VETW 725
2970

Overview of a Personal Network Prototype

Dimitris M. Kyriazanos
Research Engineer, Ph.D. Candidate, Communication, Electronic, and Information Engineering
National Technical University of Athens, Greece

Michael Argyropoulos
Research Engineer, Ph.D. Candidate, Communication, Electronic, and Information Engineering
National Technical University of Athens, Greece

Luis Sánchez
Associate Professor, Communications Engineering Department
Universidad de Cantabria, Spain

Jorge Lanza
Associate Professor, Communications Engineering Department
Universidad de Cantabria, Spain

Mikko Alutoin
Research Scientist, Adaptive Networks
VTT Technical Research Centre of Finland

Jeroen Hoebeke
Researcher, Department of Information Technology (INTEC)
Ghent University, Belgium

Charalampos Z. Patrikakis
Senior Research Associate, Communication, Electronic, and Information Engineering
National Technical University of Athens, Greece

Abstract

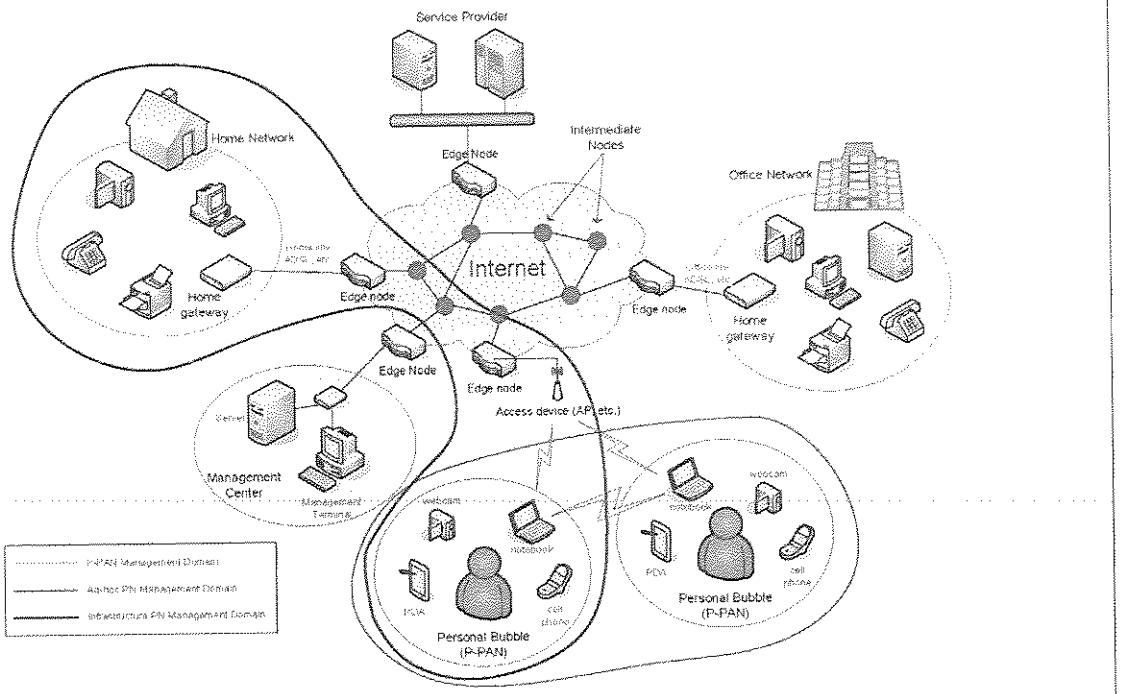
Ubiquitous connectivity and access to services is a challenging task as today's users move through heterogeneous networks and technologies while using a wide selection of devices. Personal networks (PNs) aim to provide a unified overlay network in a transparent and seamless way. In this paper, an overall view of a PN prototype is provided.

The Personal Network Concept

As emerging technologies offer an even wider variety of capabilities to users, the need for convergence and homogenization also rises. Moreover, the real needs of the user should also be taken into consideration to guarantee that provided solutions are more tailored to users' needs. The current sociotechnological status quo raises the demand for shifting environments to become smarter, more responsive, and more accommodating to the needs of the individual without jeopardizing privacy and security. These challenging requirements are encompassed by the PN concept [1], offering a self-configuring and self-organizing network of personal devices, irrespective of geographical location, communication capabilities, and mobility.

A PN is the set of all networking-capable devices that someone uses for personal purposes, including communication, financial transactions, information, and entertainment. A PN may be geographically distributed (e.g., home cluster, car cluster, office cluster) with the clusters interconnected by means of virtual private networks (VPNs) building a "personal overlay network." Despite its very dynamic nature, a PN must be strictly guarded, since the resources it interconnects contain a significant amount of personal information such as contact lists, bank accounts, passwords, or various preferences. The physical layout of a PN is presented in *Figure 1*.

FIGURE 1
The Physical Layout of a Personal Network



In this paper, we present a PN prototype—implemented during the Information Society Technologies' (IST) My Personal Adaptive Global Net (MAGNET) project [2]—that illustrates the self-configuring and self-organizing capabilities [3] required for PN networking and can also serve as an enabler for personal services. The resulting PN architecture paves the way toward PN federations, where multiple PN users with common interests and tasks can communicate and cooperate.

PN Framework and Requirements

Platforms

Before introducing the different technical solutions integrated in the PN prototype, this section reports on the platforms that make up the integrated solution, covering both hardware technologies and software framework. It is important to note that all the communications are both Internet protocol version 4 (IPv4)– and IPv6–based, depending on the final addressing schema defined and the applications in use. The integrated components support both network layer protocols for this purpose.

To assist in better understanding the platform and its components, the presentation will be based on a demonstration setup, including different scenarios that accentuate the full functionality of the PN prototype.

Hardware Platforms

- *Computing devices*: To set up the different clusters and the private personal area network (P–PAN), which is the "bubble" created by devices in proximity to the user, laptops are used to mimic high-capability devices that can be part of the users' PN (*Figure 1*). Personal digital assistants (PDAs) are also used as personal nodes to come closer to real-life situations. Summarizing, the equipment is made up of a set of laptops and PDAs forming the P–PAN and the other PN's clusters, and some PCs acting as edge devices used at the borders of the interconnecting structures. Furthermore, the functionality of the foreseen applications is provided by additional equipment (e.g., cameras, additional PCs acting as servers, a printer), used wherever necessary.

- *Communication equipment*: To emulate the wireless communications in the P–PAN, widely adopted wireless technologies (e.g., wireless PANs [WPANs], wireless local-area networks [WLANs]) have been selected. Institute of Electrical and Electronics Engineers (IEEE) 802.11b/a/g and Bluetooth technologies are the choices for the demonstration. Compliant PC cards, universal serial bus (USB) dongles, or built-in systems are used as the wireless access method. As the prototype is not only focusing on the P–PAN, but also on the PN, a communication with foreign nodes has to be established as well. Gateway nodes have been used for that purpose. For this, they include interfaces both for internal P–PAN communication (Bluetooth, IEEE 802.11 a/b/g) and interconnecting infrastructures featuring wired connections (Ethernet) as a minimum requirement.

Software Environment
The software modules used have been implemented on (and for) the aforementioned hardware platforms. As has been mentioned, the prototype is based on the use of PCs, laptops, and PDAs. The PDAs run embedded Linux OS, while the PCs are based on Linux OS, running kernel 2.6.x family. Linux OS has been chosen for the development framework, as it offers an open-source license with access not only to operating system source code, but also to free drivers for all the communication equipment.

System Requirements
In this section, the authors present a set of base requirements, following related research concerning all layers of a PN. A user-centric approach for PN design, which was adopted by the authors, can be clearly seen in some of the following requirements:

- P–PAN architecture must accommodate devices that implement different types of PAN radios. A PAN radio refers to a radio interface specification that has been defined under the auspices of IEEE 802.15 or 802.11 or in a research project such as MAGNET.
- Service and context discovery must be scalable in order to meet the definition of the potential sizes of a PN. Since PNs can potentially become rather large, the number of services and the volume of context information can also grow rapidly. The service discovery (SD) system must be able to cope with such huge amounts of data.
- P–PAN specific security mechanisms must be hidden from the end user or from applications. The only exception is the authentication phase, where the owner of a P–PAN decides which PAN devices can join his P–PAN.
- Keys and/or passwords used in authentication, integrity, and data origin protection and encryption must be installed in a PAN device so that they are not accessible from unauthorized people.
- A P–PAN must provide a mechanism that hides private services from external nodes. The owner of a P–PAN may want to not only limit access to some particular services within a P–PAN, but also limit the visibility of these services.
- Different wireless access technologies must be able to coexist within a single device. The address allocation for the nodes in the P–PAN should be automatic without the need for user intervention.
- A P–PAN is a family of IP and non–IP devices. Proxy functionality for the non–IP devices is required.
- SD must be able to function without infrastructure, i.e., in a true point-to-point way, and in a heterogeneous link technology environment.
- The SD mechanism must guarantee the integrity of SD information.
- The interconnecting structure must provide secure means for communication between nodes in a PN over insecure network architectures.
- The interconnecting structure must support P–PAN (cluster) movement, causing minimal effects to its nodes, and must not require any user intervention.
- There should be naming and addressing support for the PN devices, while address allocation for the nodes in the PN should be automatic, without the need for user intervention.
- The PN should have a routing mechanism that enables seamless PN connectivity over heterogeneous wired and wireless networks.
- The PN should be established without user intervention.
- Naming schemes must accept updates and should support local name spaces, which differ from one user to another.

Services and Applications
The end-user services used in the PN prototype are a subset of the services that a fully implemented PN system can offer. Many of the end-user services are based on access to files in different nodes and devices such as Web-based file access. Therefore, together with the end-user application programs, dynamically controlled file access has been used in the prototype to implement a user environment that covers many of the services needed in a personal network. Among others, video and audio streaming is supported and has been tested, together with other important services such as real-time surveillance monitoring and remote control of home functions and appliances (lights, washing machine, etc.).

PNs: Challenges and Prototype-Provided Solutions

In this section, the main challenges and requirements that have been tackled by the prototype are summarized. The structure follows the three abstraction levels in which the PN has been divided in the MAGNET project, namely connectivity, network, and service levels. Additionally, the mobility management is presented, since it gathers many of the requirements imposed by PN users.

Convergence of Heterogeneous Interfaces on the Connectivity Level
Connectivity level requirements appear at the cluster level. The main challenge here is the provision of mechanisms that cope with heterogeneity in the cluster. Multiple radio domains coexist in a PN cluster. To have full connectivity among them, multimodal personal nodes supply the mechanisms for handling frames coming from heterogeneous air interfaces, as required by the peculiarities of each radio domain (i.e., point-to-point connection technologies), and for selecting the most appropriate output device in case the nodes are part of several radio domains. The solution implemented for the prototype has been the universal convergence layer (UCL) [4], designed to support cluster formation and maintenance. Neighbor discovery is another issue that

has been also resolved at the connectivity level. A personal node is aware of personal nodes and devices within the same radio domain and inside its coverage area.

Finally, security is present at all abstraction levels defined in the MAGNET PN architecture [5]. Link-level security mechanisms (i.e., encryption of link-layer frames) have been exploited as far as possible during the cluster formation by providing a safe communication channel between trusted nodes on a hop-by-hop fashion. This has been accomplished by the establishment of link-level secure sessions on detection of new neighbors. Keys for these sessions derive from the PN long-term pair-wise keys.

Self-Configurability, Addressing, and Routing Challenges on Network Level

Once the nodes have established the communication paths at the connectivity level, there is a need to select the way secure and efficient information exchange is achieved. Every time nodes have to communicate with each other, they need to know both their peer names and locations. Therefore, the first task to be accomplished within P–PAN formation is the assignment of a name and an address that univocally identify the node. After the node has self-configured its basic network parameters, the next step is to find the way to interact with other personal nodes in the neighborhood as well as with foreign nodes through appropriate gateways.

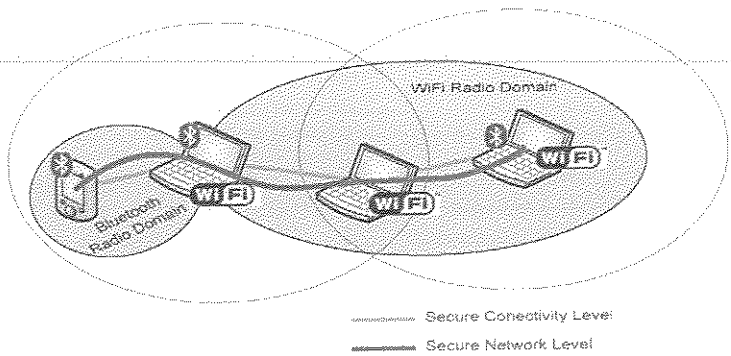
The diversity of devices requires the definition of a set of solutions allowing every personal device, independently from its characteristics, to access any other peer resource. At connectivity level the cooperation among different radio domains has been solved: all P–PAN air interfaces are grouped under a unique identifier and the link-layer mechanism chooses the appropriate interface for establishing communication with a peer. However, personal nodes are unreachable in a single hop if they are out of the coverage range. To achieve end-to-end communication, this connectivity needs to be solved at the network level. Some already known solutions are ad hoc routing protocols that enable multi-hop environments through cooperative use of resources. *Figure* 2 shows a situation where link-layer solutions are not enough and a network approach is necessary.

A P–PAN can be considered a network entity by itself, but in the PN scope, it is a requirement that communication with external nodes, either in its neighborhood or by means of infrastructure, can be established. With connectivity acquired, services can also be discovered and accessed or provided. A gateway enables connectivity to nodes outside the P–PAN while a delegated node known as the service management node (SMN) acts as a repository of the services offered by P–PAN nodes and devices. The service discovery must be as lightweight as possible so as to be feasible for any P–PAN node to make use of it (smartphones, PDAs). Delegation of the SMN is a result of a selection procedure, which occurs at the moment when connectivity among all P–PAN nodes is supplied by the naming and addressing procedure (i.e., the moment when the P–PAN is formed). Once the SMN is selected, every node is able to discover any registered service, including the gateway functionality service.

The selection procedure involves a sequence of tests in which the strongest device—from a computational and networking point of view—becomes the SMN and is based on the request parameters that fit the source peer capabilities. In the P–PAN, different paths to an outside network could be configured. Security is also a main concern in the PN scope and plays an important role in the whole architecture. From the connectivity level, there is an inherited security for each link. Securing the communication on the connectivity level may not always be feasible; therefore, nodes must be enabled with network-level solutions to guarantee the level of security needed within the P–PAN. There are many security mechanisms that can be used to protect communication. In this case, unlike in the connectivity level, the channel will be secured end to end. This would be sufficient, provided that both peers have previously identified themselves. This identification procedure is conducted at the initial steps of the P–PAN formation through the exchange of keys and identities.

Extending all above, when a foreign node or device and their provided services are going to interact with a MAGNET P–PAN or PN cluster, long-term trust relationships must be examined and secure communications between nodes should be enabled. The connectivity with a local but

FIGURE 2
Network-Level Communication



foreign node or device to the P–PAN node will depend on the security profiles available at the service and connectivity level. For the PN-to-foreign-user requests, profile mechanisms and service access control by light AA components can be used.

Unique PN prefixes are envisaged advocating the use of private or local IPv6 addresses that are different from those used by public foreign nodes as well as other private nodes. To communicate with the local-foreign node, a network address translation (NAT) function would typically be needed for Layer 3 (L3) communications. Thanks to the use of IPv6 addressing, the probability of colliding addresses is very low and there is no need for a NAT function. In the other direction, for foreign requests, the P–PAN is in need of a special authentication. This can be based on public key infrastructures (PKIs) or prior symmetric key exchange similar to the PN imprinting. An ephemeral exchange of secrets can be used to temporarily allow access to the P–PAN and PN.

In this point, we have to go one step beyond. In this scenario, we suppose that a node of the P–PAN uses a public service outside our PN. This public service may be located practically anywhere on the Internet, but not in the vicinity of the P–PAN. The prerequisite for this scenario is that P–PAN has been formed utilizing the pre-shared PN keys. Furthermore, one or more gateway nodes are set up to provide connectivity to the outside world. The P–PAN may or may not have edge routers (ERs) available. If there is no ER available, the gateway node handles the required functionalities itself. So when establishing the connection to the remote public service, gateway nodes must conclude the most suitable media for the connection. In a general case, this means that all the connection types provided by gateway nodes must be evaluated with respect to the quality of service (QoS) requirements of the service. The gateway node must provide the necessary network-layer connection functionality for the service. If the PN address space is private, then NAT needs to be performed by the gateway node or ER. Other services may additionally require proxy mechanisms from the gateway node such as port forwarding for active FTP. The gateway node provides these functionalities for the user application or delegates them to a nearby ER. However, the gateway node must not engage in the NAT function using a temporary Internet address, because then the established connection is broken once the address becomes invalid (e.g., due to mobility). In this case, the ER provides the NAT function for the cluster. This also applies if the access network is using private IP addresses.

Finally, the PN technical scenario extends all technical cases described before, not only for personal nodes and devices in the local vicinity of the user, but also for those that are farther away (at home, at work, in the car, etc.) and it describes how these personal nodes in different clusters securely communicate with each other over a fixed interconnecting structure such as the Internet. To this end, the remote clusters have established a secure communication channel between each other, transparent for the end user and applications. To the end user, the PN is seen as one virtual network offering a plethora of personal services, but at the same time hiding the details of the interconnection structure, tunneling mechanisms, PN formation, and maintenance. *Figure 3* shows the deployment for visualizing this PN technical scenario.

ER and Cluster Gateway Interaction

Any node in a PN cluster can become a gateway node. As a result of the successful completion of the ER discovery process in a PN node, an IP address of an ER is retrieved. This event is triggering an IPSec key negotiation mechanism in order to set up a tunnel between the public interface of this PN node and the discovered ER. The direct consequence of this IPSec tunnel establishment is that the PN node becomes a PN gateway node. Once the node becomes a PN gateway node, it informs the rest of the nodes in the cluster about this new capability.

PN Agent Creation/Construction and Cluster Registration

As the establishment of overlay networks to provide intra–PN connectivity relies primarily on the concept of the PN agent—whose role is to maintain key PN information for networking purposes—a description of the PN agent construction is first presented to ease understanding of intra–PN self-configuration and networking. In the PN agent concept, the following two steps occur:

- The PN agent server stores the PN agent information. If the PN agent is centralized, there is a unique server. Otherwise, the distributed servers collaborate to disseminate PN agent information and resolve queries.
- The PN agent client asks the PN agent to perform the cluster registration and deregistration actions.

When a cluster connects to an edge node, the gateway passes its cluster name to the PN agent client. The incoming cluster name is concatenated with the location information of the ER (e.g., the ER's Internet address) into a cluster name record that will be advertised to the name resolution network (i.e., to the PN agent). These records actually form the PN agent within the naming system. In this manner, the PN agent will keep the information about the cluster gateway and its attachment point IP address. The name resolvers (NRs) point-to-point overlay network exchanges the name records so that the PN agent can be accessed from any intentional NR (INR). At the time of cluster registration, the cluster nodes announce their names to the naming system. As it is shown in *Figure 4*, in order to tackle the aforementioned procedures, the PN agent has been implemented using the intentional naming system (INS)/Twine framework, where an INS application in the ERs takes the PN agent client role, while the point-to-point network formed by the INR offers the PN agent server functionality in a distributed manner.

Name-Based Tunnel Establishment

When establishment of tunnels between PN nodes is based on policies relying on names, we talk about name-based tunnel establishment. A flexible and scalable naming system such as INS/Twine has been selected to conduct the tunnel establishment and, as previously mentioned, embed the PN agent framework.

Cluster Mobility

The PN agent, using the INS/Twine framework, is capable of assisting mobility management in the PN architecture. When a cluster moves, it de-registers itself from the PN agent by removing its corresponding name record from the INRs. It then passes its name to the new visited ER, which will announce this name to the naming system. Therefore, the mapping between the cluster name and its associated

FIGURE 3
PN Technical Scenario

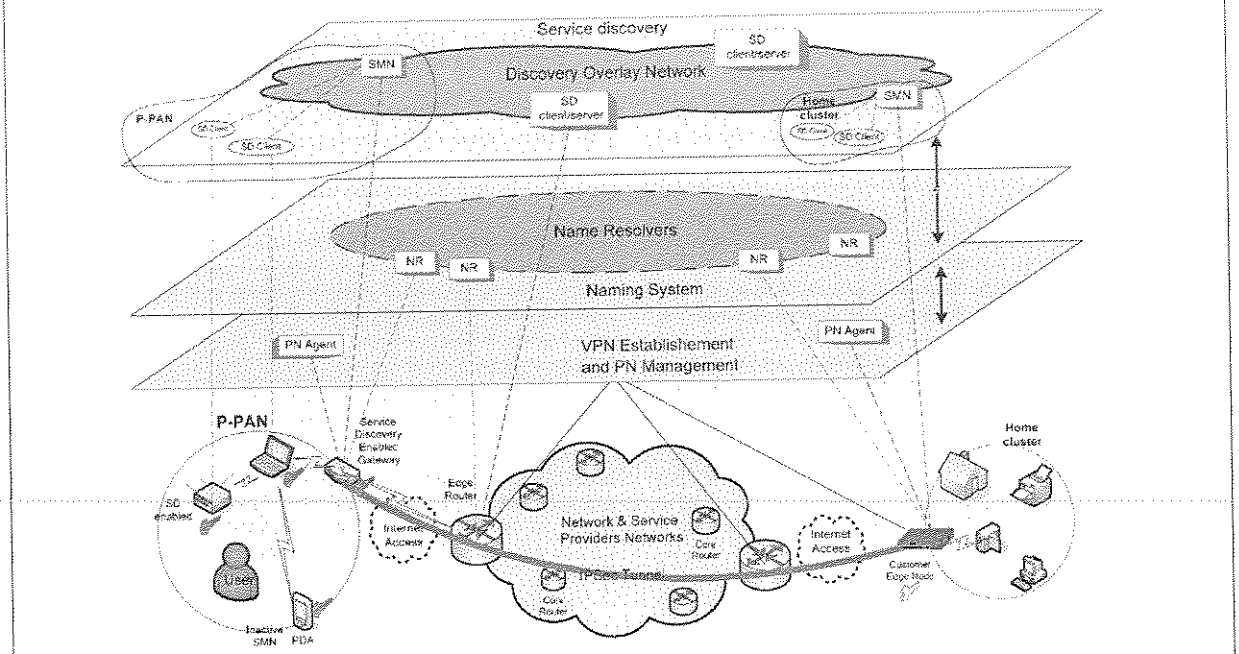
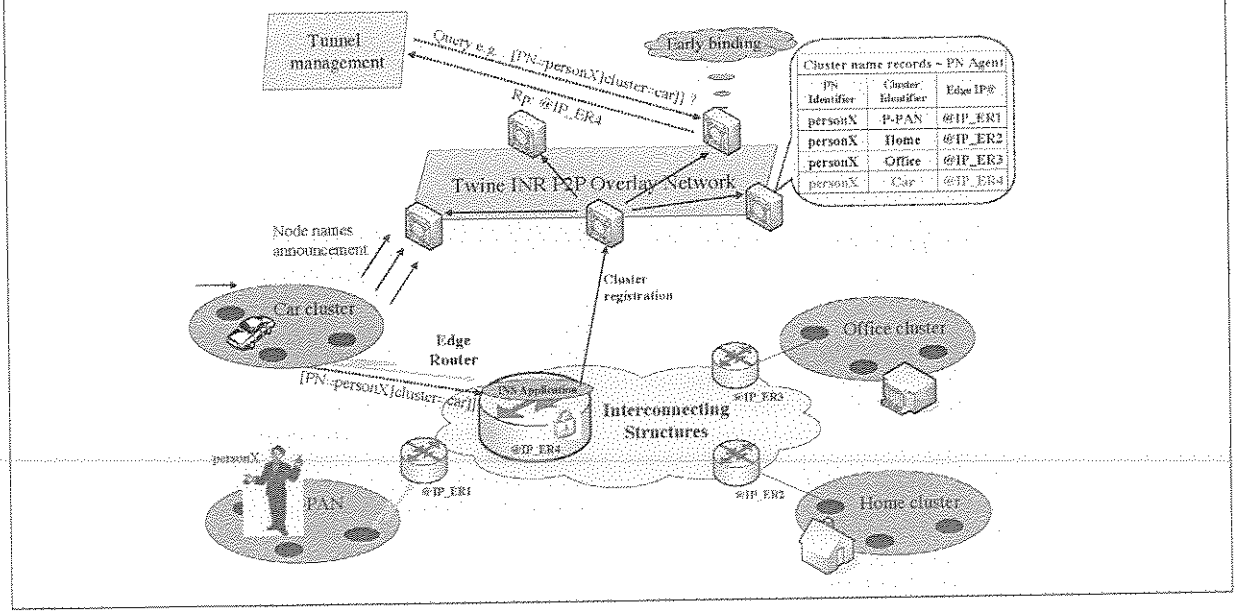


FIGURE 4
PN Agent Concept within Naming Systems

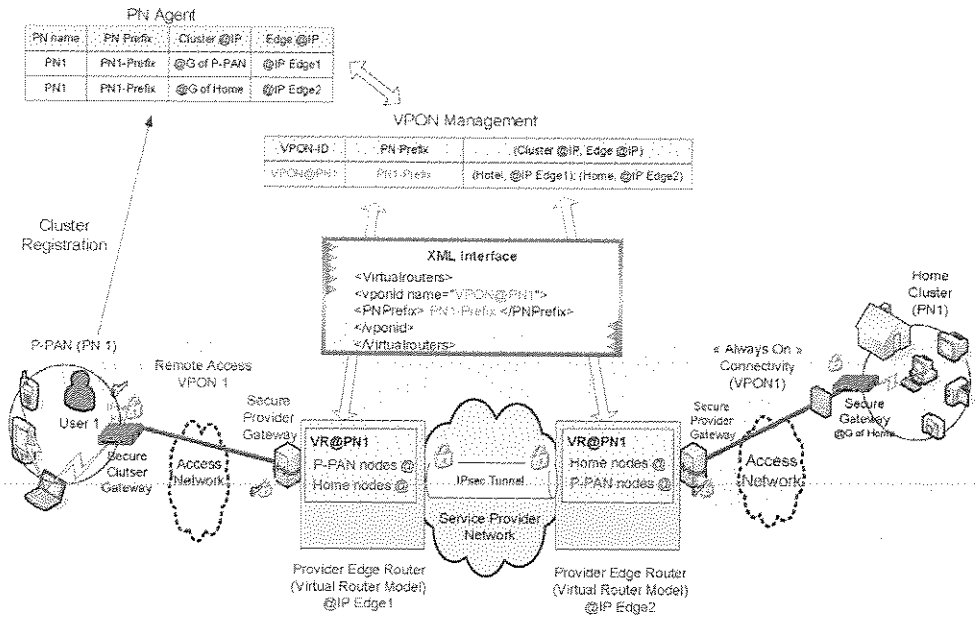


serving ER IP address will be updated. This procedure is done dynamically without user intervention and assures an always-connected behavior since the PN gateway nodes will be ready to support PN connectivity even under mobility conditions.

Virtual Router and PN Agent Interaction

As depicted in *Figure 5*, the PN agent interacts with provider edge (PE) nodes that support PN services to achieve PN networking, according to the dynamic changes in the clusters and the P-PAN. The PN agent maintains a table of registered clusters and the IP addresses of the edge nodes that

FIGURE 5
Deployment of Virtual Personal Overlay Network (VPON) Using Virtual Router Approach



are serving as their ingress and egress tunnel endpoints. It partakes in PN establishment, maintenance, and management by interacting with the naming system, addressing and routing, PN management, mobility management, and the security framework.

Cluster Mobility Management Using a Dynamic Tunneling Approach

The previous sections described cluster registration and the creation of tunnels to establish secure intra–PN communication. This section explores the mobility aspect of a roaming cluster using dynamic tunneling mechanisms. This extended section describes also the interactions between proactive routing in the P–PAN and the interfaces and information exchange with the virtual router (VR) instances [6, 7].

Figure 6 depicts a scenario where a moving P–PAN is changing its attachment point to the network. In this scenario the mobility results in a change in the PE. To maintain connectivity, management of cluster mobility must be combined with the dynamic tunneling framework. This change in the attachment point is reflected by an update in the PN agent that consequently adapts PN networking according to the dynamic changes in the clusters.

When roaming, clusters change their point of attachment (as a result of Layer-1 [L1] monitoring and the proactive routing framework in the P–PAN), the following subsequent actions take place in the VPON nodes:

- Old remote access through PE1 is canceled and a new remote access is established by the P–PAN through PE3.
- The same actions described before are repeated to establish a new inter-cluster connectivity. The PN agent and the VPON membership table are updated at run time with the new IP address of the gateway node as well as the IP address of the PE router 3.
- A new VR instance is created in the PE3, which interacts with PE2 through a static tunnel across the service provider backbone. All PEs collaborate to achieve fast-forwarding of context data and pending packets in the old PE1.

Wide-Area Service Discovery, Overlay Access Control, and Policy Management on Service Level

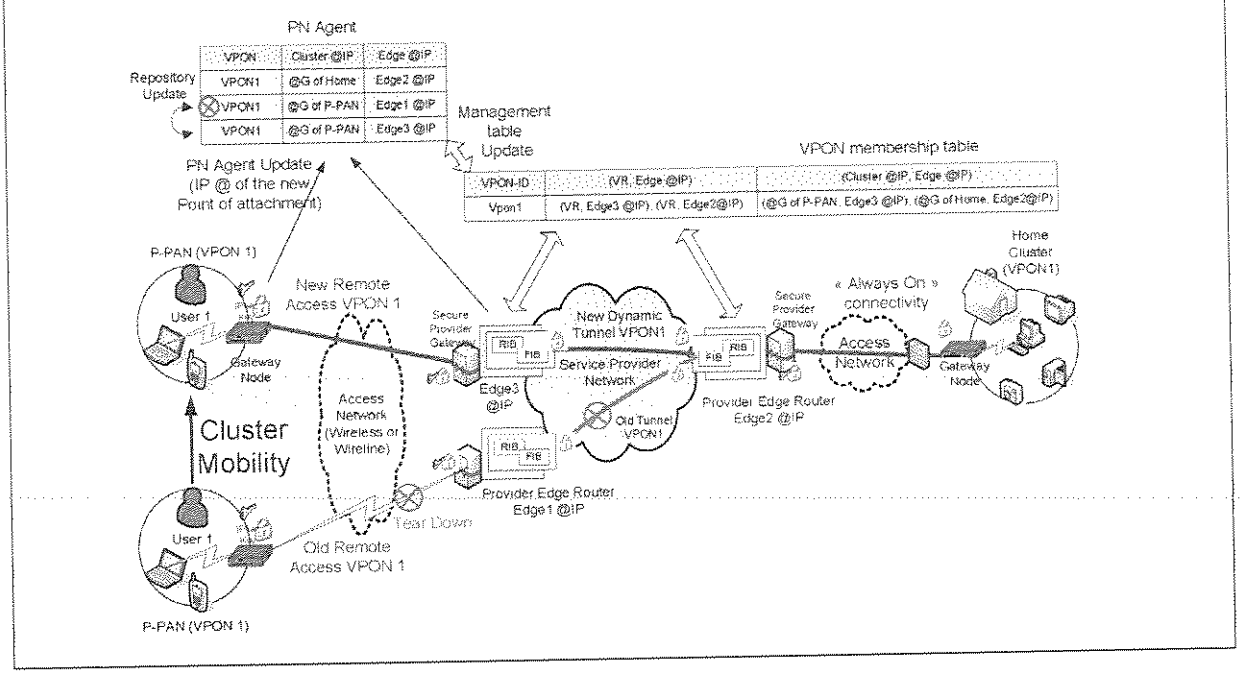
The service discovery architecture inside the P–PAN is based on a centralized approach, that is, SMN will federate all service-related needs. It acts as a repository of services registered within the P–PAN and also enables searches outside the P–PAN in case services are outside the P–PAN.

The PN–wide service discovery is achieved through a point-to-point overlay network of SMNs, as depicted in *Figure 3*. The SMN acts as a super-peer for its cluster and is part of the PN SMN point-to-point overlay network that includes all cluster SMNs as members. The P–PAN/cluster SMN super-peer is added to the PN point-to-point overlay as soon as the external connectivity is available through any of its cluster gateways.

When a P–PAN/cluster SMN receives, from its cluster service discovery client, an SD request that does not match any local services, it propagates this service discovery request within the PN super-peer overlay network to all the other

FIGURE 6

Cluster Mobility Management Using Dynamic Tunneling Approach



PN cluster SMNs. Each of these distant SMN super-peers then performs the following operations:

- Extracts search attributes contained in the received SD request
- Searches in its cluster service repository for local services that match the search attributes
- Sends an SD response for all retrieved matching local services to the SMN that initiated the SD request

The P–PAN/cluster SMN (the search initiator) gathers all the SD responses that are sent by the other PN SMNs within the super-peer overlay network in order to form the global SD response. Finally, this SMN sends back this global SD response, in the appropriate SD framework format, to its cluster service discovery client that initiated the search [8].

Access control throughout the PN is a challenging task. Besides the lack of a centralized authority due to connectivity restrictions, connectivity is again not guaranteed to every cluster inside the PN. Therefore, certain clusters might be out of reach of the owner-administrator. With respect to these problems, we present here a solution for a distributed and decentralized access control system [9].

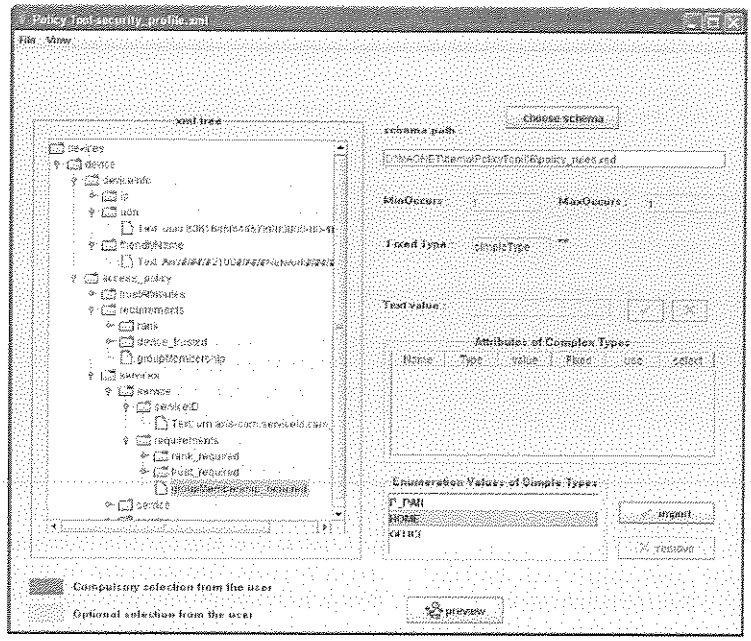
Based on the security profiles, access control modules and profile repositories were designed and developed to function in a distributed way throughout the overlay access control system formed by the interconnected set of SMNs. In this way, each SMN acts independently as an access policy officer for all the devices and access requests under its jurisdiction. Moreover, devices that are capable of holding profile repositories and access control modules subsequently perform access control in a decentralized way. For devices incapable of holding such modules, including sensors, proxies are needed.

On the other side, the user performs policy management over the entire PN using a proper administration tool. Even in case of a cluster losing connectivity to the rest of the PN, the corresponding master device is expected to block any unauthorized access requests. However, in situations of an isolated cluster, access rights and certificate revocations issued by the PN administrator will fail to reach the SMN. In order to minimize the impact of such unfortunate situations, the granting of privileges and access rights below a default high level of security should at all times be ephemeral and stamped with an expiration time. Such time stamps reduce the risk and the extent of damage caused by exploiting a lack of connectivity to the PN administration, since any expired granted rights can be revoked, even by isolated nodes, equipped with the proper modules. As a future work, time-stamping techniques and modules will be developed for enhancing the PN access control system.

Finally, any communication between modules and the policy management administration tool remains secure since it is based on the underlying security infrastructure created from the imprinting procedure, trust establishment, and subsequent key and certificate generation.

Policy management throughout the PN is achieved by properly propagating profile information updates by the PN administrator. For this purpose, a tool is provided for the policy administrator through which policies can be issued regarding entities placed anywhere inside the PN, providing policy management for the overlay network through a tree-like structure graphical user interface (GUI), shown in *Figure 7*.

FIGURE 7
Policy Management GUI



Once policies are personalized according to user interaction, propagation of policy updates throughout the PN is achieved by utilizing the SMN functionality inside the PN, properly notifying responsible SMNs for any changes in their local policy settings.

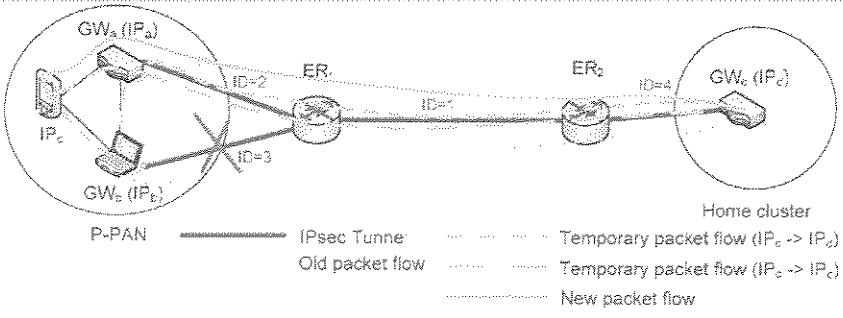
Mobility Management

The mobility scenarios described in this section explain how the PN organizes and maintains itself in the light of dynamics such as changes in gateway nodes and ERs. The way the PN protocol solutions are able to deal with these dynamics in a timely manner, while maintaining session continuity, will be demonstrated. The behavior and performance of the PN architecture will be demonstrated for three types of dynamics, which will be described in more detail.

Mobility Scenario 1

In the first scenario (see *Figure 8*), we assume a cluster that has two gateway nodes, connected to the same ER (e.g., one node connected via 802.11 and one using an Ethernet cable). One of the gateways is used to establish a connection to a remote personal node at home. Suddenly, the connection of that gateway node to the ER breaks. At that point, traffic should be re-routed by the intra-cluster routing protocol. This does not have any implications on the ongoing communication session.

FIGURE 8
Network Architecture Concerning Mobility Scenario 1



Mobility Scenario 2
In the second scenario, the roaming P–PAN (see *Figure 9*), we assume a P–PAN that is connected to an ER in the interconnecting structure through a gateway node. A communication session with a remote personal node is ongoing, thereby using a dynamic tunnel established between the local and remote ER. Due to the mobility of the P–PAN, the P–PAN looses its connectivity to the interconnecting structure and thus the current ER. Next, the P–PAN rediscovers connectivity to the interconnecting structure and an associated ER (e.g., via another access point). When connectivity is regained, the P–PAN, which has a new point of attachment to the interconnecting structure, discovers a new ER and registers itself to the new ER and the PN agent. This registration will trigger the establishment of a new tunnel between the new and remote ER. In addition, the old ER should detect that connectivity to the PN cluster has been lost and tear down the tunnel that had been established, cleaning up the existing information in the PN agent. During the whole procedure, the ongoing communication session does not break but, in the worst case, simply experiences a short delay.

Mobility Scenario 3
Finally, the last mobility scenario (see *Figure 10*) is a combination of the two previous scenarios. Now the P–PAN has two gateways (e.g., WLAN and Universal Mobile Telecommunications System [UMTS]) that are connected to different ERs. One of the gateway nodes is used for an ongoing bidirectional communication session. At a certain moment, one of the ERs becomes unavailable. The PN protocol solutions reroute the traffic so that ongoing communication session is not interrupted.

PN Prototype: A Storyline

The previous sections have described the different technical solutions implemented and integrated in the PN prototype. In this one, a unified vision will be given by defining a storyline in which different scenarios will occur following a timed sequence of events, thus resulting in the demonstrator of the prototype described in this paper. In this sense, the four main scenarios into which the prototype can be divided are as follows:

- PN formation
- P–PAN formation
- Introducing a new node in the PN
- Discovering services
- Within the P–PAN
  - Outside the P–PAN

The demonstration illustrates the situation of a journalist who needs to attend the next European Union leaders' summit in Brussels. The same day of the meeting, the journalist flies from his hometown to Brussels. He travels with his lap-

FIGURE 9
Network Architecture Concerning Mobility Scenario 2

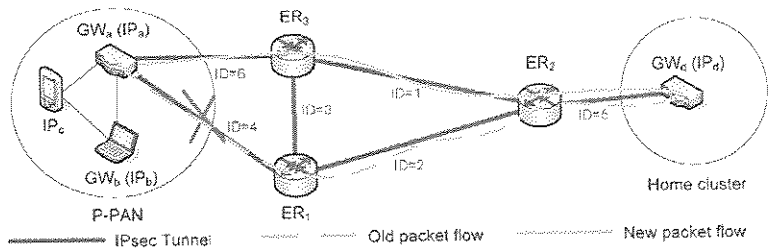
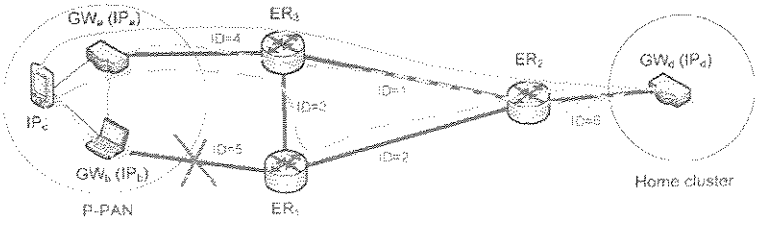


FIGURE 10
Network Architecture Concerning Mobility Scenario 3



top, mobile phone, camera, and new PDA (in the demonstration, these devices are three laptops and one PDA, respectively). As he boards the plane, he has to switch off all his electronic devices, but the rest of his personal devices are still on. At work, he has a couple more devices (two laptops—GW–O, SMN–O) and at home he has his home network with remote control and leisure facilities (another two laptops in the demonstration—GW–H, SMN–H). This situation is shown in *Figure 11*.

As can be seen, both clusters are interconnected through secure tunnels. As soon as the journalist arrives as his destination, he starts switching on the personal devices he is carrying. As shown in *Figure 12*, he first switches on his mobile phone (GW–P). As this device is able to connect to the Internet, it automatically registers himself in the PN agent to allow the establishment of the secure tunnels with the remote clusters, both at his home and at the office. The tunnels are established and the PN enlarged with a new cluster, this time the P–PAN.

Any node in a PN cluster can become a gateway node for the other cluster members, enabling remote intra–PN communication. As a result of the successful completion of the

FIGURE 11

Journalist's PN Composed of Home and Office Clusters

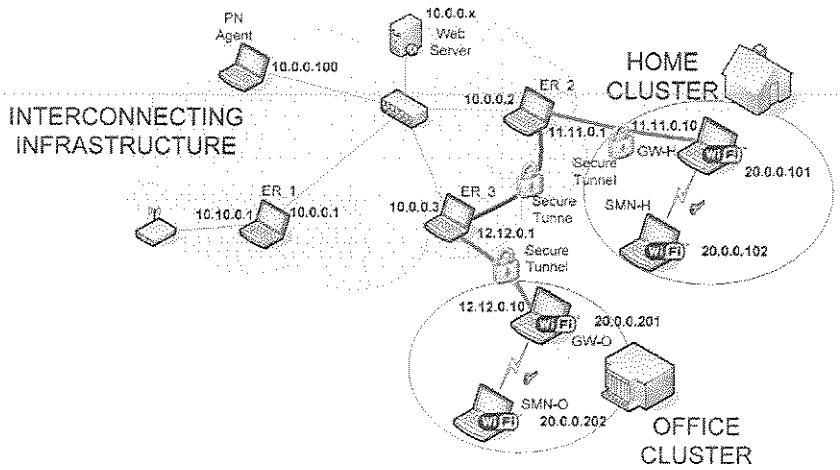
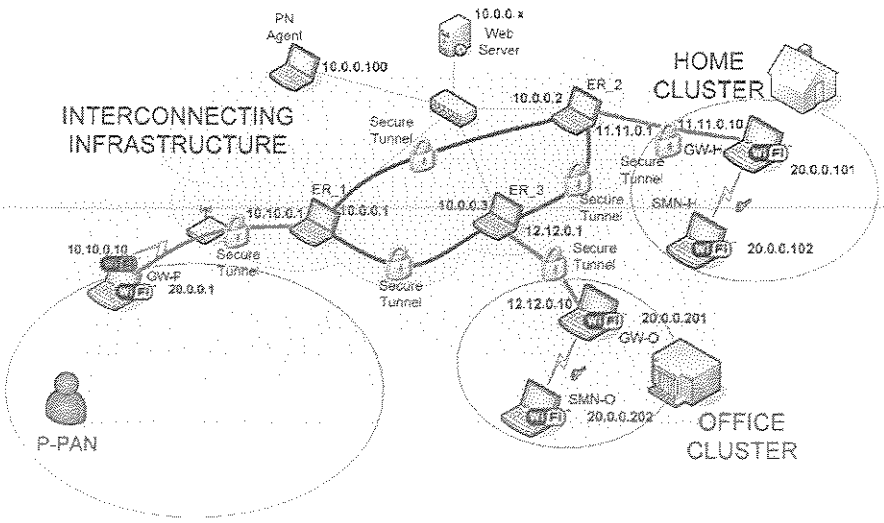


FIGURE 12

P–PAN Registration in the Journalist's PN



ER discovery process in a PN node, an IP address of an ER is retrieved. This event will trigger Internet protocol security (IPSec) key negotiation mechanism in order to set up a tunnel between the public interface of this PN node and the discovered ER. The direct consequence of this IPSec tunnel establishment is that the PN node becomes a PN gateway node. Once the node becomes a PN gateway node, it informs the rest of the nodes in the cluster about this new capability.

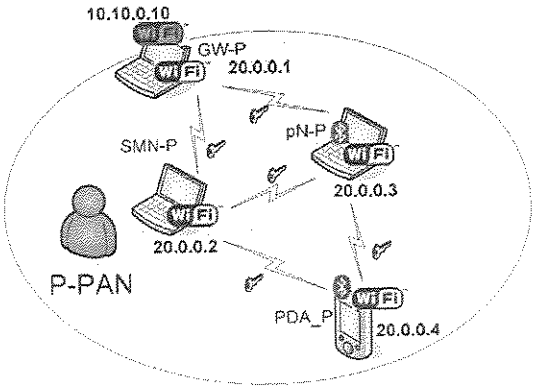
All the journalist's devices discover each other and form the P–PAN by exchanging the session keys that will allow them to communicate in a private and secure way. Finally, the rest of nodes discover the mobile phone (GW–P) as their gateway to the Internet and they are registered in the PN agent so that the rest of clusters have knowledge of the exact composition of the P–PAN. As shown in *Figure 13*, a GUI was implemented to allow the user managing the P–PAN composition. In this GUI, personal nodes appear in blue while foreign ones appear in red. Thanks to this GUI, the user realizes that he has not yet imprinted (i.e., established the long-term secrets that bootstraps the trust relationship between personal nodes) his PDA with his camera. *Figure 14* shows how the journalist can press a button on this GUI to start this imprinting procedure.

The result of this process is the exchange of long-term cryptographic secrets that will be used to derive session keys and authentication mechanisms in order to protect the communications between this pair of nodes. As shown in *Figure 15*, autonomously and transparently to the user, all his devices have formed his PN: a protected secure person-centric network that connects all his active personal devices, including personal devices at remote locations such as the home network, office network, and car network.

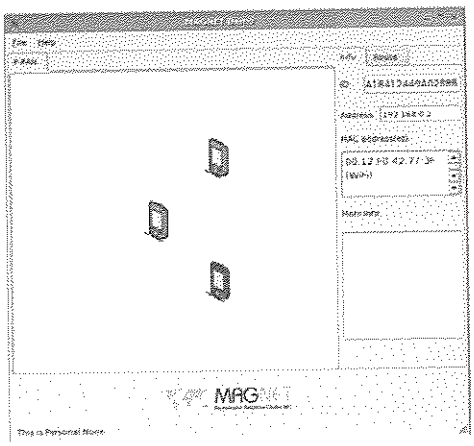
Once the PN is formed, the journalist can start accessing the services provided by all his personal devices on a secure and

FIGURE 13

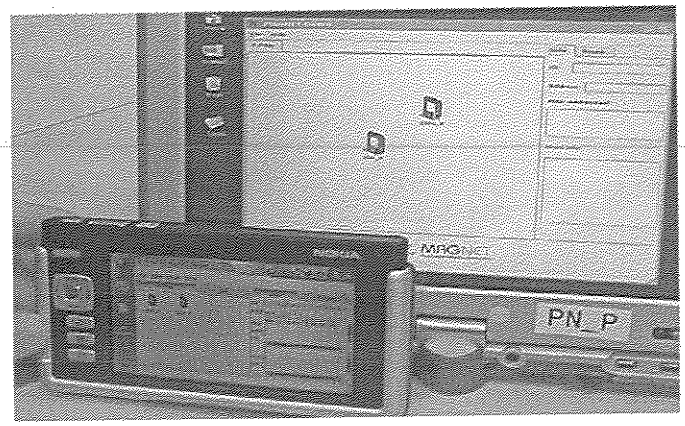
P–PAN Composition (a) and Screenshots (b), (c)



(a)



(b)



(c)

FIGURE 14
Imprinting Process

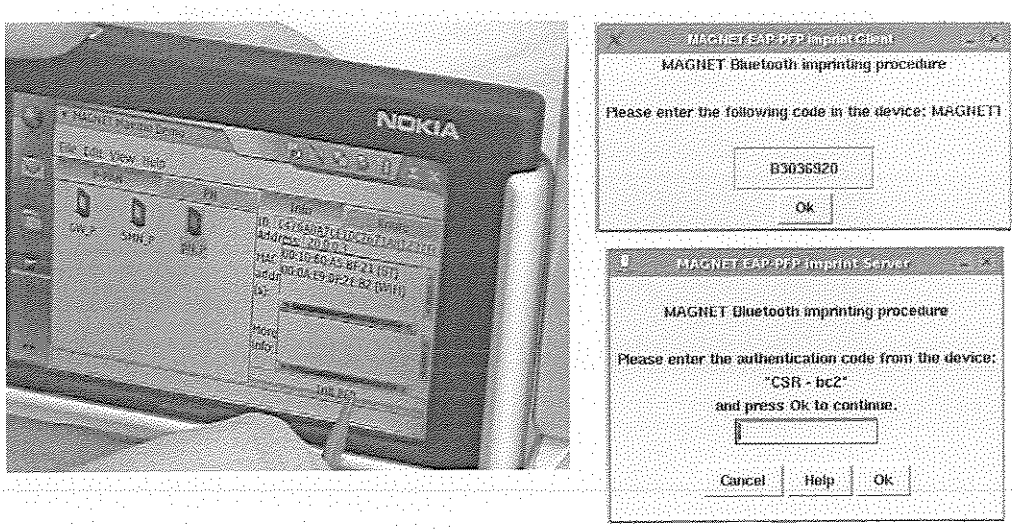
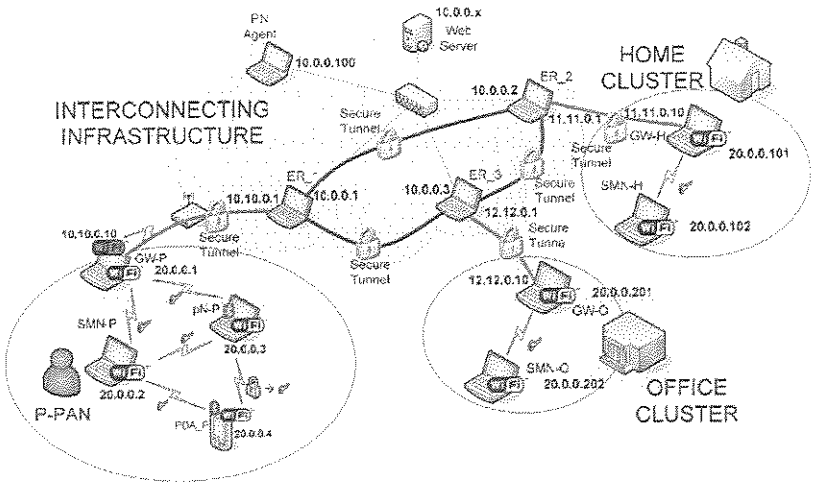


FIGURE 15
PN Composition

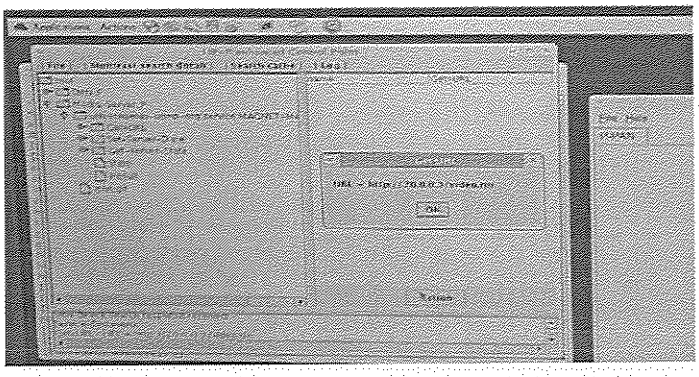


private way. The journalist is able to discover all the available services within the P–PAN as shown in *Figure 16*.

The journalist is now able to access, from his laptop, the video and audio stream his camera is generating. With his video edition application in his laptop, he starts to record the stream adding comments and excerpts. He realizes that some documentation he has in his computer in the office would be really helpful to finalize his report of the meeting. Using the same GUI shown in *Figure 16*, he discovers his content access service at his office. He is able to access all the content of his computer just by clicking a couple of buttons. Once he has finalized the report, he uploads it on a shared folder so that his colleagues are able to review it. He also starts a videoconference with his colleagues at the office to discuss the report. All the traffic is securely transported over the Internet so nobody can have access to this material.

Once he has finished his work and while waiting on the boarding gate, he takes advantage of his PN to remotely control his home appliances (he starts his washing machine and checks if he left the lights on, etc.). Finally, he has some

FIGURE 16
Service Discovery



time left and relaxes watching a movie he had recorded the previous night that is stored on his home digital video recorder.

Conclusions

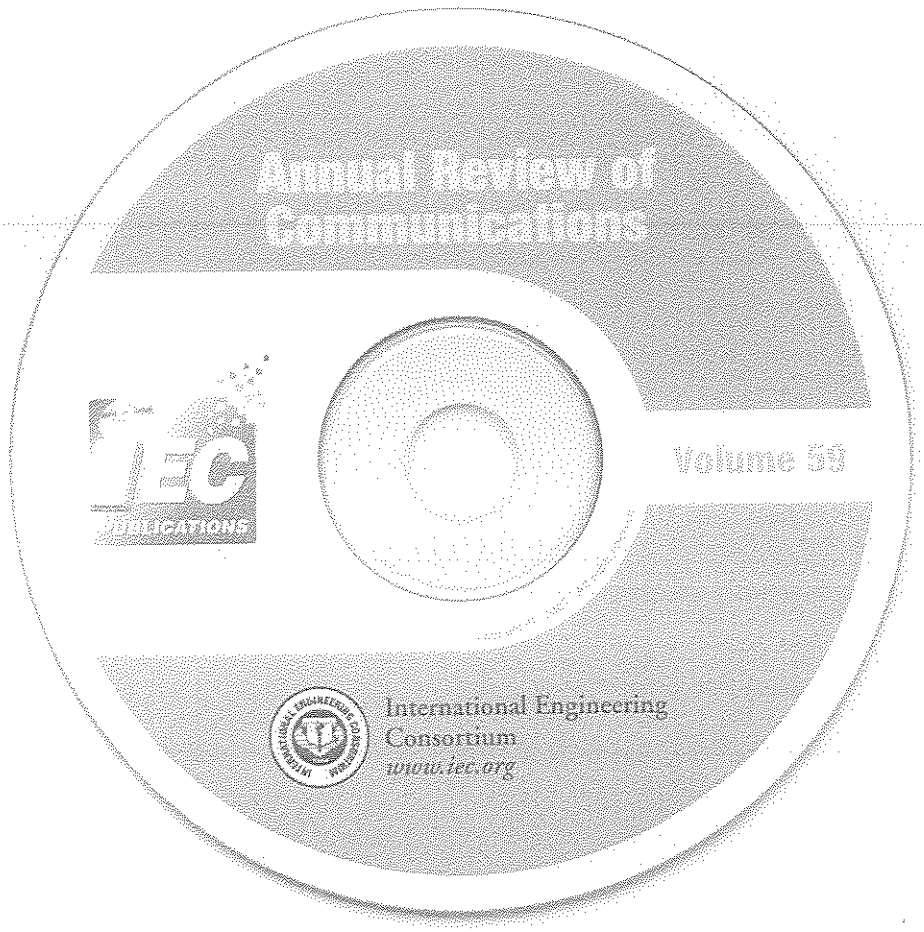
The developed PN architecture and implemented and integrated software components have led to the development of a working PN prototype, enabling secure communication between personal nodes independent of their location and personal services. Currently, this work serves as a basis to develop real pilot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

Acknowledgement

This work has been performed in the framework of the IST projects MAGNET and MAGNET Beyond [2], partly funded by the European Union. The authors would like to acknowledge the contribution of their colleagues from the consortium.

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. IST-MAGNET consortium, www.ist-magnet.org.
3. L. Munoz, et al., "A Proposal for Self-Organizing Networks," Wireless World Research Forum Meeting 15 (SIG 3), Dec. 8–9, Paris, France.
4. L. Sanchez, J. Lanza, L. Muñoz, J. Perez, "Enabling Secure Communications over Heterogeneous Air Interfaces: Building Private Personal Area Networks," Wireless Personal Multimedia Communications – Aalborg, September 2005, pp. 1,963–67.
5. M. Petrova et al., MAGNET Public Deliverable D2.1.2 "Overall secure PN architecture."
6. 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.
7. W. Louati and D. Zeghlache, "Virtual Router Concept for Communications between Personal Networks," eighth International Symposium on Wireless Personal Multimedia Communications, 2005, Aalborg, Denmark, Sept. 18–22, 2005.
8. W. Louati, M. Girod Genet, and D. Zeghlache, "Implementation of UPnP and INS/Twine interworking for scalable wide-area service discovery," eighth International Symposium on Wireless Personal Multimedia Communications 2005, Aalborg, Denmark, Sept. 18–22, 2005.
9. D. Kyriazanos, et al., "MAGNET Personal Network Security Model: Trust Establishment, Policy Management and AAA Infrastructure," Wireless World Research Forum Meeting 15 (SIG 3), Dec. 8–9, Paris, France.


Annual Review of Communications
IEC PUBLICATIONS
Volume 59
International Engineering Consortium
www.iec.org