Wireless Personal Communications **26:** 149–167, 2003.

Research Issues in Ad-Hoc Distributed Personal Networking

I. G. NIEMEGEERS [1] and S. M. HEEMSTRA DE GROOT [2]

[1] *Delft University of Technology, Mekelweg 4, 2628 CD Delft, The Netherlands*
E-mail: Niemegeers@its.tud.nl
[2] *Twente Institute for Wireless and Mobile Communications and University of Twente, The Netherlands*
E-mail: Sonia.Heemstra.de.Groot@ti-wmc.nl

Abstract. This paper discusses the research issues that need to be addressed in order to create a personal distributed environment where people interact with various companion, embedded, or invisible computers not only in their close vicinity but potentially anywhere. These systems are called personal networks (PNs). They constitute a category of distributed systems with very specific characteristics. They are configured in an ad hoc fashion, as the opportunity and the demand arise, to support personal applications. PNs consist of communicating clusters of personal digital devices, devices shared with other people and even infrastructure-based systems. At the heart of a PN is a core Personal Area Network (PAN), which is physically associated with the owner of the PN. Unlike the present PANs that have a geographically limited coverage, the Personal Operating Space, PNs have an unrestricted geographical span, and incorporate devices into the personal environment regardless of their geographic location. In order to do this they need the services of infrastructure-based networks and ad-hoc networks to extend their reach. A PN extends and complements the concept of pervasive computing. We show that PNs introduce new design challenges due to the heterogeneity of the involved technologies, the need for self-organization, the dynamics of the system composition, the application-driven nature, the co-operation with infrastructure-based networks, and the security hazards. We discuss the impact of these problems on network design, assess present and proposed solutions, and identify the research issues.

Keywords: Personal Networks, Personal Area Networks, pervasive computing, self-organisation, ad-hoc networks, context awareness, ambient networking.

1. Introduction

There is a consensus that new ICT technologies should be centered on the user; they should improve quality of life and adapt to the needs of the individual without being intrusive. The physical environment of a person, e.g., his or her home, office, car, public places he or she visits, public transportation, will become smarter, more responsive, and more accommodating to individual needs. For instance future technologies will provide location- and context dependent services and will introduce new levels of personal comfort and safety. A future is envisaged where personalization and ubiquitous access to information and communication are essential. Users will be able to create a personal profile that, according to the situation and moment, will allow them to access the most suitable communication means and relevant information. These ideas can be found in visions produced by different groups and from different perspectives. Examples are "Scenarios for Ambient Intelligence in 2010" [1], "The Book of visions – Visions of the Wireless Word" [2], "Telecom Scenarios in 2010" [3], and the vision of the Association of Computing Machinery (ACM) in "The Next 1000 Years" [4].

An implication of these visions is that there is a need for a *communication substrate* that allows a person *ubiquitous global access* to a vast number and variety of information re-

sources, ranging from inexpensive sensors and actuators, wearable digital devices, consumer appliances to utility-like large scale computing facilities. Many of these information resources will be mobile. This communication substrate will be formed by a variety of existing and future communication and network technologies.

As a consequence, new research fields are emerging, addressing different aspects of this problem. Examples are service portability and virtual home environments [5], concepts aiming at providing users with the same service experience independently of the user interface, terminal capabilities, access network technologies, and network- and service providers. Another important and related emerging area is pervasive computing[1] targeting environments where networked computing devices are ubiquitous and even integrated with the human user [6].

In this paper we introduce the new concept of a Personal Network (PN), a concept that is at the heart of pervasive computing, and could become an important means to realize service portability and virtual home environments. We will discuss its characteristics, goals, requirements, conditions and the circumstances that make it timely to research the technical issues that need to be addressed. We start in Section 2 by describing a number of scenarios involving PNs. In Section 3 we make the concept of a PN more concrete by discussing the composition and organization of a PN. In Section 4 we give an overview of the research issues brought about by the distinctive characteristics of PNs. We then go on to discuss some of these in more detail. Section 5 discusses architecture, Section 6 resource discovery, Section 7 context discovery, Section 8 self-organization, Section 9 addressing issues, Section 10 routing, Section 11 co-operation with infrastructure-based networks, and Section 12 security and accounting issues. In Section 13 we draw some conclusions regarding the future research on PNs.

2. From PANs to PNs: Some Scenario's

The concept of a PN goes beyond the concept of a Personal Area Network (PAN). The latter refers to a space of small coverage (less than 10 m) around a person where ad-hoc communication occurs, e.g., using Bluetooth [7] or IrDA [8]. This is also referred to as a *personal operating space* (POS) [9]. IEEE P802.15 [10] in particular focuses on the development of consensus standards for PANs or short distance wireless networks. These are intended to interconnect portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones, and consumer electronics. PNs extend the local scope of PANs to a global one by addressing virtual personal environments that span a variety of infrastructure- as well as ad-hoc networks.

Let us first describe some potential scenarios involving PNs:

- *A health-monitoring application:*
  A disabled or elderly person has a PAN incorporating sensing and actuating devices linked up to a health-monitoring server at home. As this person moves away from home to another location the server stays connected all the time to the sensing devices in a PN, which is formed by linking the PAN-connected devices via, e.g., a 3G network, and the Internet to the Home Network where the health-monitoring server resides.

[1] Pervasive computing is an environment where people interact with various companion, embedded, or invisible computers. It essentially means to enable networked devices to be aware of their surroundings and peers, and to be capable to provide services to and use services from peers effectively. Pervasive computing encompasses many different technologies, and is the enabling technology for such applications as e-commerce and connected home.

- *Walking through a smart building:*

  While a person walks through a smart building from room to room, a PN accompanies him/her. It interacts with the building functions and controls the lighting, enables access to restricted areas, and activates building devices. For instance, it incorporates into the PN a large wall-mounted display where the person can view an incoming video stream directed to him/her, which cannot be displayed properly on his/her PDA.

- *Business environment extended from the office to the car*

  A person leaves his/her office and enters his/her car. A PAN is established incorporating a number of car information accessories (via the on-board car network) so that he can listen to his/her corporate e-mail text read by a computer, dictate and send replies. This could be realized for instance by linking up and temporarily extending the persons PAN containing a 3G-enabled PDA with on-board speakers, microphones and a voice-recognition and -synthesis system.

- *A telepresence session:*

  One or more video cameras and high quality displays surround a person in the office and at home. These devices are incorporated, automatically and invisibly, into his/her PN as he enters the office or sits down on a couch in his/her living room. They allow him/her to start up a telepresence session via, e.g., his/her PDA, in which he can have a virtual meeting with other people for business as well as for social occasions.

  Alternatively a person on the move could carry around some high-quality portable wireless screens and cameras, which can be spread around to emulate the presence of remote participants in a session. Again this would involve the establishment of a PN involving local and remote devices.

- *A remote babysitting application:*

  Consider the case of a mother visiting a friend's house while her child is asleep at home. She might want to remotely watch and observe the child. She does this by using a PN consisting of some personal devices, e.g., a UMTS and Bluetooth capable PDA and a head set she carries with her, and, a remote pair of eyes and ears in the child's bedroom at home. The latter consist of a digital video camera, a microphone and a UMTS phone, forming a cluster of cooperating devices. But since the friend's living room is equipped with a TFT wall display including speakers, hooked up to the friend's home network and accessible to authorized guests via a Bluetooth link into the home network, she might want to use these to observe the child instead of her PDA and headset.

A way to envisage how these scenarios could happen is as follows. An individual owns a PAN, consisting of networked personal devices in his/her close vicinity, e.g., attached to the body or carried in a briefcase. This PAN is able to determine its context (e.g., where it is), interact and link up with devices in the environment or with remote devices in order to temporarily create a PN. This PN provides the functionality (e.g., office functions in the car) the individual wants at that very moment and in that particular context.

Referring to the multisphere model proposed in the WWRF Book of Visions [2] a PN runs across the spheres defined around a person: starting from the PAN sphere and ranging via the immediate environment, the instant partners, the radio access and the interconnectivity sphere to the cyber world sphere. It reaches out to whatever resources or partners are needed to support and enhance a person's private and professional activities. These resources and partners are not necessarily in the immediate geographic vicinity of the person.

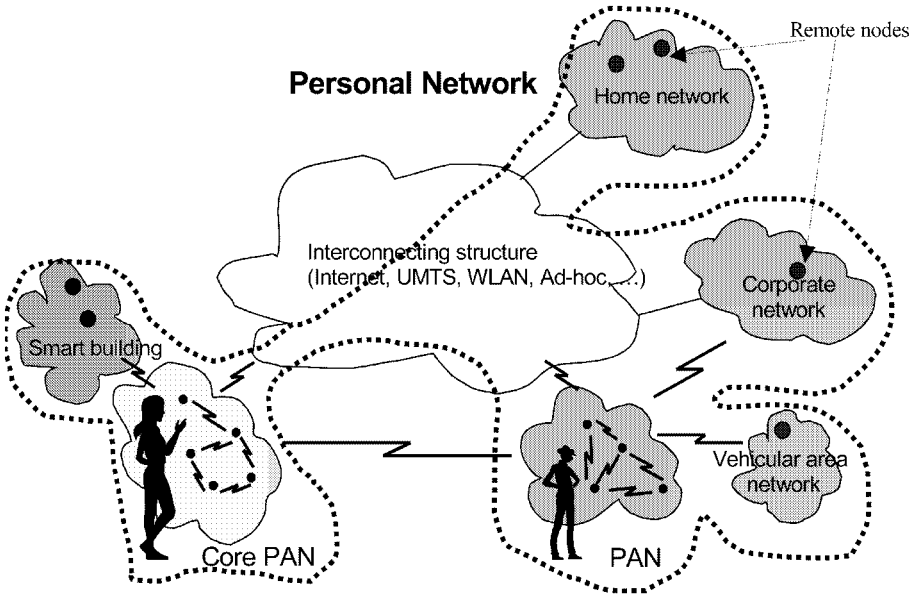

Figure 1. Personal Network.

PNs are very much centered on a person and his/her needs. They will be dynamic in composition, configuration and connectivity depending on the time, place and circumstances, the resources required and the partners one wants to interact with.

We envision a PN to have a core PAN, consisting of devices, which a person carries with him/her most of the time, e.g., a combined PDA-cellular phone. This core PAN will, if its owner desires so, look out continuously for what the electronic environment has to offer. Alternatively, if a user values privacy or isolation under given circumstances, his/her core PAN will isolate itself from this environment. The core PAN is extended, on-demand and in an ad-hoc fashion (driven by the opportunity and the applications), with personal resources or resources belonging to others (organizations or people). The resources that can become part of a PN will be very diverse. One could think of, e.g., computers, PDAs, phones, headsets, displays, cameras, Internet-enabled appliances, sensors and actuators. There are many more devices with communicating and processing capabilities that will emerge in the coming years (this is the main rationale for the IPv6 protocol). These resources can be private or may have to be shared with other people. They may be free or one may be charged for their usage.

The extension of the PAN with remote devices will physically be made via infrastructure-based networks, e.g., the Internet, an organization's intranet, or via ad hoc networks such as another persons PN, a vehicle area network or a home network. Figure 1 illustrates the concept.

3. The Composition and Organization of a PN

Like a PAN a PN is intimately associated with a person. However it is a much more complex structure, geographically distributed and, its composition is determined by the application and context a person and his or her PN is operating in.

Our assumption is that a PN consists of five types of components:

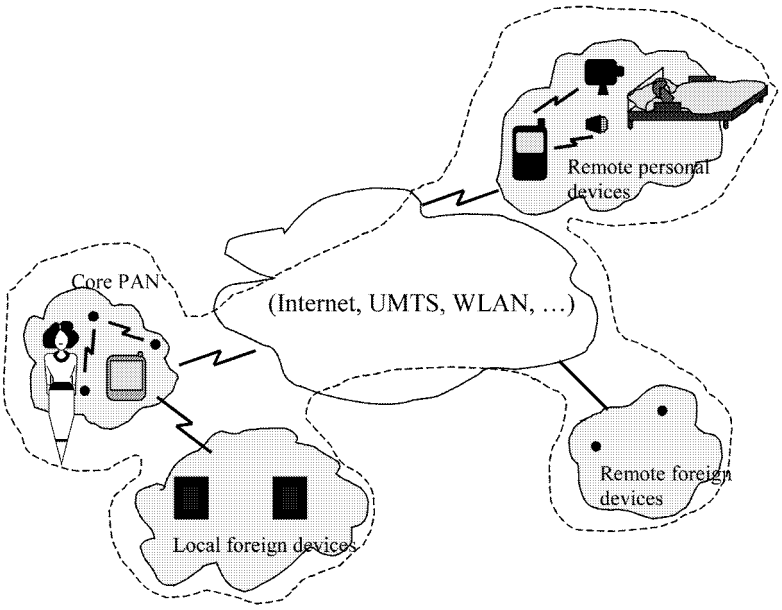

Figure 2. Components of a Personal Network.

- A *core PAN* consisting of personal devices in the close physical vicinity of a person and moving around with that person. The core PAN is an essential component of a PN.
- *Remote personal devices*, which could be grouped into a cooperating cluster and which are linked to the core-PAN via interconnecting structures.
- *Local foreign devices* or *clusters* thereof, which are owned by other parties and could either be reserved solely for the PN owner or be shared with other people. They are linked to the core-PAN via interconnecting structures.
- *Remote foreign devices* or *clusters* thereof, which are linked via interconnecting structures, and again can be shared with others or be reserved for the PN owner.
- *Interconnecting structures*, which can be infrastructure-based or ad hoc networks, e.g., the Internet, a UMTS network, a WLAN infrastructure.

Figure 2 illustrates the different components of a PN using the remote babysitting scenario presented in the previous section. The composition and organization of the PN will be determined by the applications it is intended to support and by the context it and its owner are operating in. It is clear that a particular application will require particular resources and services. This implies that particular devices or clusters of cooperating devices will need to be incorporated in the PN, e.g., in the remote babysitting example, a camera and a microphone in a specific geographical location are essential. Not always will the request for a particular service lead to the demand for specific devices, e.g., when a person in an airport lounge wants to print documents he or she is receiving, any printer in the persons vicinity might do.

4. Research Issues

It should be clear that in order to realize the concept of PNs a dynamic, a context-aware and application-driven communication substrate is needed for the many, and to a large extent unknown, applications that will be developed in the future. This substrate should be able

to incorporate many networking and link-level technologies and will have to interface with middleware which delivers generic services to the applications.

Some of the requirements and conditions, which make the design of PNs challenging, are:

- The very dynamic and unpredictable topology.
- The mobility of a PN and its components.
- The need for self-organization.
- The heterogeneity of the underlying link technologies.
- The variety of power, processing and storage constraints of the involved devices.
- The need for fast localization of devices and services.
- The geographical spreading of a PN.

In this vast problem domain, we focus on the communication aspects, and in particular, the architectural – and networking issues. However there are also issues, which are specific to PNs, in particular regarding middleware, the link layer and the physical layer, including MAC issues and radio access interfaces. These were discussed in [11]. In this paper we focus on the following crucial issues:

- The architecture of PNs.
- Resource discovery.
- Context discovery.
- Self-organization and adaptation.
- Addressing and routing.
- Co-operation with infrastructure-based networks and other interconnection structures.
- Security and accounting.

Important considerations for designing protocols and mechanisms for PNs are:

- The timeliness of the processes, directly tied to the user perception, e.g., how fast is a PN aware of changes in its environment and how soon can applications take this into account.
- The usage of communication bandwidth, since in a radio environment bandwidth will always be scarce.
- The complexity of the protocols and procedures: since many personal devices have restricted processing and storage capacities, the code footprint should be small.
- The energy consumption due to processing and communication should be low given that personal devices may have very restricted battery capacity.
- Devices may only intermittently be accessible due to mobility, energy conservation, and radio link characteristics.

Robustness and availability may be essential for certain applications, e.g., health related. This will be a difficult problem given the ad hoc and dynamic nature of a PN.

5. Architecture

The architecture of a PN concerns the structuring (or decomposition) in terms of functional entities and the way these entities interact with each other via underlying services (e.g., communication, authentication, etc.) to achieve the overall functionality required by the applications. An example of such functionality is the automatic discovery and secure incorporation

of a resource into a PN. The goal is to ensure that the technical design is consistent and coherent and that it will satisfy the requirements on network functionality. A crucial requirement of the architecture is that it is future proof with respect to the incorporation of new technologies.

In particular architectures need to be developed for the following PN functions:

- The organization and maintenance of the PN configuration such that particular applications can be run. This includes the discovery of resources.
- The discovery and maintenance of the PN context.
- The handling of QoS across heterogeneous and dynamically changing link layers and network nodes.
- The provisioning of a secure and private communication environment.
- The co-operation with a potentially large variety of infrastructure-based networks.

We will discuss these topics in more detail in the following sections. In terms of creating an architectural framework the following generic issues need to be resolved for each of the PN functionalities:

- Which co-operating entities need to be defined to provide a particular functionality?
- How is the mapping of functional entities to physical devices in a PN? Is it highly centralized or strongly distributed?
- How is the model for co-operation between the functional entities, e.g., is it a tightly coupled co-operation, is it in an asymmetric client server mode or a symmetric peer-to-peer mode?
- What underlying communication services and protocols are required between these functional entities?

In order to answer these questions a number of trade-offs have to be considered. In particular: the richness of the functionality needs to be balanced against the resulting software footprint, the processing-, storage- and communications requirements, the energy consumption, the response times to changing conditions and to application requests, and the robustness in the face of the network dynamics.

Relevant for PNs is the work on middleware architectures for mobile distributed systems. A survey can be found in [12]. This paper also considers hybrid systems, which consist of mobile ad hoc subsystems and infrastructure-based parts. A PN is in principle also a hybrid system. A concrete architecture involving a PN-like particular architecture is described in [13]. This solution solves many problems by relying on a dedicated infrastructure-based proxy, not unlike a home agent in Mobile IP. It leads to similar signaling-like overhead since the proxy is involved in many of the functions we discussed. Another significant approach which takes into account the restrictions and characteristics of future mobile pervasive computing devices is JXTA [14]. JXTA defines architecture for peer-to-peer computing based on an overlay network model and protocols for, e.g., service discovery, security, routing, etc. The architecture and protocols are kept minimal in order to increase the chances of achieving interoperability.

6. Resource Discovery

In order to form a PN capable of supporting a particular application with a particular quality, methods are needed for discovering what resources are available at different levels. A PN must be able, starting from its core PAN, to discover what devices, networks and services are around that it has the opportunity to link up with. This is what we call *resource discovery*.

For resource discovery, specific questions that need to be answered are:

- How should resources be characterized in terms of their functionality and their quality, such that their identities and capabilities can be communicated?
- How can a PN find out which resources are around and available either locally or remotely?

Let us now examine some techniques for resource characterization and discovery.

Resource Characterization
There are two aspects involved in resource characterization: *functionality* and *physical characteristics*. Examples of functionality are: display, loudspeaker, temperature sensor, communication device, router, and data host. A device and in particular a cluster may have multiple functionalities. For example, in the remote babysitting application, a single baby-videophone device may incorporate a camera, a microphone and a device with a UMTS or WLAN radio interface. The physical characteristics determine the quality with which the functionality is provided (a form of QoS). Examples are: the resolution of a display, the remaining energy in the battery of a portable device, the processing capacity of a computer, the available storage capacity for hosting data, and a measure of the trustworthiness of a device.

Given the variety of very different consumer and professional applications to be expected, a general description framework is needed, which allows describing, communicating and advertising the capabilities of devices and clusters of cooperating devices. Such a framework could, e.g., be based on XML [15]. An example of a resource description system, which seems to be well suited for use in PNs, is the Intentional Naming System (INS) developed at MIT [16]. It defines a language based on attributes and values, which allows applications to describe what they are looking for and not where to find it. INS specifically aims at resources in dynamic mobile ad hoc systems and is scalable to large numbers of resources within a domain. The same paper also analyses the shortcomings of present resource discovery techniques such as the IETF Service Location Protocol (SLP) [17], Sun's Jini service directory [18], the Simple Service Discovery protocol (SSDP) [19], universal plug-and-play [20], and Berkeley's service discovery service [21]. These solutions are not suitable for PNs, because they do not provide for the dynamism to be expected in PNs and preclude ad hoc operation since they involve infrastructure-based servers.

Techniques for Resource Discovery
Two types of strategies can be considered for resource discovery: proactive strategies and reactive strategies. In a proactive strategy, a PN attempts to be continuously aware of its environment and resources are available so that when a particular application needs to run, it can right away be determined whether this can be supported and the time needed to have the service available can be shortened. In a reactive strategy, actions are only undertaken when a particular application needs to be run. Depending on the time constants of the various processes involved, e.g., the mobility of the user, the fluctuations in radio channel characteristics, the processes of connection and disconnection of energy and cost aware devices, one or the other strategy will be better. These strategies have been explored in depth in the context of routing in mobile ad hoc networks [22].

The two usual techniques for discovering resources are:

- Advertising, i.e., through beacon messages, entities broadcast information about resources to devices in their neighborhood.

- Soliciting, i.e., an entity looking for resources broadcasts a query message and gets eventually a response from devices that have knowledge about the availability of resources.

Advertising and soliciting are standard techniques used in wireless and mobile networking, e.g., in IEEE 802.11 WLAN both are used to connect mobile devices to an Access Point, and Mobile IP relies on router advertisements for mobile hosts to get connected and obtain a care-of-address. These principles can also be applied in PNs.

A less common method, which allows a device to be in a passive mode, is to overhear unencrypted parts of communication between devices in its neighborhood, i.e., messages not addressed to the device. From this it may be able to deduce the presence of certain resources in its neighborhood. A technique with a lot of potential consists of an entity combining context information with a learning process. An entity acquires and retains knowledge about the availability of resources in a particular context. Examples are, e.g., knowing that one enters one's car may imply that there is voice recognition and synthesis equipment available or, when a person enters his or her office or home, the PN knows already what is available without having to go through a discovery process. Another alternative is to acquire this knowledge through "hearsay". A friendly device or network in its proximity tells it right away all it knows about the resources that are accessible so that the persons PN does not have to go through a learning process, and can concentrate right away on establishing the desired services.

An example of a resource discovery mechanism, which takes these considerations into account and relies on an efficient spreading of resource information using a "hearsay" approach, has been developed in the IBM DEAPspace project [23].

7. Context Discovery

The context of a PN and its owner is still a vaguely defined concept. We can refer to the research in context-aware mobile computing [24]. According to [12] context is everything that can influence the behavior of an application. Context-aware applications exploit information about, e.g., the geographical location, the time of day, the available equipment, the interaction history and the presence of other people to provide the user with a service, which is best suited to his/her present situation [12].

However, a new element is introduced in PNs, which makes context-awareness a more complex issue than in PANs. Since a PN may have a geographical spreading, which causes different parts of the PN to operate in different environments simultaneously; one will have to find ways to resolve the resulting effect on the applications. The knowledge that parts of a PN are physically in a hostile environment may inhibit certain sensitive applications. An example is the case where a PN strictly operating in a physically secure environment such as an office building is allowed to run business applications, while a PN in a less secure place like a public restaurant precludes the running of the same applications. Moreover multiple applications with different environment-related restrictions or opportunities are likely to coexist. This implies, e.g., that for particular applications the incorporation and use of certain devices or resources may be undesirable. The owner of the PN also determines the context, e.g., the geographical location of a person, the time of day, and the explicit or implicit wishes to use particular services determine which devices and network elements will be incorporated in a PN.

Discovering what context a PN or its components are operating in is in general important since it may determine what applications are allowed to run and what entities are needed

to make these applications possible. In Section 6 we already hinted at the fact that context discovery can also be important for resource discovery, e.g., the knowledge that a person is entering a car may trigger the extension of a PN with on-board devices such as voice recognition and synthesis equipment.

The questions that need to be answered are:

- What constitutes the context for a PN and its parts, and how should it be characterized and represented? E.g., how do we characterize a public place, a private home, the office and one's private car?
- How can a PN find out which context its parts are operating in? One has to distinguish between the core-PAN and eventual other private clusters of devices belonging to the PN.
- Each of these has to detect what context it is in. For each, techniques could be applied that are applicable to PANs as well.

Characterizing the context is an open issue being researched in context-aware computing. Let us now examine some principal techniques for context discovery.

Techniques for Context Discovery
Some potential methods are:

- Being told by the surrounding devices, through advertising or beacon messages, e.g., when entering a public WLAN hotspot, or by entering a car.
- By asking the environment, i.e., sending query messages.
- By listening in on messages in the environment providing one is authorized to do so.
- By determining the absolute or relative geographical position and by having knowledge about the implications of a particular geographical position, e.g., knowing that one has entered one's office or knowing that one is close enough to a particular facility.
- By making an infrastructure-based association, e.g., a device can remember that a car has a WLAN base-station with a certain ID and in its neighborhood are more devices such as a car stereo and a microphone.
- By direct user intervention, e.g., the user can indicate that he or she wants to operate with a particular profile, for instance in a business mode, implying that some predetermined resources will be needed or the user may hit a button when privacy is desired.

Context characterization and discovery are very much research topics with no crystallized solutions [24].

8. Self-Organization

In general, PNs will consist of a large variety of heterogeneous entities (devices and clusters of devices) connected in an ad hoc and dynamic fashion. The state of these entities may change from active to stand-by or sleeping and disconnected during the running of applications. The constituent entities and the links that interconnect them may change frequently due to the radio link characteristics, mobility and state changes of devices (e.g., turning themselves of to save power). Access to infrastructure-based networks and servers (the Internet in particular) may not always be available or may be incidental. Under these circumstances network management cannot rely on specific functionality (e.g., such as DHCP) to be available in particular servers. The PN needs to be self-organized, meaning that there is no reliance on infrastructure-based servers, e.g., a DHCP server, and that there is no server functionality long-term associated with

particular network entities. This is a problem, which is inherent in mobile ad hoc networks and is more severe in PNs than in PANs.

In configuring and reconfiguring a PN one can consider a number of levels of connectivity (assuming a layered architecture of a PN). The first one is at the physical and link level, the second one is at the network level, further at the distributed computing or middleware level, e.g., between distributed objects offering operating system-like generic functions, and ultimately at the application level, where distributed application entities spread over the PN components cooperate to run a particular application.

In order to establish connectivity, entities will have to use resource discovery and context discovery at various levels. Ad hoc topologies will have to be established for supporting the cooperation between distributed entities. To what extent these topologies are kept in system states will depend on the dynamics of the PN at various levels.

At link level for WLANs, the self-organizational techniques are embedded in standards such as IEEE 802.11. For Bluetooth networks, likely to be an important link technology for the device clusters constituting a PN, the self-configuration of the elementary piconets containing up to eight nodes is part of the standards. The self-configuration of so-called scatternets consisting of multiple piconets however is still a topic of research. The issues are the time complexity of the algorithm, the number of messages exchanged, which is related to the energy consumption, and the quality of the resulting scatternet in terms of the efficiency, of radio channel usage, the network diameter, which is important for message delay, and the degree of connectivity of nodes, which relates to the relaying load of bridging nodes. Solutions are provided for nodes with a limited number of nodes (maximum 36) in [25] and a scalable solution is described in [26]. All solutions assume that nodes are all within radio range of each other. In [27] an algorithm is proposed for fixed scatternets with nodes that are not all within range of each other. All these solutions for self-organising Bluetooth networks only address the initial configuration. The TSF protocol [28] on the other hand considers a dynamic environment where nodes are allowed to join and leave. Moreover it does not require that every node be within radio range of every other node. The problem faced in PNs, where nodes join and leave already established clusters dynamically are not yet solved.

For the network level the problem has been studied extensively. Many routing strategies have been devised and analysed [22], e.g., long distance geographic routing is a technique, which relieves the nodes from keeping volatile network state information about distant nodes and links. In Section 10 this is discussed further. At the middleware level, there is a lot of ongoing research but no crystallized solutions yet [13]. At the application level the large diversity of potential application characteristics makes it a wide-open field.

Specific solutions for self-organization of PNs can benefit from the fact that there is some structure present in a PN as we have sketched in Section 3. This may suggest solutions, which use a hierarchical approach, e.g., giving a central role to the core PAN and some essential devices. But this is not a necessity.

9. Addressing

Addressing in PNs is related to the identification of resources, which was discussed in the previous section. Where resource identification or naming mainly relates to the application level, addressing is related to the actual transport of messages to specific network elements. We

do not consider link level addresses, which will be determined by the specific link technologies that are used, e.g., as defined by IEEE 802.

What is specific for PNs regarding addressing is that

- They have a composite and heterogeneous structure, consisting of devices and cooperating ad hoc clusters of devices linked via different link technologies.
- The devices within a cluster are moving with respect to each other, complete clusters are moving with respect to each other, with respect to single devices incorporated in the PN and with respect to the infrastructure-based networks that tie them together.
- Some of shared or public devices temporarily incorporated in a PN may have their own addresses.

The structure of a PN would favor some form of hierarchical addressing. If IPv6 addressing will be used the mechanisms used or proposed in IPv6 to establish an address space when networks attach to each other or merge are likely solutions. On the other hand not all devices in a PN may have IP addresses and be equipped with an IP stack.

An interesting point of view is taken in [13]. PNs are intimately tied to a particular person. For applications involving parties in the outside (external to the PN) world wanting to communicate with a PN, it makes sense not to demand that they know which particular device in a dynamic ad hoc PN needs to be addressed, but to send the message to "the person". This implies that a network address (e.g., an IP address) is associated with a person. One could realize this by, e.g.,

- Any device or a set of devices belonging to the PN recognizing the person-associated address (anycasting), and forwarding the message to the device on which the application is known to run at that moment. Any node at the periphery of a PN with connections to infrastructure-based networks could be a candidate for that role.
- Having a specific device, e.g., a kind of home agent or proxy, with this address, which has the specific role of knowing the state of the PN and forwarding the message to the appropriate device. This is the solution chosen in [13].

10. Routing

There are some specific aspects to routing in PNs, which makes that most solutions proposed for mobile ad hoc networks are not suitable:

- Routing takes place at different levels: routing within a PAN (intra-PAN routing), routing within a PN, which may involve other infrastructure-based and ad-hoc networks, including other PANs (intra-PN routing), and routing among different PNs (inter-PN routing).
- There may be multiple radio links to interconnect devices (e.g., WLAN and Bluetooth) and to connect to infrastructure-based networks (e.g., cellular and WLAN).
- It has to deal with strong heterogeneity of nodes and (radio) links.
- It has to be very power efficient (at least for some nodes) and bandwidth efficient.
- It may have to be cost efficient, given the use of infrastructure-based networks, which charge for their services.

Routing in ad-hoc networks has received a lot of attention in recent years. In particular, the efforts around the mobile Ad Hoc Networking (MANET) [30] Working Group of the

Internet Engineering Task Force (IETF) have resulted in many protocols. Even when this work provides valuable insight in the problem, it has mostly concentrated on homogeneous nodes and single parameter optimization. A good overview of routing protocols for mobile ad hoc networks is given in [29]. A number of proposed techniques use principles used in fixed networks, e.g., link state, distance vector, source routing and hierarchical routing schemes. Specifically new for mobile ad hoc networks is the concept of geographic position assisted routing, which has the advantage that the intermediate nodes do not have to keep large routing tables in storage, which is a burden for small mobile devices. Some of the routing protocols proposed are hybrids. An illustrative example is found in [30] where a combination is used of a geographical technique for long distance routing and a distance vector protocol in the proximity of the destination.

Research is needed on routing in PNs, taking into account the following:

- We can make use of the fact that a certain hierarchy can be recognized in the structure of a PN. This leads to the distinction between intra-cluster and inter-cluster routing. This is shown in Figure 3. Another reason to introduce hierarchy in routing is the inequality between the capabilities of the different network elements, limiting for instance the routing capabilities of certain nodes. Link technologies such as Bluetooth also impose a hierarchical scheme.

- Scalability in terms of numbers of network nodes may not seem the overriding concern, since unlike other ad hoc networks like sensor networks, PNs might not contain a huge number of devices, because of the personal nature of many of the devices. However we should be careful not to exclude a priori scenarios where a PN incorporates a very large number of devices. Moreover scalability will still be a concern because of the limited processing and storage capacities of many personal devices.

- Routing should take into account multiple points of connectivity of network elements with the infrastructure based-networks and with each other. Multipath routing should be considered for reasons of seamlessness, capacity, reliability and cost, e.g., a reliable UMTS link with QoS guarantees for voice and a less reliable but cheaper WLAN link for file transfer or streaming video transfer may be combined to support a single session. An example of infrastructure-oriented routing is shown in Figure 4.

- Routing will have to consider multiple constraints, e.g., transmission power, energy consumption, bandwidth usage, delay and QoS and cost of usage of the resources in infrastructure-based networks.

- It is likely that routing in PNs will not rely on a single routing protocol, but combine various protocols to support an application.

- The presence of an infrastructure-based network may offer opportunities for more efficient and less energy and bandwidth consuming routing in a PN by utilizing paths through this network instead of, e.g., ad hoc multi-hop routing within an ad hoc cluster belonging to a PN.

An example of a routing protocol for a PN like network is described in [13], which uses a hierarchical approach.

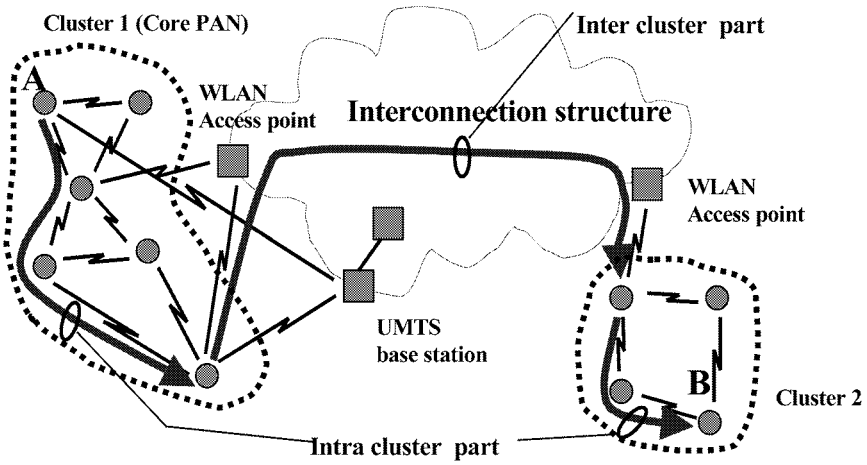

Figure 3. Routing in PNs (from A to B).

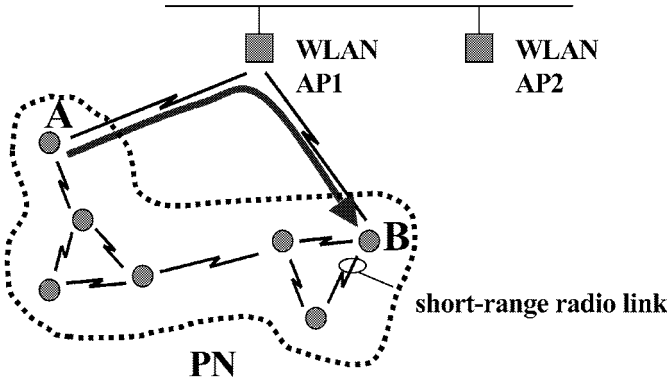

Figure 4. Infrastructure-oriented routing.

11. Co-Operation with Infrastructure-Based Networks and Other Interconnection Structures

There are two reasons why PNs may want to co-operate with infrastructure-based networks and other interconnection structures and use their resources and services. They might want to extend themselves with remote devices or remote networks and they might want to access specific services delivered by servers that are not part of the PN.

The types of infrastructure-based networks a PN might need to co-operate with are:

- Public cellular networks, e.g., GPRS and UMTS.
- Public or private fixed networks, e.g., one of the temporary nodes of a PN may be a stationary device with both radio interfaces and a fixed connection to the Internet, an organization's intranet or extranet, or a private home network.
- Public or private WLAN infrastructures, e.g., wireless campuses, WLANs in airport lounges, cities, train stations and inside trains.

Co-operation with fixed infrastructures poses a new set of problems. Up to now solutions have been proposed and implemented for single terminals or hosts interacting with such infrastructures, in particular in the context of cellular systems and Mobile IP. In PNs we no

longer have single terminals (like in cellular systems or WLANs) or hosts (like in Mobile IP), but a very dynamic and heterogeneous mobile ad hoc network wanting to establish co-operation with the infrastructures. This implies, e.g., that existing solutions either do not work any longer or have to be modified.

One of the main concerns is that for many applications one would like that the establishment and maintenance of the co-operation is seamless.

The specific issues that need to be addressed are

- Routing: the presence of an infrastructure may offer opportunities for more efficient and less energy and bandwidth consuming routing in a PN.
- Establishing and maintaining QoS for particular applications, across a diversity of network and link technologies throughout the PN.
- Roaming and (vertical) handovers: here seamlessness is an important issue, in particular, how to deal with QoS during handovers.
- Environment and position awareness and tracking, where the infrastructure may provide information to PN nodes.
- Ways to use specific functionality, e.g., caching and processing offered by the infrastructure.
- Dealing with the mobility of terminal devices and subnets will in general ask for new solutions. Part of a PN, the core PAN, moves around with its owner, while other remote parts may remain stationary. Worth mentioning in this context are the activities on mobile networks within the Mobile IP Working Group [31] of the IETF and the work on extensions of mobile IP for mobile ad-hoc networks interconnection [32, 33, 35].

Interaction with other networks will also have a strong impact on security and may have accounting consequences. This will be discussed in the next section.

12. Privacy, Security and Accounting

The concept of a PN will only inspire trust and be accepted by its users when a sufficient level of security is guaranteed. Since PNs are very much centered on the needs of an individual, measures will have to be taken to protect the privacy of the owner of the PN.

PNs rely to a large extent on wireless links, which makes them vulnerable to eavesdropping and malicious interference. However, this is the same problem as faced by all wireless communication (see e.g. [36]). Solutions developed in wireless LANs, short range and cellular radio link technologies will be part of the security measures in PNs.

The ad-hoc nature of PNs will pose serious challenges for authentication and authorization. In particular security threats are posed by:

- The opportunity-driven incorporation of foreign devices into PNs.
- The incorporation of remote own devices through third party networks.
- The linking up or merging with other PNs and with infrastructure networks.
- The loss of own devices may not jeopardize the privacy and security of the rest of the PN.

PNs are nomads with respect to the infrastructure; this implies that they in turn also pose a threat to other networks. They will have to be properly authenticated and authorized. Another concern is raised because PNs may make use of the resources of other persons or organiza-

tions. Furthermore they rely occasionally on network infrastructures. This may not come for free and may require an accounting and charging mechanism.

The ad-hoc and distributed nature of personal networks often excludes the use of centralized servers. A different approach to security based on distributed key exchange and authentication is required. A major challenge here is to find solutions that are efficient in bandwidth usage and at the same time able to deal with the large variety of handheld and other portable devices and their constraints, as limited computing resources, limited battery, limited input/output capabilities. Partial solutions to the problems mentioned above have been reported in [37–41].

13. Conclusion

In this paper we have introduced the concept of Personal Network (PN). A PN extends and complements the concept of pervasive computing by creating a personal distributed environment where people interact with various companion, embedded, or invisible computers not only in their close vicinity but potentially anywhere, i.e., independent of their geographical location.

The concept of PN starts from a Personal Area Network (PAN) and extends its reach to incorporate remote personal, shared or public devices or even networks, such that a communication substrate is formed on which personal applications can run independently of the physical location of the needed resources. A key idea is that a PN is configured in an ad hoc fashion, as the opportunity and the demand arise, to support personal applications.

We showed that this concept introduces new challenges: the heterogeneity of the involved technologies, the need for self-organization, the dynamics of the system composition, the application-driven nature, and the security hazards. We have discussed the impact of these problems on network design. We have shown to what extent these issues are subject of ongoing research. Although many of the results could be applied to the PN domain, research activities focused on this specific area are needed to make the concept of PN a reality.

References

1. K. Ducatel et al., "Scenarios for Ambient Intelligence in 2010", IST Advisory Group (ISTAG), European Commission, Brussels, www.cordis.lu/ist/istag.htm, 2001.
2. W. Mohr et al., (eds.), "The Book of Visions 2000 – Visions of the Wireless World", Version 1.0, Wireless Strategic Initiative, www.wireless-world-research.org, November 2000.
3. J. Zander et al., "Telecom Scenario's in 2010", PCC, KTH, Sweden, 1999.
4. ACM, "The Next 1000 Years", *Special Issue of Communications of the ACM*, Vol. 44, No. 3, 2001.
5. F. Daoud and S. Mohan, "Service Portability and Virtual Home Environments", Guest editorial, *IEEE Communications*, Vol. 40, No. 1, pp. 76–77, 2002.
6. S.K. Gupta, W.-C. Lee, A. Purakayastha and P.K. Srimani, "An Overview of Pervasive Computing", Guest editorial, *IEEE Personal Communications*, Vol. 8, No. 4, pp. 8–9, 2001.
7. Bluetooth, http://www.bluetooth.com/
8. IrDA Standard, http://www.irda.org/
9. C. Bisdikian, P. Bhagwat and N. Golmie, "Wireless Personal Area Networks", Guest Editorial, *IEEE Network*, Vol. 15, No. 5, pp. 10–11, 2001.
10. IEEE, www.ieee802.org/15/about.html
11. I.G. Niemegeers and S.M. Heemstra de Groot, "From Personal Area Networks to Personal Networks: A User-Oriented Approach", *Kluwer International Journal of Wireless and Personal Communications*, Vol. 22, No. 2, pp. 175–186, 2002.

12. L. Capra, W. Emmerich and C. Mascolo, "Middleware for Mobile Computing", www.cs.ucl.ac.uk/staff/L.Capra/middlewaresurvey.pdf, 2002.
13. R. Kravets, C. Carter and L. Magalhaes, "A Cooperative Approach to User Mobility", *Computer Communication Review*, Vol. 31, No. 5, pp. 57–69, 2001.
14. B. Traversat, M. Abdelaziz, M. Duigou, J.C. Hugly, E. Pouyol and B. Yeager, "Project JXTA Virtual Network", Sun Microsystems, Inc., February 5, 2002.
15. T. Bray, J. Paoli and C.M. Sperberg-McQueen, "Extensible Markup Language Recommendation", http://www.w3.org/TR/1998/REC-xml-19980210, World Wide Web Consortium, March 1998.
16. W. Adjie-Winoto, E. Schwartz, H. Balakrishnan and J. Lilley, "The Design and Implementation of an Intentional Naming System", *Operating Systems Review*, Vol. 34, No. 5, pp. 186–201, 1999.
17. J. Veizades, E. Guttman, C. Perkins and S. Kaplan, "Service Location Protocol", RFC 2165, IETF, June 1997.
18. Jini ™, http://java.sun.com/products/jini/, 1998.
19. Y. Goland, T. Cai, P. Leach, Y. Gu and S. Albright, "Simple Service Discovery Protocol/1.0", IETF Internet Draft, expired December 1999, June 1999.
20. Microsoft, "Understanding Universal Plug and Play", White Paper, http://upnp.org/download/UPNP_UnderstandingUPNP.doc, Microsoft Corporation, 2000.
21. S. Czerwinski, B. Zhao, T. Hodes, A. Joseph and R. Katz, "An Architecture for a Secure Service Discovery Service", *Proceedings ACM/IEEE Mobicom*, pp. 24–35, 1999.
22. C.E. Perkins, *Ad Hoc Networking*, Addison Wesley, 2001.
23. M. Nidd, "Service Discovery in DEAPspace", *IEEE Personal Communications*, Vol. 8, No. 4, pp. 39–45, 2001.
24. G. Chen and D. Kotz, "A Survey of Context-Aware Mobile Computing Research", Department of Computer Science, Darthmouth Computer Science Technical Report TR2000-381, Darthmouth College, 2000.
25. T. Salonidis, P. Bhagwat, L. Tassiulas and R. LaMaire, "Distributed Topology Construction of Bluetooth Personal Area Networks", *INFOCOM 2001, Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, Proceedings, IEEE*, Vol. 3, pp. 1577–1586, 2001.
26. C. Law and K.Y. Siu, "A Bluetooth Scatternet Formation Algorithm", *Global Telecommunications Conference, 2001, GLOBECOM '01, IEEE*, Vol. 5, pp. 2864–2869, 2001.
27. G.V. Zaruba, S. Basagni and I. Chlamtac, "Bluetrees-Scatternet Formation to Enable Bluetooth-Based Ad Hoc Networks", *ICC 2001, IEEE International Conference on Communications 2001*, Vol. 1, pp. 273–277, 11–14 June 2001.
28. G. Tan, A. Miu, J. Guttag and H. Balakrishnan, "Forming Scatternets from Bluetooth Personal Area Networks", MIT Laboratory for Computer Science, MIT-LCS-TR-826, 2001.
29. X. Hong, K. Xu and M. Gerla, "Scalable Routing Protocols for Mobile Ad Hoc Networks", *IEEE Network*, pp. 11–21, July/August 2002.
30. J. Hubeaux, T. Gross, J. Le Boudec, and M. Vetterli, "Toward Self-Organised Ad Hoc Networks: The Terminodes Project", *IEEE Communications Magazine*, January 2001, pp. 118–124.
31. IETF MANET Working Group, http://www.ietf.org/html.charters/manet-charter.html
32. J. Broch, D.A. Maltz and D.B. Johnson, "Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks", in *Proceedings of IEEE International Symposium on Parallel Architectures, Algorithms, and Networks*, Perth, Australia, June 23–25 1999, pp. 370–375.
33. U. Jönsson, F. Alriksson, T. Larsson, P. Johansson and G.Q. Maguire Jr., "MIPMANET – Mobile IP for Mobile Ad Hoc Networks", in *Proceedings of the IEEE/ACM Workshop on Mobile and Ad Hoc Networking and Computing*, Boston, U.S.A., August 11 2000, pp. 75–85.
34. C. Perkins and H. Lei, "Ad Hoc Networking with Mobile IP", in *Proceedings of the Second European Personal Mobile Communication Conference*, Bonn, Germany, September 30–October 2 1997, pp. 197–202.
35. V. Typpö, "Micro-Mobility within Wireless Ad Hoc Networks: Towards Hybrid Wireless Multihop Networks", Department of Electrical Engineering, University of Oulu, Finland, Diploma Thesis, August 2001.
36. T. Karygiannis and L. Owens, "Wireless Network Security: 802.11", Bluetooth and Handheld Devices, National Institute of Standards and Technology (NIST), U.S., 2002.
37. C. Candolin and H. Kari, "A Security Architecture for Wireless Ad Hoc Networks", *IEEE Milcom 2002*, Anaheim, California, October 7–10, 2002.

38. B. Awerbuch, D. Holmer, C. Nita-Rotaru and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures", in *ACM Workshop on Wireless Security (WiSe) in conjunction with MobiCom 2002*, Atlanta, Georgia, September 28.
39. C. Xenakis and L. Merakos, "On Demand Network-wide VPN Deployment in GPRS", *IEEE Network*, Vol. 16, No. 6, pp. 28–37, 2002.
40. J. Yong, M. Gerla and R. Gadh, "Providing Multilayer Security Support for Wireless Communications across Multiple Trusted Domains", UCLA Computer Science Technical Report, 020032.
41. L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks", *IEEE Networks*, Vol. 13, No. 6, pp. 24–30, 1999.

Ignas G.M.M. Niemegeers got a degree in electrical engineering from the University of Gent, Belgium, in 1970. In 1972 he received an M.Sc.E. degree in computer engineering and in 1978 a Ph.D. degree from Purdue University in West Lafayette, Indiana, U.S.A. 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 at the Computer Science and the Electrical Engineering Faculties of 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 on ICT and applications. Since May 2002 he holds the chair Wireless and Mobile Communications at Delft University of Technology, where he is heading the Centre for Wireless and Personal Communication (CWPC) and the Telecommunications Department. He is an active member of the Wireless World Research Forum (WWRF) and IFIP TC-6 Working Group on Personal Wireless Communication. He was involved in many European research projects, in particular ACTS TOBASCO, ACTS PRISMA, ACTS HARMONICS, RACE MONET, RACE INSIGNIA and RACE MAGIC. His present research interests are Beyond 3G wireless infrastructures, UWB networks, ad-hoc networks, Personal Area Networks and Personal Networks, Mobile IP and ubiquitous computing and communication.

Sonia Heemstra de Groot received a M.Sc. degree in electrical engineering from Mar del Plata National University, Argentina, in 1983, she did post-graduate studies at the Philips International Institute resulting in a second M.Sc. degree from Netherlands University Federation For International Cooperation (NUFFIC) in 1986, and a Ph.D. degree in electrical engineering from the University of Twente, The Netherlands, in 1990. From 1991 to 1998 she was a lecturer in the Tele-Informatics and Open Systems group of the Faculty of Electrical Engineering at the University of Twente. Since 1999 she is an associate professor in the area of networking at the Faculty of Computer Science of the same university. She has been managing the participation of the University of Twente in the European projects BELSIGN, ACTS TOBASCO, ACTS PRISMA, and ACTS HARMONICS. In 2001 she joined the Wireless Multimedia Research Group at Ericsson EuroLab Netherlands (ELN). Since 2003 she holds the position of chief scientist at the Twente Institute of Wireless and Mobile Communications in The Netherlands. At this moment she is project manager of a Dutch project on 4th generation mobile networks, involving academic institutes and industry. Her present research activities include access networks, wireless and mobile networks, and ad-hoc networks. She is a member of the IFIP TC-6 Working Group on Personal Wireless Communication.