecture (GSM 3.02, version 6.1), ETSI, 1997.

[5] 800 MHz TDMA Cellular Radio Interface – Mobile Station – Base Station Compatibility, EIA/TIA IS-136, 1994.

[6] Mobile Station – Base Station Compatibility Standard for Dual-Mode Wide Band Spread Spectrum Cellular System, EIA/TIA IS-95, 1993.

[7] *IEEE Personal Communications Magazine* Special Issue, “Third Generation Mobile Systems in Europe,” Davide Grillo Guest Editor, Vol. 5, No. 2, April, 1998.

[8] C. E. Perkins, D. Johnson, “Route Optimizations for Mobile IP,” Internet Draft, November, 1997.

[9] P. Calhoun and C. E. Perkins, DIAMETER Mobile IP Extensions, Internet Draft, November 1998.

[10] S. Kent and R. Atkinson, Security Architecture for the Internet Protocol, IETF RFC 2401, November 1998.

[11] J. K. Zao and M. Condell, Use of IPSec in Mobile IP, Internet Draft, November 1997.