WIRELESS WORLD
RESEARCH FORUM

# Autoconfiguration and Self-management of Personal Area Networks: a New Framework

Rui Campos[1, 2] and Manuel Ricardo[1, 2]

[1]School of Engineering of the University of Porto (FEUP), Portugal
[2]Institute for Systems and Computer Engineering of Porto (INESC Porto), Portugal
Rua Dr. Roberto Frias, 378
4200-465 Porto, Portugal
e-mail: {rcampos, mricardo}@inescporto.pt

***Abstract*— In the Beyond 3G vision, users will carry multiple devices forming cooperative networks, known as Personal Area Networks. Some of the existing technologies enable this type of networks, such as Bluetooth or IEEE 802.15.4, but a unified framework capable of self-organizing and deploying them dynamically still has to be defined. These networks are also envisioned to be connecting dynamically to the Internet, and may use two IP versions and their corresponding autoconfiguration mechanisms.**

**In this paper we present a new framework, named Autoconfiguration and Self-management of Personal Area Networks (ASPAN) which enables the automatic and dynamic deployment of Personal Area Networks in the heterogeneous personal environments envisioned for the next generation networks.**

***Index Terms*— Dynamic autoconfiguration, Personal Area Networks, Self-organization, Self-management.**

## 1 Introduction

FUTURE communication networks, also known as Beyond 3G (B3G) networks, will be characterized by a movement towards ubiquitous communication. This includes an increasing range of wireless and wired technologies, multihomed devices, and mobility within and of networks, in addition to the mobility of the end users. In this new communication scenario, user intervention should be minimized and technology should seamlessly adapt to user's needs; communication networks should be plug and play and adapt dynamically and automatically to different networks contexts, while the user is moving around. Moreover, the integration of electronic devices with computing capabilities within clothes, walls, or even in the human body will enable the creation of new computation environments and bring up new communication models, where these devices form cooperative networks, such as Body Area Networks (BANs) and Personal Area Networks (PANs). On the other hand, it has become consensual within the networking community that the Internet Protocol (IP) will be the base protocol for B3G networks. The Internet will play a central role, supporting all type of multimedia data and services, from classical ones, such as web browsing, e-mail, and video streaming, to more QoS demanding services, such as Voice-over-IP (VoIP) or video conferencing. The Internet will be the base network to which all networks and devices need to be connected, and through which they acquire global connectivity.

Today, small incipient cooperative networks such as Bluetooth [1] PANs can be created. However, they still require manual configurations and networking expertise. Bluetooth does not provide any mechanism to adapt automatically to scenarios where, for instance, a PAN is changing its point of attachment to the Internet dynamically. On the other hand, future IP networks may be characterized by heterogeneity; different protocol suites operating simultaneously (IPv4, IPv6), and multiple addressing schemes (private IPv4, public IPv4, and IPv6) can be used. In addition, new autoconfiguration frameworks will be required for scenarios where an entire network connects to the Internet. In this context, enabling the automatic and dynamic creation of PANs and dealing with the dynamics associated with future communication scenarios poses new requirements to the future mobile communication systems in terms of autoconfiguration and self-management.

Intensive research on this field is being carried out. Some ongoing European projects [2,3,4,5,6] and multiple discussion forums, such as the Wireless World Research Forum (WWRF) [7], discuss and address these topics, and point out solutions; other solutions, concerning Personal Area Networking, are also proposed in [8,9]. However, to the best of our knowledge no solution solves the problem stated in this paper. Our proposed framework addresses this problem and is expected to be installed in the everyday life devices carried by end-users, such as laptops, Personal Digital Assistants (PDAs), and mobile phones. Our framework, named Autoconfiguration and Self-management of Personal Area Networks (ASPAN), enables the deployment and self-organization of PANs from the networking point of view, and addresses the connection of the self-created PAN to external networks, namely to the Internet, dynamically and automatically.

The rest of the paper is organized as follows. In Section 2 we describe the state of the art concerning autoconfiguration in IP networks and Personal Area Networking. Section 3 describes the problem and Section 4 details the ASPAN framework. Section 5 presents the related work and, finally, Section 6 draws the conclusions.

# 2 State of the Art

The state of the art is characterized from two perspectives: autoconfiguration in IP networks and Personal Area Networking.

## 2.1 Autoconfiguration in IP Networks

Autoconfiguration mechanisms for IP networks can be classified in two categories: stateful and stateless autoconfiguration.

### 2.1.1 Stateful Autoconfiguration

**DHCP**. Dynamic Host Configuration Protocol (DHCP) [10] provides a framework for passing configuration information to hosts, using a client/server model. It is based on the exchange of four signalling messages. The client broadcasts a *DHCPDISCOVER* message in order to discover available servers; it may receive one or more *DHCPOFFER* messages and, after selecting one of the servers, it broadcasts a *DHCPREQUEST* containing the identification of the selected server. Finally, the server replies with a *DHCPACK* message containing the assigned address and optional information. With the advent of IPv6 a new DHCP version (DHCPv6) [11] came up, considering a different operation model: 1) a well-known multicast address is used by clients to address all the servers in the link, instead of broadcasts; 2) unlike DHCPv4, which is used to perform the whole host configuration, DHCPv6 can be used to just complement the stateless mechanism; 3) the messages defined for DHCPv6 are different in name and format. In real implementations, DHCPv4 and DHCPv6 are used independently for dual-stack hosts. Possible solutions to integrate the two frameworks are specified in [12].

**PPP/IPCP**. Point-to-Point Protocol (PPP) [13] is used as the standard transport framework for multiple network layer protocols over serial links. Typically it is used by a host connected to an Internet Service Provider (ISP). In conjunction with other two components – a method for encapsulating multi-protocol datagrams, and a Link Control Protocol (LCP) for establishing the data-link connection – PPP defines a family of Network Control Protocols enabling autoconfiguration of different network layer protocols. The Internet Protocol Control Protocol (IPCP) [14] is defined to configure IP over PPP, namely to autoconfigure IPv4 addresses; extensions allowing configuration of optional information are specified in [15]. The protocol is based on the exchange of two messages, *Configuration-Request* and *Configuration-Ack*, and it may involve more than one negotiation round if a peer does not accept the configurations requested by the other. After IPv6 came up, the IPv6CP was defined [16]. IPv6CP specifies the same two configuration messages, and provides the means for the negotiation of an interface ID used to configure the link-local address at the local end of the link; autoconfiguration of a global address and optional information can be performed by using IPv6 stateless autoconfiguration (see below) and DHCPv6.

**Packet Data Protocol (PDP) Context**. Cellular networks can interwork with IP networks through a node called Gateway GPRS Support Node (GGSN). GGSN is responsible for delivering the required configuration parameters to a Mobile Station (MS) upon PDP context Activation [17]; before this, the MS shall perform a GPRS Attach [17] to a so-called Serving GPRS Support Node (SGSN) placed between the MS and GGSN; the messages *Attach Request*, *Attach Accept*, and *Attach Complete* are exchanged. The PDP context Activation involves the three entities; the MS interacts with the SGSN which, in turn, interacts with the GGSN. The MS sends the *Activate PDP Context Request*, indicating the PDP type (e.g., IPv4, IPv6) and requesting an address and optional information; the SGSN contacts the GGSN in order to activate the PDP context, and the MS receives the *Activate PDP Context Accept*. The information carried in this message depends on the PDP type. In IPv4, it contains the assigned address and optional information, whereas in IPv6 it provides an interface ID used by the MS to configure a link-local address; IPv6 stateless autoconfiguration and DHCPv6 can be used to configure the global address and optional information.

### 2.1.2 Stateless Autoconfiguration

**Dynamic Configuration of IPv4 Link-Local Addresses**. The Dynamic Autoconfiguration of IPv4 Link-Local Addresses was deployed by the IETF Zeroconf Work Group [18], and is now available as an IETF RFC [19]. Multiple operating systems, such as Windows XP and Linux, implement it as an alternative to DHCP. In this solution a host can automatically configure an IPv4 address within the 169.254/16 prefix, which can be used for communicating with other devices in the same link. First, the host generates a random IP address using the 169.254/16 prefix. Next, it performs duplicate address detection using an Address Resolution Protocol (ARP) probe, in order to assess if the address is already in use; if a reply is received, it must consider that the address is being used by other terminal and must try a new address. Finally, the host assigns the IP address to the local network interface, and link local connectivity becomes possible.

**IPv6 Stateless Autoconfiguration**. This solution, specified in [20], defines the steps carried out by a host to autoconfigure its network interfaces in IPv6, without using a centralized service. The autoconfiguration process comprises the generation of a link-local and a global address, and a Duplicate Address Detection procedure, in order to verify the uniqueness of the autoconfigured addresses on a given link. The autoconfiguration of a link-local address is performed upon network interface activation, and after combining the well-known prefix FE80::0/10 with the interface identifier (ID), based on the MAC address; configuration of a global address is accomplished by combining the prefix announced by a local router, using the Router Advertisement messages defined in [21], with the interface ID. In addition, Router Advertisements contain two flags, M and O, informing the host whether DHCPv6 server should be contacted to acquire addresses and/or to obtain optional information.

**Stateless DHCP for IPv6**. The stateless DHCPv6 service [22] is intended to be used by nodes that have already configured an IPv6 address, through the IPv6 stateless autoconfiguration mechanism or manually, but need to acquire optional information such as the addresses of DNS or SIP servers. This solution is a lightweight version of the stateful DHCPv6, specifying a subset of the protocol messages and avoiding state information maintenance for each individual client. It is well suited to be deployed in networking scenarios where IPv6 autoconfiguration is based on the stateless approach. In order to obtain the optional information, a client sends an *Information-Request* message towards a well-known multicast address, and receives a *Reply* from the server containing the required information.

## 2.2 Wireless Personal Area Networks

Bluetooth [1] has become the de-facto standard for enabling Personal Area Networks. It defines a set of profiles aimed at being used for different applications, such as transfer of a stereo audio stream, control of TVs and Hi-fi equipment, file transfer, and serial cable emulation providing a simple wireless replacement for existing RS-232 based serial communications applications. However, the relevant profile from Personal Area Networking viewpoint is the so-called PAN profile. This profile enables easy creation of Bluetooth-based PANs by providing Ethernet emulation over Bluetooth. In this sense, deploying IP over Bluetooth becomes easy too, and un-modified Ethernet payloads can be transmitted between Bluetooth devices using the Bluetooth Network Encapsulation Protocol (BNEP); this feature also enables the bridging between Bluetooth and Ethernet networks.

The PAN profile defines the formation of a PAN in the following situations: (1) ad-hoc IP networking by two or more Bluetooth devices in a single piconet[1]; (2) external network access for one or more Bluetooth devices. Each Bluetooth device may implement one of the following services: PAN User (PANU), Gateway Node (GN), or Network Access Point (NAP). The profile specifies three scenarios: Network Access Points, Group Ad-hoc Networks, and PAN User to PAN User. In the first scenario there is a node deploying the NAP service which is able to provide access to some external network, such as Ethernet or cellular network; this device acts as a bridge or router between the Bluetooth PAN and the external network; the other devices connect to it as PANUs. In the second scenario, Group Ad-hoc Networks, devices cooperate to create a stand-alone PAN; one of the devices acts as the master and implements the GN service; the other devices are slaves and connected to the master as PANUs. The third scenario provides a point-to-point connection between two PANUs and enables direct communication between them only; this scenario is equivalent of connecting two devices using an Ethernet cross-over cable.

The PAN profile specifies IP as its major internetworking protocol. Apart from the Bluetooth features, the specification [1] provides the Request For Comments (RFCs), the address assignment, and the name resolution techniques required to enable IP over Bluetooth. The address assignment for IPv4 is based on the Dynamic Configuration of IPv4 link-local addresses mechanism described in Section 2.1.2; for IPv6, the mechanisms also defined in Section 2.1.2 must be supported.

Bluetooth also specifies the Service Discovery Protocol (SDP) which enables the automatic discovery and advertisement of the services each Bluetooth device can offer to the other devices on the same link. For instance, by using this protocol, a PANU device can search for devices in the neighbourhood offering the NAP service in order to gain access to the Internet.

In the scope of the Institute of Electrical and Electronic Engineers (IEEE), the IEEE 802.15 Working Group for WPAN [23] is developing standards for Personal Area Networks or short distance wireless networks. These WPANs address wireless networking of portable and mobile computing devices such as laptops, PDAs, peripherals and mobile phones at the data link layer (layer 2 of the OSI model). This work group has been partitioned in Task Groups (TG) which deal with specific sub-areas within the Personal Area Networking area. The IEEE 802.15.1 Task Group (TG1) has reviewed and provided a standard adaptation of the Bluetooth Specification version 1.1 for the Medium Access Control (MAC) and physical layers. The IEEE 802.15.3 (TG3) has provided a standard for high-rate (20Mbit/s or greater) WPANs, whereas the IEEE 802.15.4 (TG4) is chartered to investigate a low data rate solution with multi-month to multi-year battery life and very low complexity, whose potential applications are sensors, interactive toys, smart badges, remote controls, and home automation.

# 3 Problem Statement

The current communication paradigm from end-user perspective is almost based on stand-alone terminals. The traditional scenario is to have end-users carrying more than one device with networking capabilities, that are, however, loosely or not cooperating with each other on behalf of the user. For instance, the user utilizes her mobile phone to make phone calls and send SMSs, the PDA as an electronic agenda, and the Laptop as the major device to perform heavy and demanding work, such as writing documents, making presentations, and surf the web. However, in spite of this traditional scenario, the creation of incipient PANs is currently possible, namely by using Bluetooth; in fact, it is becoming frequent for a user to utilize her mobile phone as a mean to provide Internet access to her laptop, for example. This kind of networks represents the embryo for the PANs of the future.

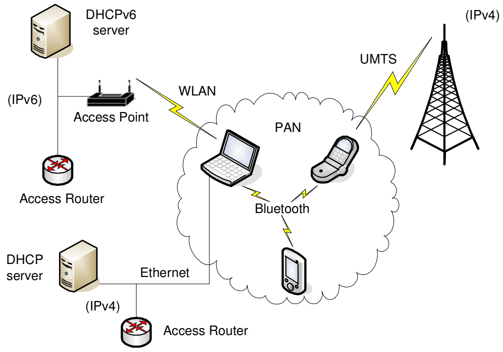

Fig. 1. Example Scenario for Beyond 3G networks from end-user perspective.

[1] A piconet consists of one Bluetooth device operating as a piconet master communicating with up to 7 active Bluetooth devices operating as slaves.

Fig. 1 illustrates the envisioned networking scenario for B3G networks from the end-user perspective, where multiple terminals around the user form a PAN; this network should be able to self-organize according to dynamic network contexts and user needs, so that the involvement of the user is limited to the definition of the policies governing the connection of the PAN to the access networks providing global connectivity. A major assumption for next generation networks is that they will be IP-based. In this context, the Internet will play a central role. It will be the base network to which all networks and devices need to be connected, and through which they acquire global network connectivity. Then, the user's PAN shall be able to dynamically and automatically connect to the Internet taking into account the available wireless interfaces within the PAN, the access networks in the neighbourhood granting access to the Internet, the IP version and autoconfiguration mechanisms supported by such networks, and the policies defined by the end-user. The scenario in Fig. 1 shows a user's PAN connecting to various access networks (points of attachment) along the time. For example, at a given moment in time, the PAN is connected through UMTS to have Internet access, but later on it may decide to switch from that connection to the WLAN access, because it offers better performance and lower cost. This requires the dynamic and automatic adaptation of the PAN to the changes in the surrounding environment.

The transition from a terminal-based to a network-based communication paradigm poses new requirements that are not addressed by legacy technologies. The solutions currently deployed and being investigated for IP networks are mostly terminal-based. For instance, the autoconfiguration mechanisms defined for IP networks and described in Section 2.1, basically assume that the entity being autoconfigured is a stand-alone device. Besides, the heterogeneity found in IP networks, where two IP version and corresponding autoconfiguration coexist brings up the efficiency problems and new research topics, when it comes up to the autoconfiguration of entire networks, that we have illustrated in [24]. As shown in Fig. 1, the different access networks a PAN may connect to may support different IP versions and autoconfiguration mechanisms that influence the way the PAN is configured internally. For example, when changing from the UMTS connection to the WLAN connection reconfigurations are required, namely concerning the IP addresses assigned to the Bluetooth interfaces, the autoconfiguration mechanism to be used to acquire the proper IP addresses and optional information, as well as the configuration of the devices themselves; the mobile phone does not need to act as an IPv4 router anymore and the laptop needs to be configured as an IPv6 router in order to provide Internet access to the PAN. A detailed analysis of the required reconfigurations, when the PAN changes its point of attachment while moving around is provided in [24].

On the other hand, in spite of the advances in Personal Area Networking area, namely provided by the Bluetooth technology, deploying PANs in the way above-mentioned is still impossible. The different technologies described in Section 2.2, standardized in the context of the IEEE 802.15 work group, target Personal Area Networking scenarios, but are limited when it comes to the full dynamic and automatic connection of PANs to the global Internet, since they only address the MAC and physical layers. Rather than being considered as stand-alone solutions for WPANs, in the context of B3G networks, these solutions must be assumed as part of an overall framework addressing B3G scenarios. Such new IP-based solution must integrate these wireless technologies into a single framework, and must select the most suitable technology according to the network context and user needs, as we have defined before.

The deployment of a Bluetooth PAN by using the PAN profile described in Section 2.2 is not a full automatic process. It involves some user intervention, namely in the configuration of the roles played by each device forming the PAN; in addition, when deploying IP over it further configurations may be required. For instance, let's assume the scenario in Fig. 1. Suppose that the mobile phone can offer Internet access through the UMTS network to the laptop and PDA, which belong to the same user. In order to enable this scenario the mobile phone has to be manually configured as a Bluetooth NAP by the user, and as a bridge or IP router between the PAN, formed by the three devices, and the UMTS network, so that the PAN is able to get global connectivity. Subsequently, the user has to configure the laptop and the PDA as PANUs that search for the NAP service offered by the mobile phone by using the Bluetooth SDP protocol; for the sake of simplicity, we assume that the mobile phone is the only device in the neighbourhood offering the NAP service; if  this is not the case, the Bluetooth built-in security mechanisms can be used to enable mutual authentication of devices and avoid situations where either the PANU connecting to the NAP is unauthorized, or the NAP is a rogue device.

If we consider that a PAN is static, i.e., the point of attachment is always the same every time devices come together to create the ad-hoc network, a set of pre-configurations may be created in order to render the configuration process automatic, after the first time. However, when the PAN moves around, the point of attachment and the device offering global connectivity may change. Therefore, multiple reconfigurations may be required in order to dynamically adapt to new network contexts. Concerning the scenario in Fig.1, when the PAN switches from the UMTS access to the WLAN access, reconfiguration of the roles of the Bluetooth devices is required, apart from the reconfigurations we have mentioned above. Currently, this has also to be performed manually and may involved network expertise. Additionally, as scenarios become more and more dynamic, doing such reconfigurations becomes a difficult and cumbersome task; the scenario becomes even worst to be deployed manually if two IP versions are considered.

# 4 ASPAN Framework

In order to cope with the dynamics and self-management requirements imposed by future communication networks, we propose a new framework, named Autoconfiguration and Self-management of Personal Area Networks (ASPAN). ASPAN aims at being used in heterogeneous communication environments where two IP versions (IPv4 and IPv6) and the corresponding autoconfiguration mechanisms coexist; in addition, it targets the Personal Area Networking scenario. This new framework deploys four main mechanisms regarding self-management and autoconfiguration for a PAN:

1. Mechanism for negotiating automatically the proper IP version and autoconfiguration framework to be used within a PAN, regarding the characteristics of the devices forming the network and the current point of attachment, in scenarios where the PAN is connected to the outside;

2. Mechanism for automatic and dynamic selection of the best point of attachment of the PAN, based on user-defined policies and network context;

3. Mechanism for configuring automatically and dynamically the PAN's devices, according to the negotiations and selection performed by the mechanisms defined in 1 and

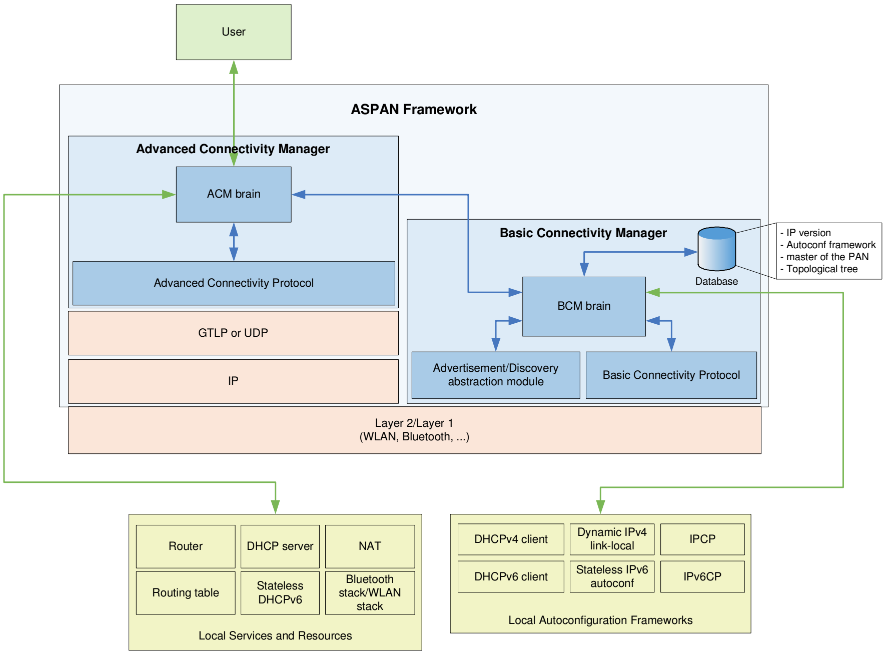

Fig. 2. Architectural Model of the ASPAN Framework.

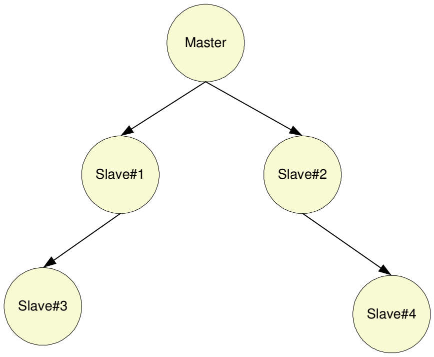

Fig. 3. Topological tree maintained by the BCM.

2, e.g., configuration of a PAN device as a Network Address Translator (NAT);

4. Mechanism for dealing with joining and leaving of PAN devices, including multi-hop scenarios.

## 4.1 Architectural Model

Fig. 2 illustrates the architectural model of the ASPAN framework. It comprises the Basic Connectivity Manager (BCM) and the Advanced Connectivity Manager (ACM). The BCM runs over Layer 2 protocols since it acts before IP connectivity is configured. BCM interacts with the local autoconfiguration frameworks and selects the mechanism negotiated a priori with the peer BCM(s) by using the Basic Connectivity Protocol (BCP); it also has to interact with the local IP stacks (IPv4, IPv6) in order to enable/disable the proper protocol stack according to the IP version negotiated with the peer BCMs. The BCM interacts with the ACM in order to, for example, inform the latter that basic connectivity is established, pass information about the IP version and autoconfiguration mechanism used to establish the basic connectivity, and start the basic connectivity establishment. The ACM, apart from interacting with the BCM, interacts with local services and resources, as shown in Fig. 2. ACM performs the required local configurations according to the services it gets from and offers to the other PAN devices, and taking into account the policies defined by the user, which may specify for example the preferable point of attachment. The announcement of services by a device is performed using the Advanced Connectivity Protocol (ACP) between ACMs. The ACP protocol can run either over the GANS Transport Layer Protocol (GTLP) or directly over UDP. GTLP is specified in the Ambient Networks project [2,3] and it is aimed at transporting signalling information between Ambient Networks; it is an extension of the General Internet Signalling Protocol (GIST) specified in [25]. GTLP supports names and single-hop non-path related signalling, besides IP addresses and multi-hop signalling along a data path supported by default by GIST. If running over GTLP, ACP can use the services offered by this protocol, which include reliability and security.

## 4.2 Advertisement and Discovery

Advertisement and discovery in ASPAN is based on legacy mechanisms, such as WLAN and Bluetooth. For that reason, we define an Advertisement/Discovery abstraction module, inside the BCM, which abstracts the details of each layer 2 technology. Regarding security, namely the authentication of the discovered PAN devices, a pre-shared key mechanism is used. The shared key is derived automatically from the ID specified by the user (see below) to identify the PAN and by applying an hashing algorithm, such SHA-1 [26], or the algorithm defined in [27].

## 4.3 Master-Slave Model

In the ASPAN framework, a master-slave model is assumed. When devices come together to form a PAN one of them is elected as the master of the network using an election algorithm. Afterwards, the master device is in charge of managing the connectivity aspects of the PAN, namely the detection of the potential points of attachment and detection of new devices willing to enter the PAN; for that purpose it receives notifications from the other devices within the PAN – the slaves. The master device stores locally a topological tree where it stands as the root, as shown in Fig. 3; the topological tree is stored within the database shown in Fig. 2 inside the BCM. This enables the detection of new devices connecting to the PAN, as well as of devices leaving the network, namely in multi-hop scenarios, where devices are connected through multiple physical links. Furthermore, this enables the ASPAN to inform the user about the set of terminals currently participating in the PAN and the way they are organized; dissemination of this information to the other devices of the PAN can be performed on-demand, i.e., every time a slave requests it explicitly.

## 4.4 Joining Mechanism

When a user's device is joining the PAN, it firstly discovers the device(s) of the PAN in the neighbourhood by using the proper layer 2 mechanisms. There may be more than one PAN device connected to the same link, as illustrated in Fig. 1. However, the joining device contacts only the master of the PAN. Thereby, after detecting the presence of one or more devices, the joining device broadcasts a BCP JOIN message requesting to join the PAN, and the master device replies to this; the other devices ignore the request. After getting a reply from the master, the joining device learns about the IP version and autoconfiguration framework to use. Every time the master detects a new device, it waits for a request. Otherwise, if it does not receive such request, it ignores the detected device, simply because either it does not support ASPAN framework or it is not interested in joining the PAN. After the new node joins the PAN, the master updates the topological tree and the joining node notifies the master, by using the ACP protocol, about the network accesses it can provide to the PAN.

## 4.5 Leaving Mechanism

The leaving mechanism uses the topological tree shown in Fig. 3. When the PAN is composed by devices connected to the same link, things become simple, because all the devices are aware of the others' presence. When we consider multi-hop, where devices are connected through multiple physical links, the topological tree of Fig. 3 is needed. Every device connected to the PAN regularly scans its link. When it detects that some partner in that link has left the PAN, it notifies the master, which knows the PAN topology. Using that information, the master updates the topology accordingly. If the leaving node is the master device, a new master is elected between the remaining devices and either the topological tree stored within the old master is transferred to the new master or it is created from the scratch at the new elected master by some mechanism to be defined.

## 4.6 User Intervention

ASPAN assumes the following, regarding the end-user intervention:

- The user has to identify explicitly each device belonging to the PAN; this identification is carried out by assigning them the same PAN ID;
- The user has to specify the policies governing the attachment of the PAN to the multiple points of attachment it is able to connect to while moving around.

# 5 Related Work

Several proposals address the problems above-mentioned. In the following we present some of them. However, to the best of our knowledge there is no proposal coping with the whole problem; some target the deployment of ad-hoc networks, while others address the connection of moving networks to the Internet.

**Mobile Ad-hoc Networks (MANETs)**. MANETs represent a framework providing communication in multi-hop scenarios. In this solution, each device acts as a router and runs some routing protocol to maintain connectivity with the other devices belonging to the same MANET. In fact, the MANET solution could be used to implement the example scenario of Fig. 1; each terminal could act as a router and run some routing protocol and autoconfiguration framework. Nonetheless, in order to get global connectivity either through IPv4 or IPv6, routing protocols [28] and MANET autoconfiguration mechanisms [29] for both IP versions should be run. The major shortcoming of this approach is efficiency, since routing and autoconfiguration protocols would be running for both IP versions regardless the current IP version available. Besides, each device must act as a router what may represent another disadvantage, namely in devices with limited battery lifetime, due to the additional battery consumption. On the other hand, in the base MANET framework, there is no mechanism capable of selecting the most appropriate gateway towards the global Internet taking into account the user requirements. Some routing protocols have been extended to support gateway discovery, but the selection process depends on the default gateway configuration. In order to overcome this limitation new mechanisms are proposed in [30,31] dealing with multi-homed ad-hoc networks, i.e., networks providing multiple connectivity options to the Internet. However, the IP heterogeneity characterizing the current Internet is still not addressed, and efficiency problems are still present.

**AN Case Study**. Considering a scenario similar to Fig. 1, in [32] a solution enabling automatic and dynamic creation of a PAN and selection of the proper access network is provided. The solution is based on the Ambient Network (AN) and Network Composition concepts being studied in the IST Ambient Networks project [2,3]. This solution considers IPv6 and does not cope with the heterogeneity coming up with coexistence of IPv4 and IPv6; therefore, it just solves part of the problem.

**TurfNet**. The TurfNet solution [33] represents a new network paradigm enabling the integrated operation of networks with different address realms (e.g., IPv4, IPv6), thanks to the so-called TurfNet gateways. In this context, a TurfNet is defined as an autonomous network domain, encompassing its own address space and associated control plane functions (e.g., routing, address allocation, name-to-address resolution) integrated into the TurfControl. This solution enables the merging of multiple TurfNets into a single TurfNet and the simple interoperation between TurfNets.

TurfNet could be used to implement the scenario shown in Fig. 1; each network in the scenario – the PAN and the various access networks – could be considered as TurfNets comprising a TurfNet gateway to enable their interoperation. Nevertheless, the node implementing the TurfNet gateway inside the PAN has to change according to the PAN movement and, currently, the TurfNet framework does not support this feature.

**Network Mobility (NEMO)**. The IETF NEMO WG is chartered to specify a mobility management framework for entire networks. The base NEMO specification is provided in [34]. It extends Mobile IPv6 to support mobile networks, where a Mobile Router performs mobility management for the entire network. The drawback of this solution is the support of IPv6-only networks; in a realistic scenario, it seems crucial to consider both IP versions. The solution proposed in [35] extends NEMO for supporting IPv4; however, it assumes that the IP infrastructure has to be IPv6, which seems a bit unrealistic. Therefore, at least some automatic IPv6-over-IPv4 tunnelling needs to be provided, in order to connect transparently the Mobile Router of the mobile network to the IPv6 infrastructure. This solution demands support from the infrastructure in order to terminate the IPv6-over-IPv4 tunnel; this is something not specified in [35]. There is a further solution [36] defined in the NEMO context, which addresses the cooperation of multiple MRs in a mobile network connected to the Internet; this solution proposes a new protocol, the Mobile Router Cooperation Protocol (MRCP), used between MRs, in order to address multihomed mobile networks. The protocol enables MRs to share link quality information, so that the best connection to the Internet is selected. Nevertheless, the same shortcoming identified before is also present here: only IPv6 is supported, according to the base NEMO specification. Furthermore, nothing is said about MR automatic discovery, which reveals to be very important in dynamic scenarios such as Fig. 1, where devices may dynamically join and leave the mobile network.

**IST MAGNET project**. The MAGNET project [5,6], addresses user-centricity, personalization and personal networking. The project supports the concept of Personal Networks (PNs) as an extension to the classical PANs. The PAN around the user is extended with clusters of remote devices belonging to the same user. In order to implement this paradigm a Distributed Personal Network Agent Management Framework is defined, which must be supported by the network infrastructure. The establishment of dynamic secure tunnels between remote devices of the PN across the Internet can, in this way, be supported. This framework specifies IPv6 as the enabling technology. When compared to our solution, this proposal presents two major drawbacks. Firstly, it requires modifications to the network infrastructure, in order to deploy the Distributed PN Agent; secondly, it considers IPv6 to support the PN environment, ignoring the heterogeneities also found in IP networks.

**Virtual Device on PAN**. In [8] is proposed the notion of “virtual” device over a PAN. This solution defines the PAN middleware that abstracts the user and applications from the specific devices forming the PAN, and copes with the dynamics of the movement and presence of different type of devices. The solution uses a classical distributed systems approach, where the main goal is to render the distributed system fully transparent to the user and applications; thus, when running over the PAN middleware, applications think they are running over a classical device. By defining the ASPAN framework, we aim at a similar goal, but follow a different approach; we do not hide the devices connected to the PAN and define a network-oriented approach instead. An important advantage of the PAN middleware is the possibility of sharing resources other than network access, such as processing power, battery power, and memory. However, the major disadvantage is the fact that applications must be modified if they want to benefit from the new features provided by this framework. In the ASPAN framework, since the data plane is unmodified legacy applications can still run without any modification. In addition, the virtual PAN solution overlooks networking aspects we are addressing, namely the IP heterogeneity and dynamic reconfiguration of devices according to the network context; IP is just taken for granted and the focus is mostly on rendering the distributed system transparent to the user.

**Personal Mobile Hub**. In [9], the concept of Personal Mobile Hub (PMH) is defined to support inter-device communication within a PAN as well as Internet access for the PAN. The PMH represents the central point through which the other devices of the PAN connect to each other. Also, the PMH acts as a mobile internet router, i.e., it acts as a proxy for the other devices connected to it, such as laptops, PDAs, medical sensors, and so forth; in [9] the authors report the hardware and software implementation of a customized PMH, whose major function is to allow cellular phone connectivity to a PAN over Bluetooth. Although the scenarios considered as basis by this solution match with the scenarios considered for B3G networks, its major drawback has to do with the static configuration of the device playing the PMH role, in contrast to what is envisioned to happen in future networks, where the device acting as proxy to the Internet will change dynamically according to the network context.

# 6 Conclusion

In this paper we proposed a new framework, the Autoconfiguration and Self-management of Personal Area Networks (ASPAN), which is envisioned to be used in B3G networking environments. These environments are expected to support two IP versions, the corresponding autoconfiguration mechanisms, multiple enabling wireless technologies, and self-management of devices/networks. The proposed solution enables the automatic and dynamic autoconfiguration of a Personal Area Network, and enables the selection of the best point of attachment according to the network context and user-defined policies.

The design and specification of the ASPAN framework is currently being finalized. The next step of our work is the development of a prototype for the proof-of-concept.

## Acknowledgment

The authors would like to thank the support of the Portuguese Foundation for Science and Technology (FCT) under the fellowship SFRH/BD/19429/2004/.

## References

[1] D. Sönnerstam et al., *Specification of the Bluetooth System* (version 1.2), November 2003.

[2] Norbert Niebert et al., *Ambient Networks: an Architecture for Communication Networks Beyond 3G,* IEEE Wireless Communications Magazine, vol.11, pp.14-22, April 2004.

[3] IST Ambient Networks Project, http://www.ambient-networks.org.

[4] IST Daidalos Project http://www.ist-daidalos.org.

[5] IST MAGNET Project http://www.ist-magnet.org.

[6] Mikko Alutoin et al., *Towards Self-organising Personal Networks*, in Proceedings of the 1st International ACM Workshop on Dynamic Interconnection of Networks (DIN'05), September 2005.

[7] Wireless World Research Forum (WWRF) http://www.wireless-world-research.org.

[8] Tore E. et al., *Building a Virtual Device on Personal Area Network*, in Proceedings of the 11th IEEE International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2003), October 2003.

[9] Dirk Husemann et al., *Personal Mobile Hub*, in Proceedings of the 8th International Symposium on Wearable Computers (ISWC'04), November 2004.

[10] R. Droms, *Dynamic Host Configuration Protocol*, RFC 2131, 1997.

[11] R. Droms, et al., *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, RFC 3315, July 2003.

[12] T. Chown, et al., *DHCP: IPv4 and IPv6 Dual-Stack Issues*, Internet Draft, draft-ietf-dhc-dual-stack-04 (work in progress), October 2005.

[13] W. Simpson, Ed., *The Point-to-Point Protocol (PPP)*, RFC 1661, July 1994.

[14] G. McGregor, *The PPP Internet Protocol Control Protocol (IPCP)*, RFC 1332, May 1992.

[15] S. Cobb, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*, RFC 1877, December 1995.

[16] D. Haskin, et al., *IP Version 6 over PPP*, RFC 2472, December 1998.

[17] 3GPP TS 23.060, *General Packet Radio Service (GPRS) Service description Stage 2*, v6.10.0, September 2005.

[18] IETF Zeroconf WG, http://www.zeroconf.org.

[19] S. Cheshire, et al., *Dynamic Configuration of IPv4 Link-Local Addresses*, RFC 3927, May 2005.

[20] S. Thomson, et al., *IPv6 Stateless Address Autoconfiguration*, RFC 2462, December 1998.

[21] T. Narten, et al., *Neighbor Discovery for IP Version 6 (IPv6*), RFC 2461, December 1998.

[22] R. Droms, *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*, RFC 3736, April 2004.

[23] IEEE 802.15 Working Group for WPAN, http://www.ieee802.org/15.

[24] Rui Campos and Manuel Ricardo, *Dynamic Autoconfiguration in 4G Networks: Problem Statement and Preliminary Solution*, in Proceedings of the 1st International ACM Workshop on Dynamic Interconnection of Networks (DIN'05), September 2005.

[25] H. Schulzrinne and R. Hancock, *GIST: General Internet Signaling Transport*, draft-ietf-nsis-ntlp-08 (work in progress), Internet Draft (work in progress), September 2005.

[26] D. Eastlake et al., *US Secure Hash Algorithm 1 (SHA1)*, RFC 3174, September 2001.

[27] Q. Dang and T. Polk, *Hash-Based Key Derivation*, Internet Draft, draft-dang-nistkdf-00 (work in progress), October 2005.

[28] Tadeusz Wysocki et al., *A Review of Routing Protocols for Mobile Ad Hoc Networks*, Elsevier, vol. 2, no. 1, pp.1-22, January 2004.

[29] C. Bernardos and M. Calderon, *Survey of IP address autoconfiguration mechanisms for MANETs,* Internet Draft, draft-bernardos-manetautoconf-survey-00 (work in progress), July 2005.

[30] K. Sethom et al., *Gateway Selection in Multi-homed Ad Hoc Networks*, Internet Draft, draft-sethom-adhoc gateway-selection-00 (work in progress), July 2005.

[31] T. Calçada and M. Ricardo, *Extending the Coverage of a 4G Telecom Network using Hybrid Ad-hoc Networks: a Case Study*, in Proceedings of the Fourth Annual Mediterranean Ad Hoc Networking Workshop, June 21-24, 2005, France.

[32] Cornelia Kappler, Nadeem Akhtar, Rui Campos and Petteri Poyhonen, *Network Composition using Existing and New Technologies*, in Proceedings of the 14th IST Mobile & Wireless Communications Summit, Dresden, June 2005.

[33] S. Schmid et al., *TurfNet: An Architecture for Dynamically Composable Networks*, in Proceedings of the First IFIP TC6 WG6.6 International Workshop on Autonomic Communication, Berlin, Germany, October 2004.

[34] A. Petrescu, V. Devarapalli, R. Wakikawa and P. Thubert, *Network Mobility (NEMO) Basic Support Protocol,* RFC 3963, January 2005.

[35] K. Shima, *IPv4 Mobile Host/Network support for NEMO Basic Support Protocol,* Internet Draft, draft-shima-nemo-v4prefix-01 (work in progress), October 2005.

[36] H. Morioka, *Mobile Router Cooperation Protocol*, Internet Draft, draft-morioka-nemo-mrcoop-00 (work in progress), July 2005.