

# Final Program



**International Wireless Summit 2005**  
Aalborg, Denmark, September 18-22

Wireless Personal Multimedia Communications



Wireless Science Park - Business Meeting & Exhibition





Strategic Workshop



*Organized by*





ISBN: 87-90834-82-8

Copyright: © 2005 by WPMC Steering Board

Copyright and reproduction permission: All rights are reserved and no part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the publisher. Notwithstanding, instructors are permitted to photocopy isolated articles for non-commercial classroom use without fee.

## Self-organization and mobility in Personal Networks\*

Mikko Alutoin<sup>†</sup>, Kimmo Ahola<sup>†</sup>, Sami Lehtonen<sup>†</sup>, Luis Sánchez<sup>††</sup>, Jorge Lanza<sup>††</sup>,  
Jeroen Hoebeke<sup>‡</sup>, Gerry Holderbeke<sup>‡</sup>, Ingrid Moerman<sup>‡</sup>,  
Marc Girod Genet<sup>‡‡</sup>, Wassef Louati<sup>‡‡</sup>, Rasmus L. Olsen<sup>\*\*</sup>

<sup>†</sup>VTT Technical Research Centre, P.O.Box 1202, FIN-02044 VTT, Finland  
mikko.alutoin@vtt.fi

<sup>††</sup>Network Planning and Mobile Communications Lab, University of Cantabria, Santander, Spain

<sup>‡</sup>Ghent University - IMEC, Sint-Pietersnieuwstraat 41, B-9000 Ghent, Belgium

<sup>‡‡</sup>INT-GET, rue Charles Fourier, 91011 Evry, France

<sup>\*\*</sup>Aalborg University, Niels Jernes vej 12, 9220 Aalborg SØ, Denmark

**Abstract**—Personal Networks (PN) is an emerging concept where user experience as well as privacy and security in networking are emphasized. This paper describes how these goals are met by a PN architecture that relies on self-organization of one's personal devices into a personal network. Collocated devices organize themselves in private clusters in an ad hoc manner and the isolated clusters are interconnected over the Internet.

**Key words:** *Personal Networks, Service Discovery*

### 1. INTRODUCTION

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

The personal nodes are opportunistic and communicate via any technology that is available. They organize themselves in clusters which in turn form the PN. Connectivity between the clusters is maintained transparently to the changes in the underlying physical network environment and access. A special cluster is the Private Personal Area Network (P-PAN) which is best

characterized as the wireless bubble around the user. It consists of portable devices and other wireless wearable gadgets. A cluster is interconnected with other clusters through a wireless Internet access point (and a tunnel through the Internet). Examples of clusters are networks that consist of devices at home or inside a vehicle.

This paper is organized as follows. First it is described how the personal nodes form and maintain clusters via sending periodic beacons to their neighborhood and how a pre-shared long-term secret is leveraged in neighbor authentication and in providing security and privacy for the communications. After covering the aspects of self-organization at the cluster level, the solutions for service discovery, naming and inter-cluster connectivity are presented. The conclusions and further work are given in Section 5.

### 2. CLUSTER FORMATION

The term cluster is defined as a network of personal nodes connected to each other by one or more network technologies and characterized by a common trust relationship between each other. The trust concept is transitive, meaning that long-term pair-wise shared keys are used when forming clusters and the PN. Before two nodes can authenticate each other (or encrypt messages between each other) they must have negotiated the long-term shared key, called the *PN key*, using the so-called

\*The authors wish to thank all the members of the IST MAGNET project in which this work was conducted.

MAGNET - My personal Adaptive Global NET - is a worldwide R&D project within Mobile and Wireless Systems and Platforms beyond 3G. MAGNET will introduce new technologies, systems, and applications that are at the same time user-centric and secure. MAGNET will develop user-centric business model concepts for secure Personal Networks in multi-network, multi-device, and multi-user environments. MAGNET has 37 partners from 17 countries, -highly acknowledged Industrial Partners, Universities, and Research Centres.

FP6-IST-IP-507102

[www.ist-magnet.org](http://www.ist-magnet.org) <<http://www.ist-magnet.org/>>

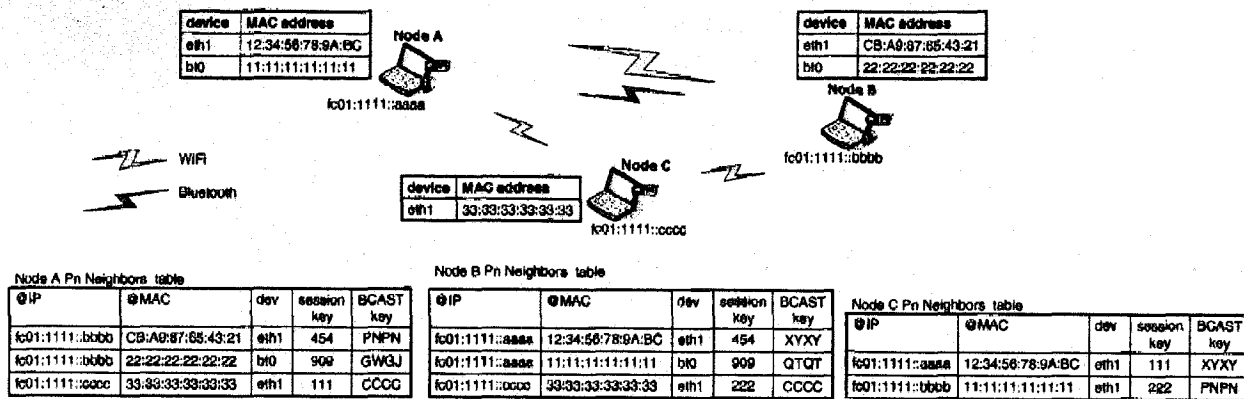


Figure 1. P-PAN formation example with neighbor tables

imprinting procedure [1]. Each node stores this information in the form of a *peer record* that contains the following information: a peer identifier (a unique identifier associated to the personal node) and the PN key associated with it. The major benefit from this scheme is the limited effect of a theft or loss of a node; only the peer records that relate to the lost node need to be revoked in the remaining nodes. The imprinting procedure is only the baseline over which the trust is built in the ad hoc cluster formation. In this sense, a beaconing process has been implemented in order to form and maintain the neighbor relationships within the cluster.

### 2.1. Neighbor discovery

Fig 1 depicts an example of a cluster with three nodes. Nodes A and B can communicate via both WiFi and Bluetooth. Node C has only WiFi radio. The nodes establish and maintain their neighbor relations by broadcasting periodic beacons on each of their network interfaces. The beacon is unencrypted and contains the identity of the sending node.

Upon the reception of a beacon, it will be checked if the peer is already registered in the neighbors table; if it is already registered, then the entry will be updated by reinitializing the expiration timer. If the neighbor is not already registered an authentication method will be called in order to assure that the discovered node is really a personal node. The authentication is based on the peer record and performed through a three-way handshake (Challenge – Response – Success). Besides authentication, the handshake includes negotiation of a symmetric, short-term unicast key, called the session key, as well as exchange of asymmetric broadcast keys. The handshake is performed on per interface basis, even in the case where two nodes can communicate via multiple radio technologies.

The unicast key is used both for encrypting and decrypting whereas the broadcast key is used only for decrypting. (The most viable way to implement a secure broadcast is to let each node generate the broadcast key

for itself and use shared key cryptography to encrypt the messages node by node.) If one of the nodes is not able to encrypt/decrypt layer 2 frames, then layer 3 encryption must be used (e.g. IPSec).

### 2.2. Intra-cluster routing

All newly discovered and authenticated nodes are dynamically added to the cluster. As a consequence, a cluster is a dynamically and gradually expanding or shrinking entity. In order to enable network level connectivity within the multi-hop cluster, routing capabilities that can deal with the ad hoc characteristics are needed. As these self-organizing and self-maintaining capabilities can already be found in the ad hoc routing protocols, it is a natural idea to build (to a certain extent) upon ad hoc network routing techniques and solutions.

Over the last few years, numerous routing protocols have been developed for ad hoc networks. Basically, these protocols can be categorized in the following two classes depending on the way they find routes: proactive routing protocols and reactive routing protocols. Proactive routing protocols or table-driven routing protocols attempt to have at all times an up-to-date route from each node to every possible destination. This requires continuous propagation of control information throughout the entire network in order to keep the routing tables up-to-date and to maintain a consistent view of the network topology. These protocols are typically modified versions of traditional link state or distance vector routing protocols encountered in wired networks, adapted to the specific requirements of the dynamic mobile ad hoc network environment. Reactive or on-demand routing protocols only set up routes when needed; when a node needs a route to a destination, a route discovery procedure is started. This procedure involves the broadcasting of a route request within the network. Once a route is established by the route discovery phase, a route maintenance procedure is responsible for keeping the route up-to-date as long as it is used. In the literature, many simulation studies have

been performed in order to evaluate the performance of proactive and reactive routing protocols. They all come to the conclusion that each technique has its advantages and drawbacks in terms of delay, overhead, scalability... and can outperform the other depending on the network context and traffic conditions.

In order to choose between both solutions, one should analyze the expected characteristics of a cluster of personal nodes. Concerning the network topology and node characteristics, it can be assumed that a roaming P-PAN is mainly a small-size, battery-powered, network with a slowly changing composition and low internal mobility. The other, larger clusters mainly consist of static devices with both wired and wireless interfaces often connected to a power supply. Consequently, scalability is not the main factor to favor either proactive or reactive solutions. Concerning the protocol overhead, proactive protocols require link monitoring in order to detect new links and link breaks, whereas reactive protocols don't. However, within a cluster of personal nodes, this task is actually taken care of by the cluster formation process, which is inherently proactive and can inform a proactive routing protocol about the link status. Therefore, for an isolated cluster, the main factors to decide whether to use reactive or proactive routing are the expected traffic patterns and the resulting delays, but even in this case the network context allows additional improvements to the protocols (e.g. caching). However, when taking into account the connectivity to the nodes that are outside the cluster, the differences between proactive and reactive become more distinct. These connections go via the *gateway node* that is a personal node, within the cluster, that has received an Internet address from an access point. First of all, the proactive routing protocol efficiently allows the propagation of gateway (and even QoS) information within its routing updates. In addition, due to the proactive routing information, a personal node can immediately decide whether the destination is located within the same cluster or within some remote cluster, reachable via the gateway node. This results in an easier and more efficient, in terms of overhead and latency, extension of the intra-cluster routing protocol to PN-wide routing.

Based on the above considerations, a proactive approach is chosen for the intra-cluster routing. The protocol relies on the neighbor discovery module for the detection of new links and link breaks, events that will trigger the propagation of routing updates. In addition, the routing updates include the propagation of gateway information, so every personal node knows about the available gateways and can select the most appropriate one. Further, regardless of the number of physical interfaces, each node receives only one IP address which it uses for the PN connectivity. This means that even if multiple radio links exist between two nodes, the routing protocol only observes this as one network connection.

The details of managing the heterogeneous interfaces are hidden from upper protocol layers by the Universal Convergence Layer (UCL) which is located between the link and the network layer. This leads to two-phase routing: first the routing table, which is built using the proactive routing protocol, is used to select the next-hop node and then the physical interface, for packet transmission, is selected independently by the UCL. Finally, both the control and data packets (except for the cluster formation beacons) are secured using the unicast or broadcast keys exchanged during the neighbor discovery process. In section 4 it is discussed how isolated clusters are interconnected over an IP network, e.g., the Internet.

### 3. SERVICE DISCOVERY

The dynamicity of Personal Networks is reflected to the service level in such way that the availability of any services in the PN will change over time. To enable the user to keep track and manage services, a Service Discovery (SD) system is required to assist the user in maintaining information of services within the cluster and the PN. An evaluation [2] of a centralized versus decentralized approach to SD was performed. The conclusion was that at the cluster level services should be managed centrally, whereas at the PN level the peer-to-peer (P2P) model is more preferable.

#### 3.1. Service management node

Within the cluster an entity called Service Management Node (SMN) is introduced to take the role of the SD central node. The SMN maintains an up to date repository of service information within the cluster based on a modified version of UPnP and Bluetooth SDP. Furthermore, the SMN represents its cluster in the large-scale SD (external/remote) P2P overlay network, which is explained in the next subsection.

The Service Assistant Node (SAN) has the same software as the SMN, but the SAN is inactive and awaiting for a potential SMN handover. This could be the case where the current SMN fails for some reason (e.g. the SMN runs low on battery or gets out of communication range). The election of the new SMN among the SANs could be based on multiple different features. The cost function could include a combination of values referring to battery status, computing capabilities, network interfaces and database storage capacity. The result of applying this function, from now on called SNW (Service Node Weight), summarizes the node capabilities and is used to identify the most capable one to become the SMN.

Whenever a SAN wants to become an SMN it announces its capabilities by broadcasting the SMN Challenge Request within the cluster (see Fig. 2). This implies the use of a cluster-wide multicast/broadcast address which will be interpreted by the routing

algorithm in order to make the message to flood the whole cluster. The node considers itself as the SMN of the cluster, unless some other node denies this by replying with the SMN Challenge Response message. The reception of this message leads to quit the SMN state. This master election protocol allows transitory stages where more than one node would consider itself as the SMN. However, the stages last less than the SMN Advertisement period which can be considered as the stabilization time.

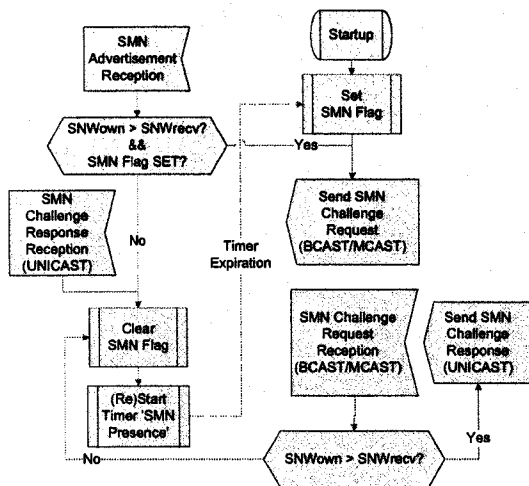


Figure 2. SMN Election flowchart

### 3.2. INS/Twine super-peer network

INS [3] is a naming and resource discovery system. It introduces intentional names for service or query descriptions. The intentional name structure is a hierarchical arrangement of attribute-value pairs that allows high flexibility in describing queries and services. INS/Twine [4], depicted in Fig. 3, is an enhanced version of the INS.

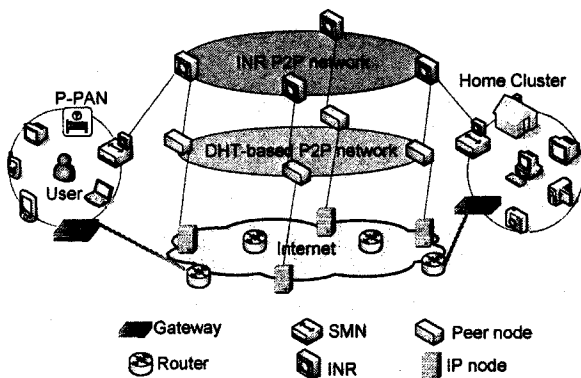


Figure 3. INS/Twine super-peer network architecture

The INS/Twine architecture includes a distributed P2P network of Intentional Name Resolvers (INR) which distribute resource, service and naming

information to each other for storage, and collaborate to resolve the service and name queries. The INRs work on top of a Distributed Hash Table (DHT)-based P2P network (see Fig. 3). The INS/Twine system was selected to provide a scalable wide-area discovery for legacy SD protocols. Any attribute-based service description of any legacy SD protocol, such as UPnP, can be stored in the INS/Twine system [5], [6]. The INS/Twine module within the SMN implements an INR via which the cluster connects to the core INR P2P network. The core INRs residing within the static infrastructure are common to all PNs.

## 4. PN FORMATION

Clusters are interconnected via the Internet using dynamic tunneling in the IP layer [7]. These tunnels can be seen as virtual links in an overlay network of clusters forming the PN. The inner IP addresses in the tunneled packets are the site-local IPv6 addresses that are used in the PN level addressing. Each PN is allocated its own PN prefix (from the fc00::/7 address space [8]) so that packets belonging to different PNs can be classified easily on the cluster edge.

Tunneling can demand a lot of CPU power if the cluster needs to be connected with a number of remote clusters. To this end, the gateway node, having limited battery and CPU power, can outsource this functionality to an edge router that resides in the provider edge. The use of edge routers is described in detail in [9], [10]. Edge routers can also be used in providing PN services, such as content adaptation, traffic shaping or a roaming firewall [10].

### 4.1. Semi-centralized cluster discovery

As the gateway node receives an Internet address it engages itself in the PN formation process. A key entity in the PN formation is the *PN agent* that keeps track of the locations of the gateway nodes in terms of their Internet addresses. To enable this, all gateway nodes must register their Internet addresses (and the cluster composition) with the PN agent whenever possible.

The INS/Twine super-peer network is used to provide a distributed PN agent functionality and the location of a remote cluster can be resolved during the name resolution or using a separate query.

### 4.2. Inter-cluster tunneling

The PN formation clearly has a proactive component to it, because the gateway nodes register continuously to the PN agent. (Another option would be to use IP multicasting for finding the gateway nodes on-demand, but this suffers from scalability problems and not all IP networks support multicast.) However, the actual inter-cluster tunnels could be established either proactively or reactively. The proactive approach adopts always-on

tunnels and therefore guarantees low latency for inter-cluster connections. In the reactive approach the need for tunneling is detected dynamically. One option to manage this on the cluster edge is to initiate the tunnel setup upon a reception of an incoming packet addressed to an unknown destination. This certainly leads to increased latency when compared to the proactive approach. However, usually the communication session is preceded by a name-to-address resolution query. Therefore the gateway node can predict the need beforehand and thus shorten the latency for the tunnel setup.

The virtual links between the clusters utilize IPSec (in tunnel mode). The gateway nodes can derive the IPSec shared key by applying the same type of handshake that is used during the cluster formation or by using, for example, IKEv2 phase 2.

When it comes to the cluster mobility, the basic idea is that the PN level network address of the personal node does not change; it is the PN routing algorithm and the dynamic tunneling mechanism which cope with the node mobility. This approach is quite original and it remains to be specified how to maintain the PN connectivity over the inter-cluster virtual link as the cluster roams from one Internet access point to another. It is anticipated that edge routers [9], [10] are needed to support seamless mobility and session continuity.

#### 4.3. Inter-cluster routing

The PN agent provides only a rendez-vous point for the gateway nodes. In addition, an inter-cluster routing protocol is needed, so that changes in the cluster composition can be communicated in a peer-to-peer manner between the gateway nodes. Notice also that two clusters might be connected by a third cluster belonging to another PN, without any infrastructure. In this pure ad hoc scenario, the inter-cluster routing protocol is needed to provide route aggregation between the distinct PNs and more importantly, to isolate the routing algorithms of the clusters in order to promote diversity among the PN solutions.

### 5. CONCLUSIONS

The Personal Network (PN) architecture, which is presented in this paper, is based on the proactive cluster formation and routing schemes, combined with an INS/Twine super-peer network taking care of naming, service discovery, and cluster discovery. Clusters are interconnected over the IP network(s) using dynamic tunneling. The cluster formation is based on a pre-shared secret which is used in the peer authentication procedure that is initiated upon reception of a beacon from a new neighbor. The proactive approach to cluster formation goes together with a proactive intra-cluster routing protocol which in turn makes cluster self-organization easy as the cluster composition is known by all nodes.

The INS/Twine super-peer network is used as an anchor point for the clusters as well as for the PNs. The core of this overlay network resides static and the clusters join the network via their Service Management Node (SMN). The SMN election has been outlined as a flowchart in the paper. This network provides also the so-called distributed PN agent functionality via which clusters locate each other in order to establish and maintain the dynamic inter-cluster tunnels.

A prototype of the described system is underway. Further work includes also comparisons of proactive and reactive routing schemes as well as investigating hybrid schemes combining both proactive and reactive components.

### REFERENCES

- [1] IST MAGNET Project, Deliverable 4.3.2, "Final version of the Network-Level Security Architecture Specification", <http://www.ist-magnet.org/publications.html#WP4>, Feb. 2005.
- [2] Ghader M., Prasad N., Olsen R.L., Mirzadeh S., Tafazolli R., "Secure Resource and Service discovery in Personal Networks", *WWRP12*, Toronto, Canada, November 4-5 2004.
- [3] Adjie-Winoto W., Schwartz E., Balakrishnan H., Lilley J., "The design and implementation of an intentional naming system", *In Proceedings of the 17th ACM Symposium on Operating Systems Principles*, pages 186-201, Kiawah Island Resort, South Carolina, December 1999. ACM Press.
- [4] Balazinska M., Balakrishnan H., Karger D., "INS/Twine: A scalable peer-to-peer architecture for intentional resource discovery", *In Proceedings of the First International Conference on Pervasive Computing*, pages 195-210, Zurich, Switzerland, August 2002. Springer-Verlag.
- [5] Louati W., Girod Genet M., Zeglache D., "UPnP extension for wide-area service discovery using the INS/Twine Framework", *PIMRC 2005*, Germany, September 2005.
- [6] Louati W., Girod Genet M., Zeglache D., "Implementation of UPnP and INS/Twine interworking for scalable wide-area service discovery", *WPMC 2005*, Denmark, 2005.
- [7] IST MAGNET Project, "A Network Architecture for Personal Networks", *Proceedings of IST Mobile and Wireless Communications Summit*, Dresden, Germany, 19-23 June 2005.
- [8] Hinden R., Haberman B., "Unique Local IPv6 Unicast Addresses", Work in progress, <http://www.ietf.org/internet-drafts/draft-ietf-ipv6-unique-local-addr-09.txt>
- [9] IST MAGNET Project, "Networking in Personal Networks", *Workshop on Applications and Services in Wireless Networks (ASWN 2005)*, June 29th - July 1st 2005.
- [10] IST MAGNET Project, Deliverable 2.4.2, "Active Networking: Definition and Validation of Concepts and PN Solutions", <http://www.ist-magnet.org/publications.html#WP2>, June 2005.