Architectures for Intra-Personal Network Communication

R. V. Prasad, Martin Jacobsson, Sonia Heemstra de Groot[‡], Anthony Lo, Ignas Niemegeers
Wireless Mobile Communications
Faculty of EEMCS, Delft University of Technology
Delft, The Netherlands
{vprasad, m.jacobsson, a.lo,
i.g.m.m.niemegeers} @ewi.tudelft.nl

[‡]Twente Institute for Wireless and Mobile Communication
Institutenweg 30, 7521 PK
Enschede, The Netherlands
Sonia.Heemstra.de.Groot@ti-wmc.nl

ABSTRACT[1]

Personal Networks (PN) is a new concept related to pervasive computing with a strong user-focus view. The key to a successful PN realization is a general network architecture that is capable of bridging different current and future technologies and offers a homogeneous and clear view to the end-user. In this paper, we focus on forming a PN by connecting remote personal devices using infrastructure-based IP networks, including 3G networks and WLAN hotspots. One way is to upgrade the current access networks with new functionality to support PNs. Since many devices in PNs are mobile and battery powered, this may help them to achieve a faster service and to save energy. However, to deploy such functionality is not easy and may hamper the adoption of PNs altogether. Therefore, we propose an intra-PN communication architecture that will work over current IP networks. To discern the above proposal we also give a detailed picture of PN network architecture and infrastructure supported PNs. We believe that this will help the success of PNs.

Categories and Subject Descriptors

C.2.1 **[Network Architecture and Design]**: *Wireless communication*

General Terms

Management, Design.

Keywords

Personal Networks, Gateway nodes, Edge Routers, PN Agent.

1. INTRODUCTION

Personal Networks (PN) [5] is a new concept related to pervasive computing with a strong user-focused view. 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 mobile ad hoc networks (MANET). 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-configurable and support many different types of networks and devices. Figure 1 shows a future PN scenario.

WMASH'05, September 2, 2005, Cologne, Germany.

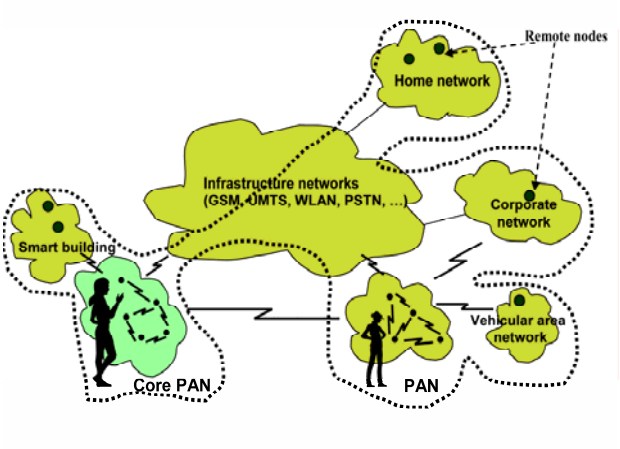

Figure 1. An example of a Personal Network

The key to a successful PN realization is a general network 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 and at the same time co-operate with existing networks such as infrastructure networks and other fixed networks. In this regard popularity of Internet Protocol (IP) should also be noted.

Both IEEE 802.11b and IEEE 802.11g [3] wireless standards have been widely-adopted and used for wireless connectivity. WLAN Hotspots based on IEEE 802.11b or 802.11g are often located in heavily populated places such as airports, train stations, libraries, marinas, conventions centers and hotels. Devices with newer operating systems can bootstrap to connect to these networks. These networks usually have a DHCP server and can offer Internet connectivity to a user by assigning IP numbers on the fly. Thus it is obvious that the newer development in technology cannot forego IP infrastructure to be useful and really applicable to the end users at present. Thus PNs must be capable and flexible enough to be able to make use of current and future communication networks. For direct communication between a person's devices, PN must be able to use ad hoc wireless communication technologies such as Bluetooth [2], Wireless

[1] While a part of this work is sponsored by the IST MAGNET project and Freeband PNP2008 projects, some aspects presented here do not necessarily reflect the views of MAGNET and PNP2008.

Local Area Networks (WLAN) [3] in ad hoc mode, low rate WPANs, IEEE 802.15.4 [4] and other future technologies. To interconnect personal devices in different locations, PN must be able to use infrastructure-based networks such as UMTS and GPRS networks, WLAN hotspots, wired and wireless broadband access networks and other evolved future versions of these access networks. We think a PN solution must be able to operate even when minimal functionality is offered by the access network. Another important criterion for the success of PN is the *trust* that people can have in the system. Systems like PN are extra vulnerable because of their mobile and wireless nature. The owner should be able to remain anonymous and personalize his devices so that the system can distinguish between his devices and devices belonging to someone else [8].

2. PN ARCHITECTURE

As shown in Figure 2, the IST MAGNET project [6, 9] has proposed a PN architecture, which is composed of three abstraction levels; the connectivity, the network and the service abstraction levels [12]. The connectivity abstraction level consists of various wired and wireless link layer technologies, organized in radio domains, including infrastructure links. The link layer will allow two nodes implementing the same radio technology to communicate if they are within radio range. To allow any two nodes within a PN to communicate, a network abstraction level is needed. The network level divides the nodes into Personal and Foreign Nodes and Devices, based on trust relationships. Trust relationship is a way nodes can gauge trust worthiness of other nodes with whom they interact. There can be different levels of trust relationships. Only nodes that are able to establish long term (permanent) trust are personal and can be part of a user's PN. Personal Nodes that are 'nearby' and have such a long term common trust relation form a 'Cluster'. Clusters can communicate with other clusters via infrastructure network. The service abstraction level which incorporates two types of services; public and private services is on top.

In our architecture [6,7,10], the home network of a person will be one cluster, the car network second, the P-PAN (term used for a cluster around the person) a third and so on. The link layer technology used to form a cluster will limit the geographical spread and size of a cluster. All clusters, work as local networks and therefore need their own independent networking solutions such as self-configuration, self-maintenance, addressing, routing, etc. However, the clusters can merge and split without extra effort.

The formation and maintenance of clusters is a purely local process and does not need any support from infrastructure. Clusters are dynamic in nature. Nodes are switched off and on as well as roam and might suddenly show up in a different cluster. The cluster formation in PNs is to keep Foreign Nodes out of the domain and only include Personal Nodes. This is done by using special authentication and authorization mechanism [8, 11]. It is always advisable to use intra-cluster mechanisms to provide communication between Personal Nodes as often as possible, since it is likely to be more efficient than using inter-cluster mechanisms since Inter-cluster mechanisms involves interconnecting structure. Clusters are defined from a connectivity and trust perspective. When clusters want to communicate with remote clusters through their GW nodes, they need to be able to locate each other a requirement that will be met by the PN agent.

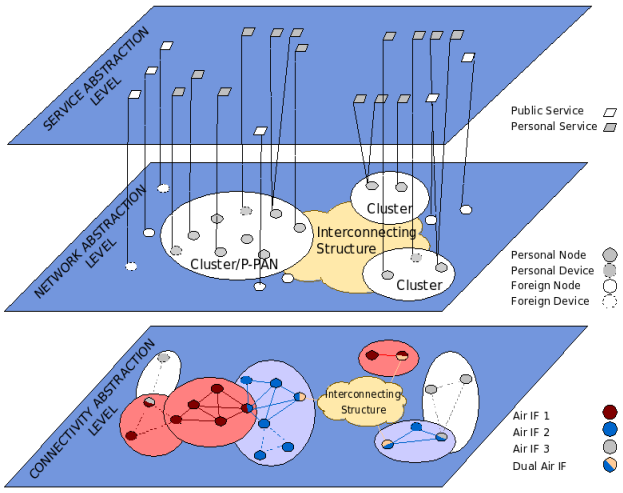

Figure 2. The abstraction level views

3. TWO APPROACHES FOR INTER - CLUSTER COMMUNICATION

3.1 Edge Router (ER) - based Inter-cluster Communication

The MAGNET architecture deals with PN formation using three important entities, namely, PN agent, Edge Routers, and Gateway nodes. Figure 3 shows the typical PN architecture with multiple clusters at the network level. The figure also shows the connectivity between the major entities of a PN in different clusters. Each cluster consists of at least one GW node which in turn connects to an ER. The ERs establish tunnels with each other on the Internet and thus enable PN connectivity. MAGNET proposes this architecture due to some important reasons and assumptions. We shall examine these three important entities here that enable inter-cluster connectivity and at the same time explain the characteristics of an ER-based architecture for PNs.

3.1.1 Gateway Nodes

A Gateway node is a personal node within a cluster that enables connectivity to nodes outside the cluster. GW nodes have some special requirements such as address translation, set up and maintenance of tunnels, filtering of incoming traffic, etc. They should preferably be powerful devices since the tasks required by such a node might be quite heavy. The process of finding capable GW nodes with links to foreign nodes or the infrastructure is the task of the cluster. The selection of GW nodes depends on several aspects, such as power, connectivity, etc.

3.1.2 Edge Routers

Edge routers are endpoints in the interconnecting structure such as the Internet that communicate with GW nodes and support them by offering PN functionality. On behalf of a cluster, an ER can communicate with the PN agent(s) (see Section 3.1.1) and could take care of the tunnel establishment and management. ERs being fixed and powerful devices, and being in the infrastructure network, can also take the load from GW nodes such as remote service discovery, service repository, etc. Thus, the ER can relieve the GW nodes of their bulk of work and allow them to reduce their power consumption with respect to signaling/maintenance vis-à-vis other ERs and PN Agent.

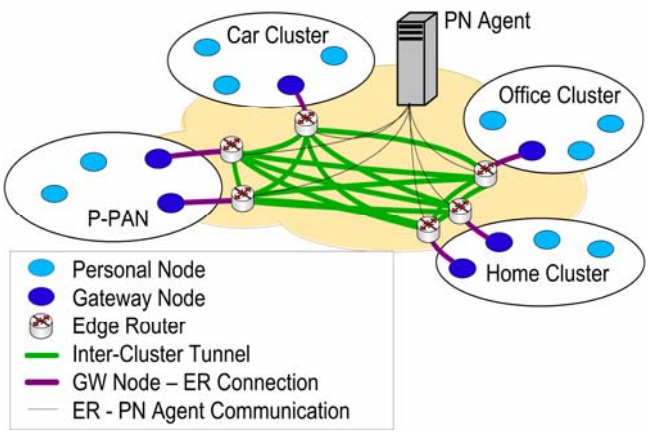

Figure 3. PN connectivity using Edge Routers

GW nodes in the clusters are often mobile and battery-powered, above functionality may therefore overload GW nodes. Thus it is useful if overhead is placed in the ERs. Further, multiple tunnels (ER non-selective) between two clusters can also improve inter-cluster communication and provide resilience. When there are multiple paths, the choice of a specific tunnel can then be made based on the QoS requirements.

The MAGNET architecture proposes to have always tunnels between all the clusters and arguments are in favor of putting control for tunnel establishment in the ERs and not in the clusters. It favors an always-on, ER based tunnel building and maintenance policy, in which tunnels are established and maintained between ERs as and when a cluster is connected to the interconnecting structure through an ER. Thus ERs provide an overlay network for PNs. This can be harnessed by the nodes of PNs efficiently without bothering about the connectivity with the other nodes. We call this an *optimized* way of supporting PN connectivity taking into account the nature of PN nodes and its capacity. This is nothing but placing intelligence in the network layer or infrastructure so that higher layers do less complex work regarding network connectivity.

Remark: Users need to trust the operator of an ER to a larger extent since ERs will support the internal mechanisms of the PN. In the case that an ER is not available or not trusted, the GW node itself would have to act as an ER.

3.1.3 PN agent(s)

In the ambit of MAGNET, it is a management entity located in the interconnecting structure (the Internet) that keeps track of each PN node and all clusters in a PN. Its functionality can be distributed. Since, the ERs, usually, would not know the address of the PN agent before they get a query from a GW node, there should be some mechanisms for the ERs to know the address of the PN agent. Each personal node knows the IP-address(es) of the PN agent(s) of the PN it belongs to. ERs build an overlay network of ERs for a particular PN using PN Agent(s). Clusters that have obtained access to the interconnecting structure announce their presence to a PN agent. More precisely, the ERs send a registration to the PN agent.

In summary, we have the PN with nodes having flat addressing, pro-active routing and always-on tunnels. The advantages of the ER-based solution are: (1) The GW nodes can be lightweight; (2) PN setup and maintenance is easy with the help of ERs; (3) communication between two nodes in a PN or in fact with nodes in other PNs is simple; (4) network formation is fast and can easily support session mobility.

3.2 Inter-cluster Communication without ERs

Edge routers, here, represents routers in the infrastructure that need to be built with special PN functionality. Without ERs, GW node now needs to be available to the other clusters and be a little more intelligent. Furthermore, good amounts of support need to be sought from PN agent(s) when the ERs are no longer in the picture.

3.2.1 Why Edge router less solution?

The ERs are infrastructure entities that are to be explicitly designed for PN architecture. They possess the following drawbacks: (1) *ERs share PN functionality:* that is public service providers need to build these entities and maintain them; (2) *ERs are hard to deploy:* since ERs are routers with PN functionality, it is difficult to get into the infrastructure with new devices; (3) *ERs need to be trusted:* since, the tunnels are from ERs the security information needs to be shared with them; (4) *ERs do not reduce the complexity of the architecture:* that is ERs still need a fully equipped PN agents and GW nodes.

3.2.2 Changes in the GW nodes

In MAGNET, the ERs are to provide a seamless overlay network for the PN clusters. The GW nodes would have operated on a virtual network that is sitting above the public IP network as and when required by connecting to the ERs. Now the GW nodes are to be the inter-cluster tunnel endpoints as shown in Figure 4. There are two ways a GW node can connect to the interconnecting structures, either using a public IP address or NAT [1].

GW nodes having public IP numbers: If the GW nodes have public IP addresses, they would be able to form the route with the help of PN agent. The PN agents are updated by each GW node with their location and care of addresses (CoA). The PN agents therefore know the address of all GW nodes with infrastructure access. Lightweight IPSec tunnels can be established between the GW nodes to transfer the intra-PN communication over the interconnecting structures. The tunnels are secured using shared keys distributed during the personalization step of the GW nodes.

The connection between two GW nodes can be: (1) *Always on inter-cluster tunnels*: Here the GW nodes initiate the tunnels with the help of PN agents and build a quasi permanent connection with all present GW nodes in the PN and keeping these tunnels intact as long as possible; (2) *On demand inter-cluster tunnels*: In this case, every GW node keeps a connection with the PN agents and updates them with their location. Tunnels between GW nodes are only established when needed. This means that a GW node only needs to update other GW nodes to which it has active tunnels with its new CoA. Except for this, it will work exactly the same as the always on inter-cluster tunnels. The tunnels are created above the IP layer and are actually formed by authorizing the GW nodes with each other using the shared trust relationship. The basic idea here is to use lightweight tunnels between the GW nodes and do away with ERs. In the always on inter-cluster tunneling solution, a normal ad hoc routing protocol can be used without modification over the inter-cluster tunnels as they are

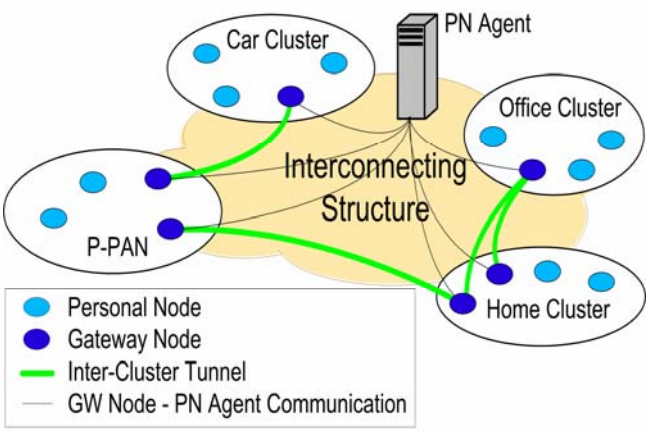

Figure 4. PN formation with GW node (without ERs)

always up and look like normal links to the routing protocol. However, in the on demand inter-cluster tunneling this is not possible. Each GW node should know to which cluster to establish a tunnel before establishing it. The easiest solution to this problem is to let the PN agent to also know the member nodes of each cluster. A GW node can then consult the PN agent before establishing a new tunnel. The PN agent will be able to tell which cluster and which GW node can be used to establish a tunnel to that cluster.

Gateway Nodes behind Firewall: When the GW nodes are not on publicly routable IP, the PN agent has to take care of establishing the connectivity between them. Popular methods such as STUN [13] and TURN may be used here for NAT traversal. These protocols take the least overheads and are transparent to the IP layer. Therefore the above paradigm can still be worked out. However, there will be some difficulties if and when the NAT is symmetric/restrictive on either side. Then the PN agent can be used to relay the packets between the GW nodes and the transactions are still secure. If this happens often, the PN agent may need to be powerful and have a good network connection. Several strategically placed PN agents may be a good option.

3.2.3 Functions of the PN agent without ER

The functions of the PN agent in this scenario consist of all the functions explained in Section 3.1. The additional functions include handling the trust relationships for the GW nodes. A database for holding the addresses of GW nodes, and thus the clusters of a PN is also needed. PN agent has to switch the packets in case two GW nodes could not communicate directly with each other. In this scenario the PN agent will have to route the packets through. PN agent might have to run STUN servers etc., for P2P connectivity when required. PN agents are to be powerful to enable more traffic to go through it.

There advantages are: (1) Avoidance of network elements like the ERs and thus no special support required from Infrastructure; (2) A PN agent can be run on any system with public IP so that it can be customized according to the users' requirements without being tied to ERs in the Infrastructure; (3) Circumventing more investment for the infrastructure deployment and avoiding extra intelligence in the network; (4) Can encourage many of the existing Internet '*Presence*' service providers to popularize the concepts of PN technology and thus a wide reach/use; (5) Connecting to another PN or foreign nodes would be easy if the service is offered by well known 'presence' enablers when there is no common radio link; (6) This architecture can attract application service providers since, it tries to be similar to many P2P solutions – in the sense that GW nodes talk to each other directly at PN level – and thus can be universal in nature.

4. CONCLUSIONS

In this paper we have introduced a general architecture for PNs. We explained two approaches for PN formation with some requisite changes in the infrastructure (vide a network elements) and without any such changes. With mandatory use of ERs, PN connection is possible only if there is a support of a 'PN capable' interconnection structure. It is advantageous since, the internal PN nodes will not be stressed with the overheads of communication setup though this needs the help of service providers. Service providers have to incorporate PN capability and it becomes highly restrictive for large scale deployment. Without ERs, falling back on GW nodes makes GWs heavier and a bit more complex. Yet, the PNs can be deployed in the present Internet. PN is capable of becoming another disruptive service like Internet telephony. We are in the process of implementing our ideas on IPV6 tunnels.

5. REFERENCES

[1] Aboba, B. and W. Dixon, "IPsec-Network Address Translation (NAT) Compatibility Requirements", *IETF RFC 3715*, 2004.

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

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

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

[5] Ignas Niemegeers, Sonia Heemstra de Groot, "Research Issues in Ad-Hoc Distributed Personal Networking", *Wireless Personal Communications*, Vol. 26, No. 2-3, pp. 149-167, Kluwer Academic Publishers, Aug-2003.

[6] IST-507102 MAGNET/WP2.1/INT/D2.1.1/R/PU/001/1.0, "*Conceptual Secure PN Architecture*", January, 2005.

[7] IST-507102 MAGNET/WP2.4/IMEC/D2.4.1/PU/001/1.0, "Architectures and Protocols for Ad-Hoc Self-configuration, Interworking, Routing and Mobility", December, 2004.

[8] IST-507102 MAGNET/WP4.3/UNIS/D4.3.2/PU/1.0, "Final Architecture of the Network-Level Security Architecture Specification", March, 2005.

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

[10] Martin Jacobsson, Jeroen Hoebeke, et al, "A Network Layer Architecture for Personal Networks", *In the Proc. of Workshop on My Personal Adaptive Global Net: Visions and beyond*, Shanghai, China, Nov., 2004.

[11] Martin Jacobsson, Ignas Niemegeers, "Privacy and Anonymity in Personal Networks", In *Proc. International Workshop on Pervasive Computing and Communication Security (PerSec'05)*, Kauai Island, Hawaii, USA, March, 2005.

[12] Martin Jacobsson, Jeroen Hoebeke, et al., "A Network Architecture for Personal Networks", To be presented in the *14th IST Mobile and Wireless Communications Summit*, Dresden, Germany, June, 2005.

[13] Rosenberg, J., Weinberger, J., et al, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", *IETF RFC 3489*, March, 2003.