2314.
515.

Networking in Personal Networks

Wajdi Louati, Wassef Louati, Jeroen Hoebeke, Gerry Holderbeke, Ingrid Moerman, Mikko Alutoin, Kimmo Ahola and Djamal Zeghlache[1]

***Abstract*—This paper addresses networking in terms of tunnels and overlays establishment, naming, addressing and routing for Personal Networks (PN). A number of concepts to achieve PN networking and management are presented. A PN Agent is introduced in the PN architecture. The PN Agent supplies information about Clusters, which constitute the PN, in order to enable networking within the PN. The paper also explores the use of edge routers in the overall framework to support PN services and PN networking via the Virtual Private Network (VPN) paradigm. The Virtual Router concept, well established for layer 3 VPN solutions in networks, is advocated to resolve scalability and latency requirements in PN networking. A hybrid solution involving both user and provider provisioned VPNs to establish Personal Network overlay is suggested to find a compromise between scalability and security requirements. Proactive and reactive routing along with flat and subnet based addressing for PN are also covered by this contribution.**

***Index Terms*—Personal Networks, Virtual Personal Overlay Networks, Naming, Addressing, Routing.**

I. Introduction

The Personal Network (PN) concept is an extension of the Personal Area Network (PAN) including all of a person's devices, nodes, services and applications. These may reside anywhere in the wireless bubble around the user defined as the Private PAN (P-PAN) in IST project MAGNET [1] and in Personal Clusters (such as the home, car and office Cluster). Figure 1 depicts the concept with the P-PAN gaining access to an office Cluster via interconnecting structures. The focus of this paper is on the networking of the devices in the PN through the establishment of dynamic Virtual Personal overlay Networks (VPON) [2]. To address networking in the PN, the paper covers naming, addressing and routing in addition to tunneling. The analysis considers scalability, flexibility, complexity for users and providers, and security to compare a number of tunneling, addressing and routing alternatives for PN networking. An overview of the Personal Overlay Network Framework, which covers tunneling, naming, addressing and routing, is given in section 2. Further, in personal networks, the concept of a PN Agent, responsible for maintaining up-to-date information about the PN constituents and their point of attachment, will be introduced to enable and ease PN networking and management. This concept, together with details on its integration in the naming system is presented in section 3. Section 4 is devoted to Virtual Personal Overlay Network (VPON) deployment and provides details on how the various frameworks interact and exchange information to achieve PN networking. Finally, conclusions are made in the last section of the article.

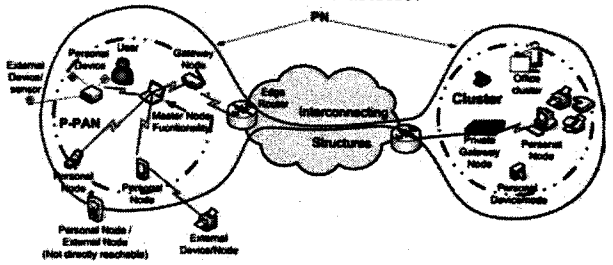

Fig. 1 . Personal Network Concept

II. Personal Overlay Network Framework

The user of the PN desires access to remote services from anywhere, at anytime, and using any device in a secure and private manner. Even tough there could be several alternatives to achieve connectivity using interconnecting structures or ad hoc networking, the paper focuses on the establishment of dynamic tunneling between Clusters of a personal network. Due to the mobility and roaming of the Cluster of devices around the user (called the P-PAN), the merging and splitting of Clusters and the dynamic changes expected in personal networks, supporting connectivity requires a powerful tunnel establishment system. Efficient and low latency deployment and management of virtual overlay networks would considerably ease the support of PNs and the creation of value added PN services by the users themselves or any third party. Assuming that a trust relationship can be established between users and providers, the deployment and management of the virtual overlays can be outsourced to a Service Provider (SP). In order to gain easy access to devices in remote Clusters, the user can make use of names instead of addresses and rely on naming systems to resolve the names. A typical user has no knowledge of any technical networking aspect and is not expected to deal with IP addresses at all. A well known naming system is the DNS that resolves access point domain names which are used in the URL descriptions. Other naming systems that are more expressive and more extensible are also suitable for PN networks [3]. This paper assumes that users

[1]This work was partially funded by IST Integrated Project MAGNET.
Wajdi Louati {Wajdi.louati@int-evry.fr}, Wassef Louati, Djamal Zeghlache, are with Institut National des Télécommunications, France. Jeroen Hoebeke is Research Assistant of the Fund for Scientific Research - Flanders), Gerry Holderbeke and Ingrid Moerman from Ghent University-IMEC-IBBT, Dept. of Information Technology, Belgium. Mikko Alutoin and Kimmo Ahola are with Technical Research Centre of Finland (VTT), Finland.

and PN architectures will rely on names and network overlays to achieve dynamic PN interconnection. When PN users rely on a SP for networking, the provider management system shall interact with the naming system, which resolves names into addresses of personal nodes and devices, in order to establish tunnels as depicted in Figure 2.

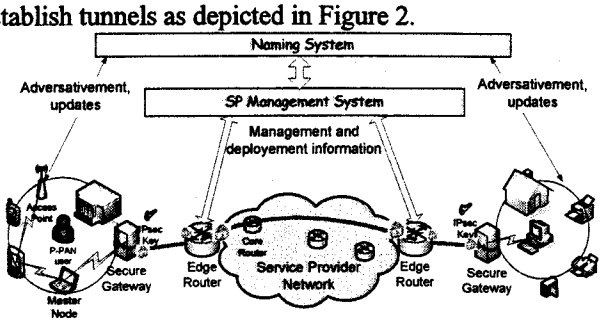

Fig. 2. Overlay Network Framework for PN

Personal Networks can also benefit from ad hoc networking paradigms. Personal Networks, like ad hoc networks, require self-organizing and self-maintaining networking capabilities that can deal with their dynamic behavior. Therefore, the PN networking solutions can build on ad hoc networking techniques and concepts. For instance, ad hoc routing protocols and distributed addressing schemes with duplicate address detection can be deployed for providing network connectivity in this dynamic network environment. However, the specific Personal Network context with its overlay architecture, will allow much more efficient and intelligent solutions than those currently proposed for traditional ad hoc networks.

The next subsections of this paper address dynamic overlay network deployment, naming, routing and addressing involved in personal overlay networks.

A. Virtual Personal Overlay Network

Recently, a new term called « Virtual Personal Overlay Network » (VPON) is introduced in [2] to designate virtual personal network communications between Clusters. A VPON is a set of tunnels that determines a virtual overlay of Personal Clusters on top of physical Interconnecting Structures (e.g. the Internet). The VPON nodes are the edge nodes that trigger and maintain the endpoints of the tunnels forming the overlay network. These nodes can be the user edge nodes or SP edge routers. When the Service Provider establishes the tunnels, the SP Management System controls, configures, deploys and manages the overlay network via these VPON nodes.

1) Tunneling mechanism

In the VPON context, tunneling performs three major tasks: encapsulation, transparent private addressing, data integrity and confidentiality protection. For tunneling, several protocols are available. The main IP tunneling protocols that could be used for VPONs are IPSec [4], IP-in-IP [5] and GRE [6]. IPSec tunneling has a number of strong points. IPSec is the only VPON technology to support security and data encryption in the cases where a VPON is established across non-secure networks. In this document, the IPSec tunneling technology will be used as an inter-Cluster communications within personal networks.

2) Secure Cluster Gateway

In the context of personal networks, the P-PAN and Clusters could be potentially composed of devices and nodes with low processing power and limited battery power. Implementing secure tunneling mechanisms into these nodes and devices can become inefficient. PN users would be confronted to inconvenient battery lifetime, a nuisance, considerably reduced for hand held devices and terminals over the years, PN users would not tolerate. Encryption, encapsulation and decapsulation are operations that require a lot of processing power. Hence, it would make more sense to have a user edge node (or a secure Cluster Gateway) within each Cluster provide secure connectivity on behalf of the PN nodes. In each PN Cluster, gateways could be used to partake in the establishment of tunnels and overlay networks. In this case, they need to implement IPSec. The Cluster nodes behind the gateways do not have to be IPSec capable, they simply take advantage of IPSec tunneling services offered by the gateways.

3) Network based remote access VPON

Recently two major approaches are defined within the Provider Provisioned (PP) based VPN scope [7]. The PP User Edge based VPON (or the secure Cluster Gateway based VPN in the PN context) and the PP provider router based VPON (or Network based VPON). In both solutions the tunnels are deployed and managed by the SP. The main difference between these two solutions is where the tunnel endpoints reside. In the User Edge based solution, the VPON service is provisioned in the Cluster Gateway equipment whereas in the second approach, the VPON service is provisioned in the provider edge router. Due to the scalability limitation and the high management complexity faced by the SP in the user edge based solution, the Network based solution seems the appropriate model to overcome the scalability and complex management limitations. Indeed, the provider routers can provide powerful processing and plenty of capacity to establish several tunnels at the same time. This will prove particular valuable for PN to PN communications when PN federation is used to extend the personal network concept to group communications. Secure tunnels are deployed between the provider edge routers to ensure private and secure connectivity across the SP backbone. However, the main drawback of the network based solution is that the access link between the user edge and the SP backbone is not secure. The Cluster nodes can, however, establish a remote access to the VPON via a secure tunnel across the access Network (e.g. IPsec or SSL/TLS based remote access). A Secure Provider Gateway located in the SP edge network terminates the remote access tunnels from Clusters. This Provider Gateway is responsible for authentication, authorization and access to the VPON. This results in concatenated tunnels deployed between Secure Cluster Gateways and provider edge routers. This solution called Provider Provisioned Network based remote access VPON [2] will be used for PN networking to provide secure and private connectivity between remote Clusters as depicted in Figure 3.

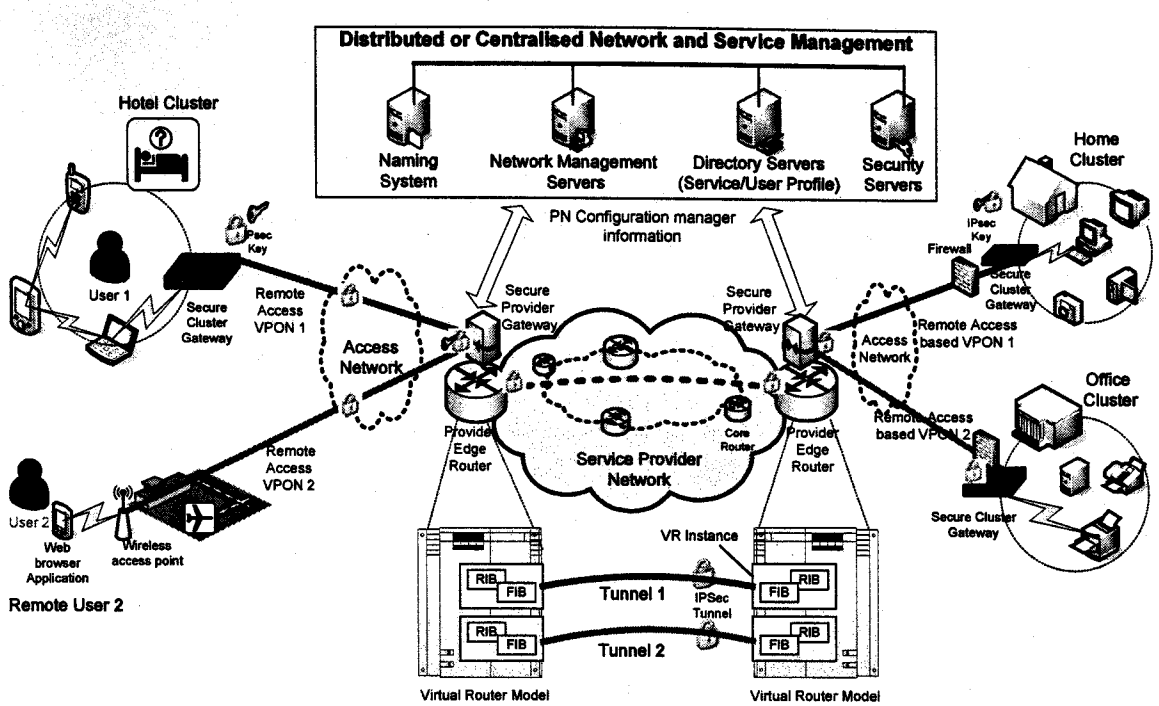

Fig. 3. Network Based Virtual Personal Overlay Network

This solution reduces configuration and management complexity, provides VPONs in a flexible and scalable manner and eases the introduction of value added services.

In order to separate traffic flows coming from different PNs, the Virtual Router (VR) concept is advocated for the provider edge router [8]. A Virtual Router is an emulation of a physical router in the software layer which handles VPON Networking. Many instances of VRs may be running on a single physical router with each VR having independent routing (Routing Information Base) and forwarding (Forwarding Information Base) tables isolated from each other Figure 3). This solution provides per VPON routing, addressing, QoS and service management capabilities for Personal Networks. This approach enables isolation of traffic flows between VPONs sharing the same edge router. Once the VPON user is connected to the SP network via a remote access conducted by the Secure Provider Gateway, the Service Provider Management ties the Cluster identity with the appropriate Virtual Router Instance dedicated to the specific VPON.

A. PN Addressing

A Personal Network is a virtual overlay network. This overlay, although it is established on top of existing Interconnecting Structures such as the Internet, should be able to operate as a stand-alone network, shielded from the outside world. To this end, Personal Networks should have their own IP address space (the PN address space), separated from the Internet address space. This means that a Personal Node will be visible in two address spaces: the PN address space and the Internet address space. Internet addresses are used for communication with existing Internet services and Internet hosts. The PN address is used for intra-PN communication, and in the future also for PN-to-PN communication. These PN addresses will act as local addresses that are not visible in the Internet address space, as they are only used for direct communication between Personal Nodes or being encapsulated when sent over existing Interconnecting Structures. The above discussion brings on the following requirements for the PN addressing scheme:

-- Local addresses separated from the Internet address space.

-- Non-overlapping address spaces for different Personal Networks in order to allow PN-to-PN communication.

-- Large address space in order to accommodate all Personal Nodes

Based on the above requirements we have chosen to use IPv6 addresses having the following format [9]:

TABLE I. PN IPV6 ADDRESSING SCHEME

7 bits	1 bit	40 bits	80 bits	
			16 bits	64 bits
Fc00::/7	L	PN prefix	Subnet ID	Interface ID

The specific use of the field is as follows (Table 1):

-- Prefix fc00::/7: the prefix denotes that the PN addresses are site-local addresses rather than globally routable IPv6 addresses

-- L = 1: the setting of the L bit denotes that the PN prefix is locally assigned

-- PN prefix: each Personal Network will use its own PN prefix.

With the above addressing scheme, 80 bits are still left for further assignment of addresses to the individual nodes within the PN. Two possible solutions exist, namely subnet-based addressing and flat addressing. With subnet-based addressing, each Cluster of the PN will have its own subnet ID (16 bit)

and all Personal Nodes within the same Cluster will share this common ID. This addressing scheme has the advantage that the address of the Personal Node reveals its location (in terms of the Cluster the node resides in) within the PN, information that can be efficiently used for route aggregation by the PN routing protocols. However, a major drawback of this scheme is that each time Clusters merge or split, the addresses of the involved nodes change with the obvious implications on the routing protocols and the ongoing communication sessions. As splitting and merging of Clusters is an operation that will occur frequently (e.g. home Cluster splits in P-PAN and home Cluster, P-PAN merges into office Cluster), this addressing scheme is not the most efficient solution. To this end, we propose a flat addressing scheme, in which all nodes within the same PN only share the common PN prefix. The only drawback of this addressing scheme is that now the address does not reveal any information on the location of the node within the PN. However, this drawback can be solved efficiently by deploying efficient naming schemes, using ad hoc routing techniques and exploiting the context and architecture (e.g. Edge Nodes) of the PN, as will be discussed in the following sections. In addition, a flat addressing scheme results in a much lower overhead in the address assignment and maintenance, as addresses do not need to be changed during Cluster merge (or split).

1) PN address auto-configuration

Once a node has been granted access into the PN through an imprinting or another secure procedure [10], it is configured with a valid PN address. The nodes are capable of generating globally unique Interface ID's by mapping their MAC address to a 64 bit IEEE EUI-64 identifier [11]. This ensures global uniqueness of each PN address. In addition, the newly added personal node receives the first 64 bits of its PN address from an existing PN node in order to construct a full IPv6 address.

B. PN Naming

Besides addresses, PN users can use names to communicate with their personal devices. The work reported here is based on the INS (Intentional Naming System) [3], a naming, resource discovery and service locating system. INS uses intentional names as service descriptions and a hierarchical arrangement of attribute-value pairs to provide flexible description of an object intent or service. The INS architecture is mainly composed of INS Applications and an Intentional Naming Resolver (INR) network. An INR is an entity that maintains the mapping between intentional names and their locations (mainly their IP addresses) in the network. This mapping is stored in a data structure called a name-tree. The INRs self-configure into an application-level distributed overlay network (Figure 4). Any node in the PN or in the interconnecting structure can potentially act as an INR.

INS Applications, which may be services or clients, interact with the INRs. A service advertises its name to an INR. The INRs exchange the name descriptions (intentional names and their addresses) so that they can be accessed from any resolver. A client can consequently discover from an INR the existing names in the network. A client can also ask an INR, in an early binding operation, to resolve an intentional name to its IP address, behaving in this case like the Domain Name System (DNS).

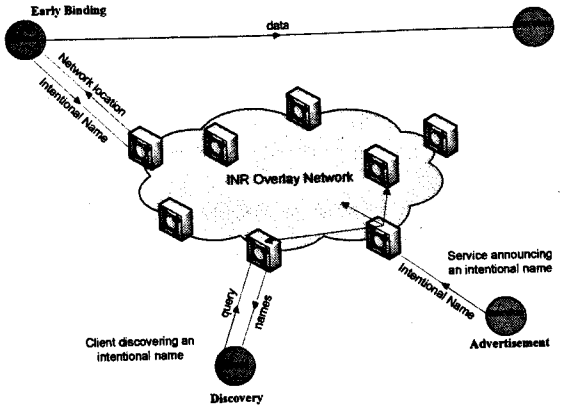

Fig. 4. INS Architecture

With INS, PN node names can be composed of different attributes describing the node and its location such as the PN and the Cluster identifier attributes. These location attributes can be assigned by a third party entity to guarantee uniqueness of names and descriptions. For example, the PN identifier can be given by a central PN server (or a PN Agent) and the Cluster identifier can be given by a Cluster Gateway. A PN node name could be: [device=camera] [service=transmitter] [Cluster=office] [PN=personX].

Attribute-based naming (INS like) and subnet-based addressing have similar philosophy since both have a hierarchical structure providing information on the location of a Personal Node within the PN. The naming system can provide the missing location information to the flat addressing approach. Using naming over subnet addressing provides redundant location information without resolving any of the merging and splitting challenges encountered in subnet addressing.

Naming systems are used to provide permanent identifiers and can thereby assist Cluster and node mobility. This requires only an update of the mapping between the node or Cluster name and its associated address. This update takes place naturally and proactively in naming systems by the nodes and Clusters themselves. The naming system will be used also to implement the PN Agent needed for the personal network framework.

C. PN routing

A PN can be seen as one ad hoc network of Personal Nodes, in which proactive or reactive ad hoc routing techniques can be deployed in order to establish paths between communicating nodes. However, existing solutions for mobile ad hoc networks cannot be adopted as is, due to the specific nature of Personal Networks. First of all, a PN has a specific architecture, consisting of geographically dispersed Clusters that form a virtual overlay network. Protocols can take advantage of this architecture in order to reduce overhead, latency and energy consumption and improve

scalability. In addition, each PN Cluster can be seen as a small ad hoc network with some specific characteristics dependent on the type of the Cluster:

TABLE 2. CLUSTER CHARACTERISTICS

Roaming P-PAN	Static Clusters (home or office Cluster)
▪ small-size network ▪ slowly changing composition ▪ low internal mobility ▪ mainly wireless, battery powered devices ▪ dynamics: P-PAN changing its point of attachment to the Interconnecting Structure, P-PAN merge (and split) with Cluster, e.g., car Cluster and home Cluster	▪ medium-size network ▪ mainly static devices ▪ lot of devices connected to power supply ▪ both wireless and wired interfaces ▪ dynamics: Cluster merges (and splits) with the P-PAN

Again, the deployed routing protocol can be adapted in order to take into account this network context, creating more efficient solutions than feasible within traditional ad hoc networks.

Secondly, the choice of the routing protocol strongly depends on the chosen addressing scheme. Combinations of proactive and reactive routing with both flat and subnet-based addressing are possible, but do not always result in an optimal solution.

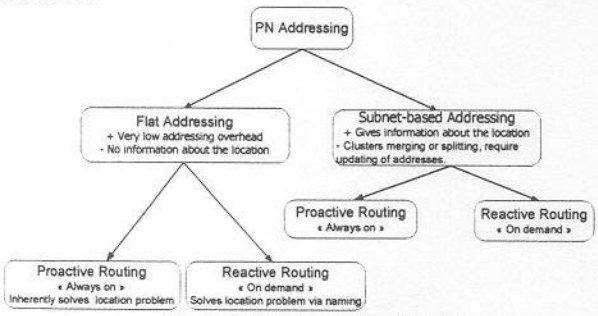

Fig. 5. Addressing and Routing diagram

For instance, combining proactive routing with subnet-based addressing is not an interesting solution, as proactive routing with flat addressing achieves the same performance without the overhead of subnet-based addressing. Figure 5 provides an overview of all possible combinations. In section 4, we will discuss both a proactive and reactive solution based on the preferred flat addressing scheme.

III. PN AGENT CONCEPT

To establish tunnels between Clusters one needs to be capable of locating the Clusters. To provide this location information and assist PN management, the concept of a PN Agent is introduced [1]. The Agent can be either a centralized or a distributed functionality maintaining up to date information about the PN constituents and their points of attachment. The PN is a repository holding information mostly about the PN Clusters and especially the P-PAN. The agent partakes in PN establishment, maintenance and management by interacting with the naming system, addressing and routing, VPN management, mobility management and the security framework. The PN Agent interacts with providers and edge routers that support PN services to achieve PN networking according to the dynamic changes in the Clusters and the P-PAN.

In this paper the PN Agent maintains a table of registered Clusters and the IP addresses of the edge routers that are serving as their ingress and egress tunnel endpoints. Since INS is a distributed locating system capable of maintaining information about nodes, Clusters names and locations, it has been selected to incorporate also as the PN Agent functionality. This results in distributed PN Agent within the INR overlay network.

A. PN Agent integration in the INS naming system

The edge routers, irrespective of their location and the business model at hand, can offer a number of services to the PN Clusters. They can actually implement a naming service such as an INS Application (Figure 6). When a Cluster connects to an edge router, the gateway passes its Cluster name composed of the Cluster identifier and the PN identifier (e.g. [PN=personX][Cluster=car]) to the selected INR (which could be implemented in the edge routers). The incoming Cluster name is concatenated with the location information of the edge router (e.g. edge router's Internet address) into a Cluster name record (e.g. [PN=personX] [Cluster=car] + @IP_ER4). The name record is advertised to the INR network (Cluster registration) for future PN name resolutions. The naming system stores and maintains in the INRs the Cluster name records and this forms actually the PN Agent within the naming system. The INR overlay network exchanges the name records so that PN Agent can be accessed from any INR. At the time of Cluster registration, the Cluster nodes announce their names to the naming system.

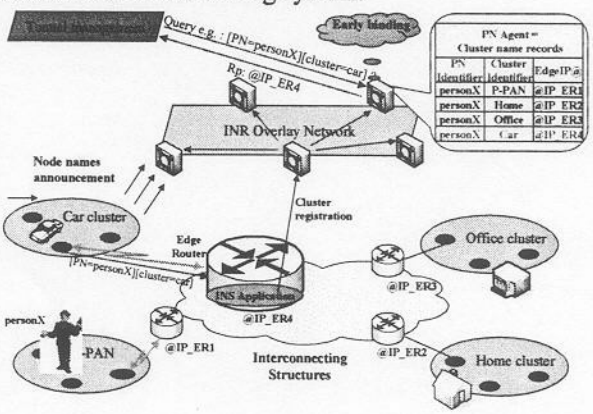

Fig. 6. PN Agent concept based on naming

IV. PERSONAL OVERLAY NETWORK DEPLOYMENT

This section presents different scenarios and architectures to deploy a Virtual Personal Overlay network. Two main solutions are defined: Proactive based VPON and Reactive based VPON. For both solutions, the flat addressing is adopted as addressing scheme. Each scenario is described according to interactions between the dynamic tunneling, the addressing, the routing and the naming system.

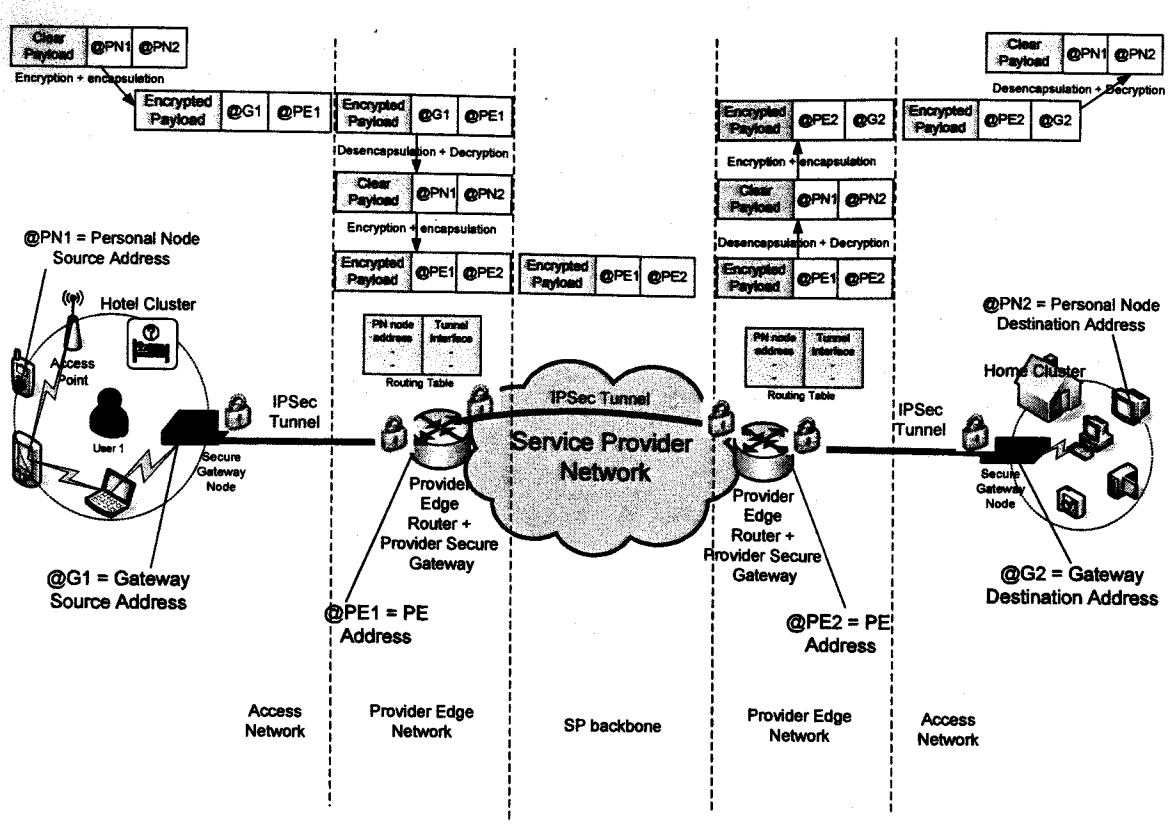

Fig. 7. Concatenated IPsec tunnels mode

There are two cases that can be encountered for roaming P-PANs, either the visited networks are trusted (or a trust can be established with securely discovered edge routers), or such trust can not be established. The trusted Service Provider case is addressed first and details on VPON deployment are provided. The untrusted case will be described at the end of the paper, since the mechanisms are fairly similar to the trusted case, only the differences and the general structure of the end to end tunnel establishment will be emphasized.

A. Trusted Service Provider - secure gateway based networking

In this case, the PN user trusts the Service Provider to deploy and manage the Virtual Personal Overlay Network. In order to reach the SP Network in a secure manner, each Cluster establishes a secure IPsec tunnel from its secure Gateway to the provider Secure Provider Gateway. The Provider Gateway, which can be integrated in the Provider Edge (PE), is responsible for terminating the tunnels and authenticating and authorizing the roaming P-PAN to access the VPON.

Figure 7 depicts a PN node "pn1" that wants to connect to a remote PN node "pn2". The secure Cluster Gateway "G1" encrypts the original packet sent from "pn1" and encapsulates it in a new header. These G1 constructed packets are sent to the Secure Provider Gateway. In order to facilitate the scenario, the Secure Provider Gateway address is the same as the Provider Edge Router address (@PE1) since both are combined. Therefore, the outer addresses of the packets carried by the tunnel are the source address of the Cluster Gateway (@G1) and the destination address of the Secure Provider Gateway (@PE1). The provider edge router PE1 decapsulates and decrypts (via the integrated secure gateway) the packet to retrieve the original PN nodes addresses (@pn1, @pn2) to route the packets. A packet classifier within PE1 should distribute each packet belonging to the same VPON to the appropriate Virtual Router instance according to the PN prefix field in the destination address (@pn). The routing table of the VR maintains the PN node addresses and the tunnels interfaces deployed across the SP backbone. The trusted Service Provider can see the original PN data payload in clear.

In order to provide secure data transport across the SP backbone, another IPsec tunnel is needed between the PEs involved in the VPON. As shown in Figure 7, "PE1" encrypts, encapsulates and sends packets to "PE2" that will perform the same tasks as edge router "PE1". Finally, the packets are sent to the secure destination Gateway "G2" that decapsulates and decrypts them to extract the original packet sent by personal node "pn1". These extracted packets are sent to node "pn2" by Gateway "G2".

1) Proactive based Personal Overlay Network Deployment

This section presents the VPON deployment using proactive PN routing with flat addressing. When a Cluster Gateway connects to the Provider Edge Router via a secure remote access, the following actions take place:

1. The Cluster Gateway registers itself with the PN Agent (see section III.A). For example, in Figure 8, the user 1

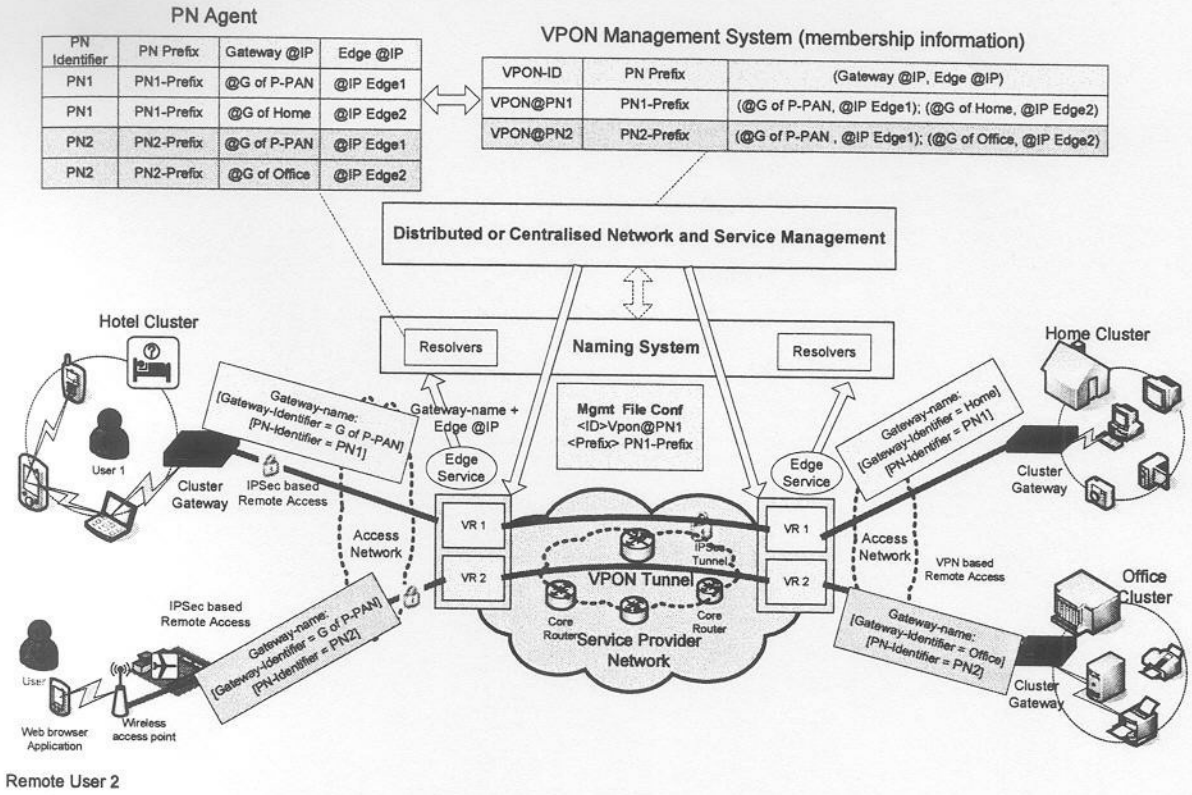

Fig. 8. Proactive based Personal Overlay Network Deployment

Gateway passes its Cluster name ([PN=PN1] [Cluster=Hotel]) to the provider edge router after discovery of (and establishment of trust with) this router. The provider edge router concatenates its IP address with the Cluster name and transmits the resulted name record to the PN Agent.

2. The PN Agent interacts with the VPON management system to achieve the VPON membership information and define the VPON-ID [12] needed for the VPON creation and establishment. The VPON membership information determines which Edge Routers and PN Clusters are members of a specific VPON. Therefore, the VPON membership table includes entries composed of the PN identifier (the *PN Prefix* in this case) and a vector containing the Cluster identifier along with its serving edge IP address. Each entry is identified by a unique VPON-ID which specifies the VPON membership information. A pair of Virtual Routers associated to the VPON-ID will be created in the Edge Routers.
3. The management network installs then the Virtual Router instances in the Edges relying on the PN Prefix.
4. The Cluster Edge Node sends a routing update containing the list of Cluster Nodes to the created VR instance. This table acts as a proactive routing table for that specific VPON.
5. A VPON membership information update is sent to the Provider Edge Router, informing about the registration of other Clusters belonging to the same VPON. This can occur only if the VR instances have already been created.
6. The Virtual Routers, associated to the VPON, can now establish dynamic tunnels across the SP backbone to connect the Clusters.
7. Upon establishment of tunnels, the involved Virtual Routers will exchange the contents of their proactive routing tables. A per-VR routing protocol instantiations (e.g. using the BGP protocol) can be used to distribute the VPON topology and reachability information.

The end result of the above procedure is an "always on" Virtual Personal Overlay Network between all Clusters of the PN. In addition each Edge Router will know already for each Personal Node, the Cluster where the node is located. Upon changes in the Cluster composition or location, the Edge Routers will update and exchange PN routing information. Therefore, this approach assumes that the Edge Routers actively establish and maintain tunnels between all Clusters of the PN, based on a tight coupling with the PN Agent.

The only overhead for the Clusters consists of executing the proactive intra-Cluster routing protocol. All other overhead is handed over to the Edge Routers and the PN Agent. As the proactive routing in combination with the dynamic tunnel establishment & maintenance instantaneously keeps track of Cluster dynamics and Cluster movements, mobility and session continuity is supported with this approach.

When the Provider Edge Router receives incoming traffic from different VPONs, a packet classifier should distribute each PN packet to the appropriate Virtual Router instance according to the PN prefix field defined above.

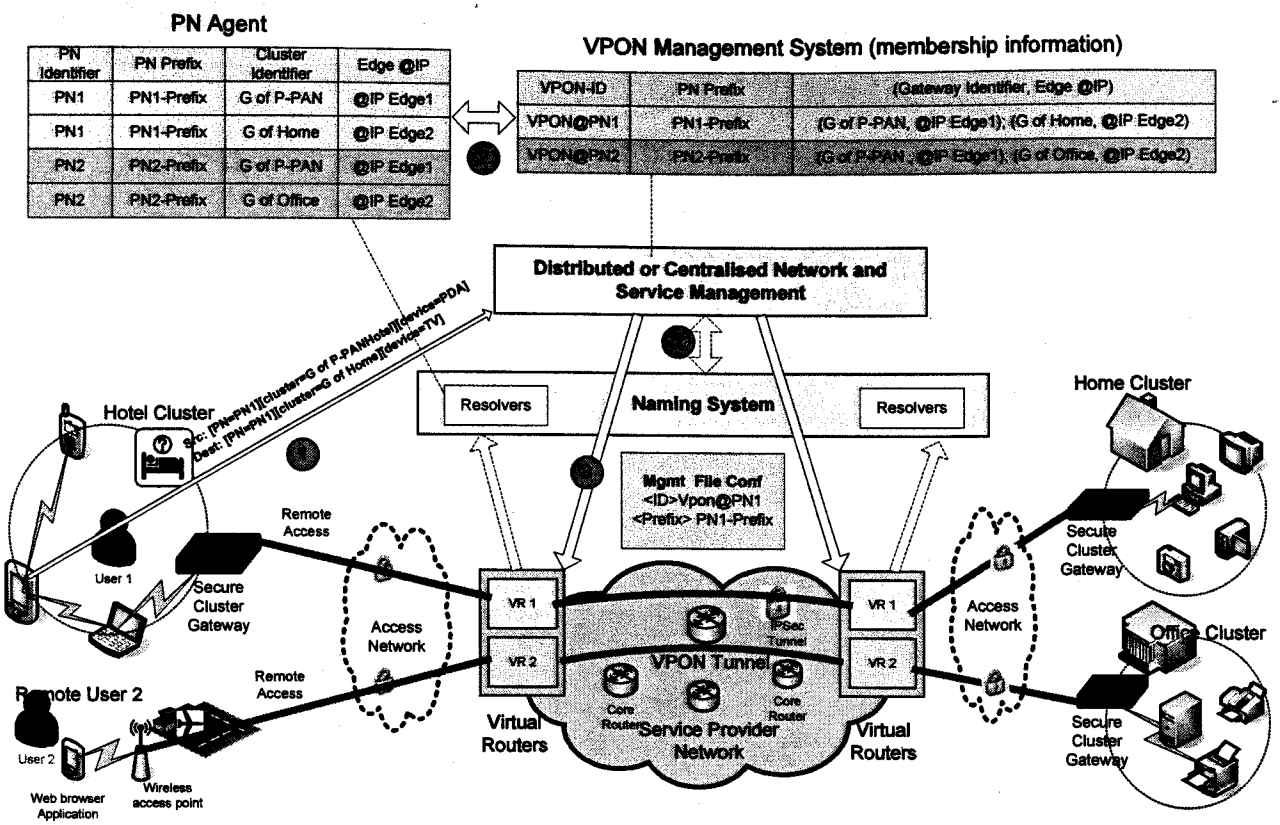

Fig. 9. Reactive based Personal Overlay Network Deployment

1) Reactive Personal Overlay Network Deployment

This section presents the VPON deployment using reactive inter-PN routing with the flat addressing and naming approach. Each node name includes the Cluster name (e.g. [device=PDA][Cluster=Gateway of P-PAN][PN=PN1]). Thus, the node intentional name embeds the cluster location of the node through the Cluster name.

1. When two nodes from different Clusters want to communicate through a VPON, the source node sends a first management packet to the management plane including the source and destination node names (Figure 9).
2. The VPON management examines those names and deduces the edge routers where the correspondent Clusters are attached by asking the PN Agent using early binding.
3. The management uses the membership table to determine the Cluster Gateway and its corresponding physical Provider Edge router (PE). If the Virtual Router is not already installed, then the management will create a new instance. The management system sends the tunnel endpoints parameters via a management protocol to the appropriate Provider Edge routers. The PN Prefix is used to identify the tunnel interface in the VR routing table.

The end result of the above procedure is an "on demand" Virtual Personal Overlay Network between the Clusters of the PN. The tunnel is triggered by the source node when the need arises. This mechanism can handle Cluster mobility. When a Cluster moves, it passes its name to the new edge router which will announce this name to the naming system. This way, the mapping between the Cluster name and its serving edge router IP address will be updated. Following this update, the VR instances will be updated and relocated for the on going session.

B. Networking via untrusted visited Service Providers

When trust can not be established with provider edge routers, a number of situations can be encountered by the roaming P-PAN or Clusters. Depending upon context, a given approach may have to be adopted to circumvent the absence of trust. The paper reports a number of possible solutions based on the nodes in the end to end path that the PN constituents do trust so that networking can be achieved in a secure way in the PN. A mix of methods relying on IPSec tunneling modes are presented for scenarios based on where the first PN services support resides between the PN end nodes. The objective is to analyze each scenario and conduct a comparison on the basis of scalability, flexibility for Service Providers to offer value added services to the PN and complexity. The considered scenarios, depicted in Figure 10 that provides details on tunneling mechanisms, correspond to:

- A hybrid approach combining PE and Gateway based VPON deployment. In this case, an IPSec Tunnel mode is established between the secure Cluster Gateways. This scenario assumes that offered services can be trusted but the user does not want to send PN data in clear nor reveal

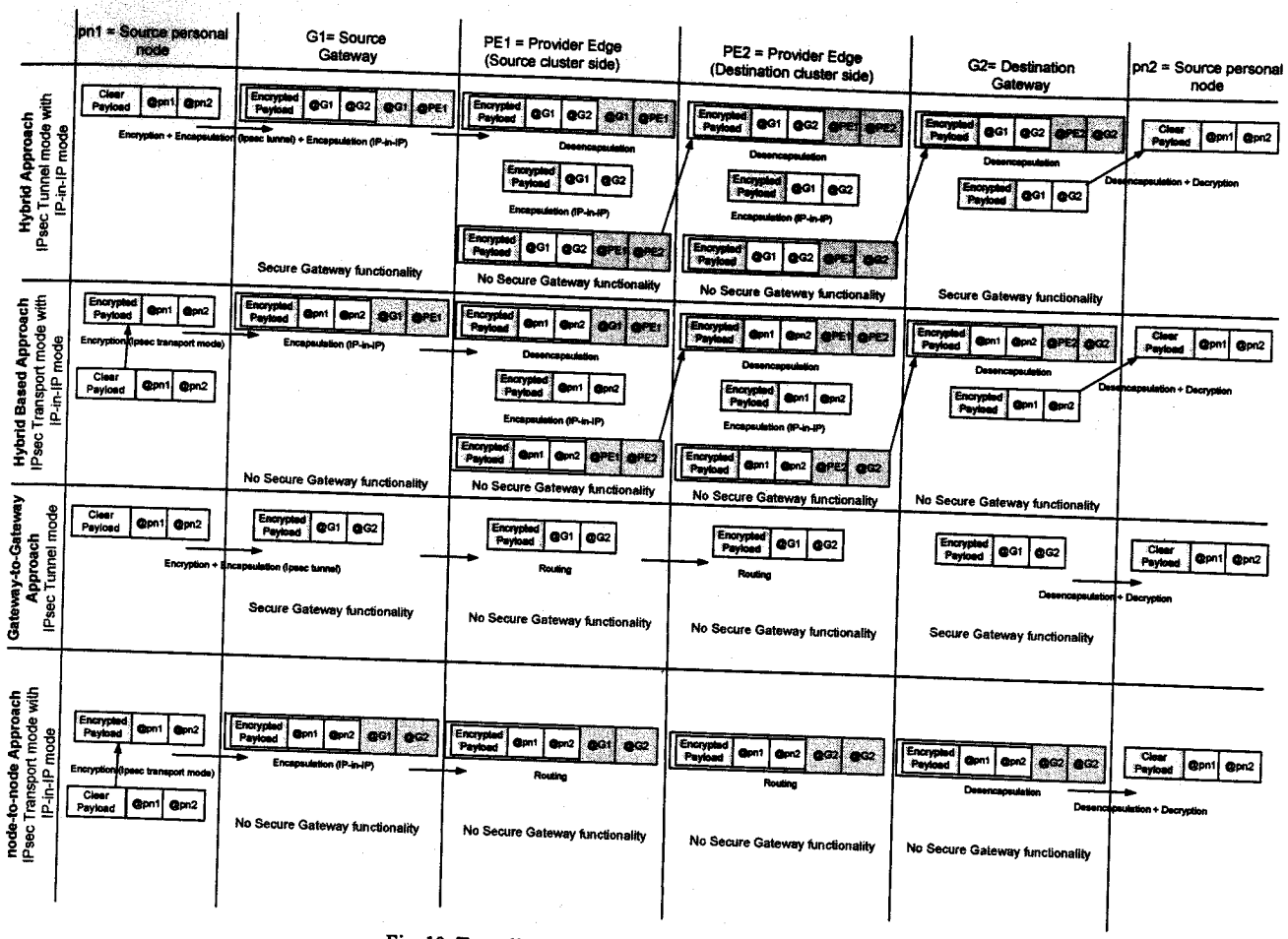

Fig. 10. Tunneling modes in the untrusted visited SP case

its internal addressing. The network provider can see the appropriate headers to provide QoS and traffic management. The objective of the IP in IP tunnel between the secure Gateway (G1) and the provider edge (PE1) is to be able to reach the SP. The provider is responsible for VPON deployment in the interconnecting structures and connectivity with the PN Agent and management.

- A second hybrid approach based on nodes rather than Cluster Gateways. An IPSec transport mode is used between the end nodes, also encrypting the data, but leaving the internal addresses visible.
- A gateway to gateway approach using IPSec tunnels between Cluster Gateways. The SP is passive and only provides bearers for data transport in a transparent mode.
- The fourth scenario relies on PN nodes to achieve end to end connectivity. All intermediate nodes act transparently and have no access to any packet payload data.

V. Conclusion

A number of viable networking architectures for Personal Networks (PN) are presented in this paper. Their strengths and weaknesses are discussed from the viewpoints of scalability, complexity, security, performance, robustness, and maintenance. When designing a PN architecture, choices need to be made on addressing, naming, routing and mobility management. In this paper, the PN architecture is based on the Virtual Personal Overlay Network (VPON) concept where a number of Clusters are interconnected using dynamic tunneling and where the nodes within the PN share a private IPv6 address space. The Network based remote access approach is presented in this paper as a VPON solution to achieve secure and private communication between Clusters. This solution relies on the Service Provider that is responsible for deploying and maintaining tunnels between provider edge nodes. This method reduces management complexity and improves scalability as only one tunnel needs to be established from each Cluster to the SP. A trust relationship must be in place between the PN users and the Service Providers so they can manipulate and manage PN traffic and thereby offer PN services support to the users.

A number of conclusions can be drawn concerning routing and addressing. Flat addressing can be used with either proactive or reactive routing for PN networking. Flat addressing is not sensitive to Cluster merging and splitting in the PN. Subnet based addressing on the other hand requires address updates during these events. Even if subnet based addressing facilitates route aggregation it causes problems during Cluster mobility, merging and splitting.

Flat addressing can benefit from location information

provided by naming systems when it is combined with reactive routing. Flat addressing and proactive routing also seem to be a good match despite the important overheads and scalability issues due to frequent updates of routing tables in the overlays. The proactive approaches appear also as adequate for intra PN networking and communications. For inter PN interactions involving collaborating PN users and PNs, the reactive paradigm may be more appropriate. In federation of PNs over overlay networks, networking will be mostly on demand and an always on mode of operation will not necessarily be needed.

There are multiple options to orchestrate the VPON depending upon the division of functionality between the PN and the network or Service Providers. Due to the limited resources of the user's handheld devices, it would be beneficial for the user to outsource some of the PN functionality to the provider nodes or network entities. The selected scenario and solution depends upon trust establishment, business models that are in place and the organization of the value chain. This paper explores a number of solutions assuming trusted and not trusted network and SPs and describes a number of viable PN architectures where operators could support Personal Network Services. The selection of a solution depends essentially on the preferences of the users and providers and their agreements. This paper makes no assumption on business models and agreements between actors. It does, however analyze the PN architecture from a technical standpoint to pinpoint areas where additional effort is needed to foster personal services. The objective is to identify to what extent providers and users can open their networks (via open programmable frameworks) to support PN services and offer value added services to PN users.

REFERENCES

[1] MAGNET Project, "My personal Adaptive Global NET", http://www.telecom.ece.ntua.gr/magnet/test2/ objectives.html

[2] W. Louati, D. Zeghlache, "Network based Virtual Personal Overlay Networks using Programmable Virtual Routers", *IEEE Communications Magazine*, to be published by August 2005.

[3] W. Adjie-Winoto, et.al, "The design and implementation of an intentional naming system", Proc. 17th ACM SOSP, Dec. 1999

[4] IP Security Protocol charter, http://www.ietf.org/ html.charters/ipsec-charter.html

[5] W. Simpson. IP in IP Tunnelling. RFC 1853, 10/95.

[6] Farinacci, D., et.al, "Generic Routing Encapsulation", RFC 2784, March 2000.

[7] Carugi, M. and De Clercq, J. "Virtual private network services: scenarios, requirements and architectural constructs from a standardization perspective", *IEEE Communications Magazine*, vol. 42, no. 6, June 2004, pp. 116-122;

[8] P. Knight, et.al, , "Network based IP VPN Architecture using Virtual Routers", http://www.ietf.org/internet-drafts/draft-ietf-l3vpn-vpn-vr-02.txt (work in progress), April 2004.

[9] Hinden, R, Haberman, B, "Unique Local IPv6 Unicast Addresses", http://www.ietf.org/internet-drafts/draft-ietf-ipv6-unique-local-addr-09.txt (work in progress), Jan 2005.

[10] IST-507102 MAGNET : Conceptual secure PN architecture, December 2004.

[11] Hinder, R, Deering, S, "Internet Protocol Version 6 Addressing Architecture", http://www.ietf.org/rfc/ rfc3513.txt , April 2003.

[12] B. Fox, B. Gleeson, "Virtual Private Networks Identifier", RFC 2685, September 1999

ASWN 2005

Applications and Services in Wireless Networks

Editors
Hossam Afifi
Djamal Zeghlache

ASWN 2005 Workshop Proceedings

Collection INT

IEEE

5th Workshop on Applications and Services in Wireless Networks
June 29th - July 1st, 2005
Paris, France

IEEE COMMUNICATIONS SOCIETY

ASWN 2005

5th Workshop on Applications and Services in Wireless Networks

June 29th - July 1st, 2005

ASWN 2005 is the fifth workshop on Applications and Services in Wireless Networks. The workshop addresses the challenges and advances in future wireless applications and services that span all wireless architectures and technologies, such as cellular, WLAN, WPAN, ad hoc, and sensor networks. The format of the workshop is based on three-day single-track sessions, with presentations of invited and regular papers from academia and industry. This year's special theme is the impact of newly emerging technologies, such as personal networks, sensor networks and P2P on wireless applications and services. The workshop addresses also, through a Panel, the impact of these disruptive technologies including nanotechnologies, on the organization of the value chain in wireless services and on the information society.

9 782915 618082

ISBN 2-9156-18-08-9
Price : 50 euros

INSTITUT NATIONAL DES TÉLÉCOMMUNICATIONS
9, rue Charles Fourier - 91011 EVRY Cedex - FRANCE
téléphone : +33 (0)1 60 76 40 40
télécopie : +33 (0)1 60 76 43 25
www.int-evry.fr

This volume contains papers presented at the fifth workshop on Applications and Services in Wireless Networks (ASWN 2005).

Editors: Djamal Zeghlache and Hossam Afifi
Wireless Networks and Multimedia Services Department
Institut National Des Télécommunications
9, rue Charles Fourrier
91011 Evry Cedex France

ISBN: 2-9156-18-08-9

Printed by the Institut National des Télécommunications
9, rue Charles Fourrier
91011 Evry
France