Personal Networks: From concept to a demonstrator

Jeroen Hoebeke, Gerry Holderbeke, Ingrid Moerman, Wajdi Louati, Wassef Louati,
Marc Girod Genet, Djamal Zeghlache, Luis Sanchez, Jorge Lanza,
Mikko Alutoin, Kimmo Ahola, Sami Lehtonen, Jordi Jaen Pallares

***Abstract*—offering ubiquitous availability of personal services, data and applications is the goal of a Personal Network, a secure self-organizing network encompassing all of a person's devices independent of their geographical location, communication capabilities or mobility. This paper presents the main Personal Network concepts and provides a detailed description of how these concepts are translated into a real architecture and software components, integrated in a working demonstrator.**

***Index Terms*—Personal Networks, network architecture, virtual router, demonstrator**

I. Introduction

As an increasing number of heterogeneous devices becomes networked, ranging from mobile communication equipment to home electronics, people will need flexible network solutions in order to make the services offered by their personal devices accessible at any time and from any place. However, users need not partake in (or be burdened by) any technical complexity to realize this ubiquitous connectivity. User privacy must be provided and the user privacy safeguarded. These challenging requirements are encompassed by the Personal Network (PN) concept [1], offering a self-configuring and self-organizing network of personal devices irrespective of geographical location, communication capabilities and mobility. The IST MAGNET project has worked on the development, implementation and integration of building blocks and software components needed to realize this PN concept at the network level and the production of a working demonstrator. This paper will briefly introduce the main generic PN concepts and provide details on the resulting PN architecture built in part around the virtual router concept [2][3]. Self configuration and organization of PN clusters, proactive routing and service discovery are also part of the overall PN architecture but will not be emphasized in this paper. The implemented demonstrator illustrates the self-configuring and self-organizing capabilities required for PN networking but can also serve as an enabler for Personal Services through the development of a service framework within MAGNET. The resulting PN architecture paves also the way towards PN federations where multiple PN users with common interests and tasks can communicate and cooperate.

J. Hoebeke (Research Assistant Fund for Scientific Research – Flanders), G. Holderbeke and I. Moerman, Ghent University – IMEC, Belgium.
W. Louati, W Louati , M. Girod Genet and D. Zeghlache, Groupe des Ecoles des Télécommunications- Institut National des Télécommunications (GET-INT), France.
L. Sanchez and J. Lanza, Universidad de Cantabria, Spain.
M. Alutoin, K. Ahola and S. Lehtonen, VTT Technical Research Centre, Finland
J. J. Pallares, Fraunhofer Institut FOKUS, Germany

II. The PN Concept

A PN is characterized by the ability to discriminate between personal nodes (PN nodes) and non-personal or foreign nodes. PN nodes (i.e. personal nodes belonging to the same PN) share a common trust relationship different from the relationship they may have with foreign nodes. Physically neighboring PN nodes can securely discover and identify each other and establish subsequent security associations. Direct secure communication is then possible. Of course, PN devices have different interfaces or limited range and communication therefore often extends a single hop. To this end, ad hoc networking between PN nodes interconnects non adjacent nodes, resulting in the formation of clusters (see Figure 1). The geographical distribution of these clusters, will force PN nodes to use access to an interconnecting structure (e.g. the Internet) through gateway PN nodes in order to communicate.

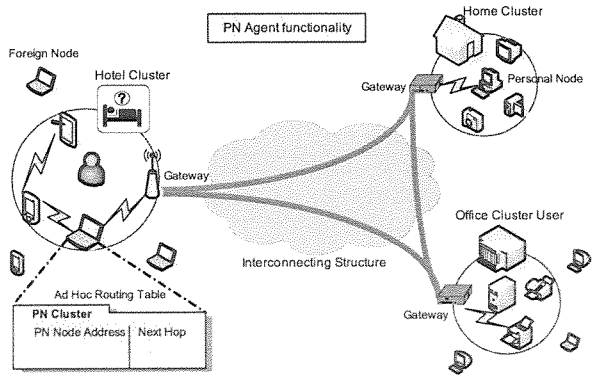


Figure 1: Personal Network concept

Discovery on how to reach remote clusters is offered by an entity called the PN Agent. Once this knowledge has been acquired with the help of the PN Agent, dynamic tunneling between remote clusters is used to establish secure PN-wide communication.

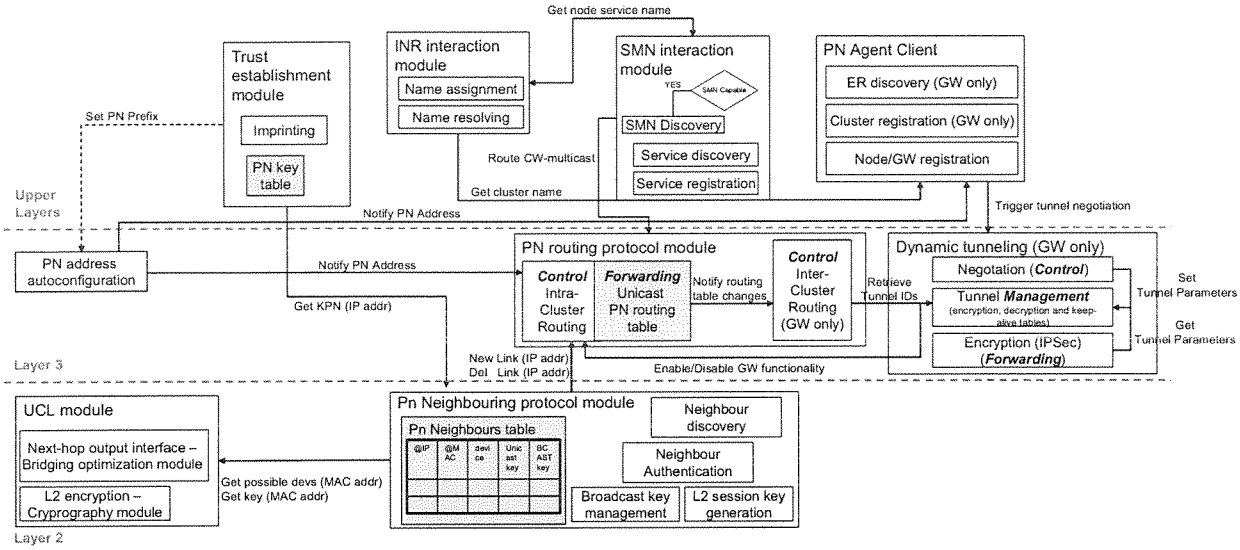


Figure 2: Personal Node architecture and components

Starting from the previous introduction of the main components in the PN concept, the actual PN demonstrator architecture will be presented by describing the translation into a specific architecture based on virtual routers. Note that alternative mappings (e.g. using NEMO paradigms) of the PN concept into a detailed PN architecture and network solutions were also the subject of research within MAGNET.

III. From Concept to Implementation

In the following subsections we will give a step-by-step discussion of how the PN concept is translated into a real architecture and software components and how the components interface to provide all required functionality. In depth descriptions can be found in MAGNET companion papers [3][4][5][6][7] addressing each a facet of PN networking and maintenance and specific building blocks.

A. Personal Node Architecture and Components (Figure 2)

For Personal Networking, the concept of trust is essential. To this end, an imprinting module in the PN node establishes a trust relationship with other PN nodes, i.e. the generation of long term trust keys bound to the other PN nodes' identifier which are stored in a PN key table. Currently, this pair-wise user assisted imprinting procedure needs to be done once between each new device introduced in the PN and each existing PN device (in the future, transitive imprinting will facilitate this process). In addition, during imprinting the PN prefix (unique for each PN) is spread amongst the PN nodes. From this PN prefix, each node generates a local PN IP address, consisting of the prefix and a unique suffix (PN address auto-configuration module).

Once trust has been established, neighboring PN nodes can discover each other through beacons, containing the node ID, the PN neighboring module periodically sends. If a beacon from a not yet discovered PN node is received, a neighbor authentication procedure is triggered. This procedure derives a temporary pair-wise session key from the long term trust key, used for encryption of unicast traffic at layer 2 (Note: alternatively, higher layer end-to-end encryption mechanisms could be used). In addition, the PN node will announce its broadcast key to its new neighbor, used for encrypting broadcast traffic. All information is stored in a PN Neighbor Table. At this point, a secure layer 2 communication link has been established between two neighboring PN nodes.

In order to use this link at the IP level, the PN IP address of a new neighbor is communicated to the PN routing protocol module, which implements a proactive distance vector based ad hoc routing protocol. The new routing information is further propagated to existing neighbors, enabling intra-cluster communication. The PN Neighboring protocol module will also report link breaks to the routing protocol, which are currently detected by the absence of beacons.

As already stated all intra-cluster communication, including routing protocol messages, is confined within the cluster and secured through encryption, using the negotiated unicast and broadcast keys. A Cryptography module in the UCL (Universal Convergence Layer) is responsible for this task. As a PN node can have multiple interfaces, the UCL is responsible for hiding this heterogeneity to the higher layers, in particular the routing protocol. Each PN node only has one PN IP address, independent of the number of interfaces, and the routing protocol only determines for each packet the next hop PN IP address, after which it is forwarded to the UCL. Next, the UCL will select the appropriate interface and apply the required encryption technique.

A name resolution module is implemented within the PN node to resolve names into addresses when names are used to identify PN nodes. The considered and implemented PN naming system is based on the INS/Twine framework [6] that implements a dedicated entity called the Intentional Name Resolver for name management and resolution. It is a scalable system since all large-scale naming operations are performed

through a peer-to peer overlay network of name resolvers.

The cluster-wide service management and discovery is centralized. A cluster central service entity, called Service Management Node (SMN), has been proposed and implemented. Each capable PN node (in terms of memory, computational power and battery capacity…) is a potential SMN and implements the SMN functionalities within a SMN interaction module. This module handles all the multicast/unicast service discovery and management messages and is linked to the PN routing protocol module. This SMN is also designed for providing name-based service discovery and obviously needs to perform service node name to address resolutions during the discovery process. The SMN integration module is therefore linked to a name resolver, for name resolution operations, through the name resolution interaction module. The SMN is also linked to the PN Agent client modules in PN nodes or gateways (see section III.B) for retrieving the PN and cluster id information. This information extends the service location and owner information and is used to refine and personalize the PN/cluster service registrations and discovery.

The above software components have been implemented on a Linux platform using kernel modules, Click Router components and C code. The end result of the described software components and their interaction is the complete cluster self-organization, ranging from the establishment of trust up to intra-cluster routing over heterogeneous interfaces.

B. The Virtual Router Concept to Enable PN-wide Connectivity

The next step in achieving complete PN self-organization is the establishment of inter-cluster connectivity. Some nodes in a cluster will act as gateway nodes, providing connectivity to the outside world. This gateway functionality is propagated by the intra-cluster routing protocol, resulting in a default route entry in the PN nodes' routing table. As such, all remote PN traffic will arrive in these gateway nodes and needs to be forwarded to the correct remote cluster over secure tunnels. This implies the need of three closely related components: a repository to retrieve cluster location (PN Agent), dynamic tunneling and inter-cluster routing.

Before discussing in more detail the implementation of these components, we will first explain some design choices. First of all, we have chosen to implement a proactive PN architecture, meaning that the dynamic inter-cluster tunnels are established and maintained and inter-cluster routing information is exchanged as soon as clusters have connectivity to the outside world. In order to offload complexity (tunnel management, mobility management…) from the PN nodes, to enable additional functionalities (QoS, network provider support…) and to facilitate PN federation (see section V), the Network based Virtual Personal Overlay approach has been introduced. This approach is based on Edge Router (ER) technology to support PNs connectivity and inter-cluster routing through the use of the Virtual Router (VR) concept. The VR is an emulation of a physical router in the software layer that provides per PN routing, addressing and management. In Figure 3 an overview of the resulting architecture that has been implemented is given and its principles and functions will now be explained in more detail.

In order to realize PN-wide connectivity, the gateway node will first perform ER discovery. When an ER in the access network has been found and selected, the PN Agent client module in the gateway will register the cluster with the central PN Agent server, which serves as a repository to store and retrieve information of which clusters are online and to which ER they are connected… Upon successful registration of a new cluster, the PN Agent will interact with the involved ER to start the installation of a new VR instance for the new PN. This VR will act as the routing table for forwarding inter-cluster traffic belonging to one specific PN. Secure tunnels to remote ERs that have clusters of the same PN connected to them are also established. In case no ER is available in the access network, it is foreseen to place this ER functionality in the gateway nodes.

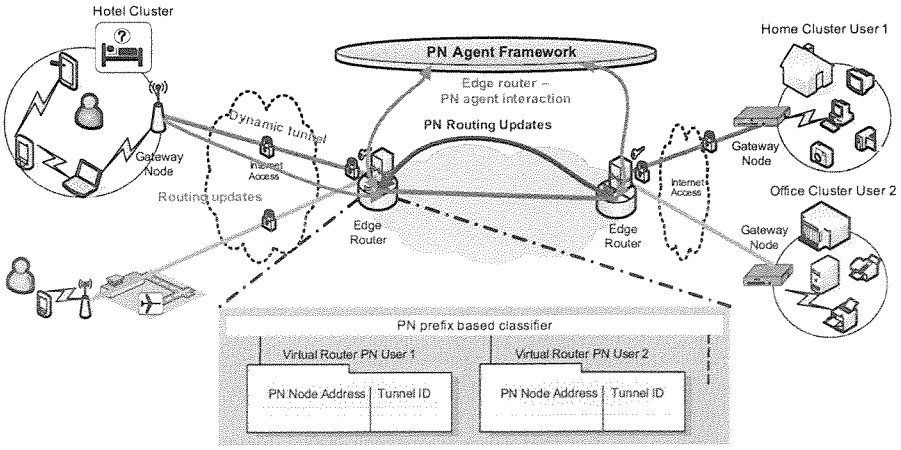


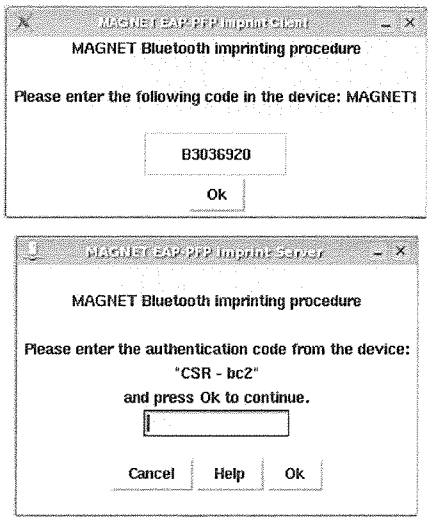
Figure 3: Personal Network architecture based on Virtual Routers

In addition, a successful registration will trigger the dynamic establishment of an IPSec tunnel between the GW and its ER (the ER is authenticated using certificates). Each tunnel from/to an ER is given a unique ID. From that point on, all communication means to realize secure inter-cluster communications are in place, except for the inter-cluster routing.

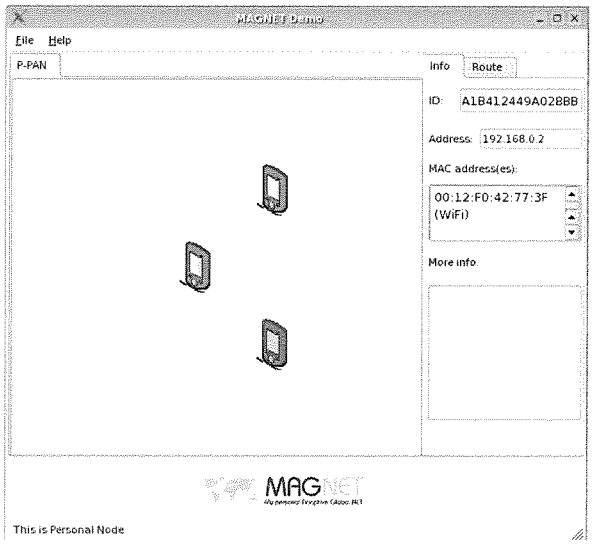
In order to realize efficient inter-cluster forwarding the GW node will propagate right after the tunnel establishment all PN addresses of its intra-cluster routing table and from that point on, all changes in this table, to the ER. The ER will store the received routing info in the VR together with the tunnel ID of the tunnel over which the info has been received. In addition, this routing information is exchanged with the remote ERs that have clusters of the same PN connected to them. Consequently, each VR for a specific PN will contain all PN addresses of devices that are online within that PN together with the identifier of the tunnel through which they can be reached, thus enabling proactive inter-cluster connectivity.

When a cluster deregisters, all dynamic information (tunnel info, VR instance in ER) is removed. Deregistration can be done explicitly by the GW node (e.g. when turning off the GW device) or by the ER when the tunnel with the GW breaks (e.g. for a roaming cluster). In the latter case, the cluster can roam to a new access network (and ER), restarting the process. It is envisioned that the use of private PN addresses, quick VR deployment and dynamic tunneling together with the aid of context information and transfer, can hide mobility from the higher layer protocols. Also, in case no ER would be present in the access network, the VR concept could still be applied directly to the GW node (1 VR in the GW), thereby reusing the same software components and protocols.

Again, the above architectural components and software building blocks have been implemented and integrated on Linux laptops and Nokia 770 devices using Click Router components, Java software and existing (or modified) Linux software. In Figure 4 some illustrations of the PN implementation in a simple configuration are shown (currently using IPv4 PN addresses, but support for IPv6 is foreseen).



a) GUI of the imprinting software both at the client and server side



b) PN node GUI showing 1 neighboring PN node (its ID, PN IP address and MAC) and 2 foreign nodes

```
NEIGHBOUR TABLE node192.168.1.3
FORMAT: [neighbour deviceType]
      192168.1.1  PN_ENABLED

ROUTING TABLE node192.168.1.3
FORMAT: dst : nextHop  hopCount  pred  tag  gw
      192168.1.1 : 192.168.1.1    1  192.168.1.3  1  TRUE   SELECTED
      192168.1.3 : 192.168.1.3    0  192.168.1.3  1  FALSE
```

c) Terminal output of PN node (PN IP 192.168.1.3) with 1 neighbor used as gateway to access remote clusters

```
Virtual Router PN 192.168.1.0
      192168.1.1 [ (1 ER_ER) ]
      192168.1.2 [ (2 GW_ER) ]
      192168.1.3 [ (1 ER_ER) ]

                  TUNNELMANAGER
ID 2:
(22.22.22.254 -> 22.22.22.252)
Enc. keys (0101010101010101 , 0202020202020202 , 0303030303030303 )
Dec. keys (0404040404040404 , 0505050505050505 , 0606060606060606 )
PNprefixes( 192.168.1.0 )
ID 1:
...
```

d) ER terminal output showing 1 Virtual Routing table (with 3 PN nodes online) and dynamic tunnel management

Figure 4: Illustration of PN implementation

IV. PN Implementation as Enabler for Personal Services

The proposed and implemented naming system, which also integrates the PN Agent concept in the design, is a flexible and scalable peer-to-peer system. This is possible because the naming architecture is also a device, resource and service discovery as well as a locating system.

This framework has been combined with existing local SD frameworks and the cluster SMN to provide PN-wide discovery [6]. The resulting flexible and extensible architecture acts as an enabler for PN services. The PN user can discover, locate, access, use and control services. The user can even add services into the service description database (the name tree of the naming system in the current design) if desired. This wide area discovery architecture is connected to PN nodes GUIs to enable the user to discover and visualize active services offered by PN nodes and foreign nodes via the SMN. The user can achieve this in a very flexible manner by selecting nodes presented on the GUI or by using any of a device name, a service name, a service type (using even wildcards to get all available matching services) and using location information. PN users can also trigger services based on context information.

The proposed and implemented PN architecture and service discovery framework [7] includes security mechanisms through the definition and the use of user and profiles. The implemented profiles (for user, environment, node and node security) can be included in the service descriptions stored in the name tree.

V. PN Implementation as Enabler for PN Federation

The above implementation brings the Personal Network concept closer to reality, by demonstrating a self-organizing overlay network of all of a person's devices, enabling a lot of potential applications and services. Of course, many communication patterns involve the interaction of multiple persons having common interests for various professional and private services (collaborative working, virtual meetings...). To this end, the MAGNET Beyond project will further build upon the results achieved within the MAGNET project to enable PN federation, a cooperation of multiple devices in different PNs. Again trust, but now group trust, will be a major cornerstone for the establishment of the PN federation. In addition PN federation definition and management (ownership and control of the federation, establishment, storage of PN federation policy, role of PN Agent, access control...) will impose even more challenges than in a single PN.

However, from the network connectivity point of view the PN implementation based on the VR concept can serve as an interesting enabler for end-to-end connectivity in PN federations as indicated in [3]. Assume a PN federation has been defined and multiple PNs have been established using the VR concept (see Figure 3). When a node A of this federation, located in a cluster belonging to PN 1 and connected to ER 1, wants to communicate with another node B of the federation, located in a cluster belonging to PN 2 and connected to ER 2 the following will happen. The traffic is forwarded to the gateway node of the cluster, which in turn will forward it to ER 1. In order for the traffic to arrive at the destination node B, it is sufficient to transfer (partially) the routing info in VR of PN 2 from ER 2 to VR of PN1 in ER 1 and establish a new tunnel between ER 1 and ER 2. As VRs are software routers that can be efficiently installed, removed and migrated, they provide a very flexible means to enable end-to-end communication within PN federations. In addition, as they run in powerful ERs, this can be realized in very short time scales. As such, our implementation already provides a first building block towards real PN federation. However, multiple additional challenges are still open and need to be addressed within MAGNET Beyond.

VI. Conclusion

The developed PN architecture and implemented and integrated software components have led to the development of a working demonstrator, enabling secure communication between Personal Nodes independent of their location and Personal services. Currently, this work serves as a basis to develop real Pilot services and prototypes and as an enabler for PN federations.

About MAGNET Beyond

MAGNET Beyond is a continuation of the MAGNET project (www.ist-magnet.org). MAGNET Beyond is a worldwide R&D project within Mobile and Wireless Systems and Platforms Beyond 3G. MAGNET Beyond will introduce new technologies, systems, and applications that are at the same time user-centric and secure. MAGNET Beyond will develop user-centric business model concepts for secure Personal Networks in multi-network, multi-device, and multi-user environments. MAGNET Beyond has 32 partners from 15 countries, among these highly influential Industrial Partners, Universities, Research Centres, and SMEs.

References

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

[2] W. Louati and D. Zeghlache, "Network based Virtual Personal Overlay Networks using Programmable Virtual Routers", IEEE Communications Magazine, vol. 43, no. 8, Aug. 2005, pp. 86-94.

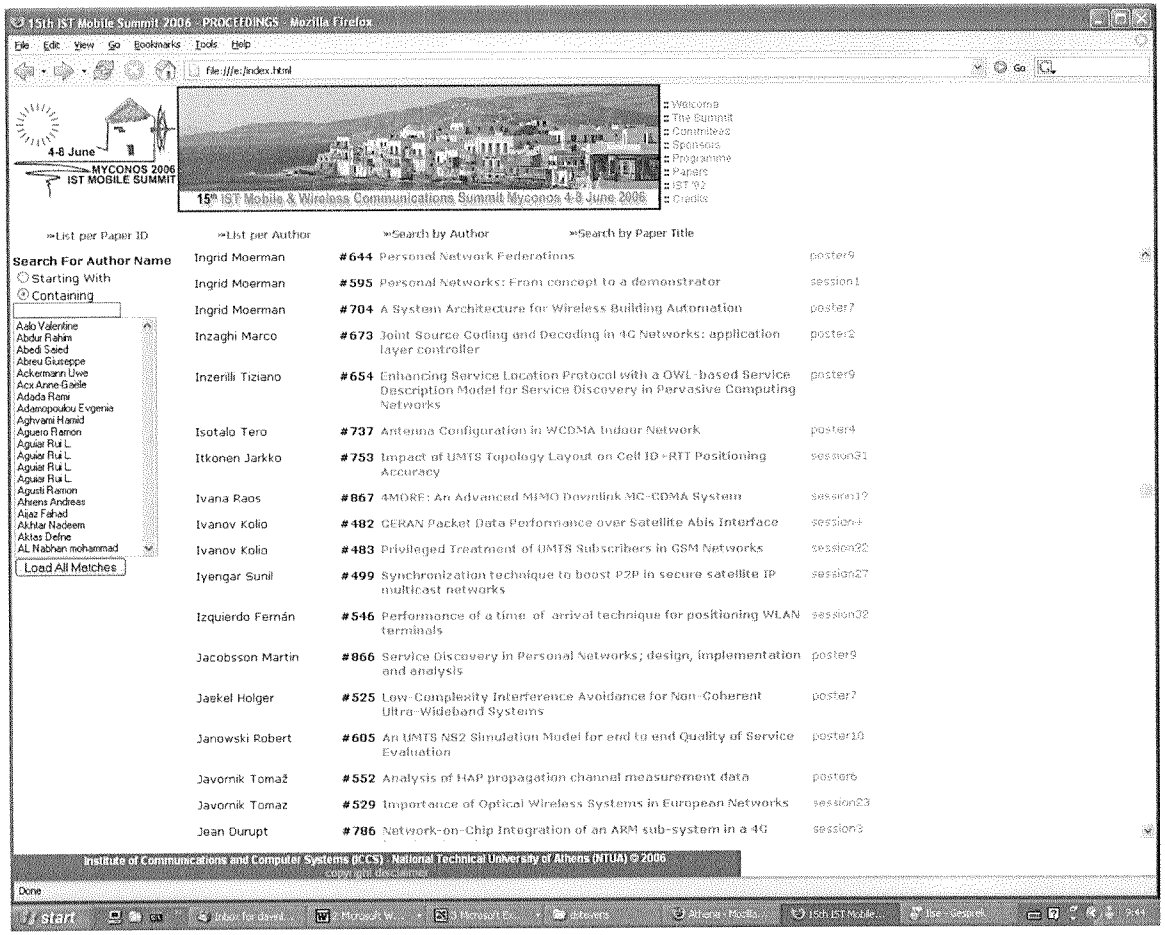
[3] W. Louati and D. Zeghlache, "Virtual Router Concept for Communications between Personal Networks", The eighth International Symposium on Wireless Personal Multimedia Communications, IEEE WPMC 2005, Aalborg, Denmark, Sep. 18-22, 2005.

[4] L. Sanchez et al., "Prototype Concepts of a PAN/PN Terminal and Infrastructure network support", IST-507102 MAGNET Deliverable D2.2.1, Dec. 2004.

[5] L. Munoz, et al., "A Proposal for Self-Organizing Networks", Wireless World Research Forum Meeting 15 (SIG 3), Dec. 8-9, Paris, France.

[6] W. Louati, M. Girod Genet and D. Zeghlache, "Implementation of UPnP and INS/Twine interworking for scalable wide-area service discovery", The eighth International Symposium on Wireless Personal Multimedia Communications (WPMC 2005), Aalborg, Denmark, Sep. 18-22, 2005.

[7] M. Ghader et al., "Resource and Service Discovery: PN Solutions", IST-507102 MAGNET, Deliverable D2.2.1, Dec. 2004.


15th IST Mobile Summit 2006 - PROCEEDINGS - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
file:///e:/index.html
4-8 June
MYCONOS 2006
IST MOBILE SUMMIT
15th IST Mobile & Wireless Communications Summit Myconos 4-8 June 2006
Welcome
The Summit
Committees
Sponsors
Programme
Papers
IST '02
Credits
»List per Paper ID
»List per Author
»Search by Author
»Search by Paper Title
Search For Author Name
Starting With
Containing
Load All Matches
Ingrid Moerman #644 Personal Network Federations poster9
Ingrid Moerman #595 Personal Networks: From concept to a demonstrator session1
Ingrid Moerman #704 A System Architecture for Wireless Building Automation poster7
Inzaghi Marco #673 Joint Source Coding and Decoding in 4G Networks: application layer controller poster2
Inzerilli Tiziano #654 Enhancing Service Location Protocol with a OWL-based Service Description Model for Service Discovery in Pervasive Computing Networks poster9
Isotalo Tero #737 Antenna Configuration in WCDMA Indoor Network poster4
Itkonen Jarkko #753 Impact of UMTS Topology Layout on Cell ID+RTT Positioning Accuracy session31
Ivana Raos #867 4MORE: An Advanced MIMO Downlink MC-CDMA System session12
Ivanov Kolio #482 GERAN Packet Data Performance over Satellite Abis Interface session4
Ivanov Kolio #483 Privileged Treatment of UMTS Subscribers in GSM Networks session22
Iyengar Sunil #499 Synchronization technique to boost P2P in secure satellite IP multicast networks session27
Izquierdo Fernán #546 Performance of a time of arrival technique for positioning WLAN terminals session32
Jacobsson Martin #866 Service Discovery in Personal Networks; design, implementation and analysis poster9
Jaekel Holger #525 Low-Complexity Interference Avoidance for Non-Coherent Ultra-Wideband Systems poster7
Janowski Robert #605 An UMTS NS2 Simulation Model for end to end Quality of Service Evaluation poster10
Javornik Tomaž #552 Analysis of HAP propagation channel measurement data poster6
Javornik Tomaz #529 Importance of Optical Wireless Systems in European Networks session23
Jean Durupt #786 Network-on-Chip Integration of an ARM sub-system in a 4G session3
Institute of Communications and Computer Systems (ICCS) - National Technical University of Athens (NTUA) © 2006
Done
start


15th IST Mobile and Wireless Summit
MYCONOS
GREECE
2006
4-8 June
MYCONOS 2006
IST MOBILE SUMMIT