telektronikk 1.07

Personal Networks

Telektronikk
Volume 103 No. 1 – 2007
ISSN 0085-7130

Editor:
Per Hjalmar Lehne
(+47) 916 94 909
per-hjalmar.lehne@telenor.com

Editorial assistant:
Gunhild Luke
(+47) 415 14 125
gunhild.luke@telenor.com

Editorial office:
Telenor R&I
NO-1331 Fornebu
Norway
(+47) 810 77 000
telektronikk@telenor.com
www.telektronikk.com

Graphic design:
Design Consult AS (Odd Andersen), Oslo

Layout and illustrations:
Gunhild Luke and Åse Aardal,
Telenor R&I

Prepress and printing:
Rolf Ottesen Grafisk Produksjon, Oslo

Circulation:
3,700

Networks on networks

Connecting entities through networks – in technological, societal and personal terms – enables telecommunication. Networks occur on different levels, form parts of larger networks, and exist in numerous varieties. The artist Odd Andersen visualises the networks on networks by drawing interconnected lines with different widths. Curved connections disturb the order and show that networks are not regular but are adapted to the communication needs.

Per H. Lehne, Editor in Chief

Contents

Personal Networks

Status

Guest Editorial – Personal Networks

RAMJEE PRASAD

Ramjee Prasad is Director of Center for Teleinfrastruktur (CTIF) at Aalborg University, Denmark

Danish King Harald Blåtand – for whom, a thousand years later, Bluetooth for wireless personal area networks was named – is known for uniting parts of Sweden, Denmark and Norway. Uniting computers, mobile phones, and personal devices is the goal of Wireless Personal Area Networks (WPANs), which are meant to become a major part of future mobile communication networks and the future generation (FG). This introduction provides an abstract view of what a WPAN is, or should look like.

The Personal Area Network (PAN) is a network for *you*, for *you and me*, and for *you and the outer world*. It is based on a layered architecture where different layers cover the specific types of connectivity (see Figures 1 – 3).

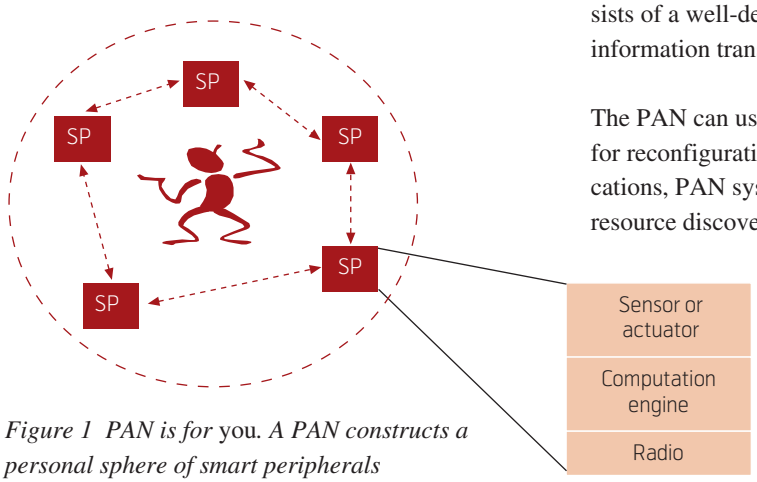


Figure 1 PAN is for you. *A PAN constructs a personal sphere of smart peripherals*

This connectivity is enabled through the incorporation of different networking functionalities into the different devices. So, for the stand-alone PAN, the person is able to address the devices within his personal space independently of the surrounding networks. For direct communication of two persons (i.e. their PANs), the bridging functionality is incorporated into each PAN. For communication through external networks, a PAN implements routing and/or gateway functionalities.

Layer-oriented scalable architecture supports the functionalities and protocols of the first three layers and provides the capability to communicate with the external world through higher layer connectivity. It provides the appropriate middleware structures and consists of a well-defined protocol stack, with identified information transfer through appropriate interfaces.

The PAN can use various access technologies, calling for reconfiguration. Moreover, according to the applications, PAN systems provide automatic service and resource discovery, provide QoS (e.g. for multimedia applications), and are scalable in t erms of network size.

PAN invisibility is essential to the user, and so, PAN devices are able to adapt themselves automatically to the environment and can, for

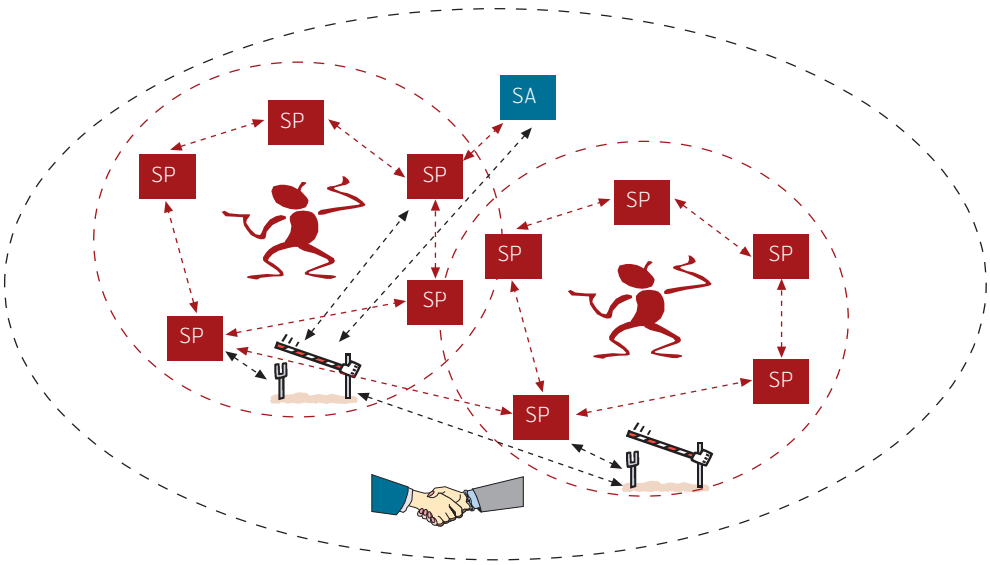


Figure 2 PAN is for you and me. *When people and appliances meet, PAN becomes a dynamic distributed application platform where gatekeepers are needed*

ISSN 0085-7130 ©Telenor ASA 2007

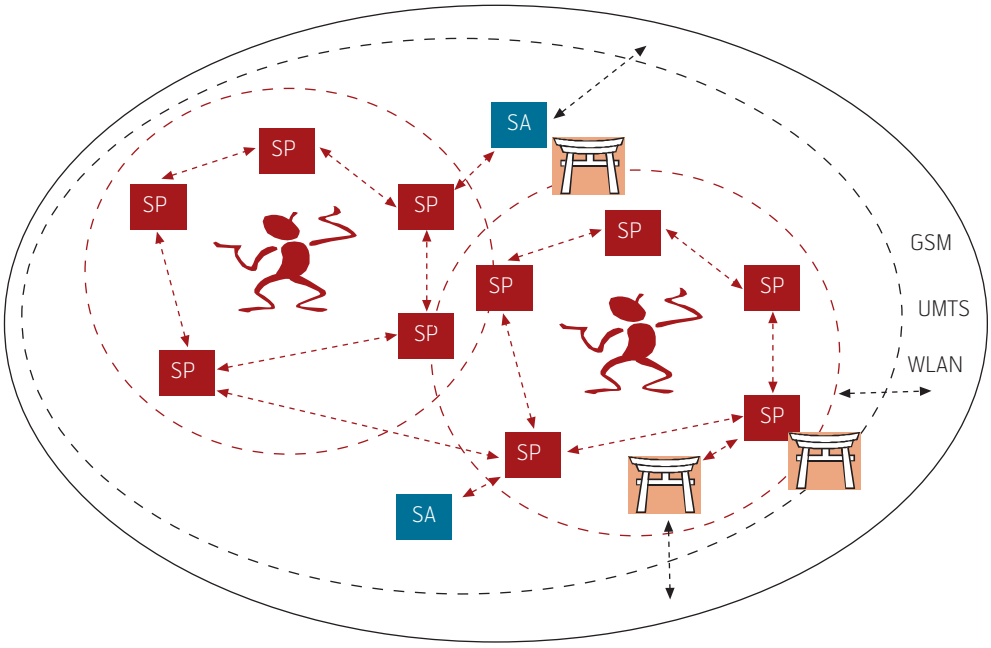


Figure 3 PAN is for you, me, and the outer world. *Extending your reach requires a multimedia gateway as well as a distributed resource control with Quality of Service (Qos). (GSM: Global System for Mobile communication, UMTS: Universal Mobile Telecommunications System)*

example, download the appropriate applications and access techniques automatically.

Frequency planning and coexistence with the existing systems is important for designing novel PANs. PAN-oriented applications mostly use the unlicensed frequency bands. For the higher data rates, the 5 GHz frequency band, and possibly the 60 GHz, can be used (Figure 4).

The concept of the personal network (PN) goes beyond the commonly accepted concept of a PAN. The latter refers to a space of small coverage around the person where ad hoc communication occurs. This is also referred to as a personal operating space (POS). PNs extend the local scope of PANs by addressing virtual personal environments that span a variety of infrastructures (as well as ad hoc networks). Even though we have described the PAN view as addressing the problem of the communication between *you and the outer world*, PN extends the PAN concept even further, as the POS can be distributed all over the world. Figure 5 illustrates the concept of personal networks. An important new element suggested by the figure is that the composition, organisation, and topology of a PN are determined by its context. By this we mean that the geographical location of a person, the time of day, the electronic environment, and the explicit or implicit wishes to use particular services determine which devices and network elements will be incorporated in a PN.

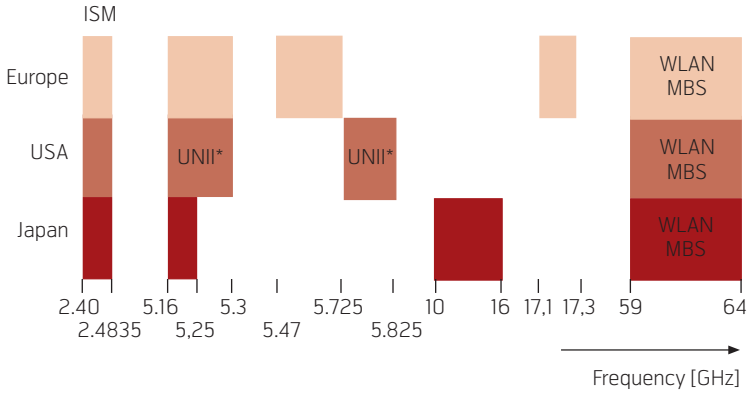


Figure 4 Frequency bands (MBS: Mobile Broadband System, UNII: Unlicensed National Information Infrastructure)

ISSN 0085-7130 ©Telenor ASA 2007

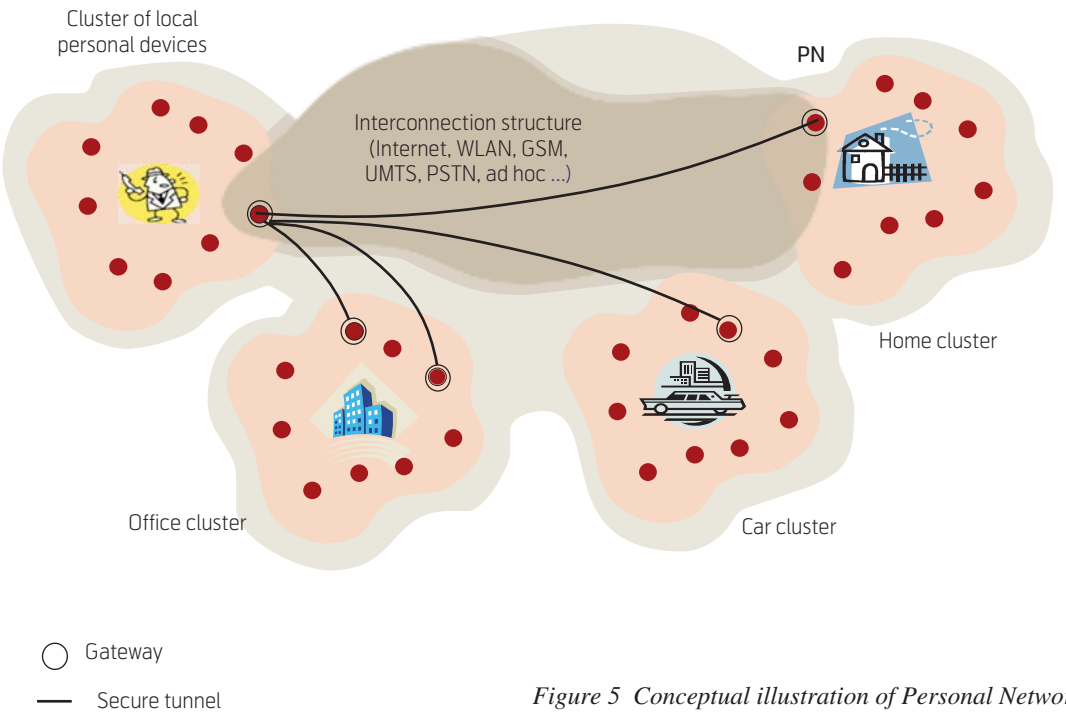


Figure 5 Conceptual illustration of Personal Networks

The present issue is composed of 12 contributions that cover the results of PACWOMAN (Power Aware Communications for Wireless OptiMised personal Area Networks, URL: http://www.imec.be/pac-woman/), MAGNET (My personal Adaptive Global NET, URL: http://www.ist-magnet.org), and MAGNET Beyond (My personal Adaptive Global NET Beyond, URL: http://www.ist-magnet.org).

The personal network is the future for the wireless and the mobile communications. In the view of the author, future generation (*FG*) can be defined by the following equation:

$$B3G + PN \triangleq FG$$

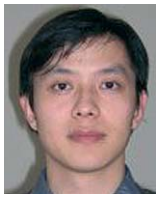
where *B3G* stands for beyond third generation, which is defined as the integration of existing systems to interwork with each other and the new interface.

Ramjee Prasad is a distinguished educator and researcher in the field of wireless information and multimedia communications. Since June 1999, Dr. Prasad has been with Aalborg University, where currently he is Director of Center for Teleinfrastruktur (CTIF), and holds the chair of wireless information and multimedia communications. He is coordinator of European Commission Sixth Framework Integrated Project MAGNET (My personal Adaptive Global NET) Beyond. He was involved in the European ACTS project FRAMES (Future Radio Wideband Multiple Access Systems) as a Delft University of Technology project leader. He is a project leader of several international, industrially funded projects. He has published over 500 technical papers, contributed to several books, and has authored, co-authored and edited 20 books. He has served as a member of the advisory and program committees of several IEEE international conferences. In addition, Dr. Prasad is the coordinating editor and editor-in-chief of the Springer International Journal on Wireless Personal Communications and a member of the editorial board of other international journals. Dr. Prasad is also the founding chairman of the European Center of Excellence in Telecommunications, known as HERMES and is now the Honorary Chair.
Dr. Prasad has received several international awards; the latest being the Telenor Nordic 2005 Research Prize. He is a fellow of IEE, a fellow of IETE, a senior member of IEEE, a member of The Netherlands Electronics and Radio Society (NERG), and a member of IDA (Engineering Society in Denmark).
Dr. Prasad is advisor to several multinational companies.

email: prasad@es.aau.dk

Wireless Personal Area Networks – The PACWOMAN Vision

YAODA LIU



Yaoda Liu is a PhD candidate at Aalborg University, Denmark

Together with the advance of wireless communication technology, the person centered network concept has been evolving to the concept of Wireless Personal Area Network (WPAN) in the last decade. WPAN is foreseen to bring new services to the user and improve our daily life. For researcher and network operator, a promising area has been opened up. In this paper, we introduce our vision on future Wireless Personal Area Network developed in a pioneer project in this field.

1 Introduction

During the last decades, we have seen the explosive development of wireless communication technologies. Many technologies have been brought to our daily life and have been proven to be successful, e.g. GSM and WLAN. And many more technologies, such as UMTS and WIMAX are on the way to commercialization world-wide and hopefully to a success. At the same time, the networking technology for wireless communication is paving the way for a new paradigm, i.e. from the model of fixed–mobile to the model of mobile–mobile. With such a model, many networking technologies are being developed, e.g. wireless mesh networks, mobile ad hoc networks, wireless sensor networks. With all these technologies, a wireless terminal is enabled to communicate with other wireless terminals directly without sending traffic through an intermediate node connected to the wired network.

From the success of GSM and WLAN, it is not difficult to conclude that the service enabled by the technologies for the end user is a key factor for the success of a technology. Following this logic, there has been a strong consensus on the requirement for new technologies:

- *Person Centered:* Technologies should be centered on the user, improving quality of life and adapting to the individual. While the traditional communication paradigm aims to establish the communication link between devices, the focus now shifts to the communication among the persons and services.

- *Pervasive Service:* The communication and computing technology will tend towards "invisibility" and "calmness" [1]. The offered services tend to be pervasive, causing minimum distraction to the user with respect to their configuration and usage. The computing environment is becoming smarter and more responsive, with devices being able to establish disposable, seamless connection to the required resource.

The concept of wireless personal area communication is developed as an implementation of the personal centered communication paradigm. IST-PACWOMAN[1)] (**P**ower **A**ware **C**ommunications for **W**ireless **O**pti**M**ised personal **A**rea **N**etworks) is a research project in the fifth framework program of the European Commission that has been devoted to this topic as a pioneer step to the future personal communication paradigm.

In this paper, we introduce the PACWOMAN vision[2)] on the future WPAN. We start with a discussion of the emergence of the person centered concept and the WPAN paradigm, followed by the design objective and technical challenges foreseen by the PACWOMAN consortium. We then discuss the role of network and service provider in the WPAN paradigm, and end the paper with some concluding remarks.

2 Emergence of Wireless Personal Area Network

Besides the explosive development of communication and networking technologies in the last decade, the person centered communication concept has been evolving. With the person centered concept, the future communication paradigm is believed to move from communication between devices to communication between people. With such a concept, the underlying communication and networking technologies tend to be invisible and transparent to the user so that the requirement on the user's technological background and the distraction to the user can be minimized.

1) *The PACWOMAN consortium consists of IMEC (Belgium), CPK/AAU (Denmark), CSEM (Switzerland), Lund University (Sweden), MILTECH (Greece), MOTOROLA (UK), ICCS/NTUA (Greece), Universtiy of Cantabria (Spain).*

2) *Most of the material in this paper is derived from the PACWOMAN project.*

ISSN 0085-7130 ©Telenor ASA 2007

The addresses of sources/destinations in communication links are determined either by the person that owns the device, the service they are capable to offer, or the resource's contents. This causes radical changes in the design, for example, in addressing (content-based or capability based), security etc. As a consequence, new research topics are emerging, addressing different aspects of this problem. Some examples of new exciting research fields are discussed in the following, although we do not aim at providing an exhaustive list of them. The first examples are service portability and virtual home environments [2], concepts aiming at providing users with the same service experience independently of the user interface, terminal capabilities, access network technologies, network providers, and service providers. Another important and related emerging area is pervasive computing targeting environments where networked computing devices are ubiquitous and even integrated with the human user [3].

Due to the increasing demand of connected anywhere, the wireless communication technology has been playing a more and more important role in the person centered communication paradigm. The paradigm shift mentioned above implies different approaches to the development of wireless communications. As concluded by the Wireless World Research Forum (WWRF) [4], a purely technical vision for the wireless development is not enough. In other words, the investigation of, for example, new network technologies or radio interfaces will not be sufficient to come to grips with the future. Rather, such a technical view must be broadened or complemented by:

- Person-centered approach, looking at new ways users will interact with the wireless systems;
- New services and applications that become possible with the new technologies;
- New business models that may prevail in the future, overcoming the by now traditional user, server, provider hierarchy.

There is an essential difference in thinking about the 4th generation (4G) wireless systems compared to the way 3G and other present wireless standards are produced. While the latter standards have been put in a technology-driven development process, early 4G philosophy is being approached from an application viewpoint, with an implied assumption that technology will follow to enable the realization of the application vision [5]. The essence is to provide a ubiquitous networking capability in which questions of data speeds are rendered irrelevant by the universal availability of more bandwidth than the vast majority of users would ever need.

The 4G wireless communications will tend towards personal [6]. The user will no longer be "owned" by any operator: the users, or their trusted agents, will select at each instant the best system available that is capable of providing the required service and performance. The selection will be made according to the user's profile, the type of data stream and the traffic load on the available networks.

WPAN comes into play as an implementation of the personal centered communication paradigm. Technically a WPAN is a networked collection of devices in the geographic vicinity of a person. This collection of devices forms a wireless "bubble" around the person, referred to as Personal Operating Space (POS). Besides the connection among the personal devices within a WPAN, the WPAN should also provide the user and the devices with a seamless, ad hoc connection to the world out of the POS. The organization of WPAN is expected to be transparent to the user, but provide the user with much better experience of service. One example[3)] scenario could be a user at home having a video conversation with the customer; when the user moves to a room with a big screen (e.g. laptop, or LCD TV), the big screen can join the user's POS, and according to the user preference specified beforehand and current situation of the room (e.g. anyone else in the room), the video conversation may be moved to the big screen from the phone screen.

The present notion of WPAN came about as an accretion of several developments and tendencies. Some of them were strongly interrelated from the very beginning; nevertheless, all tendencies now tend to be merged into a unique conception. These factors led to the emergence of the PAN, which traced its independent evolutionary line afterward, defining own application scenarios and motivating the appearance of new applications and services.

- **Bridging different wireless standards**. Today, we are surrounded by a diverse set of wireless access technologies applied in wide-area cellular networks (GSM, IS-95, IMT-2000), personal communication systems, and wireless local area networks (802.11, HIPERLAN). Most of these systems, however, are still tailored towards a narrow and specific application scenario. Hence, there is a need for a single universal wireless communication system that offers a user-friendly and efficient way to access information with a variety of devices such as

3) *The example is inspired by a demonstration of NICT, Japan, in the CTIF-Kyoto joint workshop, Aalborg, Sept, 2006.*

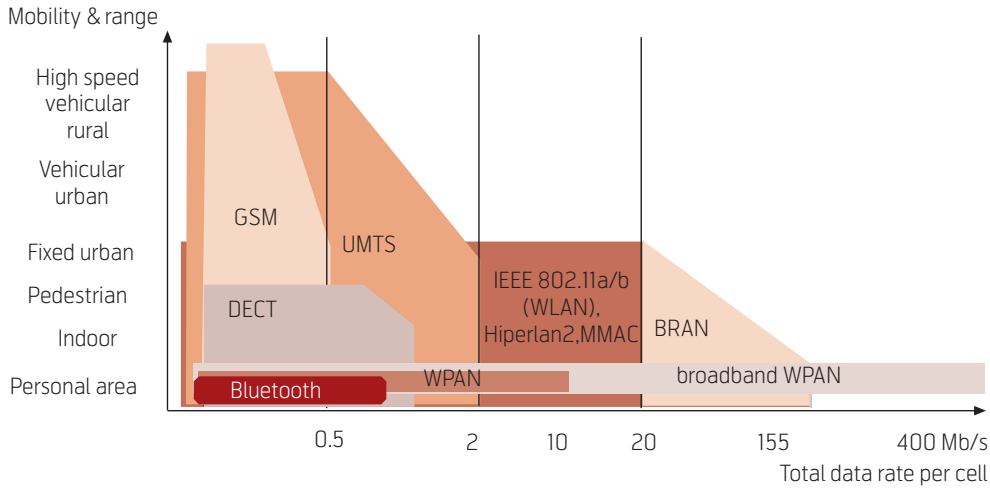


Figure 1 The settlement of the existing and future wireless technologies

mobile PCs, mobile phones, PDAs, pagers, and digital cameras. Such wireless solutions would bring together all these technologies applied in different sectors and at the same time provide a universal and ubiquitous connectivity solution between computing and communication devices.

- **Very high wireless data rates**. The user's need for bandwidth is increasing continuously. In fact, the need for higher data speeds had driven the evolution of 2G wireless systems to the 3G UMTS. Further increasing demand of data rates beyond UMTS requires usage of pico-cells. The low-power, picocellular nature of WPANs implies high spatial capacity, i.e. it enables a more efficient spatial reuse of the radio spectrum. The short-range wireless networks, such as WPANs and WLANs can support significantly higher data rates than the ones offered by the 3G wireless systems. Figure 0.1 depicts the mobility vs. data rate graph for the existing and future wireless technologies.

- **Cable replacement**. Here we refer to the initiatives for developing a cable replacement technology or "last meters" technology instantiated through the specifications of IrDA, HomeRF and Bluetooth working groups. Each of these technologies surpassed their initial targets, offering far more flexibility to the electronic devices than the mere cable replacement.

- **Ergonomic settlement of personal electronic devices**. This is in close relation with the cable replacement. The possibility of wireless interconnection of proximal devices motivates investigation of new computing structures, directed towards the *calm technology* [8]. For example, the PDA's keyboard can be a control interface to all other personal devices.

- **Ubiquity of Internet access**. The number of access points to the wired Internet has grown significantly. People have a need for Internet access everywhere: at homes, enterprises, public spaces. The WPAN will equip the individual with a "wearable" Internet access.

- **Cheaper hardware**. The shrinking semiconductor cost, as well as the lower power consumption for signal processing, make it feasible to build/upgrade personal computing devices with wireless communication capability.

3 Design Objective and Technical Challenges

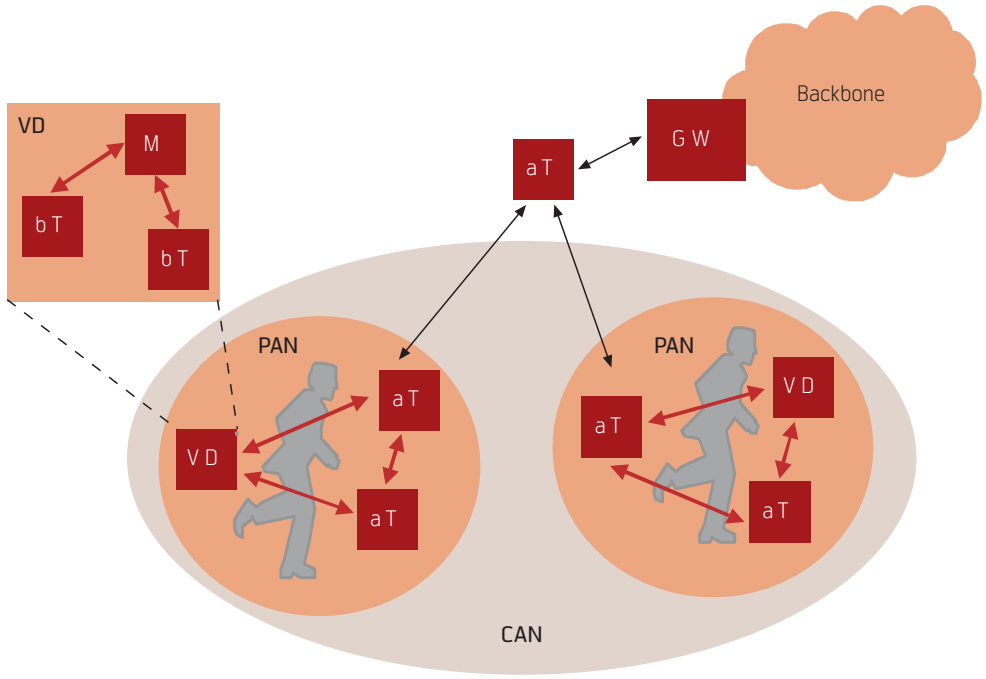
In this section we present the PACWOMAN vision on the development of future WPAN communication systems. The main design objectives of WPAN technology foreseen by the PACWOMAN consortium are:

- *Low power consumption:* The low power consumption is a critical issue since the rate at which battery performance has been improved is fairly slow compared to the explosive overall growth in wireless communications. Therefore, the wireless protocol itself should employ economic usage of the battery energy.

- *Operation in the unlicensed spectrum:* The WPAN systems use license-free wireless links, because it is the only way to achieve ubiquitous connectivity without adverse impact to an existing wireless infrastructure.

- *Low cost and small package size:* The low cost, small size single-chip solution is the economic and ergonomic conditions for widespread use of the WPAN technology.

ISSN 0085-7130 ©Telenor ASA 2007



bT = basic Termnal
aT = advanced Terminal
M = Master terminal
GW = Gateway
VD = Virtual Device
PAN = Personal Area Network
CAN = Community Area Network

Figure 2 PACWOMAN network architecture

- *User friendly operation:* For widespread use of the WPAN technology, user friendly operation is another ergonomic condition. From a technological point of view, the solution should provide seamless connectivity and services to the user in an auto-configured manner.

- *Context awareness and adaptability:* To provide the user with seamless connectivity and services, the understanding of surrounding environments (context) the capability of adaptation of the underlying technologies utilizing the awareness to the context are very important.

A user-centric network architecture has been suggested by the PACWOMAN consortium as illustrated in Figure 2, which contains a 3-level hierarchy, namely PAN, CAN and MAN. A user is surrounded by various devices moving together with the user or temporally around, potentially with different technologies and capabilities. Despite heterogeneity in technology and capability, all these devices are connected and form the WPAN in the following manner. Basic terminals (BTs) with low capability (computational, battery, communication) are attached to some advanced terminal (AT), forming a virtual device (VD). Multiple users can form a Community Area Network (CAN), either with ad hoc connectivity or with infrastructural connectivity.

Based on the above network architecture, the main characteristics and challenges of future WPAN communication systems have been derived as follows.

Heterogeneity in devices

WPAN devices can be categorized taking into consideration the applications for which they will be targeted. Roughly, we can distinguish between Low Data Rate (LDR) devices, in which binary transmission speeds are usually below tens of kilobits per second and Medium/High Data Rate (M/HDR) devices, characterized by capacities of up to tens of megabits per second. The former group will basically comprise sensors and actuators, whereas high capable devices, generally known as Advanced Terminals (AT) within the PACWOMAN nomenclature, such as PDAs and laptops are illustrative examples of the second group. Interoperability between devices belonging to the two different groups is a key issue, as not many solutions have been proposed to overcome this problem. Traditionally, IP has served as a global interconnection technology, but it is more likely that the LDR devices, due to their inherent characteristics, will not be IP capable, so a different approach must be taken. Within the PACWOMAN project, a hierarchical approach has been followed. The proposed scheme assumes that a single person might be wearing a number of LDR devices, known as BT within the PACWOMAN architecture, which will be able to commu-

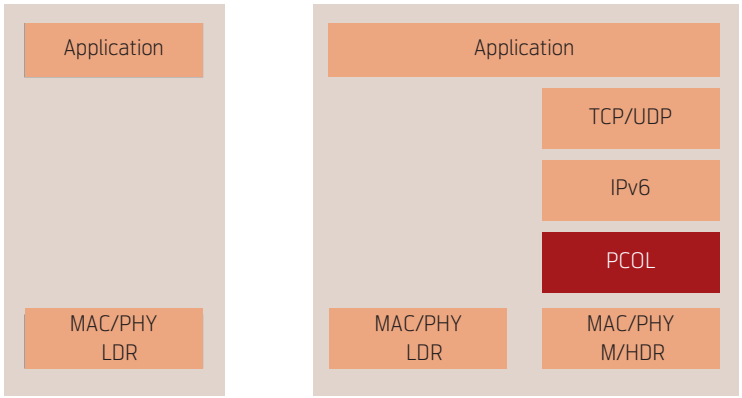


Figure 3 Basic terminal and Master protocol stacks

nicate by means of a proprietary protocol with an M/HDR terminal, being characterized by having a dual protocol stack as shown in Figure 3. This terminal will act as a Master for the BTs and will be acting as a manager of communication between all BTs belonging to the same user, establishing a traditional star topology and forming what has been called the Virtual Device within the PACWOMAN project. The Master node will also act as a "gateway" for the communication between all BTs and entities out of the virtual device.

In this way, the PACWOMAN architecture brings about a novel concept where Layer 2 mechanisms are used to cluster low-capability, low-power and low-cost devices, while at Layer 3 traditional routing techniques are used, apart from their legacy role, to allow the rest of the devices within the PACWOMAN architecture to access the information provided by the BTs.

Heterogeneity in terms of bit rates and capabilities of the devices that will be part of the architecture is a fundamental feature to be tackled. The coexistence and interoperability of heterogeneous technologies are mandatory steps towards the achievement of the next wireless communication user centered paradigm and, more specifically, of the WPAN concept.

Ad hoc routing support

At the moment, commercial wireless communication systems rely on an adjacent infrastructure, and most of the time a communication comprises just one wireless hop; that is, from the mobile terminal itself to the first point of attachment to the network (a base station in the case of cellular communications or an access point with WLAN architectures). However, it is foreseen that the terminal to terminal communication will play a key role in the future wireless communication system. The major advantage of terminal to terminal communication is the potential of co-operation between terminals, which may enhance the spectrum efficiency as well as the network coverage. The main requirement for such architectures can be summarized as follows:

- Willingness of intermediate nodes to relay information for other nodes as the source and the destination may not be on each other's physical vicinity;
- Capability of self-organizing and self-configuring in a distributed manner due to the lack of a central management entity.

IETF MANET working group is devoted to the provision of ad hoc multi-hop connectivity. In the last decade, tremendous efforts from both academia and industry have been spent in this filed.

Compensation for wireless link impairments

Wireless links are exposed to constraints such as high bit error rate and limited throughput. These characteristics are due to the intrinsic limitation of the radio channel. Although to some extent those are compensated for by the link layer techniques that are included within the different technologies (channel coding, medium access control and error control), the behavior exhibited whenever IP traffic is layered over these wireless technologies differs from being acceptable, with the obvious result of performance degradation (decreasing throughput and/or increasing latency). Hence, complementary machinery is needed to compensate for wireless link impairments; this complementary machinery has been approached from two differentiated points of view; in terms of modifying the proper higher protocols so as to adapt them to the characteristics of wireless channels, or by proposing intermediate layers that hide the wireless impairments to the upper layers, which do not need to be further modified.

Technology independency

The PACWOMAN architecture design has been done to be platform-independent. A large number of wireless access technologies are envisaged to co-exist in future wireless communication spaces, so the necessary methods for them to inter-work seamlessly have to be deployed. In this sense, the corresponding wireless network driver(s) and link layer protocol(s) should be accessed from upper layer protocols and applications for control purposes, in a generic manner, independent of the type of technology that is being used (in the same way upper layer protocols and applications access the underlying protocol stack through the socket interface for data purposes).

Thus, a common interface is required for both wireless drivers and lower layer protocols to be uniformly

accessed by upper layer protocols. Such a common interface, that resembles the traditional API, should support the necessary service primitives for (1) configuration of wireless drivers and link layer protocols, (2) retrieval of statistics, and (3) event handling.

Service and applications deployment support

Unlike in the fixed Internet, services and applications in the Mobile Internet will have to take into account the specific characteristics of different mobile environments. This can be achieved by constructing a service/application framework from a set of generic service elements in the middleware. In recent years, terms like pervasive and ubiquitous computing are gaining a lot of relevance and the middleware concept, based on a distributed software infrastructure, appears as a good choice to fulfill their requirements. Future services and applications will need to be parameter/context aware, which concerns the user profile, user location, network context, underlying technology, and so on, so as to adapt their behavior accordingly.

Power consumption

WPAN devices such as laptops, palmtops and PDAs exhibit an upper bound on the operation time due to power (battery) constraints. Power consumption is directly related to the processing tasks that a device runs, as well as the communication tasks. From the networking perspective, the communication task and related processing tasks are of most interest. With the commercialization of WPAN, the communication tasks are expected to be grow explosively, which consequently leads to faster battery exhaustion. Mitigation techniques should be enforced to reduce power consumption as much as possible without sacrificing the overall networking performance. This optimization task involves almost all layers in the OSI protocol stack. Potential optimization techniques with respect to power consumptions are

- *Power control at physical layer:* By tuning the transmission power to a lower but yet high enough level, power consumption is expected to be minimized. As a side effect, interference is also expected to be lower.

- *Error control at link layer:* Adding error correction codes adaptively according to channel condition could potentially minimize the overall transmitted data volume, consequently minimizing the power consumption.

- *Medium Access Control protocols at link layer:* It plays an important role in reducing the power consumption due to collisions.

- Routing protocols at network layer:
  - Routing protocols taking into account other metrics than hop count (e.g. channel condition), together with the above techniques should be able to achieve lower power consumption.

  - Efficient algorithms for routing information collection (e.g. link state updates) are foreseen to reduce the power consumption for routing purposes.

4 PAN and CAN Optimization Layer

In this section, we present some technical results brought by the networking package of PACWOMAN. We start with the introduction of the PAN and CAN Optimisation Layer (PCOL), followed by some adaptation schemes built on top of the PCOL layer.

PCOL is an enabling technology designed specifically for WPAN communication systems as shown in Figure 4. In this sense, data packets will traverse a set of protocol boosters that aim at optimizing the network and communication performance managed by the PCOL, while the control plane will embrace a number of different components that will cope with some management task.

PCOL data plane

PCOL will accommodate a diverse set of protocol boosters, i.e. link layer targeted to packet processing during transmission/reception to/from the wireless driver, so as to enhance performance of particular types of traffic.

Each of the different boosters will be applied to downstream traffic (meaning traffic going out of a particular host), according to both its particular requirements and the varying conditions (channel quality, remaining energy level, etc.). In this sense, the PCOL will adapt its operation in order to optimize communication performances while maintaining a power aware activity.

PCOL control plane

PCOL control plane contains all the necessary machineries to fulfill the PACWOMAN requirements.

Layer 2 service discovery

Ease of use and auto-configuration, as well as service discovery are mandatory topics to be tackled within the WPAN communication system. The Layer 2 Service Discovery module will be in charge of the automatic selection of a Master, from all the possible candidates, within a single PAN. In addition, it will perform the corresponding actions so as to allow the rest of PACWOMAN devices to reach the information provided by the BTs.

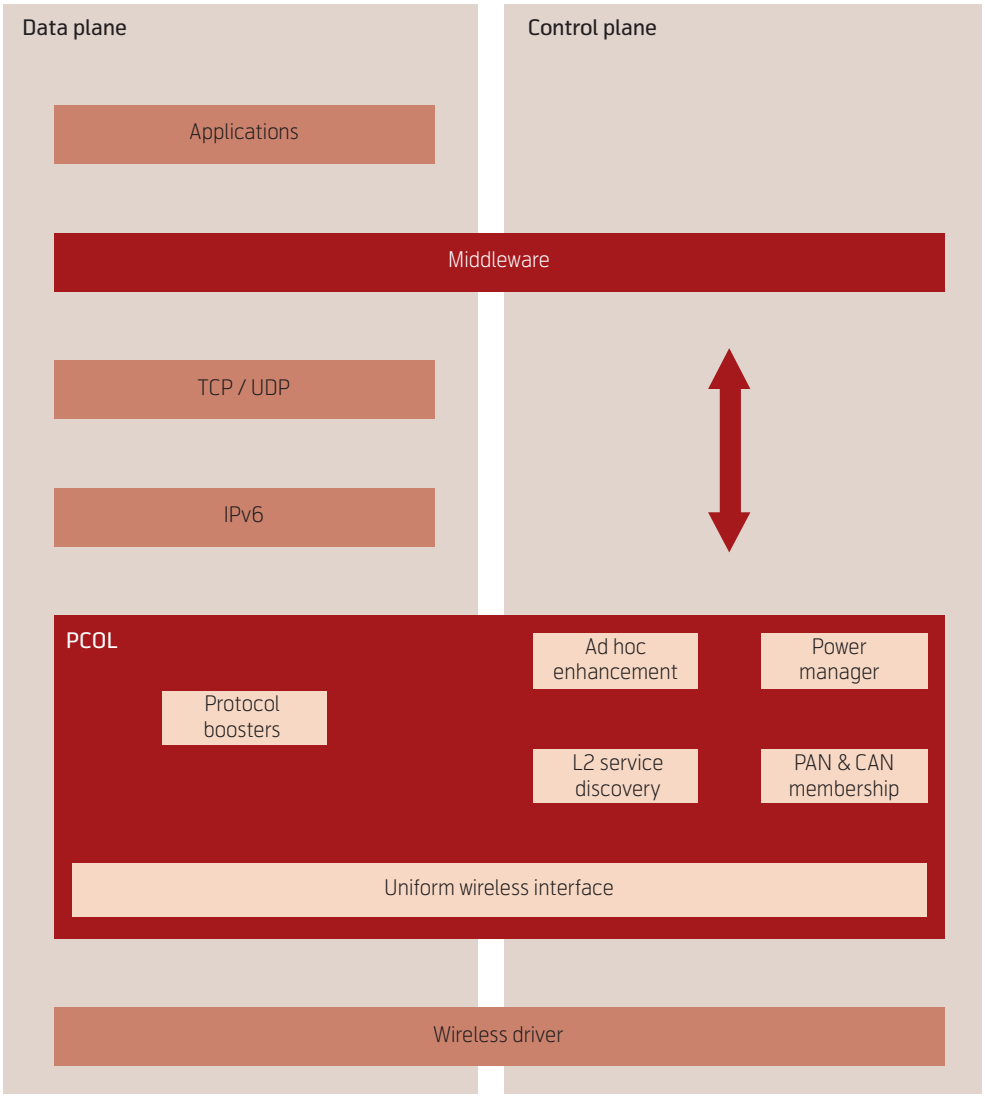


Figure 4 PCOL high-level protocol architecture

Power manager

Battery awareness is one of the major requirements of a WPAN communication system. The power manager module will be in charge of optimizing energy consumption within an M/HDR device through utilizing the awareness towards the environmental conditions (i.e. link conditions, remaining battery level, etc). We have seen that an energy-aware solution is more likely to be achieved targeting other communication layers, specially MAC and physical levels, but taking advantage from the control possibilities that are provided by subjacent technologies, some reductions can be achieved.

PAN&CAN membership

PAN&CAN membership module is the key components for security purposes. In WPAN, security must be assured on all communication links, and it is therefore a mandatory requirement that the membership need to be implemented.

Ad hoc routing enhancement

The main goal of this module is to take the advantage of the information provided by the PCOL to adapt ad hoc routing protocols. Apart from being efficient from a performance point of view, it might help leveraging a power aware behavior using battery information and reducing the number of retransmissions. Figure 5 shows an illustrative example of how a route towards a destination could be selected using the SNR as a new metric, achieving a better communication quality (both in terms of performance improvement and error decreasing) while saving battery on the sender, which would need to perform a considerably smaller number of MAC retransmissions.

Uniform Wireless Interface

The UWI provides a uniform set of manipulation functions that hide wireless driver singularities to the PCOL.

5 Conclusion

Wireless Personal Area Network, as an implementation of the person centered networking concept, will play an important role in the next generation of wireless communication systems. The services brought by this WPAN concept are bringing new opportunities, but at the same time challenges.

In this paper, we have shown that with the current technology WPAN can already be realized as we have done in the PACWOMAN project. However, for the real commercialization, there are still a number of issues to address; service and applications, naming and addressing, throughput enhancement, efficient energy utilization, and security. To cope with those challenges, the PACWOMAN consortium has developed an enabling framework, i.e. PAN and CAN Optimization Layer.

Besides the technical challenges, business model and new services are two important issues. In the business model, the question of how the service and network providers are involved in the WPAN communication system needs to be answered. And the WPAN paradigm can never be commercialized and successful without services of interest to the end user at an affordable cost.

Acknowledgement

The author would like to thank the PACWOMAN consortium, especially the networking package (WP5) members for a fruitful project.

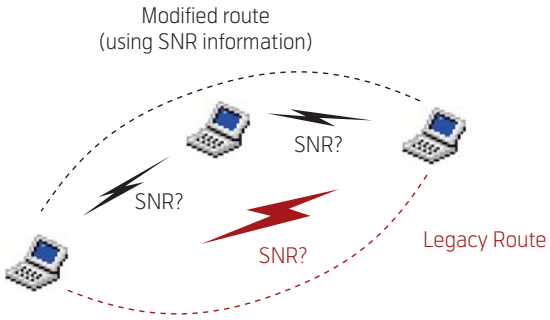


Figure 5 Example of a multi-parametric route election

Reference

1 Weiser, M, Seely Brown, J. Designing Calm Technology. *PowerGrid Journal*, 1.01, July 1996. (http://powergrid.electriciti.com)

2 Daoud, F, Mohan, S. Service Portability and Virtual Home Environments. Guest editorial. *IEEE Communications*, 40 (1), 76–77, 2002.

3 Gupta, S K, Lee, W-C, Purakayastha, A, Srimani, P K. An Overview of Pervasive Computing. Guest editorial. *IEEE Personal Communications*, 8 (4), 8–9, 2001.

4 *Wireless World Research Forum*. 2006, October 27 [online] – URL: http://www.wireless-world-research.org.

5 Richardson, P. *Personal to Global: Wireless Technologies, 2005 – 2010*. Gartner Group Inc., Research Brief, February 23, 2001.

6 Pereira, J M. Fourth Generation: now, it is Personal. *Proc. PIMRC 2000*, September 2000, 1009–1016.

7 Rabaey, J. *PicoRadio Networks: An Overview*. Berkley Wireless Research Center Focus 2000 Session, July 2000.

8 Weiser, M, Seely Brown, J. Designing Calm Technology. *PowerGrid Journal*, 1.01, 1996. (http://powergrid.electriciti.com)

Yaoda Liu received his B.Eng from Shanghai Jiaotong University, China, in 2000, and his M.Eng from National University of Singapore in 2003 with focus on Mobile Ad-hoc Networks. In October 2003 he joined Aalborg University, Denmark as a PhD candidate. Since then he has been working in the IST PACWOMAN, MAGNET, and HIDENETS projects. His research interests include algorithm and protocol design for wireless multi-hop networks.

email: yl@kom.aau.dk

Personal Networks as Business Strategy for the Wireless Communication Future

KNUD ERIK SKOUBY, KARSTEN VANDRUP

Professor Knud Erik Skouby is Director of CICT at the Danish Technical University, Lyngby

Karsten Vandrup is Senior Research Manager in Nokia Technology Platforms, Denmark

In the wake of the ongoing 3G rollout in Europe – as well as in other parts of the world – the research on *what will be the next G in mobile communication* has taken off even more rapidly than the research on a 3rd generation system did start. However – many top researchers see difficulties in just letting the technology race set the standards for the future; user and market issues must be taken into account already in the early research. This paper takes its point of departure in the quote "*3G + Personal Networks = 4G*" [1], and assesses the theories of Personal Networks in the context of future business strategies.

Assessment of the 3G Success

Until the beginning of 2006 very few outside South-East Asia would defend the idea of a success for 3G – and even here the profitability of the new service was questionable and the use dominated by 'exotic' services such as download of ring tones. This gloomy picture was supplemented by the continued success of 2G, especially GSM. By mid-2006 there were 2 billion GSM users serviced by 784 networks in 209 countries/territories [2]. Compared to this, the 3G status does not seem very impressive. WCDMA – which has now emerged as the dominating 3G standard – has 70 mill. subscribers served by 122 networks in 55 countries. The development during the first six months of 2006 has however opened for some optimism as the figures are the result of a 45 % growth in subscribers during this period. This again is arguably the result of a combined development in technology/devices and services. A number of HSDPA (the first evolution of WCDMA) products has been launched; many also supporting GSM/EDGE, thus ensuring service continuity. This has enabled especially enhanced Internet/data communication and mobile TV. This again has resulted in the first profitable 3G operations, but real take-off approaching, e.g. GSM numbers, requires devices and services demanded by a really large number of users.

Introduction to PN Applications and Services

Personal Networks, PNs, is an essential concept for developing mobile applications, services and networks in the future. The idea behind the concept is to bind all available networks together giving global connection and supporting users' technology usage both in their close vicinity (referred to the Personal Area Network, PAN) and in the more remote or distributed network islands containing work environment, location of friends, family members and other personal contacts.

A PN can be considered as an ordinary PAN, but without geographical limitations, see Figure 1. In a PAN all the devices are within a certain distance – say up to 10 metres. This gives certain suggestions of connection technologies used in the PAN (Bluetooth, IR, etc.). In a PN, devices can be separated by hundreds of kilometres and still belong to the same virtual PN. It means that in a PN, connection technologies are not only short range like Bluetooth or WLAN, but also medium range and national or continental range, like GPRS or UMTS. This calls for more service requirements for the PN as compared to the PAN. Those are especially different when we talk about technical requirements, because some issues in a PN are much more complex to achieve than in PAN. Seamless service, mobility, single sign-on, context discovery, self-organization, roaming, handover, context transfer and session continuity are the requirements that will be the main technological problems for PN. If the issues in PN could be handled with the same quality as in a PAN, then there would not be much difference from the service point of view between the PN and PAN concepts. The physical network structure would be different but the logical structure still remains the same [3].

A key feature of the PN is that the PN emphasizes the trust relationship between the user and the devices. The concept of PN can thus bring a solution for trusted communication between the many local and remote personal devices in view of the support of a variety of personalized and context-aware services. A Personal Network is a protected secure person centric network that connects all the nodes of a person over ad hoc as well as infrastructure networks and that provides context-aware services and applications. As such, it is a dynamic collection of interconnected heterogeneous active personal devices, not only the local devices centered around the person, but also personal devices on remote locations such as devices in the home network, the office network and the car network.

ISSN 0085-7130 ©Telenor ASA 2007

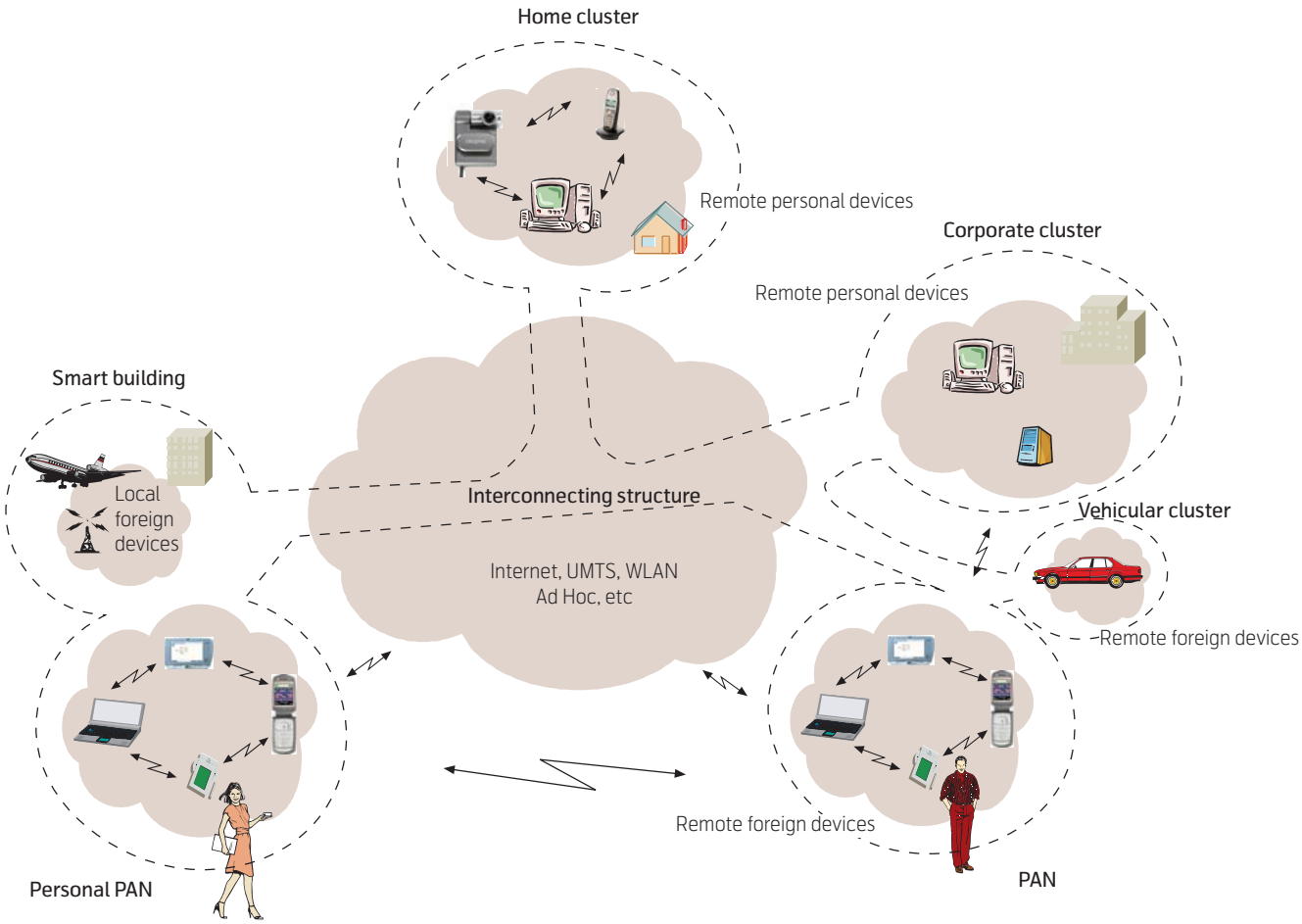


Figure 1 A Personal Network and its PANs, interconnection structure, etc. MAGNET Beyond 2006

User Requirements – the Soft Values are Becoming Harder

It is a challenge to identify and explicitly formulate needs and user requirements. Users themselves have difficulties in explicitly expressing their preferences and needs, in particular when referring to situations including future, not yet developed technologies. And if user requirements are expressed, these may change in time with the trends, new technological developments, traditions and situations in which users are active.

One tradition has found the solution in associating the notion of user requirements with methods trying to identify 'pure user needs for technology', i.e. attempts to identify what the user really needs set up as a contrast to what the market 'forces' the user to buy. This has not been very helpful in the process of choosing between different developments of technology as it tends to focus only on the user and not on the specific requirements.

To discuss choices of technology a shift is needed in the focus to analyses of how specific technologies can serve different users in specific social settings.

What is needed is a methodology expressing individual user perceptions of specific needs as requirements present in given social settings served by, e.g. the technology and components of a future PN architecture.

Based on well-established methodologies, e.g. participatory design, a template for discussing user requirements in relation to future technologies has been developed in the MAGNET project involving scenario construction. Central for the MAGNET scenario approach is that it mixes the futuristic scenario construction with participatory design principles. This makes the template relevant in a discussion of innovative user-centred situations, needs and requirements, which will challenge existing networks and technologies and call for the new solutions.

Further, *User requirements* in this setting have been specified as the result of combining user needs, socio-economic trends and business models into realized – or in this context rather expected realized demand. Business models and socio-economic trends form requirements and analyses at a different level, since the prospects of making an ICT business work in

relation to various operators and suppliers are analysed. The business model activities, on the other hand, are built on the user requirements and results of the user case studies and user involvements. This sum of two rather complicated analyses is conceptually useful in opening for analyses of the elements in technical solutions that are potentially important for commercial success [3], [4].

Several very promising technologies has over the years failed on the market, due to the lack of user acceptance, and by disqualifying themselves lacking the simplicity and readiness that are required if larger amounts of customers with various backgrounds and experiences are the main target group.

The dominant approach to user requirements in the traditional telecom industry is that services and applications are shaped by the combined influence from terminals and networks developed according to the current technological possibilities, i.e., user requirements are not taken into account during initial conception. Service development then involves the PAN and a combination of networks; PSTN, cellular networks, digital broadcasting networks, as well as Bluetooth, WLAN, the Internet, etc., and the combination of these heterogeneous networks.

In MAGNET, the approach to user requirements is different. The methodology to describe and develop an understanding for implementation of an efficient PN-solution in a heterogeneous, multi-modal environment involves 'technology', 'user needs' and 'economics'. A key element of 'user needs' is perceived to be quality of service – or quality of experience – associated with given private and/or business activities and its relation to the underlying technologies.

The introduction of PN services along with the associated technologies will constitute a major paradigm shift. There are currently no business models or scenarios in place for PNs; however, an enhanced understanding and knowledge of possible business model solutions as well as market and socio-economic aspects are necessary in order to achieve the full benefits of a heterogeneous communication model as proposed in the PN concept [3], [4].

Business Strategies for SMEs Based on PNs

In retrospect, providing systems to the current and past generations of mobile communication systems has been a game of the world's large enterprises, willing to invest billions of dollars, euros and yen in product development in order to be present on the market during the first hype. Later, when the technologies become commodities, the business to engage in the system and device side is significantly less attractive. Obviously, as the mobile communication business on the application side is moving into the area of more or less open operating systems, some new businesses have been created providing services and applications to the end users. In the large picture, the revenue of these businesses still only counts for a fraction of the entire business.

Moving into systems like "Personal Networks", the infrastructure is a combination of various existing communication technologies, complementary working together to provide the best possible service and/or price for the end user, and combine it with state-of-the-art PAN solutions. This opens for a variety of opportunities in the technology area, in the system area and not least in the business area.

As the businesses and services over the years have become a set of more and more complex arrangements with more technologies, systems and services offering businesses that interact closely, the traditional mobile and wireless value chain is fairly often described as a value complex.

The value complex concept as an approach to characterize "Personal Networks" can be considered as a composition of the traditional one-dimensional value chains, adding up a number of smaller value chains to construct a system. On the business and technology-provisioning side, this potentially opens for a new and strategic role for smaller and medium sized enterprises. In a personal network future, SMEs can focus their activities on one or more of these smaller value chains; build R&D, production and marketing to support this limited aspect of the value complex. The agility of the SMEs is the key argument for their central role in the new PN-based communication structure.

Why SMEs? Several surveys and reports published in the EU stress the point that the success of Europe in a globalized world very much depends on the success of its SMEs [5]. Especially in the northern Europeans states – the Nordic and Baltic countries – the business environment has a large percentage of SMEs compared with other regions of the world. And indeed successful SMEs, competing on global terms in global markets.

Some of the general challenges the traditional European SME is up against are:

- Lack of awareness of new market opportunities;

- Lack of knowledge, expertise and financial resources to carry out in-depth research in order to appropriately assess the current and potential market situation with regard to products and services in international markets;

- Lack of knowledge, technical skills and financing to effectively carry out R&D, marketing and promotional campaigns;

- Lack of specialized technical skills, financial resources and contacts with buyers/technology holders in foreign markets needed for strengthening the supply base at an accelerated pace [6], [7].

Assessments on each of these points will show that within the segment of mobile and wireless communication, SMEs will have better opportunities with a decentralized PN structure than with the traditional telecom set-up:

- By gathering together in PN developer's communities, the access to new markets and partnerships will be more visible.

- In-depth research has been carried out – e.g. by the European Commission IST research projects MAGNET and MAGNET Beyond, and as a result large parts of the technologies, market analyses, user requirements are documented thoroughly.

- The theories of Personal Networks are developed in global projects and communities, engaging researcher from Japan, China, India, USA and Europe, making PN competences present in most parts of the world.

However, the fact that the personal network sub-systems, applications and services can be approached individually, each with a complete value chain and new open markets in the context, is probably the strongest incentive for SME's to enter the world of PNs. In this type of decentralized systems, the required and focused R&D effort is manageable for SMEs – and the big players may regard them as non-threatening, but useful partners.

Conclusion

As mobile communication systems beyond 3G will be a more diverse setup, consisting of a variety of heterogeneous systems, working together in more or less transparent ways, there will be room for smaller and medium size players in the various markets of devices, applications and services.

To summarise, stepping up to the next generation of personal communication systems – e.g. by introducing Personal Networks – huge changes will take place in the business and market places globally.

Acknowledgement

MAGNET Beyond is a continuation of the MAGNET project (www.ist-magnet.org). MAGNET Beyond is a worldwide R&D project within Mobile and Wireless Systems and Platforms Beyond 3G. MAGNET Beyond will introduce new technologies, systems, and applications that are at the same time user-centric and secure. MAGNET Beyond will develop user-centric business model concepts for secure Personal Networks in multi-network, multi-device, and multi-user environments. MAGNET Beyond has 30 partners from 15 countries, among these highly influential Industrial Partners, Universities, Research Centres, and SMEs.

References

1 Prasad, R, Deneire, L. *From WPAN to Personal Networks*. Artech House, 2006.

2 *GSA – The Global mobile Suppliers Association*. 2006, October 27 [online] – URL: www.gsacom.com

3 Prasad, R, Skouby, K E. Personal Network (PN) Applications. In: *Wireless Personal Communication*, 33 (3-4), 227–242, 2005.

4 Prasad, R, Farseruto, J, Vandrup, K. *MAGNET paving a path towards the future wireless communication*. ECWT, Paris, 2005.

5 European Commission. *Innovation and Research in Small and Medium Enterprises*. Brussels, 1996. European Report on Science and Technology.

6 Hibbert, E. *The Globalisation of markets – how can SME's compete?* Middlesex University Business School, 2000.

7 International Trade Centre UNCTAD/GATT. *Product and Market Development for Export*. Geneva, 1995.

Knud Erik Skouby is professor and founding Director of the Center for Information and Communication Technologies (CICT) – a center providing a focal point for multi-disciplinary research and training in applications of ICT at the Danish Technical University. His main area of research interests includes the techno-economics and regulation of the telecom sector and of new telecom applications and services. He has participated as project manager and partner in a number of international, European and Danish research projects. He has served on a number of public committees within the areas of telecom, IT and broadcasting; as a member of boards of professional societies; as a member of organizing boards, evaluation committees and as invited speaker on international conferences; published a number of Danish and international articles, books and conference proceedings in the areas of telecommunications regulation, technology assessment (information technology and telecommunications), demand forecasting and political economy.

email: skouby@cict.dtu.dk

Karsten Vandrup is Senior Research Manager in Nokia Technology Platforms, and serves as Technical Manager and Deputy Coordinator of the EU FP6 Integrated Project MAGNET Beyond. Prior to this position, Vandrup has had several positions within the Nokia Corporation in Copenhagen, Denmark, and in Espoo, Finland. He holds a degree in Telecommunications and Electronics from the Technical University of Denmark, supplemented by studies at INSEAD, UCLA and the Swedish School of Economics and Business Administration in Helsinki, Finland.
Besides his work in Nokia, Vandrup is chairman of the Technology Foresight Council – Mobile and Wireless Technologies under the Danish Ministry of Science, Technology and Innovation, and holds seats on a number of boards, advisory boards and steering committees, both national and international.

email: karsten.vandrup@nokia.com

PN Business Models and Strategies – The Operator's Perspective

SU-EN TAN, RUNE ROSWALL

Su-En Tan is a Post-Doc at CICT, Denmark

The EU project MAGNET-Beyond has examined the impacts of Personal Networks (PN) on business models for existing infrastructure-based network vendors and operators. In the current communication markets, companies deliver services to customers in cooperation with other market players building on different business models. The aim has been to examine the implications of PNs on existing business model and business strategies of the mobile operator. This work consists of two main elements: a) A presentation of the business model concept and its implications for PNs and mobile operators, b) examinations of the PN business model as well as possible business models and strategies that the operator could develop for the PN.

Rune Roswall is Senior Business Manager at TeliaSonera, Sweden

1 Introduction

The main emphasis of this report is on business models and business strategies of the present day mobile operator in the Personal Network (PN) environment. The main objectives are the identification of the impacts of PNs over existing infrastructure-based networks and the development of new business models and business strategies within the context of MAGNET (My personal Adaptive Global NET) leading to profitable endeavours for the mobile operator. The aspects considered are related to usage situations, economics, markets and sociological factors[1)] [1].

The work primarily builds on theoretical approaches to business modelling as well as input from technological research in the PN area. The potential usability of the work will be for the architectural work on PNs and, consequently, for the work on standardization.

We conceptualize PNs in the following manner: 'PNs are configured with functionality supporting secure tunnels, as the opportunity and demand arise to support personal applications. PNs consist of communicating clusters of personal and general digital devices shared with others and connected through various suitable interconnection agreements[2)] [1]. PNs thus comprise potentially of 'all of a person's devices capable of network connection whether in his or her wireless vicinity, at home or in the office[3)] [1]. The PN concept is closely related to, for instance, the Virtual Home Environment concept promoted in 3GPP and other similar concepts related to the use of heterogeneous networks for delivering personalized services to end-users[4)]. However, the specificity of the MAGNET project on PNs is the focus on Personal Area Networks (PANs), P-PANs (Private PANS) and peer-to-peer organized networks. The implication is that there is an emphasis on the self-organized aspects of networks and applications.

Standardisation bodies like ETSI often refer to convergence as the convergence of fixed and mobile networks. From this reference point ETSI could foresee convergence in other telecommunication domains, informatics, broadcasting and entertainment. Converged mobile services are predicted to change the telecoms world.

Many mobile and fixed telecommunication operators like Telenor, TeliaSonera and Tele Danmark are facing declining voice revenues. Today they show an immense interest in Internet protocol (IP) services such as voice-over-IP (VoIP) and rich multimedia services.

Convergence allows Operators to deliver services on their own networks as well as to subscribers utilizing roaming on other networks and they will have a chance to compete beyond price.

The convergence of different mobile and wireless technologies has resulted in a need for operators to reassess their earlier business models and to develop new ones to address this phenomenon. In PNs, different types of access technologies will work hand in hand to deliver communication and services to users.

1) *MAGNET: Annex 1 – 'Description of Work', 2003, page 40.*

2) *MAGNET: Op.cit., page 6.*

3) *Ibid. page 6.*

4) *See, e.g., Jani Suomalainen: 'Service provisioning in the Virtual Home Environment', Helsinki University of Technology Telecommunications Software and Multimedia Laboratory, htth://www.tml.hut.fi/T110.551/2002/papers/May/Jani.suomalainen.pdf, and UMTS World, Virtual Home Environment, http://www.umtsworld.com/technology/vhe.htm*

 ISSN 0085-7130

This has important consequences for business modelling. Generally, business modelling is a supply side exercise. User needs, targeted market segments and value propositions must be part of the modelling exercise. Basically, however, business modelling deals with the relationships between the players on the supply side in order to determine how they can service the needs on the demand side. In the case of PNs, the demand side has to be directly involved in the creation of business models. The reason is that user groups can set up parts of the network infrastructure and construct and deliver the services themselves, and will often only need to interconnect and work together with commercial network providers for parts of the network and service delivery assignments. PNs will therefore often consist of combinations of service delivery relations (i.e. from a business enterprise/operator to an end-user) and self-organized networks and applications.

PN business modelling may also contribute to standardisation work. Standards Development Organisations (SDOs) look to standardise technologies within industries. Business modelling shows how different relationships exist between different actors in a value chain. This could in turn assist SDOs when looking at which technologies to standardise. Standards work looks at the entirety of the technology in question and business modelling shows the different actors involved in the technology in question. Thus, when standardisation work is taking place, different actors and their contribution to the technology may be taken into account.

2 Business Models

The business model concept is used to analyse not only the service aspect of PNs but also the organizational, technology and financial aspects of PNs. For our ongoing work on PN business modelling we are using works by [4], [2], [5], [6] and [7]. Making use of the paper by Faber et al. (2003), we have analysed the four interrelated design domains, which are shown in Figure 1. It should be noted that the Faber model bears much similarity to the Osterwalder model, and that other related ontologies and models exist.

There are four basic constituent elements in this business model ontology: Service design, technology design, organisation design, and finance design. Using this business model ontology, it is possible to include all relevant elements of business modelling and, in the context of the present paper to examine the implications of the development of the PN concept for existing mobile and wireless operators.

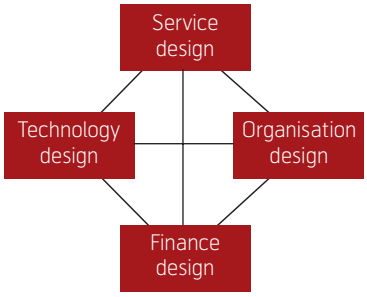


Figure 1 The four inter-related design domains [2]

Because the finance domain is somewhat related to the charging model of a PN, it is possible to make use of the finance design of the business model to analyse and describe what the PN charging model will look like. The four domains are interrelated domains such that decisions made in one or the other would in some way affect what happens in another domain. Briefly, the four domains are described here [2]:

Service Design: Description of the service (value service) that this network of companies will offer to a target group of users.

Organisation Design: Description of the network of different actors that is required to deliver the value services to the end users. Also the roles played by each actor in the network.

Technology Design: Description of the fundamental organisation of the technical system and technical architecture that is needed to deliver the value service.

Finance Design: Description of revenue that is intended to be obtained or earned from the value service. It includes risks, investments and revenue division amongst the different actors.

The present day mobile operator's business model may be represented by Figure 2. In this model, the mobile network operator is expected to be the main customer facing unit of the value chain. Other members of this model are the portal/content aggregator, the service providers, the ISP, the mobile device manufacturer, other types of network providers (fixed, Wi-Fi and other mobile network operators) and the network equipment vendor. These are the main players in this particular business model but there are obviously other smaller members that have not been indicated here. The relationships between the different players are indicated by the arrows drawn, and the different services and revenue exchanges are also indicated. What is important to note here is that this business model represents the mobile network operator as the most significant role

ISSN 0085-7130 ©Telenor ASA 2007

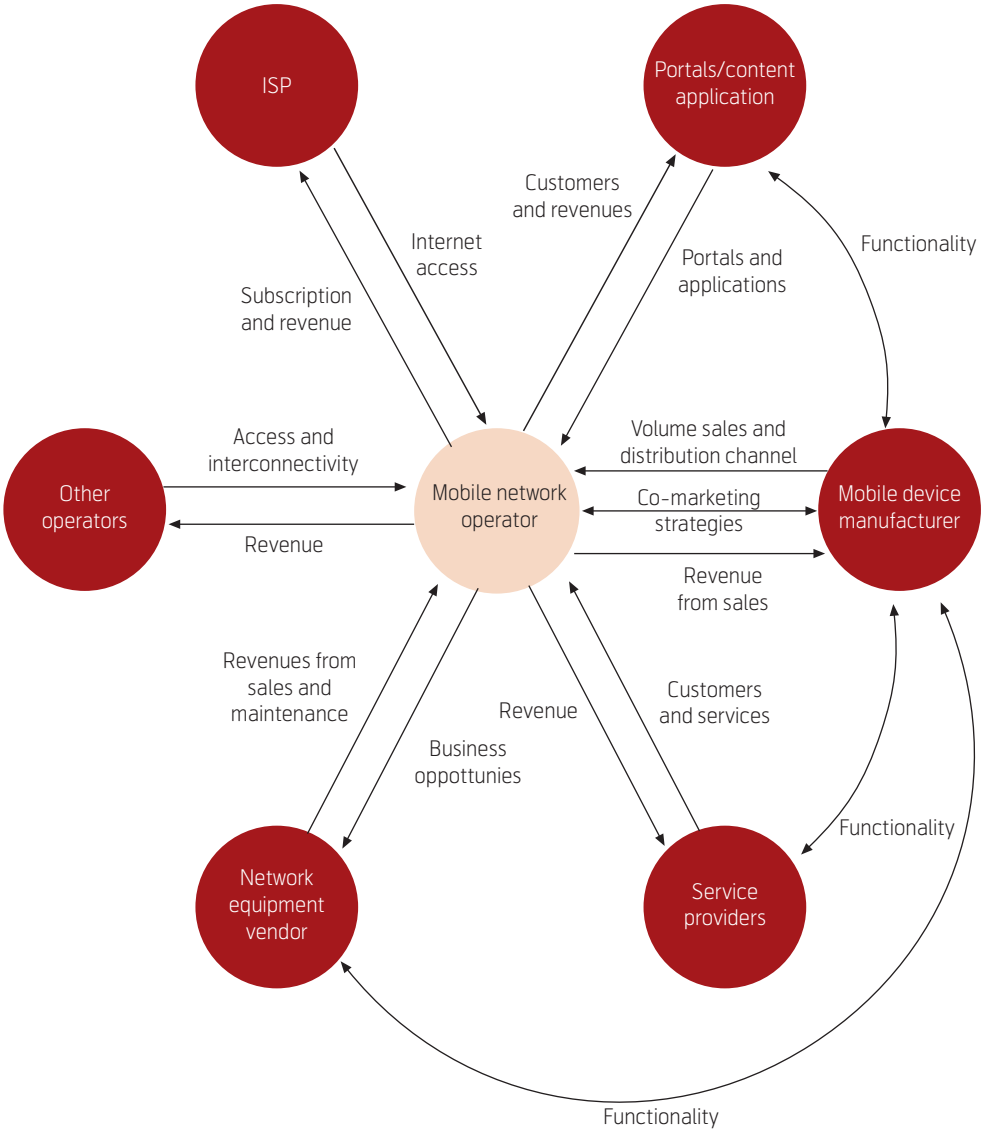


Figure 2 Business model of today's mobile industry

of the value chain. Although different actors all are looking at increasing revenues, the mobile network operator seems to be in the best position to create new business different from its traditional core business in mobile service provisioning.

As the mobile industry moved towards 3G and data services, the mobile operator showed interest in taking over some of the functions that were previously performed by other actors. This is the natural way to act for the mobile operator as their operational costs must be reduced while new service concepts are developed in order to increase their efficiency and ARPU (Average Revenue per User). Several tasks that are performed by other actors may soon fall under the domain of the mobile network operator. Examples include Mobile Virtual Network Operators (MVNOs), portal and content aggregation, payment services and also service provisioning.

The model shown in Figure 2 is valid for today's mobile industry but it may also be valid in a PN environment though the number of actors and their roles may change. It is, however, just as likely that new business models will be presented in the future PN environment.

The business model shown in Figure 2 is an evolution from the 2G or GSM business model. Earlier business models were simpler because there were few or no data services at all offered for the users. However, as technology has evolved and data services have been more popular, the business model can be represented as in Figure 2. Newer services and applications will make changes to partnership relations and the business model of the mobile operator.

In this model it would be difficult for other roles to emulate in a short time span because of the many advantages held by the mobile network operator. In

a PN environment, however, the role of the mobile network operator may change.

The mobile operator's role today is developed from the 2nd generation operator role, with the addition of mobile data services. The market for present day packet based data network services is still considered very young and will continue to grow. Voice still plays a big role in the operator's revenue stream, but as the volume increases, the revenues from data services are likely to increase even more rapidly due to added value and efficiency. The operator's service offerings are changing with the new technologies that are being introduced. This also results in organisational changes as well as in the network operators' financial performances.

In a converged arena, the business model adopted by operators would also change. Convergence results in new services and new ways of combining services. It also results in new business opportunities. Earlier, the industry saw the convergence between fixed and mobile services. Today, we still see this, but with the addition of further convergence between wireless and mobile technologies. With wireless technologies becoming ever more popular, some operators have taken wireless technologies as a complementary product to their mobile services and offered them in packages to users. Convergence has therefore led to operators redefining their business model and making changes to the way old services are sold.

The future mobile industry will likely be personalised and quite industry specific in terms of its offerings.

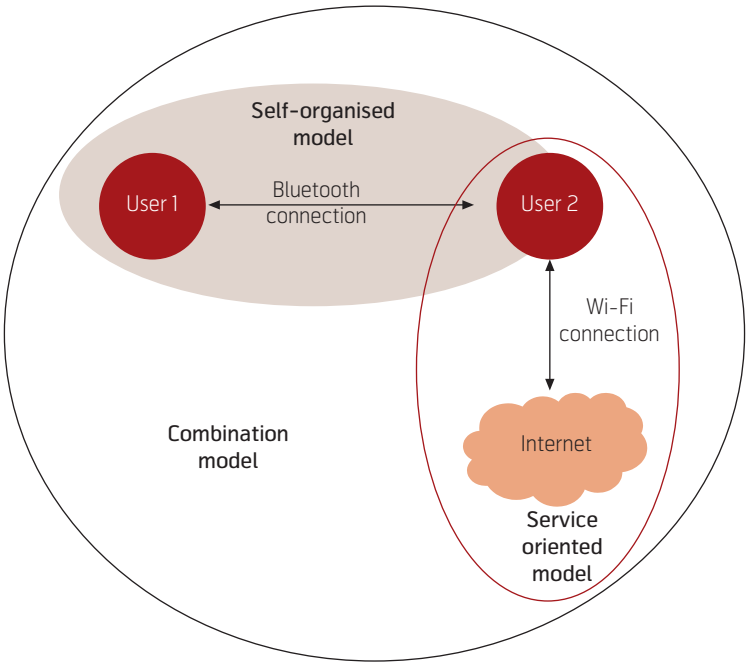


Figure 3 Examples of self-organised, service-oriented and combination models

General services like voice and simple data services would probably still be offered but value added services and applications over and above these general offerings will be more important for the actors of the value network.

The business model design domains as developed by Faber et al. and used here are not static models in practise. Variable and relation changes result in a dynamic model that is being adjusted constantly. The balancing of all these factors and variables is what creates a dynamic model. Changes in one domain will likely affect one or more of the other domains. The effect may not always be direct but could sometimes be observed as an indirect consequence.

3 PN Business Model

MAGNET is all about Personal Networks or PNs. A PN is the total network made up from P-PANs and an interconnecting infrastructure. Communication within a PN can be anything from short range communication between personal devices (e.g. between a laptop and a mobile phone) to wide coverage communication such as UMTS [8]. In a personal network, the user is responsible for choosing between the available choices. The business model in a PAN or PN environment has been categorised into a self-organised and a service-oriented business model, or into a combination of both. Figure 3 shows the differences between each of these definitions.

The self-organised model is a model where no financial exchange takes place, for example there could be two users connecting to each other's devices using Bluetooth. It is also possible to refer to the model when a user connects to a Wi-Fi network without paying for this service (it may already be paid for by his company or it belongs to a friend). In a technical context, a self-organised network is based on its own capabilities and preferences in contrast to externally forced actions. By combining the financial definition of the self-organised model and the technical definition of a self-organised network, the self-organised business model is the one that is formed based on its own actions independent of any external chargeable resources (i.e. no financial transaction in the immediate sphere).

The service-oriented model is a model where a financial transaction takes place. In this case there will be a payment by the user to the Wi-Fi Service provider in exchange for connecting to the Internet.

The combination model would encompass both earlier models where a self-organised and a service-oriented model exist. This will probably be the most

common case in a PN environment, where there will be different types of communication, either through a network operator's connection or through a personal peer-to-peer connection.

Ad hoc networks may exist in any of the combinations. Since ad hoc networks are defined as being wireless self-organising systems formed by the co-operating nodes within the communication system, they form temporary networks[5] with a dynamic and decentralised topology. Self-organised networks can therefore be built upon PN agent networks in the MAGNET scenario.

The Magnet Beyond project participates actively in the IETF and other Standardisation groups.

Routing in personal networks poses two special challenges. First of all traditional IP and Mobile network solutions are reasonably stable. In a personal network, the network topology is constantly changing.

Second, in traditional routing the solutions rely on distributed routing databases, maintained in either the network nodes or specialized management nodes. In mobile ad hoc networks, nodes cannot be assumed to have persistent data storage, and they cannot always be trusted.

The Internet Engineering Task Force (IETF) and its mobile ad hoc networking groups MANET, Nemo and autoconf have studied solutions that have addressed those challenges.

4 Operator's PN Business Model

The PN bring a lot of new opportunities for the different members of the industry, and particularly so for the mobile operator. The mobile operator has always enjoyed a dominant position in the mobile industry and in a PN environment, this could continue.

In the PN, there will be new functions that a mobile operator will wish to take up. One example is the PN agent. The PN agent is a management entity located in the interconnecting structure (most likely to be the Internet) that keeps track of each Personal Node and all the clusters within a PN. Because there are many ways to implement a PN agent, it is viewed more as a concept than a physical node. The PN agent may be centralised and under the control of an operator or service provider or distributed over several operators. It can also be hosted by the user's terminal [3].

P-PANs and PNs are likely to play a big role in the mobile operator's future service offering. For the mobile operator of today, one of the challenges is the convergence of different networks: fixed, mobile and wireless. Fixed network operators have been offering a wide range of services from networking to applications and software to clients in order to provide a more comprehensive suite of services and a one-stop-shop option. Vertical integration of services has played a part in the growth of the fixed network operator for some time now. With mobile operators moving into the same service offering, there are several things first to consider[6]:

- Ability to integrate different network types
- Availability of devices for use
- Customised applications/software for each market
- Simple Charging and Billing
- Differentiated Quality of Service
- Personalisation of Services, Security and Privacy

The mobile operator seems to be moving onwards from their present 2G or 3G business models into new waters. The 3G and beyond business models are different for different operators. Depending on the strategy that the company has adopted, the different operators could choose different aspects of 3G to pursue.

One important new capability of the PN that could affect the mobile operator is that of a self-configuring network. A self-configuring network is a network that is able to simplify the life of the user by configuring itself to the user's needs and requirements based on a set of pre-defined and configured rules or policies. This is in theory the P-PAN network concept itself. The P-PAN is a network that is able to automatically configure itself, based on earlier set requirements and information in order to give the best trusted connectivity available. Its goal is to make things easier for the user.

For the future there will be new business models related to the mobile operator role. Mobile Operators could offer Edge routers/PN-Agents with PPAN connectivity services in their networks. They could also offer managed PN services enabling easy authentication, authorisation, and billing for users with multi-access support. New business models would be required for such services.

5) *http://fismat.umich.mx/adhocnow/ – cited 280705.*

6) *There are probably other factors to consider but those listed here are of great importance to the mobile operator and their service offering in a PN concept.*

5 The Future Mobile Operator – General Aspects

The Mobile Operator faces a future full of new opportunities as well as threats, depending on the way it sees it. Although the Mobile Operator's core competencies are to build and manage mobile networks, this will not be enough in the future industry where converged services and technologies will be integrated. In the mobile value chain, it is likely that the Mobile Operator will continue to play a significant role. The Mobile Operator has already taken up secondary roles in service and content provision and transaction management.

Most often the Mobile Operator has a strong financial position and some of them could be active players when it comes to finding good positions in the future value networks and Business Models. With this financial strength, several important attributes that the Mobile Operator needs to further develop could be:

- Brand
- Service differentiation
- Simplicity
- Trust and security
- Customer service.

Whichever area the Mobile Operator chooses to move into or to integrate into its present business, these features will continue to be needed. A good brand name not only catches the attention of potential users, it also invokes a feeling of trust when users recognise the brand name.

Trust and security are particularly important features when it comes to financial transactions. This also applies when personal data is exchanged. Mobile Operators will have to work closely with financial institutions to develop processes where these two features are of the utmost importance. A working relationship with security firms will also be needed in order to provide secure transactions to users.

Efficient customer service and help services gained from past experiences should become an integral part of the Mobile Operator's business processes. This service can also be seen as a means of channelling the customer's requirements, needs and preferences to the Mobile Operator which the operator can then use to improve services.

Service and product differentiation are needed to address different corners of the market. Some users find certain services more important and useful to others. Also, to differentiate their service from other mobile operators, it is also possible that special or unique services will play a distinguishing role. With so much competition amongst Mobile Operators, price is one way to differentiate and with schemes such as pre-pay or flat rates with data services, mobile operators can then differentiate themselves from others. Of course, other service differentiation methods exist for example after sales service and customer care or bundling of services.

Simplicity and ease of use are something that users would want, even as the number of services and applications increases. This is one area where the Mobile Operator has an advantage over the other actors. The Mobile Operator is in the best position to integrate different services and to offer them as one simple package to users. The customer expects to be able to communicate and connect to the services over distances, at any time and everywhere. There should be no technical borders as to service availability and roaming. Life should be made simpler and not more complicated with new services. Services should be intuitive to use and technology should be invisible.

In order to survive, the Mobile Operator beyond 2010 will have to face key issues such as:

1 Implications of a converged mobility – broadband environment
2 Business refocus
3 Network sharing
4 Finding new and profitable business models.

The traditional strengths of the operators in the value chain network have been their network assets, but now there is a tangible shift towards brands, organisation and market channels.

There is a consensus among network operators that long-term convergence of voice and non-voice networks must be more than an exercise in cutting costs. The main drivers of change will be to find values around mobile and broadband. The focus of the industry has to shift towards services and there will be an increased competition from players from other important industry sectors.

The future operator will mainly sell access and a range of applications, content, devices and services. Operators have to formulate new business strategies that in co-operation with its customers could derive values from intelligent edge applications and devices. In the long term, operators will have to evolve from being network service providers to being communications enablers. The new opportunities could include tools for proper interoperability management of home, public, business and other private networks.

6 Operator's PN Strategies

As PNs and other new concepts in technology as well as new technologies are introduced to the mobile industry, they provide a multitude of new areas which old players can get involved in. For the mobile operator, being the player with the greatest market influence at this point in time, it is likely that related services would fall under their service offering. Network provisioning will not be sufficient to carry the mobile operator into the future but together with other services, the mobile operator will be able to provide a significant number of value-added services that are not part of their business today. In a PN environment, some areas (old and new) which could lead to new revenue streams for today's mobile operators could be:

- Customer aggregator
- Value network integrator
- Content provider or content aggregator
- Clearinghouse for Billing, DRM and Security
- Financial service provider
- Mobile, Internet and
- Ad Hoc Network Service Provider (providing Hosting services, Edge routers, PN agents etc.)

The above list[7)] mentions some of the possible roles that the mobile operator could go into. Some of these roles are already in place but others are new and could become a requirement in a PN scenario. As the industry actor with the most customers today, the mobile operator has a large potential base with which to work with. For the mobile operator, two key functions to concentrate on could be converged services and the personalisation of PN services for its customers.

One aspect to note in the PN scenario is that the network operator's role in the PN will probably depend very much on the type of industry it is addressing. As we move from a general market to one that is specialised and personalised in many ways, the business models will become more industry specific to address the needs of each particular industry.

Industry specificity may result in the mobile operator and other players coming up with differentiated services for each case and for groups of users within each case. Of course, it all depends on the business strategy that the players choose to adopt and the business models developed. Within the general PN concept, the business model will still be used to describe the different operators' relationship with each other, their relationships with content aggregators, service and application providers, device manufacturers, platform and equipment manufacturers or providers, and also other peripheral players in this mode. However, for the specific cases, different business models may be in place and therefore relationships between actors could differ for each of the cases.

The Regulator is responsible for the allocation of spectrum, definition of usage policies and rules but also for handing out penalties for violation of responsibilities. Players in this area include the government, regulation authorities, event associations and standardization groups.

PNs are expected to operate in two different modes, High Data Rate (HDR) and Low Data Rate (LDR). PN technology could be temporarily deployed at local sites like a sports arena or an accident area. Spectrum issues might have time, cost, interoperation and location based constraints.

Publishing rights (DRM) might be a possible conflict area. The 2001 European directive on copyright forces member states of the European Union to implement legal protections for DRM. Digital Rights Management however has an uncertain legal status in many countries since the content rights of users and content publishers are ill-defined.

Customer aggregator

PNs and WLAN have the advantage over UMTS or GPRS of providing high bandwidth at low cost. The Mobile Operator could provide the end-user with detailed position information about their reachable WLAN interconnection points.

Locations where PN Networking will be common need interconnection to IP networks. Many mobile operators have already got UMTS and also WLAN-networks. While WLANs today address areas where professional users have a special interest to connect it might also be useful for the operator to consider locations such as shopping malls, city centres and various public arenas for their future WLAN roll out.

UMTS deployment is a common pan-European initiative with special licence requirements on coverage, capacity and roll out. WLAN and WiMAX technologies are global initiatives which are developing independently and quickly in many environments. Due to the different scopes of the technologies there might be delays in their convergence.

The service could be combined with information about the closest Internet connection and other useful information such as price, network load and other

7) *The authors acknowledge that other new roles could exist for the mobile operator that have not been listed here.*

services offered at the interconnection points such as printing or other non-technical services.

Value network integrator

The Mobile Operator could offer a complete concept for P-PAN clusters and support them with customer care, billing, sales and marketing. Overall technical support for PN technology could be added (installation, operation and maintenance etc). The technology should be so simple that anybody could install and operate it.

In a future with maybe thousands of PPAN clusters the cost for the roaming, DRM and security processes will be much too large for a small PN operator. A Mobile Operator can use its knowledge and experience to set up necessary agreements and processes to cost effectively deal with a large number of business partnership agreements. The costs could be financed by small transaction fees as a percentage of the value and/or a fixed fee per transaction.

The billing alternatives for a PN operator are to:

- Invoke their own billing system
- Use the billing system of an ASP
- Use the billing systems of the mobile operators.

Billing systems are expensive and set up will cause time delays for the service launch plan. To buy a billing system is therefore not a realistic option for a small and independent PN operator.

The competitive advantage for a Mobile Operator vs. an ASP is the customer base and the existing billing procedures for mobile services. There are also national accounting laws that could complicate this matter further. In principle it is also possible to use prepaid cards issued by the Mobile Operator to pay for the network access.

Service and content distribution

PNs will enable new ways of broadcasting and/or multicasting. The mobile network can be used to distribute services or content to a limited number of distribution points. The advantage of using the mobile network instead of the fixed network is that the distribution points may be mobile or be located in locations beyond the reach of the fixed network.

The content could be forwarded from the distribution points to the end-users via WLANs or P-PANs. This provides an opportunity for a limited number of individuals who are within the communication range of the distribution point to consume content of common interest. They could also share the cost of providing content to the distribution point via the mobile network.

*m*Commerce

A PAN gateway related to a special individual and no one else should be able to communicate with Point of Sales (PoS) terminals enabling *m*Commerce. The PN-device could then be used as an electronic wallet. The PoS terminal will have to verify the credit worthiness of the individual customer requesting the service and check the user's unique rights to use the dedicated terminal. Security is absolutely essential for possible *m*Commerce applications.

The central position that mobile operators hold today means that they will probably have a significant share of the PN and are able to hold a strong position in the PN market. However, these operators will have to adapt to a new type of business where they are not just selling access or bandwidth. Service provisioning and other value-added services will be important in the PN market and the operator is in a good position to provide all these. The ability to develop new services and to change focus is likely to be key ingredients to the mobile operator's role in the PN.

Operators have good abilities to compete with ICT houses by offering total support for PN Services. They have a unique ability to make combined service packages from PN Network and other services. Another role could be to provide global PN roaming support.

7 Conclusion

In the current communication markets, companies deliver services to customers in cooperation with other market players using different business models. The aim of this work has been to examine the implications of PNs on existing business models, which means development of business models for PNs.

The business model concept has been examined and made operational by adopting the business model ontology developed by Faber et al. There are four basic constituent elements in this business model ontology: Service design, technology design, organisation design, and finance design. From the business models sketched out it is possible to see a multitude of opportunities for the actors in the value network like the mobile operator and the device manufacturer with respect to PNs. The implementation of the business model will be dependent on existing market conditions and actor capabilities.

One of the MAGNET project's goals is to utilize the PN technologies to make the public life much easier. The public life covers the individual's interaction with the public system. This includes the welfare system, tax system, libraries, transportation, schools, nursing homes, and health care system just to mention some.

PNs will consist of a self-organised model, a service oriented model and a combination model. The operator's role in the PN is still undefined but its dominant role in today's mobile industry ensures that it has a good chance of succeeding in the many opportunities that will arise from PN services.

New business strategies and business models will have to be developed to cater to the operator's new working environment. PNs present both threats and opportunities to the mobile operator. Some new and thrilling roles that could be further developed by the Mobile Operators are Customer Aggregation, Value Network Integration, Service and Content Distribution and *m*Commerce.

In the long term a split-up of the Value Network could be foreseen and Partnership Relation Management will be increasingly important to boost the market for PN Services.

Acknowledgement

This paper describes work performed under the supervision of the Magnet-Beyond project which is part of the EU's IST program. MAGNET-Beyond is a continuation of the MAGNET project (www.ist-magnet.org). MAGNET Beyond is a worldwide R&D project within Mobile and Wireless Systems and Platforms Beyond 3G. MAGNET-Beyond will introduce new technologies, systems, and applications that are at the same time user-centric and secure. MAGNET Beyond will develop user-centric business model concepts for secure Personal Networks in multinetwork, multi-device, and multi-user environments. MAGNET Beyond has 30 partners from 15 countries, among these highly influential Industrial Partners, Universities, Research Centres, and SMEs. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the Magnet-Beyond Project. The authors would like to thank all members of the Magnet-Beyond Project, who have contributed to the development of the concept presented in this paper.

References

1 MAGNET. *Description of Work*. Annex 1, 2003.

2 Faber, E et al. *Designing Business Models for Mobile ICT Services*. 16th Bled Electronic Commerce Conference, Bled, Slovenia, June 2003.

3 IST-MAGNET. *Refined Architectures and Protocols for PN Ad-Hoc Self-Configuration, Interworking, Routing and Mobility Management*. October 2005. (IST-MAGNET WP2, Task 4, D.2.4.3 Draft)

4 Osterwalder, A, Pigneur, Y. *An e-Business Model Ontology for Modelling e-Business*. 15th Bled Electronic Commerce Conference, Bled, Slovenia, June 2002.

5 Afuah, A, Tucci, C L. *Internet business models*. New York, McGraw-Hill/Irwin, 2001.

6 Methlie, L, Pedersen, P. *Designing business models for customer value in heterogeneous wireless networks*. Bergen/Grimstad, May 2005.

7 Porter, M. *Competitive Advantage*. New York, Free Press, 1985.

8 Niemegeers, I G, Heemstra de Groot, S M. *From Personal Area Networks to Personal Networks: A User Oriented Approach*. Personal Wireless Communications, Kluiwer Journal, May 2002.

9 IST-MAGNET. *Socio-Economic Impac and Business Models for PNs*. December 2005. (IST-MAGNET WP1, Task 4, D1.4.1b)

Su-En Tan is a post-doc researcher with the Center for Information and Communication Technologies (CICT) at the Technical University of Denmark. She recently completed her PhD in Electronics and Communications from the same university. She is currently working on the IST MAGNET-Beyond project.

email: suen@cict.dtu.dk

Rune Roswall, MSc BA, graduated from Linköping Technical University in 1975 and holds an MSc Degree in Technical Physics / Applied Mathematics and a B.A. Degree in Economics. Rune Roswall is primarily responsible for technical and business development within TeliaSonera Sweden, focusing on Multi-Access, Wi-Fi technology, IPv6 and Peer-to-Peer networking. At present Mr. Roswall is working with Business Models, User Requirements and User Profiles for Personal Networks for the European 6 FP Magnet Beyond project.

email: rune.roswall@teliasonera.com

Interconnection and Billing Policies for Personal Networks

RAJEEV R PRASAD, VASILEIOS S KALDANIS

Rajeev R. Prasad is Director in Sabita Holding, Denmark

Vasileios S. Kaldanis is Research Engineer in National Technical University of Athens

MAGNET proposes a dynamic shift in the business model from supply centric to demand centric models. Policies for access and interconnections would need to be addressed in order to maximize the social welfare and competition. Billing would be a complex issue that would need readdressing with the changes in the paradigm. Requirements of internet's stakeholders and the telecommunications' stakeholders would have to be integrated in a single billing model.

1 Introduction

My Personal Adaptive Global Network (MAGNET) will develop user-centric business model concepts for secure Personal Networks (PN) in multi-network, multi-device, and multi-user environments. By means of adding personal network into the definition of architecture the focus of the legacy business model shifts more towards users' needs and requirements.

It is assumed throughout the MAGNET project that the user requires greater access to a variety of data. There would be a multitude of sources from transmitting and/or accessing information. Since the market entrance of GSM the value added service offered is increasing and with that the business model is evolving, as we notice in the case i-mode and 3G. Around 1994 state control over the incumbents throughout the European Union started to dilute and policies were put in place to facilitate greater competition among network providers. With the evolution of the mobile telecommunication the personalisation towards the user has also been enhanced, thus the personal area network technologies have started penetrating the market, such as Bluetooth and Zigbee.

Wireless Personal Area Network (WPAN) has enabled new applications under different user scenarios where the WPAN expands the coverage area.

Certainly, network providers retaining their central role in the business model would seem ideal since they have the economies of scope and scale and the billing mechanism to facilitate cost and traffic control. Wireless Local Area Network (WLAN) has witnessed a diverging business model where wireless internet service providers (WISP) and independent WLAN providers are driving the value chain, with billing and network managed by them.

Network operators have also entered this market and some by acquiring WISPs. The business model will be the key determinant in devising the policies for interconnection and billing.

Table 1 presents a list of scenarios generated per theme as provided in [1]. These cases share themes with one another; therefore a common platform can be used by the content provider to provide service.

	Diabetes case	Smart shopping	Student case	Mobile gaming	Distributed work	Digital living	Whole person	Virtual home truck	Emergency case
Transportation	X				X		X	X	
Entertainment		X	X	X		X	X	X	
Society/Citizen	X					X	X		
Health care	X								X
Emergency	X								X
Surveillance	X		X			X	X	X	
Collaborative work			X		X		X	X	
Community	X	X	X	X	X	X	X	X	
Travelling	X				X			X	
Education			X						
Shopping		X					X		

Table 1 MAGNET users' case and themes

ISSN 0085-7130 ©Telenor ASA 2007

Such as in the case of Health Care, the hospital could be providing service over its personal network and then the question would arise of how the billing and interconnection could be managed if the business model were to be service/content provider centric?

The question that arises from implementation of a MAGNET concept such as MAGNET.Care[1)] is how is the service managed? There is a multitude of interconnections and a multitude of formats of data. We propose a possible concept for billing and look into Internet Engineering Task Force's (IETF) and 3GPP's efforts in understanding the requirements of users.

The expansion of PAN towards a PN will stress the existing radio spectrum due to the increasing demand for data anytime and anywhere. Therefore, the traffic needs to be optimally managed, for which we propose converged billing. Telecom operators who must share revenues and profits coming from multiple services, content or application providers whose customers expect to receive a single bill for all the services they subscribe to. Adoption of the right billing strategy among telecom operators will lead to better service exploitation, optimization and integration or interoperation of future solutions with existing network.

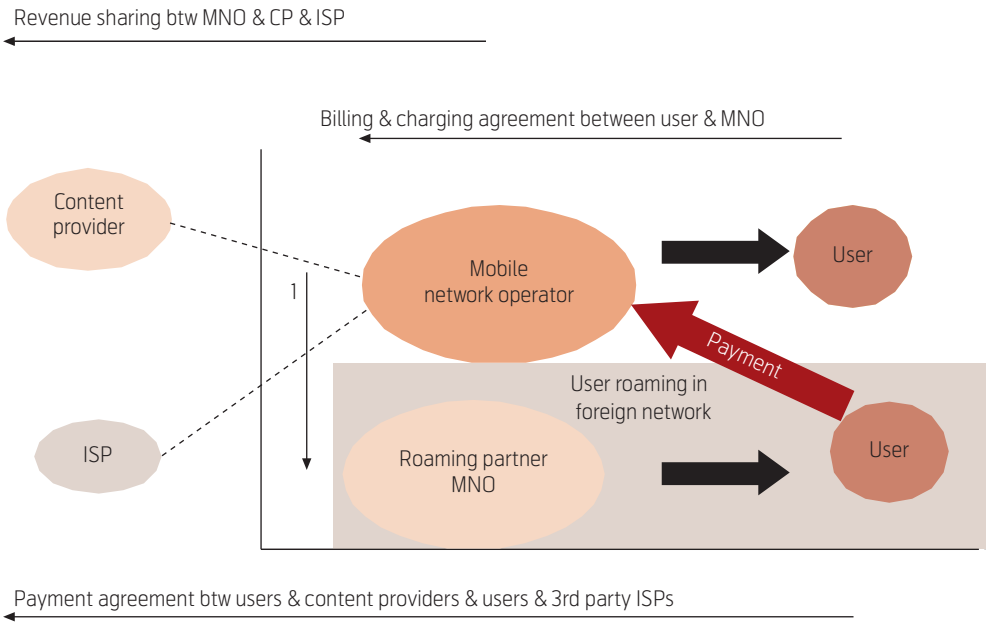
This paper will present the evolving business models based on network provider centric and service/content provider centric in Section 2. Section 3 will determine the problems relating to access pricing and interconnections in the PN environment and the subsequent section, Section 4 will address how billing will be managed for the users/subscribers and the access costs. Section 5 will be the conclusions of the study.

2 Business Model

The supply chain has become a major focus in the telecom industry, many papers have been published proposing a shift in the business paradigm [2–4]. The value chain will be less supply driven and more demand driven than before. Addressing the dynamics in the value chain is essential since it opens the gate to the uncertainties in regulating the interconnections and billing mechanisms for PNs.

Currently, the mobile industry is mobile network provider (MNO) centric as illustrated in Figure 1. In this situation the user/subscriber has a contract with the MNO who also manages the billing system.

In case of 3G the practice among the operators is aptly illustrated also in Figure 1, it is via the MNO that the user can access the services and contents. The revenue generated is shared among the providers, for which the billing is managed by the MNO. Since the liberalisation in early 90s and common EU policies were brought into place in order to catalyse competition, operators expanded into new markets.



1: Access Contract for Network sharing charges & User roaming revenue sharing

Figure 1 MNO Centric Business Model

1) *http://www.ist-magnet.org/pr*

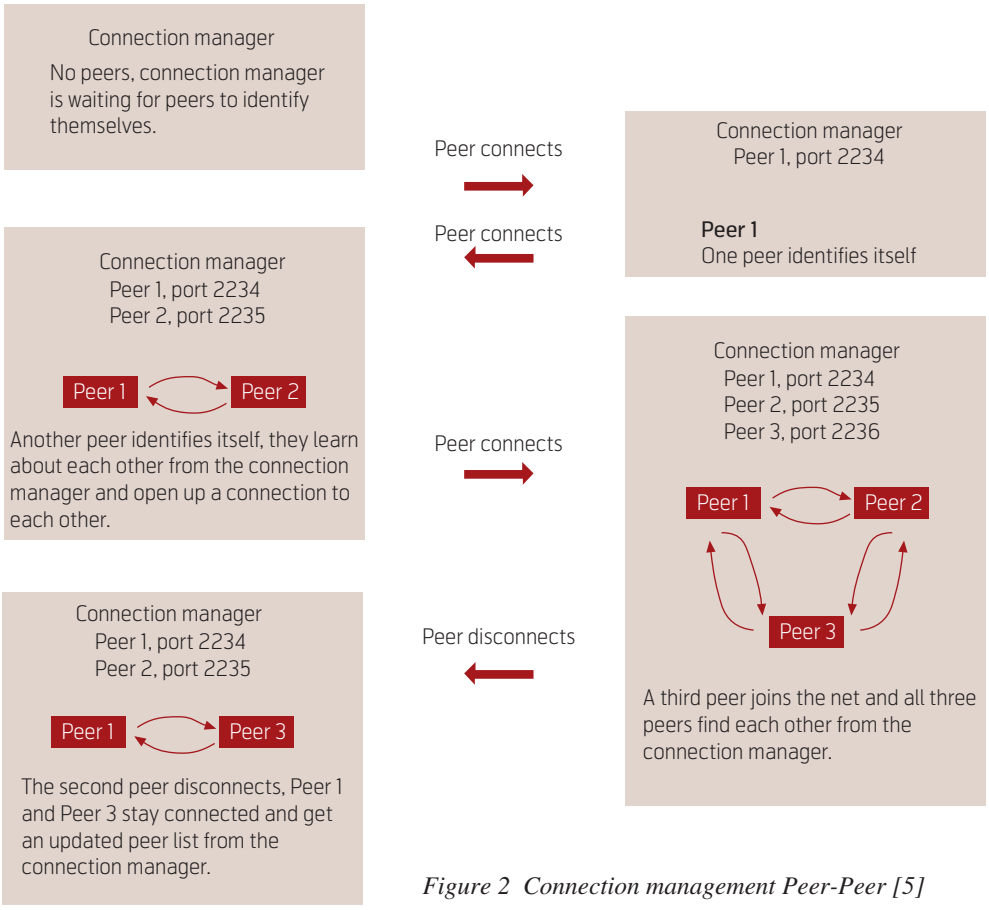


Figure 2 Connection management Peer-Peer [5]

The regulations stipulated incumbents to share their network at a fair price with the new operators. Over the years this has made the market more efficient and has diluted the power of the incumbents, the business model evolved into new MNOs leasing the network from the incumbents and/or the carriers by placing themselves as mobile virtual network operators. Nonetheless, this shift did not change the business model fundamentally, except added another stakeholder in the value chain. However, this led to diffusion of power from the supplier as the competition grew and the market forces were more strongly determined by the users' needs and requirements. Internet represents a close to equilibrium business model, the users of the Internet participate in providing contents and services too for both financial and non financial purposes.

The user makes an independent contract with the internet service provider (ISP) and service/content provider. The internet allows the user/subscriber to co-create in the virtual domain and also allows the user to build peer-to-peer network. Figure 2 illustrates the architecture for a peer-to-peer network.

This is facilitated by a service provider such as Kazaa, eDonkey, iMesh etc. Similarly, PN is exhibiting development of use cases where peer-to-peer will be possible, hence the business model would be service/content provider specific. In user cases such as mobile gaming the user will be able to play by establishing peer-to-peer network, the PN would further enable users to also multicast similar to Internet Relay Chat (IRC) protocol. IRC is provided by entities like MSN, the server forms the backbone of IRC, providing a point to which clients may connect to talk to each other, and a point for other servers to connect to, forming an IRC network.

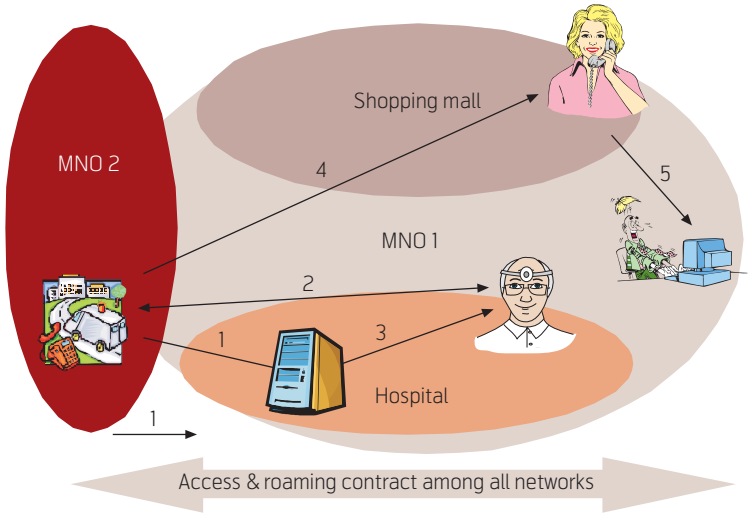
In MAGNET.Care the scenario developed suggests integration between various networks and Internet.

Figure 3 represents users moving and communicating haphazardly. There is intra-PN communication, communication to and from other networks etc. The data being exchanged is from voice to high data rate being transmitted, e.g. from an ambulance and/or user accessing information from an Internet site. In this scenario we are assuming that a service provider is not the same as an MNO, thus the business model is service/content provider centric.

In this scenario the content provider is controlling the charging and billing, moreover presence of the mobile operator in the model MNO can also be substituted in several use case scenarios. A shopping mall (service and/or content provider) can deploy its own network and a user visiting the shopping mall can conduct trade over the mall's network. This value

chain can also get more dynamic if the mall allows remote access to its network, and then the MNO will also be a participant in the value chain. Finally, the dynamism of the model is more enhanced with the possibility of deeper convergence between telecommunications and other industries. There will be a need for a coherent and equilibrium inter-industrial business model, in order to attain value flow.

Now we have described two different business models, the latter is comparable to the business activities conducted on the Internet. However, in the telecommunication industry network interconnection is a critical issue and also limitation of the bandwidth. Inexpensive technologies such as WLAN are allowing much smaller players to enter the network market, where they are able to provide network coverage to a city centre. Furthermore, with the advent of mobile nodes that can roam between cellular network and WLAN the interconnection issues thus become a more dominant aspect.



1. Ambulance accessing patient's record
2. Doctor accessing patient's record
3. Multicasting
4. Exchanging data
5. Sending alert to family

Figure 3 Service/Content Provider Centric BM

3 Interconnection Policies and Personal Networks

Attempting to model an appropriate billing scheme for personal networks several approaches could be followed based on existing solutions as applied by MNOs today. As described before the two general approaches (MNO centric and service/content provider centric) may able to provide a possible hybrid billing solution in the case of PAN/PNs where numerous interconnections occur dynamically among different actors.

In an MNO centric model approach where the underlying network infrastructure is owned by the mobile operator itself, the expected interconnection policies will not be much different than what it is right now. However, in the case where the service/content providers maintain their own network infrastructures as a channel to distribute their digital products (e.g. a WLAN in the city centre) these providers may cannibalize into the high return market area of the MNOs. For example, voice over IP (VoIP) is quite a cheaper solution than cellular voice calls; therefore, demand for this service would be greater. Consequently, a roaming PN user may choose to perform a long distance voice call exploiting the VoIP capability of his PDA rather than making a more expensive cellular call, using a service provider's application (e.g. skype) via its own enabling private network. In this way, the PN user could effectively benefit from peer-to-peer technologies in order to avoid the imposing roaming costs of cellular networks.

Without MAGNET technologies, supporting a roaming user equipped with a PDA capable of accessing all wireless network technologies requires a direct negotiation regarding access fees while also providing efficient billing management handling among the infrastructure owners end-to-end. The user may seamlessly roam from a 3G network to a WLAN one with no service break, e.g. mobile gaming online in an IRC comparable architecture. The user's requirement will be certainly not to receive different bills for every time he walks in and out of a cellular network to WLAN. Nonetheless, a user who is either conducting high data rate transfer and/or has high elasticity to price will require being able to switch to a high bandwidth and/or inexpensive network.

The access pricing is essential to be established in order to avoid ineffectiveness in ex-post application of Competition Law. Since the first steps towards liberalisation until 2002 incumbents still have considerable strength, most notably in local loop, not much competition is observed and the unbundling is progressing slowly [6]. Several papers [7] have analysed one-way and two-way access scenarios to mitigate anticompetitive behaviour and to also encourage other ex-ante objectives.

In the PN case where we assume the co-existence of small access network owners such as a shopping mall, unbundling the local loop (ULL) is not essential for the shopping mall; however calls originating from a UMTS network and terminating in the shopping mall creates a one-way access. Manifesting the power with the MNO to determine the access price with the

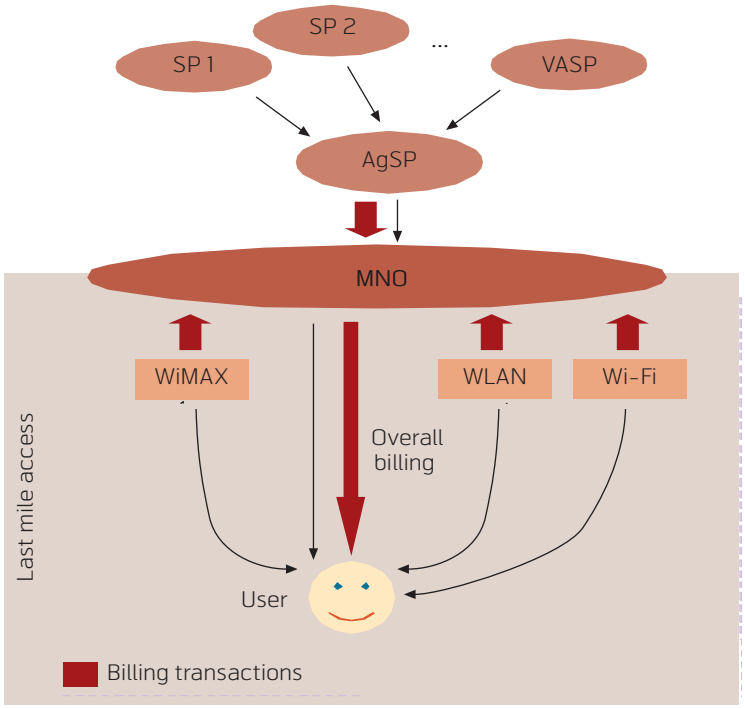


Figure 4 A PN billing scheme via MNO

shopping mall also exposes the mall to predatory pricing, excessive pricing, price squeeze, etc. by the MNO, for instance.

ULL becomes a lesser issue for MNO who does not have infrastructure covering the last mile and who owns the WLAN network in the shopping mall under a revenue sharing context, for instance. The MNO can circumvent the incumbents of last mile by pricing techniques and also by innovative technology, e.g. WIMAX (see Figure 4).

As seen in Figure 4, the concept of pricing PNs using the last mile access (network and services) via the home or a roaming MNO is illustrated. Several service providers (SPs) can be aggregated by an Aggregated Service Provider (AgSP) and make their services available to an MNO via specific interfaces. Furthermore, the MNO itself may establish Service Level Agreements (SLAs) with local third party network infrastructure providers (e.g. WLAN, Wi-Fi, short range WiMax, etc) in order to simplify the billing process for its client who aims at using a plethora of cost effective PN services. Each local network/service access provider (as an SLA partner of the MNO) may individually charge the client for the relevant service costs consumed directly at his monthly account bill. In this way the client can have a direct access to web services by paying low cost connectivity for his PN (see [16]).

In a PN scenario the interconnection access charge does not vary from how it is today regarding local loop and therefore does not warrant a new theory. The regulatory bodies will have to consider the interconnection under the one-way and two-way access context. In our scenario of a shopping mall complication of a two-way access is foreseeable if the service/content providers have their own infrastructure. The regulators will face following issues in determining a fair access price [7]:

The first issue concerns optimal access pricing and whether it should be reciprocal; the access price should be offset against the social welfare maximisation where the total industry profit is sufficient to cover the total fixed costs. Regarding reciprocal pricing, agreement can easily be reached between operators originating similar size traffic or similar marginal costs. However, an operator starting from scratch will find it more difficult to enter a two-way access agreement.

The second issue in the PN with the smart shopping scenario we have to regard is whether the mall's network is competing with the MNO's network or are they complementary? Nonetheless, the size of the traffic over a mall's network would be a combination of WLAN and WPAN techniques, so potentially the size of a single user's data could be larger if originating from the mall's network and terminating in an MNO's or carrier's network as opposed to vice versa. Should the price be determined by the regulators or the market? If determined by the market information symmetry becomes a critical issue, where perfect competition will have to be assumed [6].

Finally, according to Laffont (2001) [8], all interconnection costs will be set at competitive level if the missing price is recovered. He is referring to the calling party pays principle; there is a missing price, namely price for receiving costs. This pricing model was resorted to in the Indian market, but is now abolished although it is a lucrative marketing strategy for operators. Nonetheless, the case is not attractive for users.

The main item to address is the billing management. This is a major issue to tackle when we are expecting peer-to-peer network (see Figure 2) and multicasting that is comparable to IRC protocol services in PN. As illustrated in Figure 3 the service/content provider is managing the billing, however how would the roaming cost be managed?

4 Billing Management and Roaming

Mobile business models of the present are MNO centric and will continue to be so as long as billing is performed based on the typical roaming process of

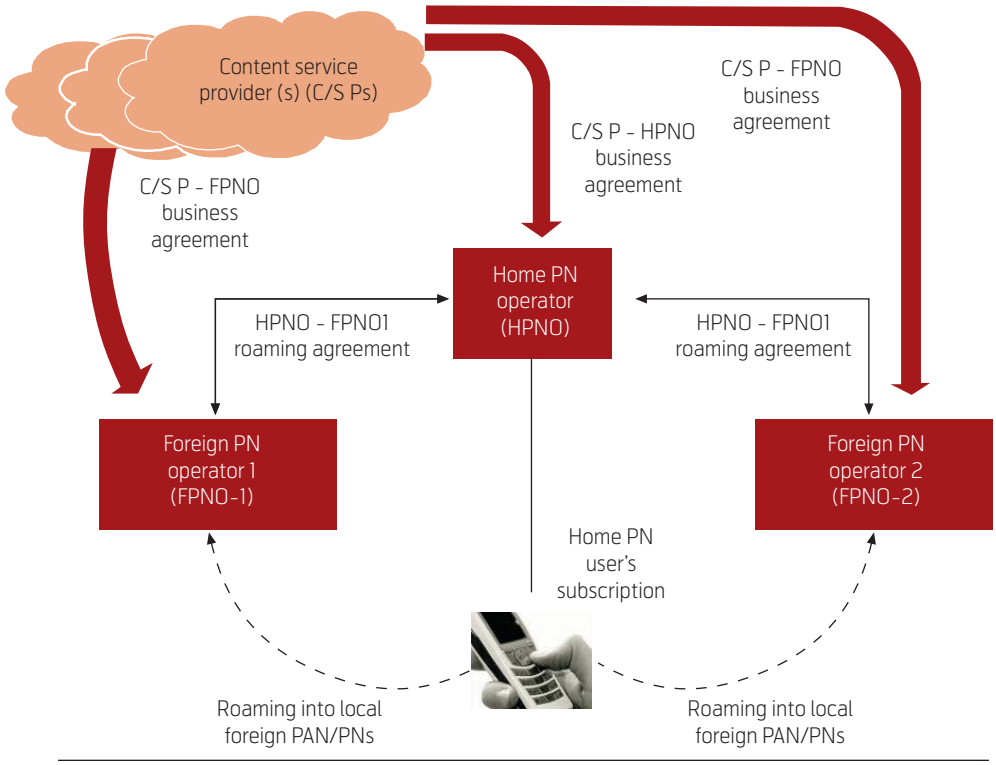


Figure 5 Proposed billing scheme for PNs

GSM [10]. In Figure 5, we adopt the traditional business modelling method when billing a mobile subscriber who is roaming into another network (foreign) away from his home network. The logical extensions to the MNOs are the Home PN Operator (HPNO) and Foreign PN Operators (FPNOs) which are responsible for supporting user mobility on networking level and service level as well. Any service the user discovers in any visiting PAN/PN could become available to him/her as long as a billing agreement among HPNO – FPNOs can be established.

Although the concept of PN operator still has not been clearly defined within the MAGNET framework, ideally it can be used for the sake of the billing process. Any roaming user currently away from his originated PAN should be able to define/verify himself in any foreign network. In other words, there should be a secure interaction among agents able to verify that this user is really what he claims. That is probably the most secure way of authenticating a user who cannot acquire a certain level of trust by another local user in the foreign network, in order to become attached to that.

In a service/content provider centric business model where they also own the infrastructure e.g. MAGNET.Care, shopping mall etc. billing can be performed by this provider; however we will certainly notice a complication in the management of roaming fee among a plethora of small networks. The second issue to address is that the MNOs should be prepared to cater to larger traffic size which would also be more sporadic than what it is today. The solution would have to be a combination of access technology and billing [10], not only facilitating the cost incurred for the network operators but to control the traffic as well. Among the use cases in PN we observe deeper convergence between Internet and mobile communications. Therefore, an integrated platform for charging, accounting and billing is required. The Internet Engineering Task Force (IETF) and 3GPP have been addressing the requirements of stakeholders for the 3G market.

IETF [11–13] are addressing the changing needs of users, ISPs and service/content providers. Users are willing to pay additional charges in order to ensure a better quality of the provided services. It is apparent that each stakeholder has their specific requirements for the billing and charging. This makes the billing method complex to integrate, since the user's demand is for a one-stop billing.

One of the options available is to outsource the activity of billing and charging to a clearing house. 3GPP Working Groups and UMTS Forums [14, 15] analysed the users' requirements and those of the other stakeholders in the value chain in the UMTS network.

Users/Subscribers essentially require from a UMTS network a single bill and charging which is simple

and easy to follow. MNOs' requirement is to be able to manage various billing models which cater to traditional billing as well as dynamic profile based access control. Within MAGNET we have come to the conclusion that applications such as Diabetes require dynamic profile based access control. The service provider gives varying level of access to different stakeholders, so the access to a patient's record to a doctor will be extensive and for instance to a friend it should be limited.

A layered charging architecture approach is structured in three layers: transport, service and content are some of the requirements of the MNO. The management of each layer will be conducted separately and hence the charging can be applied autonomously. Theoretically, it seems feasible however that this model is not in line with the users'/subscribers' requirements.

Perhaps a pseudo bundle-charging would be of preference to the user; here we are referring to a concept where the user pays a single fee for a package. The MNO offers a charge to the user which is a combination of fees from services/contents in the package which has been opted by the user.

However, from the independent content/service providers' point of view, there is an emerging demand that each authorised player should be able to apply dynamically the desired pricing policy for its services' usage. These requirements are building the platform for the case we have presented in this paper.

One hypothesis that can be presented is that billing and charging for users/subscribers is a consequence of perception. Which means, since users/subscribers would like to see one-stop billing, they only pay their monthly bill for subscription to the network which also includes voice and low data rate services. While in the process of using other forms of contents/services they are charged instantly at the time of purchasing the service.

5 Conclusions

Personal network concept is leading towards deeper convergence between telecommunications and other industries, hence allowing also service/content providers to drive the industry. Coherence in the confluence of business models of several different industries will have to be managed. Internet business model is the most comparable to the paradigm personal network is moving towards. The complexity in the management of access and interconnection would still exist; nonetheless at this stage of R&D in MAGNET it still does not seem that a new theory would be warranted; whereas billing would require to be addressed as infrastructures could be afforded by service/content providers and we can witness multitudes of such hotspots.

Due to Mobile Network Operators' large client base and position in the value chain as an operator, billing could be managed by them. Clearing house is another option available. Whichever model chosen, it should complement the chosen business model and provide the equilibrium between all stakeholders.

Acknowledgement

The authors of this paper would like to acknowledge all the contributions that different companies and persons have made in relation to the MAGNET project and especially the contributions to WP1.

References

1 *User requirement for PN to drive the definition of a valid architecture*. (MAGNET Report, D1.1.1b)

2 Koutsopoulou, M, Kaloxylos, A, Alonistioti, A. Charging, Accounting and Billing as a Sophisticated and Reconfigurable Discrete Service for next Generation Mobile Network. *IEEE Semiannual Vehicular Technology Conference (Fall VTC2002)*, Vancouver, Canada, September 2002.

3 Henten, A, Saugstrup, D. *The PN Concept in a Business Modelling Prespective*. Copenhagen, Denmark. (CTI Working Papers, No. 95)

4 Prasad, R, Kaldanis, V et al. *Paradigm Shift of Business Models and its impact on Billing in Personal Area Network: A Diabetes Case Study*. Shanghai, MAGNET Workshop, November 2004.

5 PCOM:I^3 internal report.

6 Prasad, R, Monti, M. *Billing and Pricing for Personal Network within MAGNET Project*. Italy, WPMC 2004.

7 Buigues, P. *Latest Progress in LLU as reflected by sector enquiry*. LLU hearing, 8 July 2002. (Downloadable from EC website)

8 Armstrong, M. Network interconnections in Telecommunications. *Economic Journal*, 108, 545–564.

9 Laffront, J J, Rey, P, Tirole, J. Network Competition: I. Overview and Nondiscreminatory Pricing. *Rand Journal Economics*, 29, 1–37, 1998a.

10 Panagiotakis, S, Koutsopoulou, M, Alonistioti, A, Kaloxylos, A. Generic Framework for the Provision of Efficient Location-based Charging over Future Mobile Communication Networks. *IEEE 13th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2002)*, Lisbon, Portugal, September 2002.

11 Aboba, B, Arkko, J, Harrington, D. *Introduction to accounting management*. 2000. (RFC 2975) 2006, October 27 [online] – URL: http://www.ietf.org/rfc/rfc2975.txt?number=2975

12 Carle, G, Zander, S, Zseby, T. *Policy-based accounting*. 2002. (RFC 3334) 2006, October 27 [online] – URL: ftp://ftp.rfc-editor.org/in-notes/rfc3334.txt.

13 Jonkers, H, Hille, S. *Accounting Context: Application and Issues*. 2000. http://www.aaaarch.org/doc06/file-11249.pdf

14 3GPP. *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Charging and Billing (Release 5)*. June 2001. (3G TS 22.115 version 5.1.0)

15 3GPP. *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging principles (Release 4)*. September 2001. (3G TS 32.200 version 4.0.0)

16 *WiFi access in airports for mobile subscribers*. Available from: http://www.lufthansa.de

Rajeev R. Prasad received his BSc (1999) from the International School of Economics in Rotterdam, The Netherlands, and his MSc (2002) in Corporate Finance and International Business from Aarhus School of Business, Denmark. He was a strategy manager in PCOM:I^3. Furthermore, he launched a new company, Wireless Integrated Billing and Security (2003), licensing Billing and CRM software for WLAN and provided solutions for the network architecture and deployment of WLAN.
Currently, Rajeev is Strategy Director in Sabita Holding, a Danish company responsible for investments in wireless communication. Rajeev has authored several academic papers and has written a chapter in a book "802.11 WLANs and IP Networking: Security, QoS, and Mobility". His academic work has been in the fields of Economics of Innovation, Economics of Network and Corporate Strategy.

email: rajeev.prasad@sabita.biz

Vasileios Kaldanis received his bachelor degree (1998) in Physics from the Aristotle University of Thessaloniki in Greece. In 2001 he joined the Centre for Telecommunications Research (CTR) in King's College, London as a research engineer, where in 2002 he obtained his MSc in Electronic research. Since 2002 he has been working as a research engineer in the National Technical University of Athens (NTUA), where in 2005 he obtained his MBA in Techno-Economic systems. Since 2006 he is also a PhD candidate in the Department of Electrical Engineering and Computer Science of NTUA in reconfigurable networks. He has worked as a consultant for several mobile operators and other telecom companies as OSS/BSS support engineer, and his academic research experience includes active participation in numerous IST European projects (CAUTION, CAUTION++, MAGNET, MAGNET Beyond), publishing numerous papers, articles and journals. His background experience is in the area of wireless/mobile IP core and access networks, system implementation/integration, software development, service & application development, resource management for GSM/GPRS/UMTS and 4G wireless systems, business modelling and techno-economic analysis for mobile telecom & satellite solutions.

email: vkaldanis@telecom.ntua.gr

Extending Private Personal Area Networks to Personal Network Federations in Heterogeneous Ad Hoc Scenarios

LUIS SANCHEZ, JORGE LANZA, LUIS MUÑOZ

Luis Sanchez is a PhD Student at the University of Cantabria (UC), Santander, Spain

Jorge Lanza is a PhD Student at the University of Cantabria (UC), Santander, Spain

Luis Muñoz is a Professor at the University of Cantabria (UC), Santander, Spain

Personal Network (PN) is an emerging concept which combines pervasive computing and strong user focus. The idea is that the user's personal devices organize themselves in a secure and private personal network transparently of their geographical location or the access technologies used. The user expects the network to be always ready for supporting his necessities without requiring too much user involvement. Additionally, the PN must be ready to share the services it provides to the user with other users that have been authorised in order to allow the collaboration between the PNs' users. The PN Federation concept is presented as a secure cooperation between a subset of devices belonging to different PNs for the purpose of achieving a common goal or service by establishing an alliance. This paper will present firstly the mechanisms developed for the self-configuration of the Private Personal Area Network (P-PAN, the cluster of personal devices that are around the user) for describing afterwards how an extension of these mechanisms can seamlessly support the establishment and use of a PN Federation in the case that several P-PANs come together

1 Introduction

Take the concept of pervasive computing and combine it with strong user focus and you get Personal Networks (PN) [1], [2]. PN is a collection of one's most private devices referred to as personal nodes. From a technical point of view, the PN is seen to consist of devices sharing a common trust relationship. Security and privacy are the fundamental properties of the PN, as well as its ability to self-organize and adapt to mobility and changing network environments.

The IST project MAGNET [3] vision is that Personal Networks (PNs) will support the users' professional and private activities, without being obtrusive while safeguarding privacy and security [4]. A PN can operate on top of any number of networks that exist for subscriber services or are composed in an ad hoc manner for this particular purpose. These networks are dynamic and diverse in composition, configuration and connectivity depending on time, place, preference and context, as well as resources available and required, and they function in cooperation with all the needed and preferred partners.

The PN consists of clusters of personal nodes. One cluster is special, because it is located around the user. The clusters are connected with each other via an interconnecting structure, which is likely to be infrastructure based.

In order to protect the privacy of the user and the integrity of the PN, security measures are used to encrypt the user's data when it is sent outside of the device, i.e. using a wireless medium or the infrastructure. The user can reach all of his or her devices using a variety of underlying networking technologies, which are invisible to the user. The user only sees the services that are available in the PN and on foreign nodes that have been made available to the user.

Nonetheless, personal communications cannot be restricted to the services provided by the devices the user owns, but the possibility to interact with other users' PN has to be enabled in order to support the user in his/her private and professional activities. The concept of PN Federations (PN-F) is an even more challenging one since the relations between users have to be managed and the security has to be reinforced in order to not open security holes while allowing authorized users to cooperate with you. PN Federation is a secure cooperation between a subset of devices belonging to different PNs for the purpose of achieving a common goal or service by establishing an alliance. It can be established through interconnecting infrastructures (namely infrastructure case) or by direct communication between PN nodes (namely ad hoc case).

This paper presents the mechanisms that end up in the self-formation of a secure network of all the personal devices around the user, the P-PAN. Besides, it will describe how the extension of these mechanisms enables the establishment and use of PN-Fs in the ad hoc case. The paper is structured as follows: In Section 2 a survey of the work that has been done on the personal networking area as well as the key distinguishing points that differentiates it from the work described in the paper will be presented. Section 3 will sketch the mechanisms specified for the self-configuration of P-PANs putting emphasis on the support of the heterogeneity and the security. The extensions needed to the aforementioned mechanisms as well as the newly introduced procedures that are

ISSN 0085-7130 ©Telenor ASA 2007

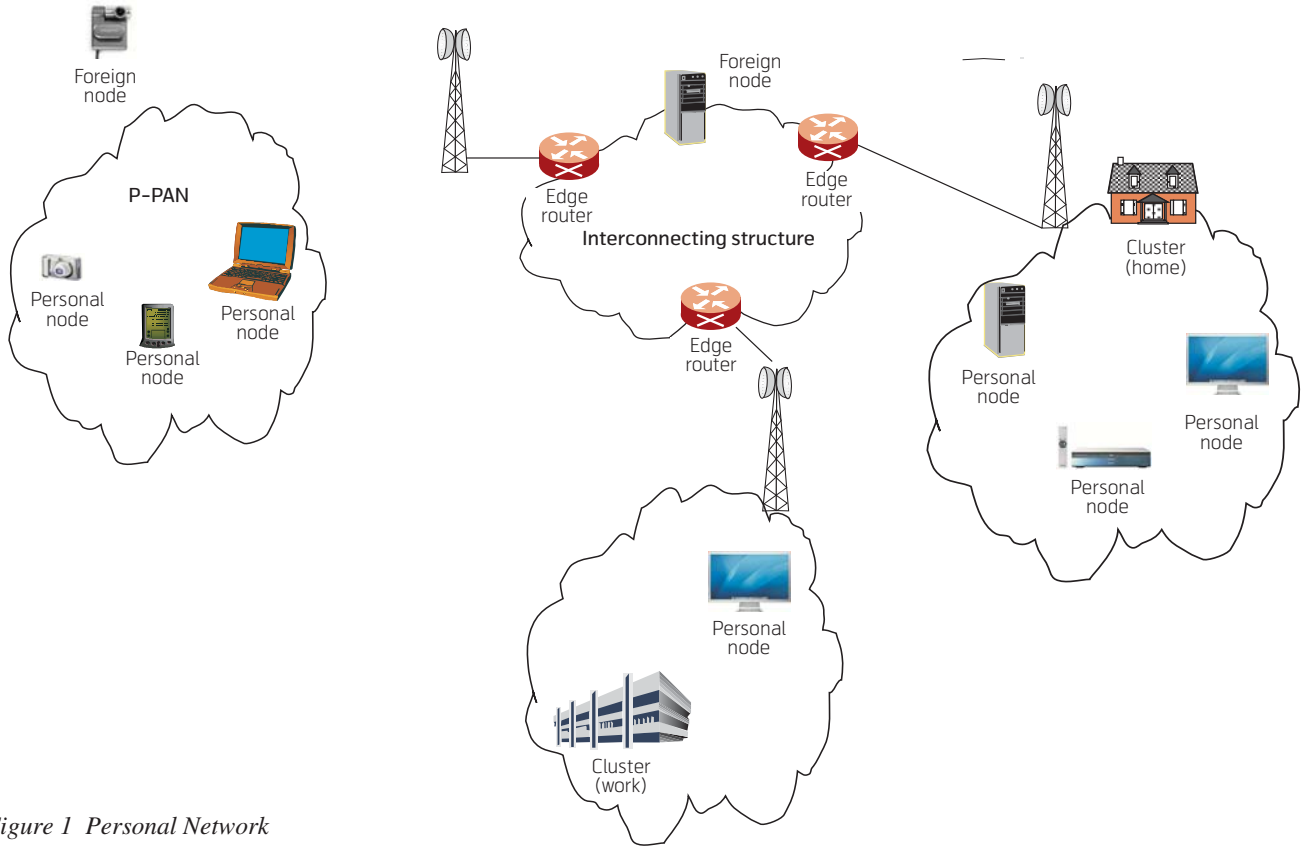


Figure 1 Personal Network

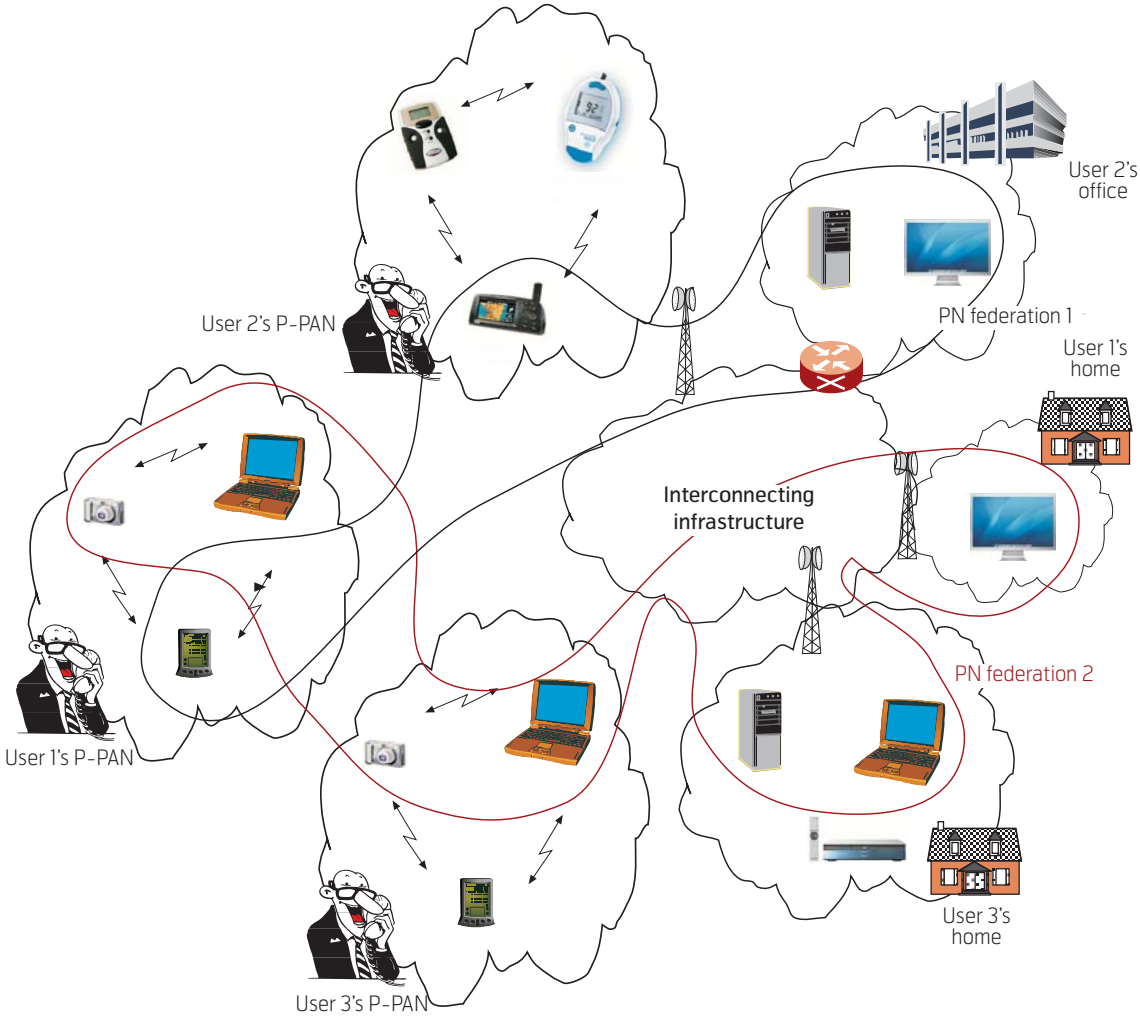


Figure 2 Personal Network Federations

ISSN 0085-7130

needed to establish and use a PN-F in the ad hoc case will be introduced in Section 4. Finally, Section 5 summarises the main conclusions from the paper.

2 Related Work

Starting with the PACWOMAN IST project [5], [6] the research on the personal networking area has gathered quite a lot of attention. More and more, the person is accompanied by a variety of devices with growing capabilities that provide to the user an increasing number of services. Contrary to other initiatives that explore fields like wireless personal area networking [7], mobile ad hoc networks [8] or self-configuration [9], [10] in isolation focus on optimizing the characteristics of each field without having much in mind about the others. The solution proposed here presents an integrated approach that copes with the different connectivity, networking and service requirements in order to accomplish the aforementioned vision of an autonomous and self-organized secure Personal Network.

The traditional view of personal area networks [7], [11]–[13], where the problem is limited to a radio coverage issue does not fully cope with the real requirements of the user that wants his/her nodes to be networked but without compromising his/her privacy, intimacy, etc. It is needed to develop a network that extends its coverage depending on privacy and security relations between the nodes, thus being able to join the same collaborative network and offering its services seamlessly to the user which owns all of them.

Most of the security frameworks that are nowadays deployed are based on third parties [14], [15] that enable users to be authenticated to each other, and to use the information in identity certificates (i.e. each other's public keys) to encrypt and decrypt messages travelling to and from. Personal Networking should not depend on third parties giving the full control of his/her devices to the user. Some security solutions [16] work in a more distributed way exploiting the web-of-trust feature. Nevertheless, it is not fully compliant with the requirements imposed by Personal Networks. The PN security architecture in general and the secure P-PAN formation in particular are based on bilateral long term trust relationships between PN devices that are bootstrapped directly by the user [17].

3 Personal Networking Concepts and Terminology

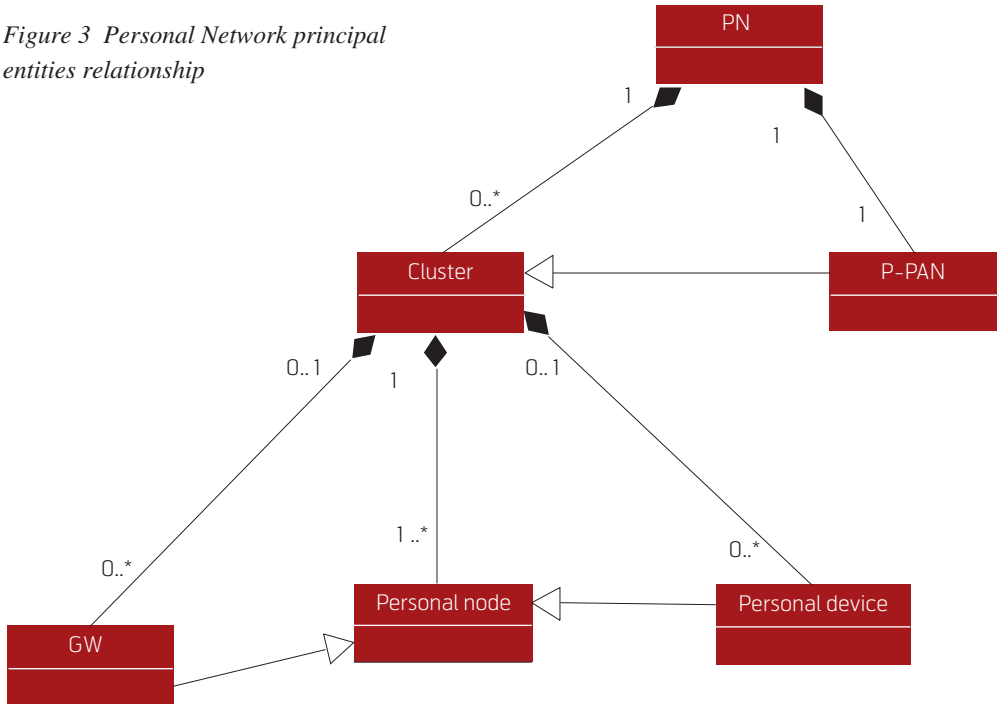
This section presents the main entities that comprise the proposed Personal Network architecture, defining as well, the terminology that will be used in this paper when describing the architecture and the different solutions adopted to support the formation and operation of Personal Networks.

As shown in Figure 1, the PN consists of clusters of personal nodes. One cluster is special, because it is located around the user. The clusters are connected with each other via an interconnecting structure, which is likely to be infrastructure based. In order to protect the privacy of the user and the integrity of the PN, security measures are used to encrypt the user's data when it is sent outside of the device, i.e. using a wireless medium or the infrastructure. The user can reach all of his or her devices using a variety of underlying networking technologies, which are invisible to the user. The user only sees the services that are available in the PN and on foreign nodes that have been made available to the user.

In this section, the terms and key concepts that are used in the PN architecture will be presented and defined.

- *Device*: Any communicating entity.
- *Node*: A device that implements IPv6 and/or IPv4.
- *Personal Node*: A node related to a given user or person with a pre-established trust attribute. These attributes are typically cryptographic keys with a permanent (as long as not cancelled, redefined or revoked) trust relationship.
- *Private Personal Area Network (P-PAN)/Cluster*: A network of personal devices and nodes, characterized by a common trust relationship, which can communicate with each other without using non-personal nodes. Nodes and devices in a cluster can become members of a P-PAN when a person enters an area where the cluster nodes are located.
  A P-PAN is often referred to as a personal bubble around a person.
- *Personal Network*: A Personal Network includes the P-PAN and a dynamic collection of remote personal nodes and devices organized in clusters that are connected to each other via Interconnecting Structures.
- *Trust Relationship*: is established when two parties communicate and determine with a measure of certainty each other's credentials to set up a secure communication channel using encryption mechanisms. When devices and nodes want to establish a secure communication channel, they build a trust relationship by whatever means possible.

Figure 3 Personal Network principal entities relationship



- *Imprinting*: A procedure to bootstrap a trust relationship between two nodes that basically consist of an authenticated key exchange.

- *Gateway node (GW)*: A Personal Node within a Cluster that enables connectivity with the Interconnecting Structures.

- *Interconnecting structures*: Public, private or shared wired, wireless or hybrid networks such as a UMTS network, the Internet, an intranet or an ad hoc network.

- *Foreign node*: A node that is not personal and cannot be part of the PN. Foreign nodes can either be trusted or not trusted. Whenever trusted, they will typically have an ephemeral trust relationship with a node in a PN.

Figure 3 indicates how the PN entities defined in this section relate to each other. Note that the P-PAN is a materialization of the Cluster concept. The difference between the P-PAN and the rest of the PN Clusters is that the user is in the surroundings. This difference only takes importance on the so-called Service Abstraction Level (see Section III). Therefore, in the remainder of the paper we will use both terms without distinction.

4 P-PAN Formation

The proposed scheme aims at being a fully distributed approach for resilience and efficiency reasons which will act in a proactive way for having always the P-PAN formed for the user to not suffer from additional delay and which will assume only security and privacy boundaries for the P-PAN contour.

4.1 Supporting Heterogeneity

The capability of working in a heterogeneous environment is a must for future personal networks. This heterogeneity will be mainly reflected in terms of the different air interfaces that will coexist in these scenarios requiring additional schemes to handle this heterogeneity.

The concept of isolating the upper-layers from underlying wireless technologies and thus providing real multi-mode can be achieved by introducing a Universal Convergence Layer [18]. The UCL will mainly act as an enabler for backward and forward compatibility by defining a common interface towards the network layer while managing several different wireless access technologies independently of their PHY and MAC layers. In this sense, the solution adopted makes it possible for the nodes to have a single IP address independently of the number of air interfaces

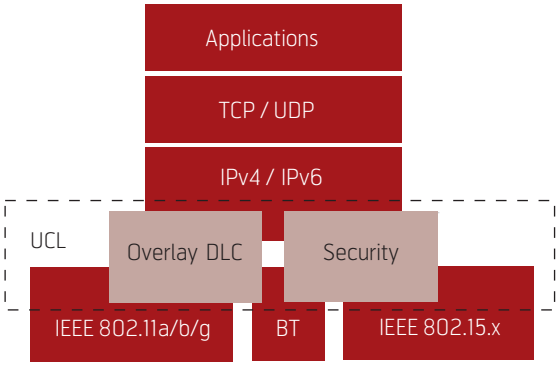


Figure 4 UCL High-Level Architecture

ISSN 0085-7130 ©Telenor ASA 2007

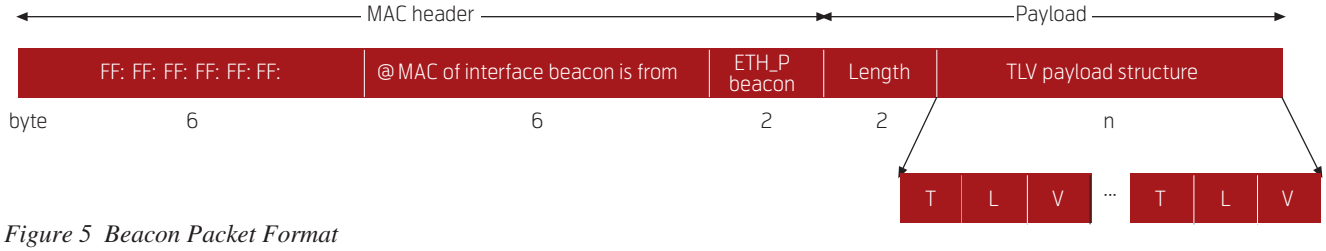


Figure 5 Beacon Packet Format

it has. This way the routing protocol placed in layer 3 will be able to settle routes embracing multiple radio domains in a completely seamless manner.

The combination of these two techniques, UCL plus ad hoc routing protocol, enables the solution proposed to manage the heterogeneity that will appear in the P-PAN environment.

From a security perspective, one of the most important design goals of UCL is to make sure that use of a heterogeneous radio specific legacy security system does not cause any additional security vulnerabilities. In order to accomplish this, UCL includes a key derivation function which generates radio specific link keys from the long term PN keys generated during the P-PAN formation exercise. In addition to making parallel use of different radio systems secure, the presence of UCL also provides an opportunity to upgrade or even complement the legacy radio systems used in MAGNET.

4.2 Enforcing the Security

This is the key feature to be provided for the P-PAN formation. In this sense, the objective of the following mechanisms is to assure that only personal nodes are members of the P-PAN and that any personal node in the area is also able to participate in the network.

As a result of the pairing procedure [17], the peers derive a long-term shared key that is subsequently used to secure the communication between them. Each device must store this information securely in the form of a device record. A peer record mainly contains the following information: (1) Peer identifier – a unique identifier associated to the device; (2) PN key – the shared secret derived from the pairing process.

Nevertheless, this imprinting procedure is only the baseline over which the trust is built in the P-PAN formation. In our solution, we assume the support given by the UCL [18], which deals with layer 2 encryption so authenticity and integrity of received frames can be immediately assured.

Firstly, a beaconing process has been implemented in order to be aware of the immediate neighbours continuously. The periodicity of the beacons is to be designed depending on the dynamicity of the cluster. In this sense, context discovery and context awareness techniques could be applied to the inter-beacon time.

The beacons are used for advertising the node presence. Mandatory payload field: Node ID – 20 bytes public identifier. Currently it is derived as a digest over the peer's public DH (Diffie-Hellman) key used during the imprinting procedure. Optional payload field: Node name – Human friendly identifier. Used for UI purposes only.

Upon the reception of a beacon, it will be checked if it is already registered in the neighbours table; if the peer is already registered, the entry will be updated by reinitializing the expiration timer associated (note that there could be multiple entries for a single identifier, each of them with a different associated device so as to allocate multimode devices). If the neighbour is not already registered an authentication method will be called in order to assure that the discovered node is really a personal node. It is important to note that each entry is unique by the pair: identifier of the neighbour and device from which the beacon was received. In this sense, it will be needed to perform a different authentication process for each of the air interfaces with which it is possible to communicate with the neighbour.

The authentication is performed through a three way handshake (Request – Response – Success) in which the long-term shared key is used to verify the identity denoted by the identifier field in the beacon received.

The same procedure is used for neighbour authentication and exchange of link session keys used at UCL level for Intra P-PAN communications encryption. The following notations are used:

- | – concatenation
- HMAC(key, data) – hashing function
- g^x – public Diffie-Hellman key
- N_X – nonce
- E(key, data) – symmetric encryption

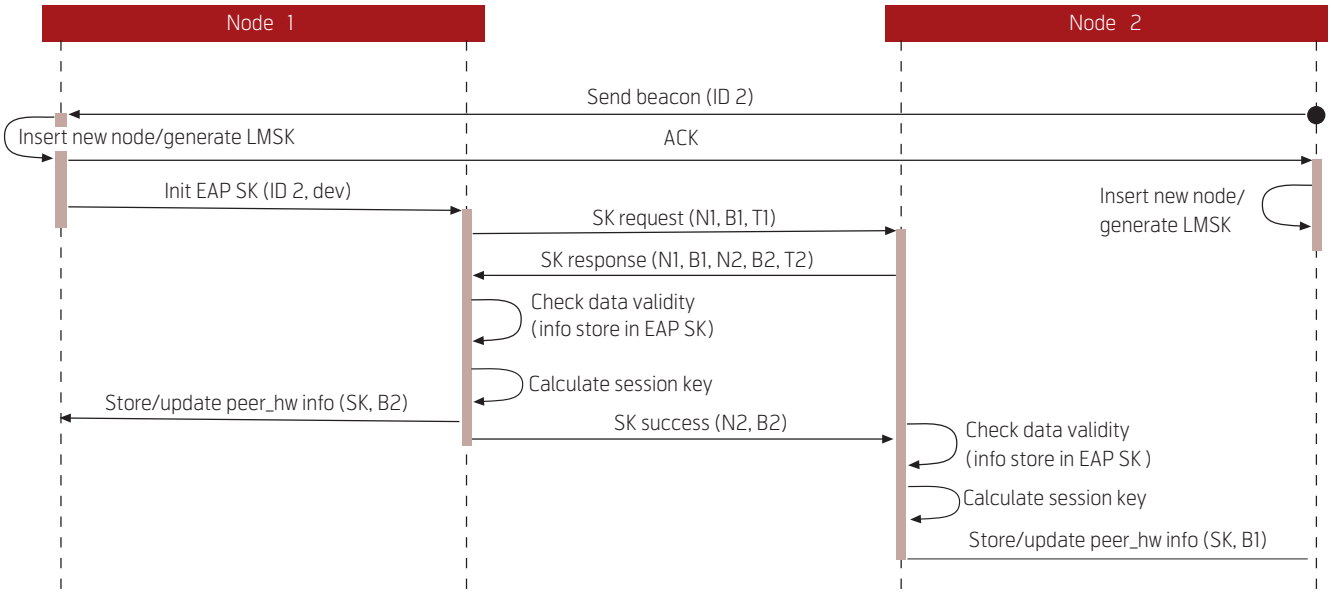


Figure 6 Session and broadcast keys exchange protocol

device	MAC address
eth1	12:34:56:78:9A:BC
bt0	11:11:11:11:11:11

device	MAC address
eth1	CB:A9:87:65:43:21
bt0	22:22:22:22:22:22

device	MAC address
eth1	33:33:33:33:33:33

Node A Pn neighbors table

@IP	@MAC	dev	L2 key	BCAST key
fc01:1111: bbbb	CB:A9:87:65:43:21	eth1	454	PNPN
fc01:1111: bbbb	22:22:22:22:22:22	bt0	909	GWGJ
fc01:1111: cccc	33:33:33:33:33:33	eth1	111	CCCC

Node B Pn neighbors table

@IP	@MAC	dev	L2 key	BCAST key
fc01:1111: aaaa	12:34:56:78:9A:BC	eth1	454	XYXY
fc01:1111: aaaa	11:11:11:11:11:11	bt0	909	QTQT
fc01:1111: cccc	33:33:33:33:33:33	eth1	222	CCCC

Node C Pn neighbors table

@IP	@MAC	dev	L2 key	BCAST key
fc01:1111: aaaa	12:34:56:78:9A:BC	eth1	111	XYXY
fc01:1111: bbbb	11:11:11:11:11:11	eth1	222	PNPN

Figure 7 P-PAN formation example neighbours tables

Symmetric encryption is done using AES cryptographic algorithm with a key length of 256 bits.

- Node 1 receives a beacon from Node 2
- Node 1 sends EAP_request / MAGNET_SK (E($LMSK_{1\_2}$, $N_1 \mid B_1 \mid T_1$))
- Node 2 replies with EAP_response / MAGNET_SK (E($LMSK_{1\_2}$, $N_1 \mid B_1 \mid N_2 \mid B_2 \mid T_2$))
- Node 1 sends EAP_success / MAGNET_SK (E($LMSK_{1\_2}$, $N_2 \mid B_2$)

where $LMSK_{1-2}$ (Link Master Session Key) is calculated as HMAC_SHA_256 (K_{PN}, "MAC_1+MAC_2").

Use of the MAC addresses of the candidate radios in the derivation function ensures that different pairs of hardware adaptors of a radio subsystem share different link keys even for the same pair of devices. This is particularly relevant in the presence of detachable wireless interface adaptors (USB or card based).

The SK_{1-2} (link layer Session Key) is computed as HMAC SHA-256(g^{1-2}, $N_1 \mid N_2$) and is valid for T_2 seconds ($T_2 \leq T_1$). This procedure is run any time a new neighbour is discovered by a peer and whenever the derived session keys expire.

Besides the authentication process, upon the addition of a new entry, the layer 2 session key generation and exchange procedure will be triggered.

On a heterogeneous scenario like the depicted one the information necessary is stored in tables upon successful finalisation of the authentication and key exchange procedure.

Finally, if the layer 2 session key exchange has successfully ended, the nodes' broadcast keys (the one for the air interface associated) will be exchanged so each one will have the counterpart broadcast key in order to use it for decryption.

Figure 7 shows an example of which information the nodes would manage after a P-PAN is formed.

For the authentication and layer 2 keys distribution, Extensible Authentication Protocol (EAP) primitives are used to transport the information exchanged. Advanced Encryption Standard (AES) is used for encrypting the frames at the UCL. Additionally, as shown in Figure 8, packets are signed to enforce the integrity of the information.

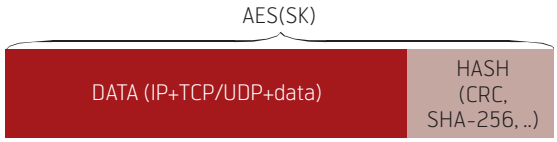


Figure 8 Data PDU Format after UCL

Authenticity, integrity and privacy are assured by using this format. Together with the flat addressing scheme described in Section 4.3, this allows the UCL to filter personal traffic and prevent any impersonation attack. This is, if a packet comes from or is directed to a personal IP address, it will only be allowed to pass through the UCL security checks if such packet has been encrypted using a personal link session key.

Once the aforementioned procedures have been accomplished all the communications between personal nodes within the P-PAN are assured as long as each of the components of the network is trusted through them.

4.3 Intra P-PAN Communications

The self-configuration of the P-PAN starts with PN address autoconfiguration for which stateless autoconfiguration will be used. To this end, it is specified that the PN address consists of a concatenation of a 40 bit PN prefix and a 64 bit Interface ID which is mapped from a MAC address using the IEEE EUI-64 format [20].

As already introduced, the P-PAN will be an IP network composed by personal nodes that are able to communicate using different kinds of PAN radio technologies. On the other hand, Mobile Ad hoc Networks (MANETs) offer the capacity of a self-configuring and self-healing network able to deal with the dynamics inside the P-PAN.

The solution adopted is to use a proactive ad hoc routing algorithm which takes advantage of the beaconing process used for neighbour detection for link appearance and breakage and that is able to maintain an updated vision of the network in all the nodes belonging to it. In this sense, a personal node will always know which are the rest of the members of the P-PAN it is currently in.

Intra P-PAN communications is then enabled to embrace a heterogeneous multihop path as long as the combination of the UCL and the ad hoc routing protocol allows it.

5 PN Federation Formation and Use

In [19] the PN-F cycle was divided into two main stages, the first one dealing with the management and control, in which the definition and the participation of the PN-F is agreed, and the second one dealing with the networking, in which the actual mechanisms for securely interconnect devices belonging to different PNs take place.

This section will sketch how an extension of the procedures specified for the P-PAN formation in Section 3 can support the two steps that comprise the networking stage of the PN-F cycle, namely PN-F Formation and PN-F Use, in the ad hoc case.

5.1 Trust Establishment

The imprinting procedure leverages a node to node trust that is supervised by the user. A similar approach can be followed in the case of PN-Fs in which the trust is established between PNs and both users are involved. This is the first extension necessary. The primary keys exchanged in this case would be shared between all the nodes belonging to both PNs. This way, whenever two nodes that are members of different PNs have been paired, they will have a pre-shared secret that they can use to authenticate each other, similarly to the way two personal nodes would authenticate each other. These pre-shared keys would have different characteristics from the personal keys. In this sense, while a personal primary key shared between two personal nodes is only destroyable upon user revocation, the key shared between two PNs can be ephemeral and destroyable upon expiration or due to misbehaviour of one of the users.

In the primary personal keys case, the nodes store the keys using the Node ID as index. Then when the two nodes meet, the appropriate primary key is selected based on the Node ID information embedded in the beacon packets (Figure 4). For the PN-PN case, the keys should be stored based on a common PN Identifier that all PN nodes would share. Additionally, this information should also be embedded within the beacon packets. This is another extension needed to support PN-Fs. Thus, mandatory fields for the bacon payload (Figure 4) are finally both the Node ID and the PN ID.

Following this approach, a node has N-1 primary keys (where N is the size of the PN). Each of them is associated to each of the other N-1 personal nodes in the PN. Also, it would have 1 primary key per PN with whom a previous “imprinting” procedure has been carried out. The same primary key is used to derive the session keys with all the nodes in the neighbouring PN.

Another possibility that would not require the users to meet beforehand in order to exchange the primary keys is the use of a typical PKI structure such that each PN Identifier is signed by a Certification Authority (CA) that is trustable for both users. In this case, whenever two nodes from different PNs meet, they firstly would have to exchange a shared secret based on the information stored in each other’s certificates. Then, the procedure would be the same as if the secret would have been shared using a pairing procedure as the one used for personal nodes.

It is important to note that this trust establishment is only meant to enable the authentication of nodes. Further authorization to make use of the services provided by the user PN should be based on this authentication. Besides, the solutions proposed enable node authentication but if really sensitive information might be disclosed, user authentication should be put on top.

5.2 Mesh Connectivity Establishment

Taking into account the extensions described in the previous section, it is easy to see that in the ad hoc case of a PN-F, i.e. when several P-PANs come together, the result at connectivity level will be a full secure mesh. Making use of the same mechanisms used for authentication, session key exchange and encryption in the P-PAN formation, nodes belonging to different PNs that are in the same radio domain will be able to authenticate each other and exchange the link session keys to be used afterwards. The main difference is that whenever a beacon arrives, the first field to be evaluated would be the PN Identifier. If it indicates that the beacon comes from a personal node, then the Node ID field would be necessary for requesting the appropriate primary key. Conversely, if it comes from another PN member, the PN Identifier would be the one used for selecting the appropriate primary key to be used in the subsequent phases.

The data is sent using the same security enforcement mechanisms (see Figure 8) independently of who is the recipient of the packet (a personal or a foreign one), since there is no reason not to protect the communications with others in the same way as you protect your internal communications.

5.3 Network overlay establishment

Once we have established a connectivity level that prevents impersonation and supports privacy, integrity and authenticity, a network overlay can be set down. This network overlay includes the nodes from the different P-PANs forming the PN-F.

The first extension to be included in order to support the formation of a PN-F is the specification of an addressing scheme. In this case, the proposed solution is to have a dedicated addressing space for each PN-F

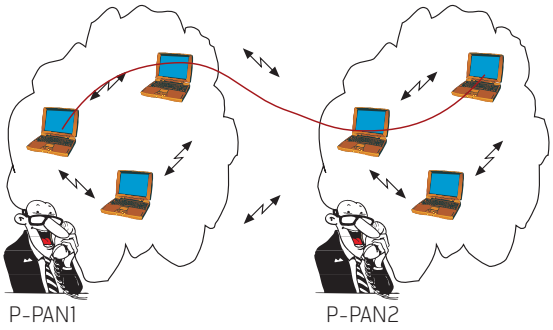


Figure 9 Ad hoc network overlay establishment for PN-F formation

a PN participates in. Similarly to the case of Intra P-PAN communications, the flat addressing does not only ease the routing procedures but is also used to prevent impersonation and to filter down the traffic that should not be allowed. In this sense, upon the reception of a packet at the edge of one of the involved P-PANs, the gateway node can, after decrypting and assuring the integrity of the incoming packet, check the IP header and decide whether to allow the packet to pass or not, depending on whether the packet comes from a PN that is a member of this federation or not.

Similarly to the P-PAN formation, the network overlay establishment will be based on the deployment of a MANET like ad hoc routing that would enable the end-to-end path discovery and maintenance between PN-F members belonging to different P-PANs. For the P-PAN case, a proactive routing protocol was chosen due to the requirement of quickly and always ready networking. Nevertheless, the use of a proactive routing protocol for the PN-F case would be too costly, mainly taking into account the possible large size that an ad hoc PN-F could have (e.g. meeting room, conference, etc.). In this case, the use of a reactive routing protocol seems more appropriate. The extension required is then two-fold: on the one hand to implement the reactive routing protocol and on the other hand to develop the mechanism at the network level of P-PAN nodes such that whenever a packet is issued to another personal node, the proactive routing is used, whereas the reactive one is called whenever the packet is destined to a PN-F node. The use of different addressing spaces enables this filtering.

Nodes will have multiple network identifiers (i.e. IP addresses) that they will use whenever they want to access a specific service provided under the auspices of a particular PN-F. In the ad hoc case of PN-F a network overlay will be established such that P-PANs of the PN-F members will form a network identified by a pre-established addressing space.

6 Conclusions and future work

Personal Networking is a promising research and economic field that imposes a big set of challenges that have to be overcome before it could be fully operational. This paper has described the mechanisms that enable the self-configuration of a Private Personal Area Network around the user overcoming the heterogeneity while reinforcing the required security. Besides, it has been shown how these mechanisms only require minor extensions to support the establishment and use of PN Federations whenever different persons with their P-PANs meet together.

Contrary to other descriptions of cluster or Personal Area Network [4], [8] that limit the concept to a matter of radio coverage (e.g. 10 m range), the concept of cluster proposed in this architecture stands on an opportunistic, distributed, multihop and proactive approach based on the trust relationships established between the cluster constituents. Further, it copes with the heterogeneity support, dynamic adaptation, infrastructureless environment survival and privacy requirements imposed by the P-PAN concept. The clusters will be as large as possible (as long as a new personal node or device is reachable through a PAN air interface, the cluster will add a new wireless hop to its structure), adding new personal nodes and devices as soon as they appear in the cluster surroundings.

The mechanisms described in this paper focuses on the connectivity and network level of the PN architecture [21]. Further procedures at service level are needed for a full-blown Personal Network and Personal Network Federation, but they were out of the scope of this paper.

Additionally, no mention of air interfaces has been included into the paper since, as already mentioned, the architecture and solutions proposed have been designed in order to support the heterogeneity in terms of radio interfaces that nowadays exists in the wireless communications area. The Personal Networking paradigm extends the short-range communications concept that is followed in typical PAN approaches. Unlike PANs, with a limited geographically coverage, PNs have an unrestricted geographical span, and may incorporate devices into the personal environment regardless of their geographic location. As already introduced the final aim of the PNs is to be an enabler for the ubiquitous computing standing on a strong user focus.

It is also important to note that a proof-of-concept implementation has been successfully integrated and used for both the validation of the techniques designed and the analysis of its conformance to the

personal networking system specifications. The description of this implementation can be found in [22].

Finally, and taking the aforementioned proof-of-concept implementation as a baseline, future work is focused on building a set of Pilot Services on top of a PN platform. The envisaged Pilot Services offer a framework to assess usability and acceptance of PN services and provide user feedback to the research activities. Pilot services will help the project assess the market potential of the overall PN architecture and services, produce exploitation plans and build the business. The feedback from the pilot will be invaluable for the research activities to further guide the research and pursue the long term MAGNET vision.

Acknowledgements

This paper describes work undertaken in the context of the IST-FP6-IP-027396 'My personal Adaptive Global Net and Beyond' IST-MAGNET Beyond project. MAGNET Beyond is a worldwide R&D project within Mobile & Wireless Communication beyond 3G. MAGNET Beyond will introduce new technologies, systems and applications that are at the same time user-centric and secure. MAGNET Beyond will develop user-centric business model concepts for secure Personal Networks in multi-network, multi-device, and multi-user environments. Please visit www.ist-magnet.org

The authors would like to acknowledge the collaboration of their colleagues from the MAGNET Beyond Consortium.

References

1 Niemegeers, I G, Heemstra de Groot, S. From Personal Area Networks to Personal Networks: A user oriented approach. *Journal on Wireless and Personal Communications*, 22, 175–186, 2002.

2 Niemegeers, I, Heemstra de Groot, S. Personal networks: Ad hoc distributed personal environments. *Med-HocNet, IFIP Conference on Ad-Hoc Networks*, September 2002.

3 FP6-IST-IP-507102. *My personal Adaptive Global Net*. IST-MAGNET project. 2006, October 31 [online] – URL: www.ist-magnet.org

4 Gustafsson, E, Jonsson, A. Always best connected. *IEEE Wireless Communications*, 10 (1), 49–55, 2003.

5 *Power Aware Communications for Wireless Opti-Mised personal Area Network, PACWOMAN*. IST-2001-34157. 2006, October 31 [online] – URL: http://www.imec.be/pacwoman

6 Muñoz, L, Agüero, R, Choque, J, Irastorza, J A, Sánchez, L, Petrova, M, Mähönen, P. Empowering Next-Generation Wireless Personal Communication Networks. *IEEE Communications Magazine*, 42 (5), 64–70, 2004.

7 *IEEE 802.15 Working Group for WPAN*. 2006, October 31 [online] – http://www.ieee802.org/15/

8 I*ETF Mobile Ad hoc NETworks (MANET) working group*. 2006, October 31 [online] – http://www.ietf.org/html.charters/manet-charter.html

9 *IETF Zero Configuration Networking (Zeroconf) working group*. 2006, October 31 [online] – http://www.zeroconf.org/

10 *UPnP™ Forum*. 2006, October 31 [online] – www.upnp.org

11 Shivers, O. *BodyTalk and the BodyNet: A Personal Information Infrastructure, Personal Information Architecture Note 1*. Cambridge, MA, MIT Laboratory for Computer Science, December 1, 1993.

12 Zimmerman, T G, Smith, J R, Paradiso, J A, Allport, D, Gershenfeld, N. Applying Electric Field Sensing to Human-Computer Interfaces. *CHI'95 Human Factors in Computing Systems*, Denver, May 9–11, 1995, ACM Press, New York.

13 Zimmerman, T G. *Personal Area Networks (PAN): Near-Field Intra-Body Communication*. Cambridge, MA, MIT Media Laboratory, September 1995. (M.S. thesis)

14 Austin, T. *PKI*. John Wiley, 2001. (ISBN 0-471-35380-9)

15 *Liberty Alliance Project*. 2006, October 31 [online] – http://www.projectliberty.org/

16 Zimmerman, P. *PGP Source Code and Internals*. The MIT Press, 1995. (ISBN 0-262-24039-4)

17 IST-507102 – MAGNET. *Final version of the Network-Level Security Architecture Specification*. Deliverable D4.3.2, March 2005.

18 Sanchez, L, Lanza, J, Muñoz, L, Perez Vila, J. Enabling Secure Communications over Heterogeneous Air Interfaces: Building Private Personal Area Networks. *8th International Symposium on Wireless Personal Multimedia Communications*, Aalborg, Denmark, September 2005.

19 Hoebeke, J, Holderbeke, G, Moerman, I, Jacobsson, M, Prasad, V, Wangi, N I C, Niemegeers, I, Heemstra De Groot, S. Personal Network Federations. In: *Proceedings of the 15th IST Mobile & Wireless Summit Communications Summit*, Mykonos, Greece, June 2006.

20 Thomson, S, Narter, T. *IPv6 Stateless Address Autoconfiguration*. IETF RFC 2462. URL – http://www.ietf.org/rfc/rfc2462.txt, December 1998.

21 IST-507102 – MAGNET. *Overall secure PN architecture*. Deliverable D.2.1.2, October 2005.

22 Hoebeke, J, Holderbeke, G, Moerman, I, Louati, W, Girod Genet, M, Zeghlache, D, Sanchez, L, Lanza, J, Alutoin, M, Ahola, K, Lehtonen, S, Jaen Pallares, J. Personal Networks: from concept to a demonstrator. In: *Proceedings of the 15th IST Mobile & Wireless Summit Communications Summit*, Mykonos, Greece, June 2006.

Luis Sanchez received the Telecommunications Engineering Degree by the Telecommunications Engineering School of Santander, University of Cantabria (UC), Spain, in 2002. Since 2001 he has been a researcher at the Communications Engineering Department at that university, where he is also pursuing his PhD. He has participated in several international research projects (e.g. WINE, 6HOP, PACWOMAN, MAGNET, MAGNET Beyond) corresponding to the 5th and 6th Framework Programme of the IST initiative. His research interests are focused on: 1) Personal Networking; 2) Heterogeneous Mobile Networks; and 3) Ad hoc networks.

email: lsanchez@tlmat.unican.es

Jorge Lanza received a degree in Telecommunications Engineering from the University of Cantabria (UC), Spain, in 2000. Since then he has been a researcher at the Data Transmission and Mobile Networks group of that university, where he is currently working toward a PhD in communications engineering. His research activities focus on ad hoc networks over wireless technologies, especially putting emphasis on protocol design and performance analysis of TCP/IP protocols over real test-beds, such as muti-hop wireless environments. As a member of the Technical Observatory for Smart Cards at the University of Cantabria (OTTIUC), he also works with highly regarded manufacturers, banking entities and mobile operators acquiring experience in smartcard technology, highlighting a patent request concerning security and user authentication mechanisms through mobile phones. Current research in combined mobility and security for the wireless Internet is being carried out based on the merging of wireless technologies and smartcards for current and next generation networks.

email: jlanza@tlmat.unican.es

Luis Muñoz is Professor at the University of Cantabria. He received the Telecommunications Engineering Degree by the Telecommunications Engineering School of Barcelona, Polytechnical University of Cataluña (UPC), Spain, in 1990 and the PhD also by the UPC in 1995. He joined the University of Cantabria in 1990 first as Assistant Professor of the Electronics Department and from 1996 as Lecturer of the Communications Engineering Department. He is head of the Data Transmission and Mobile Networks group belonging to DICOM. He started to work in the field of Data Transmission and Mobile Networks in 1990, first in topics related to modulation, equalisation techniques and channel coding; later in mobile networks with voice and data integration, designing and carrying out projects as TETRA for power utilities, security systems and telecontrol with real time needs. He has participated in projects of the 4th Framework of the EU R&D Programme, such as ACTS and at present he is participating in the 5th Framework IST. His group has strong relations with the Spanish Telecom operators and manufacturers companies belonging to these sectors. In parallel to this activity Dr. Luis Muñoz serves as consultant of different companies.

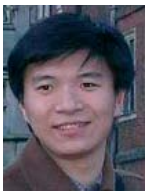
email: luis@tlmat.unican.es

Personal Networks – An Architecture for 4G Mobile Communications Networks

ANTHONY LO, WEIDONG LU, MARTIN JACOBSSON, VENKATESHA PRASAD, IGNAS NIEMEGEERS

A personal network is a network architecture which builds on various wireless networking technologies. It is responsible for glueing these wireless networking technologies to serve users. This paper considers the co-operation of several key technologies to realize a personal network; namely Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN) and Universal Mobile Telecommunications System (UMTS). This co-operation poses a new set of problems as these technologies were not designed to interwork with each other. In this paper, we present an architectural framework on which one can build a personal network using these wireless technologies. We also discuss each of these problems and propose solutions toward building a personal network demonstrator.

Anthony Lo is Assistant Professor at Delft University of Technology, The Netherlands



Weidong Lu is a PhD student at Delft University of Technology, The Netherlands

Martin Jacobsson is a PhD student at Delft University of Technology, The Netherlands

Venkatesha Prasad is a Research Scholar at Delft University of Technology, The Netherlands

1 Introduction

The next generation of wireless communications systems, commonly known as fourth-generation (4G) network [1], is envisaged to encompass a multitude of cellular and wireless networking technologies which include Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN) and third-generation (3G) cellular network. These wireless networking technologies are seamlessly interconnected by the Internet Protocol (IP) backbone network. In essence, 4G aims to transform communications architectures from traditional vertical stovepiped to horizontal integrated systems [1]. *Personal Networks* [2] are one such network architecture that can fulfill the aim of 4G with user-centric perspectives. It is a dynamic network building on the above mentioned wireless networking technologies, to facilitate personalized ubiquitous communications anywhere at anytime. Figure 1 shows the network architecture of a personal network which begins from a WPAN bubble that can be expanded or shrunk depending on the user's demands and environment. The WPAN expansion can physically be made via interconnecting structures, e.g. Universal Mobile Telecommunications System (UMTS) [3-4] and the Internet, to remote networks such as home area networks, corporate area networks or vehicular area networks. A WPAN is a network of devices which could consist of a mobile phone, a PDA, a notebook PC, a digital camera, etc. All or a parts of these devices are carried around by a person in everyday life for both work and pleasure.

This paper considers the first step toward building a personal network by enabling the co-operation between the UMTS, and WPAN and WLAN technologies. This co-operation poses a new set of problems. Current cellular and wireless networking technologies consider terminals only in isolation. In personal networks, we no longer have single terminals, but a very dynamic WPAN wanting to establish co-operation with UMTS so that it can connect with remote devices or remote WPANs. That means, current technologies are insufficient or have to be enhanced to accommodate new requirements. The major issues that need to be addressed are self-organization, establishing and maintaining quality of service for particular applications, routing and mobility management. The work presented in this paper will address all of these issues. Firstly, the state-of-the-art technologies are evaluated in view of building a personal network. We will point out the limitations with the current state-of-the-art technologies. Then, we propose solutions to these limitations within the realm of an interconnecting architecture for personal network. Finally, we present a number of ongoing key projects related to personal networks.

2 State-of-the-art Wireless Technologies

In this section, we briefly describe the state-of-the-art wireless technologies that are suitable for building personal networks, namely, WPANs, WLANs and UMTS.

2.1 Wireless Personal Area Networks

A WPAN is a short-range (typically, transmission range is limited to 10 m), low-cost and low-power consumption technology. Unlike UMTS, WPAN operates in the unlicensed Industrial, Scientific and Medical (ISM) frequency band at 2.4 GHz. The IEEE 802.15 working group is standardizing different versions of WPAN:

- IEEE 802.15.1 (Bluetooth) [5]
- IEEE 802.15.3 [6]

2.1.1 IEEE 802.15.1 (Bluetooth)

The Bluetooth specification has been made the IEEE 802.15.1 standard [5]. Hence, Bluetooth and IEEE 802.15.1 are synonymous. Throughout this paper, we use the term Bluetooth. Two or more Bluetooth

ISSN 0085-7130

Ignas Niemegeers is Professor at Delft University of Technology, The Netherlands

devices sharing the same frequency-hopping sequence form a piconet, which is a star topology. The smallest unit of a WPAN is known as piconet. Within a piconet, a Bluetooth device can play either one of the two roles: master or slave. Each piconet may only contain one master device and up to seven slave devices. Communication in a piconet is organized in such a way that the master device polls each slave according to a certain polling algorithm. A slave device is only allowed to transmit after being polled by the master device as depicted in Figure 2. Different piconets employ different frequency-hopping sequences to prevent mutual interferences. Bluetooth offers gross bit rates of up to 3 Mb/s.

Bluetooth defines not only a radio interface, but a whole communications stack that allows devices to find each other and advertise the services they offer. The core Bluetooth protocol stack, which consists of Layer 1 and 2, is illustrated in Figure 5. Bluetooth Network Encapsulation Protocol (BNEP) provides an Ethernet-like interface to the upper layer. Communications at the Logical Link Control and Adaptation Protocol (L2CAP) layer in a piconet can only be

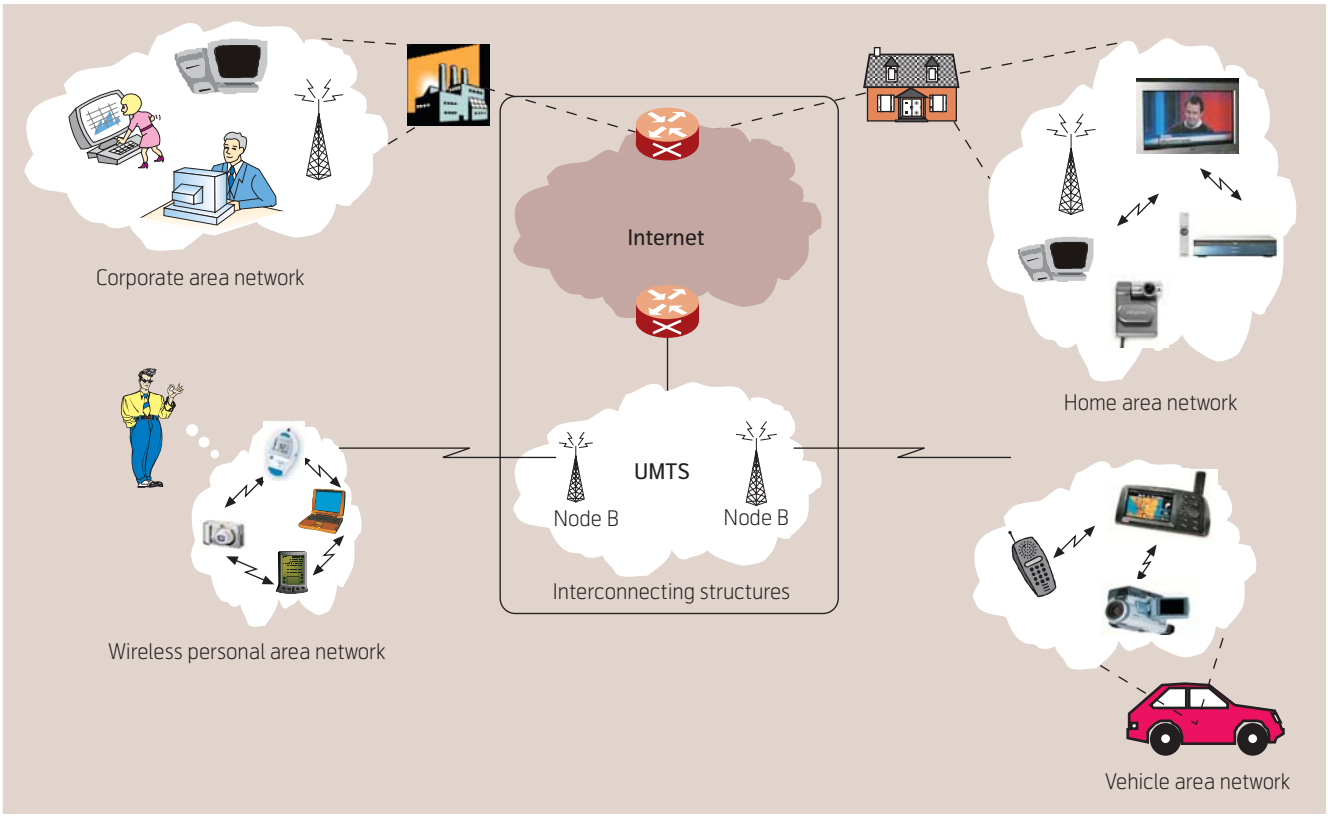


Figure 1 Personal Network

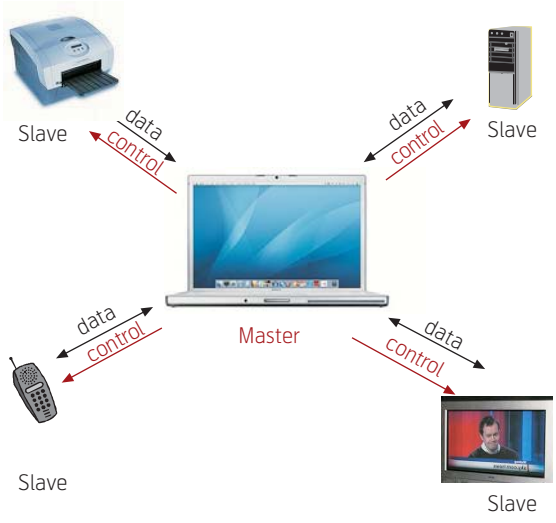


Figure 2 Bluetooth Piconet Architecture

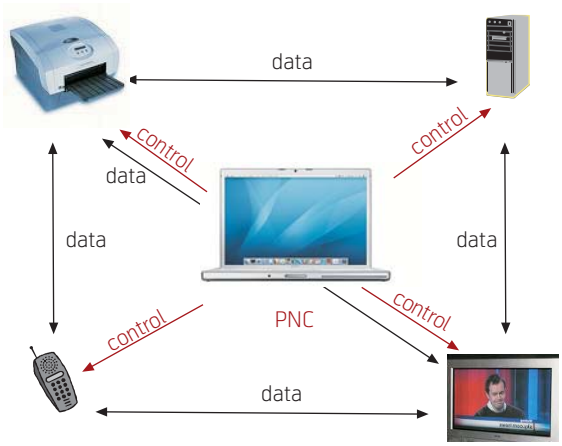


Figure 3 IEEE 802.15.3 Piconet Architecture

ISSN 0085-7130 ©Telenor ASA 2007

between the master device and a slave device. The master device acts as an Ethernet bridge at the BNEP layer forwarding packets that are not destined for itself.

2.1.2 IEEE 802.15.3 High Data Rate WPAN

Unlike Bluetooth, IEEE 802.15.3 [6] offers high gross bit rates of up to 55 Mb/s. An IEEE 802.15.3 piconet is a distributed topology with a central controller known as Piconet Controller (PNC). The PNC differs from the Bluetooth master in that it is responsible for scheduling the communication between the devices but the data traffic may not pass through the PNC. That means, the devices in the piconet can communicate on a peer-to-peer basis as shown in Figure 3. Each piconet may only contain one PNC device and up to 255 slave devices.

The IEEE 802.15.3 standard only defines Layers 1 and 2, namely, the Physical layer and the Medium Access Control layer as depicted by the center block diagram in Figure 5.

2.2 Wireless Local Area Networks

Currently, IEEE 802.11 [7] is the most mature and widely deployed WLAN technology. It also operates in the unlicensed frequency band of 2.4 GHz. The IEEE 802.11 standard defines two modes, namely, infrastructure and ad hoc. In the former mode, the IEEE 802.11 devices form a star topology with an access point as the central controller. For non-real-time services, the devices communicate with the access point through a random access technique while a polling scheme is used for real-time services. In the ad hoc mode, the devices communicate with each other directly on a peer-to-peer basis as shown in Figure 4. The IEEE 802.11 standard only defines Layers 1 and 2 as shown in the right block diagram of Figure 5.

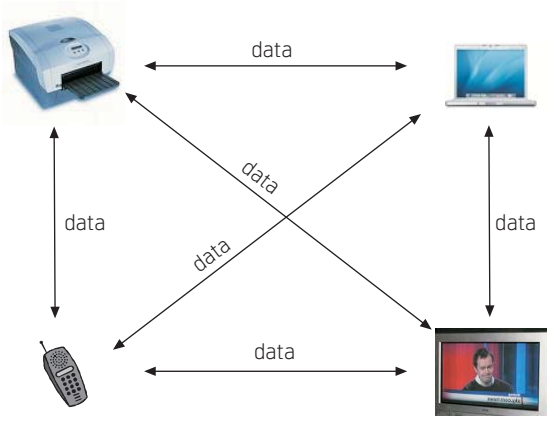


Figure 4 IEEE 802.11 Ad Hoc Mode Network Architecture

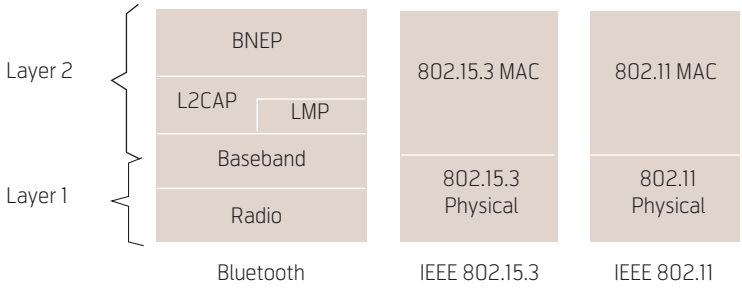


Figure 5 Protocol Architecture of Bluetooth, IEEE 802.15.3 and IEEE 802.11

Each of the above-mentioned state-of-the-art wireless technologies provides its own mechanism for WPAN formation or self-organization. In personal networks, a WPAN consists of heterogeneous devices. In this case, the WPAN formation mechanism defined in each wireless technology is insufficient. However, in the next section, we will describe the design of a personal network gateway architecture which can be used in the formation of such a heterogeneous WPAN.

2.3 UMTS

The UMTS network architecture [3-4] is depicted in Figure 6 which consists of a User Equipment (UE) (the UMTS term for mobile station) and two independent land-based network segments: the UMTS Terrestrial Radio Access Network (UTRAN) and the core network. The latter is composed of the Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN) which are interconnected via an IP network. The SGSN keeps track of the location of individual mobile stations and performs security functions and access control. The GGSN encapsulates packets received from external IP networks and routes them toward the SGSN. The UTRAN consists of the Radio Network Controller (RNC) and Node B (i.e. the base station) connected by an asynchronous transfer mode network. The RNC is in charge of the overall control of the logical resources provided by Node Bs. A UE communicates with the Node B through a radio interface based on Wideband Code Division Multiple access (WCDMA) technology. The

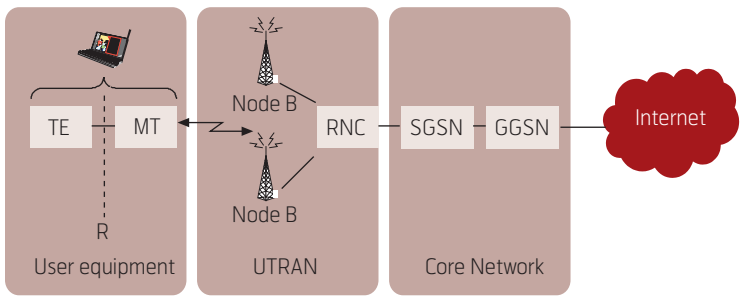


Figure 6 UMTS Network Architecture

ISSN 0085-7130

UE in turn consists of two disjoint entities, namely, the Terminal Equipment (TE) and the Mobile Terminal (MT). The TE and MT entities can reside in different physical modules interconnected by the *R-reference* point. The TE hosts the application and user-interaction, while the MT is in charge of all the UMTS communications-related tasks. Figure 7 shows the protocol stacks of UMTS, which comprise the user plane and the control plane. The user plane consists of a layered protocol structure providing user information transfer, along with associated information transfer control procedures. The control plane consists of protocols for control and support of user plane functions.

Currently, the notion of WPAN, which comprises a group of TEs associated with a single MT, does not exist in the UMTS standards. What has been defined in the standard is a protocol for point-to-point communication between an MT and a TE over a serial physical link which can be a cable. Point-to-Point Protocol (PPP) is used to establish such communications between MT and TE, where the MT serves as a modem. However, in our context, we have a number of TEs which are grouped into a Bluetooth or an IEEE 802.15.3 WPAN, and the MT functions as a personal network gateway which will be described in the next section. Instead of using PPP for communication, the group of TEs and the MT are networked using Bluetooth or IEEE 802.15.3.

3 Personal Network Architecture

A key component in the WPAN is the *Personal Network Gateway* (PNG) which seamlessly connects a WPAN or a WLAN to UMTS as shown in Figure 8. Unlike other devices in the WPAN, the PNG is multimodal, i.e. it contains different protocol stacks. On the WPAN/WLAN side, it houses the Layer 1 and Layer 2 of Bluetooth, IEEE 802.15.3, and IEEE 802.11, and on the other side it is the UMTS user plane and control plane radio access protocol stack as depicted in Figure 9. The UMTS user plane is connected to the Bluetooth, the IEEE 802.15.3 and the IEEE 802.11 at the IP layer. The PNG can also assume the role of master or PNC in Bluetooth or 802.15.3, respectively.

In addition to providing UMTS connectivity, the PNG also facilitates communication between devices which are equipped with different technologies. For example, a Bluetooth-enabled device can communicate with an 802.11-enabled device via the PNG. In this paper, we assume that there is only one PNG in

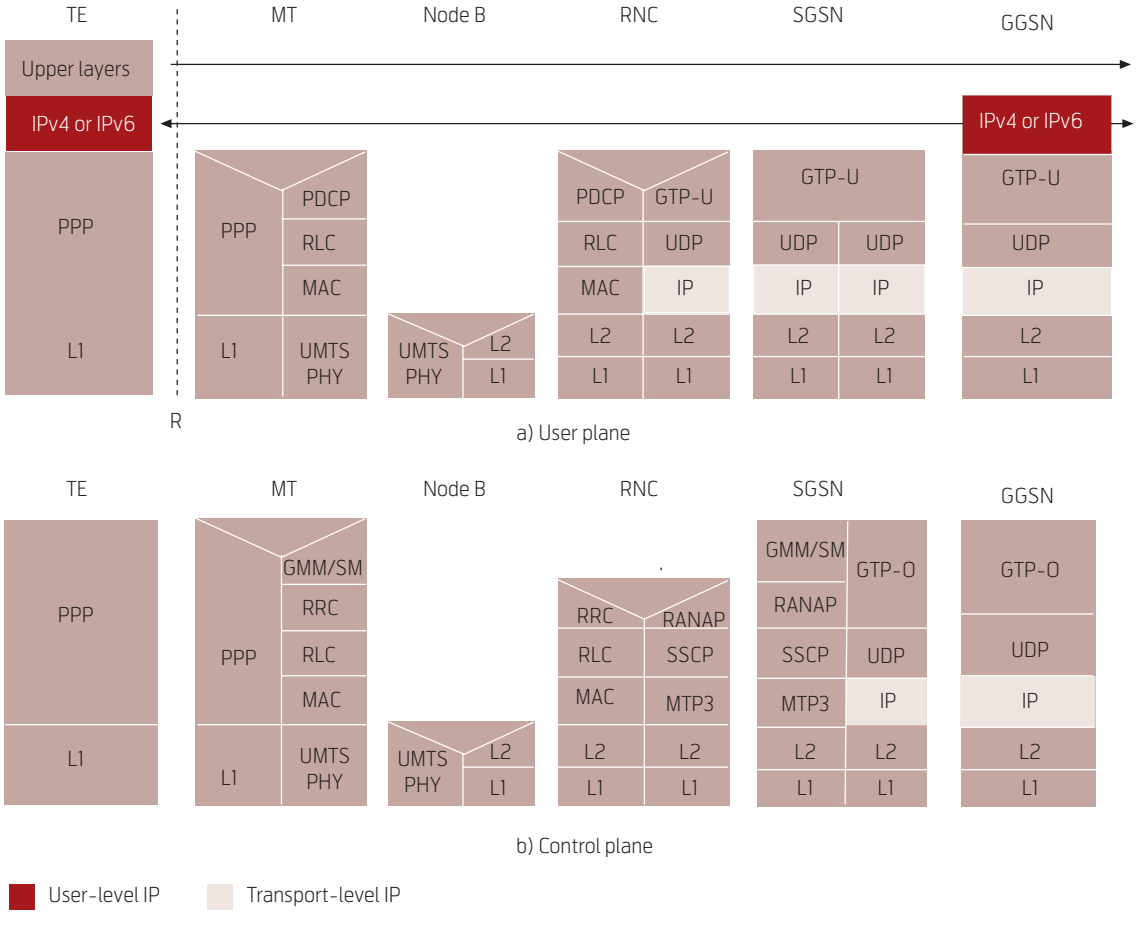


Figure 7 UMTS Protocol Architecture

ISSN 0085-7130 ©Telenor ASA 2007

a WPAN or WLAN and the rest of the devices in the WPAN or WLAN are single-mode, i.e. either Bluetooth, 802.15.3 or 802.11. In the scope of this paper, a user's WPAN is not limited to Bluetooth- and 802.15.3-enabled devices but may also include 802.11-enabled devices due to the popularity of the WLAN technology. The PNG operates as a bridge in order to link Bluetooth-, 802.15.3- and 802.11-enabled devices together. Using a bridge, the different devices appear to be connected on the same subnetwork. Bridging is recommended because it provides efficient communication in a small sized network such as WPAN. If two communicating devices are more than one hop away, then multi-hop communication is utilized. This will be described in subsection 3.3.1.

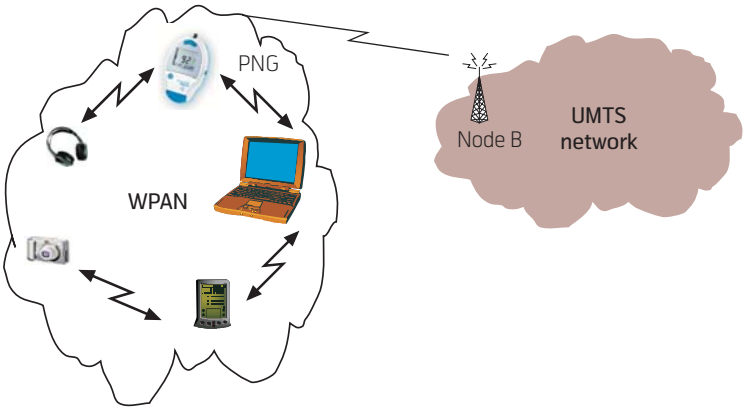


Figure 8 Personal Network Gateway

3.1 Self-Organization

WPAN is a self-organized ad hoc network which is automatically formed with little or no user intervention. The WPAN formation mechanism is provided by Layer 1 and Layer 2 of the WPAN. The WPAN formation mechanism of Bluetooth and IEEE 802.15.3 is provided by the Inquiry and the Association procedures, respectively. For the IEEE 802.11 ad hoc mode, any device within radio range can be directly addressed without forming a subnetwork by using the Scan procedure. The formation of a WPAN, which comprises devices of different wireless technologies, will be coordinated by the PNG using the WPAN formation mechanism of its wireless technology because it has multiple interfaces. The procedure is described in subsection 3.1.1.

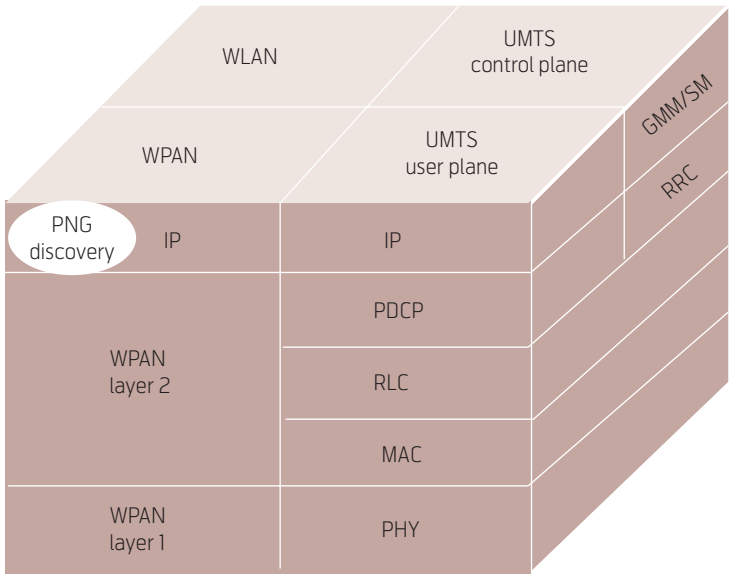


Figure 9 Personal Network Gateway Protocol Architecture

Once the WPAN is formed, it can operate either as a stand-alone ad hoc network or as a subnetwork of the interconnecting structure. In the latter, the PNG acts as the gateway and provides seamless connectivity to the UMTS network which is in turn connected to the Internet. Before any device in the WPAN can send and receive traffic from the interconnecting structure, it must be able to obtain a valid IP address and configure the PNG as the default router.

3.1.1 Personal Network Gateway Discovery

The PNG provides connectivity to the interconnecting structure, and therefore also needs to acquire unique IPv4 or IPv6 addresses for the WPAN devices. In order to use the PNG, devices in a WPAN must be able to find it even if the PNG is several hops away from the devices. Hence, the PNG discovery mechanism must also facilitate route construction between the device and the PNG in the event of a multi-hop scenario. The PNG discovery can be realized proactively or reactively. In the latter approach, the PNG discovery is triggered by a WPAN device, while the former is initiated by the PNG. To leverage the advantages of the two approaches, a hybrid approach is appropriate for PNG discovery. The PNG discovery protocol comprises two messages: `PNG Advertisement` and `PNG Solicitation`. PNG Advertisements are periodically broadcast into the WPAN by the PNG. The period between two consecutive PNG advertisements must be set to an optimum value so that the WPAN is not flooded to avoid wasting WPAN radio resources. If a device in a WPAN wants to learn about the PNG immediately, it can broadcast a PNG Solicitation which triggers immediate PNG Advertisements. These two messages could be defined as new Internet Control Message Protocol (ICMP) message types.

3.1.2 Address Auto-configuration

Two addressing schemes can be envisaged here considering both IPv4 and IPv6. We call the first of these two schemes "Private Address Auto-configuration" and the second one "Global Address Auto-configuration".

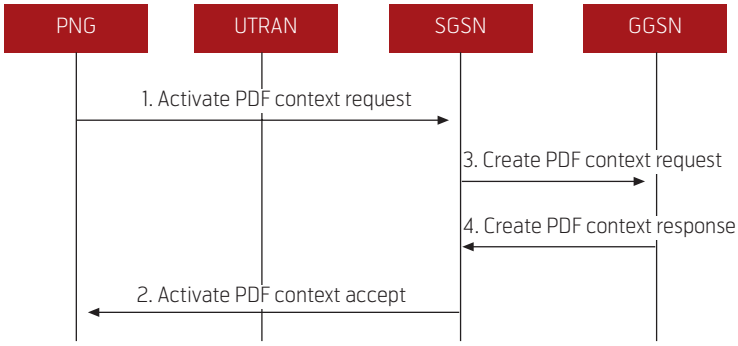


Figure 10 PDP Context Activation Procedure

Private Address Auto-configuration

In this scheme, the WPAN is assigned a single globally unique IP address. That means, the WPAN appears as a single point of presence on the Internet. The globally unique IP address is allocated to the PNG and the rest of the devices in the WPAN are assigned with private IP addresses which are not globally unique. Hence, a Network Address Translator (NAT) [8], which is located in the PNG, is employed to translate private IP addresses to the global routable IP address for packets emanating from any device in the WPAN, and vice versa. Both IPv4 and IPv6 support auto-generation of private addresses, viz. RFC 3927 [9] and RFC 2462 [10], respectively. The PNG can obtain a globally unique IP address through the UMTS *Packet Data Protocol* (PDP) context activation which is defined in the Session Management (SM) layer of the UMTS control plane. The PDP context can be viewed as a record that holds parameters that characterize a certain connection. In other words, it is a virtual connection between the PNG and the GGSN, which is characterized by the IP address and the quality of service profile. The PDP context is stored in the PNG, the SGSN and the GGSN. With an active PDP context, the PNG is visible to the GGSN and it can send and receive data packets. Figure 10 illustrates the steps involved in the PDP context activation.

Step 1: The PNG generates the `Activate PDP Context Request` message and sends it to SGSN.

Step 2: The SGSN checks the `Activate PDP Context Request` message and generates the `Create PDP Context Request` message which is sent to the GGSN to establish a GTP tunnel between the SGSN and the GGSN. The tunnel is used as the packet routing path between the GGSN and the SGSN.

Step 3: The GGSN allocates an IP address for the PNG, which is carried by the `Create PDP Context Response` message.

Step 4: Finally, the SGSN informs the PNG of the allocated IP address through the `Activate PDP Context Accept` message.

Global Address Auto-configuration

In this scheme, each device in the WPAN is allocated a globally unique IP address. Therefore, each WPAN device is visible to external nodes on the Internet. In this case, the PNG does not need to perform address translation for the WPAN devices. This addressing scheme does not favor IPv4 because of limited IPv4 address space. For allocating globally unique IP addresses, IPv4 supports only stateful address allocation technique, while IPv6 defines two techniques, namely *stateless* address allocation and *stateful* address allocation.

For the stateful address allocation technique, the operation is similar to the first scheme except that the PNG needs to perform the PDP context activation for each device in the WPAN in order to get a globally unique IP address. The PNG also needs to perform PDP context activation to obtain an IP address for the UMTS interface. In IP-based networks, the stateful address allocation can be accomplished by means of Dynamic Host Configuration Protocol (DHCP). However, DHCP has been designed with the assumption that the DHCP client and server is one hop away.

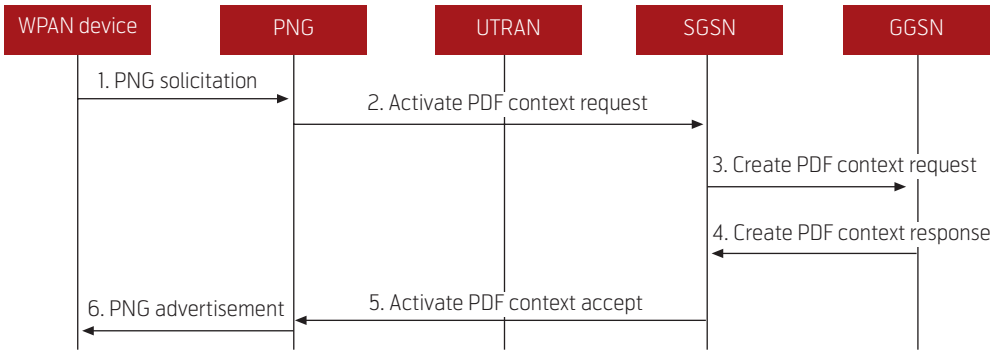


Figure 11 IPv6 Stateful Address Allocation

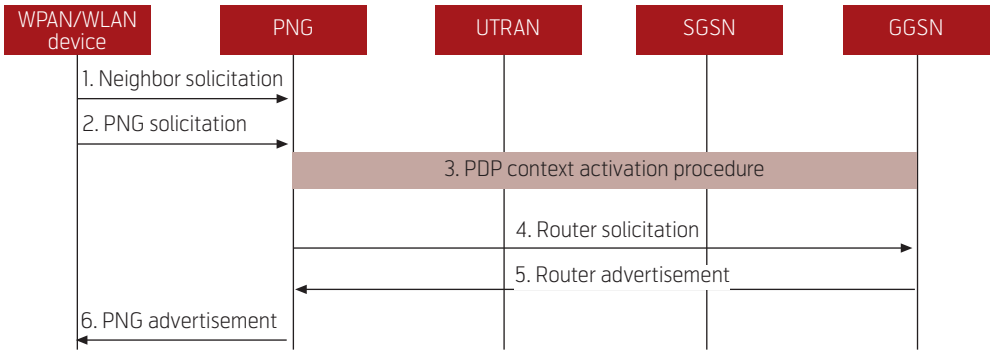


Figure 12 IPv6 Stateless Address Allocation

In WPAN, the DHCP client and the server may be multiple hops away. Hence, DHCP is not suitable for providing stateful address configuration in a multi-hop network. The PNG messages should be designed to support the stateful address configuration option. Figure 11 illustrates the operation of stateful address configuration. As shown in step 1 of the figure, the `PNG Solicitation` is used by the device in the WPAN to request for an IP address, which in turn triggers the PNG to perform PDP context activation (step 2 to step 5). Finally, the IP address allocated during PDP context activation is conveyed to the WPAN device via the `PNG Advertisement` message.

As mentioned, the stateless address allocation technique is only applicable to IPv6 since no equivalent technique exists in IPv4 for generating globally unique IP addresses. For this technique, each device in the WPAN is able to generate its own IPv6 address by concatenating a subnet prefix with an interface identifier. In IP-based networks, such a subnet prefix is contained in the IPv6 Router Advertisement messages which are transmitted by an IPv6 router. Similarly to DHCP, IPv6 Router Advertisement is not designed for multi-hop networks. The PNG messages should also support stateless address configuration in addition to stateful address configuration. The PNG can be configured to support either the stateful or the stateless address configuration. The interface identifier can be a Bluetooth, an IEEE 802.15.3 or an IEEE 802.11 MAC address. The stateless address allocation is depicted in Figure 12. The WPAN device is responsible for ensuring that the interface identifier is unique by broadcasting an IPv6 `neighbor solicitation` message to perform duplicate address detection (step 1 of Figure 12). However, the duplicate address detection cannot be used unchanged in a multi-hop scenario because the message can only reach devices one hop away. The duplicate address detection in multi-hop scenario is also present in mobile ad hoc networks. Several mechanisms have been proposed [11]. Therefore, these proposed mechanisms can be used by personal networks. If no address duplication is detected, then the WPAN device will use the interface identifier and issue a PNG `Solicitation` message (step 2). In order to get the IPv6 subnet prefix for the entire WPAN, the PNG performs the PDP context activation (step 3). Once the PDP context activation is completed, the GGSN can send an IPv6 `router advertisement` message (step 5) on the newly established PDP context. Alternatively, the PNG may issue an IPv6 `router Solicitation` message to GGSN (step 4). After the PNG receives the router advertisement message, it broadcasts the PNG `Advertisement` message to the devices in the WPAN (step 6). At the same time, the PNG constructs its IPv6 address by concatenating a randomly generated interface identifier and the subnet prefix. The interface identifier is randomly generated because the UMTS network interface does not have an equivalent IEEE MAC address. The WPAN device also generates its IPv6 address by concatenating its interface identifier and the subnet prefix.

3.2 Quality of Service

Quality of Service (QoS) is defined as a set of service characteristics that the network is requested to meet when transporting a sequence of data packets. The service characteristics can be expressed in terms of throughput, delay, loss, bit error rate, or as a relative priority of access to the network. End-to-end QoS in personal network spans across different domains: WPAN, UMTS and IP QoS-enabled interconnecting structures such as the future Internet. In such a heterogeneous environment, the end-to-end QoS will rely on the coordination of QoS mechanisms in different domains along the end-to-end communication path. Each of these domains (Bluetooth, IEEE 802.15.3 or UMTS) has its own QoS provisioning mechanisms. The challenge in QoS provisioning in personal network is to seamlessly interwork the QoS mechanism in each domain. The QoS provisioning functionality of each domain is identified and interworked as

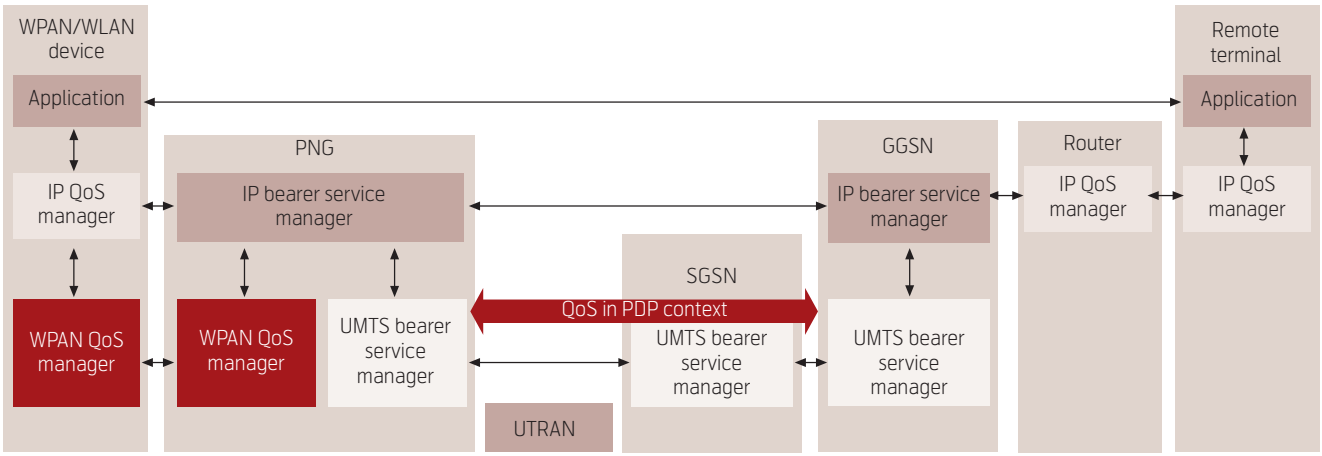


Figure 13 Personal Network QoS Management

shown in Figure 13. The interworking between QoS functionality takes place at the PNG and the UMTS GGSN. The PNG provides interworking between the WPAN QoS functionality and the UMTS QoS functionality while the GGSN deals with interworking between the UMTS QoS functionality and the QoS functionality in external IP networks.

The QoS management modules for UMTS are specified in [12-13]. UMTS achieves QoS management using a layered architecture with bearer services established at different layers between UMTS QoS management modules. The QoS management in WPAN is responsible for setting up a bearer (or connection) according to the requested QoS parameters.

The application in a WPAN device triggers the request for network service with particular QoS requirements. The application QoS requirements are sent to the IP QoS manager of the WPAN device for an IP level service. The IP QoS manager translates the QoS parameters for the WPAN QoS manager, which sets up the bearer with the required QoS between the device and the PNG. The WPAN QoS manager comprises admission control and scheduling algorithms. The admission control takes care of the radio resource allocation based on the availability while the scheduling algorithm schedules data transmission according to the QoS requirements. The same application QoS requirements, which are received by the WPAN QoS manager at PNG, are signaled to the IP bearer service manager. This in turn sets up the UMTS bearer service by initiating the PDP context activation with the required QoS. The PDP context which contains the application QoS requirements is translated for the IP bearer service manager by the UMTS bearer service manager at the GGSN. The IP bearer service manager uses the requirements for controlling the QoS with external IP networks.

For QoS control with an external IP network, UMTS specifies the use of DiffServ at the IP bearer service manager in the GGSN. For the QoS signaling between WPAN and UMTS, a number of QoS signaling protocols, e.g. Resource reSerVation Protocol (RSVP) can be used at the IP QoS manager and the IP bearer service manager in the WPAN device and the PNG, respectively. For illustration purposes, we have chosen RSVP because it can provide accurate and complete description of application QoS requirements. The basic idea is to employ RSVP as a local resource reservation protocol between a WPAN device and the PNG, and to use the QoS description contained in the RSVP messages for interworking with the QoS functionality in other networks.

The application in a WPAN device sets its QoS requirements in an RSVP PATH which is processed by the WPAN QoS manager in the WPAN device and conveyed to the PNG. Upon receiving the RSVP message, the PNG performs the following tasks: translates RSVP parameters into PDP context parameters; initiates PDP context activation procedures if RSVP PATH message is received; and negotiates the PDP context characteristics with the UMTS network. Conversely, if the QoS requirements are initiated by the external IP network, the PNG performs the following tasks: translates PDP context into RSVP parameters, constructs and sends an RSVP PATH to the recipient; and completes the PDP context modification when the RSVP RESV is received.

Figure 14 shows the signaling flows. We assume that a PDP context already exists, which is set up during the IP address allocation. The existing PDP context is referred to as the primary PDP context and supports best-effort data only. The QoS request is initiated by the external IP network. The IP bearer service manager of GGSN maps the requested QoS into PDP context parameters and triggers the GGSN-initiated PDP

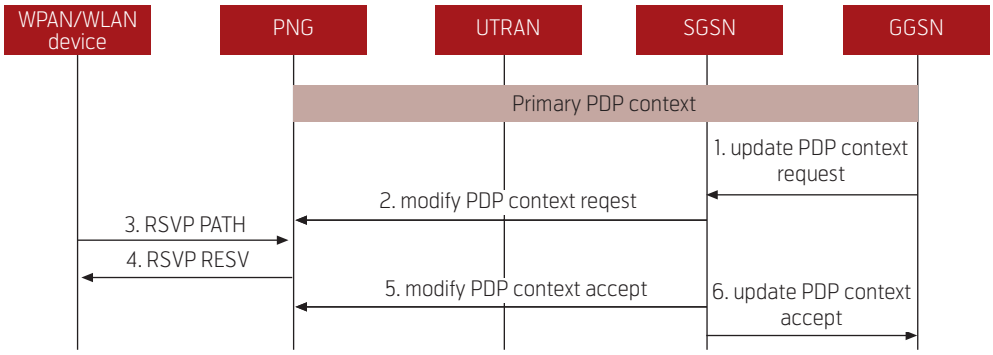


Figure 14 QoS Signalling with RSVP

context modification (steps 1 and 2 in Figure 14). Upon receiving the `Modify PDP Context Request` message, the requested QoS requirements are translated into an RSVP PATH message which is sent by the PNG. Once the PNG receives the RSVP RESV message, it triggers the `Modify PDP Context Accept` message (steps 4 to 6 in the figure).

3.3 Routing

Routing in personal networks can be categorized into two levels: intra WPAN routing, and WPAN and remote area network routing as shown in Figure 15.

3.3.1 Intra WPAN Routing

Intra WPAN routing deals with the communication between two devices in the same WPAN. That is, the communication does not involve the interconnecting structures. In a WPAN, if direct communication is not feasible due to out of radio range, then multi-hop forwarding is utilized. Multi-hop communication is an issue that belongs to the area of Mobile Ad hoc NETwork (MANET) routing which has been an active area of research for the last decade. The MANET research efforts are mostly concerted by the MANET Working Group [14] of the Internet Engineering Task Force (IETF). However, MANET mostly deals with large-scale, military-typed ad hoc networks. Furthermore, MANET assumes that the wireless technology is homogeneous, i.e. all the devices use the same radio access technology, e.g. IEEE 802.11. Conversely, multi-hop communication in a WPAN could be over different wireless technologies. For instance, a WPAN is composed of a Bluetooth-enabled device, an IEEE 802.11-enabled device and a PNG which has multiple interface including Bluetooth and IEEE 802.11. When the Bluetooth-enabled device and the 802.11-enabled device want to communicate with each other, the communication is only possible via the PNG. In addition, the multi-hop communication is over different network topologies. The size of WPAN/WLAN is relatively small as compared with the scenarios considered in MANET. Instead of designing new routing protocols, which is not the scope of this paper, state-of-the-art routing protocols can be adopted and customized to suit the need of personal networking. The idea of PNG-assisted routing seems appealing. As mentioned in subsection 3.1, the PNG co-ordinates the formation of WPAN and naturally, it becomes the central controller of the WPAN. Hence, it is fully aware of the devices in the WPAN. During the PNG discovery phase, routes are constructed between the PNG and any device that wants to join the WPAN. Therefore, the PNG can be used as a default router. For instance, if device *A* wants to send packets to device *B* in the WPAN, then device *A* sends the packets to the PNG which in turn forwards to device *B* using the route constructed during the PNG discovery phase. With PNG-assisted routing, the ad hoc routing protocol is energy-efficient and simple since the device does not need to build and maintain routing table to other devices in the WPAN. An energy-efficient ad hoc routing protocol is needed because WPAN devices are usually battery-powered. The PNG-assisted routing can result in non-optimum routes and high traffic load at the PNG. However, the performance will not be critical since the network size of WPAN is small.

3.3.2 WPAN and Remote Area Network Routing

This level of routing deals with the communication between a WPAN and another WPAN or a remote area network such as a corporate area network. The communication may involve interconnecting structures or go via ad hoc networks. In either case, the communication entry and exit point of the WPAN is the PNG or the gateway for the remote area network.

3.4 Mobility Management

Mobility management is responsible for tracking the dynamics of the personal network and users. Several types of mobility are identified within personal networks, viz. *terminal* mobility, *network* mobility and *session* mobility. To date, solutions for each type of mobility have been investigated and developed separately. In personal networks, we require a unified mobility solution that is efficient and can support all

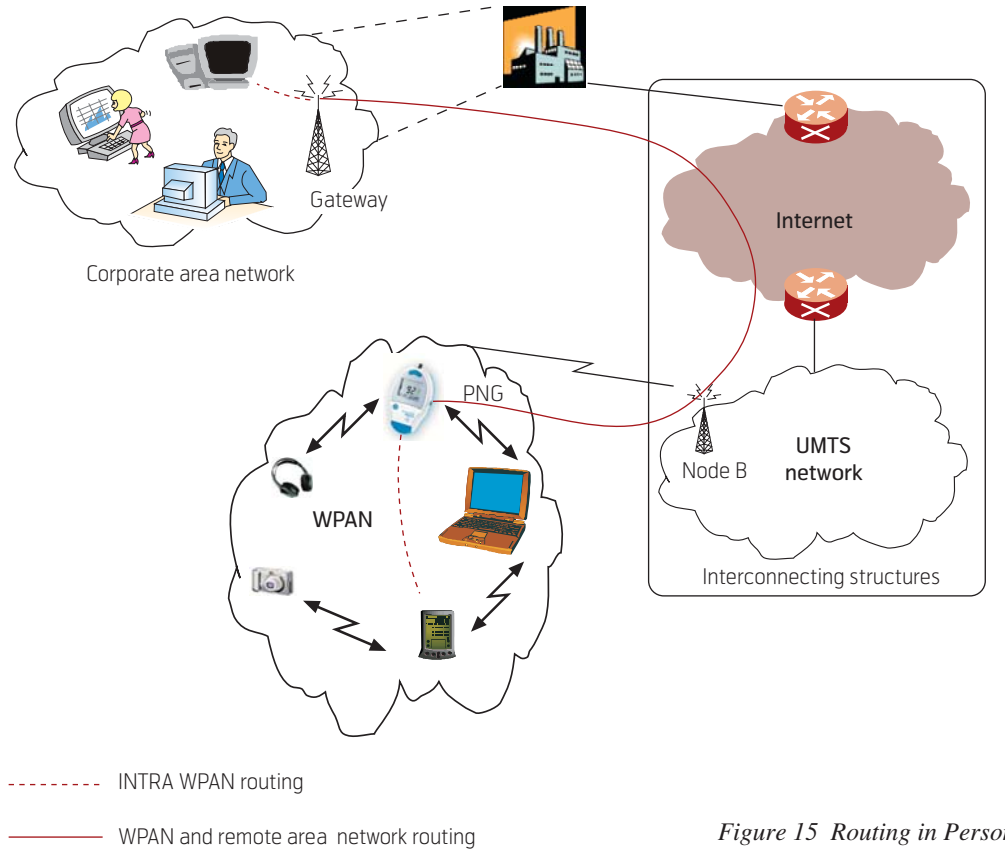


Figure 15 Routing in Personal Networks

three types of mobility simultaneously. In this subsection, we will describe such a solution.

Terminal mobility arises due to devices joining or leaving the WPAN. The WPAN generally resides in the same location as the user who will be mobile. As the user moves around his/her environment, new devices may be encountered and attached to the WPAN, similarly other devices may become detached. The IETF has standardized network-layer solutions to support terminal mobility, namely Mobile IPv4 [15] and Mobile IPv6 [16]. The IETF has also standardized and has been working on different solutions such as the Stream Control Transmission Protocol (SCTP) [17] and the Host Identity Protocol (HIP) [18]. For a comprehensive survey of terminal mobility solutions, we refer to [19].

When the entire WPAN moves as a unit and changes its point of attachment to the interconnecting structure, it is referred to as *network* mobility. For example, a WPAN switches its connection from WLAN to UMTS. The IETF has established a working group called NEtwork MObility (NEMO) [20] to standardize solutions for network mobility. NEMO aims at extending existing solutions to support network mobility in IPv6.

Session mobility concerns the transfer of an ongoing session from one device to another. A session is an active transport connection (i.e. TCP) between two communicating devices. The need for a session transfer arises when a device is detached or a new and more powerful device joins the WPAN. Session mobility is inherent to personal networks. The solutions for terminal mobility and network mobility do not cater for session mobility.

Hence, we propose a session mobility solution which leverages the advantages of Virtual Network Address Translation (VNAT) [21] and Mobile IP. The solution can also deal with terminal mobility and network mobility. Currently, IP addresses are used to identify the end-point of TCP connections. As each device is assigned a different IP address, it is impossible to transfer the TCP connection to another device without breaking and restarting the connection on another device. VNAT decouples the TCP end-point identification from the IP addresses by using virtual addresses. The virtual address is then mapped to a corresponding IP address at the Network layer. VNAT, however, relies on external servers for obtaining IP addresses, which incurs extra overhead. Instead of relying on virtual addresses and external servers, we can achieve a similar decoupling effect by using the home IP address of a device in combination with Mobile IP.

The protocol architecture, which contains the VNAT and Mobile IP layers, is shown in Figure 16. VNAT is composed of the *connection translation layer* and the *session transfer management layer*. The VNAT

connection translation is responsible for mapping the IP address used for TCP end-point identification into the IP address of the new device after the session transfer. The VNAT session transfer management facilitates the automatic migration by securing and keeping alive sessions during the migration process. Mobile IP is then used by the new device to inform the home agent of the old device to tunnel packets belonging to this session to the new device.

Figure 17 shows an example of a session transfer from device *A* to device *B* in the WPAN. The session is a TCP connection set up between device *A* and device *C* which resides in the user's WPAN and home area network, respectively. On device *A* and device *C*, the end-point of the TCP connection is identified by the IP address of *A*, IP address of *C* and port numbers as shown in the bottom diagram of the figure. The port numbers are not shown in the figure. Then, session *S* is transferred to device *B*. In order to keep the session alive, the end-point identifier remains the same as on device *A* and device *C*. On device *B* and device *C*, the VNAT Connection Translation module is responsible for mapping IP address *A* into the IP address of *B,* and vice-versa. The figure also illustrates terminal mobility. Device *B* is a foreign device in the WPAN, then it will obtain a care-of IP address. If Mobile IP route optimization is employed, the IP home address of *B*, which is used by the VNAT Connection Translation module is mapped into the care-of address as shown in Figure 17. The advantage of using Mobile IP is that functions for network mobility easily can be incorporated.

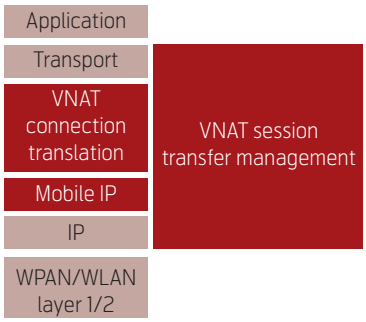


Figure 16 VNAT and Mobile IP Protocol Architecture

5 Personal Network Related Projects

In this section, we present some of the current personal network projects in Europe and around the world. Note, it is not in the scope of this paper to present an exhaustive list.

5.1 IST MAGNET Beyond

My personal Adaptive Global NETwork and Beyond (MAGNET Beyond) [22] is an Information Society Technologies (IST) project, which builds on the achievements and results of its predecessor, i.e. the MAGNET project. The objective of MAGNET Beyond is to design and develop the concept of personal network that supports context-aware resource-efficient, robust, ubiquitous personal services in a secure, heterogeneous networking environment for mobile users.

5.2 Personal Distributed Environment

The concept of personal networking is also being defined and developed by the Mobile Virtual Centre of Excellence (MVCE) at the University of Strathclyde [23]. The personal network concept is known as the Personal Distributed Environment (PDE). The objective of the PDE is to provide virtual personal network connectivity in a dynamic and heterogeneous environment, irrespective of the location of devices included in the personal network.

5.3 IBM Personal Mobile Hub

IBM has built a Personal Mobile Hub (PMH) [24] which serves as a gateway between a WPAN and the Internet. The functionality of PMH is similar to the PNG. The WPAN consists of devices worn by users such as medical sensors, wrist-watch computers, etc.

5.4 MOPED

In [25], the authors presented a networking model that treats a user's set of personal devices as a MOPED, an autonomous set of MObile grouPEd Devices (MOPED), which appears as a single entity to the rest of the Internet. All communication traffic for a MOPED user is delivered to the MOPED, where the final disposition of the traffic is determined.

5.5 MyNet

MyNet project [26] is a collaboration between Nokia and the MIT User Information Architecture group. MyNet aims to study and develop a network architecture, tools and applications for simple, secure, personal overlay networks.

5.6 Freeband PNP 2008

Personal Network Pilot 2008 (PNP 2008) [27] is a project sponsored by the Dutch Research Council under the Freeband Communication program. The project aims at developing the personal networking concept into practical technology and demonstrators.

6 Conclusion

The paper has addressed the major issues of self-organization, establishing and maintaining QoS and mobility management in personal networks. The personal network is built on top of WPANs and UMTS.

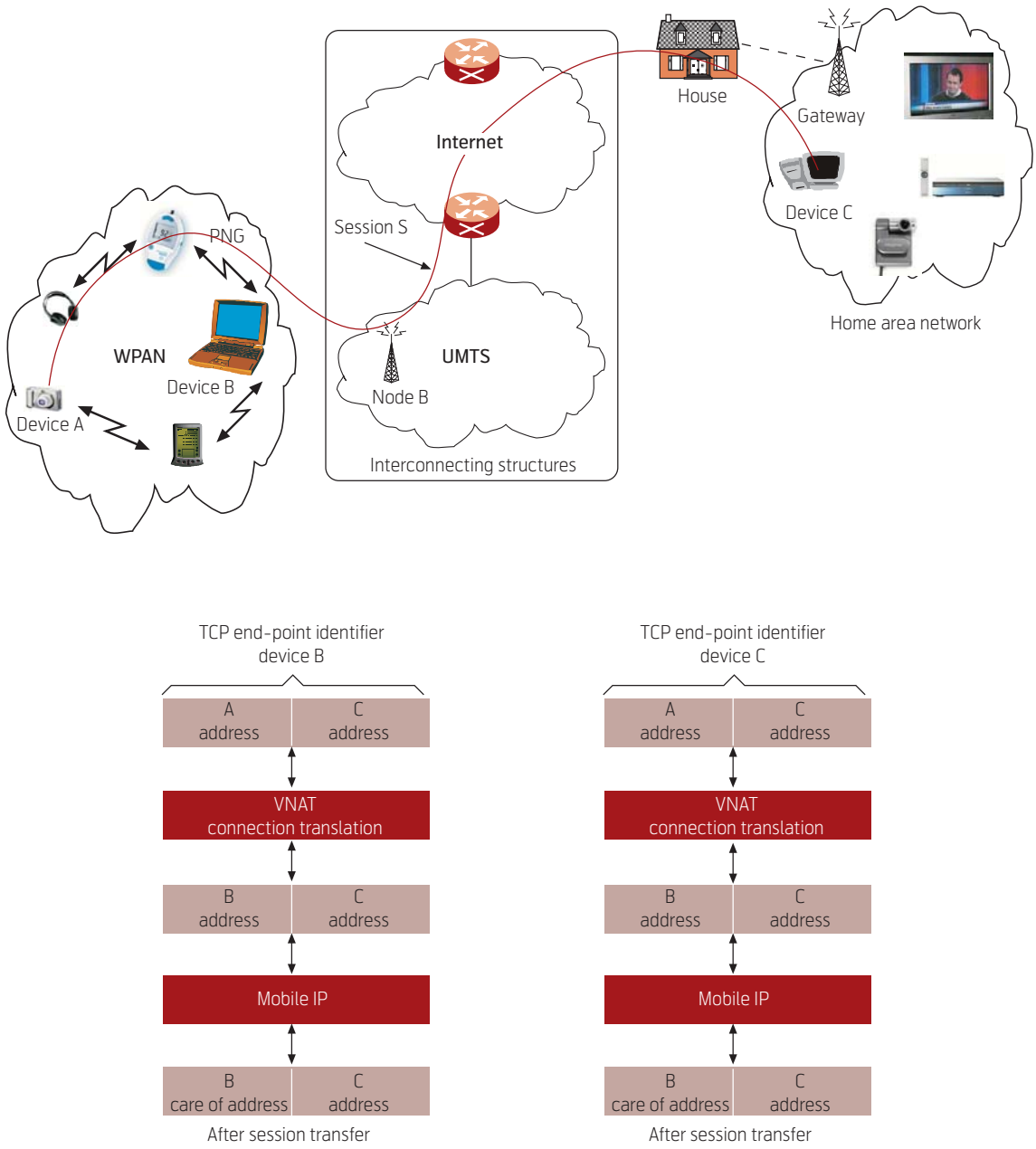


Figure 17 Session Mobility with VNAT and Mobile IP

The WPAN technologies considered are Bluetooth and IEEE 802.15.3. IEEE 802.11, which is a WLAN technology, is also considered due to its popularity. A key component in the WPAN and UMTS co-operation is the PNG which seamlessly connects a WPAN to a UMTS network. The PNG enables the WPAN to dynamically configure globally unique IP addresses and to provide routing information for devices in the WPAN. As for QoS, the QoS provisioning functionality in WPAN and UMTS was identified and interworking QoS management modules were designed to allow seamless QoS establishing by applications. We proposed a unified solution to deal with terminal mobility, network mobility and session mobility in the personal networks.

Acknowledgement

This work was partially funded by the IST MAGNET Beyond and the Freeband PNP2008 projects.

References

1 Roberts, M L et al. Evolution of the Air Interface of Cellular Communications Systems toward 4G Realization. *IEEE Communications Surveys and Tutorials*, 8 (1), 2006.

2 Niemegeers, I G, Heemstra de Groot, S M. Research issues in ad-hoc distributed personal networking. *Wireless Personal Communications*, 26 (2-3), 2003.

3 *3GPP*. Available from http://www.3gpp.org

4 Kaaranen, H, Naghian, S, Laitinen, L, Ahtianen, A, Niemi, V. *UMTS Networks: Architecture, Mobility and Services*. New York, John Wiley, 2001.

5 IEEE. *Part 15.1: Wireless Medium Access Control and Physical Layer (PHY) Specification for Wireless Personal Area Networks (WPANs)*. 2002. (IEEE 802.15.1)

6 IEEE. *Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specification for High Rate Personal Area Networks (WPANs)*. Sept 2003. (IEEE 802.15.3)

7 IEEE. *Wireless Medium Access Control and Physical Layer Specification*. 1999. (IEEE Standard 802.11)

8 Tsirtsis, G, Srisuresh, P. *Network Address Translation – Protocol Translation (NAT-PT)*. 2000. (IETF RFC 2766)

9 Cheshire, S, Aboba, B, Guttman, E. *Dynamic Configuration of IPv4 Link-Local Addresses*. 2005. (IETF RFC 3927)

10 Thomson, S, Narten, T. *IPv6Stateless Address Autoconfiguration*. 1998. (IETF RFC 2462)

11 Weniger, K, Zitterbart, M. Address Autoconfiguration in Mobile Ad Hoc Networks: Current Approaches and Future Directions. *IEEE Network Magazine*, 18 (4), 2004.

12 3GPP. *Quality of Service (QoS) Concept and Architecture*. 2006. (TS 23.107)

13 Chakravorty, R, Pratt, I, Crowcroft, J. A Framework for Dynamic SLA-based QoS Control for UMTS. *IEEE Wireless Comms. Magazine*, 10 (5), 2003.

14 *Mobile Ad hoc Networks (MANET)*. 2006, December 1 [online] – URL: http://www.ietf.org/html.charters/manet-charter.html. (Work in Progress)

15 Perkins, C. *IP Mobility Support for IPv4*. 2002. (RFC 3344)

16 Johnson, D, Perkins, C, Arkko, J. *Mobility support in IPv6*. 2004. (IETF RFC 3775)

17 Stewart, R, Xie, Q, Morneault, K. *Stream Control Transmission Protocol*. 2000. (IETF RFC 2960)

18 Moskowitz, R, Nikander, P. *Host Identity Protocol (HIP) Architecture*. 2006. (RFC 4423)

19 Le, D, Fu, X, Hogrefe, D. A Review of Mobility Support Paradigms for the Internet. *IEEE Communications Surveys and Tutorials*, 8 (1), 2006.

20 Devarapalli, V, Wakikawa, R, Petrescu, A, Thubert, P. *Network Mobility (NEMO) Basic Protocol*. 2005. (IETF RFC 3963)

21 Su, G, Nieh, J. *Mobile Communnication with Virtual Network Address Translation*. Columbia University, 2002. (Technical Report)

22 *IST MAGNET Beyond*. Available from: http://www.ist-magnet.org

23 Dunlop, J, Atkinson, R C, Irvine, J, Pearce, D. A Personal Distributed Environment for Future Mobile Systems. *Proceedings of IST Mobile Summit*, 2003.

24 Husemann, D, Narayanaswami, C, Nidd, M. Personal Mobile Hub. *Proceedings of the 8th International Symposium on Wearable Computers (ISWC)*, 2004.

25 Kravets, R, Carter, C, Magalhaes, L. A Cooperative Approach to User Mobility. *ACM Computer Communication Review*, 31 (5), 2001.

26 *MyNet*. Available from: http://research.nokia.com/research/projects/mynet-uia/index.html

27 *Freeband PNP 2008*. Available from: http://www.freeband.nl/

Anthony Lo received his combined BSc/BE degree with first class Honours in Computer Science and Electronics Engineering in 1992 and his PhD degree in Protocol and Network Engineering in 1996, all from La Trobe University, Australia. He is currently an assistant professor at Delft University of Tecnology in the Netherlands. Prior to that, he was a Wireless Internet Researcher at Ericsson EuroLab, where he worked on research and development of UMTS and beyond 3G systems.

email: A.Lo@ewi.tudelft.nl

Weidong Lu received his Bachelor's degree from Southeast University, Nanjing, China in July 2001 and his Master's degree from Delft University of Technology, Delft, The Netherlands in August 2003. In November 2003, he joined the Wireless and Mobile Communications Group in the Telecommunications Department at Delft University of Technology as a PhD student. His research topic is the Self-organization of Personal Networks and his research interests include: Wireless networking and ad hoc networks, Mobility Management and QoS in Wireless Networks.

email: W.Lu@ewi.tudelft.nl

Martin Jacobsson graduated with an MSc in Computer Science from the University of Linköping, Sweden in 2002. In 2003, he joined the Wireless and Mobile Communications group at Delft University of Technology where he is working towards a PhD degree. He has participated in several Dutch and European funded research projects. His PhD research includes ad hoc and self-organization wireless networking techniques in combination with infrastructure-based networks for personal networks.

email: M.Jacobsson@ewi.tudelft.nl

Venkatesha Prasad got his bachelor's degree in Electronics and Communication Engineering from the University of Mysore, India in 1991. In 1994 he received the M.Tech degree in Industrial Electronics and the PhD degree in 2003 from the University of Mysore, India and Indian Institute of Science, Bangalore, India, respectively. During 1994 and 1996 he worked as a consultant and project associate for ERNET Lab of ECE at Indian Institute of Science. While pursuing his PhD degree, from 1999 to 2003 he was also working as a consultant for CEDT, IISc, Bangalore for VoIP application developments as part of a Nortel Networks sponsored project. From 2003 to 2005 he headed a team of engineers at the Esqube Communication Solutions Pvt. Ltd. Bangalore for the development of various real-time networking applications. From 2005 till date he has been with the Wireless and Mobile Communications group at Delft University of Technology working on the EU funded projects MAGNET/MAGNET Beyond and PNP-2008, as well as guiding students.

email: VPrasad@ewi.tudelft.nl

Ignas Niemegeers received a degree in Electrical Engineering from the University of Gent, Belgium, in 1970. In 1972, he received an MSEE degree in Computer Engineering and in 1978 a PhD degree from Purdue University in West Lafayette, Indiana, USA. From 1978 to 1981 he was a designer of packet switching networks at Bell Telephone Mfg. Cy, Antwerp, Belgium. From 1981 to 2002 he was a professor in the Faculty of Computer Science and Electrical Engineering at the University of Twente, Enschede, The Netherlands. From 1995 to 2001, he was Scientific Director of the Centre for Telematics and Information Technology (CTIT) of the University of Twente, a multi-disciplinary research institute in ICT and applications. Since May 2002, he holds the chair in Wireless and Mobile Communications at Delft University of Technology in The Netherlands, where he is heading the Centre for Wireless and Personal Communications (CWPC) and the Department of Telecommunications. He is an active member of the Wireless World Research Forum (WWRF) and IFIP TC-6 Working Group on Personal Wireless Communications. He has been involved in many European research projects, in particular ACTS TOBASCO, ACTS PRISMA, ACTS HARMONICS, RACE MONET, RACE INSIGNIA and RACE MAGIC. Presently, he is participating in the IST projects MAGNET on personal networks, and EUROPCOM on emergency ad hoc networks.

email: I.Niemegeers@ewi.tudelft.nl

Wide-Area Publish/Subscribe Service Discovery – Application to Personal Networks

WASSEF LOUATI, DJAMAL ZEGHLACHE

Wassef Louati is a PhD student at INT, Evry, France

This paper explores the use of event-based communications to design publish/subscribe service discovery architectures that are adequate for wide-area pervasive environments. Some service discovery protocols and paradigms lack this event-based communication capability. They also often present weaknesses in expressiveness, extensibility and flexibility. Some service discovery frameworks include eventing but are limited to local area discovery. All these features and capabilities are needed to create the next generation of mobile and large-scale Internet services. A Wide-area Publish/subscribe Service Discovery (WPSD) framework meeting such requirements is presented and analyzed in terms of design and implementation characteristics. The applicability of WPSD to service discovery and management in Personal Networks is also examined.

Djamal Zeghlache is Professor and Head of Wireless Networks and Multimedia Services Dept., INT, Evry, France

1 Introduction

Service discovery allows services to advertise themselves so that clients can query and possibly access them. Service discovery is most often local and hence limited in range. With the distribution of services in increasingly large-scale environments, new paradigms for service discovery, creation and provisioning are needed to cover wider areas and prepare for this evolution. Wide-area service discovery has become a requirement and has consequently attracted much interest[1)].

Wide-area service discovery is a key enabler for wide-area pervasive environment and especially for *Personal Networks* (PN) that have gained interest recently in the research community [1]. The PN concept extends the Personal Area Network (PAN) by including *remote* personal devices in the network architecture (Figure 1). The PN can be viewed as a collection of geographically scattered clusters that can communicate via interconnecting structures or in ad hoc mode. A PN cluster is a network of devices characterized by a common trust relationship and

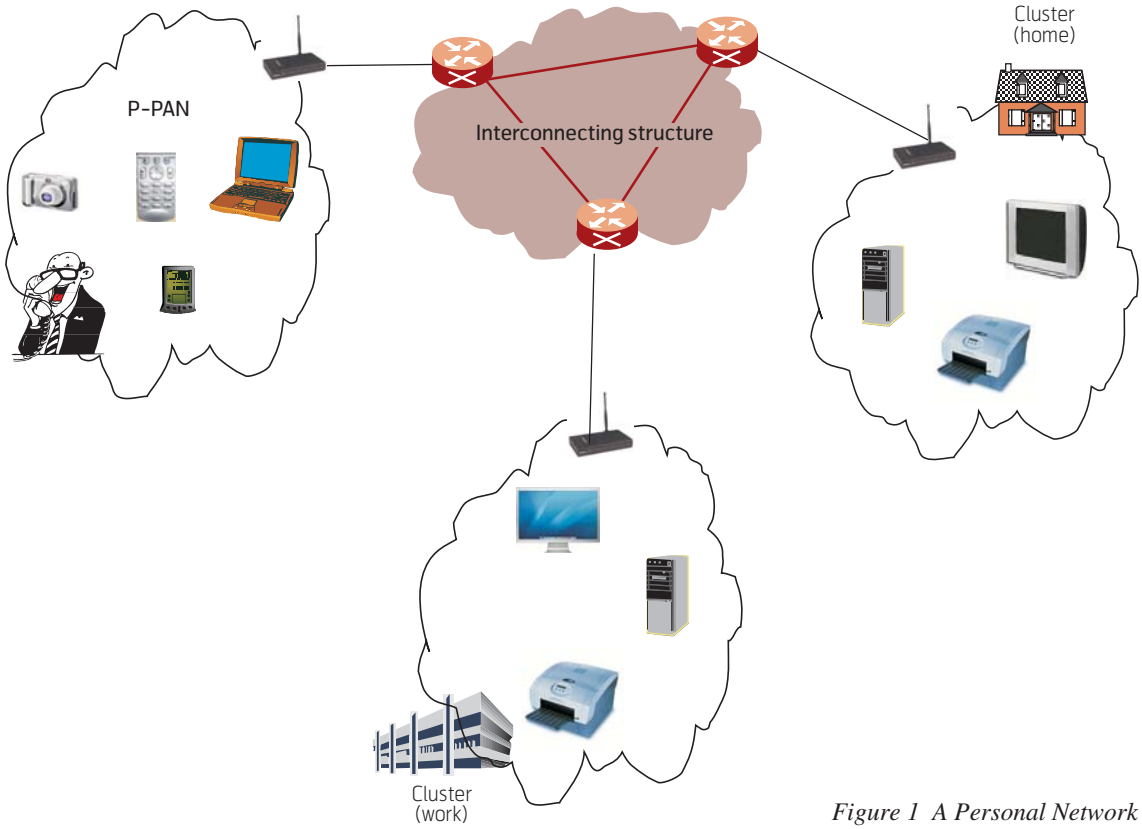


Figure 1 A Personal Network

1) *The wide-area service discovery is the current focus of the IRTF P2PRG Content, Resource and Service Discovery (CORE) Subgroup. The purpose of this subgroup activity is to define a research agenda within the P2PRG community to evaluate existing research, identify requirements, and develop solutions for wide-area P2P content, resource, and service discovery.*

ISSN 0085-7130

located within a limited geographical area (e.g. home cluster, office cluster, etc.). The PAN surrounding the user is a special cluster called Private PAN (P-PAN).

Wide-area service discovery can support many applications including service control, dynamic service creation, context awareness and network management. Personal networks can also considerably benefit from wide-area service discovery frameworks.

Clients (e.g. PN user, PN application, PN management system, etc.) need in fact to be notified about services that match their queries at service announcement times. Clients may also require to be notified about modification of state and access information of services due to mobility and dynamic changes. To perform such notifications, service discovery should embed *eventing* mechanisms.

Existing architectures supporting eventing (e.g. UPnP [2], Jini [3]) are suitable for small-area and local discovery but cannot support wide-area and remote discovery because they use synchronous or multicast communications that suffer from scalability problems.

In the context of wide-area environments, eventing is known as *event-based communication* or as a *publish/subscribe* model. In this model, subscribers describe the events (data, messages, etc.) that they want to receive from publishers, without having previous knowledge of each other's locations. The model ensures the event flow from publishers to subscribers so that notifications can be received by the subscribers. The strength of this model is its loose coupling between publishers and subscribers in time, space and synchronization. This characteristic makes event-based communication a scalable communication model that is widely used in many large-scale Internet services and mobile computing environments. A natural evolution for service discovery is thus to integrate event-based communication to provide eventing capability and achieve wide-area service discovery.

The objective of this paper is to address such service discovery frameworks and especially analyze a *Wide-area Publish/subscribe Service Discovery* (named WPSD) framework as a potential solution.

Many applications, especially PN applications and services, can benefit from WPSD. These applications need to be informed immediately about changes in context data, services states and PN networking and management.

The paper conducts its analysis of wide-area publish/subscribe service discovery by first presenting an overview of event-based middleware. This description is followed by definitions and requirements on the proposed WPSD service discovery framework. A general architecture for WPSD is then presented and a specific implementation reported. Finally, the applicability of WPSD to Personal Networks is examined.

2 Event-Based Middleware

An event-based middleware provides publish/subscribe communication between components of large-scale distributed systems. In an event-based middleware, events represent the basic or fundamental communication mechanism [4].

Event consumers express their interest, in receiving events, in the form of an event *subscription*. Event consumers are commonly called *Subscribers*. Event producers produce events, which will be delivered to all interested Subscribers. Event producers are commonly called *Publishers*. Thus, an event-based system has an asynchronous many-to-many communication model, where the Publishers and the Subscribers are decoupled. The event delivery is performed by *event brokers* that form an overlay network that routes the events from the Publishers to the Subscribers. The path is set up by *advertisements* and subscriptions sent by Publishers and Subscribers respectively.

The event-based middleware architecture has four layers (Figure 2) [4][5]. The lowest layer is the network layer. On top of this layer, an overlay network implements application-level routing (content-based, peer-to-peer (P2P), etc.). The overlay handles the routing between the application-level nodes (event brokers, peer nodes, etc.) and has a self-organizing mechanism that supports the node dynamic changes (when joining and leaving the overlay).

The event-based middleware layer provides the programmer an interface to handle the events (advertisement, subscription, publication, etc.) and manages also the storage, event filtering and notification operations in the event brokers.

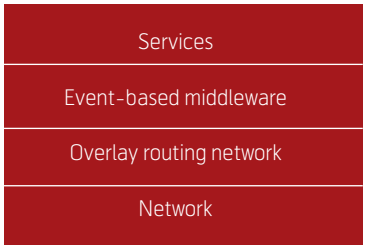


Figure 2 Event-based middleware architecture

ISSN 0085-7130 ©Telenor ASA 2007

The event-based middleware layer can benefit from extensions offered by the service layer that can provide additional services such as security and QoS. An event-based system can be extended to support QoS-aware paths between the Publishers and the Subscribers such as in [6]. Introducing security into the system can be achieved for example by making the event brokers OASIS-capable (Open Architecture for Secure Interworking Services) [7] to perform a boundary policy-based access control to the middleware. The broker would use the OASIS policy to decide if the advertisement/subscription can be admitted [8].

3 Wide-Area Publish/Subscribe Service Discovery

Event-based middleware has a layered architecture designed to offer multiple services. Service discovery can be one possible offered service. Even though some event-based systems can be tailored for service discovery, most adaptations suffer from significant overhead. The event content must be adapted to a service description and rendezvous brokers must be previously set up by the advertisement to perform notification. The best solution, as adopted by WPSD proposed in this paper, is to build an event-based system designed for service discovery from the start. The event content would be explicitly defined (service information) and the routing of events between the Publishers and the Subscribers carried out at service (event) delivery time.

3.1 Design Requirements

To design a Wide-area Publish/Subscribe Service Discovery (WPSD) system, we define a set of system requirements resulting from a mix of our experience in wide-area service discovery [9][10], the event-based middleware requirements of [4], event-based proprieties [11] and the problem statement specified recently by the P2PRG CORE subgroup in [12]. The requirements consist of:

Multiple event support

A WPSD system should notify the subscribers when new events occur:

- Appearance of new services
- Departure of services
- Dynamic changes in service state
- Changes in mobile service location
- etc.

Reliability

A WPSD system must be resilient to entity failures. The failure of a part of the system must not cause total system failure. The system must be always aware of the location of the nomadic services and their clients, especially with the emergence of wireless technologies. The system should also support the mobility of the brokers.

Scalability

The scalability is an important requirement for any WPSD system since the number of involved devices, users and services is in continuous increase.

Dynamic update

In a WPSD system, a subscriber should not receive an interrupted stream from the publisher. When a service is dynamic and/or mobile, its service information update should not be performed by removing the old information and announcing the new one. Only an update due to the new information should take place.

Security

A WPSD system should support security and privacy protection. Especially, the security mechanisms should protect the system from attacks related to the distributed architectures.

Interoperability

Many service discovery technologies can be used at the edge of a WPSD system. Thus, WPSD should be able to interact with different service discovery systems. This leads to the following interoperability requirements:

- A linking mechanism (i.e. gateway) should be used to make the translation between the WPSD and the local discovery systems when service description semantics differ.
- Gateways at the edges should have an API that supports all operations (addition, removal, dynamic update, security, etc) to enable interaction.
- The WPSD system should use an expressive and extensible service description language to be capable of translating descriptions to/from other languages.

There is a trade-off to achieve between expressiveness in the service description language and scalability [13]. A highly expressive service description language would require more processing and would make the system less scalable. The presented design in this paper takes into account this trade-off by striving for a balance between expressiveness and scalability.

3.2 Design Decisions

In this section, we describe how to integrate the publish/subscribe model in a wide-area service discovery

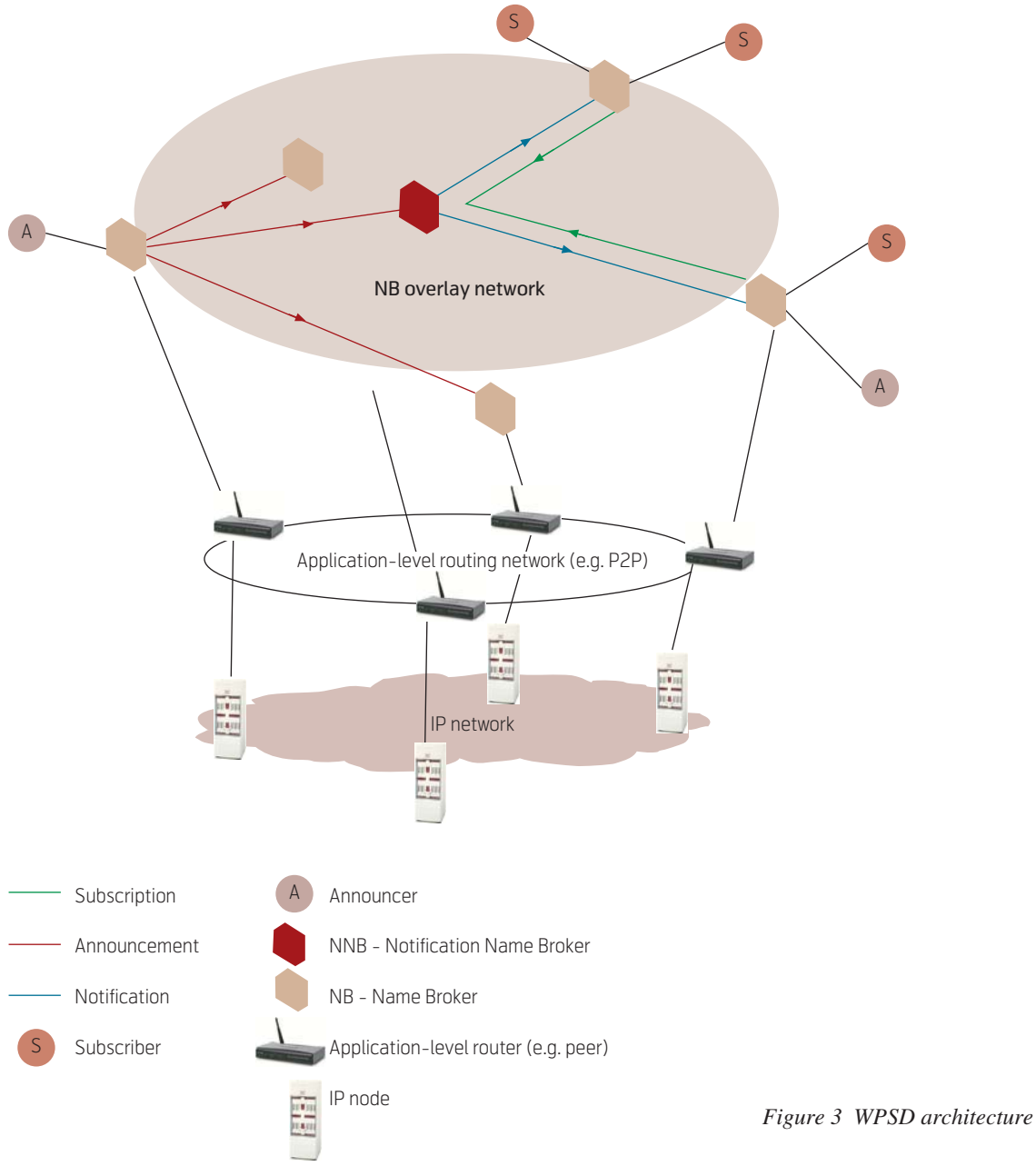


Figure 3 WPSD architecture

leading to a WPSD system. In this description, we define the required additional operations, the involved entities and their interactions.

To start with, we must select the right model that should be applied to service discovery. Mainly, there are two categories of publish/subscribe models: topic-based and content-based. Each form has its own manner of expressing the event subscriptions. The topic-based model uses a predefined set of topics or subjects to identify the events. In content-based model, the events do not have such restricted structure.

In topic-based model, the topics are not expressive. They just use predefined labels and this is not sufficiently rich to specify service subscriptions. In the content-based model, a service subscriber can make more specific service subscription using richer description formats (e.g. attribute/value pairs, XML, etc.). WPSD hence adopts the content-based model since it is more suitable for service discovery applications.

In a WPSD system, a service announces its *service information* in the form of a pair (*name*, *name-record*). The name denotes the service description (e.g. attribute/value pairs) and the name-record denotes the access information to the provider of the service, such as its IP address. By handling name to address mapping, a WPSD system acts also as a naming and name resolution system.

The producer and consumer in a WPSD system are the service *Announcer* and the service *Subscriber*. The event brokers of WPSD, called *Name Brokers* (NB), are *name information databases*. The NBs *route* names from the Announcers to the Subscribers using a *name-based routing* paradigm. The routing

occurs on an application-level routing that can be achieved using a P2P network or any other type of overlay (Figure 3).

The Subscriber announces a *subscription name* to perform one of the three subscription types below:

- *Name subscription* to be notified about names that match *exactly* all the subscription name attributes;
- *Supername subscription* to be notified about *any* name that match the subscription name;
- *Name-record subscription* to be notified about any modification of the name-record information (due to Announcer mobility or dynamic changes in environment) of the subscription name.

The name subscription is performed using the usual name announcement mechanism of the current service discovery architecture. The name-record of a subscription name is called *subscriber name-record*. The *Notifications* are performed after name information database updates by the Announcers (addition, removal, and dynamic update). For a given name update session, an NB holding the name database changes is called *Notification Name Broker* (NNB). The location and the number of NNBs for a given subscription depend on the used name-based routing of the current service discovery protocol. The notifications of the name update are sent by an NNB to the appropriate Subscribers identified by their name-records.

For example, suppose Alice wants to be notified about all her cameras (in her home, office, etc.) and dynamic changes in their states. Alice submits from her Subscriber a supername subscription like [service = camera] [owner = Alice [cluster = *]]. One or more NBs that receive the supername will play the role of NNBs. When a new camera is added or the states of existing cameras change, the Announcers related to the cameras announce or update the names. The NNBs notify Alice's Subscriber about these new changes.

WPSD introduces the ability to make dynamic updates of the announced name information. When Announcers or Subscribers move, their access information (i.e. name-records) is updated in the NBs. The corresponding NNBs notify the Subscribers so that they are always aware of the Announcers' locations.

3.3 WPSD Scalability

WPSD is intrinsically scalable since Announcers and Subscribers are decoupled, as in any publish/subscribe system. Many other factors improve the scalability of WPSD. The NBs self-configure into a distributed application-level overlay network to perform name-based routing. By integrating naming and routing in the application-level, the scalability can be maintained while highly expressive names are used.

The scalability is also improved by the load balancing ensured by WPSD. The load induced by subscription and announcement is quite balanced and reduces the risk of an NB becoming a bottleneck node in the network. This is due to the NB location that depends on the name to be routed. Since the NNB location depends on the subscription names, the notifications are issued from different NNBs. This distributes naturally the load and avoids congestion in the NB network.

Scalability and load balancing occur naturally when a Distributed Hash Table (DHT) is used as the application-level routing network in the WPSD system. DHTs, such as Chord [14], CAN [15], Pastry [16] and Tapestry [17], create structured P2P networks that, given a key, can efficiently lookup the peer at which the corresponding value is stored. The DHT storage and lookup processes scale logarithmically with the number of peers in the network. For DHT-based designs, the NB location may be determined by hashing names (announced or subscription names) and looking up the NB peers responsible for the resulting keys (i.e. the hash values). This will be illustrated with more details in section 3.6.

3.4 WPSD Security

In [18] the authors present a number of security issues and requirements in wide-area publish/subscribe systems. Based mainly on this analysis, several solutions have been proposed to secure publish/subscribe systems. Some of these solutions can be adopted and added to secure a WPSD system.

Three main security mechanisms should be addressed. First, an *access control* mechanism should be designed at the boundary of the NB network. Only authenticated and authorized Announcers and Subscribers should be able to access the NB network. To address access control, the authors in [19] present an access control mechanism based on publication/subscription message content. This is a suitable solution for WPSD since it is a content-based publish/subscribe model.

Second, a mutual *trust* should be provided between the Subscribers and the Announcers. The most advanced solution, proposed by the authors in [20], is to introduce the notion of scoping for structuring publish/subscribe systems. Scopes delimit groups of Publishers and Subscribers on the application level and

control the dissemination of notifications within the broker network. Hence, they are suitable for building groups of trust (i.e. groups whose members belong to the same authentication domain). The trust relationships in scopes are established using public key infrastructures and access control methodologies. WPSD can adopt this solution as well, especially when the NBs belong to different administrative domains.

Finally, *confidentiality* and *integrity* of the announced names, the subscription names, and the inter-broker messages should be provided. The common solution is to encrypt and sign the messages, as has been achieved by the work in [8] and [20].

3.5 The Support of the WPSD Model

The integration of the publish/subscribe model into an existing wide-area service discovery system can lead to a WPSD system. To support this integration, the selected system should be flexible, extensible and scalable. Several architectures can support the integration of the WPSD model as long as their extensions fulfill all previously mentioned requirements. In fact, this depends mainly on the *infrastructure model* of the service discovery protocol. Wide-area service discovery protocols ([21]–[25]) have normally a *structured directory*[2)]*-based* infrastructure model [26].

There are two major existing directory structures for wide-area service discovery: *flat* and *hierarchical* structures. In a flat structure, exemplified by protocols such as INS/Twine [21] and Superstring [22], directories have P2P relationships. Hierarchical structures, including SSDS [23], CSP [24] and GloServ [25] have a DNS-like directory structure.

Hierarchical structures overcome the overloading problem of directories by spawning the load on the child nodes. Nevertheless, they cannot scale easily to WPSD integration. The announcements and the notifications would propagate up and down through the hierarchy and can turn the root node into a bottleneck. Even if several hierarchies may co-exist, the hierarchies would not handle efficiently subscription names that include orthogonal attributes. For example, imagine a WPSD system having two hierarchies of directories: one based on service location and the other based on the service property. A user may subscribe to its own services located in a given geographical area. The hierarchy described would not handle this subscription in a scalable manner, since both hierarchies will be involved in the notification.

Service discovery protocols having flat structures generally rely on DHT. These protocols inherit DHT scalability, efficiency, reliability and robustness. Hence, DHT-based service discovery protocols are more suitable for WPSD integration than hierarchical approaches. The next section describes an implementation example of a WPSD system using INS/Twine, a typical DHT P2P-based service discovery protocol.

3.6 Implementation Example: WPSD Based on DHT P2P-Based Service Discovery

A viable framework to implement a WPSD system is INS/Twine [21] that attracted our interest for its flexibility, expressiveness and ability to use any kind of identities to describe objects, nodes, services while providing information on their location. This system resolves names or identities into IP addresses for networking purposes.

INS/Twine is a P2P-based service discovery protocol with an expressive, responsive and robust system designed for dynamic and mobile environments. Services are described using a hierarchical attribute-value pair naming scheme such as XML. The description is called intentional name. The INS/Twine architecture consists of a network of Intentional Name Resolvers (INRs) that provide name resolution and name-based routing. The service providers and the clients are located at the edge of the INR network.

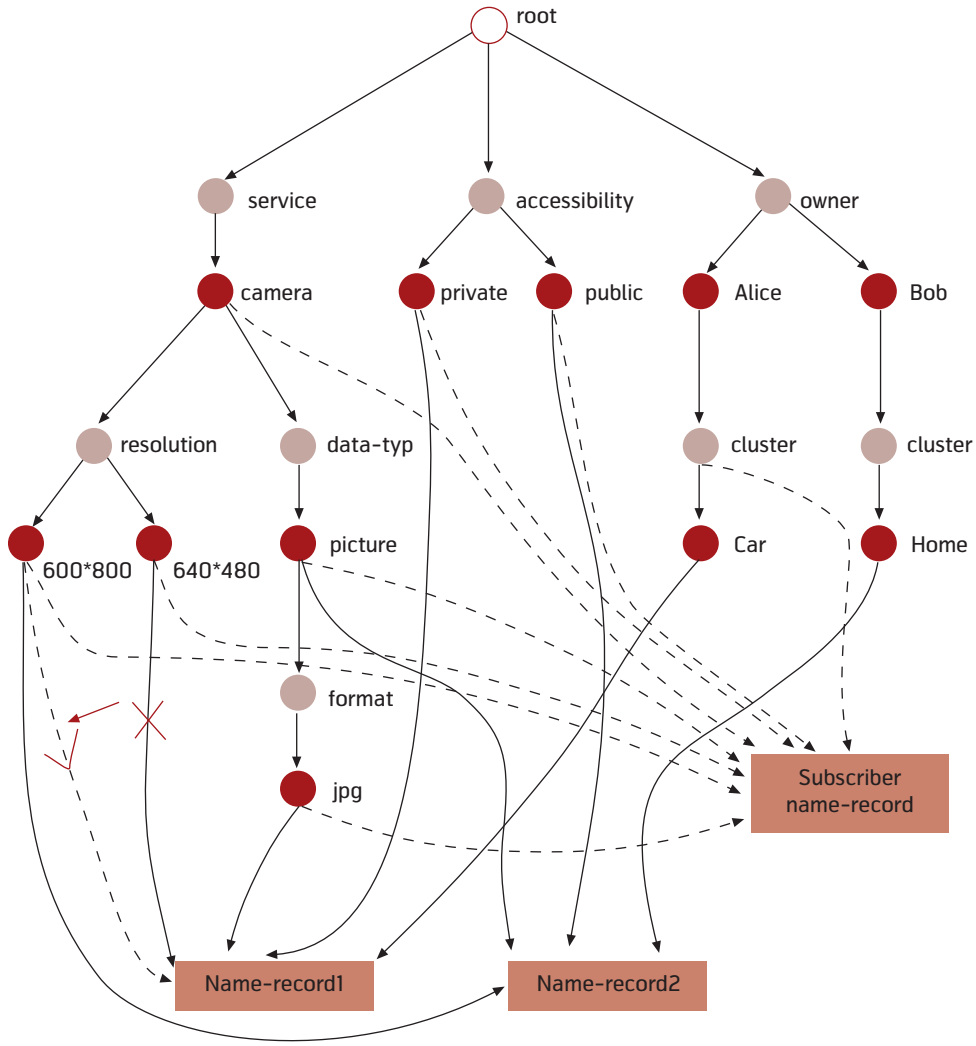
The INR name database has a data structure called a name-tree. The INRs self-configure into an application-level distributed overlay network over a DHT network to disseminate and route name information to the appropriate locations.

INS/Twine performs hash-based partitioning of service information among a subset of INRs. The querying has a similar mechanism. INS/Twine extracts each unique prefix subsequence of attributes and values from a name (an announced name or a name query). Each subsequence, called a strand, is then used to produce a separate key. INS/Twine uses a DHT process to map the keys to appropriate resolvers into which the service information or query is forwarded.

WPSD can be designed by extending the INRs of the INS/Twine framework. The resulting INRs play the role of Name Brokers (NBs). The Subscribers correspond to clients and the Announcers to service providers.

For name announcement, the name is added in the name-tree of the corresponding NBs. This is per-

2) *The directory, also often called broker or resolver, is the entity that stores service information and processes announcements and queries.*



Name-record1: of Alice name ([service=camera[resolution=600*800]
[data-type=picture[format=jpg]]][accessiblility=private][owner=Alice
[cluster=car]])

Name-record2: of Bob name ([service=camera[resolution=600*800]
[data-type=picture]][accessiblility=public][owner=Bob
[cluster=Home]])

Subcriber Name-record: of Alice supername subscription ([eservice=camera]
[accessibiltity=*][owner=Alice[cluster=*]])

Figure 4 Name database management in INS/Twine-based WPSD

formed by adding the corresponding name-record to all leaf values of the name in the name-tree (see Figure 4).

The dynamic update of a name and its access information consist of finding the corresponding name-record in the name-tree. If the dynamic update concerns the access information of the name, the update affects the name-record itself. If the name needs to be updated (i.e. updating a given value in the name), the name-record is detached from the old value and associated to the new one.

For name subscription, the subscriber name-record will be associated to the leaf values of the subscription name. In the case of the supername subscription the association will involve all the supername children values. The name-records of a matching name or supername will be associated to the values having the subscriber name-record. This association will trigger the notification action. The detachment of an association, due to name removal or update, will also trigger the notification.

The notification can be achieved by any NB corresponding to a key computed from the strands of a subscription name. To achieve scalability, one single NB is selected to play the role of the NNB. This NNB corresponds to the longest strand of the subscription name.

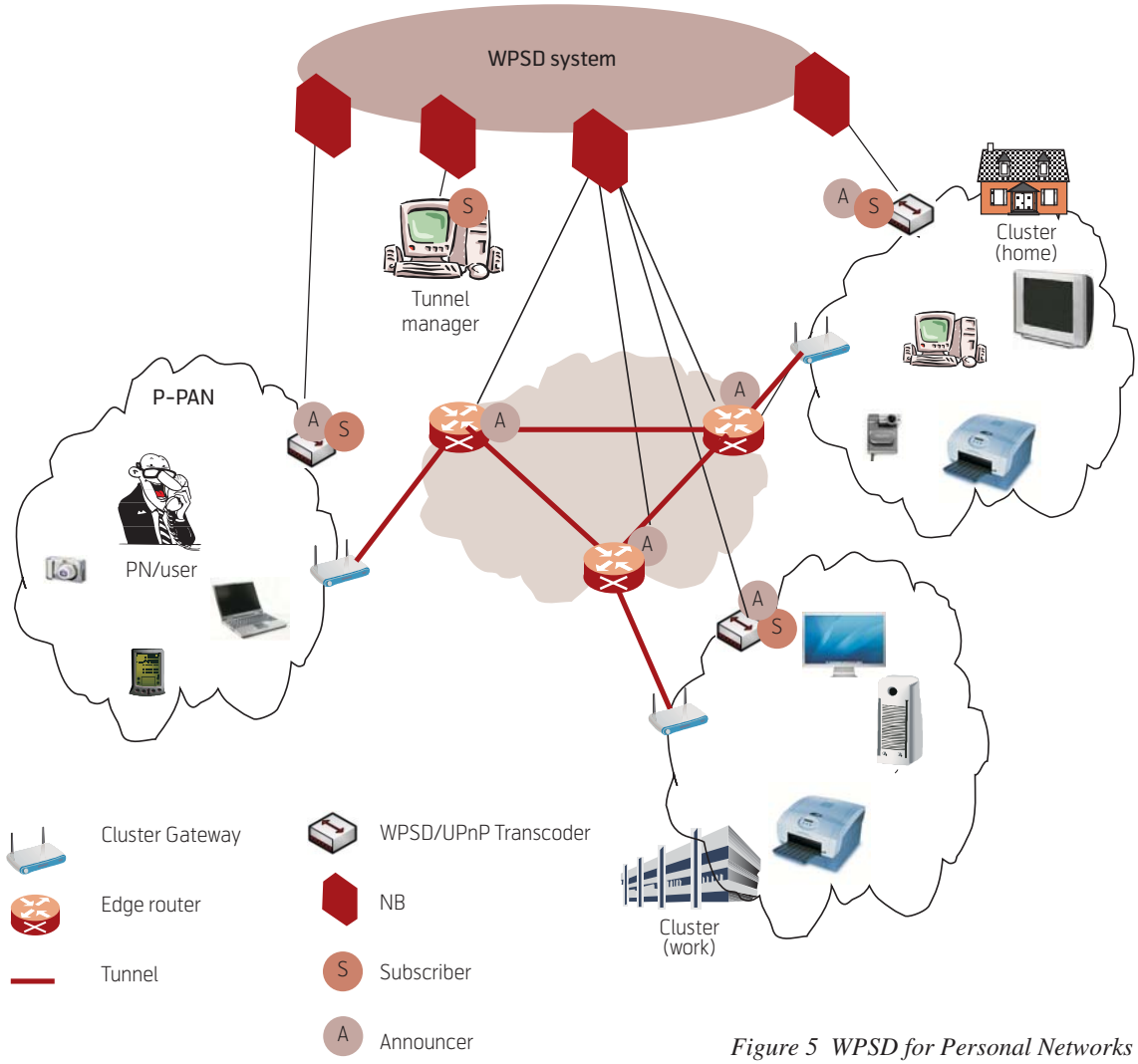


Figure 5 WPSD for Personal Networks

Figure 4 gives an example of a name-tree management. The figure illustrates a dynamic update, a supername subscription and two announced names (related to the two depicted name-records). For the dynamic update, the resolution attribute of the camera service has been updated from a camera resolution value of 640*480 to the 600*800 value.

The name-tree depicts a supername subscription ([service = camera][accessibility = *][owner = Alice [cluster = *]]). The supername is composed of four strands: (service, camera), (accessibility), (owner, Alice) and (owner, Alice, cluster). The subscriber will be notified of Alice's name as the corresponding name-record is associated to the values having the subscriber name-record. The NNB corresponds to the fourth strand, as it is the longest one.

4 WPSD Applicability for Personal Networks

In this section, we will show the applicability of the WPSD system for Personal Networks (PNs) (Figure 5) as a communications middleware between local service discovery frameworks with eventing capabilities. WPSD can also assist PN establishment and context information delivery.

4.1 WPSD-Based PN Establishment

PN networking entails the establishment of secure inter-cluster communication using tunnels. To establish tunnels between clusters, one needs to be capable of locating the clusters and their points of attachment to intermediate networks. To provide this information, the concept of a PN Agent has been introduced [27] to assist PN establishment. A possible approach is to use tunnel managers to send tunnel configuration parameters to tunnel end-points needed to connect distant PN clusters. Tunnel establishment based on policies relying on names is referred to as *name-based tunnel establishment* [28][29]. A scalable publish/subscribe naming system such as WPSD can enable PN establishment by embedding the PN Agent.

This can be achieved as follows. The tunnel end points, depicted in Figure 5 as access routers, shall include the WPSD Announcers. The Announcers

declare the names of the attached clusters. The cluster names include the PN identifier and the cluster identifiers (e.g. [PN = Bob [Cluster = Home]]). The PN Agent maintains information about the cluster names and their attachment points (the IP addresses of the access routers are in the name-records).

The tunnel management, using an embedded WPSD Subscriber, performs cluster name subscription and subscribes to the name-record of each registered cluster name to become aware of the cluster dynamics and mobility induced changes.

When a cluster changes its attachment point, the cluster name is removed from the Announcer in the old tunnel end-point and is announced by the prospective new tunnel end-point. Once the Subscriber is notified of these changes (by obtaining the IP addresses of the old and new tunnel end-points), the tunnel manager sets up the new tunnel and tears down the old one.

Clusters can frequently merge or split. For example the home cluster splits into the P-PAN and the home cluster. The P-PAN can merge with other clusters, e.g. office. During these dynamic changes, the Announcers in tunnel end points can perform updates of the cluster identifier attribute value. The advantage here is that the update can occur without completely removing or announcing again the cluster name. The active tunnels can be maintained thus avoiding additional tunnel tear downs and set ups.

4.2 UPnP Extension for Wide-Area Service Discovery Using WPSD

Universal Plug and Play (UPnP) [2] is a widely deployed local service discovery protocol. WPSD can be used as communication middleware between UPnP-enabled PN clusters. With this combination, a PN user can access, from any location, any UPnP service in any given UPnP-enabled PN cluster.

This interoperability requires the design of interworking components called Transcoders. The Transcoder translates UPnP service descriptions into WPSD names and vice versa. The Transcoder binds also the UPnP operations (announcement, discovery, and eventing) into WPSD operations and vice versa.

By using WPSD, the discovery can benefit from the most recent dynamic updates of the service descriptions. The UPnP Client of the Transcoder can subscribe to all UPnP services in its associated cluster using the UPnP eventing functionality. When receiving the updated service description from UPnP, the WPSD Announcer of the Transcoder can infer the updated attributes and achieve the value updates. Hence, the UPnP service database remains always up to date.

In addition, UPnP eventing can be concatenated to WPSD eventing if the UPnP services cannot be directly accessed remotely. The distant nodes would subscribe to the remote UPnP service through WPSD.

UPnP is just an example to illustrate the interoperability benefits of WPSD. WPSD can cooperate with other local area service discovery supporting the eventing function such as Jini [3].

Interoperability of WPSD with popular service discovery protocols and frameworks should ease its large-scale deployment and adoption as a wide-area service discovery architecture.

4.3 Context-Awareness Using WPSD

The publish/subscribe feature of WPSD can enable context awareness in Personal Networks if nodes subscribe to context information services offered by nodes acting as context sources. It would be sufficient to use a name Announcer that publishes names that correspond to key context information advertised by the context sources. The context data consumers would build from these names a subscription name and simply subscribe to automatically receive notifications about changes in context from the WPSD system. Services and applications can thus be made context aware and can adapt according to dynamic changes in the overall PN architecture and constituents.

5 Conclusion

This paper examined the introduction of publish/subscribe paradigms into current service discovery frameworks to achieve flexible, extensible and expressive wide-area service discovery architectures. This was accomplished through the design of a general and generic service discovery architecture named WPSD that relies on event-based communications. The applicability of WPSD to Personal Networks (PNs) was examined along with interoperability requirements with other discovery frameworks. WPSD can enable service discovery between remotely located PN clusters and can facilitate PN establishment and context information delivery. WPSD can easily interoperate with popular service discovery protocols to fulfill the requirements of wide-area service discovery in pervasive environments. These WPSD features should ease large scale deployment and adoption.

6 Acknowledgments

The authors would like to thank the reviewers for their valuable comments. This work was partially funded by IST Integrated Project MAGNET No. 507102.

7 References

1 *My personal Adaptive Global NET*. IST-MAGNET consortium. Available from: http://www.ist-magnet.org/

2 *UPnP Forum Website*. http://www.upnp.org/

3 *Jini Website*. http://www.jini.org

4 Pietzuch, P R. *Hermes: A Scalable Event-based Middleware*. Queens' College, University of Cambridge, UK, 2004. (PhD thesis)

5 Fiorentino, C, Cilia, M, Fiege, L, Buchmann, A. Building a Configurable Publish/Subscribe Notification Service. *IFIP International Conference on Distributed Applications and Interoperable Systems (DAIS'05)*, Athens, Greece, June 2005. Springer-Verlag. (LNCS 3543)

6 Carvalho, N, Araújo, F, Rodrigues, L. Scalable QoS-Based Event Routing in Publish-Subscribe Systems. *IEEE Internacional Symposium on Network Computing and Applications (NCA '05)*, Boston, MA, USA, 2005.

7 Bacon, J, Moody, K, Yao, W. A model of OASIS role-based access control and its support for active security. *ACM Transactions on Information and System Security (TISSEC)*, 5 (4), 492–540, 2002.

8 Belokosztolszki, A, Eyers, D M, Pietzuch, P R, Bacon, J, Moody, K. Role-based access control for publish/subscribe middleware architectures. *International Workshop on Distributed Event-Based Systems (DEBS'03)*, ACM SIGMOD, San Diego, CA, USA, June 2003. ACM.

9 Louati, W, Girod Genet, M, Zeghlache, D. UPnP extension for wide-area service discovery using the INS/Twine Framework. *IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC'05)*, Germany, September 2005.

10 Ghader, M, Olsen, R, Prasad, V, Jacobsson, M, Sanchez, L, Lanza, J, Louati, W, Girot-Genet, M, Zeghlache, D, Tafazolli, R. Service Discovery in Personal Networks; design, implementation and analysis. *IST Mobile Summit 2006*, Myconos, Greece, June 2006.

11 Meier, R, Cahill, V. Taxonomy of Distributed Event-Based Programming Systems. *The Computer Journal*, 48, 602–626, 2005.

12 Buford, J, Ross, K, Kolberg, M. *CORE Subgroup Problem Statement*. Internet Draft, January 2006. draft-irtf-p2prg-coreproblem-statement-00

13 Carzaniga, A, Rosenblum, D, Wolf, A L. Challenges for Distributed Event Services: Scalability vs. Expressiveness. *Engineering Distributed Objects (EDO '99)*, ICSE 99 Workshop, Los Angeles, CA, May 1999.

14 Stoica, I, Morris, R, Karger, D, Kaashoek, M F, Balakrishnan, H. Chord: A scalable peer-to-peer lookup service for internet applications. In: *Proceedings of the 2001 ACM SIGCOMM Conference*, 149–160, San Diego, CA, August 2001.

15 Ratnasamy, S, Francis, P, Handley, M, Karp, R, Shenker, S. A scalable content addressable network. In: *Proc. of the ACM SIGCOMM Conference*, 161–172, San Diego, CA, 2001.

16 Rowstron, A, Druschel, P. Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems. *Lecture Notes in Computer Science*, 2218, 329–350, November 2001.

17 Zhao, B Y, Huang, L, Stribling, J, Rhea, S C, Joseph, A D, Kubiatowicz, J D. Tapestry: A resilient globalscale overlay for service deployment. *IEEE Journal on Selected Areas in Communications*, 22 (1), 41–53, 2004.

18 Wang, C, Carzaniga, A, Evans, D, Wolf, A. Security Issues and Requirements in Internet-scale Publishsubscribe Systems. In: *Proceedings of the Thirty-Fifth Annual Hawaii International Conference on System Sciences (HICSS'02)*, 303.

19 Miklos, Z. Towards an access control mechanism for wide-area publish/subscribe systems. *International Workshop on Distributed Event-based Systems (DEBS'02)*, Vienna, Austria, July 2002.

20 Fiege, L, Zeidler, A, Buchmann, A, Kehr, R K, Mhl, G. Security Aspects in Publish/Subscribe Systems. *International Workshop on Distributed Event-Based Systems (DEBS'04)*, May 2004.

21 Balazinska, M, Balakrishnan, H, Karger, D. INS/Twine: A scalable peer-to-peer architecture for intentional resource discovery. *International Conference on Pervasive Computing*, 195–210, Zurich, Switzerland, August 2002. Springer-Verlag.

22 Robinson, R, Indulska, J. Superstring: A Scalable Service Discovery Protocol for the Wide-Area Pervasive Environment. *Proc of the 11th IEEE International Conference on Networks, ICON'03*, 699–704, Sydney, Australia.

23 Hodes, T D, Czerwinski, S E, Zhao, B Y, Joseph, A D, Katz, R H. An Architecture for Secure Wide-Area Service Discovery. *Wireless Networks*, 8, 213–230, March 2002.

24 Lee, C, Helal, A. A Multi-tier Ubiquitous Service Discovery Protocol for Mobile Clients. *Proceedings of the 2003 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2003)*, Montréal, Canada, July 2003.

25 Arabshian, K, Schulzrinne, H. GloServ: Global service discovery architecture. In: *MobiQuitous*, 319–325. IEEE Computer Society, June 2004.

26 Zhu, F, Mutka, M, Ni, L. Service Discovery in Pervasive Computing Environments. *IEEE Pervasive Computing*, vol. 4, pp. 81-90, 2005.

27 Louati, W et al. Networking in Personal Networks. *Workshop on Applications and Services in Wireless Networks (ASWN'05)*, Paris, France, June 29 – July 1, 2005.

28 Louati, W, Zeghlache, D. A Dynamic VPN management architecture for Personal Networks. *ASWN'05*, Paris, France, June 29 – July 1, 2005.

29 Murakami, H, Olsen, R L, Schwefel, H P, Prasad, R. Managing Personal Network Specific Addresses in Naming Schemes. *WPMC'05*, Aalborg, Denmark, September 2005.

Wassef Louati received the MS Degree in Computer Science in 2004 from Pierre et Marie Curie University (Paris, France). Currently, he is a PhD student at the "Institut National des Telecommunications" (Evry, France) in the wireless networks and multimedia services department. His main research interests include naming, service discovery and peer-to-peer architectures with a current focus on Personal Networks.

email: wassef.louati@int-evry.fr

Djamal Zeghlache graduated from SMU in Dallas, Texas in 1987 with a PhD in Electrical Engineering and the same year joined Cleveland State University as an Assistant Professor. In 1990 and 1991 he worked with the NASA Lewis Research Centre on mobile satellite terminals, systems and applications. In 1992 he joined the Networks and Services Department at INT where he currently acts as Professor and Head of the Wireless Networks and Multimedia Services Department. He is an active member of the IEEE communications Society and a member of the IEEE Technical Committee on Personal Communications. He acted as co-technical chair of the ASWN 2001, 2002, 2005 Workshops and Technical Chair of the Wireless Communications Symposium for Globecom 2003. He acts as lead scientist for INT in the European project MAGNET Beyond. He is also an expert group member of the eMobility Platform at the European level for framework program 7 and involved in WWRF working groups 2, 3 and 6. His interests and research activities span a broad spectrum of issues related to wireless networks and services. The current focus besides resource allocation is on dynamic adaptation and configuration of wireless networks and services based on context awareness and service discovery using P2P and autonomic networking paradigms. An ongoing activity relates to personal networks seen as a wide area extension of wireless personal area networks involving remotely located personal clusters. A key objective is to address the challenge of establishing overlay networks and service overlays for these networks at run time to enable dynamic and context aware adaptation of services and applications.

email: djamal.zeghlache@int-evry.fr

Challenges and Solutions in Achieving Personalisation Through Context Adaptation

RASMUS L OLSEN

Rasmus L. Olsen is a PhD student at Aalborg University, Denmark

This paper introduces the general concept of personalisation by context adaptation of client application. To achieve this, there is a need for a framework that gathers, stores, processes context data and in any other way makes the access to any relevant information easy for any client application that wishes to utilise context information. This paper addresses some of the fundamental challenges needed to be overcome before a true realisation of such a vision can be deployed. The general solution to many of these challenges is achieved through personalisation using profile information. First is presented an introduction to the Personal Network environment which this concept has been developed for. This is followed by a description of a Secure Context Management Framework, which plays a central role in the personalisation concept. Since different context information introduces different technical challenges, a short introduction to some commonly used information is described and how it relates to the personalisation concept. Finally is given a description of how different choices of architectural and security nature impact the adaptive behaviour desired for client applications.

1 Introduction

Adaptation to the environment and circumstances is an important issue for any person. People are doing this constantly without thinking about it, e.g. avoiding walking into objects, reacting in certain ways towards different people, switching off the light when wishing to sleep and so on. Humans do this without giving too much thought about many of these decisions we make every day, and even consider many of them as trivial tasks. For electronic devices this is different. Such devices need instructions in how they should behave. Even though several techniques exist today, most with its origin in Intelligent Autonomous Systems such as robotics that implements both intelligence and autonomy, such technology is still at the emerging state in the world of communication. The main reason for this is that whereas robots and other intelligent autonomous systems are typically small and closed systems with a specific purpose to serve, communication technology typically has more general purposes, and may have to adapt to a variety of situations. Furthermore, specific purposed systems are typically equipped with the necessary sensors and software to enable them to do their job, whereas mobile communicating devices may have to deal with the fact that they do not always have directly available the information needed, but will have to discover sources that provide the information needed, and then obtain the information over the network. This fact gives the mobile system an advantage over the specifically designed closed systems, as it becomes possible to use all kinds of information imaginable, but with the price of complexity of achieving a generalised methodology to achieve this.

Much research has been ongoing to make devices intelligent in this way, as for European projects examples are [E-SENSE], which is a project that aims to develop a system that captures the environmental situation of a given user by the usage of sensors organised in networks (sensor networks). The project MAGNET Beyond [MAGNETB] is focused on constructing a platform providing context information within the framework of Personal Networks, which in turn will support context aware applications. DAIDALOS [DAIDALOS] is another project working on a platform to support context aware applications. Other specific projects such as LAICA [Giacomo05 et al.] aims to use ambient intelligence to control human and vehicle flows in real life. In fact, all this activity, and also earlier activities within this field shows the potential of this concept. However, there is a long range of problems related to using context information to achieve the desired behaviours.

It is the main purpose of this paper to provide an overview of the challenges that need to be solved prior to successful deployment of context aware applications. The key solution to many of these challenges is given as personalisation using profile information as it will be explained in the paper. This links closely to the network paradigm Personal Networks, in which the basic concept is also explained in the paper. However, there are some implications to taking this approach, as will also be described.

The rest of the paper is organised as follows: The rest of the introduction is focused on introducing Personal Networks, context, context awareness and how these relate to each other. Following this, an introduction to a Context Management Framework is given in Section 2, where requirements to such a system are listed and a high level architecture is described. Challenges in managing some common context information is

ISSN 0085-7130 ©Telenor ASA 2007

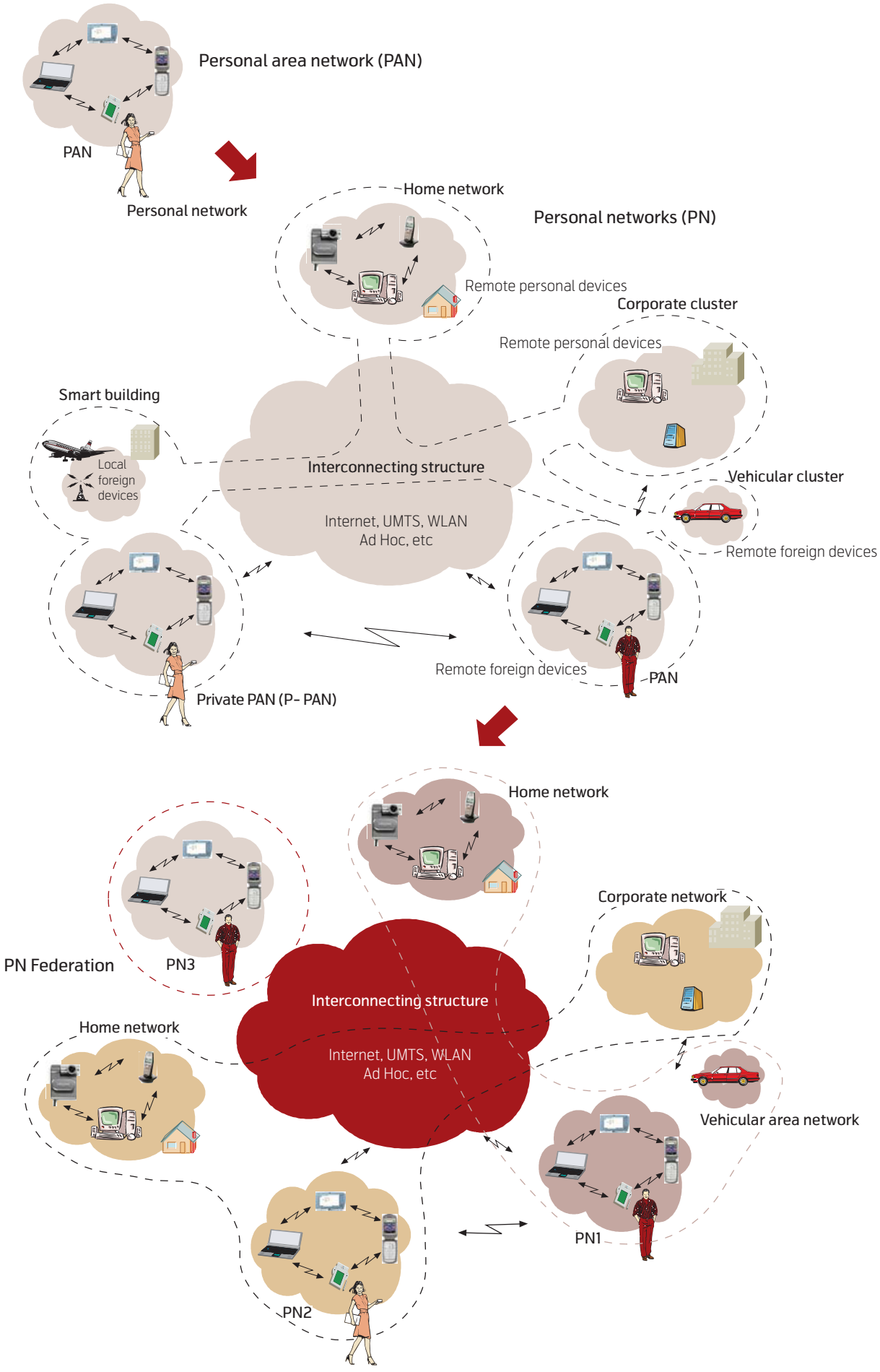


Figure 1.1 Conceptual illustration of how the PAN concept has migrated into the PN concept and further to federation of PNs [MAGNETB]

ISSN 0085-7130 ©Telenor ASA 2007

then described. Section 3 describes how profile information can be used to personalise context awareness, and finally in Section 4 implications on context awareness are discussed in terms of profile location and privacy policies. The paper concludes in Section 5.

1.1 Introduction to Personal Networks and Federation

Devices within a short geographical range being able to communicate and at the same time having a personal relation to each other can be perceived as a Personal Area Network (PAN) [Pereira00]. This concept has now existed for some time, and a natural extension to the PAN concept is called a Personal Network (PN). A Personal Network was first introduced in [Niemegeers02]. Whereas a PAN is limited in its geographical distance, a Personal Network (PN) can span a larger area, potentially globally, covering several network domains. A PN is hence a network that connects the user's PAN to remote networks, like other PANs, office networks, or home networks. Figure 1.1 illustrates the concept of PNs, showing its heterogeneous collection of networks and how it relates to the PAN concept.

In a Personal Network, a user is able to connect to his or her devices and services using whatever infrastructure is available for communication, e.g. the Internet, WLAN, UMTS or GSM. Personal networks are dynamic just as PANs, in the sense that they are created, maintained and destructed in an ad hoc manner, e.g. when a user moves around a building, nodes become a part of the network ad hoc, and may also leave the network as they move out of range or for other reasons are no longer useful to the user. The heterogeneous network composition that is a natural consequence of enabling this vision is also a characteristic of a PN.

For Personal Networks the communication between clusters is governed by security mechanisms that ensure the user's privacy and protects the devices within the network from outside attacks. This means that security is a key issue in Personal Networks, since sensitive information regarding the user, and private services will be accessible to the user anytime, anywhere, while required to be protected against intruders.

Considering that the PN is personal to the user, the case where the user wishes to share resources or services with friends, colleagues, family members or others of interest, clearly requires additional security features. The concept of sharing resources and services between PNs is considered as PN federation [Niemegeers05]. A PN federation can be established either manually by one individual inviting relevant users to a pre-selected subset of resources and/or services available in the initiating user's PN. It could also be context triggered proactively, e.g. as the user goes to a meeting, the PN federation between meeting participants is established automatically.

In fact, the context triggered PN establishment is just one example of what context information can be used for within the scope of Personal Networks. Also, service discovery or provisioning could benefit from the knowledge of the given situation of the user and service. For example finding the nearest available printer in the office building requires knowledge of the position of the user and the service, or switching the video stream from a 3G mobile phone to a nearby laptop before the 3G mobile phone runs out of battery power. However, whether a user wishes to have a PN system to make such decisions and how exactly it should react will vary. Hence, there will be an important interaction between context information, and user profile data that instructs a client application how to use it.

1.2 What is Context and Context Awareness?

In this paper the wider definition of context suggested by [Dey00] will be used as a basis for a definition on context:

> *Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and application themselves.*

Based on this definition, context in this paper will be focused around the following sub groups:

- *User context:* Any attributes describing a user's context, e.g. the activity, position, status and so on.
- *Device context:* Any attributes describing the situation of a device and its environment, e.g. battery status, OS environmental parameters such as available memory, CPU usage and so on.
- *Network context:* Any information regarding the network, e.g. link state, end-to-end delay and bandwidth, topology information, network types etc.
- *Environmental context:* Any information about the environment, e.g. the ambient temperature, light intensity, sound level etc.

These groups describe well, although still on quite a high level, what is relevant to Personal Networks (and other networks in general).

Being context aware [Dey, Pascoe99, Schilit94] means that an entity is aware of the situation it is in, and potentially can react properly to the situation, or as a minimum make decent decisions. In this paper, context awareness is defined as:

Being context aware is the ability of an entity to be aware of the current circumstances and be aware of relevant information that may influence any decision and behavioural change based on the context it may or may not take.

In practice, context awareness can be divided into two groups:

- *Proactive:* Those entities providing proactive context awareness use context information proactively to react on changes, e.g. by changing parameters and configuration to fit into the new situation or notifying a user of something.

- *Reactive:* Those entities reactively using context information typically need to know the current situation to make a decision here and now. An example is context aware service discovery, see [CASD106, ACANCASD].

This paper describes how context awareness can be achieved in both the proactive and reactive sense. A range of challenges need to be solved in order to make this concept strong enough for deployment, which is addressed in this paper. The key solution to these issues is found in personalisation using profile information, as will be explained in the paper. The reason behind this is that as individuals, users are different and want and expect different things from a system and the applications running on a system. Proactive context awareness may be seen as annoying by some, while assisting others. The settings that the paper is based on, is Personal Networks, which is introduced in the following section, for which personalisation plays a key role.

1.3 Context Description and Semantics

A particular problem in dealing with context information is how to describe and model it. Obviously, one can take any arbitrary approach if interaction with external systems is of no concerns. But especially for context, this is hardly ever the case, since context per definition largely also constitutes information about the world external to an entity. This makes it necessary for the entity to understand how other systems describe the world. It is important for a context description that it is

- Based on a proper context model, i.e a model that well describes the relevant objects and their attributes in order to be useful for client applications;

- That the description language is extensible, i.e. it is easy to add new objects to the description without having to change any interfaces;

- Understandable by all involved parties, i.e. the client application and the context provider.

Of existing technologies that can be mentioned, ontology is one of the more important methodologies used to describe context. Ontologies allow formal descriptions of concepts and attributes which allow efficient modelling between instances of concepts. Ontologies also allow for reasoning in the sense that the device can deduce certain things based on having knowledge of something else. Ontologies are hierarchically organised, which makes them useful for an object oriented model approach. One of the most important ontologies is OWL (Ontology Web Language) [W3OWL]. OWL comes in three flavours, OWL Lite, OWL DL and OWL Full. Even though they are increasingly expressive, they are also increasingly complex, and whereas OWL Lite and OWL DL are decidable in time, the full version may have endless loops. OWL is based on XML and RDF (Resource Description Framework) which also makes this ontology better understandable for client applications. Notification 3 [W3N3] is another ontology, which is basically a non-XML serialisation of RDF.

1.4 The Need for a Context Management Framework in Personal Networks

To enable context awareness in an application undoubtedly requires additional intelligence implemented within the application, concerning the observation of context and the reaction to changes that occur. Since there are many applications that may benefit from context information, it is beneficial to have a system that can monitor and manage such information to avoid applications replicating the same functionality of managing context information. Using a context management system allows the applications and their developers not to worry about problems related to management of context information, which among other things include the discovery of information sources and maintenance. A system performing these functionalities is sometimes known as Context Management system [PERNETS06]. The application would however still need to worry about reacting to context information (and interfacing the context management system). Hence, the division of intelligence required for context awareness would roughly be so that all discovery and monitoring functionalities are suited for the context management, while the reaction and usage logic will need to reside on the client. Having all management logic residing in a context management system is advantageous for a number of reasons:

- Clients will achieve a common view of the world. This is an important aspect from a user's point of view. Imagine that this is not the case and there is no SCMF, then any application, service or component being context aware would necessarily have to obtain all information by itself. Now, if there is any logic used in this process to e.g. derive higher level context information, the same context data would not necessarily be derived in the same way, leading to different context awareness, in spite of wanting the same context awareness.

- Client applications will use less processing power on inferring, monitoring etc. However, in the case of multiple clients needing access to the same kind of information computer resources can clearly be saved, since instead of having the multiple clients doing the same job, only one entity will be doing the job.

- There is always the potential for saving communication when considering multiple client applications accessing the same information over the network, compared to the case when each client application is responsible for obtaining the information required on its own. Proactive versus reactive updating schemes along with various caching strategies have an impact on the performance here, but is not further investigated in this paper.

- Clients will not need to worry about discovery and maintenance of the particular information (which also may be optimised with multiple clients), and this allows an easy interface to the information.

How the information is used is of course of no concern to the context management framework. Any decisions and reactions to the information are clearly application dependent, i.e. this kind of logic must be performed in the client.

2 Secure Context Management in Personal Networks

This section describes the requirements and challenges that a Secure Context Management Framework (SCMF) as envisioned for Personal Networks will face. There are many other initiatives investigating this topic, such as [E-SENSE], ACAN [ACAN], but in this paper the focus is on the solution proposed in the MAGNET Beyond project, as this is directly related to Personal Networks. Only a short introduction to the concept is given in this paper, see [PerNets06, CMF06] for more detailed descriptions. Following the introduction to the SCMF, an overview is given of how and why context information is specifically challenging to manage using examples of some commonly used information.

2.1 Requirements to a Secure Context Management Framework

For a context management framework to be really useful, it must fulfill a set of requirements. These come from the client applications and the individual user. A brief summary of the key requirements that have been derived for the context management framework in [CMF06] are listed below.

§1 It must be possible to add and remove context information which the context management framework will be monitoring by the most efficient approach.

§2 The client application should have efficient access to the context information in the sense that it does not need to worry about 1) the discovery of the context source, 2) what means it should use to obtain the data, and 3) whether the data is trustworthy or not.

§3 The client application should not need to worry about the dynamics of a cluster, i.e. discovering new potential sources of information, making handover to new and potentially better sources etc.

§4 The SCMF needs to be scalable in order to cope with, not only a full sized PN, but also potentially large PN federations.

§5 The SCMF should be able to cope with missing or ambiguous context data. This is an indirect requirement from §2.

§6 The SCMF needs to support proactive context awareness, i.e. it will need to be able to send event messages to client applications to invoke reactions at the application.

§7 The SCMF must use standardized data formats, i.e. the potential sources of information use a plethora of different data formats, and for all applications to understand its output, one or more standardized output data formats must be used.

§8 The privacy of the user must be ensured by any means, either by disallowing the information to be given by the SCMF or by making the output data anonymous.

§9 All access to context data must be authenticated in order to verify that the information provided is not falling into the wrong hands.

§10 Data integrity and confidentiality must be kept at all times to ensure that the user will continue

trusting such a system. If the user ever loses trust in the SCMF, the user will most likely not use it anymore, and over time, the system will be less and less used as it will gain a bad reputation in society.

§11 Data freshness and non repudiation must be detected by the system.

In particular the requirements regarding security are of the utmost importance, as context information potentially consists of very sensitive material about the user. Using this information to enhance client applications functionality and behaviors has its benefits, but also its downside if the system leaks the information to the wrong persons.

2.2 Overview of the Secure Context Management Framework Architecture

To meet all the functional requirements set to a secure context management framework a set of functional entities can be set up in a framework. For the project MAGNET Beyond, the components shown in Figur 2.1 have been defined [PerNets06]. Instances of these components are running in one client, but as multiple instances of the SCMF are distributed across the PN, the components shown in Figur 2.1 are capable of interacting with other SCMF entities, hereby enabling exchange of context information efficiently.

A hierarchy of the different roles an SCMF entity can take ensures the required scalability of the system.

In brief, the Context Management Interface (CMI) handles all incoming requests and reformatting of input and output between the internal data structures used by the other components and the exterior world. Also queries involving different kinds of scope, e.g. scope in time and location (network as well as spatial), are handled by the CMI. The Context Aware Security Module (CASecM) ensures that the data inside the framework is secured from outside, that authentication and authorization are ensured, and that the privacy of the user is kept according to the user's wishes. The Context Access Manager (CAM) keeps track of where the data can be accessed most efficiently, e.g. if the information should be fetched through from the P&S module, DSA or through the network. The Processing & Storage unit is responsible for storing gathered data, inferring higher level context information, deriving additional metadata to the context information itself and other more processor requiring operations. The Data Source Abstraction contains the functionality to access and interact with local context data sources.

The above described components are not necessarily implemented on one node, although optimally they would be. Acknowledging that not all devices have

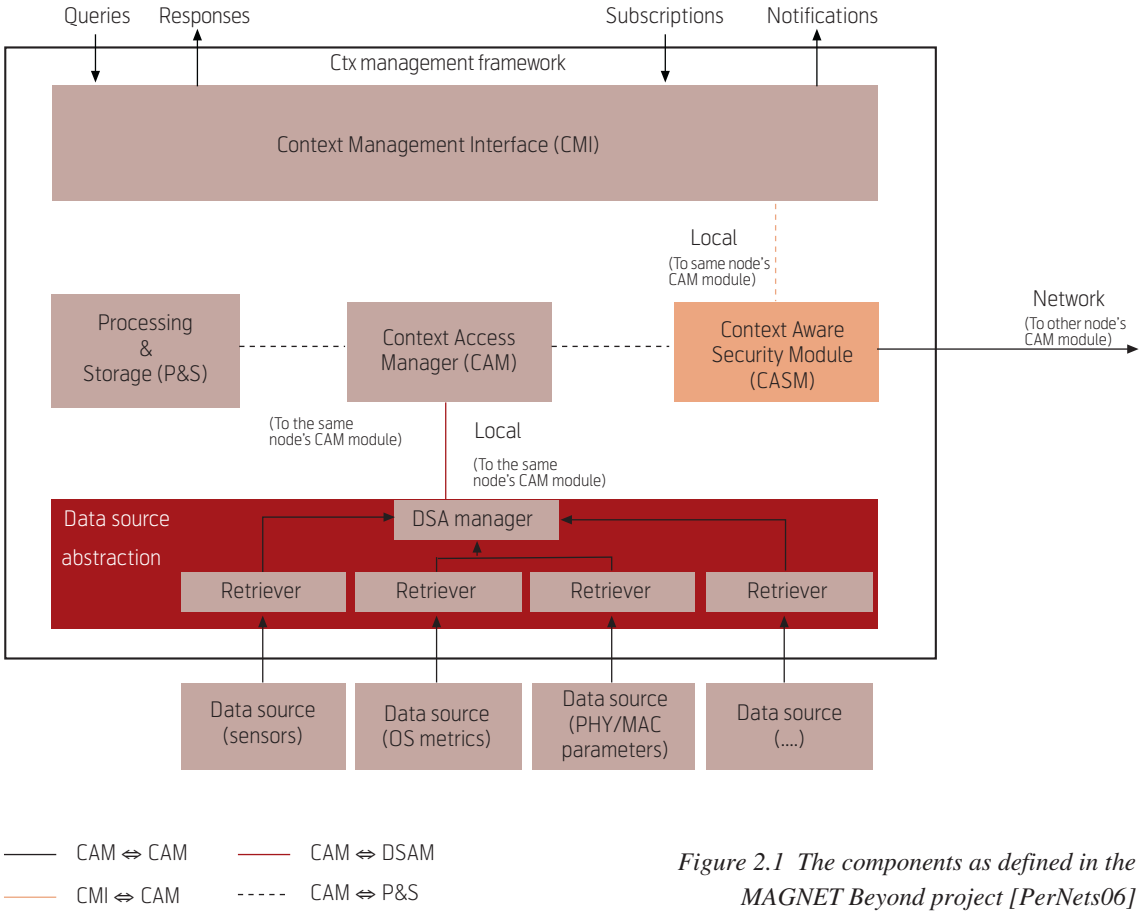


Figure 2.1 The components as defined in the MAGNET Beyond project [PerNets06]

ISSN 0085-7130 ©Telenor ASA 2007

the same computational resources available, three different entity types have been defined [PerNets06]:

- Basic Context Node (BCN) which implements a lightweight version of Figur 2.1, with none or more retrievers depending on the number of data sources available. This will have only the required functionality to efficiently access context information within the PN.

- Enhanced Context Node (ECN) which implements a heavier version of Figur 2.1 which has more intelligence attached to it to allow inferring and derivation of higher level context and additional meta data for the context.

- Context Management Node (CMN) which is an ECN, but with the special role of having an overview of all context within a cluster.

When these entities interact on a local networking level, the BCN or ECN will need to ask the CMN of any context information it does not have itself locally from its own DSA. Once known it may or may not obtain it directly from the source by subscribing, eventing or request methods. The exchange of information can be done either by value, or by reference pointers.

All interaction on global level will initially go through the CMN at first, while later subscription, eventing or request methods may be communicated between the requesting and providing entities.

2.3 Challenges in Dealing with Context Information

Managing context information is not only about the distribution, but also a matter of ensuring that the output given to the client application is unambiguous and that the probability of any error is minimised. In the following, a brief overview is given of what problem needs to be taken care of to some commonly used context information [Olesen et al. 2006]. Some more general issues, which relate to the fact that the information is typically distributed in a cluster, PN or PN federation, are such as:

- There may be multiple sources for obtaining the particular context information which may lead to inconsistency between the true and the used value, or selecting the wrong data source would potentially lead to misbehaviour in the context aware application.

- Mismatch between what is read and what is the actual value. This situation occurs in particular when accessing the information remotely, which may change value due to some external process. Through various means, it is however possible to estimate the probability of such error [mmpr06], which can be used to determine whether the information should be used or not.

- A particular context information is given in a syntax not understandable by either the SCMF or the application itself. A solution to this could be to attach transformation operators to the context itself, or pointers to where a transformation service can be found to translate the information into the desired syntax.

2.3.1 Location Information

Geographical locations has many potential usages, e.g. searching for nearby objects, showing direction to objects or even indicating how other context should be perceived. However, some issues may occur since this information can come from various sources:

- Location can be described either as a textual description, e.g. Room 203, or given as a set of coordinates. This implies that location given in different formats cannot easily be compared for e.g. distance calculation. A potential solution could be to put an attribute to the context information on where and how a location can be transformed. This would also allow transformation between different types of coordinate systems used.

- Bad tracking capabilities, e.g. if relying on a GPS signal in an indoor scenario. If the system used does not provide the functionality to inform about this, how can the context management then figure out to change the source of information?

- Security and privacy issues related to providing the location to a client application. It may not be that simple due to restrictions in the user's privacy or even legislation of a country (which may even change as the user travels around the world).

If there is uncertainty about the location, this will have severe impact on the user, e.g. if the system directs the user in the wrong direction, finding objects that are 100s of kilometres away etc. Hence, it is important for a context management system to address these issues, and as a minimum have a clear policy of what to do in such situations for then to allow application developers to decide what the application should do.

2.3.2 Time

Time is yet another important aspect in context information that needs some attention. In many cases, reacting on context will almost always depend on the right time (and place). In most cases, the SCMF would rely on the local clock on the device (if available), but there are some issues related to that

- The clock may not be synchronised. If the device does not include automatic synchronisation with some known source such as GPS, it will rely on the user having to set the clock manually. How does the system detect if the user did not do this properly? Or if it has switched to summer time? One way to address this issue is to check what other devices within a cluster consider to be the local time.

- The user may have switched time zone in relation to a travel.

- Relative time relations may not easily be described as absolute values, such as "information must be less than one hour old". What will happen if the information is one hour and two seconds old, because of update delay, is that the information is considered invalid, while in fact it may not be. One potential solution is to describe time relations using fuzzy membership functions. However, this requires an agreed definition of the membership functions that is available for all nodes within the network before such a solution can be used.

2.3.3 Device Context

Dynamic and static information about the device and its local environment, e.g. the OS and its environmental parameters such as memory, cpu usage, storage space available etc., can be considered as device capabilities. There are hardly any issues regarding getting this information as these are typically provided by the OS or accessed through device profiles. How this is done is however system specific, something which needs to be taken into account when implementing such a system.

2.3.4 Network Context

The network state is fundamentally challenging context information to address. Since a PN or PN federation contains a long range of network technologies, using a plethora of communication protocol stacks, each with their own states for different purposes, and having components working in different levels of the OSI stack model, one would need to focus on a subset of information to handle. It is however important to make the SCMF so extensible that mapping new interesting information into the system would not be a problem. Two parameters that are commonly used are:

- Link and end-to-end bandwidth: What is available for the application may have an impact on what service to choose, e.g. what video stream service should be chosen. However, determining end-to-end bandwidth across a heterogeneous network such as a PN remains a challenge to be solved.

- Link and end-to-end delay: Similar to the bandwidth end-to-end delay may not be easily determined due to the heterogeneity in the network composition.

A context management framework may help to exchange information between nodes and clusters within a PN, allowing a bigger picture of the network state in a PN. This would however put additional requirements to the model used to describe a full blown PN, which may not be so simple. Furthermore, the dynamicity within a cluster is rather rapid compared to the time it may take to distribute the information, so the SCMF designer must strike the balance between the level of information distributed in the PN and the delay of doing so with the dynamicity of the information. If the changes are happening too fast to be efficiently distributed, then perhaps it makes no sense to distribute it at all, but with the result that nodes in remote clusters will have an incomplete knowledge of all context in the PN.

2.3.5 Higher Level Context Information

Higher level context information is defined here as synthesized, inferred or derived information, which is based on one or multiple context information. Inference rules or other logic operations are used to figure out types of context information that sensors or other sources cannot provide. Some examples relate especially to user activity, such as sleeping, walking, in a meeting, generally available or similar. Since this group of information is based on other context information, some unique problems occur within this group:

- If one or more context information is missing, potentially out of date or in other way not completely trusted, the output, i.e. the inferred information, will also suffer from not being completely certain. If at least the probability of uncertainty can be estimated through the derivation, the application may be able to determine whether to trust the inferred information or not, and adapt its reaction pattern to that.

- The composition and weight of the different context information used may be individual and personal, i.e. depending on who the user is, where he is, what role the user currently has, a set of context information may be perceived in one way or another. For example how and what context information to determine if a user is busy or not, may depend on what job he or she has.

- Since multiple information may be required, the time to access and get all information may become a performance factor to be considered. Also the amount of computational resources may need to be carefully considered. On the one hand, the computations are time-wise best performed on the same

node as the requesting application, while resource-wise, a distribution of the computations and derivation may be the best option.

Without doubt, profiles become an important part when deriving higher level context information, which is also one of the aspects covered in Section 3.

2.4 How Personalized Profiles can Remedy Context Issues

There are of course many more cases, where context information gives ground to potential conflicts or misbehavior if not carefully analysed prior to the usage. It is out of the scope of this paper to perform a deep analysis of all these problems, which would also be a rather tough job, since context may consist of nearly unlimited amounts of information. However, handling these issues is not trivial either, and one must acknowledge that a solution which works for one person may not be suitable for another. For example with location, switching to another tracking system when going indoors may be fine for Person A, but for Person B who does not even like to be tracked, this may not be needed at all. Perhaps there is a reason that Person C has set the clock differently, e.g. because he likes to be in control of shifting time zones etc.

By any means, in managing context it is very important that the user has the possibility to be in control at all times. Whether the user chooses not to use a context management system, or to have partial or full control of how the system manages context, or even allow the system to do all things automatically simply because other options become too cumbersome to the user, is something that the user needs to decide.

The user may even be selective in what to control and what not to. Such choices may depend on several things, such as whether the information is trivial to the user, e.g. the ambient temperature, or if there are privacy policies related to it, such as his/her current geographical location.

Either way, knowledge about the user's preferences, will undoubtedly help the SCMF decide what to do, what not to do and what to ask the user on doing, and this is what the paper will discuss in the following sections, together with the impact of the user's decisions on the system.

3 Personalisation of Context Aware Behaviour

To address the problem of individuals and personal views on context management, profile information will play a critical role in the acceptance of any context aware behaviour. The direct influence of profile information in this sense may be divided into two groups;

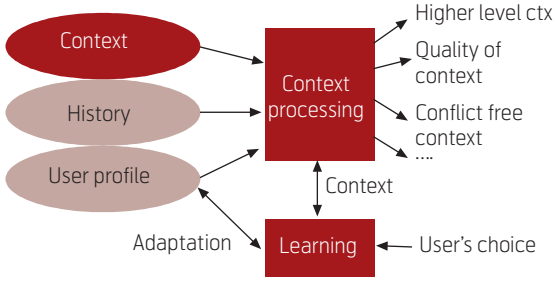
1 **Within the SCMF**, i.e. those profile data that will influence the way context is interpreted. These will necessarily depend on who the user is and to some extent what role the user has.

2 **To the client application**, i.e. the profiles will instruct the client application how to react to context or context situations.

Common to any context aware client application (i.e. any software entity that uses context information to alter its behaviour), is that there is a need for an agreement between the system and the user, on how context is understood and how the clients should react. For one person a given situation may require a specific reaction, while another person would prefer to have the application react otherwise. In fact, even the same person may require different reactions to the same situation, given that the user has different roles in the situation. User profile data is in this matter required to instruct a client application on how the particular situation or context should be perceived, and how the client should react or relate to it. It is important that all clients have access to the same profile data, which is why they in this way share the same view of context. If this is not the case, the user will risk different instances of the same class of context aware clients behaving differently to the same situation. This is not desirable and leads to the need for a common understanding of what role the user currently has, what the current context is, and what the user's preferences and settings are.

3.1 Personalisation at SCMFLevel

Figur 3.1 illustrates a general description of the relations between various information sources and processed context information. This will be a part of what is ongoing in the P&S module, depicted in Figure 2.1. There are two main active components in this diagram, the processing unit and the learning unit. The processing unit takes relevant input from the dif-



Figur 3.1 Adaptation concept on context processing using profile data [MBD121]

ferent sources, shown to the left, and performs any logic, statistical or other necessary operation to derive or infer the required output, with some examples shown to the right. The learning box, below the processing unit, is responsible for adapting user profiles based on processed context and user input, using any methodologies suitable for doing so. These two blocks form a closed feedback loop system, with the user profiles as target for manipulation. The purpose of this interaction is to enable the context processing unit to adapt its derivations and inference metrics so that in future it will output better results.

Understanding context information, and in particular higher-level context information, depends on who the user is and what role the user has. Imagine a baker and an office clerk. If the processing unit is supposed to determine whether a user sleeps or not, different information can be taken into account for each of the persons' jobs. Information such as user location, time of day, ambient brightness level and sound level may be used to infer the sleep status of a user by following pseudo rule, e.g.:

- IF (location is bedroom) AND (time is midnight) AND (ambient brightness is dark) AND (ambient noise level is low) THEN user sleeps.

Such a sentence may work well for the typical use case of an office clerk, except sometimes he sleeps at his girlfriend's or he takes a nap during the day in the weekend. For a baker, the time may not last through the whole night, as he would typically have to wake up at e.g. 3 a.m. Hence he would have a different sleep pattern that the above rule would not necessarily capture correctly. User profiles may then be applied by the processing unit to instruct how context data should be interpreted and used to infer higher level context data.

3.2 Personalisation at Client Application Level

As already stated, any application or service that is personalised will need some profile on how this is done. In this section we distinguish between those profiles that are static and those that are adaptive. The difference between these two types will have an impact on the complexity of the data structures necessary to describe the profile, as the static only depends on the profile information, while the adaptive also depends on context.

3.2.1 Static Personalisation

By static personalisation is meant the kind of personalisation that does not depend on context. This could be preference values, e.g. for

- Background colour or image of an application screen;
- Default notification sound;

and other behaviour or descriptions that are more or less static. These should of course be able to change with the user's will. What is primarily relevant for this kind of information is:

1 **What client the data is relevant for**: It is necessary to know what client a specific set of profile data is associated with.

2 **A set of attribute names and values**: For each behaviour a set of attributes and value pairs is needed to instruct the client what behaviour is being described, and to what value it needs to be set.

3.2.2 Adaptive Personalisation

Dynamic adaptation of services and application behaviour are in many cases a desired functionality for the user and will in most cases require context information, since the world that we are surrounded by is constantly changing. If the user has to manually setup the way a service or application should behave every time a parameter changes, he or she would need to do so constantly. Some examples of what adaptation of behaviour could mean are:

- Adjusting the contrast level of the display automatically to the ambient light intensity and screen colour so that the user can actually see what's on the screen. This is not necessarily an easy operation for the user to do.

- Change of notification methodology due to environmental restrictions, e.g. silence ringing when going to the cinema, which people tend to forget even with the reminders often provided, or increased sound volume in noisy environments.

- Adjustments of video resolution when streaming; in cases where the network conditions are changing often as in the wireless domain, it may be preferable to shift to a lower resolution to maintain a smooth view.

- Output stream re-direction to more capable devices, e.g. in case of the video stream, which may be viewed originally on the user's mobile phone, may automatically be switched to her TV screen or laptop for better view, performance or due to lack of resources on the current device.

Common for these examples, and for all other cases, is that the adaptation is user and application specific and depends on context information. In fact, to

achieve this kind of operations, a set of information needs to be available for the application to do so, primarily:

1 **What client this information is relevant for**: The following information must somehow be linked together with a specific client type, i.e. the context adaptation profile data for a calendar application will most likely not be the same as for a tourist guide application, simply because they focus on different objectives, require different inputs etc.

2 **What context to react on**: This depends on the service/application and to what extent this information is available.

3 **How to react on it**: This depends on the service/application and who the user is, and what role the user has. In some cases, context information may not be available, or only related context is available, in which some instructions are needed for the application to know what to do then.

4 **How to deal with uncertain information**: If context has been accessed remotely, there will always be attached some uncertainty, whether this information has changed during the update. How the application should react, if the probability of using outdated context information is very high should also be specified. Such action depends not only on the service/application and their requirements to the context used, but also on what kind of person the user is.

In the above examples, adjusting and changing the video stream depends strongly on what the user really desires, how much the user wishes to be in control (which may also depend on how technically knowledgeable the user is), the current role of the user etc. Such information needs to be accessible by the client anywhere within the PN, and furthermore, if two similar clients, e.g. two calendar applications are running on different nodes within the PN, they should adapt similarly.

It is clear from the two different situations, i.e. static and adaptive personalisation, that the adaptive requires much more information, simply because there is a need for additional information on what information is needed, and how it should be treated. This overhead of information is something that will impact the performance of the overall system behaviour, e.g. reaction time, network traffic, processing power (and system resources in general) etc., and hence one of the major challenges with this concept is to minimise the costs of these metrics and still be able to personalise in a satisfactory way.

3.3 Dealing with Uncertain Information: Being Optimistic or Pessimistic

No matter what kind of personalisation is being utilised, the client of the context management framework will need to consider one particular issue; namely that the information accessed may be remotely accessed. This fact may induce inconsistencies between what is obtained and what is actually there, i.e. some event may have changed the value of the information accessed. The Secure Context Management Framework will, based on different statistical information, be able to estimate the probability of a mismatch between the returned context information, and the true value (which is a particular problem that always occurs when accessing remote information, see [mmpr06]). This information is valuable to any client application, since it can be used to determine whether the information should be used or not. In this way an *optimistic* or *pessimistic* client behaviour can be obtained. *Optimistic* means that the client may take chances on context information, while others would prefer or even require a more *pessimistic* system that requires the system to be very confident on the context information before being used.

To exemplify the difference, client A may require a pessimistic view on information such as location data for directing a blind person to and down the stairs in his home, the client may take a pessimistic view to avoid the person being directed wrongly down the stairs hereby avoiding injuries to the person. Client B, who needs network context to provide a link to a resource for the person's PN, may be more optimistic towards the information given, since the consequences of invalid information are less dangerous to the user. The loss in taking a pessimistic view on context is that client A will become more reluctant to adapt to a given context than an optimistic client. However, client B, who takes an optimistic view of location data, risks the adaptation being error prone, but will more likely adapt to the changes detected by the SCMF.

The level of *optimism* may depend on the individual application, but may also be a general system attribute, depending on what type of person and role of the user, that clients per default will take. The individual part will need to be a part of a service profile, while the general system attribute can be a part of the user profile data.

Whether it will be per client or a global attribute, there is a need to define the level of *optimism* that a client or user wishes to have (which could also be based on the role of the user, and to the extreme based on other context information). As context information will be equipped with an indicator of how likely it is of being wrong when accessed (the mismatch probability, see [mmpr06]). A simple methodology, as for the user, is

to define an indicator, *optimism* defined in the interval [0;1], which simply describes the level of probability that the context information has to have before the system will consider it useful. A 0 indicates a completely pessimistic system (which can also be viewed as a non context aware system), and a 1 indicates a fully optimistic system. Using the Fuzzy Logic [Lefteri et al.] operator, *Not*, the level of *pessimism* is also defined as not(*optimistic*) which equals one minus *optimism*. The user or a user's role would necessarily have to be somewhere in between zero and one, in order to be really useful.

4 Client Access to the Data and Its Implications

In this section, it is analysed how different strategies of accessing the profile data may influence the desired context aware behaviour. First is given a discussion on a centralised versus decentralised solution, followed by a discussion on how security and privacy policies impacts implicated entities.

4.1 Local Versus Remote Storage of Profile Data

The personalisation concept is, as stated, based on profile information, which must be present somewhere within range of the application. The SCMF offers two basic approaches for accessing this information, which are A) a distributed approach, and B) a centralised approach.

To achieve this, two basic principles on where to store the necessary information can be used, see Figure 4.1:

A) A **distributed** solution: All the information is distributed within the PN and is accessible through the PN:
   - Consistency problems may become a problem when maintaining the data. Different distribution algorithms and strategies may be applied with varying impact on read access delay, inconsistency probability and generated network traffic, which need to be weighted against the importance of keeping data relatively fresh in the PN.
   - Maintenance is harder since the information is distributed and may involve more complex operations to ensure that all nodes have access to the data. Updates may not necessarily happen in one go, since not all nodes in a PN may be accessible at that time.
   - This approach ensures data is available at all times, hence suitable for PNs, where connectivity to infrastructure is not always present.
   - Data can be kept inside the PN, which is a plus for users who do not trust or for other reasons do not want to put this kind of data on a central repository, and potentially place their trust in third party entities.

B) A **centralised** solution: All the information is accessible through one specific node, e.g. a GUP server [3GPPGUP] or a private node in e.g. the user's home, either through SCMF or directly:
   - This minimises consistency problems with the data, i.e. updates are done on one master copy, and replicates may exist in the various clusters.
   - Maintenance of the data is easy, since this is done in one place (leading back to consistency problems).
   - Such a system relies heavily on that node being accessible at all times. If this is not the case, then the information is not known. This can be remedied to some degree by storing locally cached information, while updates may not be detected easily, leading to inconsistency problems.
   - Potential third party solutions, such as GUP, need to be entrusted by the user. Some users may like this, and some may not like it very much, since potentially sensitive personal data will be stored at this server.

Whether to take the centralised or decentralised approach may influence the experience of personalisation for the user, as the metrics consistency, read access, availability and so on are important for how the system behaviour is experienced by the user. Since the choice here will have an impact of consistency between the obtained and actual data (when remotely accessed), this may influence the level of optimism/pessimism the user desires.

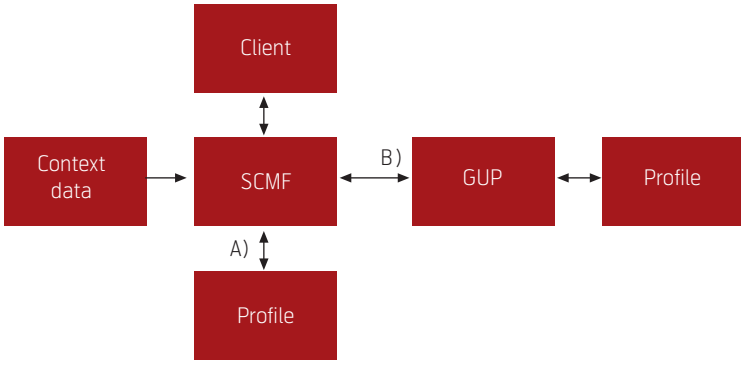


Figure 4.1 Approaches for a client to access SCMF maintained profiles [MBD121]

4.2 Security Implications on Accessing Context and Profile Information

Whatever approach the client takes in accessing the personalisation information, it will eventually need to access context information (those who personalises by adaptation). Since there are two fundamental different client types, **push** and **pull**, these two types will be described in the following:

4.2.1 Pull Types of Clients

In this case it is the user that initializes the communication with the service, invoking a client application etc. This can be done either locally on the node, or remotely through e.g. the Service Management Framework (in that case it would be the SMN). Either way, authorization and authentication are necessary operations conducted when invoking the client. In this setting, the client will hereafter have the possibility of keeping the credentials for authorization and authentication during a session, when accessing the information needed through the SCMF. This will of course require additional functionality in the client, but so will the adaptive behaviour desired.

4.2.2 Push Types of Clients

For Push types of clients the user does not initiate the communication with the client. This also means that in most cases the clients that require access to context and profile data do not necessarily have the credentials to gain access to the information. This may mean that, depending on the local security policy (and the overall user's security policy and levels), context or profile data may not be accessible to the requesting entity.

4.2.3 Impact of Anonymous Context Information on Clients

In either case, the client service or application must be able to accept that profile and/or context information may be only partially or not accessible at all, due to security policies alone. Another obstacle that must be accepted by the client, is that the information may be available but has been anonymised, e.g. a user that does not like to reveal his exact GPS position to an unknown, but useful service may (according to the policy) reveal a blurred and/or textual position, e.g. the name of the city he is currently in. This must be acceptable to the service in order to respect the privacy of the user.

This potential issue of anonymising context and profile data to the client will without doubt impose difficulties in enabling the personalisation concept that is desired. Even without this issue at hand, a client will potentially be able to utilise a plethora of information (the total set of context information and profile data goes towards infinity, considering that definitions of these are so broad). Furthermore, the fact that there can be alternative and anonymous name spaces for both context data and user profiles indicates the difficulty of implementing something that is more than a prototype. Hence, the work done here will be based on standards and possible extensions of these.

Considering anonymous context and profile data to become standardised (which seems reasonable alone from the fact that everybody then will be using these formats, hereby truly anonymising the user), a client could implement standardised behaviours for the anonymous data provided. This could be the case for both push and pull clients. Furthermore, there would also be a need for a default way to handle when the information is missing due to policy restrictions, not accessible information or because the level of optimism/pessimism dictates that the information should not be used. Hence, the road ahead for ensuring that this does not become a problem, is a standardised semantics for anonymised context data.

5 Conclusion

Adaptive behaviour is a key issue in current and future applications and communication means. One way of achieving this adaptive behaviour is to enable applications, services or other subsystems with the ability of being context aware. It is important for any entity to react properly to its environment, to know what is going on around it, hence the term context aware. As described in this paper, this is also the case for Personal Networks, whereas a Secure Context Management Framework is envisioned to assist the client application and its developer to overcome certain aspects in the management of this information. This framework was briefly described along with a set of sub problems related specifically to context information that needs to be addressed prior to a successful deployment of the framework. The key solution in addressing many of these issues is found through personalisation of context management, which is done through profiles. This concept can exist on two levels; the SCMF level and the application level. The profiles on the SCMF level instructs the SCMF on what it should do in certain situations where there are possibilities for ambiguous data conflicts, invalid data, how to interpret sets of context information, and so on. On the application level, the profiles instruct the application on how to be context aware, i.e. what reaction pattern the application should take in a certain situation.

The main point of this paper is that any context based reaction may be individual from person to person, i.e. one person may have trust in the system or wish not to interact with a potential cumbersome system setup,

while other people would prefer to be in control at all time or not allow such systems at all to operate for privacy concerns. Furthermore, certain groups of people would prefer certain reaction patterns, while others prefer other reactions, and so on. Rules and inferring of context information are also a matter of who the person is, what role the user has, and how he/she prefers the system to behave.

In fact, the problem can be boiled down to the question of whether a user would like to have this kind of proactive behaviour or to what level the user would accept it and still find it useful. The answer to this question is clear: let the user decide. The technical solution to how to achieve context awareness without being obtrusive to the user is on the other hand not trivial, but will require that the user accepts a more proactive system. This may perhaps be the most challenging task of all; to convince users worldwide that such a system is trustworthy and actually beneficial to the user.

The key challenges that need to be dealt with prior to the success of context aware systems, are manifold; the model and description of context is not trivial and depends in many cases on more specific use cases. Descriptions need to be accessible and standardised for all involved parties in the process, otherwise the context aware system will not be able to understand the information provided by surrounding systems or vice versa. A good formal description of context relies on a good context model, whereas ontologies seem to be the road ahead. But as the world is quite complex, with many relations between world objects, a good model is not easy to achieve. Indeed much work has been done in this area, but undoubtedly there is still more work to be done. A good model of context and their relations to others, may also be the key to resolve for conflicting context information which surely is a problem for context aware systems. However, as already stated, context is difficult because it constitutes many different types of information, neither resolving the context conflict will be an easy task to do, but it is nevertheless an important functionality for context aware applications and services in order to function properly.

A particular problem with any type of context aware client is that it will from time to time need information about the user that may be rather private. No doubt, the user will require an absolute secure system which enforces privacy policies, which is a challenge in itself, but the real challenge for context awareness to become a true success is whether the user will accept that a system uses information about the user such as her current geographical position, her current activity, mood or other information that may reveal the situation the user is in. As a minimum, context aware systems will have to ask the user once in a while whether this information is okay to use or not for this and that purpose. Over time, the context management system may learn from this input and ask less and less the user for advice. It is at all times important that the user is able to maintain control of such privacy rules. A particular problem that needs to be addressed is proactive context awareness, which the user does not necessarily want, and maybe seems like spam to the user. In other cases the user might desire such behaviour to some degree. Since most users will not like to constantly change the settings of these behaviours, there is an important need to strike the right balance between user interaction, system and application behaviour. If this balance is not achieved, then there is a great risk for context aware systems to fail on the market.

Acknowledgement

The author of this paper would like to thank everyone in the MAGNET Beyond project for fruitful discussions. In particular the author would like to thank Martin Bauer and Luis Sanchez for their contribution to and development of the secure context management framework.

References

[3GPPGUP] Salsano, S. *Presentation of the IST Simplicity project*. 3GPP SA1 meeting, Povoa de Varzim, Italy, July 2005. (Doc. num. S1-050725)

[ACAN] Khedr, M, Karmouch, A, Liscano, R, Gray, T. Agent-Based Context-Aware Ad Hoc Communication. In: Karmouch, A et al. (eds.). *MATA 2002*, LNCS 2521, 105–118, Springer Verlag, 2002

[ACANCASD] Khedr, M, Karmouch, A. ACAN Ad-Hoc Context Aware Network. *Proceedings of the 2002 IEEE Canadian Conference on Electrical and Computer Engineering*, 1342–1346, 2002.

[CASD106] Olsen, R L et al. Experimental analysis of the influence of context awareness on service discovery in PNs. *Proceedings of IST Summit 2006*, Mykonos, Greece.

[CMF06] Bauer, M et al. Context management framework for MAGNET Beyond. Invited paper, *Joint MAGNET Beyond, e-SENSE, DAIDALOS and CRUISE IST workshop*, Myconos, Greece, June 2006.

[DAIDALOS] *DAIDALOS*. Available from: http://www.ist-daidalos.org/

[Dey00] Dey, A K. *Providing Architectural Support for Building Context-Aware Applications*. Georgia Institute of Technology, 2000. (PhD thesis)

[Dey] Dey, A K, Abowd, G D. *Towards a better understanding of context and context-awareness*. College of Computing, Georgia Institute of Technology. (GVU Technical Report GIT-GVU-99-22)

[E-SENSE] *E-SENSE project website*. Available from: http//www.ist-esense.org/

[Giacomo05 et al] Cabri, G, Ferrari, L, Leonardi, L, Zambonelli, F. The LAICA Project: Supporting Ambient Intelligence via Agents and Ad-Hoc Middleware. *Proceedings of the 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05)*. Linköping University, Sweden, 13–15 June 2005, 39–44.

[Liscano03] Liscano, R, Ghavam, A. Context Awareness and Service Discovery for Spontaneous Networking. *AdhocNow 03*, 2003.

[Lefteri et al] Tsoukalas, L H, Uhrig, R E. *Fuzzy and Neural Approaches in Engineering*. John Wiley, 1997. (ISBN 0-471-16003-2)

[Niemegeers02] Niemegeers, I G G, de Groot, S H. From Personal Area Networks to Personal Networks: A user oriented approach. *Journal on Wireless and Personal Communications*, 22, 175–186, 2002.

[Niemegeers05] Niemegeers, I G G, de Groot, S M H. FEDNETS: Context-Aware Ad-Hoc Network Federations. *Wireless Personal Communication*, Springer, vol 33, June 2005

[MAGNETB] *MAGNET Beyond project website*. Available from: http//www.magnet.aau.dk/

[MD2.2.1] Ghader, M et al. *Resource and Service Discovery: PN Solutions*. MAGNET Deliverable 2.2.1, IST-507102, Dec. 2005.

[MD2.2.3] Olsen, R L et al. *Service, resource and context discovery system specification*. MAGNET Deliverable 2.2.3, IST-507102, Dec. 2006.

[MDB121] Olesen, H et al. *The conceptual structure of user profiles*. MAGNET Beyond deliverable 1.2.1, IST-507102, September 2006.

[mmpr06] Olsen, R L, Schwefel, H P, Hansen, M B. *Quantitative analysis of access strategies to remote information in network services*. To be published at Globecom, 2006.

[Olesen et al., 2006] Olesen, H et al. *Scenario construction and personalization of PN services based on user profiles and context information*. Invited paper, Joint MAGNET Beyond, e-SENSE, DAIDALOS and CRUISE IST workshop, Myconos, Greece, June 2006.

[Pascoe99] Pascoe, J, Ryan, N S, Morse, D R. Issues in developing context-aware computing. *Proceedings of the International Symposium on Handheld and Ubiquitous Computing*, Karlsruhe, Germany, Sept. 1999, Springer Verlag, 208–221.

[Pereira00] Pereira, J M. Fourth Generation: now, it is Personal. *Proc. PIMRC 2000*, 1009–1016, September 2000.

[PerNets06] Sanchez, L, Lanza, J, Olsen, R L, Bauer, M, Genet, M G. A generic context management framework for Personal Networking environments. *Proceedings of First International Workshop on Personalized Networks*, San Jose, California, July 2006.

[Schilit94] Schilit, B N, Adams, N I, Want, R. Context-aware computing applications. *Proceedings of the Workshop on Mobile Computing Systems and Applications*, 85–90. IEEE Computer Society, Santa Cruz, CA, 1994.

[Simplicity] *Simplicity project website*. Available from: http://www.ist-simplicity.org/.

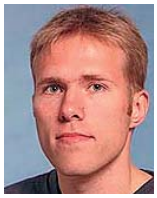
[W3N3] *Notation3 (N3) A readable RDF syntax*. Available from: http://www.w3.org/DesignIssues/Notation3.html

[W3OWL] *W3C OWL overview*. Available from: http://www.w3.org/TR/owl-features/

Rasmus Løvenstein Olsen received his MSc in Electrical Engineering from Aalborg University in 2003 with focus on antenna control for satellite communication. He has been very active in the pico-satellite program of Aalborg University called AAU-Cubesat. In 2004 he started in the IST project MAGNET where he has been working with Context Aware Service Discovery for Personal Networks. He is currently engaged in the project MAGNET Beyond where he is active in the design of a Secure Context Management Framework for Personal Networks. He is also pursuing a PhD degree on the topic of context aware service discovery. email: rlo@kom.aau.dk

Personal Network Directory Service

MIKKO ALUTOIN, SAMI LEHTONEN, KIMMO AHOLA, JORI PAANANEN



Mikko Alutoin is a Research Scientist at Technical Research Centre of Finland (VTT)

Sami Lehtonen is a Research Scientist at Technical Research Centre of Finland (VTT)

Kimmo Ahola is a Senior Research Scientist at Technical Research Centre of Finland (VTT)

Jori Paananen is a Senior Research Scientist at Technical Research Centre of Finland (VTT)

Personal Network (PN) is an emerging computer networking concept where security and privacy of communications as well as user centricity are emphasised. In this article we put forward a novel web service called Personal Network Directory Service (PNDS) that provides user authentication in the Internet by acting as a trusted third party and certificate store. This is required to facilitate authenticated inter-PN communications. In addition, we propose a method for building PN *federations* where a group of PNDS users share a secure virtual packet network. We demonstrate via concrete screenshots how user creates a PNDS account, gets a PN certificate, and finally joins a PN federation.

Introduction

The communications styles and paradigms are changing and the pace is breathtaking. The past ten years from the mid 90s to the present day were all about the Internet revolution and mobile phones. These two phenomena together changed our lives more than anybody could have ever imagined and many think that such growth in the industry can never return. Others are not so pessimistic and see the huge potential that lies in combining the Internet's openness and the wide range of emerging wireless technologies. The table is set up for cool applications and services taking advantage of rapidly growing bandwidth (in both fixed and wireless) and the flexible packet networking technology.

So far we have seen a promise of what the new technologies can deliver. Skype and Google are the biggest success stories of this decade when it comes to Internet applications. It is tempting to say that they are showing the way for others as well. Nevertheless, the two companies seem to have adopted very different strategies; while Google is eager to disclose its Application Programming Interfaces (API) as web services [1], Skype has remained very much isolated from the other players. Only time will tell which strategy will be more successful financially. We argue nevertheless that Google's way of disclosing its technology via web service APIs promotes innovation. Not everybody needs to re-invent the wheel, but players can utilise each other's APIs to produce new applications and services. This gives ground to a new kind of value net where the service provider needn't own and operate all the software components that the service comprises, but can rely on third party web service APIs. The dividends and cash flows within such value nets are interesting topics of their own, but are outside the scope of this article, which is more technology oriented. The article describes a novel web service named Personal Network Directory Service (PNDS). The main idea behind PNDS is to provide means for user authentication, which is an elementary component of any Internet service. The authentication is bootstrapped using the GSM's Short Message Service (SMS) after which public key certificates [2] can be used for authentication and encryption of Internet communications. This results effectively in a so-called *single sign-on* architecture [3],[4] where the user is seamlessly authenticated after an initial user-assisted login to the system. Moreover, it is shown how the PNDS can be used to implement a multi-user virtual packet network referred to as *PN federation*. To this end, two real-life scenarios are presented, in order to illuminate the background and motivation of the technical design. Finally we compare PNDS briefly with existing single-sign on solutions and discuss further work needed to make use of the developed technology.

Personal Network

Personal Network (PN) is an emerging paradigm where user's personal devices appear to form an isolated network regardless of their physical location [5]. Co-located devices organise themselves in so-called *clusters* and the clusters are inter-connected using virtual links (e.g. IPSEC tunnels). Virtual links typically exploit public networks (i.e. the Internet), whereas the intra-cluster links are either fixed (e.g. Ethernet) or wireless (e.g. Bluetooth, WLAN). Security and privacy are inherent properties of the PN and the applications need not worry about them at all. Figure 1 gives an idea of the concept.

From a technical perspective PN is actually a Virtual Private Network (VPN) – only authorised devices are able to join. Compared to the traditional VPNs, the PN is perhaps much more advanced in terms of self-organisation capabilities and heterogeneity in the supported networking environments, but its topology is still bounded by the device ownership rather than anything else. There are basically two ways by which the ownership can be determined: by pre-shared secrets [6] or by a Public Key Infrastructure (PKI) [7]

ISSN 0085-7130

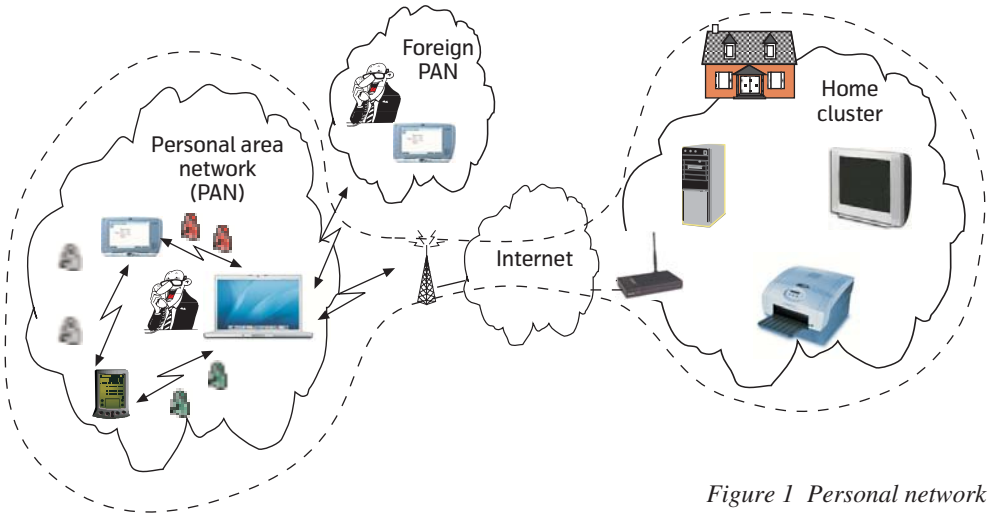


Figure 1 Personal network

based system. The former approach was thoroughly explored in the EU funded IST MAGNET project (FP6-IST-IP-507102) [8]. The PNDS, which is a PKI-like approach, is being studied in a continuation project called IST MAGNET Beyond (IST-FP6-IP-027396) [9].

Personal Network Directory Service

PNDS consists of a web service API and a database behind it. This database stores information about PNs as well as PN federations and participants in these federations; who created it and who maintains it (i.e. has the ability to add or remove participants or edit participant attributes).

Figure 2 shows the initial business model for the PNDS where only a single service provider is engaging in offering the service. It can be argued that this centralised architecture is vulnerable to single point of failure and that it traps users to a single service provider. The authors would like to denote that the ultimate goal is a multi-provider environment where different PNDS service providers can jointly provide the service. However, for initial piloting the centralised architecture may well be used to demonstrate the idea as well as the PN and PN federation concepts.

PN Certificates

Thus, the PNDS service provider(s) is a trusted third party. It stores public keys and provides *PN certifi-*

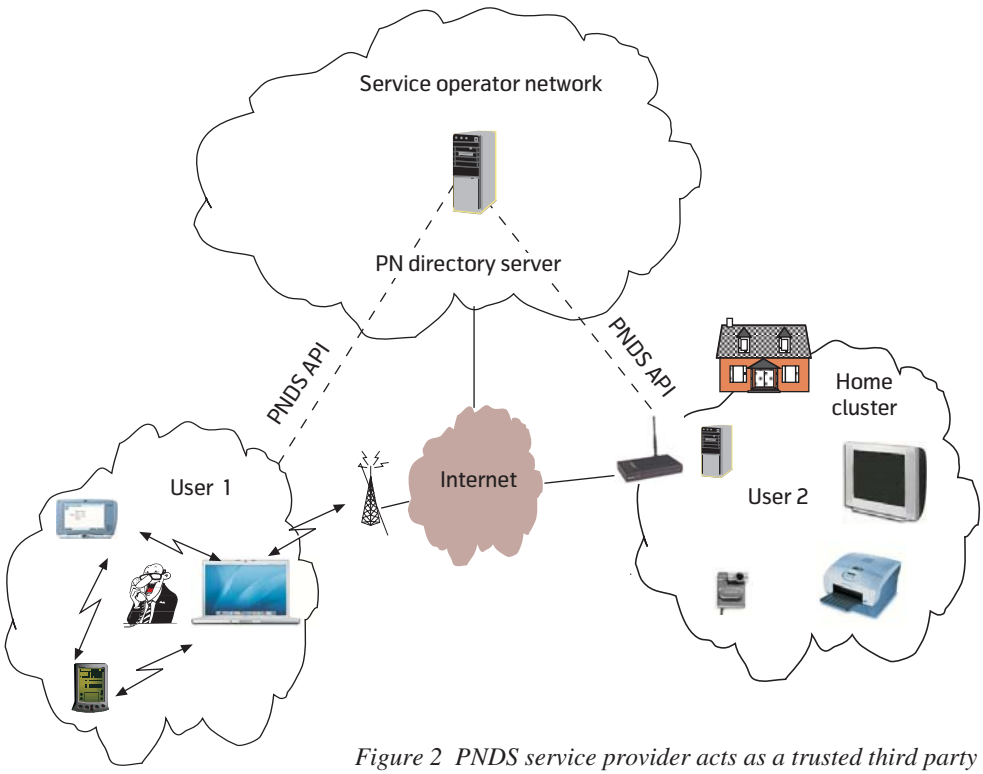


Figure 2 PNDS service provider acts as a trusted third party

ISSN 0085-7130 ©Telenor ASA 2007

cates for those public keys. A PN certificate binds together a public key and a PN name so that others may authenticate the user, provided that they trust the certificate issuer and its ability to authenticate the user to whom it has signed the PN certificate. Therefore, in order to deliver the certificate signing service, the PNDS must authenticate the user credibly. Otherwise, anyone could take over a well-established PN name and thereby steal one's digital identity. To this end, the user is required to create a PNDS account as shown in Figure 3.

The above data are sent via PNDS API's new_user method call and the PNDS account is created in the database. A random password is associated with the account so that the subsequent method calls from the user can be authenticated. This PNDS password is sent to the user via GSM's Short Message Service (SMS) as illustrated in Figure 4. Use of SMS ensures fairly reliable user authentication.

All the PNDS method calls are encrypted using Secure Sockets Layer (SSL), so that the PNDS password is never sent in clear-text through the Internet. The PNDS service provider itself can also be authenticated via SSL, if the PNDS client terminals have its root certificate. Except for the new_user method, all other PNDS methods require the user's GSM Number and the PNDS password as arguments. Therefore the user needs to log in, before using the actual PNDS API and proceeding to fetch a PN certificate and create PN federations, for example. The main login screen of the PNDS client application is shown in Figure 5.

The above constitutes actually a so-called *single sign-on* system. The user signs on once to the PNDS client and can be authenticated via PN certificates ever since, without having to introduce any further user names and passwords. Figure 6 shows how the client application fetches a PN certificate for a PN name. The PN certificate is written for the complete PN name which in this case is "+35840123456". Note that the PN name needn't reveal the user's GSM number, but PN certificates can also be written for pseudonyms, such as "knight_rider". In this case other users do not know who is behind the pseudonym, but the PNDS service provider can still store this information for legislative purposes, for example.

Figure 3 Creating a PNDS account

Figure 4 The user's PNDS password is sent via SMS

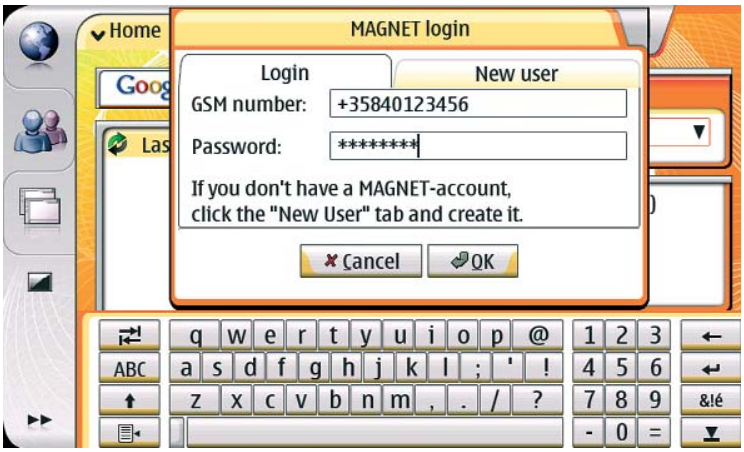


Figure 5 Logging in to the PNDS client application

PN Federations Using the PNDS

As mentioned already, the PNDS can be used to broaden the PN concept to include also the so-called *PN Federations* (PN-F) where two or more different persons set up a shared virtual packet network, in order to achieve a common goal [10]. To make things more tangible, we will first present two different scenarios where PN federations could be used. Then we will introduce a concept called *PN federation profile* and discuss its design in the light of the two scenarios.

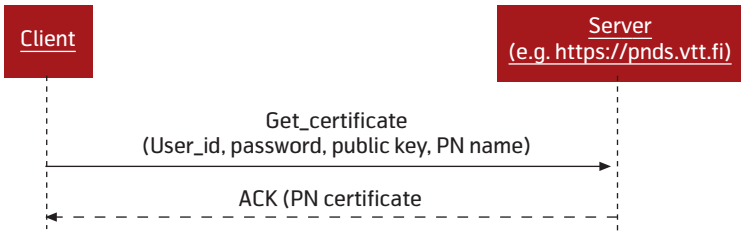


Figure 6 Certifying a public key using PNDS API

Football Club Federation

A football club manager needs to keep in touch with the players, in order to arrange the training times and prepare for the matches. He also wants to deliver some confidential material to the players and inquire into their health status. To this end he sets up a PN federation. The nature of the federation is long-term, since the team is quite static. Every now and then a player gets transferred, but then the manager can take action and erase the player from the federation and invite the new player to the federation. The federation should remain operational even if the manager is on a holiday with all of his personal devices switched off. Sometimes the manager wishes that the vice manager administrates the federation for him.

Lecture Federation

A lecturer at the university would like a possibility to set up a temporary ad hoc network for the duration of the lectures. This would be useful for distributing the lecture material as well as to perform a scientific study among the students using a digital questionnaire. Even small exams could be easily carried out using laptops and the temporary network. To implement this, the lecturer uses a PN federation. Because the nature of the virtual network is first and foremost ad hoc, the lecturer does not want to rely on having Internet access all the time. The federations are typically short-term and valid only for the duration of the lecture. The identities of the participants need not always be verified, but anonymous access to the federation might sometimes be perfectly acceptable.

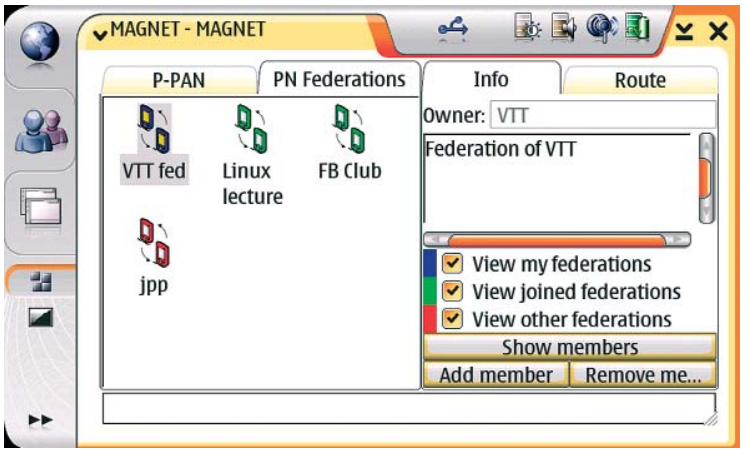


Figure 7 A student joining an ad hoc lecture federation

PN Federation Profile

The PNDS issued certificates, discussed in the previous section, provide a very good starting point for supporting PN federations. Some additional data structures still need to be defined so that the participants of the federation can be authenticated and authorised. For this the so-called *PN federation profile* is introduced. The PN-F profile is stored somewhere in the IP network, for example in the PNDS service provider's database or in the lecturer's laptop. The PN-F profile contains the following information:

- Name of the federation (and a corresponding PN-F certificate)
- Owner of the federation
- Deputies (i.e. additional federation administrators)
- Invitees (i.e. who are allowed to join the federation)
- Who have joined the federation
- Passphrase
- Federation's private key (corresponding to the federation's PN certificate)
- Federation's group key

Let us next discuss the items in the PN-F profile in the context of the specific requirements they are designed to satisfy.

Authentication of a Federation

As a user seeks to join a federation, she must feel secure in the sense that she is about to join just the federation that she has intended. For example, no malicious person should be able to "take over" a federation and start gathering private data of its users. Another point is to be prepared for unintentional mix-up of two federations due to almost similar federation names or a typing error from the user's side. Fortunately certificates can be used to fight against these threats. A key to this is to realise that the federation name in the PN-F profile can be just a similar kind of globally unique identifier as is the PN name (see previous Section). After all both PN and PN-F are virtual networks, so it is only logical to use the same kind of naming scheme. Just like any PN, also the PN-F needs to have a certificate from the PNDS, so that the participants may authenticate the federation while trying to join. We refer to this certificate as the *PN-F certificate*.

The federation's name may contain the owner's PN name, but it does not have to. It might just be that the

federation owner does not wish to reveal his/her GSM-number (or not even PN pseudonym). Thus, instead of math-lecture.+35840123456 the name can just be math-lecture, for example.

In the lecturer scenario, it could be that the Certificate Revocation Lists (CRL) [2] of the PNDS are not available, due to lack of Internet access. (CRLs are used to list certificates which have been revocated, because the corresponding private key has been compromised, for example.) However, the lecturer can prepare for this by having the certificates automatically renewed on a daily basis, while sitting in her office where Internet access is available. This way the certificate's issuing date will be only a few hours old and the students can be fairly sure that the federation's private key has not been compromised meanwhile.

Admittance to a Federation

The owner of the federation has maximum access rights to manipulate the PN-F profile. The owner can also manipulate a list of additional federation administrators, in order to give access rights to some deputies, for example the vice manager of the football club. The owner and deputies are identified by their PN names. These fields are primarily there to authorise the manipulation attempts of the PN-F profile itself, but they can also be shown to the federation participants, if the owner so wishes.

By default the federation is empty. Everyone, including the owner, needs to explicitly join the federation. For authenticating participants, while they first try to join the federation, there are two partially overlapping mechanisms: PN certificates and federation passphrases. To join a PN-F, the user always needs to have a PN certificate (i.e. a certified public key), but the certificate need not necessarily be issued by the PNDS – also self-signed certificates can be used in cases where the federation owner wishes to allow anonymous participation in the federation. When a PNDS-issued certificate is used however, it offers a nice way to authenticate the origin of the join request. To this end, there is an optional list of *invitees*, in which the owner may record the PN names of the people who are authorised to participate in the federation. For example, when creating a federation for the football club, the club's manager may invite only the members of the club to the federation and then store their PN names to the invitee list. PNDS then sends an SMS-invitation to the invitee where he is advised to join the federation. As the club members try to join the federation they will identify themselves with a valid PN certificate. After verifying the certificate, it is checked whether the PN name is included in the invitee list or not. In the case that the name is found in the list, the request is automatically authorised. If the PN name is not in the invitee list, then the request can be either rejected or left pending. A *pending request* is one that the system tries to verify from the federation's owner subsequently. The owner can of course deny the system to generate any pending requests altogether.

There are however cases when the invitee list and/or pending requests are not satisfactory. Think of the lecturer at the university, for example. She would like to set up a temporary PN-F for the duration of the lecture. The problem is that the number of participants is overwhelming and listing their identities in the invitee list beforehand is not something that the lecturer enjoys doing. In this case the federation passphrase comes to the rescue; the lecturer announces the federation name and the passphrase to the students. Any student can now enter the federation with a self-signed certificate by merely typing the federation passphrase when prompted for it. Omitting the whole passphrase from the equation would not be such a good idea, since then the number of mix-ups would increase. This is because in the university campus there could be multiple federations to which users can join accidentally, if the passphrase is not checked.

Federation Participation Certificate

After the mutual authentication and the admittance of the join request, the federation participant shall be able to operate fully within the federation. This means that all other federation participants should be able to verify that the participant has been admitted. This could be done in various ways. One option would be to check the PN-F profile. This would however fail if the PN-F profile cannot be accessed right then. To remedy this, we introduce *PN-F participation certificates* which are obtained along with the return message of a successful join request. See Figure 8, for example.

The PN-F participation certificates are usually signed by the PNDS, but in the ad hoc case also the PN-F owner can sign them. In the latter case the chain of

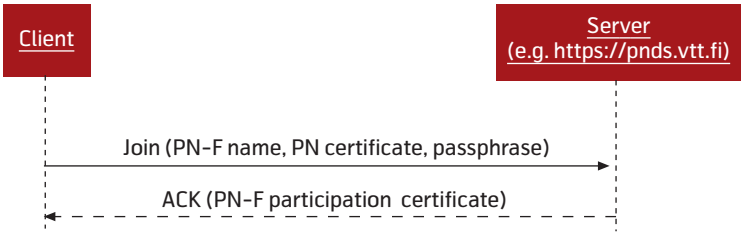


Figure 8 Student fetching a PN-F participation certificate

ISSN 0085-7130

trust goes as follows: PNDS root certificate > PN-F certificate > PN-F participation certificate. In the former case, the middle part can be omitted. In the football club federation, it is the PNDS which signs the PN-F participation certificates as it is handling the admittance to the federation (according to the invitee list). In the lecture scenario, it is the lecturer. The name, for which the PN-F participation certificate is made, can be, for instance, Laura@math-lecture or anonymous012@math-lecture.

Message Authentication

A federation is fundamentally a network layer concept. This means that the federation of a message is revealed by the IP layer packet headers. This way the overlapping federations interfere with each other as little as possible: messages of unknown federations can be discarded in the network layer without further processing. But how is a message's federation authenticated? A scheme [11] where each IP packet is signed and the signature is included as an IPv6 extension header could be used. This offers a nice solution, but only for IPv6 based communications. Another solution is to implement a layer 2.5 (between MAC and IPv4) for conveying the signature. But should the messages be signed with the participant's private key or with the *federation group key* which all the participants share? The latter option is somewhat more straightforward, as it does not require the recipient to know the sender's public key. However the former option provides more security. Probably both options should be supported.

Encryption of Communications

Typically the federation communications should be encrypted by leveraging the public key of the message recipient. Before the encrypted message can be sent, it could be checked whether the recipient holds a corresponding PN-F participation certificate. For group communications, such a method is nevertheless not very useful. Consider the lecture scenario where the students are taking an exam. The lecturer sends the questions for everyone using a broadcast message over the ad hoc radio network. This saves a lot of bandwidth compared to each student individually fetching the questions from the lecturer's laptop. If the lecturer wants to encrypt the questions for some reason, it is not possible to use any participant's public key, of course. Instead, the federation group key must be used for encrypting the broadcast messages. (A similar scenario, where encryption adds more value, is an ad hoc meeting in an airport lounge where the meeting chair distributes a confidential memo to the other participants.)

Related Work

There exists schemes which share some of the characteristics of the PNDS. In Liberty Alliance framework [3], for instance, it has been defined how a group of web service providers may federate their user accounts. The service providers seek to obtain knowledge about each other's user account databases (with a permission from the user). This is called *identity federation*. As the providers trust each other (via a circle of trust), they can offer the so-called *single sign-on* user experience: user needs only sign-on to one service provider after which he can be seamlessly authenticated to the others as well. This is useful, because today the various web accounts of a user are in pieces all over the Internet and the only connection between them is the user. (Fortunately many web browsers, such as Mozilla Firefox, can nowadays remember passwords for various web logins, which helps a bit.)

The main idea in Liberty Alliance is that a web service provider can rely on a trusted third party, called *identity provider* in this context, when it comes to user authentication and authorisation. As a user tries to access a service via HTTP, the HTTP server asks the identity provider to authenticate the user. This is achieved using HTTP redirection. After the identity provider has authenticated the user, it provides a credential called *artefact* for the HTTP client. The client tries to use the service again, but this time provides also the artefact to the server. The server contacts the identity provider in order to map the artefact to a user identity. Then, after knowing the user's identity, the server can proceed to the authorisation phase.

The Liberty Alliance framework is clearly defined from the service provider perspective; it assumes a clear distinction of providers and consumers. However, when it comes to PN federations such a division does not exist and therefore the architecture for PN federations should be more peer-to-peer oriented. Moreover, the Liberty Alliance framework is specifically designed for HTTP, whereas the PNDS is more protocol agnostic. The most distinct difference is nevertheless with respect to ad hoc and group communications: clearly the Liberty Alliance as such does not meet the requirements of, for example, the lecture federation presented in this article. This is because identity provider is not allowed to be offline and because group communications are not dealt with at all.

Windows Live ID (previously known as .NET Passport or Microsoft Passport Network) [4] is a single sign-on system for web systems. Live ID is based on authentication server, which asks for username and password. The server returns a time-limited GLOBALAUTH-cookie. The authentication server sends to

a user an ID-tag that the authentication and the commerce server had previously agreed upon. The commerce server will send a LOCALAUTH-cookie to the user as return to the ID-tag. The need to authenticate is thus handled as long as these cookies are valid. When the user logs out of Live ID, the cookies are removed.

Other identity protocols (based on URLs) are openID [12], Yadis [13], Light-Weight Identity (LID) [14]. The main differentiator between the PNDS and other means of identity management is that even though the authentication is done with the help of the service provider, the mechanisms (i.e. certificates) are useful also when the service provider is not accessible, e.g. in ad hoc networks.

The 3GPP is working on the so-called Generic Authentication Architecture (GAA) which defines how *subscriber certificates* are obtained from a mobile operator's Certificate Authority (CA) [15]. The 3GPP approach is in general very similar to the one described in this paper. There are some major differences however. Firstly, the architecture in [15] is more decentralised; a number of CAs, referred to as *PKI portals*, are used to write certificates. In order to do this, a PKI portal needs to contact the Home Subscriber System (HSS). In the PNDS approach the subscribers fetch the certificates from one central CA which also maintains the subscriber records. Another difference is how CA authenticates a subscriber. In [15] the authentication is based on the private key that is stored in the subscriber's SIM-card. We use SMS-based authentication. In the 3GPP GAA the certificates are fetched using HTTP Get (with Digest authentication) whereas we use XML-RPC [16] over SSL and the PNDS password as such for subscriber authentication. The CA's root certificate is hard coded in the XML-RPC client. Finally, the concept of PN federations is not addressed in the 3GPP GAA in any form.

Conclusions and Further Work

This article introduced a novel web service called Personal Network Directory Service (PNDS) that can be used to support federations of Personal Networks (PN). The approach is to utilise the described PNDS API for first retrieving certificates for one's public key, and then for joining to the PN federation. It was illustrated how a chain of trust can be built in order to facilitate ad hoc federations and how communications within the federations can be authenticated and encrypted. The support for ad hoc scenarios and group communications in general is what distinguishes the PNDS from the existing single sign-on solutions.

Currently the authors are working on supplementing the PNDS API implementation. So far methods for creating PNDS account, getting PN certificates and creating federations have already been implemented, as well as the counterpart client software of which the screenshots above were taken. The next steps will involve implementing the Join-method. The user experience that we have managed to create is so far very satisfying. PNDS is however only one part of the architecture on which federations are built. To make federations happen, further work is required in the areas of mobility management, middlebox traversal, and service discovery. Also applications that leverage the capabilities of the PN federations need to be built. When it comes to the ad hoc federations, advances in MANET protocols, such as in duplicate address detection and IP address autoconfiguration, are required. The majority of these issues will be dealt with in the remaining period of the MAGNET Beyond IST project where a PN pilot system is being built. The pilots shall be conducted during the first half of 2008.

References

1 *Google APIs*. http://code.google.com/apis.html

2 IETF. Housley, R, Polk, W, Ford, W, Solo, D. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 3280, April 2002.

3 *The Liberty Alliance project*. http://www.projectliberty.org

4 *Windows Live ID*. http://www.live.com

5 Jacobsson, M et al. Network Architecture for Personal Networks. *14th IST Mobile & Wireless Communications Summit 2005*, Dresden, Germany, 19-23 June 2005. European Information Society Technologies (IST) programme. Dresden (2005), 5 p.

6 IST MAGNET Project, Deliverable 4.3.2. *Final version of the Network-Level Security Architecture Specification*. http://www.ist-magnet.org/public+deliverables/phase1wp4, Feb 2005.

7 IETF. Chokhani, S, Ford, W, Sabett, R, Merrill, C, Wu, S. *2003 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. RFC 3647, Nov. 2003.

8 Hoebeke, J et al. Personal Networks: from concept to a demonstrator. *Proceedings of the IST Summit 2006*, Myconos, Greece, June 2006.

9 *IST Project MAGNET Beyond (IST-FP6-IP-027396)*. http://www.ist-magnet.org

10 Hoebeke, J et al. Personal Network federations. *Proceedings of the IST Summit 2006*, Myconos, Greece, June 2006.

11 Candolin, C, Lundberg, J, Kari, H. Packet level authentication in military networks. In: *Proceedings of the 6th Australian Information Warfare & IT Security Conference*, Geelong, Australia, November 2005.

12 Recordon, D, Fitzpatrick, B. *OpenID Authentication 1.1*, May 2006. http://openid.net/specs/openid-authentication-1_1.txt

13 Miller, J. *Yadis Specification version 1.0*. March 2006. http://yadis.org/papers/yadis-v1.0.pdf

14 *Light-Weight Identity (LID)*. http://lid.netmesh.org/wiki/Main_Page

15 3rd Generation Partnership Project, TS 33.221 version 6.3.0, Technical Specification Group Services and System Aspects, Generic Authentication Architecture (GAA). Support for subscriber certificates (Release 6), March 2006.

16 *XML-RPC Homepage*. http://www.xmlrpc.com

Mikko Alutoin entered Helsinki University of Technology (HUT) in 1995 and received his MSc in Electrical Engineering, majoring in telecommunications in March 2000. He did his Master's thesis for Nokia Networks, where he worked as software engineer for a few years during 1998–2001. Since 2001 he has been working as Researcher at Technical Research Centre of Finland (VTT) and has participated in a number of international EU research projects. He is also a post-graduate student at HUT.

email: mikko.alutoin@vtt.fi

Sami Lehtonen started studying information technology at Lappeenranta University of Technology in 1996. His working career began at VTT in 1999 in the Networks group. Besides working he continued his studies and graduated as a Master of Science in technology in April 2003. He is working at VTT in the Security team as a Research Scientist. In June 2006 he got his CISSP (Certified Information System Security Professional) certification #94049. He was a member of the information security risk assessment group that operated under the Finnish National Information Security Advisory Board in the Finnish Ministry of Traffic and Communications. Later he was a member of the Committee on Information Security in Critical Infrastructure at Finnish Communications Regulatory Authority.

email: sami.lehtonen@vtt.fi

Kimmo Ahola received his MSc degree (telecommunications) from the University of Jyväskylä in 1997. He has worked ever since at Technical Research Centre of Finland (VTT) on various international (e.g. EU, EURESCOM) and national projects concerning mainly IP systems and protocols. Currently he is Senior Research Scientist and team manager in the Adaptive Networks team.

email: kimmo.ahola@vtt.fi

Jori Paananen received his MSc degree (telecommunications) from Helsinki University of Technology (HUT) in 1983. Since then he has worked at Technical Research Centre of Finland (VTT) on research projects in the area of mobile and IP software systems and protocols. Currently he is Senior Research Scientist in the Adaptive Networks team.

email: jori.paananen@vtt.fi

Risk Analysis in an 'Insecure Wireless World'

SOFOKLIS KYRIAZAKOS, NEELI PRASAD

Sofoklis Kyriazakos is Assistant Professor at Aalborg University, Denmark

Neeli Prasad is Associate Professor at Aalborg University, Denmark

Risk analysis is the process that each operator should go through to determine the risk exposure. This risk is linked with the possibility of the damage that could happen either from intruders or by misuse of the resources. The goal of risk analysis is to determine the probability of potential risks and estimate the overall damage at an annual basis in order to define new policies and measures. In the wireless world the major feature is the air-interface, however these systems also follow the same practices to determine the risk probability, while emphasis should also be given to the characteristics of the transmissions and the related vulnerabilities. In this paper we deal with the issue of risk analysis for wireless systems regardless of the access technology.

1 Introduction

The paper is organized as follows. Section 1 is an introduction to risk analysis in a wireless environment and presents the structure and the sections of the paper. In Section 2 we present typical cases and scenarios. In this initial study, we present two cases; namely the multi-operator diversified radio environments and the Personal Networks. The reason why we focus on these two is that they both construct major categories where networking environments and topologies can be classified. In other words, if asset identification and harm estimation are performed for these scenarios, then every networking architecture can be addressed by referring to these models. In Section 3 we identify the network resources and the assets. These will be considered in the subsequent steps in terms of failure probability and harm estimation. Assets for network operators are not only tangible, e.g. system components, but intangible as well. Under intangible assets we should consider user satisfaction, operator's reputation, etc. All assets are placed in a tree structure so that we can easily see the impact of an outage in a network component. In Section 4 we estimate the threat likelihood and the related harm. In regard to the threat likelihood there is a categorization based on the frequency of occurrence of a failure or outage; however, it is important to asses the probability for a given duration. This is meaningful, as a risk assessment study should refer to a specific time-frame, e.g. one calendar year.
In Section 5 we proceed with the risk assessment methodology. This is a set of equations that calculate the total exposure, which is the final outcome of the risk assessment exercise. In Section 6 we present an example of risk analysis. This example is neither the multi-operator diversified radio nor the Personal Network; however, it shows the proposed methodology for a UMTS environment. This is because the above-mentioned scenarios are complicated configurations and in order to show how the methodology is structured, we have described a UMTS scenario and then we extend the study to the complicated situations. In this example we place the network components of a UMTS network in a tree structure and we calculate the probability of an outage in any node, as well as the harm. For each node of the tree both the probability and the harm are calculated if we list all kinds of threats, e.g. denial of service, unauthorized access, and we assess the probability and the resulting cost. Finally, in Section 7 we sum up with the conclusions and the future work.

2 Use Case and Scenarios

There are several use cases and scenarios associated with the proposed procedure, however we clustered them into two categories; namely (a) multi-operator diversified radio environment and (b) Personal Networks. The reason for this split is that they have a different philosophy in terms of who operates the network and if this is based on the concept of base station – mobile terminal and/or ad hoc communication. However, in Sections 3-6 we analyze the example of a UMTS network that is more tangible and we explain how this can be extended for the two use cases described bellow.

2.1 Multi-Operator Diversified Radio Environment

The development of wireless systems has evolved in an unimaginable way during the last two decades. In cellular wireless systems the so-called First Generation (1G) is already antiquated. The dominant Generations, which are nowadays in the limelight, are 2G, 2.5G and 3G. In Europe their representatives are GSM (Global System for Mobile Communication), GPRS (General Packet Radio Service) and UMTS (Universal Mobile Telecommunications System) respectively and they belong in the terrestrial wide area cellular systems. The circuit-switched GSM provides very slow data rates (9.6 – 14.4 kb/s) to satisfy the burst applications, even after the appliance of

 ISSN 0085-7130

High Speed Circuit Switched Data (HSCSD), it does not overcome the limit of 40 kb/s. Packet-switched networks, based on the access network of GSM with actual changes only in the core network (GPRS), appeared with the promise of higher bit rates (theoretically 172 kb/s), but in practice the maximum bit rate achieved is about 45 kb/s.

The UMTS access network follows a different approach, in comparison to GSM and GPRS, making the achievement of higher data rates more feasible. UMTS typically offers data rates up to 384 kb/s, even if in theory a 2 Mb/s transfer rate is possible. Nevertheless, the actual performance of UMTS has still to be verified during real operation conditions with heavy network loads.

On the other hand, there exist various wireless systems such as global area systems (e.g. satellite systems), wireless personal area networks (WPANs), which are formed by wireless communications between devices using technologies such as

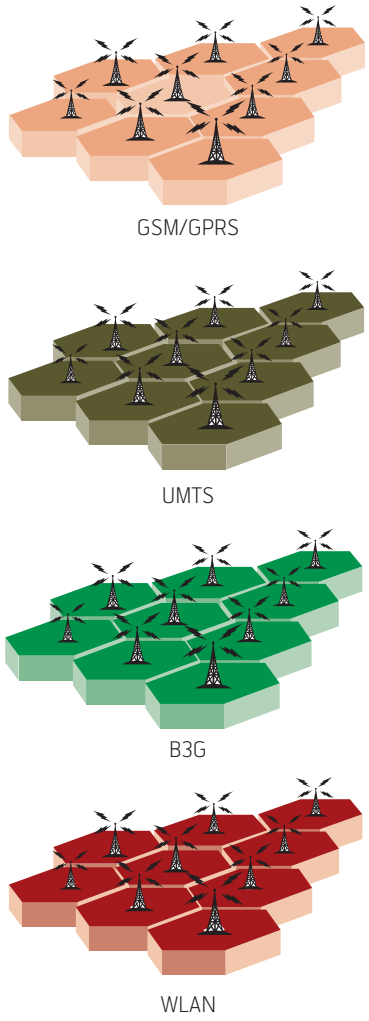


Figure 1 A diversified radio environment consisting of several access networks of one operator

Bluetooth [1] or IEEE 802.15 [2] and WLANs (e.g. IEEE 802.11a, IEEE 802.11b or HIPERLAN) [3][4][5]. These kinds of network provide incomparably high data rates. For example the 802.11b WLAN provides throughput up to 5 Mb/s, while the data rates in 802.11a can be up to over 25 Mb/s, with the perspective of reaching in the future the inconceivable, for today, limit of 155 Mb/s.

The co-existence of these technologies results in a heterogeneous set of wireless communications systems. Its active components are based on different theoretical backgrounds and are optimized for different ranges, exposing a great challenge for potential co-operation of all existing and emerging systems in a complementary way, in the concept of a 3GB (beyond 3rd Generation) system [6]. Such a hybrid 3GB system is examined in this paper, focusing on the efficient interworking of three different cellular access networks (GSM, GPRS, UMTS) with WLANs under a unified and hierarchical resource management model. At this point it has to be mentioned that the 3rd Generation Partnership Project (3GPP), the body that drives the standardization work for 3rd Generation mobile communications, has already foreseen the need for cooperation between WLANs and 3rd Generation systems and has published a feasibility study regarding their interworking [7].

Enhanced IP networking technologies are used to integrate current and future systems to a unified super-network, enabling a truly seamless mobile Internet, beyond the simple wireless access to the Internet, thus extending the scope of a monolithic system. The Internet Protocol version 6 (IPv6) does not only offer virtually unlimited address space, but also constitutes the technical foundation for evolutionary networking, offering also interoperability and interconnectivity with respect to security, mobility and Quality of Service (QoS) [8].

The major challenge in such a heterogeneous networking environment is to exploit the advantages of WLAN systems focusing on their seamless integration in composite radio environments. More specifically, a WLAN network is easy to deploy in hot-spot areas and can offer high data rates, thus achieving increased QoS, while the installation costs are limited. However, the subscriber should be able to roam between different access technologies seamlessly. In addition, it is a common research scenario to have several operators offering access to the same geographical area in a cooperative scheme. This might involve vertical-vertical handovers that occur when a user of one operator that makes use of resources of a specific RAT moves seamlessly to another operator by accessing resources of another type of RAT.

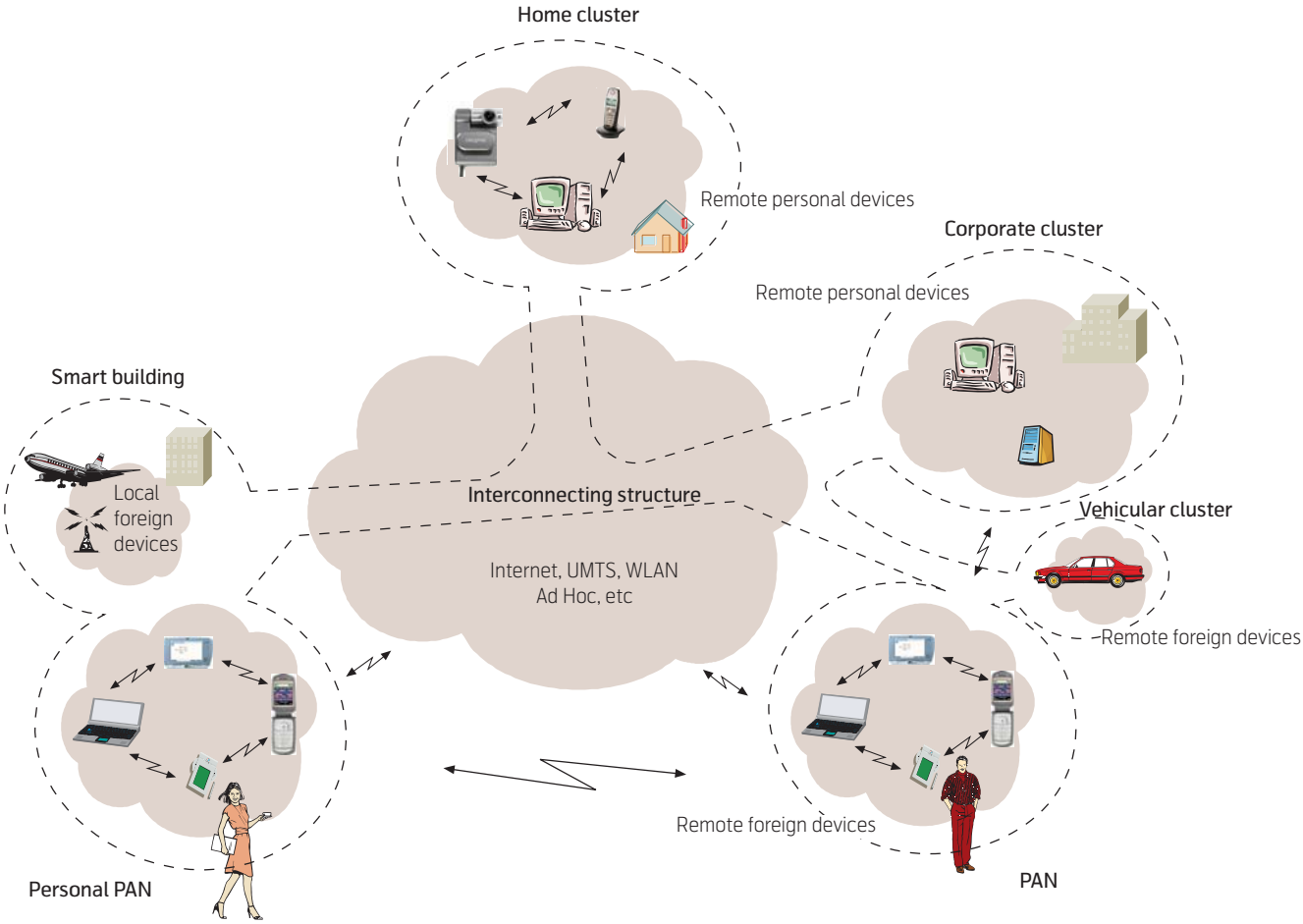


Figure 2 The MAGNET Beyond architecture for Personal Networks [9]

2.2 Personal Networks

There are several architectures of Personal Networks. The one described in this section is based on the MAGNET Beyond [9]. Figure 2 shows the system architecture from a high level point of view. In this scenario a user owns several clusters. Each of the clusters forms an ad hoc local area network. All clusters together form a global, always for the user accessible network.

The architecture is described in more detail in [10], while routing in the PN is explained in [11]. In order to be able to perform a risk assessment study, the system environment should be described, because threats depend on it. The geographical location is important, because a network, which has its elements far apart, will probably have more threats to face than a local network. Also, there probably will be more threats to a wireless network in a crowded city than in a wireless network in a rural area. Besides the location, the actors are very important. Who and/or what is able to interact with the system in what way?

The PN's location can be anywhere and everywhere. Because of the ubiquitous nature of the network, its components can find themselves almost everywhere, where the user wants them to be. This means the PN can be acted upon by almost everything and everyone you can think of. However, we can distinguish a few situations where the clusters of the PN can be located:

- at home (Home network)
- at work (Corporate network)
- in your car (Vehicle network)
- on body (Core PAN or PPAN)
- any other remote cluster

The clusters are interconnected via tunnels over wireless and/or over a wired interconnection infrastructure. This interconnecting structure is shared by lots of other PNs from different people. The MAC protocols used for the sharing of this structure are very important both from a Quality of Service as well as security perspective.

The primary actor in the PN is the owner of the network. Other actors can be network providers, service providers, others requesting services from the PN, anyone who the user sends a message or anyone who sends a message to the user, etc. In a specific use case the actors can be described in more detail.

PN is an omni-technological concept. In principle, every existing wireless or wired technology can be used and the network must be compatible with future technologies. The goal is that all these different technologies can interact seamlessly.

From the network requirements, architecture and environment, a list of network parts, which will require security attention, can be made. The requirements listed below are requirements found directly in the system requirements presented in [9] or derived from them or from the network architecture and environment.

- All wireless radio links should provide fair MAC schemes. Also wireless links can be weak, because potentially, anyone can pickup the signal, as it is broadcast in every direction.

- The first thing two nodes must do before they can establish a secure link, is to communicate with each other over an *insecure link*. This communication must establish a secured link. The way this insecure communication happens is very important for the system security, because a piconet should be joined by a hostile node.

- Only trusted nodes are allowed to have access to trusted data. This implies that different levels of trust have to be assigned to data.

- The packets will flow through the network using a multi-hop IP protocol. This multi-hop routing should be done securely. Basically every router is a potential access point for an attacker.

- All nodes should be able to automatically setup clusters and a PN. This means that this automatic setup should check the trustworthiness of other nodes and clusters, because there is no user to check it. However, another requirement is that the user should have a single GUI to manage all devices which are part of the PN. Should the user always be asked whether a node should be accepted, even after the system has found the node to be trustworthy?

- In case of handover, the target network should be trusted.

- Between the cluster connection points, which are at the gateway nodes, of a PAN to other clusters a secure link should be established.

- Remote cluster discovery and authentication should be done securely.

- The network's topology will change constantly due to mobility or entering and leaving nodes. This means that the roles of nodes may constantly change, for example the function of the gateway node may switch to other devices. Every time a change is happening the secure links will have to be established again. This means that every topology change is a potential moment of weakness, which attackers can take advantage of.

- End user's sensitive data stored in personal devices must be protected such that no disclosure of data is allowed without permission of the user.

- PN must provide a mechanism which hides private services from foreign nodes.

- Because Service Discovery (SD) is one of the main features of the PN it requires extra attention. There should be different trust levels for services, which define which data can be used for the service. Context Discovery is a special case of SD and contains personal information which should be kept confident.

- Every device which has special privileges, for example a master of a service or a gateway node, should have a power check. Before running out of power the device should send a message to the rest of the cluster that someone has to take-over the functionalities. This message should be sent, such that there is enough time for the cluster to relocate the functionalities to other nodes. If this is not done (thus, when the device loses power before take-over), is it then possible for another (hostile) device to take its place, without the rest of the network noticing? A usual take-over should be done by authentication of the two nodes: the old and the new one.

- Sleep mode is a power saving mode. This implies that the security measures running on a device in sleep mode can't be too heavy. And how do you prevent deprivation attacks?

- Communication with a foreign PN will require a good policy and model on trust.

3 Asset Identification

An asset can be a tangible item, a grade or level of service, staff or information. The question that should be answered is what needs to be protected. Following asset groups can be identified:

- Networking infrastructures and equipment
- Software

- Operator's reputation
- Confidentiality of information (protection of databases, voice calls, SMSes, etc.)
- Availability of Resources and Services
- Integrity of information

All the above assets are then presented in a structured tree, either directly or indirectly. Network components are presented as leafs in the tree, while reputation, churn, etc, are considered in the harm estimation. The tree has several levels, each one describing a network layer. For instance, Level 1 might be the physical layer that can be the air-interface and transmission network in a cellular system. In Level 2 we need to breakdown the further components of the air-interface and transmission network respectively. The same happens to Levels 3, 4 and all hierarchical levels that we initially decide to split the complete system. As we move towards the end of the tree we will end up with components such as databases, e.g. HLR, SMS servers that are network assets and might be vulnerable.

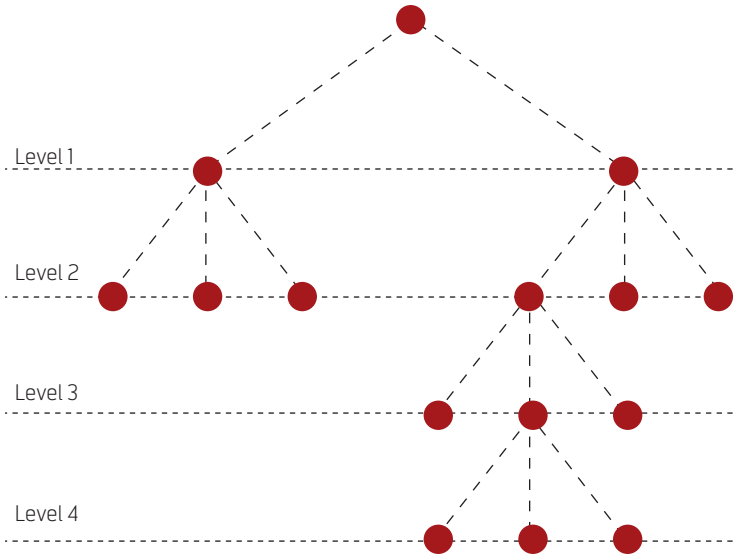


Figure 3 Network asset tree

4 Threat Likelihood and Harm Estimation

Multiple threats can be associated with one asset. Only those threats that could reasonably be expected to occur, or those that will result in identifiable consequences should be considered when performing the exercise of risk analysis. Source of the threat may be used in determining its probability.

Following rating convention is proposed:

- Negligible
- Very low (2-3 times every five years)
- Low (once every year or less)
- Medium (every six months or less)
- High (once every month or less)
- Very High (multiple times per month or less)
- Extreme (multiple times per day)

However, after the initial threat likelihood categorization, it is required to asses the probability in percentage rates referring to a given duration.

In Figure 4 one can see the tree with the network assets and a practical way to estimate the threat likelihood to have an attack in one of the network components, i.e. the leaf in Level 4. This might be a specific database. If the initial classification is *High*, i.e. once a month and we refer to a calendar year the probability of having such an incident is 3.29 %, assuming that the impact of an incident has practically one day duration. One of the major advantages of structuring the assets in tree infrastructures is that quite often the

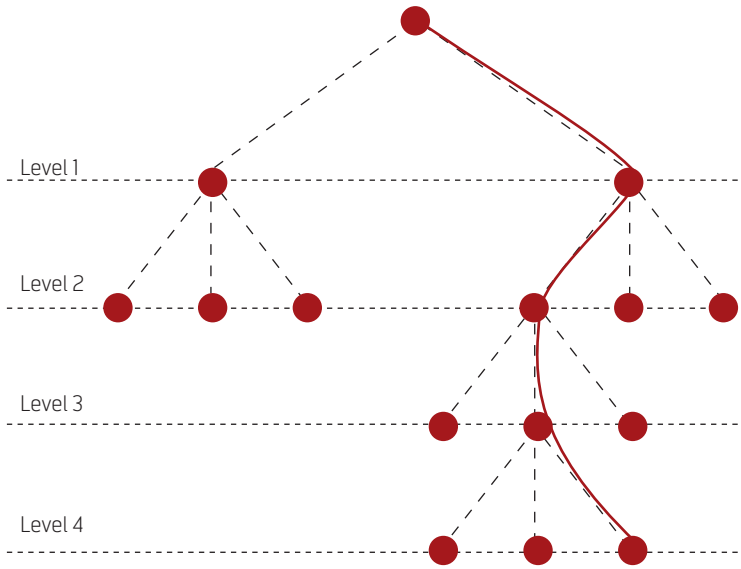


Figure 4 Path calculation

failure probability that depends on a shortcoming on another component can be calculated by multiplying failure probabilities of the above nodes. However, this is not applicable for non depending failures.

5 Risk Assessment Methodology

The risk assessment exercise is based on the following calculation. The goal is to estimate the profit loss of the operator from a probabilistic perspective so that the operator can calculate to what extent he can invest on security.

Following parameters are defined:

ISSN 0085-7130

K : total exposure (€)

f_i : Failure in asset i

k_i : exposure for failure in asset i

$p(f_i)$: probability of failure in asset i (%)

h_i : harm in asset i

$$K = \sum_i k_i \quad (1)$$

$$k_i = p(f_i) * h_i \quad (2)$$

$$K = \sum_i p(f_i) * h_i \quad (3)$$

Therefore, the operator needs to estimate the probability of having a failure in each network asset and estimate the related harm. It should be highlighted that failure probabilities and costs are only presented for 'leafs' that have no 'children' (additional branches below).

6 Example of Risk Analysis

In this section we analyze the examples of UMTS and the extensions to multi-operator diversified environment and PAN. In the examples we form the relevant trees and we calculate the threat likelihood and the harm cost.

6.1 Risk Analysis in UMTS Networks

Following example shows in a very simply way the methodology used to estimate the costs as a result of a failure in a UMTS network in a period of six months. Based on the initial study, i.e. analysis of data from the data-warehouse we have listed the approximate probabilities of failure in each of the nodes, as well as the recovery costs and other costs related to the incident.

Although the failure possibility of a node can be retrieved from a statistical datawarehouse of the operator it is always recommendable to perform this exercise by calculating the threats. In this example we will examine one of the nodes, namely HSS and we will estimate the cost of such harm (Table 1).

The above calculation should be carried for each of the elements presented in Figure 5, so that it is possible to make the calculations, as these listed in Table 1.

At this point it has to be highlighted that the costs are only indicative and they might significantly vary between operators vendors. By applying equation (3) for the above table we have:

$$K = \sum_{i=5,6,8,\ldots,13} p(f_i) * h_i = \sum_{i=5,6,8,\ldots,13} k_i = 348{,}000€$$

This can be translated as the costs that result from the failure of the network over a period of six months. Therefore, the operator should consider taking measures that will minimize the above amount and the costs of these measures should be obviously less.

6.2 Risk analysis in multi-operator diversified radio environment and PN-network

In the previous section we have seen a simplified application of this risk assessment methodology for UMTS environments. In the multi-operator diversified radio environment scenario, the first difference is that there should be a Level where the RAT technologies are presented. These can be for instance GSM/GPRS, WLAN, SB3G, etc. Under each of these nodes, the complete tree should be presented in the same way as for UMTS. Apart from the different RATs, the existence of one more Level on top is required to define the operator. Under each different operator that has an SLA with the serving operator, there is no need to have the whole hierarchy under-

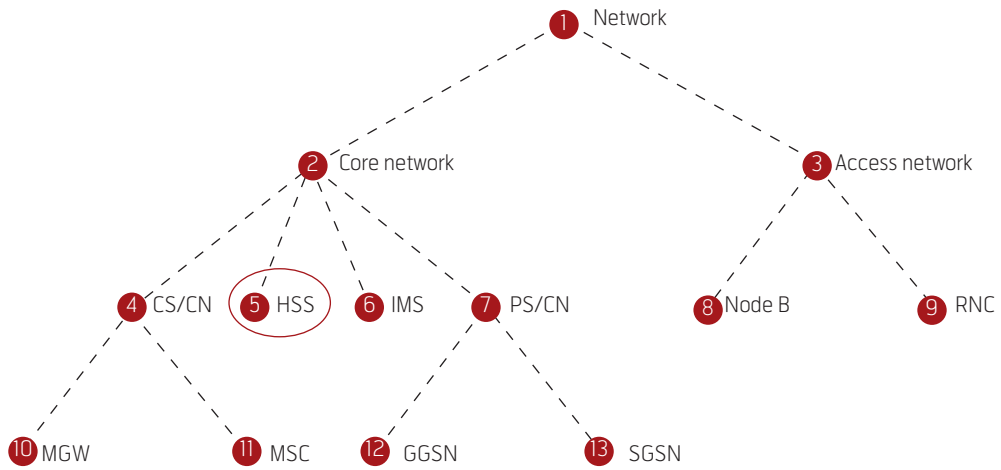


Figure 5 Risk analysis in a UMTS network

neath, just to know the probability of a total failure. To complete the methodology, apart from the calculations presented in 6.1, we should consider the failure probabilities from the other operators and other RATs, since the traffic that cannot be served due to a damage can be shifted to another network segment.

In the case of PN and PAN this is more complicated and the correct model that should be applied varies with the scenario. First we have to define the Personal PAN and the threats that result from vulnerabilities in the sensors and devices belonging to this group. Other nodes might be all other PANs that one user can have access to or be accessed by, since these might lead to attacks and damages. Finally, the underlying telecommunication networks should also be considered, since vulnerabilities there might result in severe attacks that should be calculated in the risk assessment.

Both scenarios will be examined in detail under the framework of the future research activities of the authors for risk assessment.

HSS threats	Probability	Cost	Weighted Cost
1) Unauthorized access to data	0.20 %	680,000€	136.000€
a) violation of confidentiality	-	-	-
b) eavesdropping traffic or control data	-	-	-
c) masquerading	-	-	-
d) traffic analysis	-	-	-
e) browsing, inference, etc.	-	-	-
2) Threats to integrity	0.10 %	196,000€	19,600€
3) Denial of service	0.15 %	80,000€	12,000€
a) intervention: jamming or protocol failures	-	-	-
b) resource exhaustion	-	-	-
c) abuse of services	-	-	-
4) Repudiation	0.15 %	94,000€	14,100€
5) Unauthorized access to services	0.08 %	750,000€	60,000€
6) Physical damage	0.32 %	1,745,000€	558,400€
Total	**1 %**	**-**	**800,000€**

Table 1 HSS treat estimation

7 Conclusions

In this paper we have proposed a simple methodology for risk assessment that can be applied in any network operator. The advantages and novelty of the method are the classification of all network assets into a tree and the calculation of the failure probability for a given time-frame. The harm estimation is based on separate studies that should be carried out, while at the end the end-result is the estimated cost that the operator will pay due to the network vulnerabilities. This is a good indication of the investments that an operator should make in order to minimize the failure probability and increase network performance. The method is accurate since it can be validated with existing data and well structured, as not only the assets, but also the threats are classified and weighted.

In the future, this methodology will be implemented in a simulator that will be fed with data from a data warehouse.

i	*f(i)*	$p(f_i)$	*h(i)*	*k(i)*
1	Network	-	-	-
2	Core Network	-	-	-
3	Access Network	-	-	-
4	CS-CN	-	-	-
5	HSS	1 %	800,000€	8,000€
6	IMS	5 %	2,000,000€	100,000€
7	PS-CN	-	-	-
8	Node B	3 %	480,000€	14,400€
9	RNC	1 %	3,000,000€	30,000€
10	MGW	2 %	1,200,000€	24,000€
11	MSC	3 %	3,600,000€	108,000€
12	GGSN	2 %	1,600,000€	32,000€
13	SGSN	2 %	1,600,000€	32,000€

Table 2 Risk Assessment Table

References

1 The Bluetooth Special Interest Group (SIG). *Specification of the bluetooth system, version 1.1*. 2001. Available at http://www.bluetooth.org

2 Roberts, G. *IEEE 802.15 Overview of WG and Task Groups*. Available at http://grouper.ieee.org/groups/802/15/pub/Tutorials.html

3 IEEE. *Supplement To IEEE Standard For Information Technology- Telecommunications And Information Exchange Between Systems- Local And Metropolitan Area Networks- Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications: Higher-speed Physical Layer Extension In The 2.4 GHz Band*. 2000. (IEEE Standard 802.11b-1999) (ISBN 0-7381-1811-7)

4 IEEE. *Archived – Supplement to IEEE standard for information technology telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: high-speed physical layer in the 5 GHz band*. 1999. (IEEE Standard 802.11a-1999) (ISBN 0-7381-1809-5)

5 ETSI. Broadband Radio Access Networks (BRAN), *HIPERLAN Type 2, System Overview*. ETSI TR 101.683 (VI.1.2), 2000.

6 Tselikas, N et al. Architectural framework for resource management optimisation over heterogeneous wireless networks. In: *Proc. ITCom (Information Technologies and Communications) SPIE conference*, Orlando, Florida, USA, 7-11 September 2003.

7 3GPP, TSG Services and Systems Aspsects. *Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking*. 3GPP TR 22.934 (V6.2.0), 2003.

8 Stallings, W. IPv6: The New Internet Protocol. *IEEE Communications Magazine*, July 1996, 96–108.

9 All Work Packages. *MAGNET System Specification*. IST-MAGNET Beyond, Deliverable 1.1.1, 2006.

10 Olsen, R et al. *Service, Resource and Context Discovery system specification*. IST-MAGNET, Deliverable 2.2.3, 2005.

11 Jacobsson, M et al. *Refined Architectures and Protocols for PN Ad-hoc Self-configuration, Interworking, Routing and Mobility Management.* IST-MAGNET, Deliverable 2.4.3, 2005.

12 Australian Communications-Electronic Security Instruction 33 (ASCI 33). *Handbook 3 – Risk Management*, version 1.0. 2004.

13 Australian Government, Department of Defence. *Defence Signals Directorate*. http://www.dsd.gov.au/

Sofoklis A. Kyriazakos studied Electrical Engineering in RWTH Aachen and specialized in Wireless Systems in the Chair of Communications Networks. He then moved to the Telecommunications Laboratory of the National Technical University of Athens (NTUA), where he received his PhD in the area of RRM in Wireless Networks and MBA in Techno-economic Systems. He his currently working as Assistant Professor at Aalborg University, Denmark and his research areas are RRM in Systems Beyond 3G, Risk Analysis, Traffic Estimation and Business Modeling. He has performed a large number of publications in journals, book chapters, conferences and standardization bodies.

email: sk@kom.aau.dk

Neeli Rashmi Prasad is Associate Professor and Head of Wireless Security and Sensor Networks Lab, part of Wireless Network including Embedded systems Group (WING), Center for TeleInfrastruktur (CTIF), Aalborg University, Denmark. She received her PhD from the University of Rome, Italy, in the field of "adaptive security for wireless heterogeneous networks" in 2004 and MSc (Ir.) degree in Electrical Engineering from Delft University of Technology, The Netherlands, in the field of "Indoor Wireless Communications using Slotted ISMA Protocols" in 1997. She joined Libertel (now Vodafone NL), Maastricht, The Netherlands in 1997. From 1998 to 2001 she worked as Systems Architect for Wireless LANs in Wireless Communications and Networking Division of Lucent Technologies (now Agere Systems), The Netherlands. From 2001 to 2003 she was with T-Mobile Netherlands as Senior Architect for Core Network Group. From 2003 to 2004 she was Senior Research Manager at PCOM:I^3, Aalborg, Denmark. Neeli Prasad has published widely and has supervised several Masters and PhD students.

email: np@kom.aau.dk

Coexistence Concept for the Implementation of LDR/HDR WPAN Multimode Devices

MAURO DE SANCTIS, JOHN GERRITS, JULIAN PÉREZ VILA

Mauro De Sanctis is Assistant Professor at Department of Electronics Engineering, University of Roma "Tor Vergata", Italy

John Gerrits is with CSEM S.A. in Neuchatel, Switzerland

Julián Pérez Vila is Research and Development Engineer with Telefónica I+D, Spain

This paper defines the guidelines for the implementation of multimodal devices with Frequency Modulation Ultra Wide Band (FM-UWB) and Multi Carrier Spread Spectrum (MC-SS) air interfaces (AIs) for short range Low Data Rate (LDR) and High Data Rate (HDR) connections. Several novel scenarios have been proposed which require the simultaneous exploitation of LDR and HDR Wireless Personal Area Network (WPAN) connections. The possibility of performance degradation when one AI is transmitting and the other one is receiving is discussed. It has been found that MC-SS transmission can impact the FM-UWB reception. Furthermore, an overview of collaborative and non-collaborative coexistence mechanisms is provided. Finally, the architecture that allows the efficient exploitation of the two AIs in one device is proposed.

1 Introduction

System scalability deals with the exploitation of the most appropriate access network/technology. The necessity for the user terminal to transmit and receive towards and from different radio access networks requires a certain level of reconfigurability of the radio interface in order to allow the exploitation of different access technologies (e.g. MC-SS, FM-UWB, etc.) and different standards (e.g. IEEE 802.11a, IEEE 802.15.3 or IEEE 802.15.4).

Most of the past work on multimode terminals focused on the integration of Wireless Local Area Network (WLAN) and Cellular Wide Area Network (WAN) network terminals [1]. In addition to this kind of integration, also the different network access standards defined by the IEEE 802 working groups can be integrated. IEEE 802 standards define only the physical layer (PHY) and Medium Access Control (MAC) layer of a given interface. For end-to-end services and their architectural view of the network, other core network elements have to be defined. An interesting research topic concerns the development of multimodal WPAN devices capable of exploiting simultaneously the IEEE 802.15.3-based HDR interface and the IEEE 802.15.4-based LDR interface [2]. This is a new concept of cooperation between access networks/technologies since there is not only a swap of access networks dictated by coverage issues or transmission rate shift, but it is envisioned a sort of cooperation aimed to enhance: QoS provisioning, power and/or bandwidth efficiency, reliability and availability. We aim to apply this concept to the multimode WPAN devices where the PHY transmission bit rate of the LDR interface ranges from a few bits per second (b/s) to 100 kb/s and the transmission bit rate of the HDR interface ranging from 28.87 Mb/s to 130 Mb/s.

While in such multimode terminals there exists a gap in the transmission bit rate, the features of the IEEE 802.15.3 based MAC allow to decrease the system throughput to cover this gap. The final result is the availability of an effectively integrated dual-mode WPAN device that provides a very large range of transmission bit rates seamlessly and transparently to the user.

The aim of this paper is to define the guidelines for the implementation of dual mode LDR/HDR WPAN devices. The definition of guidelines encompass:

- Discussion of the need to develop dual mode LDR/HDR devices by identifying several multimode application scenarios;
- Analysis of the interference between the LDR and HDR air interfaces of reference;
- Analysis of coexistence mechanisms for the mitigation of the interference within a device;
- Proposal of a protocol architecture which effectively exploits the dual mode capability of the device.

In order to introduce and discuss such guidelines, we have organised the paper as follows. In Section 2 several scenarios for multimode LDR/HDR WPAN devices are proposed. Section 3 analyses the interference between the two proposed AIs. In Section 4 coexistence mechanisms are discussed, while in Section 5 the protocol architecture which enables multimode LDR/HDR WPAN devices is proposed. Finally, conclusions are drawn in Section 6.

ISSN 0085-7130

LDR applications	HDR applications
Wireless mouse or keyboard connection	Video streaming
Wireless printer connection	Tele conferencing
Low quality audio/voice transmission	File transfer
Data sensor transmission	Web browsing
Notebook or PDA synchronization with desktop computer	Mobile gaming

Table 1 List of applications for LDR and HDR AIs

2 Multimode Application Scenarios

In this section we will define the application scenarios where both LDR and HDR interfaces are used. The simultaneous exploitation of the two air interfaces within one multimode device can be dictated by *user needs, scenario requirements* and/or by *efficiency improvement*. Simultaneous exploitation of air interfaces does not mean that they simultaneously transmit and/or receive, but it means that both interfaces are powered on, have established a connection and have data to transmit or receive.

User needs can lead to multimode application scenarios when both LDR and HDR applications are running on the same multimode device. This is the case where the user device is connected in LDR and HDR transmission with several other wireless devices (mouse, headphone, printer, sensors, mobile game player, file repository, etc.). In this case the data flow of one single connection is independent of each other.

On the other hand, *scenario requirements* can lead to the need for a multimode device (i.e. translational bridge) capable of forwarding data received from an LDR (HDR) connection to a HDR (LDR) connection. In this case the data that flow through the HDR (LDR) connection depend on the data that flow through the LDR (HDR) connection.

Finally, when one of the two AIs is experiencing bad transmission conditions the user satisfaction can be enhanced by the *efficient exploitation* of the multimode capability of the devices. The mentioned bad conditions can be raised by: interference with other wireless technologies (e.g. WLAN), buffer load, remaining battery energy, coverage.

There are five different scenarios that require the simultaneous operation of the LDR and HDR air interfaces. In the following subsections, the five scenarios are outlined and the main features of the multimode application scenarios are listed in Table 2.

2.1 Multimode Scenario for Multiple Traffic – Scenario no. 1

Accounting for the application requirements in terms of minimum data rate, we can identify several categories of applications for HDR and LDR AIs respectively. Typical applications that require LDR and HDR AIs are listed in Table 1.

The simultaneous exploitation of different applications can be dictated by the user needs. An example of this multimode scenario is shown in Figure 1 where the central notebook is provided with the multimode LDR/HDR AIs and is connected with several devices through LDR and HDR connections. Since each connection is independent of each other, this type of scenario does not require the interoperability and/or interworking between LDR and HDR AIs for data transmission. However, it could require the cooperation of the two AIs for the management of the coexistence in terms of interference avoidance.

2.2 Multimode Scenario for Aggregate Traffic – Scenario no. 2

This scenario is characterised by the exploitation of many LDR connections and one HDR connection where the aggregation of the LDR connections flows. The transmission links of the multimode scenario are bidirectional; however, in the following we are going to identify the direction of transmission of the useful data.

Scenario no.	Type of scenario	Number of devices	Level of complexity	Interoperability requirements
1	Generated by user needs	many	low	none
2	Generated by efficiency improvement and/or scenario requirements	many	medium/high	yes
3	Generated by efficiency improvement	2 or more	medium/high	yes
4	Generated by efficiency improvement	2	medium/high	yes
5	Generated by efficiency improvement	2	medium/high	yes

Table 2 List of features of multimode application scenarios

ISSN 0085-7130 ©Telenor ASA 2007

In the first example of this scenario (see Figure 2) the multimode terminal DEV1 collects data from several LDR devices/sensors (S1-SN) by using the FM-UWB interface and transmits an aggregate HDR data traffic (e.g. data-sensors' traffic) to a single mode terminal DEV2 (e.g. a data base) by using the MC-SS air interface.

In the second example of this scenario (see Figure 3) the direction of the transmission is the opposite with respect to the previous example since the objective of the transmission is to deliver data to different devices; when the data to be delivered are the same for all the devices S1-SN, this example can be considered as a broadcasting scenario.

In this second case, the function of the multimode device DEV1 is to disaggregate the traffic sent by the single mode device DEV2.

The aggregate traffic scenario is meaningful when direct connections between DEV2 and S1-SN cannot be established for different reasons:

- DEV2 is a HDR single mode device and S1-SN are LDR single mode devices;
- DEV2 and S1-SN are out of coverage;
- Privacy/security motivation does not allow to connect DEV2 with S1-SN.

Following these considerations, the multimode scenario for aggregate traffic is generated by user needs or efficiency improvement. In this scenario, the multimode terminal DEV1 acts as a translational bridge which operates above the MAC sublayer and is capable of converting IEEE 802.15.4 MAC frames into IEEE 802.15.3 MAC frames and vice versa.

2.3 Multimode Scenario for LDR Applications – Scenario no. 3

In this scenario, depicted in Figure 4, the requirement of the connection between DEV1 and DEV2 in terms of data rate is less than 100 kb/s; since both air interfaces can satisfy this requirement and both HDR and LDR connections can be established, an interoperable parallel link can be set up where the data can be delivered by using the momentarily available or momentarily most suited AI. In this case, the multimode terminal (DEV1) acts as a dynamic switch, routing data coming from the application layer to the most suited interface. The most suited AI can be identified on the basis of interference level with other radio technologies (e.g. WLAN), error rate, buffer load, etc. The coverage area of the LDR and HDR radio technologies overlaps and hence their usage

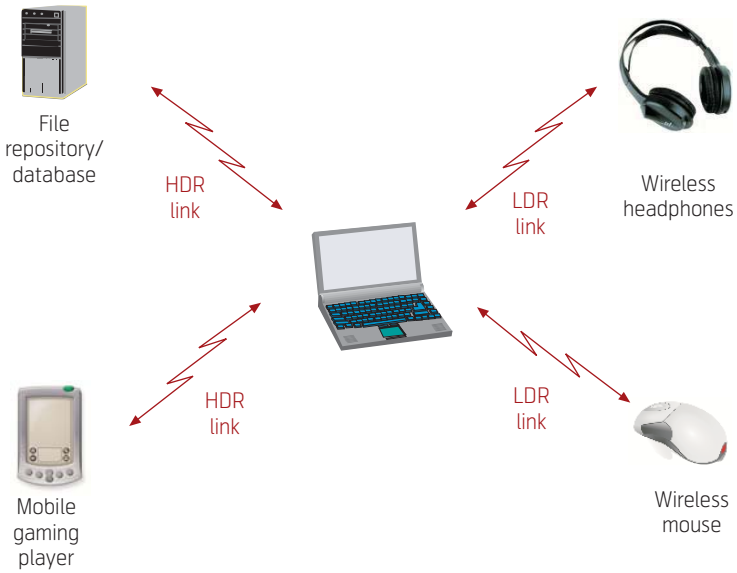


Figure 1 Multimode scenario for multiple traffic

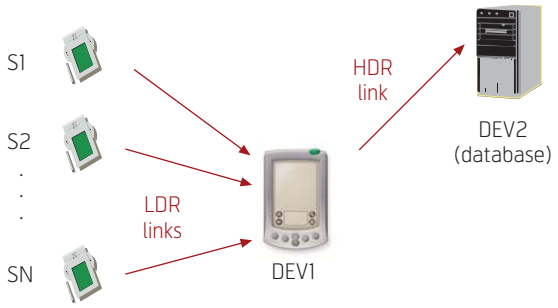


Figure 2 Multimode scenario for aggregate traffic (aggregation of traffic)

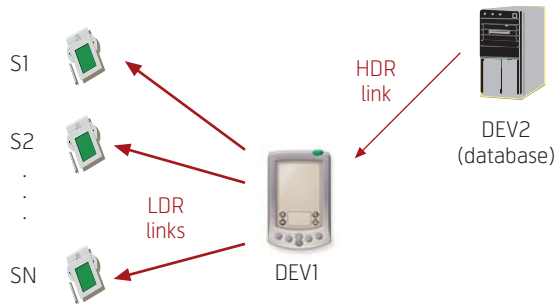


Figure 3 Multimode scenario for aggregate traffic (disaggregation of traffic)

can be combined in order to obtain the best possible connection according to a certain criterion [3] in order to enhance the efficiency of the connection between DEV1 and DEV2.

2.4 Multimode Scenario for HDR Applications – Scenario no. 4

When the proper MC-SS-based interface for the running HDR application (see Table 1) cannot be momentarily used because of interference with other technologies

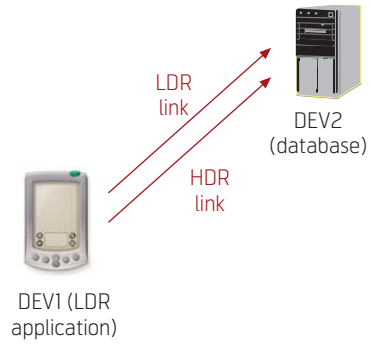


Figure 4 Multimode scenario for LDR applications

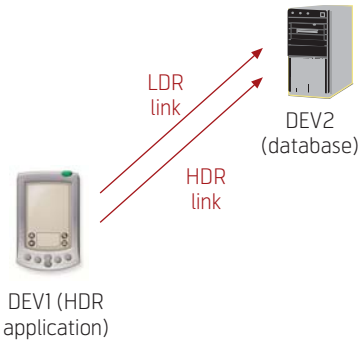


Figure 5 Multimode scenario for HDR applications

(with e.g. WLAN), remaining battery energy, buffer load or coverage issues, the possibility of using two transmission technologies allow to combat the momentary issue and to improve some efficiency metrics.

The difference between this scenario, depicted in Figure 5, and the previous one is due to the data rate transmission requirements of the running application. In scenario no. 3 the data rate transmission requirements of the running application is lower than 100 kb/s, while in scenario no. 4 the data rate transmission requirements of the running application is higher than 100 kb/s. In scenario no. 3 the need to establish an interoperable parallel link is needed in order to improve the bandwidth efficiency of the system, while scenario no. 4 improves the power efficiency of the system.

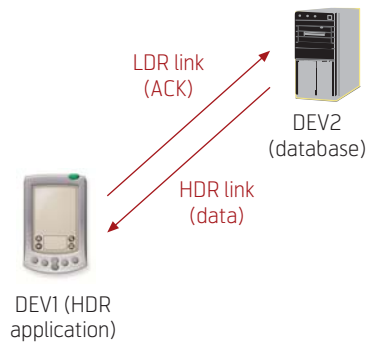


Figure 6 Multimode scenario for HDR asymmetric transmission

Both scenarios no. 3 and 4 are able to counteract the interference that can be generated by other radio technologies over one of the two AIs.

2.5 Multimode Scenario for HDR Asymmetric Transmissions – Scenario no. 5

In this scenario (see Figure 6) a HDR application with asymmetric bandwidth requirement (e.g. a file transfer) is running on the multimode device (DEV1) which is connected to a multimode device (DEV2) through both LDR and HDR links. In the case of reliable data transfer by using TCP at the transport layer the transmission is characterised by a large amount of useful data transfer with high bandwidth requirements on the forward direction (from DEV2 to DEV1) and a small amount of data transfer (acknowledgements) with low delay requirements on the reverse direction (from DEV1 to DEV2).

An efficient exploitation of the dual connection is the use of the bandwidth efficient HDR interface for the transmission of data and the use of the energy efficient LDR interface for the transmission of the ACKs. This scheme of transmission allows to avoid the inefficient use of time slot of the HDR connection for the transmission of small size ACKs and increase the energy efficiency of the system by using the power efficient LDR AI for the transmission of ACKs.

Even if the possiblity of simultaneously using LDR and HDR AIs has already been addressed in the past, scenarios no. 3, 4 and 5 propose novel efficient methods of exploiting dual mode devices.

3 Interference Between FM-UWB and MC-SS

3.1 WPAN Air Interfaces

Although the MAC layer of the IEEE 802.15.3 standard for HDR WPAN and the MAC layer of the IEEE 802.15.4 standard for LDR WPAN are well established, the physical layers are still rather undefined. Multi Band Orthogonal Frequency Division Multiplexing (MB-OFDM) and Direct Sequence Ultra Wide Band (DS-UWB) are the main candidates for the physical layer of the HDR standard, while Direct Sequence Spread Spectrum (DS-SS), Chirp Spread Spectrum (CSS) and Impulse Radio Ultra Wide Band (IR-UWB) are the main candidates for the physical layer of the LDR standard.

The act of defining the two air interfaces for HDR and LDR WPAN has been fairly uncoordinated, resulting in coexistence issues of the proposed air interfaces when operating in the same environment.

We have selected two air interfaces for LDR and HDR WPAN with the aim of minimizing system complexity, energy consumption and coexistence issues. In the following we describe the selected air interfaces [2].

LDR Air Interface

The LDR air interface uses FM-UWB techniques and is a scalable air interface technology aimed at short-range (< 10 m) LDR (< 100 kb/s) applications, which is characterized by a low power consumption and ease-of-implementation on an integrated circuit [4]. FM-UWB uses double FM; a low modulation index digital Frequency Shift Keying (FSK) is followed by high modulation index analogue FM to create a constant envelope UWB signal. The estimated power consumption is up to 3.5 mW for the transmitter and 7.5 mW for the low-complexity receiver. Though Frequency Division Multiple Access (FDMA) techniques at sub-carrier level can be exploited to accommodate multiple users in extremely simple devices, the PHY is mainly targeted to operate with the IEEE 802.15.4 MAC, in which Time Division Multiple Access (TDMA) is applied.

HDR Air Interface

For the HDR system, an Orthogonal Frequency Division Multiplexing (OFDM) transmission based PHY with spreading in frequency domain is developed, which operates in the 5.2 GHz bands allocated to Wireless Access Systems (WASs). The maximum data rate without MIMO is approximately 130 Mb/s and the system bandwidth is 40 MHz; however an alternative solution with 20 MHz is also specified to ensure compliance with regulatory bodies. Though spreading in frequency domain is applied, it is not used as multiple access scheme, thus resulting in a Multi Carrier Spread Spectrum (MC-SS) transmission scheme [5]. The chosen TDMA being compliant with the foreseen IEEE 802.15.3 MAC scheme avoids multiple access interference. The objective of the frequency domain spreading is to exploit diversity and to average out interference from other systems. Further, the number of spreading codes can be varied resulting in increased flexibility and scalability.

Interference Between LDR and HDR AIs

Table 3 shows the main parameters of the selected LDR and HDR air interfaces. The interference between FM-UWB and MC-SS is an important issue. The major differences are the transmission power (34 dB of difference) and signal bandwidth. Signal attenuation as a function of distance is almost equal,

Parameter	FM-UWB	MC-SS
Transmit power	-14 dBm	+20 dBm
RF centre frequency	4.5 GHz	5.25 GHz
RF signal bandwidth	500 MHz	36 MHz
RF signal envelope	Constant	Strongly varying
Predominant Modulation	FM	AM
Path loss @ 1 m	45 dB	46.5 dB

Table 3 Characteristics of FM-UWB and MC-SS air interface

since the two operating frequencies are relatively close to each other. Figure 7 shows the received power at a distance *d* for free space propagation conditions for both air interfaces.

The situation becomes rather clear after inspection of this Figure. The maximum received signal from the FM-UWB transmitter at 10 cm distance is the same as the level received 5 m away from the MC-SS transmitter. It is worth noting that the interference between the proposed FM-UWB and MC-SS systems can be classified as out-of-band interference. Interference from MC-SS to the FM-UWB system is very likely to happen and therefore it is the major issue of our interference investigations.

In the next subsection we will investigate which Signal-to-Interference Ratio (SIR) can be tolerated and what would be required in terms of interference mitigation for various scenarios like collocated (0.1 – 10 m distance) and remote (> 10 m) systems.

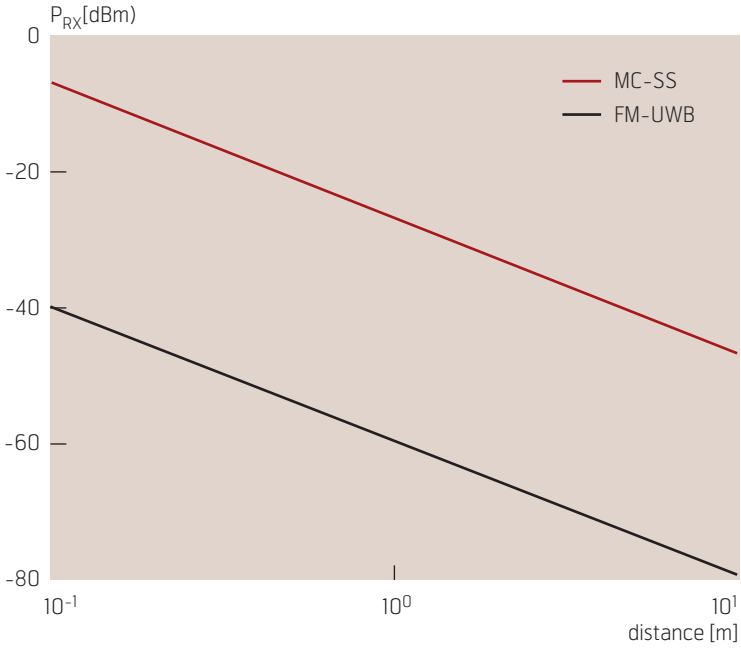


Figure 7 Received power as a function of distance for FM-UWB and MC-SS

ISSN 0085-7130

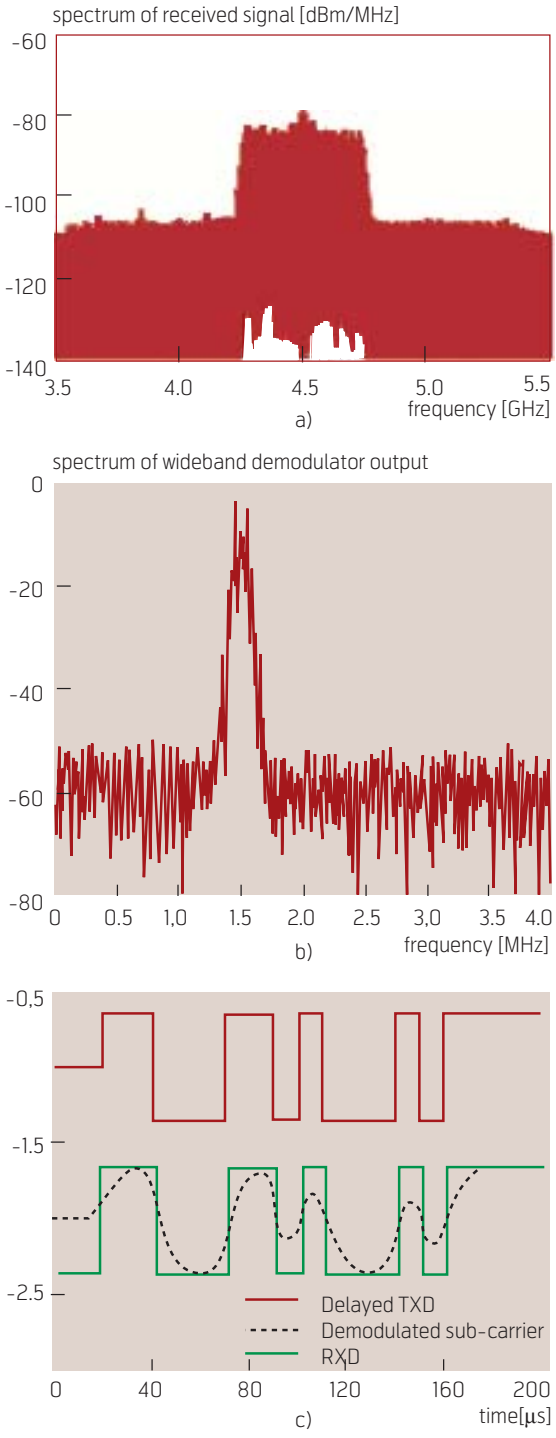


Figure 8 AWGN case with SNR = 10 dB, a) RF input signal, b) after wideband FM demodulator, c) comparison of transmitted and received data

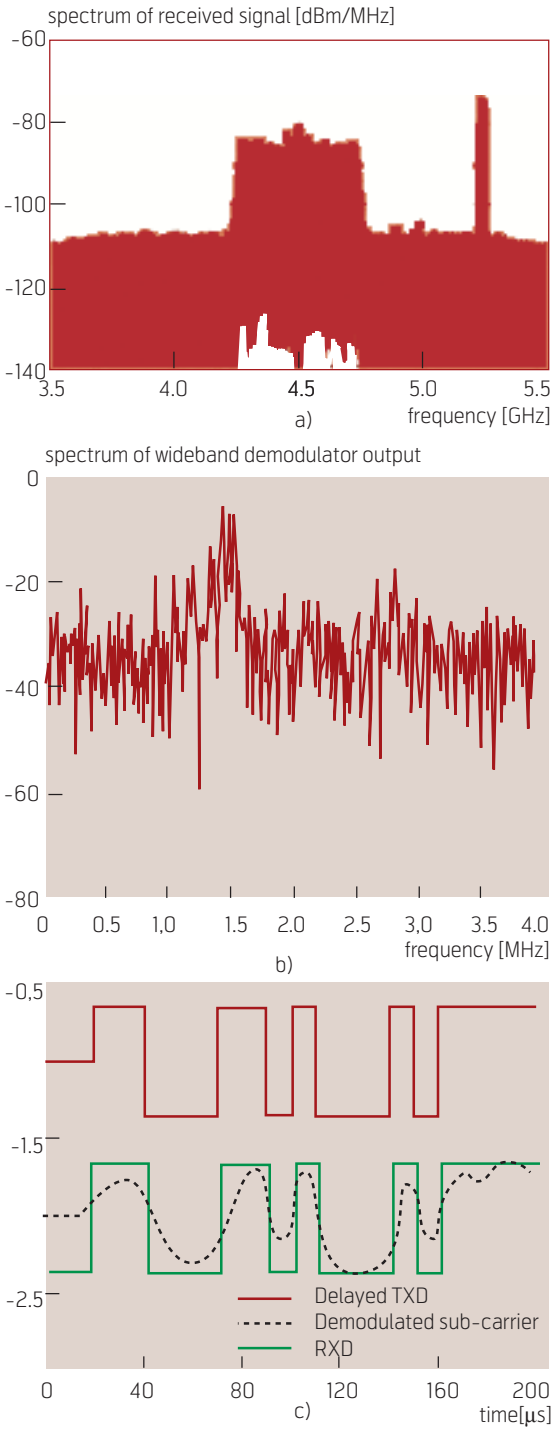


Figure 9 MC-SS interference with SIR = 0 dB, a) RF input signal, b) after wideband FM demodulator, c) comparison of transmitted and received data

3.2 Influence of MC-SS on FM-UWB

MC-SS signals like all multi-carrier signals show relatively strong envelope variations. MC-SS signals are demodulated by the wideband FM demodulator. Both the AM and FM components yield a signal at the demodulator output. The part of the demodulated MC-SS signal falling within the sub-carrier bandwidth of the demodulated FM-UWB signal determines the sub-carrier SIR degradation.

It was found that a SIR up to -2 dB (interferer 2 dB stronger than wanted signal) can be dealt with without significant BER degradation (BER < $1x10^{-3}$). Figures 8, 9 and 10 show three situations:

- FM-UWB with AWGN SNR = 10 dB
- FM-UWB plus MC-SS, SIR = 0 dB
- FM-UWB plus MC-SS, SIR = -6 dB

ISSN 0085-7130 ©Telenor ASA 2007

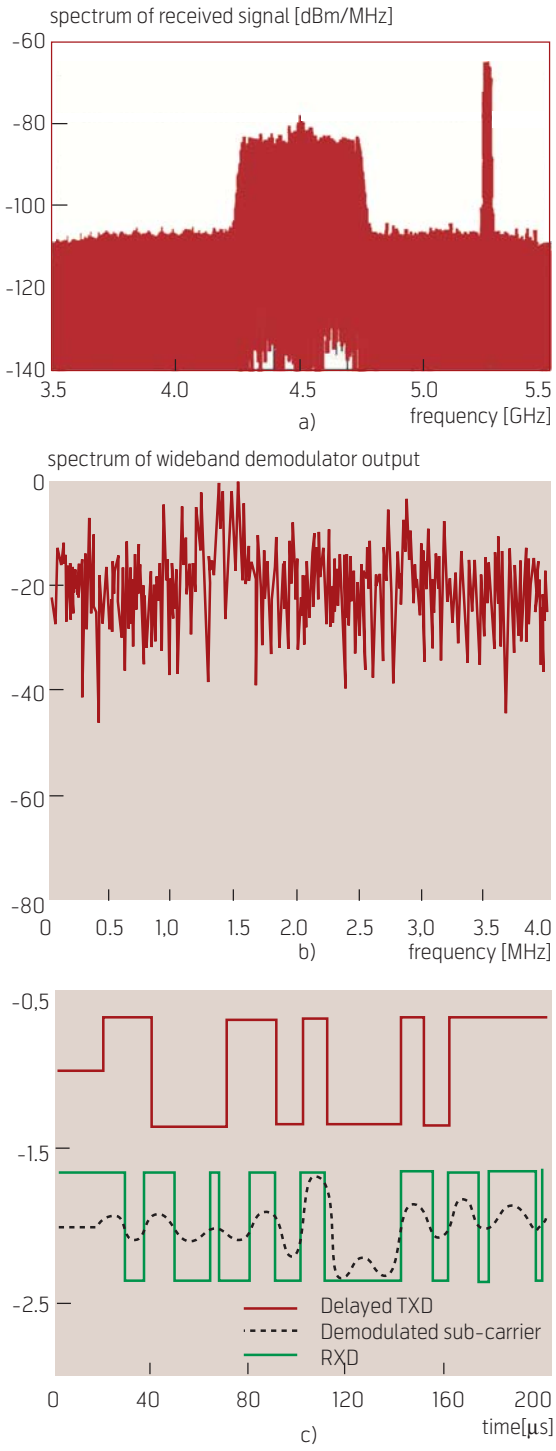


Figure 10 MC-SS interference with SIR = -6 dB, a) RF input signal, b) after wideband FM demodulator, c) comparison of transmitted and received data

For each case the following three sub-Figures are shown:

a) the spectrum of the received RF signal showing the FM-UWB signal plus interference;

b) part of the spectrum after the wideband FM demodulator containing the FSK sub-carrier and noise;

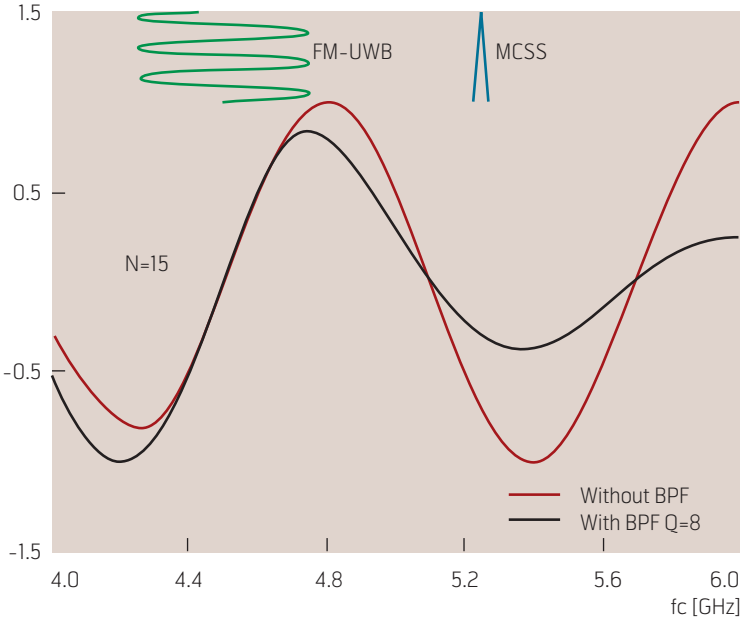


Figure 11 Transfer function of the wideband FM demodulator, with and without LNA BPF

c) time domain view of the delayed transmitted data TXD, the lowpass filtered FM demodulated sub-carrier signal, and its hard-limited version: the received data RXD.

These figures illustrate how the received data is affected by the interference. For the sake of clarity, only a period of 200 µs (20 bits) is shown.

At SIR = 0 dB, the FM-UWB 100 kbit/s system easily survives with low BER. However, the lowpass filtered sub-carrier demodulator signal (dotted black) starts to show visible distortion.

At SIR = -6 dB (interferer 6 dB stronger than wanted signal) the sub-carrier SNR has become too low for demodulation.

3.2.1 Physical Layer Interference Mitigation Techniques

The wideband FM demodulator is sensitive to both frequency and envelope variations of the signal [4]. The red line in Figure 11 shows its transfer function for a delay time t equal to $N = 15$ times one quarter period of the centre frequency, i.e. 833 ps. Since the delay line demodulator has no bandwidth limitation, MC-SS signals at 5.25 GHz will also be demodulated. By limiting the demodulator input signal bandwidth, ideally to 4.2 – 4.8 GHz, signals outside that bandwidth will be attenuated and the interference will be lowered. The black line in Figure 11 shows an example of a simple bandpass filter implemented in the LNA. The following three paragraphs address filtering that can be achieved inside the FM-UWB

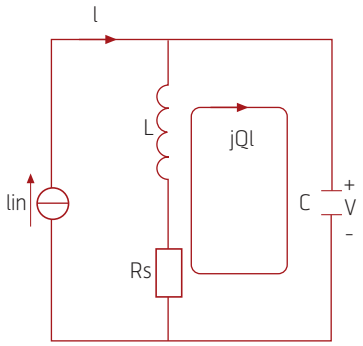


Figure 12 Parallel resonant circuit

receiver as well as by using external filters and also by lowering the antenna efficiency at 5.25 GHz.

LNA Filtering

The Low Noise Amplifier (LNA) can be exploited to implement additional bandpass filtering around the FM-UWB centre frequency of 4.5 GHz, e.g. by using a parallel resonant load in the LNA as shown in Figure 12.

With $p = j\omega$, its transfer function in the frequency domain is given by:

$$H = H_0 \frac{\frac{\omega_0}{Q}p}{p^2 + \frac{\omega_0}{Q}p + \omega_0^2} = \frac{H_0}{1 + jQ\frac{\omega}{\omega_0} - jQ\frac{\omega_0}{\omega}}$$

By introducing a variable named detuning ν defined as:

$$\nu = \frac{\omega}{\omega_0} - \frac{\omega_0}{\omega} \approx 2\frac{\omega - \omega_0}{\omega_0} = 2\frac{\Delta\omega}{\omega_0}$$

The resonator transfer can now be rewritten as:

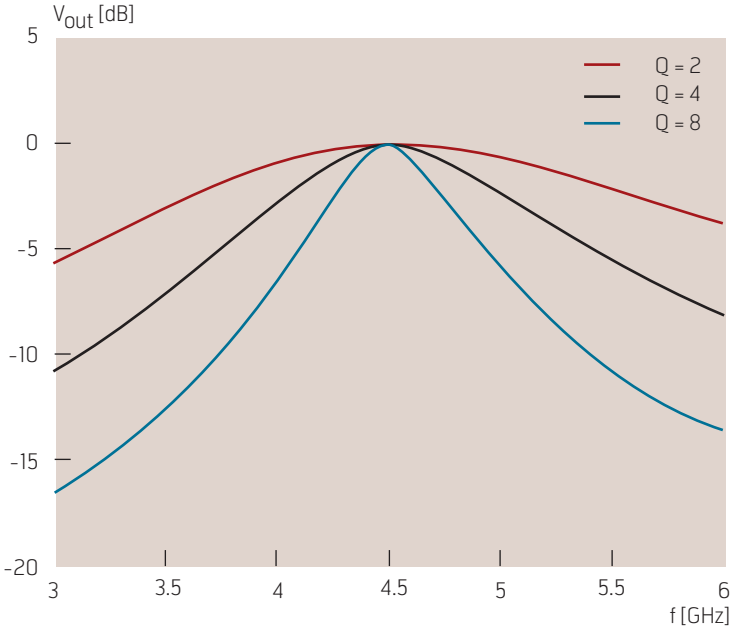


Figure 13 Normalised resonator transfer function with Q as parameter

$$H = \frac{H_0}{1 + jQ\nu}$$

This 2nd order resonator is fully characterised by its resonant frequency ω_0, quality factor Q and the maximum value of its transfer function H_0 which has the dimension of impedance for the circuit shown in Figure 13. The impedance of the parallel resonant circuit is given by:

$$Z = \frac{V}{I} = \frac{R_p}{1 + j\omega R_p C - j\omega\frac{R_p}{\omega L}}$$

$$= \frac{R_p}{1 + jQ\frac{\omega}{\omega_0} - jQ\frac{\omega_0}{\omega}} = \frac{R_p}{1 + jQ\nu}$$

Its magnitude and phase are given by:

$$|Z| = \frac{R_p}{\sqrt{1 + Q^2\nu^2}}$$

The resonant frequency and quality factor are given by:

$$\omega_0 = \frac{1}{\sqrt{LC}}$$

$$Q = \frac{\omega_0 L}{R_s} = \frac{R_p}{\omega_0 L} = R_p\sqrt{\frac{C}{L}}$$

Figure 13 shows the magnitude of the normalised transfer function for various Q values. Clearly, with increasing Q, out-of-band signals are more attenuated. A practical limit for the quality factor is the bandwidth of the FM-UWB signal which needs to fit within the filter's bandwidth. Therefore, Q values higher than 8 are not recommended. This yields 7 dB of attenuation at 5.25 GHz, not enormous, however, it comes for free.

External Filtering

The attenuation of the MC-SS signal can be increased by using an external filter. Figure 14 shows the measured transfer function of a commercial filter available from Taiyo Yuden. This filter as an insertion loss of 1 dB at 4.5 GHz and an attenuation of 23 dB at 5.25 GHz. The filter size is small and it can be easily placed between antenna and FM-UWB receiver.

Filtering by the Antenna

Antennas can be designed to have notches in their frequency characteristic. In [6] a CPW fed planar UWB antenna of small size and having a frequency band notch feature at the MC-SS frequency band (5.25 GHz) is presented. Figure 15 shows the antenna. The slot (the smile) in the upper part of the metallisation lowers radiation efficiency around 5.25 GHz. The authors claim attenuation values between 5 and 10 dB at 5.25 GHz.

3.2.2 Interference in Practical Situations

With the combination of internal and external filtering with an antenna that has notches in its frequency

characteristic, an attenuation between 30 and 40 dB of the MC-SS signal at 5.25 GHz appears feasible. What does this imply for the practical situation between LDR and HDR far apart and close to each other? The following two paragraphs provide the answer.

Interference Between Remote AIs

With 35 dB of additional attenuation of the MC-SS signal, the received signal at distance *d* from an FM-UWB and MC-SS transmitter become equal, see Figure 7. Remembering that an SIR down to -2 dB is acceptable, this roughly means that the FM-UWB reception is not disturbed by MC-SS signals that origin from a transmitter further away than the FM-UWB transmitter. Interference from remote HDR devices can thus be tolerated.

Interference Between Co-located AIs

Interference from co-located HDR devices, that may be closer than the LDR devices, will be a problem. It is necessary to design higher layer coexistence mechanisms when the physical layer has no more margin.

4 Coexistence Mechanisms

There are two categories of coexistence mechanisms: collaborative coexistence mechanisms where the two interfering AIs/networks exchange information and non-collaborative coexistence mechanisms where the exchange of information is not allowed [7]. The possibility of exchanging information is quite easy when the two AIs are co-located in the same dual-mode terminal. Collaborative coexistence mechanisms enable the use of multiple AIs at limited levels of interference by a smart scheduling of the channel access, thereby suffering from some performance degradation. These mechanisms are employed on the MAC and higher layers and require control information exchange among active peers.

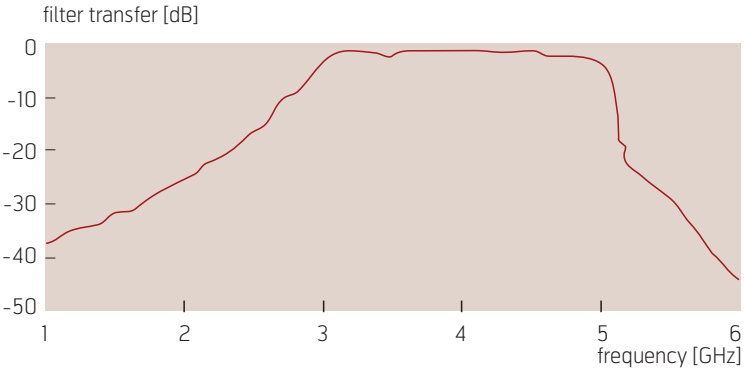


Figure 14 Measured transfer function of Taiyo Yuden bandpass filter

Non-collaborative coexistence mechanisms involve either only the PHY, or the PHY and MAC layers, and they do not need an exchange of control information between active peers. These methods basically exploit fluctuations of the channel quality in time, frequency, or space, to optimize the form of the transmitted signals with the aim of minimizing distortion by cochannel interference at the receiver. Their performance depends on the availability of information and the capability to predict the encountered cochannel interference.

Various proprietary collaborative coexistence mechanisms exist to coordinate the radio activity in order to prevent simultaneous operation of co-located AIs.

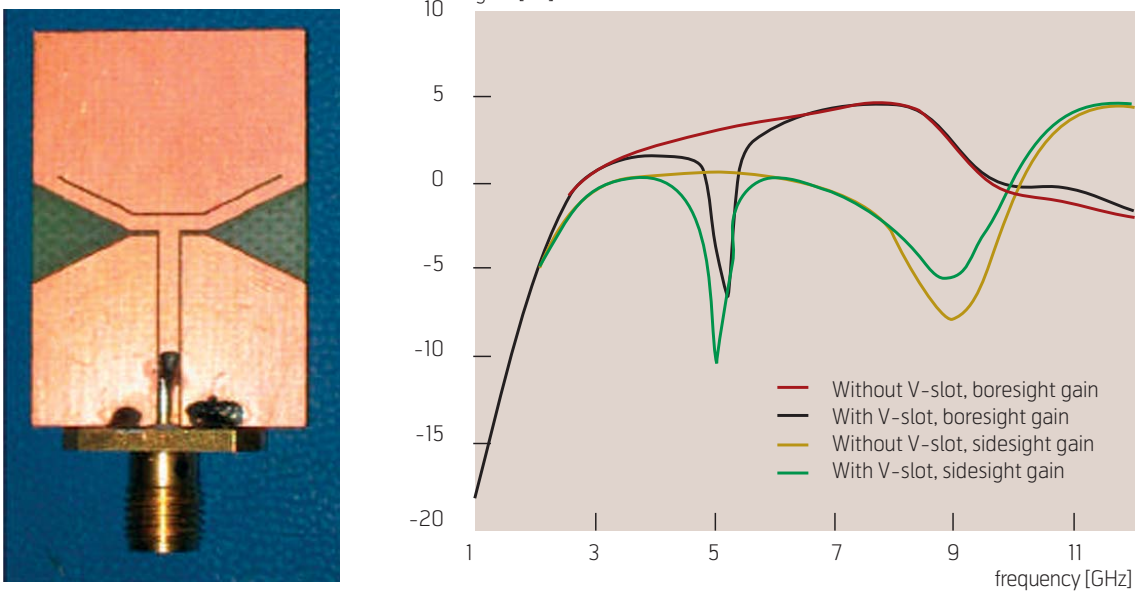


Figure 15 Planar UWB antenna with notch at 5.25 GHz and its gain

ISSN 0085-7130 ©Telenor ASA 2007

Most of them are designed to manage the coexistence of Bluetooth and WLAN systems [8]. The approaches vary in detail but essentially act to interleave operation in order to make the operations appear simultaneous. The techniques address the scheduling and priority setting of the two systems, making trade-offs on transmission duty cycle, idle times, and packet type (data, beacon). The packets of one system can be sent while the other is idle and vice versa; the end effect is to deliver reliable communication on both systems with a negligible loss of throughput. This is a time division approach which depends on the duplex method and the multiple access scheme of the two AIs.

There are three approaches that belong to the category of collaborative mechanisms:

1) Host software approaches (driver-level and dual mode switching);

2) MAC-level approaches;

3) System level approaches covering the entire wireless sub-system.

Host Software Approaches

The host software approach is a time-division approach, essentially based on the separation of the operational periods for each AI, and it has two possible implementations:

1) *Dual-mode radio switching*. This approach works by completely suspending the operation of one AI while the other is operational. There are two methods to implement it. The first method requires turning off the non-operating AI without signalling to other nodes in the network. The drawback of this method is that it can reduce performance. The second method acts as a signal to other network nodes that the operation of the AI is suspended.

2) *Drivel-level switching*. This approach is similar to the previous one but the functionality of control is managed at the driver level and it includes user-dependent switching, discriminatory switching, successful-transmission switching, statistical switching and time delay switching. In this approach, application transmit requests delivered to the operating system, are mediated at the driver level, thereby avoiding simultaneous transmission and collisions. This approach degrades the throughput because only one AI is active at a time; as a result, systems using driver-level transmit switching can suffer from dropped packets. As with dual-mode radio switching, this approach does not switch quickly.

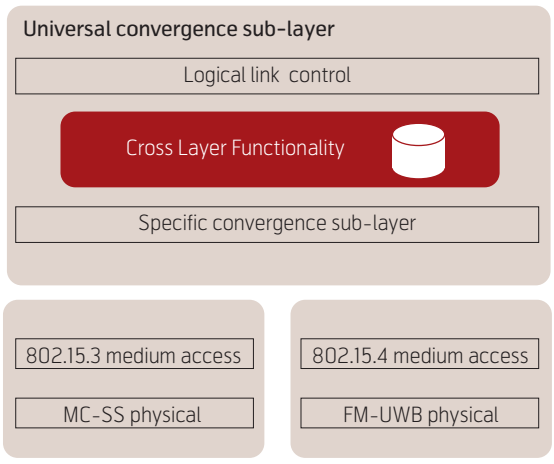


Figure 16 Protocol architecture of the multimode terminal

MAC Level Approaches

In the MAC-level switching we can apply one of the following solutions: to modify either MAC layers (802.15.4-based LDR MAC and 802.15.3-based HDR MAC) or to develop a new and self-contained module that communicates with both MACs.

In both cases this approach performs approximately the same functionality of driver level switching, but adds a predictable latency, and it would be the suitable solution to establish high performance coexistence mechanism in case of real time transmissions. This technique does not suffer from transmitting signals into incoming receptions.

Furthermore, since MAC-level switching is performed in the baseband, it is able to change the operational interface at a much faster rate than host software approaches.

System Level Approaches

This approach encompass the entire wireless sub-system: for example, a driver-level switching technique may generate the best user experience in a low bandwidth synchronisation scenario, while MAC-level switching will manage interference much more effectively for real time or voice traffic, or when a user has wireless peripherals such as speakers or a keyboard.

5 Protocol Architecture

The protocol architecture (see Figure 16) includes the Universal Convergence Layer (UCL) and two different radio air interface stacks, one for LDR based on a IEEE 802.15.4 medium access control layer and FM-UWB physical technology, and a second stack for HDR based on IEEE 802.15.3 medium access control layer and MC-SS physical technology.

The UCL is the component which is going to provide a common abstraction of every air interface; in this sense, the UCL is able to provide convergence of management and data operations over both air interfaces.

The protocol architecture of the UCL is composed by two sublayers, the Logical Link Control and the Specific Convergence Sub-Layer:

- The Logical Link Control (LLC) provides the common abstraction to control and transmit data over several radio air interface technologies. Inside the LLC there is an internal database which contains information associated to every radio air interface. According to this information the LLC is able to ensure the coexistence of several radio air interface technologies in the PAN through multimode optimisation mechanisms.

- The Specific Convergence Sub-Layer (SCSL) is in charge of the convergence of frames and service operations between the LLC and specific radio air interface stacks.

Through these entities and functionalities, the UCL will

- Provide both management and data operation over several radio air interface technologies;

- Support upper layers with information about current configuration of MAC and PHY functionalitites in a multimode PAN;

- Coordinate coexistence optimisation and activation of specific optimisation mechanisms for specific air interface layers.

6 Conclusion

This paper has presented the issues arising from the simultaneous exploitation of LDR and HDR WPAN air interfaces within the same environment. Several scenarios have been proposed which clarify the need for multimode LDR/HDR WPAN air interfaces. The two air interfaces for the LDR and HDR WPAN have been outlined focusing on the need for high coexistence levels. It has been found that, even if LNA filtering, external filtering and antenna filtering are good solutions for the management of interference between FM-UWB and MC-SS AIs, when the two AIs are located close to each other, MAC and higher layers mechanisms are needed to allow coexistence.

Acknowledgement

This work is supported by the European Commission under the FP6 MAGNET Beyond Integrated Project. The authors wish to acknowledge the collaboration of the partners involved in the work package 3 of this project.

References

1 Bantas, S et al. Architecture considerations and integrated-passives-based design for a dual-mode GPRS-WLAN SiGe RF transceiver. *IEEE 58th Vehicular Technology Conference*, 4, 2237–2241, October 2003.

2 De Sanctis, M et al. *Coexistence Concept for the Implementation of the FM-UWB and MC-SS RA Solutions*. IST-027396 MAGNET Beyond project deliverable D3.3.1, June 2006.

3 Ferreira, L, Serrador, A, M. Correia, L M, Svaet, S. *Concepts of Simultaneous Use in the Convergence of Wireless Systems*. COST 273, TD(04)102, June 2004.

4 Gerrits, J F M et al. Principles and Limitations of Ultra Wideband FM Communications Systems. *EURASIP Journal on Applied Signal Processing*, Special Issue on UWB-State of the Art, 2005 (3), 382–396, March 2005.

5 Schoo, K et al. MC-SS for Personal Area Networks – A Combined PHY and MAC Approach. *14th IST Mobile & Wireless Communications Summit 2005*, Dresden (GE), 19–23 June 2005.

6 Kim, Y, Kwon, D H. CPW-fed planar ultra wideband antenna having a frequency band notch function. *Electronics Letters*, 40 (7), April 2004.

7 IEEE. *Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands*. IEEE, August 2003. (IEEE Standard 802.15.2)

8 *Wi-Fi™ (802.11b) and Bluetooth™: An Examination of Coexistence Approaches*. Mobilian Corporation, 2001. (White paper)

Mauro De Sanctis is Assistant Professor at the Department of Electronics Engineering, University of Roma "Tor Vergata", Italy. He received the "Laurea" degree in Telecommunications Engineering in 2002 and the PhD degree in Telecommunications and Microelectronics Engineering in 2006 from the same university. He was involved in the MAGNET (My personal Adaptive Global NET) European FP6 integrated project and in the SatNEx European network of excellence; he is currently involved in the MAGNET Beyond European FP6 integrated project as WP3/Task3 leader. In 2006 he worked as post-doctoral research fellow for the ESA/ARIADNA extended study named "The Flower Constellation Set and its Possible Applications". He is/was involved in several Italian national research projects: ICONA (Integration of COmmunication and NAvigation services) from January 2006 to December 2007, SHINES (Satellite and HAP Integrated NEtworks and Services) from January 2003 to December 2004, CABIS (CDMA for Broadband mobile terrestrial-satellite Integrated Systems) from January 2001 to December 2002. He was involved in the DAVID satellite mission (DAta and Video Interactive Distribution) and is currently involved in the WAVE satellite mission (W-band Analysis and VErification) of the ASI (Italian Space Agency). In the autumn of 2004, he joined the CTIF (Center for TeleInFrastructure), a research centre focusing on modern tele-communcations technologies located at the University of Aalborg, Denmark. He is currently serving as Associate Editor of the IEEEAerospace and Electronic Systems Magaqzine. His main areas of interest are: satellite networks and constellations (in particular Flower Constellations), stratospheric platforms, resource managment of short range wireless systems.

email: mauro.de.sanctis@uniroma2.it

John F.M. Gerrits received the MScEE degree from Delft University of Technology, the Netherlands, in 1987 with final thesis on the design of integrated high-performance harmonic oscillator circuits. In 1988 he joined the Philips T&M division in Enschede, the Netherlands, where he designed integrated oscillator and data-acquisition systems for oscilloscope applications. In 1991 he joined CSEM in Neuchâtel, Switzerland, where he has been involved in both system and circuit design of a single-chip low-power VHF radio receiver for hearing aid applications and of a single-chip UHF transceiver for ISM applications. His current work involves system and circuit design of UWB radio systems, RF and EM simulation techniques and measurement methodology. He is currently working towards his PhD on the fundamental aspects and practical realizations of FM UWB communication systems at Delft University of Technology. He is editor and co-author of the book Low-power design techniques and CAD tools for analog and RF integrated circuits *published by Kluwer in 2001. He is the winner of the 2006 European Conference on Wireless Technologies Prize and holds three European and one US patent.*

email: john.gerrits@csem.ch

Julián Pérez Vila received his high engineering degree in Computer Science, Software Engineering speciality, from the "Universidad Pontificia de Salamanca" in Madrid, 1997-1998. Following his engineering studies he worked as an analyst-programmer of Meta4 tools for internal systems of the company El Corte Ingles, adapting payroll, human resource and accounting modules. In 2000 he began work in Telefonica I+D in the "3g consultancy group", editing and contributing several 3g reports on the demand of Telefónica Móviles, increasing knowledge regarding multiple technologies:

- *UMTS-IMS, GPRS and GSM architectures*
- *Ipv6, OSA and Quality of Service architectures*
- *Multimode terminals and data-roaming aspects*
- *Interoperability between Mobile Networks and Wireless LAN*
- *Universal user profiles, presence servers and SIP technology*

After this consultancy period he contributed research and development activities related to knowledge management and began his participation in the IST European MAGNET project, where he is coordinating the research and development contributions to the areas of context management in personal networks and multimode radio air interface technologies.

email: jpv@tid.es

The Unpredictable Future – Personalized Services and Applications Architecture

MARY ANN INGRAM, RAMJEE PRASAD, KIM SKAUE

Mary Ann Ingram is a Professor at Georgia Institute of Technology, Atlanta, USA

Ramjee Prasad is Director of Center for Teleinfrastruktur (CTIF) at Aalborg University, Denmark

Kim Skaue is CEO at C3 faculty at Aalborg University, Denmark

In this paper, we discuss our ideas for a concept we call 4G-Smart Wireless Living (4G-SMILING or 4GS). These ideas are based on the view that a focus on service is essential for the development of 4th generation wireless services. "Essential," that is, for a lucrative and efficient utilization of the communications infrastructure. In this concept paper, we imagine the highest levels of service and convenience, and what technologies, especially wireless access technologies, will be needed to realize this vision. We observe that the requirements assumed for wireless access technology in the two fields most related to 4GS, wireless communications and ubiquitous or pervasive computing, are very different, and we propose a strategy to harmonize these. We also discuss current related projects and identify some challenges to achieving the 4GS vision

Introduction

What is excellent service? Delivery of exactly what you want and need at the right time, in a manner appropriate to your immediate situation. In this paper, we consider some challenges and issues associated with realizing this with a conceptual system we call 4G-Smart Wireless Living (4G-SMILING or 4GS), which aims to provide the highest level of automated service to mobile users. 4GS would pro-actively provide a "service cocktail," intended to optimize a person's daily activities, eliminate mundane, stressing, and time-consuming work, and proactively provide services and products to improve convenience and quality of life, 24/7. We think that the most successful 4G system design will be service-driven, and that the user's internet-based agent will constantly optimize the mode of delivery of these services.

Researchers seeking to provide the highest levels of service and convenience to mobile users are found in two fields: wireless communications and pervasive or ubiquitous computing. However, they take different approaches, have different business models, and they make very different assumptions about requirements in wireless access technology. We claim that 4GS resides in the intersection of these two fields, and we suggest a strategy for achieving this intersection that focuses on access optimization. We do not provide detailed solutions to the problem in this paper. Rather, we identify likely elements of 4GS, propose a high-level architecture, review some of the current and recent related projects, and identify important challenges to realizing 4GS.

Personalization and Context Awareness

Part of knowing wants and needs implies familiarity or *personalization*. This requires an integration and organization of a user's preferences, perhaps initially determined through an interview, but later automatically adapted over time, also known as the *user profile*. The other part of knowing wants and needs is sensing, which includes traditional forms of user input, as well as non-traditional forms, such as speech recognition and on-body and off-body sensor networks. Proper exploitation of the user profile allows the user to simplify his requests. As a very simple example, a frequent patron of a particular restaurant can just ask for "the usual." An even higher level of service and convenience is when the user doesn't even have to ask. Continuing with the restaurant analogy, the wait staff recognizes the patron and immediately presents the desired meal without requiring a single word from the user.

The second restaurant example shows that sensing is important to a high level of service. Indeed, the sensed location, user activity and mood can indicate the relevant parts of the user profiles [10], as shown in Figure 1. For example, a user's profile for "home" and "eating" may invoke a certain type of music playing and a certain filter on which calls the user is willing to accept. Applications that exploit sensed infor-

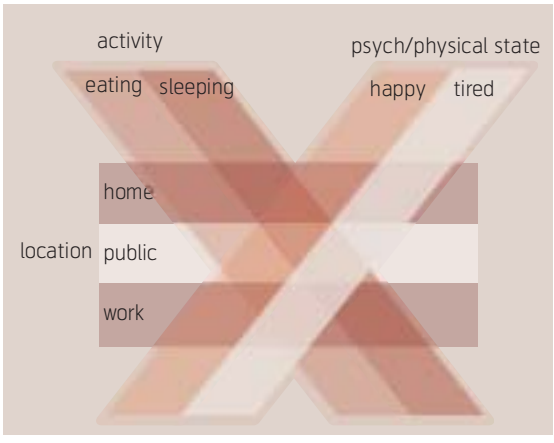


Figure 1 Example subsets of the user profile

ISSN 0085-7130

Figure 2 Proper sensing and exploitation of the user profile should minimize clumsy user data entry

mation are *context aware*. Proper utilization of the user profile and sensing technology should minimize clumsy user data input, as shown in Figure 2.

4G-SMILING (4GS) would offer a "service cocktail", which is an extremely personalized and context-aware mix of business and pleasure applications, which automatically adapts as the user moves and acts, 24/7. As the user moves through differently equipped or enabled environments, e.g. home, train, automobile, public street, office, stores, or restaurants, through different activities, e.g. relaxing, working, exercising, cooking, shopping, or visiting, and through different moods and emotions, 4GS constantly senses the changes, and presents the desired services to the user in the most efficient way.

Push, Pull, and Modalities

Computer applications are classified as *push, pull* or a combination of both [1]. Pull applications are conventional and are initiated by the end user. The user must make choices at every step and must pursue the information that he or she needs. The application has no or very little memory of past interactions with a particular user. Constant user presence is necessary, and pull applications tend to be short-running (on the order of minutes). There is no personalization. An example pull application is finding the schedule for a train and making reservations online.

A push application is the opposite of a pull application. A push application is initiated by the application. It "engages a user at the right time by proactively pushing an interactive session to the user" [1]. Constant user presence is not necessary, and push applications can run for days or more. "Right time" engagement requires context awareness and personalization or exploitation of the user profile. Although there will always be a need to retain some pull applications, the highest levels of service will come from push applications.

Push applications have a variety of ways to present information to the end user; these are called *presentation modalities* [1]. Conventional examples include websites, cell phones, email, short message service. Push applications of the future will have many more avenues to reach the user. Non-conventional examples include on-body actuators that stimulate the senses directly, creating sounds, tactile sensations, aromas, and visual displays [11]. Other non-conventional examples are off-body displays and actuators. The distinction between on- and off-body presentation modalities is particularly important with regard to wireless communications requirements, as off-body modalities may be directly connected to the wired infrastructure. This subject will be discussed in more detail in a later section.

One challenge that follows from a plurality of presentation modalities is how to map the content to each modality within the set. Currently, content producers generally provide the content in several different forms, which is unscalable and expensive [1]. Ideally, a producer need to provide only one version of the content, and then an automatic process maps the content onto the modalities [1]. The mapping should optimize a quality function, which could depend on many parameters, for example, reliability of the connection, presentation quality, power consumption on battery-powered devices and cost.

We may also consider *extraction modalities*, or ways to collect information from the end user. While the conventional ones are normally associated with pull applications (again, websites, cell phones, email, short message service), non-conventional ones, such as sensor networks, can provide the sensing technology needed for context awareness. A sensor network can include on- and off-body sensors. On-body examples are biometric sensors (e.g. blood pressure), while off-body examples include cameras and microphones with voice recognition. As with presentation modalities, the on-body modalities will impact the wireless communications requirements.

In the long term (5-10 years), deployed off-body modality packages may evolve into several standard classes, generic to many applications. However, in the nearer term (2-3 years), we do not expect them to be very standardized, and they will be sold in forms that are customized to different applications. For example, we can identify and imagine a number of off-body modality packages that could be made available to consumers and enterprises in Table 1. For example, in "Fail-Safe Cooking," the user can select one or more recipes. Flashing lights show and audio tells the user where to find the necessary items. Video demonstrates a procedure in a step-by-step way. Embedded processors and sensors in the stove or oven alert the user exactly when a cooking step is complete and turns off the heat. The challenge for

Title	Purpose	Example Components
"Basic Home Information System"	Entry level web-based personal information system (added to an existing home)	Moderately sized audio/video panels for each room, connected by WLAN, controlled by a server in the home, connected to the internet, with speech rec/synth
"Aging in Place" [2]	Enable elderly people to stay in their homes	Floor sensors (fall detector); distributed video camera network (detects habit change)
"Fail-Safe Cooking"	Simplify cooking	Thermal sensors, video displays, indicator lights, interface to stove and oven
"Game Place"	Video game entertainment	Video display, controllers
"Battery Saver Kiosk"	Offload computation and long-range communication from on-body to off-body, when in close proximity	A user device clone that plugs into the wall power socket
"CitiDisplay"	Provides information and entertainment to users in a public environment	Large video display; RFID detector; voice recognition
"Home Moods"	Creates personalized, dynamic environment in the home	Distributed audio/video, RFID detector, biometric sensors, aroma generator

Table 1 Off-body modality packages that may be offered in the near term (2-3 years)

4GS is to detect what off-body modality packages are available to the user in whatever is his current environment, and to optimally adapt the content mapping process.

Databases, Security and Privacy

A key technology associated with the user profile and its use in providing context-aware information to the user is *database management*. The user profile is a database and the various types of content that may be provided to the user are in other databases. Database management is concerned with the design of efficient protocols that *query* or *modify* databases. The usual concerns are how to efficiently tag information so that it can be located by machines with minimum delay. Network "bottlenecks" and disc access time are discussed. Communication costs, in terms of packet loss and delay, are rarely taken into account, even though the costs of wireless communication can be significant. Consideration of communication costs would be a necessary part of 4GS design. Determining control, access, and security of the user profile are other major challenges for 4GS, but the reward is a highly personalized and convenient service.

A fully developed user profile and highly perceptive sensing mechanisms will be very attractive to those who seek to harm or exploit the user. The consequence of achieving the high level of service and convenience is that the service will have exceptional access to the user. Adam Greenfield wrote, "By comparison with the World Wide Web, ubiquitous computing is vastly more insinuative. By intention and design, it asserts itself in every moment and through every aperture contemporary life affords it. It is everyware" [19]. Therefore, protection of the profile and sensor data is paramount. This level of access is similar to a surgeon's access to a patient. The patient trusts the surgeon, and by relation, all the surgeon's support staff and systems. The same level of confidentiality that is accorded to patient data must be accorded to the user profile and sensor data.

The surgeon analogy may also be considered from the point of view of advertising. The surgeon and his support staff are certainly the targets of much advertising, about drugs, medical devices and services – there is a lot of money involved. However, the patient is not exposed to all that advertising. Rather, the surgeon and staff make nearly all the decisions about what to use and how to use it. Typically, the patient trusts that the medical team is well-trained, understands his needs clearly, and is acting in the best interests of the patient. Therefore, the medical staff will expose the patient to only a limited range of treatment options, often only if the patient asks. It is anticipated that the highest level of user service will have similar characteristics. The service will employ a strong and narrow filter on advertising, based on the user profile and context information. Lower-cost versions of 4GS will admit more advertising.

Mobility and Power Management

Database management, personalization, context awareness, and confidentiality, are all topics that could be considered for exclusively wired networks. However, the convenience aspect of the best information service demands wireless communication to enable mobility.

Mobility generally implies battery power, and convenience means reasonably long battery lifetimes. A high level information service adds more functions to the current voice, video, email, and messaging that existing 3G phones have. The additional functions will require additional energy. An example of this is GPS, which is available on certain phones today and is very useful for context awareness. However, GPS is known to consume a high amount of energy, and therefore it is usually disabled on the phones. Unfortunately, battery technology moves more slowly than the technologies that depend on batteries. Thus for the services we envision, battery life will shorten unless special measures are taken.

One approach is to provide the user with frequent and convenient opportunities to recharge his or her personal devices. For example, chairs could have chargers built into the armrests.

However, another consideration is wireless link availability. Single wireless connections are inherently unreliable, and particular air interfaces, such as 3G, WLAN, or Bluetooth, may not be available in all the places that a user goes. *Multi-band software defined radio* (MB-SDR) is an attractive solution to this problem. An SDR can be programmed to work with any air interface designed for the band of the SDR [3]. Adding multi-band capability makes the radio extremely flexible. This adds reliability because the radio can use the best quality air interface at any instant. This "intelligence" for finding the best air interface is called *cognitive radio* [3]. However, it is generally agreed that a barrier to deploying SDR is its projected short battery life.

One challenge is how to determine the power and bandwidth requirements for personal devices as we move toward a world with *ambient intelligence* (AmI) and *pervasive computing*. "Ambient Intelligence represents a vision of the future where we shall be surrounded by electronic environments, sensitive and responsive to people" [4]. Pervasive or ubiquitous computing is the idea that all sorts of commonplace items in our surroundings will be able to compute.

The current trend is to pack more and more onto the handheld personal device – more computing capability, more memory, more radios (e.g. 3G, WLAN, Bluetooth, GPS), and more application software resident on the device. At the same time, the wireless bandwidth requirements are going up.

However, if we believe the AmI folks, then most of this will not be needed most of the time. Imagine walking into a room that is equipped with networked speakers, microphone, camera, other sensing devices and a visual display. This network detects your presence and authenticates you – perhaps by the RFID chip you wear or have imbedded under your skin, or by biometric sensors. You don't even have to "log-in". Conceivably, all your applications and services run on servers that are located somewhere on the internet, not necessarily near your immediate location. You may have a seat, use the wireless mouse that is conveniently on the chair arm, and proceed to scroll, point and click (if you prefer interaction the old fashioned way), or you can have a verbal dialog with the system. What are your battery requirements in this scenario? RFID batteries can last eight years or more. The bandwidth requirement between your on-body wireless device(s) could be extremely low because all they have to do is identify you and possibly send some biometric information. The off-body network, on the other hand, all has access to wired power, has a much larger display, and may have a much more reliable connection than the wireless connection to the personal device. The idea of having nearly all the presentation and extraction modalities off-body, and reliably present in our environments, seems the ultimate in convenience.

There is clearly a huge gulf between today's trend in wireless access and the AmI future. AmI assumes a great deal of infrastructure, although modular, low-cost, easy-to-install devices don't seem so futuristic (for example, consider the "Basic Home Information System" in Table 1). We propose the following strategy for achieving convergence in these two fields: that personal communication devices or terminals be considered as optional modalities when wired modalities also exist, and that an internet-based agent or middleware provider make the decisions about which modality to use at any particular time, to best serve the needs of the user.

We note that this is a generalization of the "always best [wireless] connection" idea from cognitive radio. The generalization is that the best connection may be wired and the best modality may be off-body. The generalization moves the control away from the personal wireless device or wireless service provider to an internet-based agent. This movement has profound implications on business models for services.

Convergence of these fields does not mean that wireless providers and equipment manufacturers should cease their efforts to provide faster and better wireless access to the user, because there will always be places with no or only limited off-body modalities. Also, there will be times when the user chooses not to use an off-body modality for privacy reasons. On the other hand, most of us spend a great deal of time in relatively private spaces, which in the near future can be economically equipped with off-body, pervasive computing-type devices. The great majority of these off-body devices will be connected to the internet and wired to power. Also the success of ring tones and of multi-player video gaming shows that people like to express themselves in public places and entertain themselves on a shared display. As ubiquitous computing becomes a reality, we conjecture that the percentage of time that personal communication devices require high-bandwidth connections will decline.

User Acceptance

The most sophisticated technology will not be successful if users are afraid of it or view it as too difficult to use. The biggest challenges to user acceptance are expected to be

- Hardware and software support
- Simple and intuitive user interface
- Security, privacy and protection from SPAM
- *Pulling* information to initially build the user profile.

The envisioned superior service will be a fantastic technology, assuming it all works. However, the service will have unprecedented complexity. With potentially both on- and off-body presentation and extraction modalities, and the maintenance of the user profile and the subscriptions, the level needed of *personal* hardware and software support will exceed what corporate employees have grown to expect from their information technology (IT) support department.

Assuming the system works, then the user interface must be simple enough for a non-technical person to use easily. Of course, the interface should include voice recognition and voice synthesis. However, with sensing technology and context awareness, other forms of communication may be possible, for example, off-body video sensors could interpret minimal hand motions in the air instead of mouse movements and clicks. One research group thinks that the detection and synthesis of emotion will be the key to the success of human-machine interaction [12].

The quality of the user profile is central to the usefulness and convenience of 4G-SMILING. Once the user profile is initialized, then conceivably, it can be automatically updated through a combination of context awareness, mood sensing, and occasional user inputs. We imagine that mood sensing could be performed by an "interpreter service" that would take as its inputs relevant context information (location, activity, time-of-day) and available sensed data about the user's psychological state. If it is determined that the user doesn't like something in a certain context, as shown in Figure 3, then the user profile can be updated to reflect this new information.

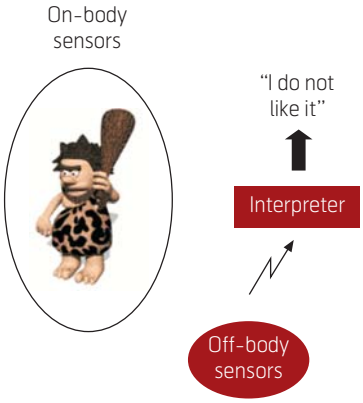


Figure 3 Example of the interpreter

A possibility for improving the user profile is "intentional perturbation". We imagine that most users will not want static profiles. Users need exposure to new things, but how fast, what and when? Of course, 4GS must include web browsing and opportunities for the user to directly modify his or her profile. In addition, however, we imagine that a variety of ways could be used to systematically perturb a user's profile, and then use the interpreter service to bring the profile to a new optimized state. Example bases of systematic perturbation may include (1) what your friends are doing, (2) purchaser communities ("others who bought this product also bought…"), (3) fashion shows and celebrity profiles, (4) systematic random perturbations, and (5) advertising.

Potential 4G-SMILING Architecture

Figure 4 shows a concept for the 4G-SMILING architecture. Enclosed within the bold rectilinear outline is the "Service Manager" (SM), which incorporates the user profile (UP), the UP editor and filter, the very important "Push Computer," various agreements that the user has with web-based services, access services, and content providers, and the "Optimal Content Mapper." Any connections from the SM to entities outside the SM are assumed to be through the internet. Enclosed within the dashed curve are local entities that we are assuming would be most efficiently located in *relatively* close physical proximity to the

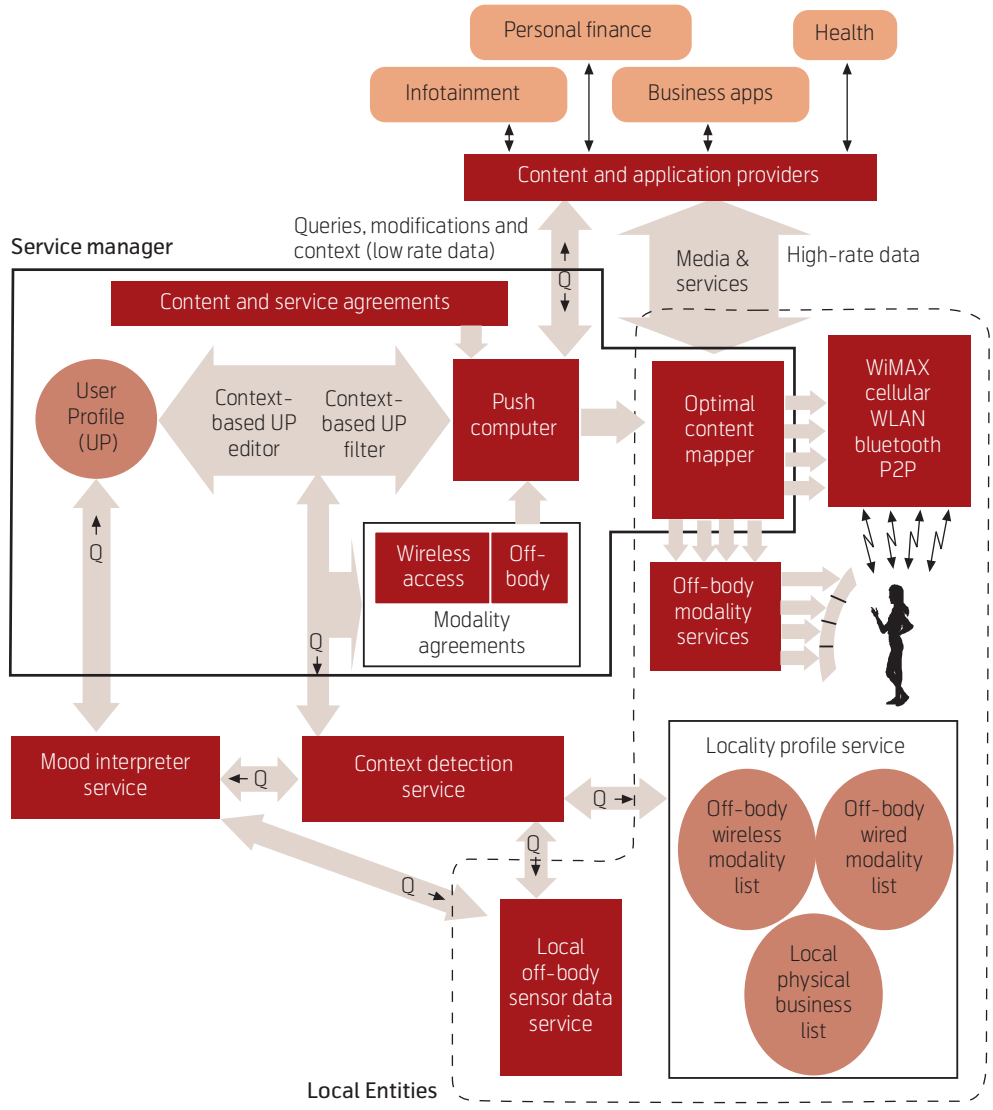


Figure 4 Possible 4G-SMILING architecture

user. These include the various wireless access points or base stations, a local directory or "Locality Profile Service," (LPS), and one or more Local Off-Body Sensor Data Services. This means that the SM could be on a server anywhere connected to the internet. The off-body modality services, such as the server controlling the "Fail-Safe Cooking" modality set, would also be local to the user. Lower-data rate services, such as the Context Detection Service, are not required to be near the user.

We observe that the Optimal Content Mapper (OCM) is both within the SM and considered a local entity. This is because the OCM will be handling high-data rate content, such as high-resolution video. If the rest of the SM is on a distant server, it would not make sense for the video to first be shipped to that distant server before being sent to the user. The OCM would need to reside on a server local to the user, possibly the same one that handles the Off-Body Modality Services.

The LPS need not necessarily be close to the user, but to have a scalable system (i.e. to avoid too much traffic at a Regional or National Profile Server), local information should be distributed in its associated locality.

The Push Computer determines the content or services that will be presented to the user. It bases this determination on (1) requests from the user or from push applications, (2) the subset of the UP that has been identified by the Context-Based UP Filter, (3) the modality availabilities and agreements, and (4) the content and service availabilities. It then requests or commands that the content or service be delivered to the user via the server that holds the OCM.

Queries and modifications can go both ways between the Push Computer and the Content and Application Providers. The most useful applications will query the Push Computer about the User Profile. For example, a "travel assistant" application may detect that a

flight has been cancelled, and will need to consult the User Profile to determine such things as friends and associates at the destination who should be notified, and user preferences about hotels so reservations can be changed. On the other hand, the Push Computer can query the applications for possible context information. An example of this is as follows. The popularity of gaming today, especially internet gaming, suggests that in the future, "virtual" context (i.e. within a game) may be as important as physical context (just ask any parent who has ever tried to interrupt a teenager playing an internet game). Finally, application history may cause a modification to the User Profile, while the Push Computer can cause a change of state in an application.

Storing the User Profile on a server, rather than on the user's personal device, may seem risky, since it will contain sensitive and personal data. However, we propose that it should not be on the user's personal device because of the nature of push applications. As stated earlier, they are long-term running programs, which will perform better with an always-on connection so they can interact constantly with other databases and applications. Having it on the internet means the user is not tied to a single personal wireless device, and enables the user to maintain and benefit from the services even if he or she temporarily loses the use of a personal wireless device. Also, storing the UP on the internet is more consistent with the notions of pervasive or ubiquitous computing, which require only RFID to identify users. Finally, we note that much sensitive and personal data (e.g. medical records) is already stored on databases not directly under users' control. The security of this UP data is of utmost importance and constitutes one of the biggest challenges of 4GS.

Some Related Fields and Projects

The 4GS vision is very interdisciplinary and includes elements in the fields of pervasive or ubiquitous computing, ambient intelligence (AmI), context awareness, cooperation between heterogeneous radio access networks, content distribution, sensor networking, location-based services, music and image information retrieval, emotion sensing, wireless network security, semantic web development [15], dynamic partitioning of hardware and software, and business model development.

There are also many existing projects that are relevant. Some are focused on a subset of relevant topics, or are focused on particular applications. Some consider different approaches. The following is a discussion of a few, mostly European, existing projects related to the 4G-SMILING (4GS) vision. They include Magnet Beyond [5], Puma [2], HUMAINE [12], MobiLife [9], Omnipresent [6], e-Sense [7], Daidalos [8], CRUISE [13] and SPICE [10]. This list only partially captures the activities going on today in this subject area.

The predecessor to Magnet Beyond (MB) is Magnet [9], which is about how to create a Personal Network (PN) that is a secure, trusted and seamless connection between a user's personal area network (PAN) and remote networks that supply the user's applications and services, such as the office network and the home network. MB extends the PN to federations of PNs that are associated with other people with whom the user would like to share information [5,14,6]. These federations are defined by the security and privacy boundary that encloses the federated PNs [5,14,6]. MB is also concerned with context awareness. Security is adapted to the service or application being used and the user profile. Service discovery within the PNs and federated PNs is made to be context aware; example contexts are location (e.g. home, office, hospital, public) and role (parent, spouse, child, employee, etc.). Device power management is also a consideration in MB. Reconfigurable hardware and adaptive mapping of algorithms onto different types of computing platforms (ASICs, FPGAs, etc.) are methods for saving battery life that are currently being investigated. In MB, peer networking is considered for the devices with the PN, and the short-range air interfaces are optimized for the PAN applications.

The focus of Magnet and MB is the provision of the secure connections within and between PNs. In contrast, the focus of 4G-SMILING is on the ultimate service application. 4GS depends on the connections to the extent that they impact the quality of the service that is delivered. 4GS starts with the application, and asks how the underlying network should be optimized to provide the best possible service to the user. Topics of relevance to 4GS that are outside the current scope of MB include:

- User acceptance
- Automatic perception of user reaction
- PN resilience and dependability
- Adaptation of content to modality
- Access rights to database, user anonymity, trust establishment
- Global service discovery outside of federated PNs
- Exploiting non-PN peer-to-peer networks for scalability and low power
- Relating content profiles and personal profiles to achieve personalized content
- Distribution and control of profile information
- Business models.

The Puma System, developed at the IBM T.J. Watson Research Center, appears to be the "first generic system for accessing Web applications from arbitrary collaboration modalities" [1]. The "collaboration modalities" are conventional ones associated with business applications (IM, email, phone) [1]. Puma is a context-aware, push application, which employs a "Pusher," which is similar to the Service Manager (SM) in Figure 4. The Pusher includes the "Push Engine," which is similar to the Push Computer of Figure 4, and a "Modality Resolver" and "Modality Bots," which together are like the OCM in Figure 4. Puma provides the "view aspects" of an application in a modality-independent format.

The 4GS vision represents an extension of Puma to include a much broader set of content and applications, and a larger set of modalities, including off-body modalities, with a mapping that minimizes power consumption on the on-body devices. 4GS also includes systematic profile perturbation and mood interpretation.

Like Puma, Daidalos considers a middleware approach to managing multiple modalities, however it restricts to on-body wireless modalities. Daidalos assumes that the telecom operator "takes the role of the service provider and offers the most crucial services to its customers," [8] and focuses on operator/provider challenges when a piece of middleware automatically chooses the "best" wireless interface in response to user mobility and needs [8]. It considers context awareness and personalization, with emphasis on quality of service (QoS), security, and how the business models change from vertical to horizontal when the user has a virtual identity that is separate from a specific air interface [8]. In contrast to Daidalos, the 4GS vision does not assume that the telecom operators are the chief providers of services. This is because there will probably be multiple modalities simultaneously available to the user, likely to be provided by different telecom operators, and the user, or at least the user's Service Manager, will choose which combination of modalities (and therefore which telecom operators) to exploit. Also, 4GS extends Daidalos to include off-body modalities, mood interpretation, and systematic profile perturbation.

Like our 4GS vision, the goal of MobiLife [9,16] is to exploit off-body modalities, however it is in stark contrast to 4GS because apparently the content and services flow through the user on-body device before being transmitted to the off-body devices. In other words, the user device acts as an intermediate server in the data path. While the MobiLife approach may be more scalable, it is not battery-power efficient and, if a wired connection to the modality is available, the MobiLife approach might provide a much less reliable connection (two wireless hops in place of a wired connection).

The e-Sense project is mainly about how to integrate sensor networks and Beyond 3G infrastructure [7]. The emphasis is on providing the internetwork connections to *enable* context awareness. The 4GS vision would extend e-Sense to support more modalities, including wired modalities, and is more application oriented.

The SPICE project addresses the challenge of how to deliver context-aware and personalized services as a user moves from one administrative domain to another [10,17]. It therefore has a lot in common with the 4GS vision. One SPICE objective is the development of semantics for the user profile data, so that the data can be efficiently used by different applications and services. Another is development of models and classification for context data. A Provisioning Framework and a Content Broker are proposed, which are similar to the Service Manager and Context Detection Service, respectively, in Figure 4. A chief difference between SPICE and 4GS is that in SPICE all the modalities are on the user's mobile device, whereas in 4GS, the emphasis is on always off-loading computation, communication, and/or modalities away from the user's personal devices to those resources in the user's environment, when they are available and when it is advantageous to do so.

HUMAINE is a European Network of Excellence project that is about developing emotion-sensitive multimodal interfaces so that humans and machines may interact in a way that is natural to the humans [18]. HUMAINE and similar work is a critical part of the 4GS vision; it will be needed for all the modalities. For example, many of the services might be delivered by a familiar face in the on- or off-body visual displays. A more explicit indication of these concepts in Figure 4 is the direct connection between the Mood Interpreter Service and the User Profile.

CRUISE (CREating Ubiquitous Intelligent Sensing Environments) is another European Network of Excellence project with the objective of coordination and network among researchers of wireless sensor networks [13]. This includes integration and sharing of testbeds and research tools. CRUISE topics are necessary for the context-awareness aspects of 4GS.

Conclusions

In this paper, we have explored and imagined some of the features of the ultimate mobile service, which we refer to as the "service cocktail" or 4G-SMILING

(4GS). Two of the most important are that it would be highly context-aware and personalized. We have observed that two fields, Ambient Intelligence (AmI) and Mobile Communications, are both dedicated to providing the mobile user with the ultimate in service, yet they make very different assumptions about the requirements for mobile wireless access. We suggest that when the user is in an AmI or similarly enabled environment, as many functions as possible and reasonable be off-loaded to the wired environment, to provide a more reliable connection, to save power, and to provide a better experience for the user. Some of the many challenges remaining to realize 4GS include detect what off-body modality packages are currently available to the user, mapping the content to each modality, security and privacy of the user profile, and how to update and intentionally perturb the user profile.

References

1 Chandramouli, B et al. Pushing the Envelope of Pervasive Access. In: *IEEE International Conference on Pervasive Services (ICPS)*, July 2005.

2 Abowd, G A et al. The Aware Home: Developing Technologies for Successful Aging. *Workshop held in conjunction with American Association of Artificial Intelligence (AAAI) Conference 2002*, Alberta, Canada, July 2002.

3 Mitola, J III. *Cognitive Radio Architecture*. Wiley, 2006.

4 *EUSAI – Second European Symposium on Ambient Intelligence*. URL: http://www.eusai.net/

5 IST. *MAGNET Beyond* (IST-FP6-IP-027396). URL: http://www.magnet.aau.dk

6 Calin, D, McGee, A R, Chadrashekar, U, Prasad, R. MAGNET: An approach for secure personal Networking in Beyond 3G Wireless Networks. *Bell Labs Technical Journal*, 11 (1), 79–98 2006.

7 *e-sense – Capturing Ambient Intelligence for Mobile Communications through Wireless Sensor Networks*. URL: http://www.ist-esense.org/

8 Aguiar, R, Farshchian, B A, Sarma, A, Einsiedler, H. Daidalos: the global architecture and its instantiations. *Proc. of the 15th IST Mobile Summit*, Myconos, Greece, 8 June 2006.

9 *IST MobiLife*. URL: http://www.ist-mobilife.org/

10 Zhdanova, A V et al. Context acquisition, representation and employment in mobile service platforms. *Proc. of the 15th IST Mobile Summit*, Myconos, Greece, 8 June 2006.

11 Kernchen, R, Mrohs, B. Context-aware multimodal output selection for the device and modality function. *6th International Workshop on Applications and Services in Wireless Networks,* Berlin, 29-31 May 2006.

12 Schröder, M, Cowie, R. Developing a consistent view on emotion-oriented computing. In: Renals, S, Bengio, S (eds.) *Machine Learning for Multimodal Interaction*. Springer LNCS 3869, 194–205, 2006.

13 URL: http://www.telecom.ece.ntua.gr/cruise/

14 Prasad, R, Olsen, R L. The unpredictable future: Personal networks paving towards 4G. *Telektronikk*, 102 (1), 150–160, 2006.

15 Hepp, M. Semantic web and semantic web services, father and son or indivisible twins? *IEEE Internet Computing*, March-April, 85–88, 2006.

16 Kernchen, R et al. Context-awareness in MobiLife. *Proc. of the 15th IST Mobile Summit*, Mykonos, Greece, June 2006.

17 *European IST-FP6 project SPICE*. URL: http://www.ist-spice.org/index.html

18 *Humaine*. URL: http://emotion-research.net/

19 Greenfield, A. *All watched over by machines of loving grace: Some ethical guidelines for user experience in ubiquitous-computing settings*. 12/01/2004. URL: http://www.boxesandarrows.com/view/all_watched_over_by_machines_of_loving_grace_some_ethical_guidelines_for_user_experience_in_ubiquitous_computing_settings_1

Mary Ann Ingram received the BEE and PhD degrees from the Georgia Institute of Technology (Georgia Tech) in 1983 and 1989, respectively. From 1983 to 1986, she was a Research Engineer with the Georgia Tech Research Institute in Atlanta, performing studies on radar electronic countermeasure (ECM) systems. In 1986, she became a graduate research assistant with the School of Electrical and Computer Engineering at Georgia Tech, where in 1989, she became a Faculty Member and is currently Professor. Her early research areas were optical communications and radar systems. In 1997, she established the Smart Antenna Research Laboratory (SARL), which emphasizes the application of multiple antennas to wireless communication systems. The SARL performs system analysis and design, channel measurement, and prototyping relating to a wide range of wireless applications, including wireless local area network (WLAN) and satellite communications, with focus on the lower layers of communication networks.

email: mai@ece.gatech.edu

For a presentation of Ramjee Prasad, please turn to page 3.

Kim Skaue was appointed CEO at C3 (Convergence, Connectivity and Communication) faculty at the University of Aalborg in 2006. The C3 faculty is a 4G innovation center. Kim Skaue has extensive experience in the telecom industry serving as Vice President Strategy and Business Development at Sonofon (Denmark) and Vice President in Telenor Nordic (Norway) with direct responsibility for building a cross Nordic mobile operation. He was the strategic architect behind the very successfull MultiPlan (vPBX) concept in Sonofon, a concept which today accounts for half of Sonofon's revenues. Besides his top management positions Kim Skaue is a board member in several companies and serves as external lecturer at Aarhus Business School teaching Innovation and Business Development. Kim Skaue holds an MSc electronic engineering – MBA in International Management and is a Top Governance graduate.

email: kim@xfon.dk

ITU Plenipotentiary Conference 2006 – PP-06,

Antalya, 6–24 November 2006
An Overview of Main Results of the Conference

ANNE LISE LILLEBØ

Anne Lise Lillebø is Director, Telenor ASA, Group Regulatory

The article gives an account of the main results of PP-06 seen from a Telenor and a Sector Member perspective.

1 Historical Background

The International Telecommunication Union (ITU) is an intergovernmental organisation and a specialised agency of the United Nations (UN) for telecommunications consisting of 191 Member States and over 600 Sector Members. ITU's main objective is to promote connectivity and interoperability between its members and to foster the development of all kinds of telecommunications worldwide.

The organisation was established in Paris on 17 May 1865 under the name of the International Telegraph Union to undertake the task of harmonising interconnection of the national telegraph networks. Norway was one of the "founding fathers" of the Union and Norway has taken active part in the work of the Union since its inception.

Sungate Port Royal Hotel, Antalya, Turkey – Venue of PP-06

ITU offers a unique partnership between Member States and the private sector by allowing the private sector to become so-called Sector Members in ITU's three sectors. With the liberalisation of the telecommunication sector in Norway, Telenor has chosen to take part in the activities of the ITU by being a Sector Member of ITU's three sectors – the Radiocommunication Sector (BR), the Telecommunication Standardization Sector (TSB) and the Telecommunication Development Sector (BDT). Norway is a Member State of the ITU and the Ministry of Transport and Communications is responsible for Norway's membership in the ITU, whereas the Norwegian Post and Telecommunications Authority (NPT) has been appointed Norway's "ITU Administration" and is responsible for the day-to-day management of ITU related matters on behalf of Norway.

2 General about ITU Plenipotentiary Conference

The Plenipotentiary Conference (PPC) is ITU's top policy-making body. The PP is held every four years and sets the Union's general policies, adopts four-year strategic and financial plans and elects the senior management of the organisation, the Council (the Union's governing body) and the Radio Regulations Board (RRB). The PP is the key event where ITU's strategy for the next four years is decided, determining the Union's ability to influence the development and growth of information and communication technologies (ICT) worldwide in the light of changes in the industry and the needs of its membership. As an intergovernmental conference only Member States have the right to send delegations to the Plenipotentiary Conference. Each Member State has one vote. A number of international organisations and Sector Members may attend the PP as observers.

3 The Plenipotentiary Conference 2006 in Antalya, Turkey

The 17th ITU Plenipotentiary Conference took place from 6 till 24 November 2006 in Antalya, Turkey,

ISSN 0085-7130

Sungate Port Royal Hotel. Taurus Mountains behind

hosted by the Telecommunication Authority of Turkey and was opened by the Prime Minister of Turkey, His Excellency, Recep Tayyip Erdoğan. The opening ceremony was also addressed by ITU Secretary-General, Yoshio Utsumi, and Turkey's Minister of Transport, Binali Yildirim. Almost 2000 delegates participated in the PP-06 from over 173 countries representing both government and the private sector as well as regional and international organisations.

In addition to the national delegations, there were observers from the United Nations and their specialised agencies, regional telecommunication organisations, intergovernmental organisations operating satellite systems and Sector Members. ETNO – the European Telecommunications Network Operator's Association – was represented as an observer.

This is the first time that the PP lasted for three weeks; previous PPs have had four weeks to finalise the work, and the time schedule was very tight. Elections of new top management attracted major attention as four of the five elected officials were outgoing and could not stand for reelection in their present elected post. Although elections started on Thursday in the first week of the conference, it took another week to finalise all the elections, and this clearly hampered the progress of the essential work which was handled in the Committees 5 and 6 and the Working Group of the Plenary. There is a growing tendency that the PPs become more and more politicised with issues such as elections taking too much time and attention.

Other issues high on the agenda of the PP-06 were questions relating to developing countries and countries with economies in transition, ITU's role regarding Internet, ITU's role in the follow up of the World Summit on the Information Society (WSIS), bridging the digital divide, the role of civil society in the work of the ITU, combating spam, enhancing cyber security and the finances of the Union.

3.1 The Tasks of the Plenipotentiary Conference

The tasks of the conference are laid down in Article 8 of ITU's Constitution

- To decide on the strategic direction of ITU and develop new policies that will shape the worldwide development of telecommunications and information and communication technologies (ICT);
- Adopt the ITU Strategic Plan which outlines the Union's orientations, goals and priorities for the period 2008–2011;
- Decide on the Union's Financial Plan that will provide the resources needed to meet the goals and deliverables set out in the Strategic Plan;
- Elect the Union's five highest-ranking officials: Secretary-General, the Deputy Secretary-General as well as Directors of the three Sectors of the Union: the Radiocommunication Bureau (BR), the Telecommunication Standardization Bureau (TSB) and the Telecommunication Development Bureau (BDT). The conference will also elect the members of the Council and of the Radio Regulations Board;
- Consider and adopt proposals for amendments to ITU's Constitution and Convention put forward by Member States;
- Treat proposals submitted by Member States to the PP-06.

3.2 Election of Chairman and Vice-Chairmen of the Conference

The Plenipotentiary Conference 2006 was very ably chaired by Dr. Tanju Cataltepe, Turkey, and Knut Smaaland, Norwegian Post and Telecommunications Authority, was elected as one of the five vice-chairmen. The vice-chairmen are elected on the basis of

Chairman and Vice-Chairmen of the Conference:

- Dr T. Cataltepe (Turkey) chairman

Vice-Chairmen:

- K. Smaaland (Norway)
- L. Reiman (Russian Federation)
- P. Mvouomo (Republic of Congo)
- H. Chono (Japan)
- M.J. Mulla (Saudi Arabia)

a fair geographical distribution among ITU's five administrative regions; viz. Region A – the Americas, Region B – Western Europe, Region C – Eastern Europe, Region D – Africa and Region E – Asia/ Australasia.

Dr Tanju Cataltepe, Turkey, Chairman of PP-06

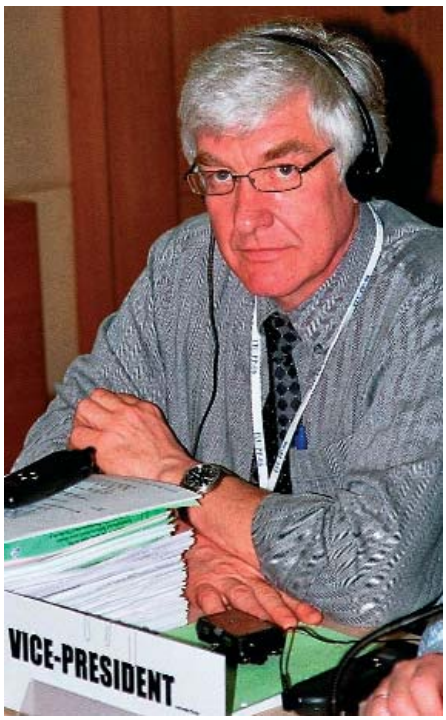
3.3 Structure of the Conference – Committees and Chairmen and Vice-Chairmen

The Plenipotentiary Conference has four statutory committees: the Steering Committee, the Credentials Committee, the Editorial Committee and the Budget Control Committee. In addition the PP-06 agreed to set up two substantive committees and one working group of the plenary:

- *Committee 5 – Policy and Legal Matters*
  To consider policy matters of the Union, to examine proposals for amending the Constitution and the Convention and to consider any other questions of a legal nature raised during the conference;

- *Committee 6 – Administration and Management*
  To consider the draft strategic plan, to prepare draft financial policies and a draft financial plan for 2008 – 2011;

- *Working Group of the Plenary on the World Summit on the Information Society (WSIS)*
  To consider issues related to the outcome of the WSIS and the Internet.



Knut Smaaland, Norwegian Post and Telecommunication Authority, Vice-Chairman of PP-06, Region B – Western Europe

Committee	Chairman
Committee 1: Steering Committee Composed of the chairman and the vice-chairmen of the conference and the chairmen and vice-chairmen of the other committees and of the Working Group of the Plenary	Dr. T. Cataltepe, Turkey
Committee 2: Credentials Committee	E. Ndukwe, Nigeria
Committee 3: Budget Control Committee	R. Gonzales Bustamante, Mexico
Committee 4: Editorial Committee	M.-T. Alajouanine. France
Committee 5: Policy and Legal Matters	K. Arasteh, Islamic Republic of Iran
Committee 6: Administration and Management	F. Riehl, Switzerland
Working Group of the Plenary on the World Summit on the Information Society	R.N. Agarwal, India

ISSN 0085-7130 ©Telenor ASA 2007

Marie-Thérèse Alajouanine, France, Chairman of the Editorial Committee (Committee 4)

4 Norwegian Delegation to the PP-06

The Norwegian delegation was headed by Eva Hildrum, Secretary General of the Ministry of Transport and Communications, and Ottar Ostnes, Director General, Ministry of Transport and Communications. Willy Jensen, Director General, Norwegian Post and Telecommunications Authority, and Jens C. Kock, Director, Ministry of Transport and Communications, were Deputy Heads of the Norwegian delegation. The delegation also included representatives from the Norwegian Post and Telecommunications Authority and Telenor ASA. Telenor was represented by Kjersti T. Hamborgstrøm, Telenor Satellite Broadcasting, and Anne Lise Lillebø, Telenor ASA.

Since the Plenipotentiary Conference is an intergovernmental conference, it is only open for direct participation from ITU Member States. Sector Members are only allowed to participate as observers without the right to speak. The representatives from Telenor were accepted by the Ministry of Transport and Communications to be members of the Norwegian delegation as delegates.

Members of the Norwegian Delegation

Member	Function	Affiliation
Eva Hildrum Secretary General	Head	Ministry of Transport and Communications
Ottar Ostnes Director General	Head	Ministry of Transport and Communications
Jens C. Koch Director	Deputy Head	Ministry of Transport and Communications
Willy Jensen Director General	Deputy Head	Norwegian Post and Telecommunications Authority
Knut Smaaland Special Adviser	Delegate	Norwegian Post and Telecommunications Authority
Kjersti Hamborgstrøm Manager	Delegate	Telenor Satellite Broadcasting
Anne Lise Lillebø Director	Delegate	Telenor ASA
Tom Dahl-Hansen Adviser	Delegate	Norwegian Post and Telecommunications Authority

5 Norwegian and Nordic Preparations to the PP-06

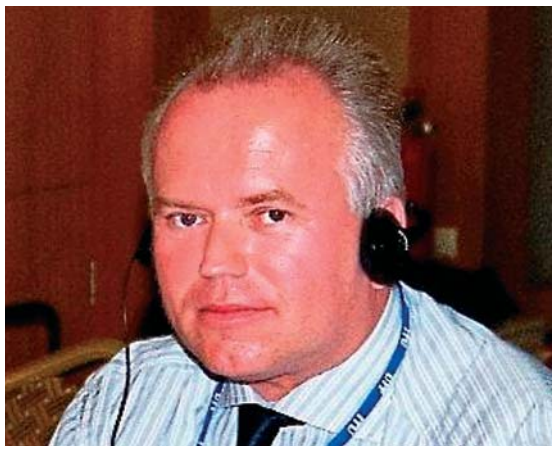
5.1 Norwegian Preparations

A preparatory meeting for the PP-06 was arranged by the Norwegian Post and Telecommunications Authority and the Ministry of Transport and Communications in July 2006 where all interested parties in Norway were invited to attend. NPT made a broad presentation of the CEPT European Common proposals (ECPs) and other relevant issues for Norway. Telenor participated in the meeting.

5.2 NITU

On the Nordic level, preparations for the PP-06 have been carried out in the NITU group (Nordic ITU cooperation) which normally meets once a year.

Eva Hildrum, Secretary General of the Ministry of Transport and Communications, Head of Norwegian Delegation



Ottar Ostnes, Director General, Ministry of Transport and Communications, Head of Norwegian Delegation

NITU is an informal group consisting of Nordic telecom regulators with representatives from the private sector invited to attend. For the last four-year period, NITU has been chaired by Norway in its capacity as ITU Council member in Region B (Western Europe). Telenor has taken part in these Nordic preparations together with representatives from the Ministry of Transport and Communications and the Norwegian Post and Telecommunications Authority. This time there were no Nordic contributions to the PP-06, as most of the preparations are done in a European context, and the Nordic countries have all been active in this work.

The Nordic countries (Denmark, Finland, Iceland, Norway and Sweden) have agreed on a rotation scheme regarding Nordic candidacies to the ITU Council. After a period of four years, Norway has decided to step down and the Nordic candidate for the Council in the next four-year period 2007 – 2010 is Sweden.

6 European Preparations for the PP-06

6.1 CEPT

Europe's regional organisation for post and telecommunications authorities CEPT – the European Committee for Post and Telecommunications with 47 member countries – has been in charge of the European preparations for the PP-06. The Electronic Communications Committee (ECC) of CEPT has a Working Group ITU dedicated to general ITU matters including the preparations for Council and the PP. Observers from APT, CITEL and ETNO have been invited to participate as observers in the meetings of the CEPT WG ITU, and this has proved very useful for the dissemination and exchange of information regarding the European positions for the PP-06.

The CEPT WG ITU set up a special Project Team – CEPT WG ITU PT PP-06 to prepare the PP-06. The PT PP-06 was chaired by Knut Smaaland, Norwegian Post and Telecommunications Authority. The aim of the comprehensive preparatory work is to develop European Common Proposals – ECPs – to be submitted to the PP-06 as European proposals. The PT PP-06 prepared comprehensive briefing material for the PP-06 and succeeded in agreeing on 28 ECPs which were all submitted as formal European proposals to the PP-06.

6.2 ETNO

ETNO - the European Telecommunications Network Operators' Association – has a Working Group ITU dedicated to overall ITU matters. The ETNO WG

Mr Dominique Würges, France Telecom; ETNO observer

ITU has been responsible for preparing the PP-06 on behalf of its members. The ETNO WG ITU is chaired by Dominique Würges, France Telecom, and has concentrated on issues of special interest to the ITU Sector Members such as the retention of the ratio between Member States contributions and the Sector Member contributions, no widening of the scope of the Union, enhanced efficiency of work of the Union, possible abolition of the International Telecommunication Regulations (ITRs), and ITU's role in a post WSIS environment. The ETNO WG ITU issued an ETNO Reflection Document on strategic development of ITU which was also submitted to CEPT PT PP-06 for consideration.

Anne Lise Lillebø, Telenor ASA and Kjersti Hamborgstrøm, Telenor Satellite Broadcasting – Delegates in the Norwegian Delegation

ISSN 0085-7130 ©Telenor ASA 2007

Members of the Norwegian Delegation: Eva Hildrum, Head, Ministry of Transport and Communications; Jens C. Kock, Deputy Head, Ministry of Transport and Communications; Knut Smaaland, Delegate, Norwegian Post and Telecommunication Authority

At the PP-06 in Antalya, ETNO was formally represented by Michael Bartholomew, ETNO Director, Thierry Dieu, Communications Manager and Dominique Würges, France Telecom, Chairman of the ETNO WG ITU.

6.3 Cooperation between CEPT and ETNO

The CEPT WG ITU and ETNO have agreed on a mutual exchange of observers, and ETNO observers were invited to attend all the meetings of the CEPT WG ITU and the PT PP-06. The cooperation between European telecom regulators and authorities and European telecom operators has taken place in a very good and transparent environment and has been highly appreciated by the private sector. Europe is one of the few regions that associates so closely its private sector to the preparation of the Plenipotentiary Conference and such cooperation is key to ensuring that the ECPs (European Common Proposals) are discussed among various stakeholders in Europe and that positions reflect market needs.

Members of the Norwegian Delegation: Willy Jensen, Deputy Head, Norwegian Post and Telecommunications Authority; Ottar Ostnes, Head, Ministry of Transport and Communications; and Jens C. Kock, Deputy Head, Ministry of Transport and Communications

6.4 The European Commission

The European Commission (EC) participates as councillor in the CEPT WG ITU and the PT PP-06 and the European Union has recognised CEPT as the competent body to carry out European preparations for major ITU conferences.

CEPT and the European Commission (EC) organised a joint workshop in Brussels on 19 October 2006 to inform embassies and diplomatic delegations in Brussels on CEPT and European preparations and policy views for the PP-06. ETNO was also invited to this workshop and Michael Bartholomew, the ETNO Director, made a presentation outlining ETNO views on PP-06 issues of interest to the private sector. This meeting was a good occasion for exchanging views on major issues prior to the conference and it provided the opportunity to explain the positions taken by CEPT.

7 Major Results from PP-06

7.1 General

As at previous conferences there was a lack of will to make decisions and a tendency to postpone decisions on important issues to the subsequent PP. Due to lack of consensus no financial plan was adopted and a number of issues such as the management and functioning of the Union, and the management of the budget will be studied by future Council Working Groups. On a positive note both ETNO and its members were fairly satisfied with the results regarding no change in scope of ITU's mandate, issues regarding Internet, the status quo of the system determining Sector Members' financial contributions and no change for the ITRs.

7.2 Elections of ITU's Top Management

The election of the Union's five highest-ranking officials, the members of the Radio Regulations Board (RRB) and the Council is one of the major tasks of the PP, and PP-06 saw a record high number of candidates for the elected posts. The incumbent Secretary-General, the Deputy Secretary-General, the Director of the Telecommunication Standardisation Bureau (TSB) and the Director of the Telecommunication Development Bureau (BDT) were not eligible for reelection, and there were a total of seven candidates for the Secretary-General, four candidates for the Deputy Secretary-General, four for the TSB Director and four candidates for the BDT Director. Only the director of the Radiocommunication Bureau (BR) was eligible for reelection, and he was not challenged by any contenders.

The PP-06 agreed to start elections on Thursday in the first week of the conference, and it took a whole

ISSN 0085-7130 ©Telenor ASA 2007

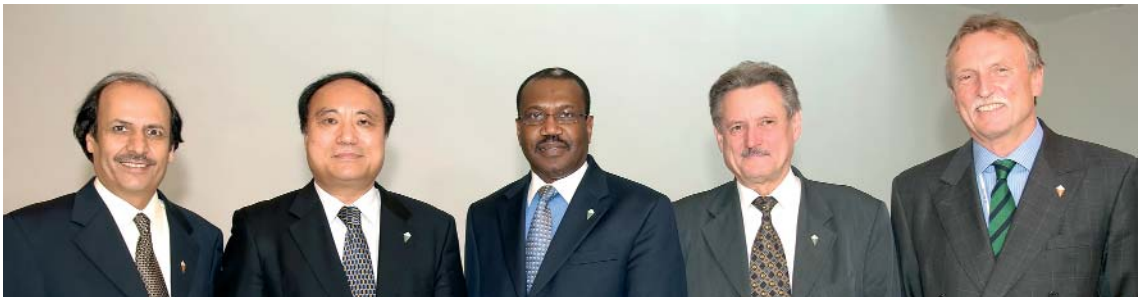


Photo: ITU/Jean-Marc Ferré

ITU's new top management. Left to right: Sami Al-Basheer, Director of Telecommunication Development Bureau; Houlin Zhao, Deputy Secretary-General; Hamadoun I. Touré, Secretary-General; Valery Timofeev, Director of the Radiocommunication Bureau; and Malcolm Johnson, Director of the Telecommunication Standardization Bureau

week to finalise elections of the top management, the RRB and the Council. Elections attract much attention, and despite good efforts from the chairmen of Committees 5 and 6, very little progress was made during this period. This is also due to the fact that many Member States with candidatures refrain from expressing views on contentious issues before the elections are finalised. From a Sector Member point of view this situation is detrimental to the progress of work and considerably reduces the efficiency of the conference. Out of three weeks, the main part of the job was performed in the last one and a half weeks!

Despite efforts to coordinate European candidatures, there were two European candidates for the post of Secretary-General, one European candidate for the Deputy Secretary-General and two European candidates for the TSB Director. This was a very difficult situation for Europe and in our opinion, it strongly weakened the possibilities of having Europeans elected to any of the four posts that were to be filled.

7.2.1 Secretary-General and Deputy Secretary-General

Hamadoun Touré from Mali was elected as Secretary-General in the third round of voting with a majority 95 votes out of 155 Member States present and voting. The required majority for election was 78 votes. Mr Touré has already served eight years as the Director of the BDT. The CEPT candidate, Mathias Kurth from Germany, received 60 votes, whereas the other European candidate, Marc Furrer from Swizerland, withdrew his candidature after the second round.

Houlin Zhao, People's Republic of China, was elected as Deputy Secretary-General by a landslide majority of 93 votes in the first round of voting. The European candidate, Carlos Sanchez from Spain, received 34 votes. Mr Zhao is outgoing Director of TSB where he has served for two terms, totalling eight years.

7.2.2 Bureau Directors

BR – Radiocommunication Bureau

Valery Timofeev from the Russian Federation was reelected as Director of the Radiocommunication Bureau in the first round. There was no candidate challenging Mr Timofeev and he received almost unanimous support from the Plenipotentiary.

TSB – Telecommunication Standardization Bureau

Malcolm Johnson of UK was elected as Director of the Telecommunication Standardization Bureau (TSB) in the third round. The other European candidate, Mr Bigi from Italy, withdrew after the first round. This election turned out to be a thriller with a close race among the remaining candidates. Mr Johnson was elected with 83 votes against 79 votes for the Japanese candidate Mr Inue. From a Sector Member point of view, we believe that Mr Johnson is well positioned to take up the challenging task of managing the TSB. For many years Mr Johnson has been an active proponent for changing TSB's way of working with the aim of speeding up activities and increasing the role of the private sector. Mr Johnson's experience of reform work of ITU will serve as a good basis for his challenging tasks in the TSB.

BDT – Telecommunication Development Bureau

Sami Al-Basheer of Saudi Arabia was elected as Director of the Telecommunication Development

ITU's top management team 2007 – 2010

Post	*Elected candidate*
Secretary-General	Hamadoun Touré, Mali
Deputy Secretary-General	Houlin Zhao, People's Republic of China
Director, Radiocommunication Bureau (BR)	Valery Timofeev, Russian Federation
Director, Telecommunication Standardization Bureau (TSB)	Malcolm Johnson, United Kingdom
Director, Telecommunication Development Bureau (BDT)	Sami Al-Basheer, Saudi Arabia

ISSN 0085-7130

Valery Timofeev, Russian Federation, re-elected BR Director, with the author

Sector (BDT) in the third round of voting with a total of 91 votes while his contender Patrick Masambu, Uganda, received 70 votes.

ITU's new management team will serve for the four-year period 2006 – 2010 and PP-06 decided that the new officials will take up their duties on 1 January 2007.

7.2.3 Elections to the Council

At present there are 46 seats at the ITU Council reflecting Article 4 in the Convention that the number shall not exceed 25 per cent of the total number of Member States. The seats are distributed among the five administrative regions of the Union as follows:

- Region A – Americas (8 seats)
- Region B – Western Europe (8 seats)
- Region C – Eastern Europe (5 seats)
- Region D – Africa (13 seats)
- Region E – Asia/Australasia (12 seats)

In Region B – Western Europe – there were nine candidates for eight seats. Norway has been a member of Council in Region B for the past four-year period, but based on the Nordic rotation scheme, Norway had decided to step down and Sweden was this time the Nordic candidate for Council in Region B. Sweden was elected with a comfortable number of votes and will serve on the Council for the next four-year period up to the next Plenipotentiary in 2010. Once more United Kingdom failed to be elected as member of the Council.

Telenor is pleased to see that the Nordic countries – through Sweden – managed to keep a seat on the ITU Council. If needed, matters of interest to our company within the remit of Council can be taken up in the Nordic cooperation group NITU, and provided that there is agreement among the Nordic Member States, this can be brought to Council by Sweden. One example of such matters is the Council Decision to open a trial of offering free electronic access to ITU-T Recommendations in 2007.

In Region C – Eastern Europe – there were eight candidates for five seats. In the elections held on 16 November, Ukraine and Poland received 94 votes each, and a second ballot took place on 17 November to determine the fifth member of the Council for Region C. In the second ballot Ukraine received 77 votes and Poland 69 votes.

From Telenor's point of view, we highly appreciate the fact that some of the countries where Telenor has mobile operations have been elected to the Council. In Region C, this applies to the Russian Federation and Ukraine and in Region E – Asia/Australasia, to Thailand, Malaysia and Pakistan.

7.2.4 Elections to the Radio Regulations Board (RRB)

The Radio Regulations Board has a total of 12 members based on a geographical distribution among ITU's administrative regions:

- Region A – Americas, 2 seats,
- Region B – Western Europe, 2 seats
- Region C – Eastern Europe, 2 seats
- Region D – Africa, 3 seats
- Region E – Asia and Australasia, 3 seats

Since Telenor has important mobile operations in Pakistan and Malaysia we note with pleasure that the candidates from these two countries were elected as members of the RRB in region E.

The results of the elections to Council for Region B – Western Europe (8 seats)

Country	*Votes*
France	140
Spain	134
Switzerland	133
Germany	132
Sweden	132
Italy	123
Portugal	121
Turkey	120

The results of the elections to Council for Region C – Eastern Europe (5 seats)

Country	*Votes*
Russian Federation	135
Romania	102
Bulgaria	99
Czech Republic	96
Ukraine	77

7.3 The European Common Proposals – ECP – Results at PP-06

CEPT Member States had submitted a total of 28 European Common Proposals (ECPs) to the PP-06. CEPT members were pleased to see that a number of ECPs were accepted by the conference. In the following focus will be on ECPs of interest to Sector Members who are members of ETNO:

ECP no 5: Sector Members observers at Council

In this ECP CEPT seeks to clarify the status of Sector Members being observers and proposes to delete the text stating that Sector Members "may be represented at meetings of the Council, ..." as it is difficult to see how a few Sector Members can represent such a diversified group as Sector Members in the three sectors of the ITU. PP-06 agreed to this deletion, and replaced "represented" by "attend" and the updated text reads as follows: "Sector Members may attend, as observers, in meetings of the Council, ...". The new text has been added to No 60B, Article 4 in the Convention. ETNO Sector Members agree with this amendment.

ECP no 8: International Telecommunication Regulations – ITRs

The current ITRs were adopted by ITU's World Administrative Telegraph and Telephone Conference (WATTC) in Melbourne in 1988. The agreed treaty represented a very delicate compromise between the countries that had just started on market liberalisation and the developing countries. The most important of the articles of the ITRs from 1988 concern "Charging and accounting" (of international telecommunications), the "International network" and "International services".

The need for a review of the ITRs was considered by the Plenipotentiary Conferences in Minneapolis in 1998 and in Marrakesh in 2002. The PP in Marrakesh resolved that Council should set up a Council Working Group (CWG) to undertake a review of the ITRs and report back to PP-06. However, this CWG did not reach any consensus and presented three different views on a possible way forward: to leave the ITRs unchanged, to amend the ITRs including adding new provisions, or to terminate the ITRs and transfer certain provisions to the CS, CV and ITU-T Recommendations.

Most European countries consider that the ITRs in their present form are substantially out of date. The ITRs no longer reflect the major commercial and operational changes which have taken place since then, especially the widespread liberalisation of telecommunications services and the competitive international telecommunications environment.

Marianne Treschow, Director-General, National Post and Telecom Agency, Deputy Head of Swedish Delegation

The European proposal to PP-06 was based on the view that the current ITRs no longer serve the purpose for which they were designed. The ECP on the ITRs proposes the following:

- ITU-T should identify the operational issues in the ITRs and if possible, develop ITU-T Recommendations for approval by the World Telecommunication Standardization Assembly in 2008 (WTSA-08);
- Further to identify which parts of the ITRs that merit treaty level status and those which are redundant (already covered in the CS/CV or obsolete);
- WTSA-08 (World Telecommunication Standardization Assembly) should make recommendations to the PP-10 on any further action including the possible termination of the ITRs;
- A decision on a possible WCIT (World Conference on International Telecommunications) should be postponed until the PP-10.

A future Plenipotentiary Conference should be given the explicit authority to terminate the ITRs. In Europe's view the holding of a WCIT is very costly and would put additional strain on the tight budget of the Union.

As a Sector Member and telecommunications operator Telenor fully supported the CEPT view in this matter. ETNO members are in favour of authorising a future Plenipotentiary Conference to revise and possibly terminate the ITRs and to transfer relevant provisions of the ITRs to the CS/CV. As an alternative ETNO members could also accept to keep status quo. However, ETNO members are opposed to the idea of

The results of the election of the Radio Regulations Board

RRB members 2007 – 2010:

Region A: Americas (2 seats)
Julie Napier Zoller, United States
Robert W. Jones, Canada

Region B: Western Europe (2 seats)
Mindaugas Zilinskas, Lithuania
Martine Limoudin, France

Region C: Eastern Europe (2 seats)
Baiysh Nurmatov, Kyrgyzstan
Wladyslaw Moron, Poland

Region D: Africa (3 seats)
Hassan Lebbadi, Morocco
Shola Taylor, Nigeria
Aboubakar Zourmba, Cameroon

Region E: Asia and Australasia (3 seats)
Ali Ebadi, Malaysia
Shahzada Alam Malik, Pakistan
P.K. Garg, India

a World Conference on International Telecommunications which is believed to open up the possibility of expanding the scope of the Union and introduce new regulation for Internet and mobile telecommunication.

This issue turned out to be one of the most contentious questions of the PP-06. Many Member States from Asia were in favour of launching yet another study of the provisions of the ITRs and wanted to postpone any decision regarding the instrument to the PP-10. While a number of Member States from the Americas wanted to retain the ITRs as is, there was a great majority of Member States from the Arab countries, Africa and certain developing countries that wanted to retain the ITRs and to amend the instrument to cover new areas.

The results of the discussions are embedded in Resolution COM5/4 "Review of the International Telecommunication Regulations": The resolution concludes as follows:

7Nordic team: Anders Frederich, Deputy Head, Swedish Delegation; Kjersti Hamborgstrøm, Delegate, Norwegian Delegation; and Jørn Jensby, Delegate, Danish Delegation

- ITU-T should undertake a review of the existing ITRs in cooperation with the other sectors, with ITU-T as the focal point. The World Telecommunication Policy Forum (WTPF) scheduled for 2009 is tasked to deal with Internet related issues, convergence and NGN. The WTPF will prepare reports and possibly opinions for consideration by ITU members.

- A World Conference on International Telecommunication (WCIT) will be convened in Geneva in 2012.

- The Council is instructed to adopt the agenda of this WCIT by 2011 and urges the sectors to carry out studies within their field of competence to prepare for the WCIT.

ITU's legal adviser informed that according to his interpretation of the CS/CV it is not appropriate for a PP to have the authority to terminate the ITRs. This can only be carried out by the legal entity which created the treaty. However, a PP can transform itself into a WCIT during or after a PP if the Member States agree to this.

CEPT members found that the compromise solution in Res COM5/4 was acceptable as a possible WCIT was postponed for another six years. The next PP in 2010 can postpone it further, if so agreed. The outcome of this issue will be a challenge to the ITU Member States especially as regards the financial consequences for the Union. Considerable preparations are required in order to hold a WCIT, and in our opinion, it is questionable whether the result will benefit the future work of ITU. From a Sector Member's point of view it is positive that there will be no change regarding the ITRs in the next six years. The whole question will come up for debate at the PP-10, and no-one can predict the development within the telecommunications field in this timeframe. It is to be hoped that the world has changed and that more Member States will understand that the ITRs are not an adequate way of regulating international telecommunications and that such countries will be able to support Europe and other countries in their efforts to abrogate the ITRs.

ECP no 11: TELECOM

The TELECOM exhibitions operate in a very competitive environment, and Europe proposes to remove the distinction between regional and worldwide TELECOM exhibitions and forums as the distinction is no longer considered relevant in the present economic

context. In the ECP it is proposed that ITU should only organise world TELECOMs which could rotate in the ITU Regions. Europe also sees a need for more transparency concerning the TELECOM Board and proposes that the Secretary-General's proposal for the composition of the Board should be approved by the ITU Council. In the ECP it is also stressed that the TELECOM events should be financially successful.

ETNO supported the CEPT proposal and underlined the commercial role of TELECOM exhibitions and that they should be organised according to market demand and not be driven by geographical or political considerations.

It turned out that this was a very sensitive issue, especially for developing countries and countries with economies in transition. It was argued that regional events would bring the potential benefits of telecommunications closer to the people of all continents by focusing on regional problems and proposing solutions adapted to local environment. The European proposal to merge world and regional TELECOM into a single global event was not supported.

The PP-06 concluded in Resolution 11 "World and regional telecommunication/information and communication technology exhibitions and forums" that ITU should continue to organise world and regional TELECOM exhibitions and forums on a regular basis, taking due account of the need to ensure the financial success of such exhibitions. The principle of rotation is retained and now it also applies to world events when several countries have submitted competitive offers. The resolution stresses the importance of having a transparent process open to all interested parties in the selection of the venue for world ITU TELECOM events. When selecting the venue the financial viability of the event should be considered as well as the results of market and feasibility studies. The composition of the Board is to be approved by Council.

It is noted that the final resolution supports the continuation of both world and regional events. Consideration of financial viability and the transparency in the selection of the venue of world events including a rotation system for deciding on the venue of regional ITU TELECOM events are welcomed by the private sector

ECP no 12: The future role of ITU in implementing the outcomes of the World Summit on the Information Society (WSIS)

The first session of the WSIS was held in 2003 and resulted in a WSIS Geneva Declaration of principles and the Geneva Plan of Action which focuses on ITU core functions of importance to the information society such as assistance in bridging the digital divide, fostering regional and international cooperation, spectrum management and development of standards.

The second phase of WSIS was held in Tunis in 2005 and adopted the Tunis Commitment and the Tunis Agenda for the Information Society where specific action lines were identified. There will be a multi-stakeholder implementation of the Geneva Plan of Action and the Tunis Agenda, and ITU was identified as possible moderator/facilitator for action line C2 (information and communication infrastructure) and C5 (building confidence and security in the use of ICTs) of the Tunis Agenda and as a potential partner for a number of other action lines (C1, C3, C4, C6, C7 and C11). Attention is also drawn to the WTDC-06 (World Telecommunication Development Conference) in Doha which adopted Resolution 30 on "The role of the ITU-D in implementing the outcomes of the WSIS".

The draft Resolution text proposed by Europe opens up the possibility of a structured and focused approach to implement the action lines identified as priorities and calls for the deployment of ITU expertise. It is pointed out that the implementation of the WSIS outcomes can be done within the current mandate of the ITU. The proposal also emphasises the need for partnerships with actors outside the ITU towards delivering WSIS outcomes.

The PP-06 agreed on Resolution GT-PLEN 6 on "ITU's role in implementing the outcomes of the World Summit on the Information Society" which reiterates ITU's commitment to take part in the multi-stakeholder follow up of WSIS and acknowledges ITU's special role as moderator/facilitator for implementing action lines C2 and C5 and requests the Council to oversee ITU's implementation of the WSIS outcome. PP-06 requests the Council to maintain the Council Working Group on WSIS – CWG WSIS – to facilitate guidance on the ITU implementation of relevant WSIS outcomes.

The agreed resolution captures Europe's views on the role that ITU may be able to play post-WSIS and recognises ITU's existing role. ETNO fully concurs with the European position that ITU's role in the follow up of WSIS can be done within its present mandate and does not see any need for widening the scope of the Union or change its name. ETNO also supports the creation of the Internet Governance Forum (IGF) agreed by the second session of the WSIS. IGF should be seen as an excellent opportunity for effective multi-stakeholder involvement in policy shaping, recognising the shared responsibility of all stakeholders.

Ian Hutchings, Head, New Zealand delegation, and Kjersti Hamborgstrøm, Delegate, Norwegian Delegation

ECP no 13: "Clarification of the responsibilities of the SG in the management of the Union and the discontinuation of the Coordination Committee"

The proposal calls for greater clarity with respect to the roles of the Secretary-General, the Deputy Secretary-General and the Directors of the three Bureaux. The CS and CV should clearly state that the Secretary-General is responsible for the overall management of the Union's resources and is accountable for this to the Council. According to the current Article 6 of the Convention, decisions can only be taken by consensus between the elected officials. This can in fact hamper decisive management and can result in Council being forced to take management decisions which should properly be for the officials of the Union. With such a clarification of the roles, Europe proposes to discontinue the Coordination Committee.

Although this ECP does not directly affect Sector Members, ETNO supported the general thrust of the proposal: to streamline management procedures among the ITU elected officials and to avoid unnecessary bureaucracy.

There was no consensus on the CEPT proposal, but elements of this ECP are included in another Resolution (Res COM5/5) which is treated in the following paragraph regarding ECP No 14.

ECP No 14: Appointment rather than election of the Directors of the Bureaux

This question is a recurrent issue and has been on the slate for a number of years. In contrast to most UN agencies that have two elected officials, ITU has a total of five elected officials. The existing arrangement of five elected officials politicises the management of the organisation and creates a lack of clarity as to who is accountable for the decisions made. Europe finds that this federal structure adds to the complexity in the management of the Union and compromises its efficiency.

Instead Europe favours a system of two elected officials: the Secretary-General and the Deputy Secretary-General. It is proposed that the Bureaux Directors should be appointed according to usual UN practice. Europe proposed to establish a Council Working Group to consider the change to an appointment process.

ETNO members have for many years argued that the Bureaux Directors should be appointed based on a professional job description. Although the present CEPT proposal goes in the right direction, ETNO would have preferred that the present PP-06 should decide on the matter instead of leaving the issue to a Council Working Group. This means that a decision can first be taken by the PP in 2010 and any implementation of a possible decision would take place for the PP in 2014.

Unfortunately there was very little support for this European proposal at the PP-06. Member States from the Americas, Africa and Asia-Pacific agreed that the status quo with five elected officials functioned in a good manner and that there was no need to change the system. From a Sector Member's point of view this is surprising when account is taken of discussions in Council on how to manage the Union and all the time spent on arranging elections of elected officials at the PP-06. Elections of the five officials were terminated on Thursday in the second week. As attention was concentrated on the elections, work in the committees suffered from lack of commitment and important decisions were deferred till after the elections. Some Administrations were clearly reluctant to discuss contentious issues as this might have an impact on the pending elections. With fewer elections to perform the work of the PP could be done in a more efficient manner and the duration of the PP could even be reduced.

The PP-06 agreed to cover issues regarding responsibilities and accountability of the elected officials, the Coordination Committee, the elections of the elected officials and reporting in the Union in Resolution COM5/5 "Study on the management and functioning of the Union". The Resolution resolves that the Council should conduct a study aiming at overall improvement of the efficiency of ITU management, addressing the following issues:

- Reporting structure in the Union
- Role, accountability, number and tenure/term of office of elected officials
- Functioning of the Coordination Committee
- Election procedures
- Responsibility, accountability and transparency of the advisory groups.

Telenor notes that this study is only open for the participation of Member States. In our view this limitation of participation is not very constructive and actually prevents the Sector Members from discussing the functioning of the advisory groups in the three sectors where they can participate directly in their capacity as Sector Members.

ECP No 16 "Follow-up of Resolution 110 (Marrakesh, 2002) (Review of the contribution of Sector Members towards defraying the expenses of the International Telecommunication Union) – Reduction of time of denunciation of Sector Members
Following Resolution 110 from PP-02, a Council Working Group reported its findings to the Council 05:

- The period of time recommended from the date when the notification of the denunciation of a Sector Member has been received by the Secretary-General is proposed to be reduced from one year to six months. The same provision will also apply for Associates. This is supported by Europe. In addition, European countries propose to modify CV480 to allow Sector Members to decrease their class of contribution in case of exceptional circumstances.

The aim of the proposal is to improve the financial oversight of Sector Members and Associates to the benefit of the financial stability of ITU.

The PP-06 agreed to these proposals and CV240 and CV480 have been modified accordingly. The conference also adopted Resolution COM6/3 "Improvement of management and follow-up of the defrayal of ITU expenses by Sector Members and Associates". Resolves 2 in this Resolution lays down that "in case of a merger between Sector Members or Associates of the same Sector, duly notified to the Secretary-General, No. 240 of the Convention shall not apply and shall thus not have the effect of requiring the Sector Member or the Associate resulting from the merger to pay more than one contribution for its participation in the work of the Sector concerned."

As a Sector Member Telenor welcomes these modifications which are better adapted to the rapid pace of the market and the financial realities faced by private-sector entities.

ECP No 17 "The terms of office of the elected officials"
In line with the current provisions elected officials are re-eligible to the same post only once, but there is no limit for an elected official presenting his candidature for one of the other four elected posts when he has finalised his two possible terms. In theory, the same person can remain in elected posts for 40 years! This prevents the possibility of having new people with fresh ideas in the management of the Union. Europe proposes changes to Article 2, No 13 of the Convention to cover this point.

Although elections are the responsibility of the Member States, the ETNO Sector Members welcomed this proposal. In our opinion, all members of ITU will benefit from a competent and efficient management, and all organisations need a degree of renewal in their management teams.

This proposal turned out to be very controversial, but after extensive discussion the European proposal was supported and the PP-06 agreed to modify Article 2, No 13 of the Convention as follows: "Elected Officials: …., and they shall be eligible for re-election once only for the same post. Re-election shall mean that it is possible for only a second term, regardless of whether it is consecutive or not".

ECP No 20: "Resolution 130 of Marrakesh on the role of ITU in information and communication network security" – Cybersecurity and combating spam
The Resolution from Marrakesh addresses ITU's role in information and communication network security. Since 2002 new threats have emerged with the global development of Internet such as spam, protection of personal data, privacy, intellectual property protection, fight against illicit content etc. that could threaten the security and stability of telecommunications networks. The World Telecommunication Standardization Assembly (WTSA) in Florianopolis in 2004 adopted two resolutions on the issue of spam: combating spam and countering spam by technical means. The second session of the WSIS in Tunis in 2005 also underlined the importance of security in ICTs in its Agenda of Tunis and established Action Line C5 "Building confidence and security in the use of ICTs" where ITU is identified as the moderator/

Wearing the same jackets from PP-98: Houlin Zhao, Deputy Secretary-General Elect, People's Republic of China, with the author

Eva Hildrum, Head of Norwegian Delegation

facilitator for this WSIS Action Line. The World Telecommunication Development Conference (WTCD) in Doha 2006 also identified cybersecurity as a priority activity of the BDT.

Europe proposed to extend the scope of Resolution 130 from Marrakesh to cover all aspects concerning possible threats to the stability and security of networks.

The PP-06 agreed to update Resolution 130 and decided on a new title: "Strengthening the role of ITU in building confidence and security in the use of information and communication technologies". The updated resolution instructs the Director of the Telecommunication Development Bureau (BDT) to develop, consistent with the results of WTDC-06 and the subsequent meeting pursuant to Resolution 45 (Doha, 2006) of that conference, the projects for enhancing cooperation on cybersecurity and combating spam responding to the needs of developing countries, in close collaboration with the relevant partners. Members are invited to develop the necessary relevant legislation and reference is made to regional initiatives such as the Council of Europe's Convention on Cybercrime. Finally the Directors of the three Bureaux are encouraged to pursue the work of security of ICTs in the respective Study Groups, relevant projects and to continue collaboration with relevant organisations.

It is expected that increased focus will be put on issues regarding security in ICTs and the role that ITU can play on the world scene.

ECP 21: "Updating and fusion of Resolution 102 of Marrakesh on the Management of Internet Domain names and Addresses and Resolution 133 of Marrakesh on the Role of administrations of Member States in the management of internationalized (multilingual) domain names"

In the wake of the WSIS, it is necessary for ITU to reassess how the Union can contribute to the realisation of the Tunis Agenda based on its expertise and recognised mandate. CEPT proposed to update Res 102 of Marrakesh dealing with IP addresses and domain names and to integrate Res 133 of Marrakesh about implementation of IDNs (Internet Domain names) into Res 102 to have only one resolution dealing with Internet resources as a whole. The proposed new resolution on Internet resources invites ITU to contribute constructively to the work on Internet governance. ITU should follow the work of the Internet Governance Forum (IGF) established by the second phase of the WSIS in Tunis in 2005. ITU is requested to improve its cooperation with relevant organisations and to participate in the development of globally-applicable principles on public policy issues related to the coordination and management of Internet resources.

There was no consensus on merging the two resolutions, but the resolutions were updated to reflect the recent development within this area after the two phases of the WSIS.

The PP-06 agreed on an updated text of Res 102 reflecting a number of CEPT's points. The updated resolution 102 is called "ITU's role with regard to international public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses". The Resolution refers to the role given to ITU in this area: that ITU is dealing with technical and policy issues related to IP-based networks including the Internet and evolution to NGN, ITU's development of ENUM, internationalised domain name and country code top-level domain (ccTLD) and emphasises that ITU should start a process of enhanced cooperation with all stakeholders in accordance with the Tunis Agenda. The Secretary-General is instructed to organise consultations on these issues among the ITU members and other stakeholders and submit propos-

als to the Council 2007 through the Council Working Group on WSIS.

Likewise, Resolution 133 "Role of administrations of Member States in the management of internationalised (multilingual) domain names" was updated. The Resolution refers to the Geneva Action Plan and the Tunis Agenda of the WSIS to advance the process for the introduction of multilingualism in a number of areas including domain names and instructs the Secretary-General to take an active part in all international discussions and initiatives on the deployment and management of internationalised Internet domain names, in cooperation with relevant organisations such as WIPO and UNESCO.

The two updated resolutions are somewhat enlarged, and seen from a Sector Member perspective, it is important that responsibilities taken on by ITU in these resolutions fall within its present mandate.

ECP No 23: "Cross-references between the CS/CV and the Radio Regulations"

In this proposal it is pointed out that the definitions of the broadcasting service and the mobile service are both in the Constitution and the Convention and in the Radio Regulations whereas all other service definitions are in Article 1 of the Radio Regulations. By deleting the definitions in the CS/CV, future WRCs will have the possibility of updating the definitions if necessary taking into account the development of convergence between different telecommunications services and without being bound by provisions in the CS/CV. Many European Sector Members were in favour of this proposal, as it would remove an obstacle to a possible change in the Radio Regulations if a future WRC should agree on changes in the definitions. However, the proposal to delete the definitions of broadcasting and mobile service from the Constitution and Convention was not very well received and did not obtain enough support to go forward.

ECP 25 Gender mainstreaming in ITU

CEPT countries proposed to amend Resolution 70 from Marrakesh in order to reflect Resolution 55 adopted by the World Telecommunication Development Conference (WTDC) in Doha, 2006, promoting gender equality towards all-inclusive information societies.

PP-06 agreed to revise Resolution 70 "Gender mainstreaming in ITU and promotion of gender equality towards all-inclusive information societies" endorsing Resolution 55 (Doha, 2006) on promoting gender equality towards all-inclusive information societies; to continue the work being done at ITU, and particularly in BDT, to promote gender equality in ICTs by

Kirsten Bak, Head, Danish Delegation

recommending measures at the international, regional and national level on policies and programmes that improve socio-economic conditions for women, particularly in developing countries; and to incorporate the gender perspective in the implementation of the ITU strategic plan and financial plan for 2008-2011 as well as in the operational plans of the Bureaux and the General Secretariat.

7.4 Budget and the Financial Plan

One of the main tasks of the Plenipotentiary Conference is to establish a basis for the budget of the Union and determine related financial limits. This implies establishing the total number of contributory units for the period up to the next Plenipotentiary Conference on the basis of the classes on contribution announced by Member States. For the past four years the financial situation of the Union has been extremely strained, and the Secretary-General has been forced to implement a number of cost saving schemes to balance income and expenditure. These measures include a system of results-based budgeting, operational planning and time-tracking, the introduction of cost recovery, and reforms to the secretariat and the business model of TELECOM.

7.4.1 Decision 5 "Income and expenditure for the Union for the period 2008 to 2011"

The definitive choice of class of contribution by Member States is made before the end of the conference. Sector Members may choose their class of contribution within a period of three months after the Conference. The Plenipotentiary Conference shall adopt the definitive Financial Plan including the upper limit of the value of the contributory unit which will serve as basis for establishing the budgets to be adopted by the Council during the financial period concerned.

It is noted with dismay that the PP-06 did not manage to adopt the financial plan for the next four-year period due to lack of consensus.

However, PP-06 adopted Revised Decision 5 "Income and expenditure for the Union for 2008 to 2011" with a total expenditure of CHF 664 million, a negative balance of CHF 39 million.

The upper limit of the amount of contributory unit of Member States for the years 2009 – 2011 shall be CHF 330,000; for the years 2008 – 2009 the contributory unit of Member States shall not exceed CHF 318,000 and a cap of CHF 85 million for the years 2008 – 2011 was set for expenditure on interpretation, translation and text processing regarding the six official languages of the Union. This means that the upper limit of the amount of the Member State contributory unit remains the same as for the previous plenipotentiary period.

The Decision contains 18 options for reducing expenditure, including

- Limitation of the number of Study Group meetings and their duration;
- Limitation of the number of days for the advisory groups to three days per year maximum. Additional meetings may be held on a cost recovery basis; i.e. costs are financed by the requesting Sectors;
- Cost savings through better management of the ITU regional presence;
- Reduction in the cost of documentation of conferences and meetings;
- Consideration of savings in languages (translation, interpretation) for Study Groups meetings and publications;
- Reduce the number of meetings of the RRB from four to three per year.

7.4.2 Ratio Between Member States and Sector Members' Contributions

Two options of the quadrennial Draft Financial Plan for the period 2008 – 2011 were proposed. The only difference between the two is the ratio for determining the contributory unit payable by Sector Members. Option 1 is based on the current ratio of one fifth of the contributory unit paid by Member States. Option 2 reflects a revision of the ratio to one fourth of the contributory unit paid by Member States. Option 1 indicates a shortfall of income of CHF 33.3 million whereas Option 2 indicates a shortfall of income of CHF 12 milllion.

A number of Member States supported a change in the ratio between Member States and Sector Members' contributions from one fifth to one fourth, representing an increase of 24 % of the value of the Sector Member unit of contribution. It was argued that the contributory unit of Sector Members did not cover the direct costs of their participation in the Sectors, and that Sector Members should pay more in line with their alleged increased rights over the last few years.

ETNO members were strongly against this unilateral increase of Sector Members' contributions only and cautioned that instead of generating more income to the sectors, such an increase could lead to Sector Members leaving the sectors or that they might prefer to go into national delegations instead. Attention was drawn to the vast contribution made by Sector Members in the work of the sectors which should be taken into account when assessing the contribution of Sector Members. It would be a very negative sign to the outside world if ITU should decide to only increase the contributions from the private sector in an effort to balance its budget.

After a lengthy and very heated debate, the ratio will not be changed at this juncture.

7.5 The Strategic Plan 2008 – 2011

The Strategic Plan for the Union for 2008 – 2011 was adopted in Resolution 71.

The resolution points to the many developments that have taken place in the telecommunication and the information and communication technology (ICT) environment that have significant implications for ITU as a whole. A total of seven goals are listed in the strategic plan:

Goal 1: Maintaining and extending international cooperation among all Member States and with relevant regional organizations for the improvement and rational use of information and communication infrastructure of all kinds, taking the appropriate leading role in United Nations system initiatives on ICTs, as called for by the relevant WSIS outcomes.

Goal 2: Assisting in bridging the national and international digital divides in ICTs, by facilitating interoperability, interconnection and global connectivity of networks and services, and by playing a leading role, within its mandate, in the multistakeholder process for the follow-up and implementation of the relevant WSIS goals and objectives.

Goal 3: Widening the Union's membership, extending participation and facilitating cooperation of an increasing number of administrations and organizations, as well as new actors, such as relevant WSIS stakeholders.

Goal 4: Developing tools, based on contributions from members, to promote end-user confidence, and to safeguard the efficiency, security, integrity and interoperability of networks.[1)]

Goal 5: Continuing to improve the efficiency and effectiveness of ITU's structures and services and their relevance to the requirements of membership and the wider global community.

Goal 6: Disseminating information and know-how to provide the membership and the wider community, particularly developing countries, with capabilities to leverage the benefits of, *inter alia*, private-sector participation, competition, globalisation, network security and efficiency and technological change in their ICT sector, and enhancing the capacity of ITU Member States, in particular developing countries, for innovation in ICTs.

Goal 7: Promoting the development of an enabling environment that assists governments in fostering supportive, transparent, pro-competitive, harmonized and predictable policies, as well as legal and regulatory frameworks that provide appropriate incentives for investment in, and development of, the information society.

7.7 Radio Related Matters

7.7.1 Implementation of Additional Corrective Measures Relating to Cost Recovery for Satellite Network Filings – Decision COM6/1

As a satellite operator Telenor has taken particular interest in this issue which has been discussed for a number of years in the Council and at various PPs. With the recent decisions made by Council 05, it is clear that certain invoices for Satellite Network Filings had been issued on an incorrect basis. However, since the accounts were already drawn up, only the PP has the authority to cancel invoices in ITU.

In Decision COM6/1 "Implementation of additional corrective measure relating to cost recovery on satellite network filings" the PP-06 decided to implement the corrective measures set forth in the Council-05 Decisions 531, 532 and 534 and in the RRB decision

Marianne Treschow, Deputy Head of Swedish Delegation, and Jørn Jensby, Delegate, Danish Delegation

(41st meeting, Geneva, 4-8 September 2006) in respect of invoices issued for the 2002-2003 period.

However, there was no agreement on the issue of cancelling unpaid invoices, and the issue was deferred to Council together with the delegation of competence to write off the debt in this area.

7.7.2 Resolution 86 (Rev Marrakesh) Processing Charges for Satellite Network Filings and Administrative Procedures

PP-06 discussed Resolution 86 at length and decided that WRC-07 should consider the matter and report to the next Plenipotentiary Conference as to whether R86 should be deleted or updated.

7.7.3 Periodicity of WRCs and RAs

The periodicity of WRC and RA was discussed and extended from two to three to three to four years. CS Article 13 "Radiocommunication Conferences and Radiocommunication Assemblies" has been changed accordingly (MOD 90, 91). The change reflects the current situation where it is not feasible to finalise the comprehensive preparations for a WRC within a time limit of two to three years. Another reason for prolonging the periods between the WRCs is also the very difficult financial situation of the Union. It is only possibly to sustain one major conference of the year without seriously affecting the balance of the budget.

7.8 Advisory Groups

A proposal from the United States to align the provisions in the Convention regarding the advisory groups in the three sectors caused considerable debate. Although the proposal might seem to be a simple alignment, it could have great impact on the way the TSAG – the Telecommunication Standardization Advisory Group – is working. The three advi-

1) *Information and communication network efficiency and security cover threats including,* inter alia*, spam, cybercrime, viruses, worms and denial-of-service attacks.*

sory groups are intrinsically different in nature and the present provisions regarding the functioning of these groups are adapted to their different nature and individual needs. The US proposal implied that the wording "... and act through the Director" should be applied to all three advisory groups. This would mean a change of substance to the work of the TSAG.

Telenor finds that TSAG functions fairly well today and the advisory group is authorised to act on behalf of the WTSA in between two WTSAs in order to be able to speed up the work of the Telecommunication Standardization Sector. From a Sector Member's point of view, there is no need to introduce a clause that in our opinion will contribute to slowing down the work of the TSAG.

There was substantial support for the US proposal, although many European Member States were against any change to the provisions regarding TSAG. As a compromise, PP-06 agreed to align the text regarding the Telecommunication Development Advisory Group, but leave the provisions regarding TSAG unchanged. CEPT and ETNO members are pleased with the outcome of the discussions, but it is expected that this issue will be raised at another juncture.

7.9 Revised Resolution 122 The Evolving Role of the WTSA

The PP-06 in Antalya updated this resolution to take into account i.a. the results of the WSIS in the Geneva Declaration of Principles which recognises ITU's core competencies in the fields of information and communication technologies and underscores ITU's role as a unique, worldwide venue for government and industry to work together to foster the development and use of interoperable and non-discriminatory standards based on openness, and which are both demand-driven and sensitive to the needs of the use. The WTSA is requested to encourage close cooperation and coordination with relevant standards developing organisations in both developed and developing countries. The TSB Director is asked to consider organising a worldwide standardisation round table and coordination meeting possibly in conjunction with WTSA, for one day immediately prior to the assembly.

Telenor agrees to this updating which captures recent developments regarding convergence and the WSIS outcome. The resolution reiterates the core tasks of the WTSA and links it to the strategic plan of the Union for the next four-year period.

7.10 Use of Terminology in ITU Resolutions

Taking into account the outcome of the WSIS, many Member States see a need for updating the terminology relating to telecommunications in the basic instruments of the Union, including a possible change of name. ETNO did not see any need to change the scope and the name of ITU, and believed that the tasks bestowed on ITU regarding the follow up of WSIS could be performed within its present mandate. There was no consensus for changing the mandate and the name, but the PP-06 adopted Resolution GT-PLEN/8 "Review of terminology used in the Constitution and Convention of the International Telecommunication Union" which instructs the Council to establish a working group open to Member States to study i.a. the use of the term "telecommunications" in the CS and CV, to identify options for integrating any new terminology in the CS and CV where appropriate and to consider what terms should be used in the CS and CV to reflect the impact of information and communication technologies (ICTs) and ICT applications in ITU activities. The Council WG will submit their final report to PP-10. From a Sector Member's point of view, it is interesting to see that this group is limited to participation from Member States.

7.11 Definitions and Terminology Relating to Building Confidence

Res COM5/7 "Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies" instructs Council to set up a Council Working Group open to all Member States and Sector Members to study the issue of terminology related to building confidence and security in the use of ICTs, and to examine and develop definitions in this regard. It is noted that this CWG will be open to the Sector Members whereas the CWG on definition of telecoms is limited to Member States!!

7.12 World Telecommunication Policy Forum

This Forum was considered by the PP-06 to be an excellent instrument for discussing matters related to information on telecommunication policy and regulatory matters on global and cross-sectoral issues. With reference to ITU's role in the follow up of WSIS and the PP-06 Resolution on the review of the International Telecommunication Regulations, it was decided in Decision GT-PLEN/A "Fourth World Telecommunication Policy Forum" to convene the fourth WTPF in Geneva in the first quarter of 2009. As indicated in the Decision it is expected that the main topic for this Policy Forum will be the discussion on the future of the ITRs.

7.13 Strengthening the Regional Presence

A number of proposals called for an increased commitment from ITU in regional activities of the membership. The Council has already adopted a number

of resolutions aiming at introducing measures to strengthen the regional presence, and similar resolutions were adopted by the World Telecommunication Development Conference in Doha in 2006. This is now reflected in the ITU Strategic Plan for 2008 – 2011 which recommends strengthening communication channels among BDT, the Member States and the Sector Members and Associates and between BDT – both headquarters and the regional offices – and the General Secretariat and the R and T sectors.

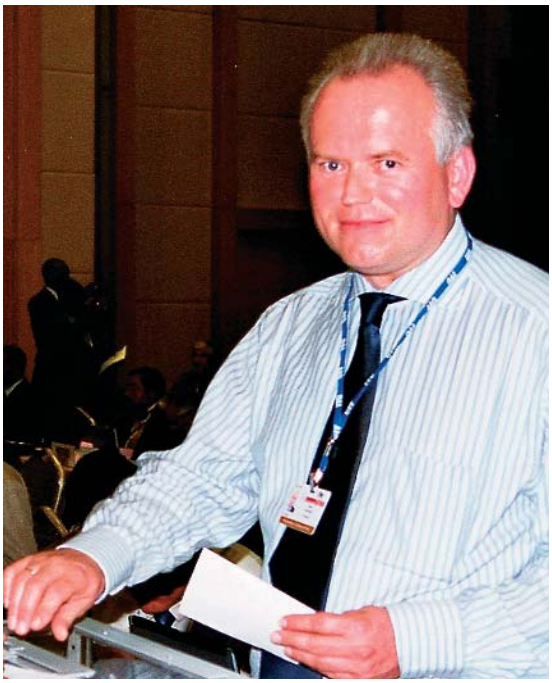
The PP-06 adopted Resolution 25 "Strengthening the regional presence" where it is resolved to carry out a review of ITU's regional presence. At the same time the regional presence should be strengthened and a broadening of the information dissemination functions of the regional presence is required. The regional offices should be expanded and strengthened and they should be provided with greater autonomy in terms both of decision-making and of addressing crucial needs of Member States in the region. The Secretary-General is instructed to include an evaluation of the effectiveness of ITU's regional presence in the United Nations Joint Inspection Unit (JIU) work programme. The Director of the BDT is instructed i.a. to develop specific operational and financial plans for the regional presence and to take the necessary measures to ensure the effective incorporation of BR and TSB activities in the regional offices.

As a Sector Member with mobile operations in a number of Asian countries, Telenor appreciates the initiative to make the regional presence more efficient and more adapted to the needs of the region in co-operation with all three sectors of the ITU.

7.14 Next-Generation Network Deployment in Developing Countries (NGN)

In the Geneva Declaration of Principles adopted by WSIS, it is emphasised that a well-developed information and communication network infrastructure and application which are easily accessible and affordable and the increased use of broadband and other innovative technologies can accelerate the social and economic progress of countries and the well-being of all individuals, communities and peoples. Account is taken of the fact that many developing countries face the task of conducting a smooth migration from existing networks to NGNs and that NGNs can facilitate the delivery of a wide range of advanced ICT-based services for building the information society.

PP-06 adopted Resolution GT-PLEN/3 "Next-generation network deployment in developing countries" where the Directors of the three Bureaux are instructed to coordinate studies and programmes under



Ottar Ostnes, Head, Norwegian Delegation

the Next-Generation Network Global Standards Initiative (NGN-GSI) of ITU-T and of the Global Network Planning Initiatives (GNi) of the ITU-D, and to coordinate ongoing work being carried out by study groups as defined by WTDC (Doha, 2006).

This Resolution puts NGN on the agenda of all countries and underlines the importance of deploying NGN and the information society world-wide, including the developing countries and countries with economies in transition.

7.15 Telecommunications in Emergency and Disaster Situations for Mitigation and Relief

In light of a number of natural disasters experienced during the past few years such as the tsunami in Asia and a number of earthquakes, there is an increased awareness of the importance of telecommunications in disaster relief. Resolution GT-PLEN/2 "The use of telecommunications/information and communication technologies for monitoring and management in emergency and disaster situations for early warning, prevention, mitigation and relief" underlines that an international standard for communication on alert and warning information can assist in the provision of effective and appropriate humanitarian assistance and in mitigating the consequences of disasters, in particular in developing countries.

7.16 The Global Symposium for Regulators (GSR)

There was overall agreement that telecommunications regulators should continue to have a specific platform

for sharing and exchanging matters concerning regulatory issues in the form of the Global Symposium for Regulators. Some Member States wanted to include the GSR in the basic instruments of the Union, but the compromise was to have a resolution – Res GT-PLEN/4 "The Global Symposium for Regulators" – where it is resolved that the GSR shall be established as a regular activity within the ITU-D programme and that the GRS should be arranged on an annual basis rotating in differing regions of the world.

As a member of the D-Sector, Telenor finds that the GRSs are very important events for regulators from all over the world. There is considerable need for exchange of information and knowledge about how a regulator should function in a modern telecommunications market, and ITU can play an important role in disseminating information and providing knowledge sharing.

7.17 Participation of Civil Society in the Activities of the Union

After the WSIS, it became clear that ITU did not cater for the participation of the civil society in its work. The WSIS concluded that all stakeholders have an important role to play in the development of the information society, and a number of Member States argued that ITU should adapt itself to the information society and to allow participation also from the civil society.

A compromise agreement was reached in Res GT-PLEN/7 "Study on the participation of all relevant stakeholders in the activities on the Union related to the World Summit on the Information Society" in which ITU is asked to conduct a study on the participation of all relevant stakeholders in the activities of the Union related to WSIS. The Council is instructed to set up a Council Working Group open to Member States – or to task an existing working group – to study a number of aspects related to this issue such as:

- Conduct open consultations on the inclusion of relevant stakeholders in the activities of ITU related to the WSIS, including additional tasks to be performed by ITU as a result of theWSIS outputs;
- Develop a set of criteria for defining which stakeholders are relevant to participate in ITU activities related to WSIS;
- Identify efforts needed to ensure effective participation of all relevant stakeholders from developing countries.

As a Sector Member it is not clear how this will evolve and the outcome will be studied when available.

7.18 Use of Six Official Languages of the Union

Res COM6/5 "Use of the six official languages of the Union on an equal footing" calls for the full implementation of the use of the six official languages (Arabic, Chinese, English, French, Russian and Spanish) on an equal footing and instructs the Council to review interim measures for interpretation and translation. The Council Working Group on Languages should continue to monitor progress and report to the Council on the implementation of this resolution.

Based on the fact that ITU is an intergovernmental organisation and part of the UN family, it is understandable that the question of languages is of crucial importance for a number of Member States. However, when considering the predicted shortfall in the financial plan and the cap set for expenditure to interpretation and translation, there is an imbalance between the wish of the PP-06 and the actual means made available for these activities. For the sake of efficiency, it would have been preferred to conduct much of the work in the Study Groups in the sectors in one langue only.

8 Future Council Working Groups Set up as a Consequence of the PP-06 Decisions

A number of issues will be studied further, either in Council Working Groups (CWGs) or in a process to be determined by Council.

The following Council Working Groups (CWGs) were established by the Council Extraordinary Session held in Antalya on 24 November 2006 immediately after the PP-06:

- Management and budget group (MBG) (Resolution COM6/6). J Mendès, Portugal, was provisionally nominated as chairman. The CWG will consist of Member States members of Council, the Secretary-General and the Directors of the Bureaux.
- Participation of all relevant stakeholders in the activities of the Union related to the World Summit on the Information Society (Resolution GT-PLEN/7). A Cristiani, Argentine, was provisionally nominated as chairman. The CWG is open to Member States only. Both Member States and Sector Members are invited to submit written contributions to the group.

- Definitions on security of ICT (Resolution COM5/7). N Kisrawi, Syria, was provisionally nominated as chairman. The CWG is open both to Member States and Sector Members.

Council Working Group to be created at the September 2007 Session of Council:

- Terminology in the Constitution/Convention of ITU (Telecommunications) (Resolution GT-PLEN/8). The CWG will only be open to Member States.

Studies to be developed by Council (process to be determined):

- Number of Member States members of Council (Resolution PLEN/1), open to Member States;

- Study on the management and functioning of the Union (number of elected officials etc.) (Resolution COM5/5) open to Member States.

Two old CWGs will continue:

- The role of ITU in the follow up of WSIS (Resolution GT-PLEN/6);

- Use of languages (Resolution COM6/5).

9 Future Conferences, Assemblies and Forums of the Union (2008 – 2011)

- World Telecommunication Standardization Assembly (WTSA), between May and November 2008;

- World Telecommunication Policy Forum (WTPF), first quarter 2009;

- World Telecommunication Development Conference (WTDC), March 2010;

- Plenipotentiary Conference (PP-10), October/November 2010;

- RA and WRC, February/March 2011.

Mexico has invited to host the Plenipotentiary Conference in 2010.

10 Entry into Force

The amendments to the Constitution and the Convention contained in the present instrument shall, as a whole and in the form of one single instrument, enter into force on 11 January 2008 between Member States being at that time parties to the Constitution and the Convention of the International Telecommunication Union (Geneva, 1992), and having deposited before that date their instrument of ratification, acceptance or approval of, or accession to the present amending instrument.

Acronyms and Abbreviations

APT	- Asia Pacific Telecommunity
BDT	- Telecommunication Development Bureau
BR	- Radiocommunication Bureau
CcTLD	- Country code Top Level Domain
CEPT	- Conférence européenne des Administrations des Postes et Télécommunications
CHF	- Swiss Francs
CITEL	- Inter-American Telecommunication Commission
CS	- (ITU) Constitution
CV	- (ITU) Convention
CWG	- Council Working Group
EC	- European Commission
ENUM	- Mapping parts or all of the ITU-T Recommendation E.164 international public telecommunication numbering plan into the Internet Domain Name System (“DNS”)
ETNO	- European Telecommunication Network Operators’ Association
GNi	- Global Network Planning Initiatives
GSB	- Global Symposium for Regulators
ICT	- Information and Communication Technology
IDNs	- Internet Domain Names
IGF	- Internet Governance Forum
ITRs	- International Telecommunication Regulations
ITU	- International Telecommunication Union
ITU-D	- Telecommunication Development Sector
ITU-R	- Radiocommunication Sector
ITU-T	- Telecommunication Standardization Sector
JIO	- UN’s Joint Inspection Unit
MS	- Member States
NGN	- Next Generation Network
NGN-GSI	- Next Generation Network Global Standards Initiative
NPT	- Norwegian Post and Telecommunications Authority
NITU	- Nordic ITU Cooperation
PP	- Plenipotentiary Conference
RA	- Radiocommunication Assembly
RAG	- Radiocommunication Advisory Group
RR	- Radio Regulations
RRB	- Radio Regulations Board
SG	- Study Group

SM	- Sector Members
TDAG	- Telecommunication Development Advisory Group
TSAG	- Telecommunication Standardization Advisory Group
UN	- United Nations
UNESCO	- UN's Educational, scientific and Cultural Organisation
WATTC	- World Administrative Telegraph and Telephone Conference
WCIT	- World Conference on International Telecommunications
WG Plen	- Working Group of the Plenary
WIPO	- World Intellectual Property Organisation
WRC	- World Radiocommunication Conference
WSIS	- World Summit on the Information Society
WTDC	- World Telecommunication Development Conference
WTPF	- World Telecommunication Policy Forum
WTSA	- World Telecommunication Standardization Assembly

Anne Lise Lillebø is Director, Telenor ASA, Group Regulatory. Her main responsibilities include spectrum management and policy matters related to international telecommuncations organisations. She has been a member of the Norwegian delegation to IUT's Plenipotentiary Conferences in 1989, 1992, 1994, 1998, 2002 and 2006. She holds a Master of Arts degree from the University of Oslo.

email: anne-lise.lillebo@telenor.com