Extending 3G/WiMAX Networks and Services through Residential Access Capacity

Frans Panken and Gerard Hoekstra, Alcatel-Lucent, Bell Labs
Delphin Barankanira, France Telecom R&D
Charles Francis and Rico Schwendener, Swisscom Innovations
Ole Grøndalen, Telenor
Martin G. Jaatun, SINTEF ICT

ABSTRACT

The transmit capacity of the access link that connects homes to the Internet is often not fully used, either because of a selected light subscription or because the user is not constantly online, leaving a surplus capacity. Many home networks are equipped with WLAN that can be received outside the walls of the home. This signal can be used to offer access to passing WLAN users who are sufficiently near the homes, potentially realizing a contiguous public radio coverage landscape of WLAN access points in urban areas. This article describes the challenges and solutions when using the surplus capacity available in broadband residential access for offering WLAN access to public subscribers, and how to integrate this solution with access and services offered by 3G and WiMAX.

INTRODUCTION

The wireless telecom industry has mainly concentrated on second generation (2G) and third generation (3G) solutions that operate in licensed frequency bands. On the other hand, the unlicensed frequencies used in wireless local area networks (WLANs) have been applied successfully as home and last mile technology in the increasingly pervasive computing environments where mobile users access Internet services. Commercially available dual-mode handsets enable mobile telephone users to save money on their phone bills when in range of a WLAN access point. Alternatively, the WLAN interface on these phones can be used as a layer 2 carrier of GSM signals, improving indoor GSM coverage [1]. Public WLAN is mainly offered by various standalone companies (scratch cards, coffee shops, airports), scattering the user’s subscriptions among various companies, which introduces a threshold for using it. The integration of WLAN in 3G devices as well as the convergence of various access network technologies indicate that WLAN is no competitor for 3G, and the unlicensed WLAN spectra can become an important and cost-effective supplement to offer network access. As a result, WLAN equipped home network facilities may become an interesting asset for fixed-wireless convergence and have the potential to realize a large international WLAN network, solving the scattered subscriptions with minimum investments.

One of the challenges in using the residential network for public access is realizing this without replacing existing home gateways, exploiting the residential equipment as is. Companies such as Google/FON apply this idea, sometimes including the offering of firmware upgrades of popular WLAN equipment to improve security or separate residential traffic from visiting traffic. The drawback of their solution arises from the fact that they exclude the access network provider and Internet service provider of the residential user from their business, lacking the potential integration when offered in conjunction with 2G/3G networks and/or WiMAX. In addition, neither quality of service (QoS) nor mobility is solved in these initiatives. Quality of service mechanisms are needed to realize continuous but bounded network consumption for public users, and also to prevent public users from dominating the wireless access network, keeping the effects on residential users within controllable limits. Network coverage planning should ensure that the unlicensed WLAN spectrum is used efficiently and without the need for manual optimization. Before mobility across a landscape of WLAN equipped houses can be realized, issues such as network discovery and seamless handovers between neighboring access points need to be solved.

The business cases of offering public WLAN by making use of residential access facilities are
studied in [2–4]. In these studies the incentive of the residential user to cooperate is always key, and rewards for this cooperation include payments or free access through access points of other participants. The software operated on the residential gateway could come from the operator environment, which makes it manageable for frequency planning, security, and QoS purposes. Ownership of the residential equipment by the service provider is not compulsory. The integration of offering residential WLAN access in combination with 3G and/or WiMAX broadens the access landscape for communication services and differs from extending the unlicensed mobile access technology [1].

The remainder of this article is organized as follows. The next section mentions the requirements and explains the solutions for offering network access to public users through residential WLAN. We then explain how to integrate these solutions with 3G and WiMAX access and services. The final section draws conclusions.

**ESSENTIAL FUNCTIONALITIES**

Home network facilities consist of a router and a modem, together referred to as the residential gateway (RG). In addition, a WLAN access point is present, which may be external or integrated in the RG. The RG can also offer services. The areas that require solutions before public network access can be offered through residential WLAN include mobility, security, and QoS; each is discussed separately below.

**MOBILITY**

While users roam in the public environment, radio conditions will eventually deteriorate as the distance from the access point increases, and consequently the desired network connectivity degrades or may no longer be available. The relatively small cell size offered by WLAN technology makes handover essential. Apart from finding neighboring access points, deciding when to perform a handover and determining the preferred AP are challenging. The optimum handover decision is likely to take into account information residing in both the network and the mobile terminal (MT). In addition, the tree-shaped residential broadband access network prevents RGs communicating directly via the fixed infrastructure; hence, applying standard handover solutions is likely to result in unacceptably long handover times.

**Handover Mechanisms** — The handover procedure is basically divided into three phases: information gathering, handover decision, and actual handover. During the information gathering phase, the MT collects information about the handover candidates, and authentication tickets are acquired for security purposes. In the second phase the best handover candidate is determined. Finally, after deciding on the actual handover, the MT associates with a new AP and initiates a fast re-authentication procedure based on the exchange of a security ticket and subsequently performs a Mobile IP (MIP) binding update.

To identify handover candidates during the information gathering phase, the MT listens for the medium access control (MAC) address of neighboring access points. Accordingly, to ascertain the capabilities of potential handover candidates, the association to the current access point is maintained, and its associated RG is used to interrogate potential handover candidates. The information exchange can be implemented using Candidate Access Router Discovery (CARD), as described in RFC 4066 and [5]. The CARD protocol allows MTs to resolve the IP addresses of the associated RG by sending the layer 2 identifier of an access point to a CARD server.

The handover decision phase identifies whether handover should take place and, where more than one handover candidate is available, identifies the best one. Factors involved in determining an optimum handover include the resource needs of the MT, the circumstances pertaining to candidate residential networks, the residential subscription, the maximum capacity available in the local loop, and conditions on the radio interface of the candidate access router. Tariff issues may be important, and the policy of the service provider may also be relevant. For example, in a heterogeneous environment with umbrella cellular coverage, mechanisms may ensure that non-real-time low-margin high-bandwidth traffic is kept out of the premium cellular network and preferentially routed over the fixed network. Other potential factors to consider include the extension of battery life on the MT, avoiding interference between MTs, and load balancing to avoid crowding in specific residential cells.

**Architecture** — Since the WLAN cells are relatively small, handovers are expected to occur frequently. This raises the need for a new regional node that integrates functions such as locating the APs, the RG associated with each AP, and part of the functionality that speeds up the re-authentication of the public user to achieve faster handover. This node is called a mobility broker (MB). The MB is intended as a regional trusted supervisory entity, managing and controlling resources as well as handling cross-domain handovers for a public user. It facilitates the fast authentication scheme, which is a prerequisite for the fast handovers needed by, for example, interactive streaming services. The functionality needed to realize the mobility mechanisms described before are located in the MT, RG, MB, and the domains of the Internet service providers (ISPs) of residential and public users (Fig. 1).

The CARD client in the MT issues requests to the CARD server in order to retrieve information about the neighboring APs. In the RG a CARD proxy is used to relay CARD requests to the MB, where a CARD server resolves available resources and capabilities of the observed APs, and replies to inquiries from CARD clients. The MB also caches user related information, such as user profiles, and generates security tickets used for fast authentication, realizing handoffs more seamlessly. By offering foreign agent gateway functionality, the MB also serves as a gateway foreign agent (a regional home agent), which speeds up the MIP binding updates.
other components shown in Fig. 1 will be explained in the remainder of this article.

SECURITY
The security objective is to develop a secure solution for public access to private WLANs and private broadband access lines. The goal is to ensure privacy for all users and optimal usage of network resources, but at the same time ensure that residential subscribers do not experience any degradation in security and privacy level. Relevant security services include mutual authentication of users vs. the network, access control, as well as confidentiality, encryption, and integrity protection of the data flow. It must not be possible to eavesdrop on wireless users; hence, mechanisms that ensure the confidentiality of information sent over the air interface are needed.

Security Mechanisms — Supporting mobility between neighboring homes without jeopardizing the security level places restrictions on how much time security mechanisms such as reauthentication can consume as part of the handover.

To ease GSM/Universal Mobile Telecommunications System (UMTS) integration, Extensible Authentication Protocol (EAP)-SIM (EAP-AKA) has been chosen as the primary authentication mechanism for public subscribers. This effectively reuses an accounting, authorization, and authentication (AAA) infrastructure that would be present in any enterprise network, but introduces a few extra hops.

Authentication relies on existing long-term trust relationships between the MB and all access points in its cell, between the MB and all ISPs in its cell, and bilaterally between all participating ISPs (this latter relationship is orthogonal to current roaming agreements between, e.g., GSM operators).

When an MT first joins the network (i.e., when it is turned on), it must perform a full EAP-SIM authentication proxied from RG to MB, then to the residential subscriber’s ISP, and finally to the public subscriber’s ISP. As a by-product of the authentication process, EAP-SIM generates a shared secret between the public subscriber and the public subscriber’s ISP. This shared secret is then passed down the line to the RG. Once the dynamic shared secret reaches the RG, it represents a dynamic trust relationship between the MT and the RG. On the practical side, it also means that the MT of the public user and the RG now have a (dynamic) shared symmetric encryption key, which is used to encrypt the wireless traffic. Details on protection and how rogue RGs can be spotted and addressed are described in [6].

Since the MT and access points do not have a preexisting trust relationship (and thus no long-term shared secret), the MT has to rely on the chain of trust described above. All data to be transmitted is expanded with a message integrity check (MIC) before encryption. When the MT decrypts the received data using the dynamic shared secret, it also verifies the MIC. A correct MIC implies that the RG most likely has possession of the dynamic shared secret; this proves to

---

1 For our purposes, a “trust relationship” can be read as a “shared secret.”

---

Figure 1. Functional architecture to open residential access facilities for public usage.
the MT that the RG is legitimate, and represents an implicit authentication of the access point.

By using different service set identifiers (SSIDs) for public and residential users, the IEEE 802.11 WLAN can be split into two separate virtual WLANs, each with their own security and encryption solution, which minimizes changes for residential users.

**Fast Authentication for Handover** — A full EAP-SIM multi-actor round-trip takes too long to support handovers for interactive services. Thus, a separate authentication technique specifically for fast handovers is required.

When the MT has a list of access points from CARD as described earlier, it requests the MB for a Kerberos-style ticket to the most likely candidate(s) (see [7] for more details). The MB is able to create such a ticket since it shares a secret with every RG and uses this secret for ticket encoding; the ticket itself can only be decoded by the respective RG. Once in possession of a ticket, the MT may perform the handover directly to the corresponding access point, and when layer 2 connectivity is established, the MT will offer the ticket to the RG. The ticket can be decoded locally on the RG and verified without involving any other actors; this implies that the handover authentication will be dramatically faster than a full EAP-SIM authentication. Subsequent to ticket verification on the RG, the MT will be granted layer 3 connectivity, and can proceed to update MIP information in the network. Note that the MT can start transmitting traffic almost immediately after associating with the new access point, but receiving traffic requires an update in the gateway foreign agent, located in the MB, with the new IP care-of address obtained as part of the handover.

**QoS**

The QoS objective is to achieve efficient network resource utilization and meet the throughput desires of users at the same time. The shared nature of the wireless medium (in an unlicensed spectrum) poses several challenges, including:

- Available resources may vary due to interference or unfavorable channel conditions of individual users, and should be shared among all stations in an efficient manner based on a user’s subscription.
- Resource consumption in the (wireless) access network should be predictable. This requires proper assignment and control of resources to each MT.
- The admittance of visiting users should be limited so that an acceptable and configurable level for residential users can be realized.
- Data originating from and destined to visiting users should be separated from residential traffic.
- The solution should fit within, but not require, the current QoS solutions offered by the IEEE 802.11e standard.

One aspect of realizing QoS is to distinguish various priority classes. If the traffic ingress volume of a network exceeds the amount that can be processed, these mechanisms are not sufficient, and QoS degradation is inevitable. This is why — besides priority — QoS solutions must include indications about volumes, specified in a traffic contract or service level agreement (SLA). The SLA determines how much traffic the parties can offer to a network. When combining traffic differentiation with SLA agreements, parties are free to operate, each within the given SLA, without affecting others. Various QoS policies can be applied to define prioritization levels for the most valued traffic (e.g., different classes of public users, prioritize residential users and allocate remaining capacity for public users, prioritize the MT closest to the AP).

In WLAN systems, the terminology load requires special attention, as the overhead of one station depends on its transmission speed and WLAN standard, and those of all other stations associated to the access point. The load on a WLAN medium cannot be uniquely determined by the data rate alone; hence, QoS traffic profiles are introduced to overcome this. A QoS profile describes the traffic SLA, defined by the average number of packets per second sent on the IP layer in the upstream and downstream directions, combined with the average number of bytes in these packets. The set of QoS profiles describes the traffic subscription of a user, retrieved from the network as part of the authentication process. Based on a combination of the QoS profiles and the current resource planning status, the conclusion can be drawn whether a user can be granted access or not (see [8] for details). If access can be granted, two QoS profiles from the set are assigned to the user, a committed profile and a peak profile.

Additional requirements to the resource planning in WLAN networks are imposed as stations may perform rate adaptation, and thereby affect the medium capacity and thus the available resources of all users associated. To counteract these and other unforeseen events (e.g., SLA contract violations by users), the QoS solution monitors the channel conditions and user traffic to take measures when traffic contracts may be jeopardized. A total of three QoS entities are defined, located in the MT (QoSMT), the RG (QoSG), and the ISP offering public access through residential WLAN (QoSRG). These QoS entities communicate to determine and achieve the desired QoS level of the users in the network. Before users gain network access, their QoS profiles must be obtained. If the RADIUS protocol is used for authentication, vendor-specific attributes are intercepted by QoSRG to obtain the set of QoS profile information sent by QoSISP. From this set of QoS profiles, QoSRG will select one profile to be committed and derive the minimum WLAN data rate needed for using this profile. The QoS profiles selected by QoSRG are communicated to QoSMT. Consequently, the MT is held accountable for not exceeding the selected QoS profile and is policed on this limit. Traffic shaping in the MT prevents packets from being deleted. In turn, QoSRG monitors at each committed QoS profile by monitoring the channel conditions, and the individual user’s data rate and traffic consumption. An MT moving away from the AP likely adapts its rate, consequently increasing WLAN airtime consumption substantially. By defining each MT’s
traffic SLAs at the IP level, the WLAN airtime increase does not necessarily jeopardize the SLA, and relatively high airtime consumption can be tolerated as long as it does not endanger the desires of other MTs. If a medium overload occurs, QoS_RG redistributes the network resources and may update the affected QoS_MT with their newly assigned profiles and rates.

**COUPLING WITH 2G/3G AND WiMAX**

This section describes how the solution that takes advantage of the surplus capacity available in the residential broadband access can be integrated in 3G networks and how it can be beneficial for WiMAX operators.

**WLAN ACCESS INTERWORKING WITH 3G**

The integration of the residential WLAN solution with 3G should use the standardized concept of WLAN interworking (3GPP TS23.234) to authenticate, account for, and bill users while enabling them to roam freely across RGs. With the proposed solution, public WLAN users can access 3G packet-switched (PS) services via the residential WLAN network.

**3G Packet-Switched Services Access** — Figure 2 presents the proposed architecture to provide interworking with 3G networks and allow WLAN users to access 3G packet services such as messaging, data access, voice communication, video communication, and proximity information. Access to the 2G/3G network in residential WLAN scenario can only be achieved through the 3G packet data gateway (PDG) by respecting the security policies in the virtual private network (VPN) device and/or firewall. This can be realized by either broadcasting a special SSID, or allowing the user to select the desired service (offered and proxied by the RG). In the second option, authentication starts after the selection. When the MT is authenticated and authorized to the 3G operator, it establishes an end-to-end tunnel with the PDG that supports the desired services; see 3GPP TS23.234 for more details. Mobile IPv4 and VPN technologies have to coexist and function together to provide mobility and security to public WLAN users.

To achieve seamless mobility, two integration solutions of MIP (MIP RFC 3344) and IPSec (RFC 4301) are possible:

- **MIP encapsulated inside IPSec:** The drawback of this solution is that IPSec MIPv4 packets cannot be processed by the foreign agent (FA). If no FA is used, the VPN tunnel needs to be re-established when the MT moves from one RG to another.

- **IPSec encapsulated inside MIP:** This solution avoids the aforementioned problems, and allows the home agent (HA) to be assigned dynamically as described in RFC 4433. The FA is able to forward MIP registration requests and replays to the HA. Nevertheless, the MIP extensions as defined in RFC 3519 [9] should be used for network address translation (NAT) traversal, and the RG firewall should be configured to allow MIP message exchange.

The second solution was chosen for achieving mobility between neighboring RGs, establishing the MIP tunnel between the MT and the HA. When using the residential WLAN network to access a 3G packet data network (PDN), a MT shall use two IPv4 addresses (IPv6 optional): its local IP address (WLAN) and home IP address (3G). The IPSec tunnel is built between the MT and the PDG, using the home address of the MT for security associations. Since the MT’s home address does not change during or after handover, the associations do not need to be updated; hence, mobility does not affect the IPSec tunnel. As MIP is the only layer involved in the handover process, the session will not be interrupted, and only the MIP care-of address will be updated. Figure 3 shows how IPSec is encapsulated inside MIP.

More than one WLAN network may be observed by an MT. For each available SSID, the MT may obtain a list of supported public land mobile networks (PLMNs) from the MB (during association but also as a result of handoff). This requires knowledge of SSIDs associated with 3G services to resolve the appropriate
candidate APs. The integration of WLAN with the 3G network should not compromise the 3G security architecture. The requirement on the serving WLAN network is to support IEEE 802.11i features. Also, MT and AAA proxy in the RG needs to support EAP-SIM (EAP-AKA) to realize the authentication.

INTEGRATION WITH WIMAX

Integrating residential WLAN networks with WiMAX networks can be beneficial for both WiMAX operators and operators offering network access to public users through residential WLANs (WLAN network operators). A WLAN network operator can use a WiMAX network as an overlay to provide continuous coverage in an area. On the other hand, a WiMAX operator can use a WLAN network to offload the WiMAX network in urban areas with heavy traffic. In this way the WiMAX operator can serve more customers with a given amount of spectrum, using the spectrum more efficiently and reducing costs for both the operator and its customers.

INTEGRATION WITH WIMAX

Integrating residential WLAN networks with WiMAX networks can be beneficial for both WiMAX operators and operators offering network access to public users through residential WLANs (WLAN network operators). A WLAN network operator can use a WiMAX network as an overlay to provide continuous coverage in an area. On the other hand, a WiMAX operator can use a WLAN network to offload the WiMAX network in urban areas with heavy traffic. In this way the WiMAX operator can serve more customers with a given amount of spectrum, using the spectrum more efficiently and reducing costs for both the operator and its customers.

Integration from a WLAN Operator’s Point of View — Figure 4 shows a possible architecture for the case where a WLAN network operator uses WiMAX to obtain continuous coverage in an area. In the simplest case the WiMAX network is deployed by the WLAN network operator and consists of a single base station (BS) that covers the same area serviced by a single MB.

The WiMAX network can also be operated by a separate operator and consist of several WiMAX BSs connected to an access service network (ASN) gateway (GW). In this case the WiMAX BSs are also connected to the WiMAX service provider’s network, possibly through connectivity service networks (CSNs) of visited service providers.

The WiMAX-WLAN gateway (WWGW) glues the WLAN and WiMAX parts of the network together. The WWGW communicates with the ASN GW using the protocols that will be defined by the WiMAX Forum for communication between an ASN GW and a CSN. The WWGW basically makes the WiMAX ASN look like an RG to the WLAN network.

Mobility can be implemented with MIP signaling, just as for the pure WLAN and integrated 3G network cases. An MT must scan both the WLAN and WiMAX air interfaces to make a list of potential APs and BSs to which it can switch, and the WWGW must include a CARD server or CARD proxy.

The MB must be able to resolve how much uplink and downlink capacity has been allocated to WLAN users in the WiMAX ASN. This can be realized relatively easily by instructing QoSRG to send the committed and peak QoS profile information and updates not only to QoSMt but also to the MB.

Integration from a WiMAX Operator’s Point of View — Figure 4 shows a possible architecture for the case where a WiMAX operator uses a WLAN network to offload the WiMAX network in an area with heavy traffic. Again, a WWGW glues the WiMAX and WLAN parts of
In this architecture the WWGW makes the WLAN network looks like a WiMAX ASN to the WiMAX network and handover implies re-anchoring the current FA to a new FA and the consequent binding updates to update the upstream and downstream data forwarding paths.

In the simplest case the WLAN network is deployed by the WiMAX operator. The WLAN network can also be operated by another operator. In this case the WLAN will also be connected to the WLAN service provider’s network.

In this architecture the WWGW makes the WLAN network look like a WiMAX ASN to the WiMAX network, and handover implies re-anchoring the current FA to a new FA, and the consequent binding updates to update the upstream and downstream data forwarding paths. It is also possible to use the WiMAX inter-ASN interface R4 to keeping existing anchor ASN GW or re-anchor at the WWGW.

Concurrent Access to WiMAX and WLAN Networks — An attractive solution for reducing the handover latency between WiMAX and WLAN networks is to let MTs use the WLAN and WiMAX radio interfaces simultaneously. One variant of this solution is to let MTs always be connected to the WiMAX network and connected to the WLAN network when this is available. To reduce an MT’s power consumption, the MT could enter WiMAX sleep mode whenever it is connected to the WLAN network. MTs for which power consumption is not important (e.g., car mounted MTs) could use both air interfaces actively whenever possible and vehicle speeds allow. Then services could be mapped to different air interfaces depending on their requirements. Capacity adaptation (e.g., when the WLAN link quality is reduced) can be implemented by selective handover between the WiMAX and the WLAN, where the decision to move a session to the other air interface depends on the supported service.

Conclusions

By using different SSIDs, an IEEE 802.11 WLAN can be split into two different separate virtual WLANs, effectively separating public and residential traffic. Each virtual WLAN can have its own security solution, where communication with the home network is a prerequisite for public users. Several technologies can be used to continue the separation within the fixed access infrastructure (e.g., virtual LANs, multiprotocol label switching, and separate asynchronous transfer mode private virtual circuits).

A service provider that supports residential access for public users stores their authentication passwords and QoS profile information. An entity that serves in a regional trusted supervisory role was considered indispensable and named mobility broker. The mobility broker manages and controls equipment in the residence and is also involved in realizing fast cross-domain handovers for public users. Mobility, QoS, and security are intertwined throughout the architecture: mobility is performed based on QoS information obtained from the network, and QoS functionality intercepts security requests and replies to have a
means to admit or reject users, while the security messages exchanged between the home gateway and the AAA server are used to pass QoS subscription information. Finally, the security solution in the mobile terminal takes advantage of the presence of a list of nearby access points resolved as part of the mobility solution and requests security tickets from the mobility broker in advance of an anticipated handover.

The architecture was designed with security solutions in mind and the purpose of providing a secured architecture, preventing security flaws when introduced in the 3G network. Since the proposed solution to extend 3G and WiMAX with residential access has minimal impact on existing WLAN networking, existing client WLAN equipment can be used. The proposed solution allows 3G session continuity to WLAN users when they make a handover. Also, route optimization and use of regional registration is possible, at the expense of the ease of IPv4–IPv6 migration. Finally, the article shows the potential of the integration of WiMAX and residential WLAN access as well as the win-win situation for both WLAN and WiMAX operators.

ACKNOWLEDGMENTS

The work reported in this article was supported in part by the IST 6FP program of the European Commission under contract OBAN, No. 001889, with the participation of Swisscom Innovations partially funded by the Swiss Bundesamt für Bildung und Wissenschaft.

REFERENCES


BIOGRAPHIES

FRANS PANKEN (Frans@alcatel-lucent.com) works as a senior member of technical research staff at Alcatel-Lucent, Hill-versum, the Netherlands. He holds an M.Sc. degree in applied mathematics and a Ph.D. degree in computing science, and his research interests include stochastic modeling and performance analysis of telecommunication networks and mobile networks.

DELPHIN BARANKANIRA (delphin.barankanira@orange-ftgroup.com) received his M.S. degree in telecommunications at ESIGELEC, a graduate school of electrical engineering in Rouen, France, in 2005. He is currently working as an R&D engineer at Orange Labs, France, since 2005. His research interests include convergence, mobility, and security for heterogeneous access networks including WLAN, WiMAX, and mobile networks. He is currently involved in the 3GPP standardization work on the evolved packet core and IMS.

MARTIN GIJE JAATUN (Martin.G.Jaatun@sintef.no) is a research scientist at SINTEF ICT, Trondheim, Norway, where he heads a research group on information security within the Department of Software Engineering, Safety and Security. He received a Master of Science degree in telematics from the Norwegian Institute of Technology (NTN) in 1992.

GERARD HOEKSTRA (gjhoekstra@alcatel-lucent.com) received his M.Sc. (cum laude) degree in electrical engineering in 1999 from the University of Twente, the Netherlands, and is involved in a Dutch government funded research program, Casimir, to attain his Ph.D. degree. After working for Alcatel’s Corporate Research Centre in Antwerp, he joined Lucent Technologies in 1999 and is currently a member of technical staff in the Bell Labs Europe department of Alcatel-Lucent.

OLE GRØNDALEN (ole.grondalen@telenor.com) received a Master of Science degree in physics from the University of Oslo, Norway, in 1987. Since then he has been working on development of interactive broadband satellite and radio systems at Telenor Research & Innovation. He has participated in several international cooperative research projects within the European Commission framework programs focusing on broadband radio access systems.

JOHN CHARLES FRANCIS (JohnCharles.Francis@swisscom.com) is a senior project leader at Swisscom Innovations, and holds a Ph.D. in electrical and electronic engineering. He has been active in the field of 3G mobile standardization, and his research interests include systems beyond 3G. In addition to managing innovation projects, he has supported Swisscom UMTS and WLAN hotspot deployment, and coordinated Eurescom consortia in the mobile area. Within the EU OBAN project, he led the work on scenarios and requirements.

RICCO SCHWENDENER (Rico.Schwendener@swisscom.com) is head of a Competence Team at Swisscom Innovations. He holds a Ph.D. in technical science and a post-diploma degree in information technology. He has been active in the field of network modeling for carrier grade networks. His research interests have included open broadband access networks, QoS in mobile networks, and cross-layer optimizations. In addition to managing innovation projects, he has supported the Swisscom Triple Play architecture development.