Migration Issues to 2.5G and 3G for Internet Protocol-based Technologies

a report by

Ioannis Fikouras *and* **Stefan Aust**

Department for Co-operative Product and Service Engineering, Bremen Institute of Industrial Technology and Applied Work Science (BIBA), and Institute of Communication Networks (ComNets), University of Bremen

Ioannis Fikouras

Stefan Aust

Ioannis Fikouras heads the Department for Co-operative Product and Service Engineering at the Bremen Institute of Industrial Technology and Applied Work Science (BIBA). He is a research scientist and project manager at BIBA, responsible for Mobile Engineering and Enterprising. He has worked at BIBA since October 1999 after receiving a diploma in Computer Science from the University of Bremen. His personal area of interest is service engineering, specifically service discovery and integrated network platforms.

Stefan Aust has been a member of the research and teaching staff at the Institute of Communication Networks (ComNets) at the University of Bremen since April 2001, where he is currently working towards his PhD/Dr-Ing Degree. He is a student member of the Institute of Electrical and Electronics Engineers, Inc. (IEEE), and a member of the German Association for Electrical, Electronic & Information Technologies Information Technology Society (VDE/ITG). Mr Aust studied electrical engineering and information technology at the University of Bremen, Germany. He received his Dipl-Ing Degree in 2001.

Introduction

Mobile Internet access accounts for only a ver y small proportion of Internet users today, even though the number of mobile users greatly exceeds the number of Internet users.[1] It is forecast that, as early as 2003, almost half of the Internet population will consist of mobile access devices.[2] Significant technological advances in recent years in the areas of mobile phones, palm-sized and even wearable computers and wireless communications, accompanied by an infiltration of the Internet in all aspects of our lives will form the main driving force behind this trend. By that time, a variety of different wireless network platforms with different properties, capable of transporting Internet traffic will be available,[3] the most prominent representatives being 2.5G (GPRS) and 3G (UMTS™) cellular networks currently deployed all over the world. In addition, the shift of operators towards licence-free frequencies and their eventual congestion will lead to the realisation of alternative dynamic network structures,[4] namely Internet-compatible, multi-hop, ad-hoc networks. An example of such networks are the increasingly popular public Internet hot spots based on wireless local-area network (WLAN) technology.[5]

Problem Statement

The various bearer technologies cannot individually cover all the requirements of the end-user in terms of coverage, bandwidth, quality of service (QoS) and cost. The GPRS cellular system allows for data connections with a bandwidth of up to 115 kilobits per second (Kbit/s). The service is packet-oriented and is optimised for data traffic, e.g. Internet downloads. Furthermore, GPRS supports high-mobility similar to that of GSM™ and supports 'always-on' connectivity, which allows a more convenient dial-in procedure for mobile users than GSM.

GPRS networks nevertheless fail to deliver the high bandwidth necessary for future multimedia applications. UMTS, on the other hand, is supposed to deliver this bandwidth but – at least during the first stages of its deployment – will not offer sufficient coverage for truly mobile users. On a different level, WLAN based on the Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.11a and 802.11b standards offer bandwidth up to 11 megabits per second (Mbit/s) or 54Mbit/s at relatively low deployment costs, but restrict the movement rate of the user to 5Mbit/s. Furthermore, WLANs require a high density of access points that makes their deployment in sparsely populated areas uneconomical.

Consequently, a technology that allows the integration of available heterogeneous and homogeneous networks into a single platform capable of supporting user roaming between them, while not interrupting active communications, will gain importance.[6] This development will be assisted by the rise of new mobile devices capable of maintaining various access interfaces that will allow simultaneous connectivity over a range of providers and technologies.[7]

Proposed Solution

Roaming of mobile users between WLAN hot spots or between GPRS/UMTS cells can be achieved with the help of the Mobile Internet

1. *P Keryer, Presentation at Visions of the Wireless World, Brussels, 12 December 2000.*
2. *European Telework Online, http://www.eto.org.uk*
3. *N Niebert, "Convergence of Cellular and Broadband Networks Towards Future Wireless Generations",* Wireless Strategic Initiative (WSI) Book of Visions 2000, *Visions of the Wireless World, Brussels, 12 December 2000.*
4. *W Mohr, "Alternative Vorschläge zur Spektrumsnutzung für IMT-2000/UMTS", Spektrumsworkshop ITU-R, Geneva, Switzerland, October 2000.*
5. *M Ward, "Write Here, Right Now",* BBC News Online, *July 2002, http://news.bbc.co.uk/1/hi/in_depth/sci_tech/2000/dot_life/2070176.stm*
6. *N A Fikouras, C Görg and I Fikouras, "Achieving Integrated Network Platforms through IP", Proceedings of the Wireless World Research Forum (WWRF) Kick-off Meeting, Munich, Germany, 2001.*

Protocol (MIP). While operator system interface (OSI) layer-2 mobility is easy to accomplish and is already supported in various systems, layer-2 solutions do not allow terminals to roam between different Internet Protocol (IP) networks, i.e. by crossing router domains. MIP operates at the OSI layer-3 and enables seamless mobility between different IP networks. MIP is achieved through a set of extensions to IP Version 4 (IPv4) and IP Version 6 (IPv6).

Providing mobility support at the network layer has the advantage of being independent of the link layer used in an access system.[8] Since MIP works at the network layer, applications that operate at higher layers can be operated on a continuous basis even when a mobile node changes its point of attachment to the Internet.

The system architecture of MIP consists of several mobile agents, namely:

- a home agent;
- several foreign agents;
- the correspondent node; and
- a mobile node.[9]

The mobile node receives the data traffic from a correspondent node via the home agent, which manages the data flow to the mobile node. When the mobile node is located at the home network, the home agent acts as a normal router. If the mobile node moves from the home network to a foreign network, the home agent receives a temporary address (care-of address) from the foreign network where the mobile node now is located. In this case, the home agent routes the data flow from the correspondent node via the foreign agent using IP-tunnelling functions. The home agent tunnels the data flow to the mobile node using the care-of address of the mobile node.

MIP uses two different tunnels: a 'forward' tunnel and a 'reverse' tunnel. The forward tunnel forwards the data traffic towards the mobile node, starting at the home agent and ending at the mobile node's care-of address. The reverse tunnel starts at the mobile node's care-of address and ends at the home agent.

Figure 1: Mobile IP Architecture

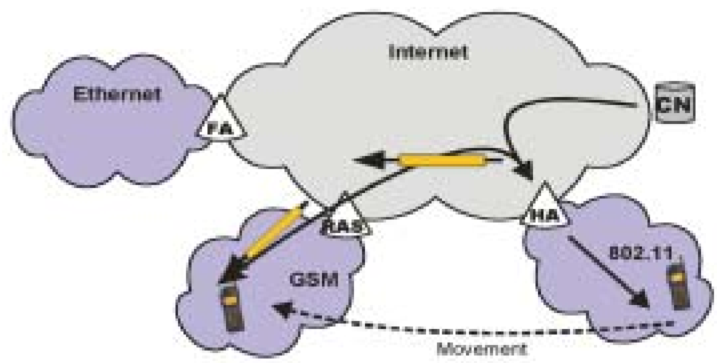
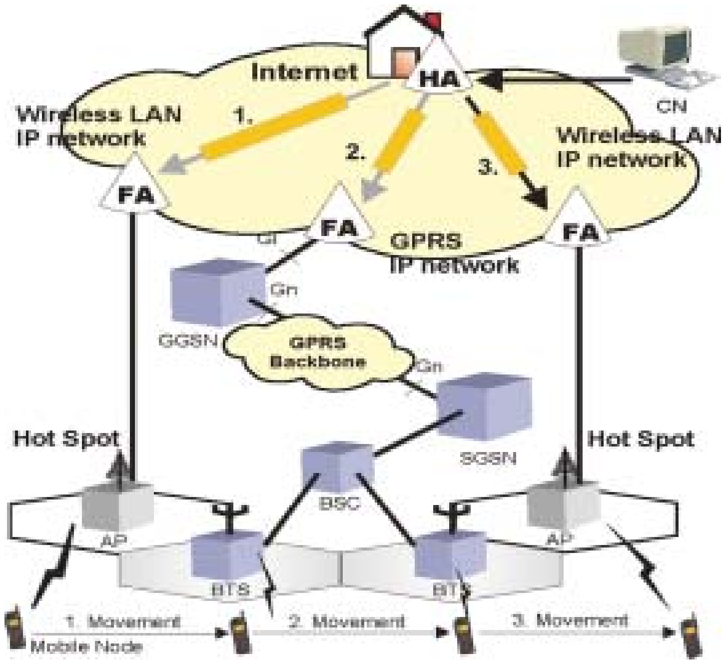


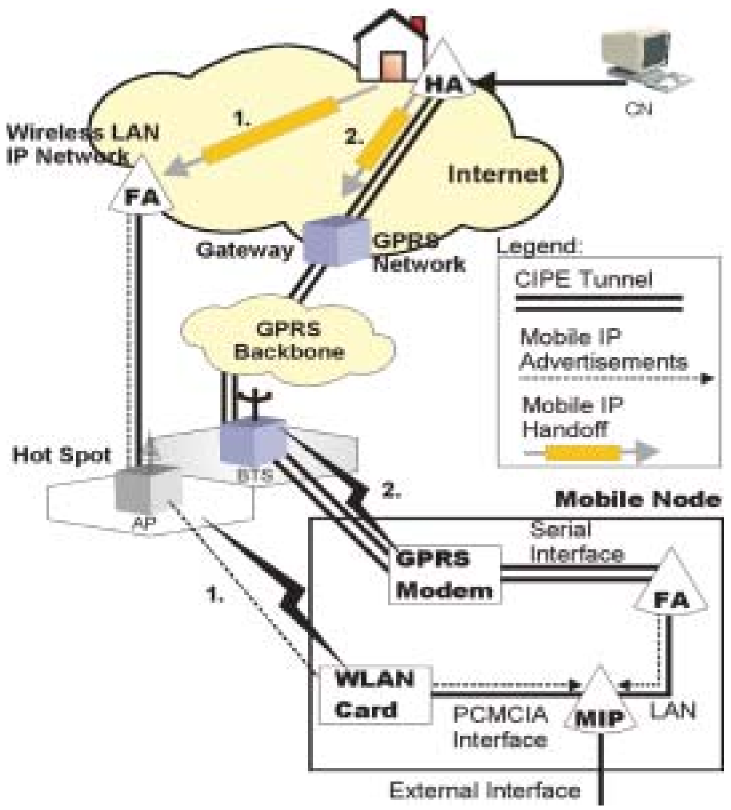
Figure 2: Seamless Mobile IP Hand-offs Between GPRS and Hot Spots



Investigation of MIP hand-offs between heterogeneous network systems has been carried out and has identified the efficiency of wireless hand-offs.[10,11] There are also QoS investigations available, which depict the QoS support for applications, which are running on an underlying MIP implementation such as mobile server and gateway systems.[12]

7. *H R Katz and A E Brewer, "The Case for Wireless Overlay 'Networks'", The International Society for Optical Engineering (SPIE) Multimedia and Networking Conference (MMNC '96), San José, California, USA, January 1996.*
8. *It should be emphasised that information from the link layer is essential for more effective and efficient support of seamless hand-offs. For example, link-layer information could be used to predict the need for hand-off between access systems and thus prepare hand-off at an optimal moment and condition.*
9. *Charles E Perkins,* Mobile IP Design Principles and Practices, *Addison-Wesley Wireless Communications Series: 1998.*
10. *K Kuladinithi, A Könsgen, S Aust, N Fikouras, C Görg and I Fikouras, "Mobility Management for an Integrated Network Platform", Mobile and Wireless Communications Networks 2002, Stockholm, Sweden, September 2002.*
11. *D Fritsch, N A Fikouras and C Görg, "Enabling WAP Hand-offs Between GSM and IEEE 802.11 Bearers with Mobile IP", Proceedings on Wireless Personal Multimedia Communications (WPMC), Aalborg, Denmark, September 2001.*

Figure 3: System Architecture



MIP and Network Address Translation

Several problems can be currently identified when performing MIP hand-offs over a GPRS network. The main issue is caused by the Network Address Translation (NAT) Protocol used by network operators to map the internal IP addresses of their subscribers to public IP addresses in order to provide Internet connectivity.[13] Issuing private IP addresses to subscribers is more advantageous to the operators as this allows them to assign an IP address to each customer without actually owning that many addresses. Considering the fact that large operators such as Deutsche Telekom and Vodafone can have many millions of customers in a single country, this is a rather useful function. The problem, however, lies in the fact that private IP addresses are not routable outside the provider's private network. Therefore, the operator offers Internet access by using a NAT gateway that translates the private IP address of each mobile node to the gateway's own external public IP address. Due to MIP functions being based on routable public IP addresses, MIP services are not attainable for subscribers with private IP addresses.

Furthermore, tunnelling functions that are used by MIP, fail due to the NAT gateway.[14] Without these tunnelling functions it is impossible to establish an MIP-based communication with the mobile user. The issue is further aggravated by firewall systems operated by many mobile operators to protect private networks from the Internet. Such systems typically perform ingress filtering, making it impossible to establish data connections through the firewall because the IP source addresses of the mobile node is not part of the local network's address space.

Currently, the Internet Engineering Task Force (IETF) is developing solutions for traversing NAT gateways when using MIP.[15] Such mechanisms are based on the MIP's registration request and reply messages that pass through an NAT gateway. Such messages can go through an NAT gateway as User Datagram Protocol (UDP) packets on port 434. An MIP extension that sends all traffic (signalling and data) via UDP tunnel at UDP port 434 is defined.

MIP and Firewalls

Mobile nodes behind a firewall sending data packets to a correspondent node with a different IP source address are usually blocked by firewalls because their source address, being the destination address of the home network, is different from the network address of the mobile node. In this case, it is impossible for the mobile node to send data packets to the correspondent node, which is located in the Internet. A solution to this problem is to implement a tunnel through the firewall so that it cannot interpret the data traffic transmitted by the mobile node.

Proposed System Architecture

A viable system architecture for MIP hand-offs between GPRS and WLAN systems has to take into account NAT gateways and ingress-filtering firewalls. The system architecture depicted in *Figure 2* describes a solution based on an MIP implementation with an additional tunnelling function implemented using Crypto IP Encapsulation (CIPE).[16] The CIPE tunnel is required to establish a direct connection from the mobile node to the home agent. Therefore, all MIP-related packets can be exchanged between the mobile node and the home agent via the additional foreign agent

12. *S Aust, N A Fikouras and C Görg, "Enabling Mobile WAP Gateways Using Mobile IP", Proceedings of European Wireless 2002, Florence, Italy, February 2002.*
13. *Blocks of IP addresses reserved for private use and not used in the Internet: 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255 and 192.168.0.0 to 192.168.255.255.*
14. *L Phifer, "The Trouble with NAT",* The Internet Protocol Journal, *Vol. 3, No. 4, December 2000.*
15. *"Mobile IP NAT/NAPT Traversal using UDP Tunnelling", work in progress, Internet Engineering Task Force (IETF), May 2002.*
16. *Olaf Tietz (2002), "CIPE – Crypto IP Encapsulation", http://sites.inka.de/bigred/devel/cipe.html*

directly. The tunnel starts at the home agent and ends at the additional foreign agent, which is located at the side of the mobile node.

The MIP software that is used does not support an additional tunnel connection. Therefore, the mobile node consists of an MIP agent and a foreign agent, which has a fixed connection to the MIP agent. The foreign agent provides the tunnel to the home agent through the NAT gateway and is connected to the GPRS network. The tunnel uses 'keep-alive messages' while the GPRS connection is not in use (for economic reasons). The foreign agent sends MIP advertisements to the MIP agent via local-area network (LAN) interface.

Furthermore, via the serial interface, the GPRS access is provided and the CIPE-tunnel is established. The MIP agent has the functionality of an MIP-enabled mobile node to support MIP hand-offs between two interfaces. The MIP agent is connected to the additional foreign agent to get GPRS access. On a second interface, the MIP agent is connected to the wireless hot spot via a Personal Computer Memory Card International Association (PCMCIA) wireless card.

This system architecture is sufficient for hand-offs between one GPRS network interface provided by a GPRS mobile phone and one WLAN-based hot spot. If the mobile node is inside the coverage of the hot spot, the MIP agent receives the MIP advertisements from the hot spot via the wireless connection. In this case, the MIP agent establishes a hand-off from GPRS to WLAN. Otherwise, if the hot spot is not accessible, the mobile node establishes a hand-off from WLAN to GPRS (vertical hand-off). This provides a permanent Internet connection allowing downloads without data interruption and minimal data loss.

Design of Vertical MIP Hand-off Requirements

For fast straight-line movements there are no problems for vertical hand-offs between WLAN and GPRS. However, in unstable hot spot areas where mobile nodes switch frequently between different networks, high packet loss is a major issue. Therefore, a hysteresis must be defined that will provide stable MIP hand-offs. The hysteresis can be realised by an additional script, which maintains two different values: a low watermark and a high watermark. The low value defines which signal strength of the hot spot is insufficient for data transmission. In this case, the mobile node establishes a vertical hand-off from the hot spot to the GPRS network and suppresses advertisements from the hot spot. The high value defines a sufficient signal strength of the hot spot. In that case, the mobile node establishes a hand-off from GPRS to WLAN. The definition of the signal strength and the values of the hysteresis depend on the particular WLAN PCMCIA card, which is used in the mobile node.

Conclusions

This article has described the system architecture of the Institute of Communication Networks (ComNets) test bed at the University of Bremen, including hand-offs between GPRS networks and WLAN systems and has presented results of the investigations of packet traces based on MIP hand-offs. Using additional tunnelling functions has eliminated the problems of NAT and firewall systems. Moreover, frequent switching during MIP hand-offs in unstable areas of WLAN coverage has been solved using a hysteresis. The investigations show that there are no significant data-packet losses during MIP hand-offs between GPRS and WLAN. This is important to meeting high QoS requirements. ■

Acknowledgments

The authors would like to thank Dr G Kadel, Dr S Hischke and B Xu from T-Systems Darmstadt, Germany, for their valuable comments within the 'IPonAir' project. This work has been presented as part of the EU Framework 5 Project Novel Modelled Analogue Data (NOMAD) and the authors would like to acknowledge the contributions of their NOMAD colleagues.