Seamless Mobility over Broadband Wireless Networks

F. Steuer, M. Elkotob, S. Albayrak, H. Bryhni, T. Lunde

Abstract — **A broadband wireless architecture with 802.11 (WLAN/WiFi) as a core coverage technology supported by 3G cellular (UMTS) as additional coverage for signaling and umbrella functionality is presented in this paper. The backbone network is wired and the individual broadband subscribers maintain a so called "Residential Gateway" (RG) which technically allows the splitting of the wireless access network provided by each residential WLAN access point into two virtual networks; one private for the RG owner and one for visiting users who roam in the vicinity of the access point. The mobile visiting users thus roam between the publicly accessible WLAN networks maintaining their session and service connectivity as they move between residential WLAN coverage areas. Both residential and visiting users are served by an architecture that provides separation between traffic types, management of quality of service, security and seamless mobility. Users are automatically authenticated and service continuity is maintained as the user moves between coverage areas. The focus of this paper is on technical aspects which enable seamless mobility and automatic authentication of users in a way which is even transparent to the applications running on their multimode mobile devices.**

Index Terms— Public WLAN, seamless mobility, Mobile IP, VoIP, VPN.

I. Introduction

Mobile terminals such as smart phones and PDAs now combine cellular and WLAN access in a single device (e.g. Nokia 9500 smart phone, HP iPAQ h63xx and O2 XDA III, PDA’s). This development in mobile terminals opens for new use of mobile services. At the same time, residential broadband access is now available in most countries using xDSL and CATV access technologies. These residential broadband access networks can also be used with wireless access for the home user and even visitors. Thus, mobile users can obtain broadband wireless access using widespread wired access network as a high capacity backhaul technology. A sample service aspect is voice over IP across any network, but many other communication services can be envisaged, ranging from mobile corporate access to education and gaming as some examples. The most crucial security aspect for a successful service includes automatic authentication, handling of VPN sessions, and the security of signaling traffic. Real time audio for voice applications (telephony) over IP is well supported in our scenarios with additional capabilities of the network to offer users access to downloads such as multimedia on demand (audio and video), streaming music as well as limited quality video streaming and video conferencing. This paper is based on joint research in the EU 6th framework programme called Open Broadband Access Network (OBAN) [1], and is based on contributions from Telenor, EuroConcepts, France Telecom, ISMB, Lucent, Motorola, NPT, ObexCode, Sintef, Swisscom Innovations, Telefonica I+D, BirdStep and Technische Universität Berlin.

A. Wireless Communications

In the OBAN architecture, local service access is provided using WLAN, while WWAN networks are used to provide uninterrupted ubiquitous service access when the user moves outside of WLAN coverage. A key aspect of the system is that authentication and handover between networks is done automatically, without intervention from the mobile user. A prototype has been established to verify the results of the research effort.

Broadband Wireless access networks represented by the Wireless LAN standards (IEEE 802.11a,b, and g) are the core coverage technology used in OBAN. WLAN is used due to its low cost and high availability in advanced mobile terminals. As backhaul technologies ADSL, SDSL, Ethernet, cable and fiber are supported as well as wireless backhaul such as IEEE 802.16/16a. Currently, UMTS FDD is used for umbrella functionality.

The proposed architecture can be used by new operators without own access infrastructure, as well as incumbent operators that already operate wired and wireless access networks. This flexibility opens for new service provider business models.

B. Cross Technology Access and Seamless Mobility

For the end user, explicit selection of access points and manual authentication to every available network is not acceptable. Thus, network selection and authentication must be automatic.

The combination of multiple access networks provides the potential advantages of a single bill scenarios and simple, integrated access to any network that the terminal supports and seamless mobility with session continuity provides a

Manuscript received April 15, 2005. This work was supported in part by the EC 6th framework program “Open Broadband Access Network”. EC contract no 001889.

F. Steuer, M. Elkotob, S. Albayrak are with the DAI-Labor, Technische Universität Berlin, Franklinstr. 28/29, 10587 Berlin, Germany ({frank.steuer, muslim.elkotob, sahin.albayrak}@dai-labor.de, Tel.: +49 30 314 21758, Fax: +49 30 314 21799).

H. Bryhni and T. Lunde are with Birdstep Technology ASA, Bryggegata 7, 0250 Oslo, Norway ({haakon.bryhni, trond.lunde}@birdstep.com}).

positive end user experience.

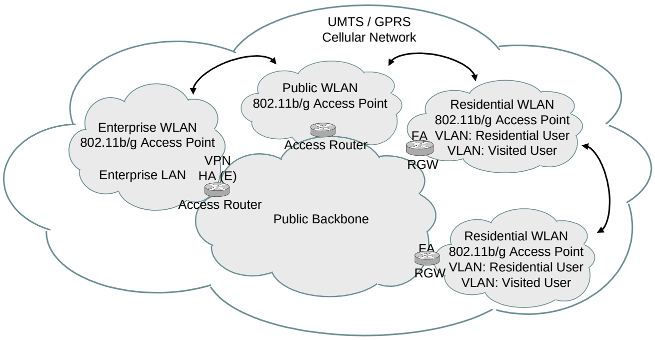

Figure 1: Roaming from enterprise to public and between "Residential Gateways" (RG)

C. Range of Target Services

Packet based communication services are the target service scenario. VoIP has the hardest requirements with regard to handover times, packet loss and delay and therefore is perfectly suited as an application used for the evaluation of user perceived and measurable performance and quality of the whole system.

Other scenarios would be using entertainment applications such as streaming music, video clips (e.g. news, sports and personalized subscriptions), in addition to office-related and document processing applications which require some degree of connectivity. The applications are thus required to support mobility with certain periodical disruptions without affecting the consistency of the sessions in which the user is engaged. At this stage there are several aspects to mention: for instance, applications have to preserve the session configuration in terms of open windows and displayed contents even while going through slight and short disruptions in the current network attachment, as well as entire change of access network. State of the art streaming applications support buffering with a sufficient size to withstand short disruptions and to resume the stream after temporary packet loss.

II. OBAN System Architecture and Seamless Mobility

A. Open Broadband Access Network System Architecture

Figure 2 details the different actors in OBAN, their relationship between each other and the OBAN architecture from a mobility management point of view. Home of the mobile nodes is the OBAN Service Provider which provides mobility management as one service within the OBAN. The entities involved in the mobility management architecture are the mobile nodes, the Foreign Agents (FAs) which are located on the RG, optional Gateway Foreign Agents (GFAs) to enable regional registration and to improve the overall system behavior and the Home Agent (HA).

B. The Residential Gateway

The Residential Gateway (RG) is the entity in OBAN which technically allows the splitting of the WLAN access network provided by each residential access point into two virtual networks, one private for the RG owner and one for visiting users who roam in the vicinity of the access point. The RG provides separation between traffic types depending on the user groups (home or visited), management of quality of service, security and authentication mechanisms. IEEE 802.1x and EAP-SIM based WLAN authentication and seamless mobility based on Mobile IP are supported by the RG.

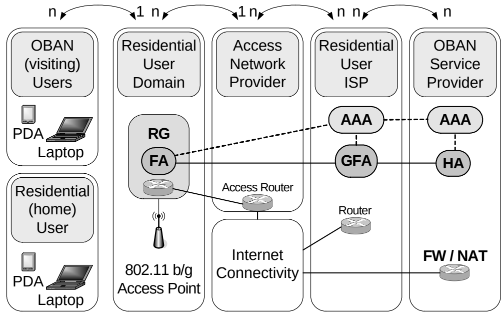

Figure 2: Open Broadband Access Network

The Mobile IP FAs located on the RG are optional just like the GFAs but their deployment improves the overall system behavior, performance and scalability. For backhaul purposes different network technologies can be deployed by the OBAN access provider. Today, asynchronous DSL is the most common technology which is suited to serve as the backhaul technology for the RGs. Besides DSL also cable or fiber can comprise the wired part and in areas where wired connectivity is not available or too expensive to be deployed. Wireless MAN technologies as 802.16/16a can also be used to provide connectivity for the RGs.

C. Coupling of Core Technologies

With the rise of 802.11 based networks the integration with traditional mobile operators' networks and especially the recently deployed 3G networks has become an important topic. In [5], the 3rd Generation Partnership Project (3GPP) details the requirements for WLAN – 3G integration. In the feasibility study [6] six scenarios for UMTS release 6 and the inter-working with 802.11 networks are defined. Scenario one and two cover common billing, customer care, 3GPP based access control and charging capabilities. Scenario three conveys the access to 3GPP packet switched services from 802.11 networks. Scenario four introduces the service continuity and scenario five adds seamless service continuity. Scenario six extends the system with access to 3GPP circuit switched services from 802.11 networks.

To achieve these different steps of inter-working several coupling approaches can be used. Three approaches can be differentiated: open, loose and tightly coupled [7].

In the open coupled approach, there is no real integration effort between 3G and 802.11 networks. Completely separated data and control paths are characteristic for this approach. Different subscriber databases and different authentication schemes are used. This approach has no implications on either

3G or 802.11 networks with regard to additional standardization efforts or hardware and software requirements. To guarantee service continuity one option is to deploy Mobile IP since it does not rely on a particular access network.

In the loose coupling approach [Figure 3], 802.11 networks are used as complementary access networks to 3G networks. Authentication of network access is based on the same subscriber database and centralized user administration, billing and accounting is possible. There is no impact on the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN). The HLR (Home Location Register) – AAA (Authentication, Authorization and Accounting) integration leads to some standardization effort. Mobility management, QoS and security issues can be addressed based on IETF (Internet Engineering Task Force) standards.

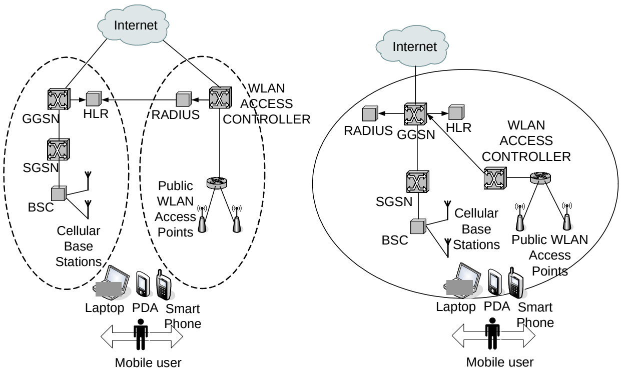

Figure 3: Loose Coupling and Tight coupling

In the tight coupling approach [Figure 3], 802.11 networks are integrated into the 3G network as an additional access technology. 802.11 access points are connected to the UMTS core network using a wireless access gateway (WAG). The same data and control paths characterize this approach. The tight coupling approach allows the highest control for the operator. It is the most complex approach with regard to needed equipment, resulting costs and standardization effort.

Unlicensed Mobile Access (UMA) is a recently proposed approach for integration of 3G networks with networks using unlicensed frequency bands like WLAN or Bluetooth with focus on voice services. The UMA Network Controller (UNC) is introduced. The UNC is integrated into the 3GPP core network via 3GPP defined interfaces. With UMA, GSM/GPRS protocols are tunneled through IP networks. This approach enables the integration of residential unlicensed networks with the mobile operators' 3G networks. 3G Circuit switched as well as packet switched services can be used from the unlicensed networks. This approach is similar to the tight coupling approach and currently evaluated by the 3GPP.

Note that the UMA standard is not considering mobility using Mobile IP, and is not integrating enterprise WLAN access and use of VPN technology to secure data sessions. In the OBAN architecture, we envisage 3G, Public WLAN, Residential WLAN and Enterprise WLAN as integrated parts of the mobile user access networks as shown in Figure 4.

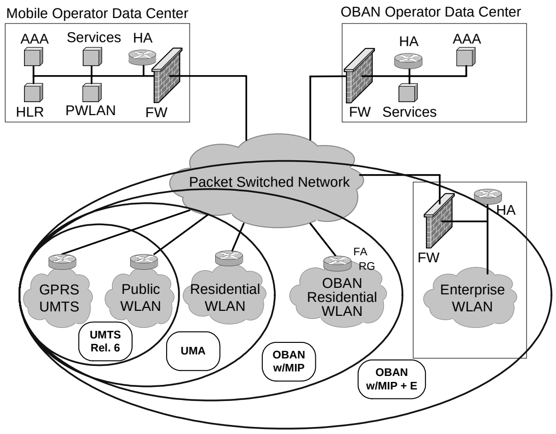

Figure 4: OBAN compared to UMTS rel. 6 and UMA

D. *Seamless Mobility*

The Open Broadband Access Network may be deployed with different architectures. Also, since fixed and mobile network operators will select different approaches on how to integrate their wireless service offerings, it is vital to ensure a mobility technique that can work across the boundaries of these network architectures.

Mobile IP [2], [3] is an IP based network layer technology independent of the underlying access network. Additionally, it is also independent of the applications and services running on top of it and can therefore be presented as an ideal candidate to solve seamless access to multiple networks. However, Mobile IP is not yet by default supported in end-user terminals and interoperability concerns must be addressed.

The key areas to focus on when providing mobility for seamless service models are handover efficiency, security and overall network architecture. Before handover efficiency is discussed, it is vital to present a client architecture model that can cater for the needs of providing a seamless service with the required security. As most users today use encryption techniques to protect their private data, this paper presents a Mobile IP solution that can interoperate with standards based legacy encryption techniques (VPN, incl. IPSEC and SSL).

The key of the client architecture is to enable tunnel based security schemes to survive handovers between network elements. By placing encryption as an overlaid component to Mobile IP, tunnel encryption endpoints will survive as they terminate in the Mobile IP address provided by the Mobile IP service.

The solution presented does however have limitations as it incurs overhead when the user moves inside a protected network. Data from inside a protected network will still be encrypted and loop via the Home Agent. To solve this problem, the suggested approach is to provide a model that provides two mobility schemes, separated by the encryption device [Figure 5]. This solves the overhead when sending data on the private Mobile IP system. Note that this method is only required in end-user terminals where VPN is used.

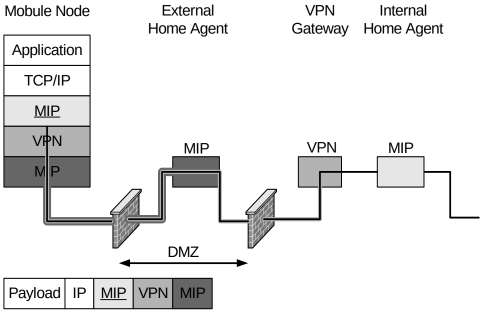

Figure 5: Two mobility schemes separated by the encryption device

In order to provide an uninterrupted user experience it is vital that handover decisions are done automatically and in a manner that ensures the best available connection according to dynamic or static priorities. The following are the factors that should cater for such decisions.

Static priorities of adapters – This represents a static priority for the different connections automatically recognized by the client. Static priorities means that the client will connect to the available network highest prioritized in the priority queue. If networks 802.11b and UMTS are both available but 802.11b has higher priority, the client will use 802.11b. But, if the signal strength of the 802.11b connection deteriorates and falls under the predefined minimum value, then the client will trigger a switch (see a more detailed explanation below under WLAN Helper Modules).

Dynamic priorities of connections – If connections are not added to the static priority queue, they should be dynamic. Selection criteria’s for the preferred network connection the client connects to will be based on dynamic priorities such as bandwidth, cost, and throughput with assistance from a client history databases. Clients must cater for traffic failures as well and should subsequently change networks if throughput falls below specified levels.

Roaming history database – The Mobile IP client should incorporate a roaming history database that assists the client in connecting to preferred network connection. This database contains valid information about previously visited networks and can use criteria’s such as efficiency, latency, configuration parameters and authentication credentials to assist in the handover process. Such historical data are not always valid since they may change over time and the clients should use historical data as a guide: it still monitors prevailing network conditions, and if they have changed, then the client will modify its behavior and update the historical records accordingly.

WLAN Helper Modules – Wireless LAN access points have a limited range. A wireless LAN intended to cover anything other than quite a small area will therefore require the installation of several access points distributed around the area. The client must incorporate software for monitoring the signal strength from access points, and transparently swapping between them to maintain optimum performance. This must be based on signal strength measurements from surrounding access points.

WLAN – WLAN handovers – The 802.11 physical medium has limitations that force an 802.11 client to be associated with only one AP at a time. During re-association to another AP or SSID (Service Set Identity), the client will have loss in connectivity. The WLAN handover algorithm should therefore also incorporate handover algorithms based on SSIDs and Signal Strength measurements. This means that the client should not only prioritize between adapters, but also between different SSIDs and the signal strength differences between the various APs. This should be made asynchronous so that rescan for APs and SSIDs can be made while the client is connected to the old network.

Authentication - For the service to appear seamless to the user also from the access control point of view, a commonly agreed authentication mechanisms such as Mobile IP MN-FA authentication, 802.1x EAP/SIM or similar should be employed in the public network, while the enterprise may deploy Mobile IP MN-FA, 802.1x EAP/TTLS or similar certificate-based authentication schemes. The advantage of Mobile IP MN-FA authentication is that no certificate management is needed, and standard AAA infrastructure is sufficient to authenticate the user. Note that a Mobile IP client can be combined with a WiFi and/or GPRS client that assist with SSID selection, setup of cellular modems and provide public WLAN hotspot directory services, etc [8].

III. Quantitative Aspects of the System

To evaluate the quantitative aspects of the system, we have used a reference installation as shown in Figure 2, where a mobile terminal (a laptop using Microsoft XP and a Mobile IPv4 client) moves between the WLAN coverage areas of residential gateway installation RG_A and RG_B both using the OBAN Residential Gateway software, and connected to a router acting as a Mobile IP Home Agent, and a FreeRADIUS server acting as the AAA server. The Mobile IP client implements the aspects discussed in the Seamless Mobility section, and provides mobility between any access network available in the mobile terminal. The user perceived QoS has been evaluated, and simple measurements of handover times have been recorded. Many factors influence the handover time, and these factors are discussed with respect to their potential influence on handover latency.

User perceived QoS was evaluated using three sample applications: Skype Voice over IP conference application, Windows Messenger (v4.7) and Cisco VPN client with Windows file sharing and Outlook/Exchange email exchange.

All three classes of applications should work seamlessly across the access points. Experiments in our test environment show that a seamless, application independent handover between RG’s can be done within acceptable time limits when using Skype, MSN Messenger and VPN access to e.g. file and email corporate services. The use of Mobile IP FA help to improve handover speed, and the latency between the RG and the HA has been negligible in our setup. Automatic Mobile

Node to FA authentication was used to open the firewall in the RG so that manual login was not needed in the visiting RG.

An advantage of the seamless mobile behaviour is that the Voice over IP conversation, the chat session, the file transfer or email session continues uninterrupted even when the network point of attachment is moved. Users of mobile terminals have been used to restart sessions, or even restart applications to reconnect to their service when they move networks. This is no longer necessary with seamless mobility based on Mobile IP supporting VPN.

In our test environment, Mobile IP handover from RG_A to RG_B was done with 80 ms latency from the Mobile IP client in the terminal decided to perform a handover until the new connection was automatically established. The presence of Mobile IP FA in each residential gateway improves handover speed, since there is no need to wait for DHCP process, which may be lengthy. Practical handover times in other scenarios are longer, in particular when handoffs to cellular networks are performed.

The following factors have shown to influence handover times negatively and when combined can result in more than one second handover time:

1. DHCP. We have experienced that certain DHCP servers, such as the Microsoft Windows Advanced Server DHCP server, does not want to assign an IP address to a new terminal before the server has "pinged" all previous users of that IP address, and ensured that the address is not already in use. This process can alone take up to one second. Significant performance improvement for co-located handovers can be done by turning off this feature in the DHCP server. It is important to note that DHCP is a limiting factor only in the case of handovers to and from the same access technology (WLAN - WLAN), since our current implementations have "make before break" functionality for inter access technology handovers (for instance UMTS connection is made available prior to the actual handover from WLAN).
2. Time from the physical link is established or removed, such as Ethernet cable insert and removal until the Windows "Link up" signal is received. This is implementation dependent and has shown to vary significantly between different network interface cards/chipsets.
3. Search for unknown SSID. If the user moves from one WLAN access area to another, the search for new available SSIDs where the user is able to authenticate (eg. in a visitor hotspot). This process is implemented differently on current WLAN cards and WLAN kits mounted inside popular terminals.
4. Finally, the latency to Mobile IP Home Agent is critical for the handover time since most protocol messages must travel from the Mobile Node to the Home Agent. Thus, the Mobile IP Home Agent should be placed in a central location such as the operator's network or close to the corporate IT infrastructure.

In order to keep the handover time within practically feasible limits, we recommend tuning DHCP servers for fast operation, make sure mobile terminals use interfaces with fast detection of link status, and use WLAN chipsets and corresponding drivers that can scan for new SSIDs without interrupting existing WLAN sessions. Finally, the HA should be placed in a central location, either in the operator core network, or in the enterprise DMZ (Demilitarized Zone) to reduce latency. For operation in global organizations, we recommend providing multiple HA's, one in each geography so all users can reach their HA with minimum latency.

IV. Conclusion

We have shown how a Mobile IP-based service can provide seamless roaming with VPN-based security in an Open Broadband Access Network. Seamless mobility is provided by support for automatic authentication and improved handover speed by using Mobile IP Foreign Agents in Residential Gateways in homes with overlapping WLAN coverage areas. 3G has been used as an overlay network, and provides network access in areas where WLAN is not available. The system provides automatic selection of network access according to enterprise or operator preferences that can be changed dynamically. Support for automatic VPN on/off features enable use-cases where users also access network resources from a secure WLAN within an enterprise (where VPN is not used), via roaming using 3G network access, over to public and residential WLAN hotspots in the Open Broadband Access Network [Figure 1]. We have also shown how standard business applications remain uninterrupted as users move their terminal between networks, and have verified that even VoIP is possible, although with minor interruptions due to buffer under run. We have analyzed handover times, and reported that the basic Mobile IP handover is done in less than 100 milliseconds. We have also identified terminal and infrastructure-specific aspects which can increase the practical handover time to more than a second, and how this can be avoided by tuning network parameters.

References

[1] OBAN Project Website: http://www.ist-oban.org/

[2] C. Perkins, "IP Mobility Support for IPv4", *RFC 3344*, IETF, Aug. 2002

[3] D. Johnson et al., "Mobility Support in IPv6", *RFC 3775*, June 2004

[4] J. Rosenberg et al., "SIP: Session Initiation Protocol", *RFC 3261*, June 2002

[5] 3rd Generation Partnership Project (3GPP), Technical Specification Group Services and System Aspects; Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking, release 6. 3GPP TS 22.234, Version 6.2.0, September 2004

[6] 3rd Generation Partnership Project (3GPP), Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking, release 6. 3GPP TS 22.934, Version 6.2.0, September 2003

[7] T. Dagiuklas et al., EVOLUTE Architecture Specification, Deliverable D2.1, EVOLUTE, IST-2001-32449, September 2002

[8] H. Bryhni, Public WLAN and seamless, secure mobility over public and enterprise networks as foundation for 4G, Proceedings of 15th workshop on Telecommunications: Mobile Internet, Slovenia 17.11. - 18.11.2003