A Network Layer Architecture for Personal Networks[*]

Martin Jacobsson†, Jeroen Hoebeke‡, Sonia Heemstra de Groot††, Anthony Lo†, Ingrid Moerman‡,
Ignas Niemegeers†

†Delft University of Technology
P.O. Box 5032, 2600 GA Delft,
The Netherlands

m.jacobsson@ewi.tudelft.nl
a.lo@ewi.tudelft.nl
i.niemegeers@ewi.tudelft.nl

‡IMEC vzw - Ghent University
Department of Information
Technology (INTEC)
Sint-Pietersnieuwstraat 41
B-9000 Gent, Belgium
jeroen.hoebeke@intec.ugent.be
ingrid.moerman@intec.ugent.be

††Twente Institute for Wireless
and Mobile Communication
Institutenweg 30
7521 PK Enschede
The Netherlands

Sonia.Heemstra.de.Groot@ti-wmc.nl

Abstract

Personal Networks (PN) is a new concept related to pervasive computing with a strong user-focused view. While several existing technologies can offer solutions to part of a person's future communication needs, there is very little work on combining these technologies into something a normal user can handle. It will undoubtedly be the network layer that should integrate a person's all devices and networks into one single network for the person; the Personal Network. This paper introduces a network layer architecture for PNs that can handle the dynamic and demanding situation a PN is facing. Discussions of some related network layer concepts, issues and possible solutions are given in the end of this paper.

1. Introduction

Future mobile and wireless systems have been discussed as visions for several years. New wireless technologies have been developed, such as Wireless Local Area Networks (WLAN) [1], Bluetooth [2] and other Wireless Personal Area Networks (WPAN) technologies [3]. All these technologies have triggered researchers and innovators to think about future mobile wireless systems that will address our need for communication and much more. As a consequence, new research fields are emerging, addressing different aspects of future mobile wireless systems.

Personal Networks (PN) [4] is a new concept related to pervasive computing with a strong user-focused view that is being developed within the IST MAGNET project [5]. PN extends a person's Personal Area Network (PAN) that surrounds him with other devices and services farther away. This extension will physically be made via infrastructure-based networks, vehicle area networks, a home network or multi-hop ad hoc networks. A person's PN is configured to support the person's applications and takes into account the person's context, location and communication possibilities. A PN must adapt to changes in the surroundings, be self-configured and support many different types of networks and devices.

The key to a successful PN realization is a general network layer architecture that can bridge different technologies and offer a homogeneous and clear view to the end-user. Since a PN should address a person's all communication needs, a PN must include not only the person's wearable and wireless devices but also devices in the home, the car and in the office, etc. It will undoubtedly be the network layer that should integrate all these devices and networks into one PN. This means that the network layer of the PN must work as a home network at home, a car network in the car, a WPAN around a person and glue all these networks together in one PN and at the same time cooperate with existing networks such as infrastructure networks and other fixed networks.

The network layer architecture we suggest in this paper is a general one which could be used in all these situations and provide one single solution, which will make it easier for normal users to setup and maintain. The underlying link layer technologies will meet the different communication needs in the different environments. A fast wireless technology can meet the requirements of bandwidth demanding multimedia traffic in the home, while short range power efficient technologies are more suitable for the network around a person on the move. The PN network layer will be the same in all these environments, but may operate in different modes to meet the requirements in the different environments. In this way, it is believed that communication between different environment and types of networks can function seamlessly.

The rest of this paper will further explain the details of the overall PN architecture and in particular the network

[*] While part of this work is sponsored by the IST MAGNET project, some aspects presented in the paper do not necessarily reflect the MAGNET view.

layer architecture. Section 2 will give a scenario and some motivations of PN, while section 3 lists some existing proposals. Section 4 introduces the three-layer architecture of a PN and Section 5 introduces the proposed network layer architecture of PN. Section 6 goes further in depth of the network layer architecture by discussing some issues and their possible solutions. Conclusions are given in Section 7.

2. Scenarios and Motivations

Transportation and logistics represent a major business industry employing millions of truck drivers. Each day, these people spend hours in their vehicle while driving, waiting or sleeping and they are often multiple days away from home. Offering these people the ability to stay in touch with their family by creating a virtual home environment, offering them the ability to stay connected with their company and clients or offering them the possibility to contact their colleague truck drivers, could have great commercial potential taking into account the large number of truck drivers world wide.

Consider a truck equipped with a mobile phone, broadband Internet access, TFT display, headset, etc. forming a cluster of cooperating devices. When finished working, a truck driver could set up an Internet connection to his home. At home, a cluster of cooperating cameras, speakers, headsets, provides the truck driver with a virtual home environment. Through this environment, he can virtually walk around, seeing his family, talking with them, playing games, etc. Figure 1 demonstrates this scenario.

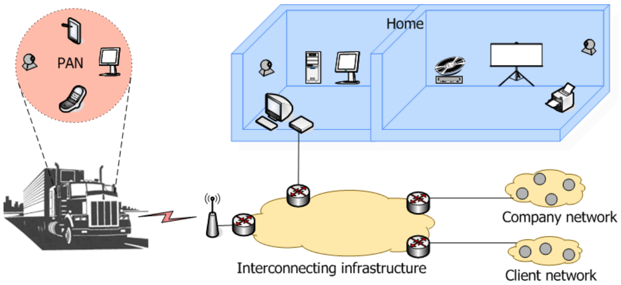


Figure 1: Virtual Home Truck

While driving, the truck driver can listen to his digital music collection by streaming it from a server in his network at home. When the truck driver stops at a parking, he can read his e-mail, search for colleagues, play a game with other truck drivers, etc. When the truck driver arrives at a client, his PAN can connect to the client's company network and download the necessary documents. The documents can be digitally signed, handed over to the client and a copy can be uploaded to the truck driver's company, reducing the administrative burden.

While several existing technologies can offer solutions to part of this scenario, there is very little work on combining these technologies into something a normal user can handle. In addition to offer the user instant access to services and communication, PN also needs to be easy to use, setup, configure and maintain as well as fast and secure. The target of PNs is to provide users with exactly that.

3. Existing Solutions

Most technologies focus on a particular aspect of future wireless communication. Here we list proposed solutions that try to meet more of a person's communication needs.

In a proposal from the University of Illinois at Urbana-Champaign and the Mobius project [6], they group devices in close vicinity into so called Mobile Grouped Devices (MOPEDs). Each MOPED is connected to a proxy (some kind of home agent) via an infrastructure connection. MOPED is not suitable for PN because it is still too dependent on the proxy and the infrastructure. Furthermore, MOPED does not address direct ad-hoc communication with other person's MOPEDs and is therefore still too limited to support the PN vision.

The Mobile VCE project has defined a concept called Personal Distributed Environment (PDE) [7]. PDE has a very similar vision to PN, but has no clear network architecture yet.

IXI Mobile [8] has a commercial product around a concept called Personal Mobile Gateway (PMG). It is basically a mobile phone with a WPAN-technology that has been extended to better manage a person's WPAN. PMG-enabled devices can communicate with each other and can also use the PMG-enabled mobile phone to connect to the infrastructure. However, all services are controlled by the operator and all external communication has to go through the operator's networks and this will not be able to meet a user's all future communication needs.

4. The PN Architecture

As shown in Figure 2, the IST MAGNET project [5] has proposed an architecture for PN, which is composed of three planes; the link layer plane, the network plane and the service plane.

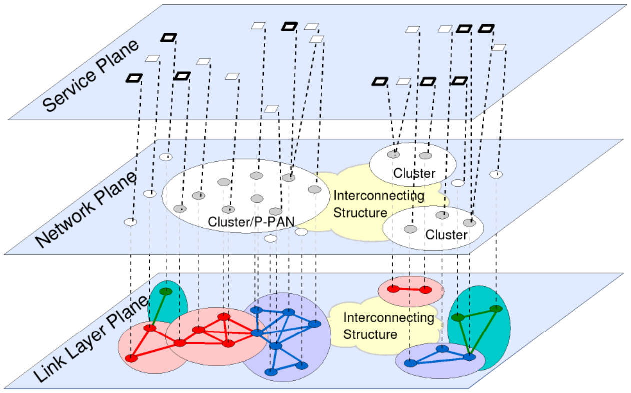


Figure 2: The Three-Layer PN Architecture

The link layer plane consists of various wired and wireless link layer technologies, including infrastructure links. The link layer will allow two nodes implementing the same technology to communicate if they are within radio range. To allow any two nodes within a PN to communicate, a network plane is needed.

The network plane divides the nodes into Personal and Foreign Nodes, based on whether a certain person owns that node or not. Personal Nodes form Clusters and Clusters can communicate with other Clusters via infrastructure. The next chapter will further develop the concepts of the network plane.

The highest plane in this architecture is the service plane. There are two types of services; public and private services. Public services are offered to anyone while private services are restricted to the owner or trusted persons by means of access control and authentication.

5. A Network Layer Architecture for PN

The network layer has to be as independent as possible from the underlying link layer so that current and future wireless communication technologies can be supported. In the Internet, IP was designed to meet this requirement and therefore IP is the proposed packet format also for wireless communication. The choice of IP also makes it easier to connect the wireless world with the Internet, which will be important also in the future.

The core idea of the architecture is to separate communication among nodes of the same user from communications of other nodes. Nodes belonging to the same owner form Clusters of Personal Nodes and they can communicate with any other Personal Node in that Cluster without using intermediate nodes not owned by the same person. The ownership is realized through a Personal Identifier (PID) that the owner uploads to all his devices. In this way, the communication, routing and other self-organizing mechanisms can be protected on a local scale. For the global scale, tunnels are established between the Clusters to both accommodate and protect the inter-Cluster communication. Figure 3 shows a high level abstraction of the proposed architecture. To further describe the architecture, some terminology and concepts will be introduced.

5.1. Concepts and Terminology

PN Node. A node with PN functionality, i.e., the node can be assigned a Personal Identifier.

Personal Identifier (PID). Each PN Node is equipped with an identifier, called PID, which could for instance be a large unique number. All devices owned by the same user are assigned the same PID to indicate that they have the same owner. In that case, the PID can also function as a shared secret for data encryption between two PN Nodes.

Personal Node. With respect to a certain PN Node, a Personal Node is another PN Node with the same PID as itself. Consider two PN Nodes: A and B. If both have the same PID, then A will consider B as a Personal Node. We can also talk about an owner's Personal Node, meaning a PN Node that has the owner's PID.

Foreign Node. Nodes with a different PID or with no PID at all. Nodes without PID or PN functionality are always considered as Foreign Nodes.

Cluster (of Personal Nodes). A Cluster of Personal Nodes is a collection of PN Nodes with the same PID that are connected to each other without help of Foreign Nodes. This means that two PN Nodes with the same PID are in the same Cluster if there is a path between them using only Personal Nodes (PN Nodes with that PID).

Personal Network (PN). Since each PN Node in all Clusters have the same PID, it is possible to establish encrypted tunnels between the Clusters. These tunnels together with the Clusters are what we consider a PN at the network layer.

Gateway Node. Some of the Personal Nodes of a Cluster might have links to Foreign Nodes. These nodes can be used by the Cluster to establish connections with local Foreign Nodes, the Internet, or other Clusters. However, being a Gateway Node requires extra functionality, which not all nodes can offer or should do. A Cluster might therefore select only a subset of the nodes to actually be Gateway Nodes.

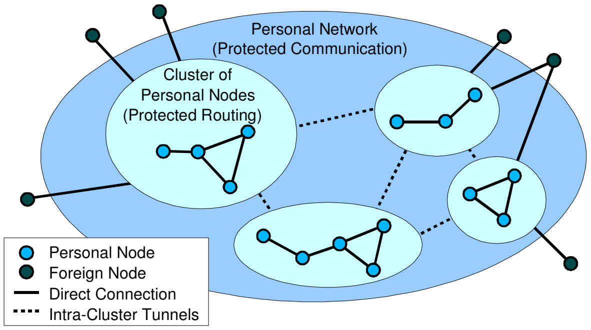


Figure 3: The Network Layer Architecture

5.2. Architectural Discussion

In this architecture, the home network of a person will be one Cluster, the car network another, the WPAN around the person a third and so on. Clusters work as local networks and therefore need their own local routing, addressing, self-configuration and other internal mechanisms. The formation of Clusters is a purely local process and does not need any support from infrastructure. The Cluster around a person is sometimes also referred to as the Private-PAN or P-PAN.

Clusters are dynamic in nature. Nodes are switched off or become available as well as roam and show up in a different Cluster. Clusters can split when a person takes some of the devices and leaves the rest behind. Likewise, Clusters can merge when a person arrives home with his wireless devices and they merge with the home Cluster.

To accommodate communication between Clusters, tunnels are established. The tunnels need to be maintained when Clusters merge, split and their nodes roam or are activated/deactivated. Clusters need to be able to find each other and Gateway Nodes must be selected as tunnel endpoints. All this must happen automatically in a fast and reliable way despite the dynamic behavior of PNs.

Gateway Nodes are also used to connect a Cluster to the outside world. They establish connections with Foreign Nodes in the vicinity of the Cluster or the Internet through an infrastructure-based network. Through the infrastructure, a Cluster can communicate with geographically distant Nodes.

It must be noted that the PID is an abstract concept and not necessary an implementation design. We have described the PID as being a unique identifier or a simple integer. While this makes it easier to explain, it is not a good implementation choice since there are many security problems involved with such an implementation. If a node gets stolen and the PID will be extracted from that device, then an attacker will have full access to the whole PN. On the other hand, if all Personal Nodes have different versions of the PID (all linked with each other in some way), it would be possible to exclude one of them when a node is stolen. Also note that the PID is not going to be used to protect services in a PN. Another security mechanism with proper authentication and access control should be used to protect services and data in a PN. The PID is there to protect the self-organization, self-configuration, internal routing, etc of the PN and its Clusters.

6. Network Layer Issues and Solutions

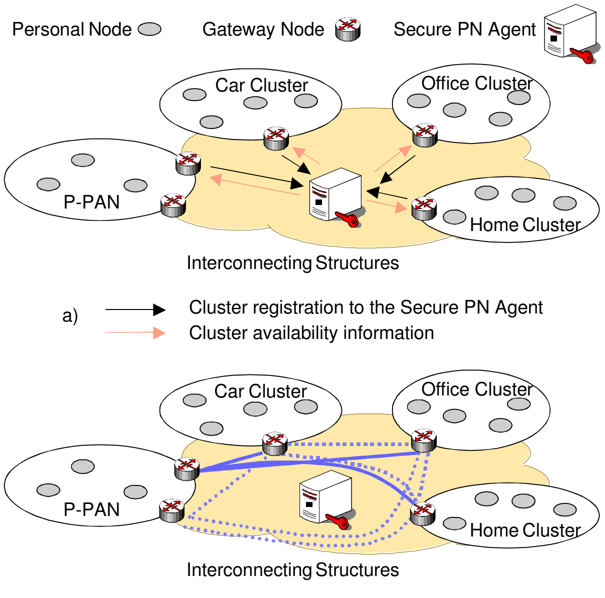
This section elaborates more on the details of the network layer of this architecture. Problems and possible solutions for organizing the Clusters in the PN, including routing and addressing, will be discussed as well as communication with Foreign Nodes and other PNs.

6.1. PN Organization and Maintenance

A PN can have multiple Clusters that are geographically dispersed. In order to form a PN and realize inter-Cluster communication, three requirements need to be fulfilled. First of all, the Clusters need to have access to the fixed infrastructure through one or multiple Gateway Nodes. Secondly, once access to the fixed infrastructure is available, the Clusters need to be capable of locating each other in order to establish tunnels between them. Thirdly, once the PN has been formed, it should be able to maintain itself regardless of changes in Gateway and Node mobility.

The first requirement, the discovery and selection of Gateway Nodes that provide access to the fixed infrastructure, can be fulfilled through the resource and service discovery mechanisms running within the scope of the Cluster. Such mechanisms are also being developed within the MAGNET project [5].

For the second requirement to be fulfilled, we introduce the concept of a *Secure PN Agent*. This concept can either be centralized, under the control of a single provider, or distributed over multiple providers or operators. Clusters that have obtained access to the interconnecting infrastructure announce their presence to the PN Agent as shown in Figure 4a. The announcements made by the Clusters need to contain at least the following essential information: the PID (to check their credentials to join a PN) and the attachment points of each Gateway Node to the infrastructure. The PN agent will communicate this information to the Cluster Gateway Nodes and this information will trigger the creation of secure tunnels between the Clusters which is shown in Figure 4b. Either only tunnels between the PAN and the remote clusters can be formed or a full mesh between the clusters can be established. The purpose of the tunnels is twofold. First, they provide secure inter-Cluster communication by shielding the intra-PN communication from the outside world. Secondly, these tunnels are established dynamically. When new Gateway Nodes are discovered or existing Gateway Nodes become unavailable (e.g. due to mobility), this information is propagated and the Gateway Nodes will react by dynamically updating the tunnels by destroying existing ones and creating new ones.


Personal Node
Gateway Node
Secure PN Agent
Car Cluster
Office Cluster
P-PAN
Home Cluster
Interconnecting Structures
a)
Cluster registration to the Secure PN Agent
Cluster availability information
Car Cluster
Office Cluster
P-PAN
Home Cluster
Interconnecting Structures

b) Secure and dynamic tunnel establishment

Figure 4: PN Formation and Maintenance

The final result is a self-creating, self-organizing and self-maintaining PN that consists of several Clusters interconnected by dynamic tunnels, providing security and hiding the Cluster mobility and Gateway Node changes from the nodes in the PN.

6.2. PN Addressing and Routing

Once the PN has been formed, intra-PN communication can take place. PN local resource and service discovery solutions will allow the Personal Nodes to learn about the available services and devices in the PN. However, in order to establish connectivity to these services and devices, addressing and routing are indispensable.

An interesting approach is to see the PN as an ad hoc network in which most of the links are wireless, some are wired and some are tunnels between the Clusters. Within this ad hoc network we can adopt a flat addressing scheme and run an ad hoc routing protocol that has been optimized for this environment. For instance, a PN internal IP prefix could be reserved and all nodes within the PN will select a PN-unique IP address with this prefix. This IP address will be independent of the location of the node in the PN. This approach has the great benefit that, in combination with the dynamic tunneling mechanisms, mobility will become completely transparent for the higher layer protocols. The ad hoc routing protocols will hide intra-Cluster mobility and the dynamic tunneling will hide Cluster mobility and Gateway Node changes.

6.3. External Communication

Communication with Foreign Nodes or infrastructure requires non-local addresses. However, when connecting through infrastructure, the Gateway Node needs a topological correct address. This address has to be obtained from the infrastructure itself using DHCP [9] or similar mechanisms. The obtained address is the one used to setup tunnels to other Clusters, so the Gateway Node needs to communicate it to the PN database.

When communicating with Foreign Nodes in an ad-hoc way, the address is not important. However, if that Foreign Node is part of someone else's PN, the PN internal addresses can not be used and this is not recommended anyway for security reasons. A random temporary address should be chosen by the Gateway Node to be used when communicating with that node. This will also have the advantage that the PN can remain anonymous if required. When another Personal Node wishes to communicate with a Foreign Node, then the Gateway Node must provide address translation between the internal addresses and the addresses used to communicate with the Foreign Nodes. However, this address translation is not that heavy in comparison with the other tasks a Gateway Node is required to perform, such as packet filtering of incoming traffic and tunneling to other Clusters.

When a Foreign Node wishes to communicate with a PN, it also makes use of the PN Agent. The location of the PN Agent is fixed and this is the only thing Foreign Nodes need to know in order to communicate with the PN. The task of the PN Agent is to find the appropriate service or node to connect with. For instance, if someone wishes to establish a phone conversation with the owner of a PN, the agent will locate a phone-capable node in a Cluster near the user and divert the incoming call to that node. For this purpose, it is important that the agent has some idea about where the user is located, but this is of course an application layer task.

7. Conclusions

A PN extends and complements the concept of pervasive computing by creating a personal distributed environment where persons can interact with various devices not only in the close vicinity but potentially anywhere. The network layer is the glue that binds all a person's devices together into one PN. We proposed a general network layer architecture that can bridge different technologies and offer a homogeneous and clear view to the end-user. The network layer is based on an ownership relation that can offer communication between a person's all devices in a secure way. In the end, solutions were presented to some of the most important issues related to the proposed architecture, such as addressing, routing, mobility management and communication with Foreign Nodes, both distant in the close vicinity.

Acknowledgments

The work presented here was partly funded by the Commission of the European Union under the project IST MAGNET [5]. This research is also partly funded by the Belgian Science Policy through the IAP V/11 contract, by The Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen) through the contract No. 020152, by the Fund for Scientific Research - Flanders (F.W.O.-V., Belgium). Jeroen Hoebeke is Research Assistant of the F.W.O.-V. We would also like to acknowledge the contributions of Weidong Lu of Delft University of Technology.

References

[1] IEEE P802.11 - The Working Group for WLAN Standards, http://www.ieee802.org/11/.

[2] Bluetooth SIG, "Specification of the Bluetooth System - Version 1.1 B", http://www.bluetooth.com/, 2001.

[3] IEEE 802.15 - The Working Group for WPAN Standards, http://www.ieee802.org/15/.

[4] Ignas G. M. M. Niemegeers, Sonia M. Heemstra de Groot, "Research Issues in Ad-Hoc Distributed Personal Networking", Wireless Personal Communications: An International Journal, Volume 26, Issue 2-3, Pages 149-167, Kluwer Academic Publishers, August 2003.

[5] IST MAGNET, http://www.ist-magnet.org/.

[6] Robin Kravets, Casey Carter, and Luiz Magalhaes, "A Cooperative Approach to User Mobility", ACM Computer Communications Review, Volume 31, Pages 57-69, October 2001.

[7] John Dunlop, R.C. Atkinson, James M. Irvine, D. Pearce, "A Personal Distributed Environment for Future Mobile Systems", In IST Mobile & Wireless Communication Summit, Aveiro, Portugal, June 15-18, 2003.

[8] IXI Mobile, http://www.ixi.com/.

[9] Ralph Droms, "Dynamic Host Configuration Protocol", IETF RFC 2131, March 1997.