Context-aware Personal Networks in Beyond 3G Systems

Ernö Kovacs, Martin Bauer, Usman Javaid, Djamal E. Meddour

***Abstract*—Beyond 3G systems will provide ubiquitous connectivity and seamless networking services based on an All-IP architecture. On the way towards 4G systems, the research goal must be to provide networking services that are truly embedded in everyday life – unnoticed, but available. In this increasingly complex world, Personal Networks (PN) provide a simple, but powerful concept to users: a network that solely belongs to him, useable for his personal goals, and not shared with others.**

Context-aware services are often regarded with suspicion and fear for the loss of privacy, hindering their wide-spread use. PNs make the use of context information much easier to accept as the context information is available and used only within the PN. Only under precisely defined conditions are context information provided outside the PN. This paper explains how PNs will be provided in B3G systems and how context information will be gathered, processed and used within the PN and in collaboration with 3G service platforms. Moreover, complementary perspectives of context information utilization are also discussed.

***Index Terms*— Beyond 3G systems, context-aware Personal Networks, service platforms, privacy-enhancement technologies.**

I. Introduction

When Personal Computers (PCs) were introduced, people thought they were simple toys, created to fulfill some special personal needs. They were wrong. PCs were easier to handle than existing mainframes, could be modified and extended as the users wished, were cheaper, and developing faster than the rest of the industry. After a slow start, they adopted the networking paradigm and are now dominating the computer industry.

Now imagine having a network that is as personal as the PC. It is a network owned and operated by one person. This person can use the Personal Network (PN) [1] in any way he wants. The owner can connect all his personal devices and decide on his own which services shall be available in the PN. The PN can be changed and updated as need be. For example, a user can easily buy a subscription to a new access service (e.g. a 3G service or a WiMAX service) and allow his PN to use it. He can add new devices and put new services into the network. This allows him to create services tailored to his own personal needs. In doing so, the PN protects the user and shields him from the rest of the network. The PN builds up his own small real estate in Cyberspace. On the first look, creating new, PN-only services might be much easier as the PN provides a shielded, single-user environment. This allows the service creator to focus on the service to fulfill (similar to the early applications on a PC).

Unfortunately, the world is not as simple as described here. The power of networks is to connect many persons and devices. This is somehow fundamentally opposite to the PN that shields its owner from the rest of the world. The set of real useful, PN-only, single user services are limited. Thus there is the need for PNs to communicate with the outside world. This need includes gathering context from the outside as well as using services provided outside of the PN. Furthermore, PNs will also be the source of context information and providing services that others might use.

In this paper we will look at future perspectives of PNs. The basic concepts of PNs have been researched in the past and have resulted in promising prototypes [2]. But most of them are looking at rather isolated, network-oriented systems, neglecting the fact that the users' situation is constantly changing, as well as the tasks they need to do. The next generation of PNs needs to take this into account adapting their structure and usage to exactly these needs of the user. In general, this type of situated computing is associated with determining the context of persons, places and objects. For automatic identification of the user's situation, we need new sensor technologies, new processing technologies and new software architectures that allow adaptation to the changes in the context of users.

In the following, we first give a introduction of PNs and their properties. Then we analyze the usage of context information first within the PN, then on the boundary of the PN, and finally between PNs and other networks. We show how PNs can become adaptive, situation and task oriented networks. We identify the needed mechanisms and concepts to be added to the PN architecture. It should be clear that this is a rather forward looking paper, although the concepts explained here are examined and implemented in research projects like IST MAGNET and IST MAGNET Beyond.

Manuscript received April 17, 2006.

The work presented in this paper has been carried out under the auspices of the IST-027396 MAGNET Beyond project. **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 has 32 partners from 15 countries.

Martin Bauer and Ernö Kovacs are with NEC Europe Ltd., Network Laboratories, Heidelberg Germany

Usman Javaid and Djamal E. Meddour are with France Telecom R&D, Core Network Laboratories, Lannion France

II. Overview of Personal Networks

A Personal Network is a secure overlay network connecting all the personal devices of a user. Attaching a device to a PN basically requires establishing a trust relationship between all devices. The first step in establishing this trust is "imprinting" the devices with the security information necessary to participate in the network.

After that we need to maintain the connectivity between these devices. Problems involved here are to establish and maintain the personal area networking setup (e.g. the PAN connectivity), the managing of different clusters (like the Personal-PAN (P-PAN), the home cluster, or the car cluster), as well as establishing and maintaining the large area network infrastructure (e.g. by selecting the right access network).

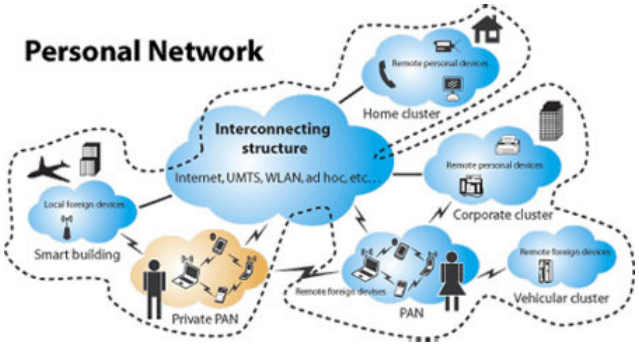

Figure 1: Personal Network

Furthermore, we need an infrastructure for managing the services within the network. The first task here is to provide the user with a good view on his Personal Network and the available services (e.g. through the respective discovery and control functions). A context-aware service discovery is provided that allows users to find services within the PN. We need PN service management functions that allow service creation in the PN, adapting the service structure to the changing PN overlay and provide high-quality user experiences. One example could be an automatic storage manager that moves recorded pictures from his digital camera to a local storage device whenever the available storage is dropping below a defined limit. As personal networks are reaching to home, we can automatically send the recorded data to the home media library and maintain different copies across different devices of the network in case we are loosing communication links or running out of battery.

A. Business models and usage scenarios

An even larger problem is to allow the normal everyday user to establish and manage a PN. Principally, there will be three types of PNs. The first one is the so-called infrastructure-less or ad-hoc PN which relies solely on the personal devices of the user and on the user to correctly set up and maintains the complete PN. The second type of PN will be infrastructure-based. In infrastructure-based PNs, a network operator or an independent service provider will operate the PN on behalf of the user. The first and important thing is that the users in this case need to trust their service provider. The service provider will manage the PN and enforce the security policies according to the agreement with the user. Additional advantages might be gained by bundling the PN services with network access services, for example from a B3G network operator.

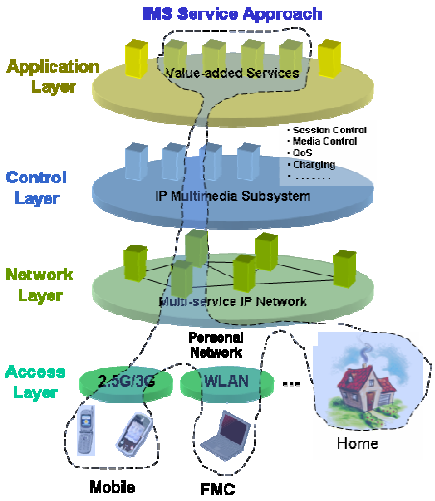

Figure 2: Infrastructure-based Personal Network

PN service providers can add value to the basic PN service by offering value-added services that after subscription can be automatically included inside the PN (see Figure 2 for an IMS-based example). A simple example for a value-added service is a pure storage service that is added to the PN. These services become interesting when for example PN services start to automatically make use of them. In the previous example, a digital camera included in a PN can discover the storage server, read a semantic description of the service, and deduce that it can copy or move digital photos to that storage server for later use. Note the fundamental difference between a service included inside the PN and a service accessed from the PN. For the later ones, we have the service model of today's Internet (e.g. home or office networks). In this case, service can be orchestrated from different provider using different technologies (e.g. Web Services or SIP).

A third type of PNs (Hybrid PNs) can be envisaged that combines the infrastructure-based approach with ad-hoc extensions by the user.

III. Context in Personal Networks

Context-aware services (CAS) are especially useful within a PN, as the normally problematic aspects of privacy and trust are solved at the PN level. CAS gathers context information about the user through sensors on the devices or information extraction from network/service elements. As this context describes all aspects of the owner's life, the fear is to lose privacy and becoming naked – in front of the whole world watching. A PN helps in dissolving this problem, as – ideally – the context is only gathered, processed, and used within the PN. The PN will handle the security and privacy needs of the user. It will react to his movements around the world, maintain the connection between his personal devices based on context information, and provide his context-aware personal services.

He can add new sensors as he wishes. He can install new context processing software that performs monitoring, logging and adaptation steps based on his context. For instance, he can install services that check on his health conditions, collect his movement data, record them in a history database, and process them in order to identify emergency situations. Contrary to existing context-aware systems, in the case of PNs, the context data will be confined to within the PN, therefore making these applications much more trustworthy to the end user.

IV. Connection to the Outside World

As explained before, a strength of PNs is that they inherently confine the communication within its borders. However, the user does not live in the isolated world of a single PN, but interacts with the outside world. We need to consider at least two cases: access to information sources and services outside of the PN and collaboration between different PNs

A. PN Firewalls

Similar to Local Area/Home Networks, PNs need to be connected to the outside world. They will access information/ services available in the global Internet and the local environment. They will also provide information to other users. For PNs, we need a strictly controlled access to the outside world. The functional entity for this is the PN Firewall. The PN Firewall is located somewhere in the PN of a user. It controls not only the inbound and outbound traffic, but especially also needs to examine the services provided to the Internet and data exchange with the outside world. This includes the definition of firewall policies giving exact definitions on how to reach nodes inside the PN and what services from the outside can be accessed.

B. Federation of Personal Networks

In order to enable the interaction between different PNs, MAGNET Beyond considers the concept of PN Federation (PN-F). A PN-F is a secure cooperation between a subset of relevant devices belonging to different PNs for the purpose of achieving a common goal or service. PN Federations will be established when the involved users need to collaborate with each other, e.g. for collaborative work, sharing resources, or just allowing network traffic to pass through.

C. Service gateways to the outside world

Services from the outside world are made available through service gateways. At the service gateway, the strict security requirements of a PN can be enforced. Furthermore, the service gateway allows utilizing the PN Service Management (PN-SM) when establishing and managing networks. The purpose of the PN-SM is to optimize and maintain a session within the complex structure of the PN. For example, in order for a SIP session to terminate at the right device close to the user, the PN-SM supports the session setup for an incoming call by routing the call to the right personal node of the user. PN Profiles can be used to determine which personal device shall terminate the call. The PN-SM furthermore keeps track of the interconnection between the different clusters and can therefore establish the media path according to the required Quality of Service (QoS) parameters. Especially the upcoming *IP Multimedia Subsystem (IMS)* will provide rich multimedia services and inter-personnel communication. Providing a service bridge to IMS services would allow the use of the SIP-based session establishment Together with the described PN Service Management.

The *Open Mobile Alliance (OMA)* is currently defining a large set of additional service enablers that can be used with the service gateway, e.g. presence, instant messaging (IM), dynamic content discovery (DCD), and others. We expect activities for a context service enabler to start very soon.

D. Context gateways to the outside world

We have two types of context use across the boundary of the PN. The first uses context from outside of the PN. At the boundary of a PN, we can gather context information mainly from sensors that are accessible to the different PN devices.

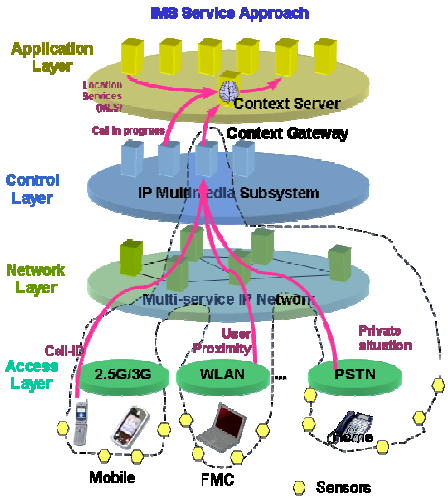

Figure 3: Context Gateway in PN

Furthermore, context can be retrieved from external context management systems. In the case of IMS, we assume a *Context Management Service* (as proposed in [4]) that users can utilize to retrieve context information about themselves, the places at which they are, and about other users.

Secondly, context information can be provided to services outside of the PN; e.g. to the Context Management service. For this, we need a PN Context Gateway. This is a functional component in the PN control plane at which privacy policies are enforced. The PN user defines which context information is made available at which granularity to which service outside of the PN. These policies are maintained and enforced at the PN Context Gateway.

V. Utilizing Context

In the following sections we discuss with the help of a scenario what kind of context is used in PNs. We highlight the usage of context in PN Services and PN Networking.

A. *Scenario Story*

Sana, a business manager, takes the train for her journey to the office. She connects to her enterprise network using the train's Wi-Fi network and her personal device, i.e., her Laptop. Using her PN, she can securely access her emails and today's agenda. As usual, she has some meetings in the morning.

As she enters her office, she finds a missed call from her colleague on her personal device (fixed phone), therefore she calls her back using her personal device, i.e. her mobile phone. Since, her colleague's office is in the same building, the Wi-Fi multi-hop capability of the mobile phone is utilized.

It is 10:30 AM – she runs to attend a meeting at the client site. She takes the company's car which is equipped with an Intelligent Transport System (ITS). While she is in the company's car park, she gets an alert on her PDA (connected to enterprise WLAN). It asks whether to download the points of this morning's meeting (with some other documents) sent by her senior manager. She accepts and directs the download to her laptop and moves towards the car. As soon as she leaves the car park, the WLAN connection is switched to the WiMax network to maintain the ongoing download operation. While driving, she makes a couple of quick calls over the UMTS network using the ITS system On her way, despite of the availability of Public Wi-Fi hotspots, the connection is not handed over from the WiMax network, because of her high mobility which may not be supported by the low WLAN coverage. On reaching the client site, her personal device, i.e., her PDA recognizes a low-battery condition, shifts over to a lower-power connection to download the last-minute edition of the documents.

It is 11:00 AM; Sana is in the meeting at the client site. During the last minutes of her discussion, she also includes her senior manager on the request of the client through the video conference.

It is 12:20 PM; Sana is taking her lunch at a restaurant. She wants to watch "News" on her favorite channel. Since, there is no public hotspot in the direct reach of her personal devices; she establishes a PN-Federation to connect via multiple hops to a nearby hotspot.

B. *Context model*

Context-awareness is the ability of a particular service/ device/network to adapt itself to a continuously changing environment. Context-aware computing can play a major role in improving the user's personalized networks. Following section presents the classification of context information from the viewpoint of Personal Networks<.

1) User Context

User context refers to the information directly related to the user. For example, Sana's location, profile, preferences, people/colleagues nearby, favorite/daily usage of applications and QoS perception, mood, activity, history, health, personality etc.

2) Personal Node Context

Any information that characterizes the situation of a personal node/device is considered as Personal Node context. For example, network connectivity and available QoS (bandwidth, delay, error rate) at Sana's personal devices, their capabilities, available services etc.

3) P-PAN Context

P-PAN context includes the information related to the personal devices in close vicinity of the person. One part of this information is obtained through context exchange between the P-PAN devices, e.g., networks available on each of her personal device, inter-device connectivity and relevant QoS capabilities of all nodes, application feedback etc. The other part is composed of the information of the environment e.g., the physical parameters that represents the environment around Sana, such as lighting, temperature, humidity, season etc.

4) PN Context

PN context includes the information related to personal resources and devices, which are not necessarily in the close vicinity of the person. PN context is collected through intra-PN context exchange. Examples are end to end network and user QoS, services available to different personal devices at Sana's PN, context information of her personal nodes and clusters in the her PN etc.

5) PN-Federation Context

PN-F context represents the information obtained through inter-PN context exchange. It is similar to PN context; however, the focus here is on groups and not on individual users. For example, Sana's PN-F context information includes her inter PN trust levels, context information of not only those PNs which are part of her PN-F but also those which are just allowing her PN traffic to pass through, and all or a part of the her PN context information.

C. *Context transfer for maintaining the PN*

In a B3G network environment, whenever a personal device roams to a new access network, services that have already been established shall be maintained. Therefore, inter-network context transfer mechanisms [5] should be developed in order to proactively exchange the operational information so that the PN can be maintained and the services can be quickly re-established. For example, while in the car when Sana changes her Point of Attachment (PoA), certain context information is proactively transferred to the new PoA in order to reestablish the files download session, as presented in Figure 4.

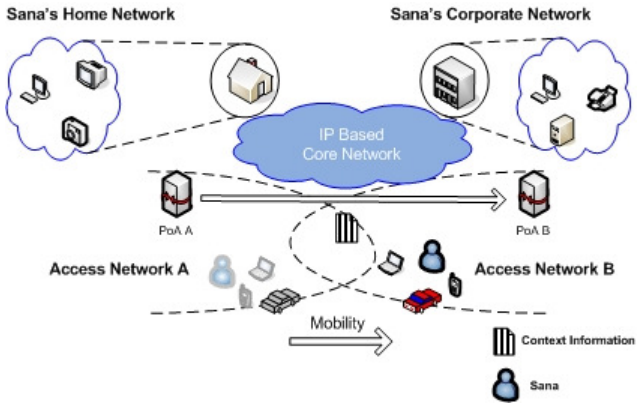

Figure 4: Context transfer for Maintaining Sana's PN

D. Scenario Discussion: Utilizing the Context Information

Context information can be utilized in application/service environments for enhanced service creation and management and in network environments towards optimized end-to-end network selection and routing [6]. The utilization of context information is being discussed in the next section under the light of presented scenario.

1) Context Usage in PN Applications/Services

In the following table we highlight the usage of context information at the service layer.

#	Scene	Context Information
1	At the train station & during travel	**Service:** Recommender suggest family travel offers, summer promotions etc. **Context: u**ser profile and preferences, mood, current activity, planned activity
		Service: IMS-based personalized IPTV: breaking news, sport news etc **Context: u**ser profile and preferences, desire-for-interrupts
2	In the office	**Service:** IMS Services (VoIP, presence), OMA DCD Push Service **Context: u**ser profile, presence
3	On the road (in the car)	**Service:** Personalize surrounding devices (e.g. the car radio with the favorite radio station) **Context:** Device discovery, user preferences
		Service: Alerts & information download **Context: d**evice discovery, device profile, preference profile
4	On the client's site premises	**Service:** In-building pathfinder **Context: a**ctivity prediction, next stop prediction
		Service: Local meeting support system, service discovery **Context:** activity prediction, group context determination
5	At the restau-rant	**Service:** PN Federation, recommender for cinema offers, restaurant promotions, latest concerts, IMS services etc. **Context:** user's profile and preferences, activity, mood

Table 1: Context usage in PN Applications/Services

It can be seen that context information from within the PN and from outside the PN is used (a) to customize services within the PN (e.g. PN Federation establishment), (b) to customize devices in the environment (e.g. favorite radio stations), and (c) to adapt services to preferences and situation (e.g. alert & information download). Furthermore, we can see that public services from outside the PN are adapted using context information from within the PN.

2) Context usage in PN Networking

In the following table, we have highlighted the context information available in the different scenes of the scenario that assists in the routing and network selection mechanisms.

#	Scene	Context Information
1	Train station	**Service:** Access to enterprise email and agenda **Context:** available networks(UMTS, Wi-Fi)
2	In the office	**Service:** Voice call **Context:** Available networks, Destination
3	On the road	**Service:** File download **Context:** Environment(car)),available networks
4	Client site	**Service:** File download **Context:** available networks**,** device Context-energy level
5	In the client meeting	**Service:** Video conference **Context:** available networks destination context(in his office, having webcam)
6	Restau-rant	**Service:** Video streaming **Context information: a**vailable networks, user preferences

Table 2: Context usage in PN Networking

With the help of the presented scenario, we have illustrated how the context information is smartly used in network selection and routing decisions. It is worth mentioning that the underlying technological choices are transparent from the user, providing her with an opportunity to concentrate on her professional activities. The intelligent devices, which are a part of her PN, therefore take the vision of seamless interoperability from myth to reality by utilizing the networking context information.

VI. Conclusion

In this paper we claim that PNs have advantages compared to existing approaches when dealing with personal information such as context especially in the area of privacy. We explain that the PN is a natural system model for collecting and processing context for a user. Furthermore, we identified the need to integrate the PN services with external services such as the IMS. We paid special attention to the use of context outside the PN and introduced a special network component, the PN Context Gateway. At this context gateway, privacy rules are enforced. We are also able to include context from external systems into the PN. Especially a context service in the IMS system would greatly expand the possibilities that can be offered to the users.

We explained these abstract requirements with a concrete scenario. Using this scenario we showed that context is advantageously used at the service and at the network layer. The described system is currently being investigated and developed in the IST MAGNET Beyond project. This project will build a PN pilot and demonstrate context-aware Personal Networks.

Acknowledgment

The authors are grateful of all the partners involved in MAGNET-Beyond projects, especially Work Package 2 for their fruitful discussions and collaborations. The views expressed in this paper are the views of the authors and not necessarily the view of MAGNET Beyond or the involved companies.

References

[1] I.G. Niemegeers and S. Heemstra de Groot, “From Personal Area Networks to Personal Networks: A user oriented approach”, Journal on Wireless and Personal Communications 22 (2002), 175-186.

[2] Luis Sanchez, Jorge Lanza, Luis Muñoz, Julian Perez, "Enabling Secure Communications over Heterogeneous Air Interfaces: Building Private Personal Area Networks", 8th International Symposium on Wireless Personal Multimedia Communications - Aalborg, September 2005, pp. 1963-1967.

[3] 3GPP TS 22.259 V7.0.0 (2006-03): 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Service Requirements for Personal Network Management; Stage 1, (Release 7)

[4] E. Kovacs, S.Gessler, M. Martin: “Impact of Context-Aware Services on the IP Multimedia Subsystem (IMS)”, WWRF#14, San Diego, May 2005.

[5] J. Loughney et al. "Context Transfer Protocol (CXTP)", RFC 4067, IETF, July 2005

[6] Usman Javaid, Djamal E. Meddour et al. “Cooperative Wireless Access Networks Convergence using Ad-hoc Connectivity: Opportunities and Issues", WWRF#16, Shanghai, April 2006