Personal Network Federations

Jeroen Hoebeke, Gerry Holderbeke, Ingrid Moerman, Martin Jacobsson, Venkatesha Prasad,
N. I. Cempaka Wangi, Ignas Niemegeers, Sonia Heemstra De Groot

Abstract—**Providing secure cooperation between a subset of relevant devices belonging to different Personal Networks (PN) for the purpose of achieving a common goal or service is the objective of the PN federation concept. This paper explores the requirements of PN federations and identifies the main research challenges and implications on the PN architecture, providing a first step into the migration from these concepts into real solutions, architecture and protocols within the MAGNET Beyond project.**

Index Terms—**Personal Networks, PN Federations, concept, requirements, PN-F cycle**

I. Introduction

The concept of Personal Networking (PN) [1], presented in [5], can bring a solution for trusted communication between the many local and remote personal devices in view of the support of a variety of personalized and context-aware services. A Personal Network is a protected secure person centric network that connects all the nodes of a person over ad hoc as well as infrastructure networks and that provides context-aware services and applications. As such, it is a dynamic collection of interconnected heterogeneous personal devices, not only the local devices centered around the person, but also personal devices on remote locations such as devices in the home network, the office network and the car network.

The IST MAGNET project has worked on the development, implementation and integration of network components needed to realize this concept. Summarized, from a high-level viewpoint, the Personal Network consists of a number of clusters. Each cluster is a connected ad hoc network of personal nodes sharing a common trust relationship. By establishing secure tunnels between clusters, remote clusters are able to communicate with each other over any interconnecting structure. In order to track the location of clusters, PN Agent functionality has been introduced. Finally, a service architecture has been defined to support a person's applications and services. In depth descriptions of these solutions can be found in the following references [4][5][6][7].

While MAGNET has focused on solutions for the PN centered around a single user, MAGNET Beyond (the successor of the MAGNET project) will address the importance of interactions between multiple PN users with common interests for various private and professional services. The objective is to extend the PN solutions with the necessary networking functionality and group trust mechanisms to enable interactions between multiple PNs. Fednets, a novel concept that first has been introduced in [2] is such an approach. This paper will elaborate on the ideas presented in [2] in conjunction with PNs and will introduce the concept of PN federation (PN-F) and its potential applications, followed by a more detailed discussion about the requirements for PN federations and the involved research challenges that need to be tackled in order to meet these requirements.

II. PN Federation Concept

A PN federation (PN-F) can be defined as a secure impromptu, situation-aware or beforehand agreed cooperation between a subset of relevant devices belonging to different PNs for the purpose of achieving a common goal or service. When communication between devices belonging to different PNs is needed to support interactive and/or cooperative services between multiple users, a federation of their PNs will be established. More precisely, on top of these PN networks, a secure overlay of participating devices will be formed, that isolates a subset of the resources in the constituent Personal Networks. The PN devices outside this overlay still provide connectivity and take part in the secure routing of data between the devices of this multi-user overlay. Within the federation, devices can communicate with each other and allow each other access to specific services or usage of resources for performing the common task.

In Figure 1, the concept of a PN-F is illustrated, together with the underlying Personal Networks that participate in the federation. Based on how the cooperation between the devices in different PNs is realized in order to establish the federation, we can discriminate between Infrastructure Based and Ad Hoc based PN federation. In Figure 1, these two different PN federations are illustrated. The first PN-F (PN-F 1) is established between devices in PN clusters that are all connected to an infrastructure network. In this federation, support functionality available in or through the fixed infrastructure can be used to assist in the PN-F definition and establishment. This can be compared to the PN Agent introduced in the Personal Network architecture.

J. Hoebeke (Research Assistant Fund for Scientific Research – Flanders), G. Holderbeke and I. Moerman, Ghent University – IMEC – IBBT, Belgium.

M. Jacobsson, V. Prasad, N. I. Cempaka Wangi, I. Niemegeers, Delft University of Technology, The Netherlands

S. Heemstra De Groot, Twente Institute for Wireless and Mobile Communications and University of Twente, The Netherlands

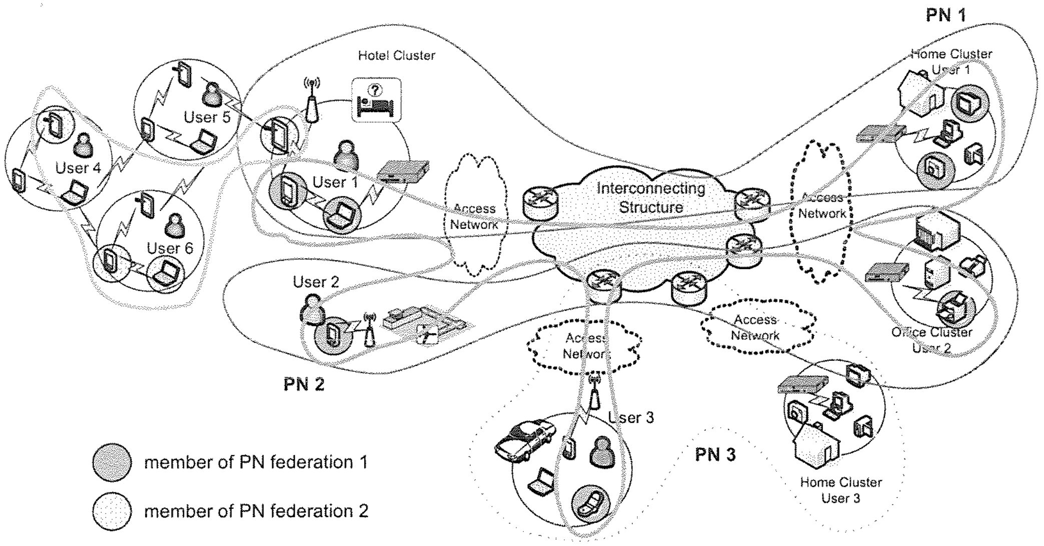


Figure 1: PN federation concept – Illustration of Ad hoc based versus Infrastructure based federations

In the second PN-F in Figure 1, the PN-F is formed in the absence of fixed infrastructure. As no infrastructure is accessible, support functionality cannot be assumed and the definition and establishment of the federation need to be done in a distributed ad hoc fashion, having implications on the solutions that need to be developed to realize PN federations. This type of federation is called an Ad Hoc PN federation and will mostly occur when nearby users collaborate within a federation and will impose different requirements on the networking solutions. Of course, hybrid federations that are a combination of these two types are also possible.

In addition, we can also classify PN federations based on a number of other characteristics. First of all, depending on the way the federations are initiated, we can discriminate between *purpose driven* PN federations and *opportunity driven* PN federations. Purpose driven means that the formation of the federation is explicitly requested or defined beforehand, whereas opportunity driven means that the federation is formed spontaneously when interesting circumstances to do so arise. In both cases, and especially in the second case, context information can play an important role. Next, depending on the lifetime of the federation, we can make the distinction between very *short-lived* federations and *longer term* federations. This distinction will have its implications on the complexity of the solutions to establish the federation. In the case of short-lived federations, solutions to setup and manage the federation need to be lightweight and simple. Longer term federations open up much more opportunities to introduce more complex and powerful management and definition mechanisms. Finally, based on the way the federation process is carried out, both *proactive* and *reactive* federations are possible. Proactive implies that the federation is established in anticipation of the use of the common goal or services provided by the federation or is maintained proactively. Reactive federations are established and used only upon request or when the opportunity arises and only as long as needed. The above classifications will prove useful to assess the requirements imposed to the PN-F definition, management and formation process when developing solutions.

III. The Need for PN Federations

While Personal Networking is focused on the communication between personal devices only, many communication patterns need to extend the boundaries of the Personal Network and involve the secure interaction of multiple persons having common interests for various professional and private services. Examples include: collaborative working, virtual meetings, resource sharing for private and professional services, family networks, virtual classrooms, distant learning, inter-vehicle networks, emergency networks…

For the above examples, common interest groups could be: family members, colleagues, friends, kids at school, public servants (e.g. in safety and security), emergency teams, etc… In all these examples, the basic requirement is that the communication is secure, self-organized, confined within the subset of collaborating devices and that only the resources, applications and services needed to achieve the common goal are made accessible. For instance, in collaborative working a PN-F could be formed between the relevant devices belonging to the different persons working on a common project. Only the resources needed for the project (e.g. files, e-mails, project schedule, whiteboard, software, agenda...) are made available to the PN-F. Further, other resources (e.g. personal files…) are shielded from your colleagues or only available through other federations, for instance with family and friends. The federation can be formed automatically, at anytime and independent of the location of the person's participating devices. In addition, as the federation is a secure overlay, no additional measures need to be taken to secure all users' data and communication. Further, a cooperative session can take place using low capability devices (e.g. participate in discussion using mobile phone), while resources can be made available remotely by the other members of in the federation. Of course, it is clear that this concept will heavily rely on the notion of group trust.

Existing solutions such as virtual private networks or peer-to-peer application overlays can only offer a partial solution as they do not provide true self-organization and end-to-end security. Further, they lack the notion of group trust and usually only focus on one specific software application [3]. In the following sections we will present the main requirements imposed by the challenging concept of PN federations.

IV. Requirements

From the examples presented in the previous section a number of important requirements can be derived that need to be fulfilled in order to realize the concept of PN federations.

Membership management: A PN-F can be seen as a cooperation of different PNs, which are the members of a PN-F, whereby devices of each of the members make resources available. The composition of the members and their resources can change over time. Therefore, mechanisms to define and initialize new federations and to define, configure, manage and store this membership information are required.

Self-organization and maintenance: A PN-F needs to be self-organized and self-maintained. This requires first of all the definition of policies and rules to determine how and when the formation of the federation will take place. Next, the overlay (in terms of services or in terms of members) should be formed and maintained without user intervention, making use of naming, routing and mobility management solutions.

Security: Security is a major aspect in PN federations as multiple PNs are involved and takes place at different levels: access to the PN-F based on membership, secure transport of data within the federation and the access rights to resources and services of the federation.

Application support: Federation members need to specify which resources, applications, services are made accessible to the federation. As such communication is confined in terms of the available resources and data. Profiles will play an important role here.

Scalability and QoS: PN federation enables a lot of potential application scenarios and addresses a large user base. As a result, the number of federations can become huge and in addition, PNs can partake in multiple federations. Therefore solutions are needed that are scalable and that can provide high-quality user experiences.

In the following section, we will discuss in more detail the challenges imposed by these requirements, their influence on the existing PN architecture and, consequently, the PN federation research issues that will be addressed within MAGNET Beyond.

V. Research Challenges

A. PN federation creation and management

In order to be able to create trustable PN federations, rules are needed that determine who is or can become member of the federation and how (membership management), which resources are made available by that member together with policies that define who is able to setup or update these rules and profiles. Based on this, we have identified two different profiles, a *PN-F profile*, which is a profile common to the federation and individual *PN-F participation profiles*, which are bound to the individual members.

The PN-F participation profile can be specific or generic. A specific one defines for an existing PN-F the resources and services the member wants to make available to that PN-F. A generic one defines user interests and requirements related to participating in or setting up new federations and the resources a user wants to make available in case a PN-F is formed based on this profile.

The PN-F profile contains the following policies, rules, agreements common to the PN-F. First of all, the PN-F needs to have a creator. The creator does not necessarily have to be a member of the federation (e.g. parents creating a PN-F that can be used by the children), a group of persons or even a third party (a service provider that creates a PN-F to connect people with common interests). The creator of a PN-F is the one that decides the rules and policies of the federation. In some cases, it can be useful for the creator to be able to change the policies of a PN-F, but in most cases it is better to not allow these policies to change at all. This makes it easier for the members to put their trust in a PN federation.

The policies of the PN-F determine how the membership is managed. Again, multiple policies are possible. The members of the federation can be defined explicitly, by using their PN identifier for instance. In case the members are not defined explicitly, rules can be defined how new members can be added to the PN-F. Members can be invited by existing members (approval needed by one, all or a quorum of the members or by the owner) to join (invitation based) or they can request to join (subscription based) upon which one, all or a quorum of the members decide to accept the request. Next to this, general formal rules can be used to define the membership management, thereby automating the membership management by checking these rules against, for instance, the user profile of new potential members. Also, owners could revoke members. Finally the complete member information, i.e. the list of all members, does not need to be stored explicitly as a web of trust could be formed.

Let us illustrate this with some examples. In the case of collaborative working, a project leader could define a PN-F where he explicitly defines all the members (project team members) and only he can add new members. A service provider can setup a PN-F for people having a common hobby where new members are added based on subscription and acceptance by all existing members. Finally, for an inter-vehicle federation, the government could define a PN-F profile with a membership rule that defines that every vehicle in the neighborhood spontaneously can join the federation in order to increase road safety.

The creation of the PN-F profile can be done beforehand (before the actual formation and use of the federation) or immediately (when the need to form a federation suddenly arises). In the latter case, a search is needed for candidate networks to federate with based on what they can offer (e.g. police man looking for medical personnel when an emergency situation occurs). For this, the generic PN-F participation profiles can be used. In order to setup these spontaneous federations, assistance from context and service discovery frameworks is also needed.

Further, the above PN-F profile contains global information, i.e. relevant for the members of the federation, which needs to be securely stored and accessible by all members. For infrastructured federations, storage can be done centralized or distributed in each PN participating in the federation, for instance in the PN Agent. For ad hoc federations, storage needs to be completely distributed. The decision where to store this information will have its implications on how the existing PN network and architecture should be extended to support PN federations. Of course, as the profile can only be modified by specific persons, strong and efficient security solutions that verify, protect and enforce the rules defined therein and their authentication are needed. In addition, updates to the profile need to be propagated to all involved parties and a lifetime could be assigned to the profile.

B. Application and service support

The PN-F profile contains global information, relevant to every member in the federation. Next to this global information, every member of the federation should be able to individually determine which devices of his PN are allowed to participate in the PN-F and which resources, services and applications of these devices are made accessible to the other members of the federation. As already stated, this information is part of the PN-F participation profile. Which devices participate in the federation is relevant if access control will already be performed at the network level. The information about which services are accessible is required at the service layer and can be implemented by defining service profiles. Accessibility to services can even further be refined in terms of members. For instance, some members of the federation are given more permissions than others.

All this information can be stored in the relevant PN devices, in the Service Management Node (a personal node responsible for the service discovery within a cluster of a PN) or in the PN Agent (entity used to locate all cluster belonging to the same PN). When a member of the federation wants to make use of some of the resources of another member in the federation, this information needs to be consulted in order to find out if this member has sufficient access rights to make use of the service. It is clear that a PN-F constrains the communication to the resources, services and applications each member makes available in the federation. This type of limitations in communication will require extensions to the existing service discovery framework developed within MAGNET [6] and a flexible interface between this framework and the applications and services in order to enforce the access rights.

C. PN federation formation, maintenance and teardown

Once the policies and the membership management information has been defined, additional information related to the formation of the federation can be stored in the PN-F profile. With the formation of the federation we mean the establishment of the actual collaboration, i.e. communication, propagation of information on available services and the use of these services.

First of all, information on how and when the federation can be formed can be part of this profile. As already explained, federations can be formed reactively or proactively. In some scenarios, it can be interesting to add to the profile that the formation of the federation is limited depending on the presence of one, multiple or all of the members, on the availability of certain resources within the federation or at specific times. In addition, once the PN-F is formed, the profile could also define a lifetime of the federation or termination criteria.

As already stated, the formation of the PN federation includes the communication, exchange of service information and the use of the services. First of all, in order to form the federation, the different personal networks participating in the federation need to be able to locate and authenticate each other. Currently, PN Agent functionality has been developed in order to locate and authenticate the clusters belonging to the same PN. This functionality needs to be extended to also provide PN to PN authentication and location based on the PN identification information.

Next, network communication needs to be established between the members of the federation. Within MAGNET, a number of alternative solutions for Personal Networking have been developed. One of these solutions builds the Personal Network as a network overlay based on the concept of Virtual Routers, thereby using its own PN routing and addressing mechanisms [7]. In order to extend this network overlay concept to support communications between PNs, extensions to the overlay concept, routing and mobility management mechanisms are needed. More information on the concept of network overlays between distributed devices can be found in [3]. An alternative solution is to not use this network overlay concept and the federation can then take place completely at the service level, forming a service overlay on top of the personal networks. Extensions to the network level solutions will be more limited and will mainly require extensions to efficiently handle mobility and for ad hoc based federations.

In both cases, the major extensions that need to be provided take place at the service level. The existing service discovery framework needs to be extended with powerful service profiles and mechanisms and protocols to allow resource and service discovery according to the policies defined in the PN-F profile and the PN-F participation profiles.

D. Context

In many PN federation scenarios, context information (user-related, network-related and environment related [4]) can and will play an important role. For instance, the initiative to create a federation can be triggered by relevant context information (e.g. an emergency situation, hobbies or interests). When a federation already has been defined, the formation and use of the federation can be initiated through context (e.g. the presence of people, time, agenda…).

Next to assisting the creation and formation of federations, context can also be exploited to support PN federation once the federation has been created. For example, in order to enhance applications running within the federation or to enhance the federation maintenance process during mobility of the members.

It is clear that the use of context information is promising to enhance PN federation, but many problems need to be tackled before efficient use of context information becomes an integral part of the federation process. Scalability issues need to be solved as the involvement of multiple parties, potentially distributed, will come with large amount of context information that needs to be exchanged, filtered and processed. In addition, this information is generated, processed or used by heterogeneous devices having different capabilities, raising questions how this information can be efficiently represented and propagated. Further, this information needs to be accurate and up-to-date. Of course, as context can reveal a lot of information related to users, privacy and security concerns must not be neglected.

E. Summary

From the above discussion, we can define for the different types of PN federation a cycle as depicted in Figure 2, consisting of the creation, participation, formation and use.

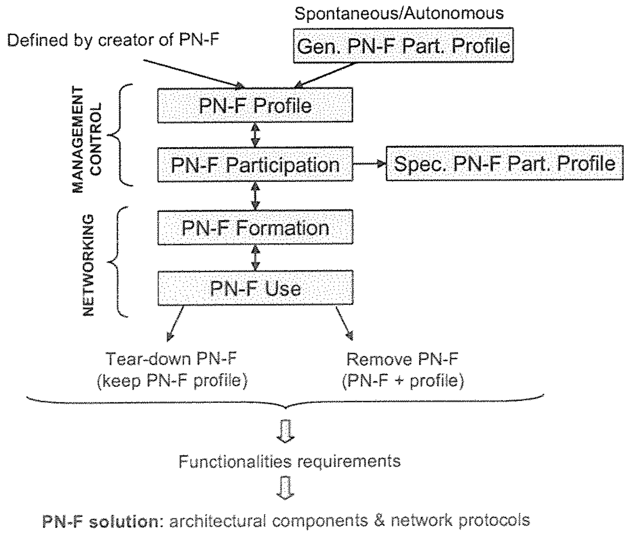

Spontaneous/Autonomous
Defined by creator of PN-F
Gen. PN-F Part. Profile
MANAGEMENT CONTROL
PN-F Profile
PN-F Participation
Spec. PN-F Part. Profile
NETWORKING
PN-F Formation
PN-F Use
Tear-down PN-F (keep PN-F profile)
Remove PN-F (PN-F + profile)
Functionalities requirements
PN-F solution: architectural components & network protocols

Figure 2: PN Federation cycle

Each of the different PN-F types can be seen as a specific path through this cycle. For each of the different phases in this cycle we have discussed the different challenges and federation concepts required to support PN federation. During MAGNET Beyond, these concepts will be materialized into specific PN-F requirements and functionalities. Once the needed functionalities and requirements have been derived, they will be translated into a complete PN-F solution, starting from the developments in MAGNET as baseline, and consisting of a network architecture, node architecture and the respective network protocols and components.

VI. Conclusions

PN federation is a very challenging concept, involving major research challenges related to the definition and management of the federations, service profiles and discovery, security, context and networking. This paper has illustrated the concept, its requirements, its research challenges and the implications on the existing PN architecture to support true PN federation. From there, a number of main corner stones related to PN federation have been defined, which will guide research in MAGNET Beyond on translating these concepts into real solutions, architecture and protocols and validating them.

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. M. Heemstra de Groot, "Research Issues in Ad-Hoc Distributed Personal Networking", International Journal on Wireless Personal Communications, Vol. 26, Issue 2-3, August 2003, pp. 149-167.

[2] I.G. Niemegeers and S.M. Heemstra de Groot, "FEDNETS: Context-aware Ad-hoc Network Federations", International Journal on Wireless Personal Communications, Vol. 33, June 2005, pp. 319-325.

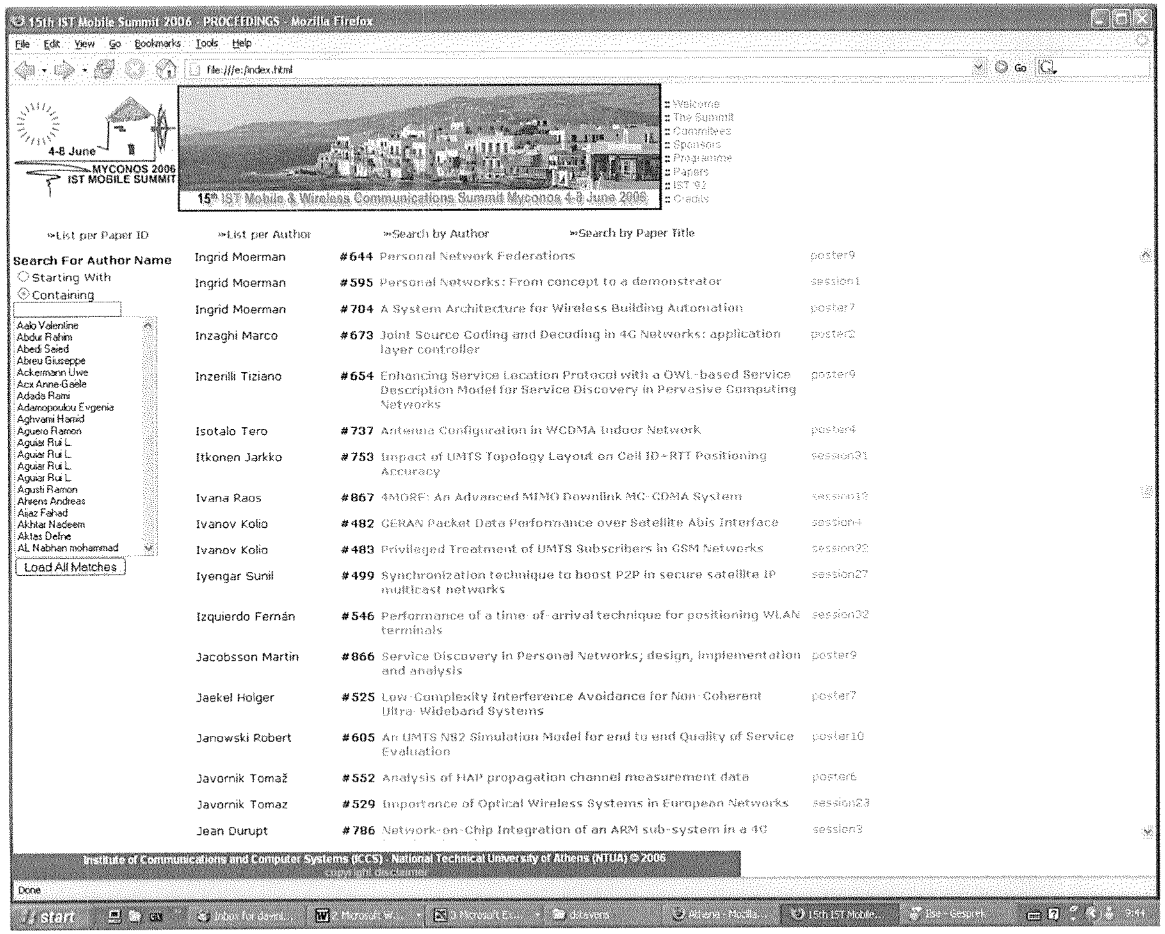
[3] J. Hoebeke et al., "Virtual Private Ad Hoc Networking", International Journal on Wireless Personal Communication, to appear.

[4] R. Olsen et al., "Service, Resource and Context Discovery system specification", IST-507102 MAGNET Deliverable D2.2.3, Dec. 2005.

[5] M. Jacobsson, et al., "A Network Architecture for Personal Networks", In the 14th IST Mobile & Wireless Communications Summit, Dresden, Germany, Jun. 19-23, 2005.

[6] M. Ghader, R.L. Olsen, M.G. Genet, R. Tafazolli, "Service Management Platform for Personal Networks", In the 14th IST Mobile & Wireless communications Summit, Dresden, Germany, Jun. 19-22, 2005.

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



Search For Author Name

○ Starting With

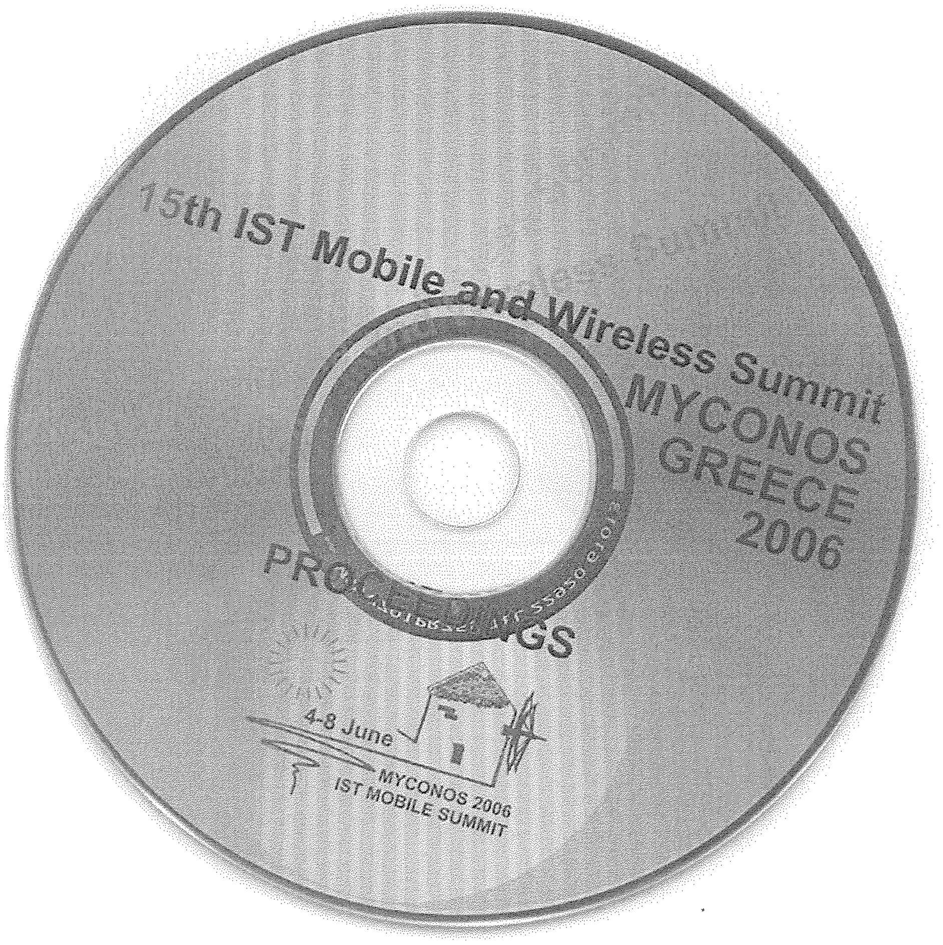
● Containing

Aalo Valentine
Abdur Rahim
Abedi Seied
Abreu Giuseppe
Ackermann Uwe
Acx Anne-Gaële
Adada Rami
Adamopoulou Evgenia
Aghvami Hamid
Aguero Ramon
Aguiar Rui L.
Aguiar Rui L.
Aguiar Rui L.
Aguiar Rui L.
Agusti Ramon
Ahrens Andreas
Aijaz Fahad
Akhtar Nadeem
Aktas Defne
AL Nabhan mohammad

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	session19
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 N82 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

copyright disclaimer


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