Federating Personal Networks over Heterogeneous Ad-hoc Scenarios

Luis Sánchez, Jorge Lanza, Luis Muñoz

University of Cantabria, E.T.S. Ingenieros Industriales y de Telecomunicación, Avda. de Los Castros s/n, 39004, Santander, SPAIN

{lsanchez, jlanza, luis}@tlmat.unican.es

Corresponding author:
Luis Sánchez.
Departamento Ingeniería de Comunicaciones, E.T.S. Ingenieros Industriales y de Telecomunicación, Avda. de Los Castros s/n, 39004, Santander, SPAIN.
E-mail: lsanchez@tlmat.unican.es

Abstract. This paper will present the specification of the solutions and mechanisms that support the creation of a Federation between Personal Networks that are located in the same area and thus can establish a direct link between each other. The idea behind the Personal Network concept is that the user's personal devices organize themselves in a secure and private network independently of their geographical location or the access technologies used. Nevertheless, in order to fully exploit the benefits of this concept, it is necessary to complement it with the mechanisms that enable the interaction between several people with a shared objective (e.g. a hobby, common project, etc.). This concept of collaboration between several Personal Networks receives the name of Personal Network Federation. This collaboration can be established in multiple scenarios but in this paper the focus will be on the case in which clusters of nodes belonging to different users are located in the same area and they can establish links on peer-to-peer manner.

Keywords: *Personal Network, Federation, Secure Association, Heterogeneity*

1 Introduction

Personal communications have experienced an extraordinary boost in the recent years. One of the novel paradigms that have appeared is the Personal Network (PN), being an emerging concept which combines pervasive computing and strong user focus. PNs are a relatively new concept 1 that allows a user to transparently interconnect all his personal devices independently of their location (e.g. in the personal area, at home, at work or in his car). A PN is a virtual network where collocated personal devices organize themselves in *clusters* which are in turn interconnected over some interconnecting structure.

Please use the following format when citing this chapter:

Sánchez, L., Lanza, J., Muños, L., 2007, in IFIP International Federation for Information Processing, Volume 245, Personal Wireless Communications, eds. Simak, B., Bestak, R., Kozowska, E., (Boston: Springer), pp. 38-53.

While Personal Networking is focused on the communication between personal devices only, many communication patterns need to extend the boundaries of the PN and involve the secure interaction of multiple people having common interests. Hence, personal communications cannot be restricted to the services provided by the devices the user owns, but the possibility to interact with other user's PN has to be enabled in order to support the user in his/hers private and professional activities. The concept of PN Federations (PN-F) is even a more challenging one since the relations between users have to be managed and the security has to be reinforced in order to not open security holes while allowing authorized users to cooperate with you.

Existing solutions such as virtual private networks 2 or peer-to-peer application overlays 3 can only offer a partial solution as they do not provide true self-organization and end-to-end security. Furthermore, they lack the notion of group trust and usually only focus on one specific software application 4. As it is discussed in 5 and 6 the current diversification of control planes requires a manual configuration of network interworking. The problem will increase in the future, with more dynamic topologies and integration of heterogeneous networks in a ubiquitous, reactive environment. Nevertheless, the solutions proposed in these cases, involved too generic assumptions and spam along a plethora of different kind of networks thus not providing practical solutions to the user centricity that is mandatory in personal networking. 7 represents a P2P Wireless Network Confederation (P2PWNC) model, in which a set of administrative domains is providing wireless Internet access to each other's users. The authors aim to replace the human administrator of roaming agreements by Domain Agents (DA), thus eliminating administrative overhead. While this research approach addresses many critical issues, it does not fully address all the emerging needs of future wireless and ubiquitous networks since it is too much focused on specific environment such as mobile ad-hoc networks.

The rest of the paper is structured as follows. In Section 2 the generic architecture of a federation between two PNs will be shown. The life cycle of the PN-F as well as the main functional entities of the PN-F architecture will be described. As already said, heterogeneity and security enforcement are key challenges for the federations' establishment. Thus, in Section 3 the proposed solutions to tackle them will be presented. Section 4 will present the specification of the mechanisms for create, form and use a PN-F over a heterogeneous Ad-hoc scenario. Finally, Section 5 will conclude the paper highlighting the main aspects of the work presented.

2 PN-F Architecture

A PN-F can be defined as a secure impromptu, situation-aware or beforehand agreed cooperation between Personal Networks of different people for the purpose of achieving a common goal or service by forming an efficient collaboration. More precisely, a secure overlay of the participating devices will be formed, that isolates a subset of the resources in the constituent devices. Within the federation, the devices can communicate with each other and allow each other access to specific services or the usage of specific resources for performing the common task.

The basic requirements are that the communication is secure, self-organized, confined within the subset of collaborating devices and that only the resources, applications and services needed to achieve the common goal are made accessible. The term federation describes the process where entities broker trust and exchange information across organizational boundaries. The WS-Federation specification 8 defines a federation as "a collection of realms that have established trust". For instance, in collaborative working, a PN-F could be formed between the relevant devices belonging to the different people working on a common project. Only the resources needed for the project (e.g. files, e-mails, project schedule, whiteboard, software, agenda...) are made available to the PN federation. Other resources (e.g. personal files...) are shielded from your colleagues or only available through other federations, for instance with family and friends. It is clear that this concept will rely heavily on the notion of group trust.

The possibilities of establishing a federation are wide and bring several ways of classifying the federations. Taking into account the duration, we can have *Short-lived* (conference network) versus *Long-term* (project network); from a triggering way standpoint we can have *Reactive* (emergency network) versus *Proactive* (family network); finally, depending on the scenario we can distinguish between *Ad-Hoc* (meeting room network) and *Infrastructure* (distant learning). While the first two ones falls under the administrative and context considerations, the last one affects highly the way the federation creation, formation and use processes can be tackled. While in the Infrastructure case, the mechanisms to be deployed can count on the existence of some entities on the Internet that provides support to all the procedures, in the Ad-Hoc case, no Internet access can be assumed and all the procedures have to be carried out among the nodes belonging to the federating PNs present at that particular moment and place. Additionally, while in the Infrastructure case the common ground can be assumed through the use of the IP protocol, in the Ad-Hoc case the connectivity level has to be solved first, meaning that the possible heterogeneity in terms of wireless technologies has to be tackled. In this paper we will focus on describing the architecture, mechanisms and solutions designed in order to allow a PN-F to be created, formed and used in an Ad-Hoc situation.

2.1 PN-F functional entities

Fig. 1 shows the generic architecture of a PN-F together with its main functional entities and the relations between them. These functional entities are:

- Federation Manager (FM): It is responsible for managing all the interactions between two PNs during the PN-F Participation phase, mainly focused on the exchange of PN-F profiles.
- Secure Context Management Framework (SCMF): It is a distributed framework that provides access to all the PN related context information. One of its responsibilities is to store the different profiles from the PN-Fs that the corresponding PN is involved in.
- MAGNET Service Management Platform (MSMP): It controls the service discovery and access. The FM will interact with it when the PN-F Participation profile is to be created. For the service discovery, the operation is centralized on

a Service Management Node (SMN), located on each of the PN clusters, while for the provision is fully distributed.

- Policy Engine (PE): Act as an interpreter and reasoner of the rules declared on the PN-F profiles to enable access control enforcement.
- Personal Network Directory Service (PNDS): Takes the role of a trusted third party. It can be used to verify the identity of the peer PN on the different phases of the PN-F and it can also host the publication of PN-Fs' and PNs' details.

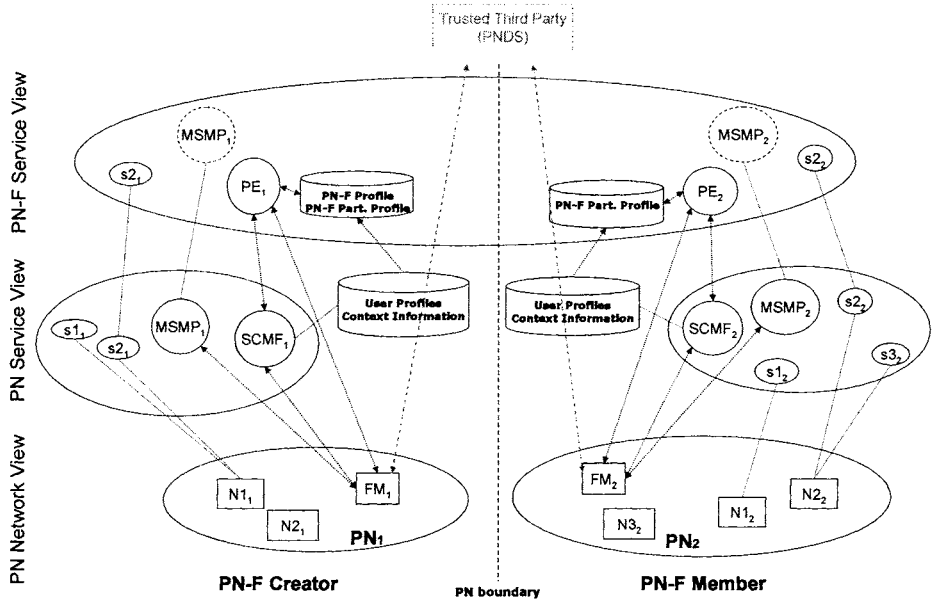

Fig. 1. PN-F Architecture and main functional entities

2.2 PN-F Life Cycle

We shortly introduce the three identified phases, as different policy rules have to be checked in each phase.

PN-F Participation: the objective of this phase is the agreement between the PN-F Creator (i.e. the PN that starts the PN-F) and one candidate PN-F Member (a PN aiming at participating on the PN-F). The basis for this agreement is the secure exchange of different PN-F profiles.

PN-F Formation: in this phase, the communication means between any two PN-F Members are deployed. The main issues solved during this phase are addressing, routing and security.

PN-F Use: This phase comprises both the discovery and provision of services offered to other PN Members. The authenticity provided by the networking solutions implemented below the PN-F service level allows the deployment of access policies for the shared resources.

3 Heterogeneity and Privacy Solutions

Up to know we have presented a generic architecture view of the PN-Fs. In the following sections we will present specific solutions for the case in which the PN-F is to be created, formed and used in an Ad-Hoc scenario.

3.1 Security association establishment

In 9 the baseline procedure for assuring privacy and security within a PN was described. This mechanism, so-called *imprinting*, basically consists on the establishment of a security association between a pair of personal nodes. Assuming that each pair of nodes within the PN had this security association, materialized into long-term bilateral shared secrets established under the supervision of the network owner, the authenticity, privacy and security in general is assured through leveraging these shared secrets whenever two personal nodes want to communicate with each other.

Following a similar approach, the communication between any two nodes belonging to different PNs can also be assured by leveraging a security association established in this case not on a node-node basis as it was the case of PNs, but on a PN-PN basis. The shared-secret will be used to protect the communication between any node of one of the PNs and another one from the other PN. Two main methods have been identified so far in order to accomplish the security association establishment. In any of the two cases, the result is that pair-wise secrets (so-called K_{PN}) are derived and associated to the peer PN identifier.

Basically, the enforcement of these keys assures the authenticity of the peer nodes (i.e. only the nodes belonging to a PN will know which K_{PN} is the correct one) and the privacy of the communication (i.e. K_{PN} is used to derive session keys that are subsequently used to encrypt the packets exchanged). Further authorization to make use of the services provided by the user PN should be based on this authentication. Besides, the solutions proposed enable node authentication but if really sensitive information might be disclosed, user authentication should be put on top.

3.2 Neighbor discovery and authentication

In the Ad-Hoc case the PN-F formation starts by discovering surrounding nodes belonging to peer PNs. A beaconing process has been implemented in order to be continuously aware of the immediate neighbors, both personal and foreign. Each node periodically sends one of these packets in order to advertise its presence not only to its personal neighbors but also to every other node belonging to other PNs. In case that the node belongs to a different PN, the receiving node acknowledges the reception and both nodes indicate to the Federation Manager the newly discovered PN indicating the PN ID.

- Mandatory payload fields:
  - Node ID: 20 bytes public identifier. Currently it is derived as a digest over the peer's public DH (Diffie-Hellman) key used during the imprinting procedure.

- PN ID: PN Name (or hash of the PN Name). Personal certificates that are used for the security association establishment are written for a certain PN Name. Uniqueness of the PN Name might therefore be guaranteed by the Authority that issues the certificate).

In case that a security association is already established with that PN, the node will be able to go into an authentication and session key derivation function in order to verify the identity the other node is claiming on its beacons.

The authentication is performed through a three way handshake (Request – Response – Success) in which the long-term shared key is used to verify the identity denoted by the identifier field in the beacon received.

The same procedure is used for neighbour authentication and for exchange of link session keys used at the Universal Convergence Layer (UCL – see Section 3.3) for privacy assurance through communications encryption.

The link layer session key is computed as HMAC SHA-256($LMSK_{1\text{-}2}$, $N_1 \mid N_2$) and is valid for T_2 seconds ($T_2 \leq T_1$). This procedure is run any time a new neighbour is discovered by a peer and whenever the derived session keys expire. $LMSK_{1\text{-}2}$ is calculated as HMAC_SHA_256 (K_{PN}, "MAC_1+MAC_2"). Use of the MAC addresses of the candidate radios in the derivation function ensures that different pairs of hardware adaptors share different link keys even for the same pair of devices.

3.3 Heterogeneity support and Security Association enforcement

The capability of working in a heterogeneous environment is a must for future personal networks. This heterogeneity will be mainly reflected in terms of the different air interfaces that will coexist in these scenarios requiring additional schemes to handle this heterogeneity.

The concept of isolating the upper-layers from underlying wireless technologies and thus providing real multi-mode can be achieved by introducing a Universal Convergence Layer 10. The UCL mainly will act as an enabler for backward and forward compatibility by defining a common interface towards the network layer while managing several different wireless access technologies independently of their PHY and MAC layers. In this sense, the solution adopted makes it possible for the nodes to have a single IP address independently of the number of air interfaces it has. This way the routing protocol placed in layer 3 will be able to settle routes embracing multiple radio domains in a complete seamlessly manner. The combination of these two techniques, UCL plus ad hoc routing protocol, enables the solution proposed to manage the heterogeneity that will appear in the Ad-Hoc PN-F environment.

From a security perspective, one of the most important design goals of UCL is to make sure that use of heterogeneous radio specific legacy security system does not cause any additional security vulnerabilities. In addition to making parallel use of different radio systems secure, presence of UCL also provides an opportunity to upgrade or even complement the legacy radio systems. Using the encryption capabilities provided by the UCL all the user data traffic sent is encrypted and signed to assure the integrity, authenticity and privacy of the information exchanged.

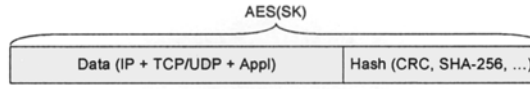

Fig. 2. Data PDU format

As shown in Fig. 2, a hash signature of the packet is applied to each packet. Additionally, the packet is encrypted using the previously exchanged session keys.

4 PN-F Specification

4.1 Scenario description

Fig. 3 presents the generic scenario over which Ad-Hoc PN-Fs might operate. As can be seen, clusters from different PNs communicates on a peer-to-peer manner where secure communications have to be assured starting from the connectivity level and that cannot rely on the support given by any third party located in the infrastructure. Additionally, many wireless technologies can be coexisting, thus at the connectivity level several radio domains can be identified forcing to establish a multihop communication path through combination of routing protocol and UCL techniques.

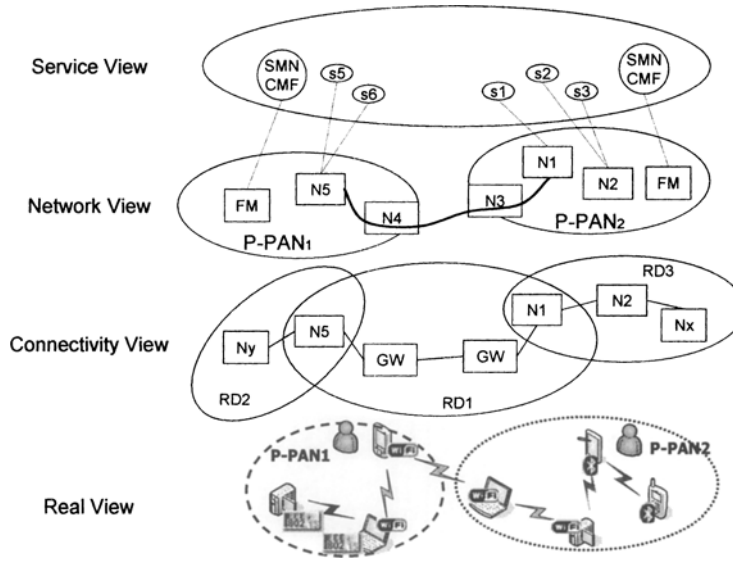

Fig. 3. High-level view of the Ad-Hoc PN-F scenario

4.2 PN-F Participation phase

The PN-F Participation phase comprises the procedures by which the information needed to join a PN-F is securely exchanged between the PN-F Creator and another PN aiming at being member of that PN-F.

The event that triggers the participation phase can be flexible chosen from user action, context (time, location, presence) etc. Once the basic mechanism works, this type of scenario building can be done later on.

The PN-F Owner will first create/generate the PN-F profile. It will define the identity and the policies and rules within the PN-F. The minimum information (i.e. public part of the PN-F Profile – **PN-F Profile$_{PUBLIC}$**) that must be present is:

- PN-F Name/ID – A unique method for identifying the PN-F
- The goal or purpose of the PN-F
- Trigger conditions, activation/closing rules
- Creator Point of Contact (PoC) – The identity of the Creator and the address where negotiation to join the PN-F can begin

Optionally, the creator might also make public additional information such as:

- Participation rules: who else is or may be invited
- Minimum service list required

This phase starts when the Creator advertises the public part of the PN-F Profile. The Publication and Discovery step can have a great variety of possibilities. For example, an invitation could be issued to people already known to the Creator via e-mail, via a local broadcast to people in the vicinity of the Creator, or posted at a known 3rd Party location, where people visit to look for others to federate with. Once the Candidate is aware of the PN-F, and after a security association has been established between both PNs, it will edit its PN-F Participation Profile, mainly consisting on the resources that it makes available to this federation, and securely sends it to the Creator. The Creator then checks whether the Candidate fulfils the federation policies and if this is the case, the private part of the PN-F Profile, (**PN-F Profile$_{PRIVATE}$**) is sent to the new Member:

- Federation Broadcast Key
- List of current federation members
- List of currently available federated services

PN-F Participation: Publication and Discovery

In case that there is not access to a supporting infrastructure that provides a repository in which PN-Fs and potential members can advertise its existence, it is necessary to specify different procedures to fulfill this step in the PN-F Participation phase.

Fig. 4 shows the publication and discovery interactions as they would occur on an infrastructureless scenario.

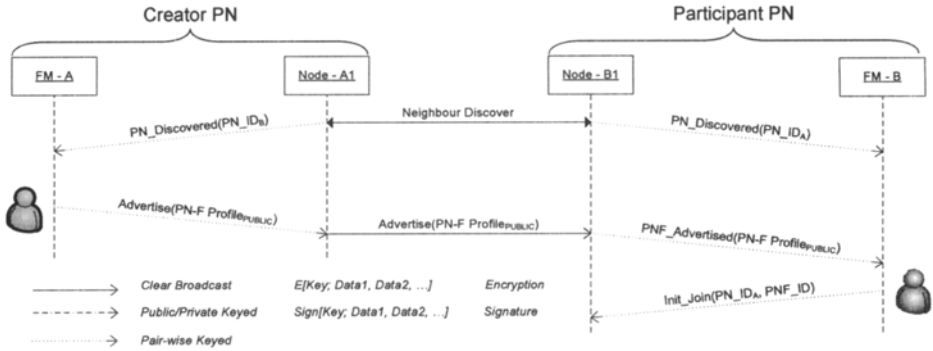

Fig. 4. Publication and discovery step on ad hoc scenarios

In this case, the PoC addresses advertised within the PN-F profile might not be usable. Typically, these addresses will be globally routable addresses for FM that is pointless in an infrastructureless environment. Hence, when the FM receives a *PNF_ADVERTISED* primitive it detects that this is an ad hoc scenario and issues an *INIT_JOIN* to the GW node from which the advertisement comes.

The *INIT_JOIN* primitive contains the following information:

- PN_ID_X: The identifier of the PN-F Creator so that the GW knows to whom address the forthcoming messages
- *PNF_ID*: The identifier of the PN-F to which the user is willing to join

This information will be used for feeding the Authentication step primitives as it will be shown in the next section.

PN-F Participation: Authentication and Security Association establishment

Up to this point in the PN-F Participation phase, the information must be taken as is with no guarantee of certainty either on the origin or the actual content.

In order to continue with the PN-F Participation phase, it is mandatory that both Creator and Candidate perform a mutual authentication and establish a security association between them so that the rest of the steps can be secured.

As stated in Section 3.1, two main authentication methods have been identified so far. The first one based on the typical PKI structure where certificates issued to PNs are used to verify its identity and to establish the bilateral security association. The second one is proposed in order to be infrastructure-independent and exploits PAC concept put forward for the imprinting of new personal nodes. In this section only a specification for the first type of authentication is presented, whereas further work will be done on the specification of an authentication method using this PAC.

It is important to note that if a previously established security association between the two PNs exists, this step can be omitted since they can use the shared secret resulting from that security association to assure the security in subsequent steps of the PN-F Participation phase. Hence, this step only makes sense for the first time the two PNs starts an interaction.

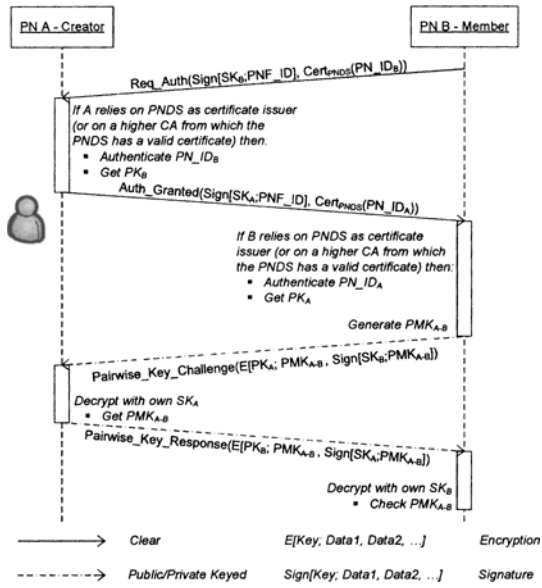

Fig. 5. Certificates based authentication

The common fields of the *REQ_AUTH* and *AUTH_GRANTED* primitives shown in Fig. 5 are:

- Sender Certificate: Issued by a commonly trusted (whether directly or by following a typical PKI hierarchy) third party, is used to both verify the sender's identity and to provide its Public Key (PK_X)
- Signature of PNF_ID: By encrypting the identifier of the PN-F subject of the interaction with its own private key (SK_X), the sender prevents using its certificate (it has to be remembered that this is public material) inadequately. This way it can be verified at the receiver that it is the actual certificate owner showing interest in starting the authentication.

Upon the correct verification of both *REQ_AUTH* and *AUTH_GRANTED* primitives, both PNs are mutually authenticated and they have each others PK.

Afterwards, the process of creating keys between the Creator and Member takes place. The Key Generation stage, used in the PN-F Formation, could be based on the Diffie-Hellman protocol, but since the Creator and Member already have a secure communication with the use of Public/Private keys then one can just generate a symmetrical key and inform the other about of it.

PN-F Participation: Join

Once this point in the PN-F Participation phase is reached the situation is as follows:

- Both PNs are mutually authenticated and share a pair-wise key that can be used to protect their communications providing privacy and origin authentication.
- The potential Member (potential since it has not yet provided its Participation Profile so the Creator can still prevent it to become full blown Member of the PN-F) has all the required information concerning the PN-F Profile and completed if required on an optional Additional PN-F info provision step.

Taking this into account, the potential Member may have already a participation profile for that type of federation, or may have none and would first prompt the user to edit it. When the user is ready and has decided to join, the *JOIN* message is sent to the creator (asynchronously to the invitation).

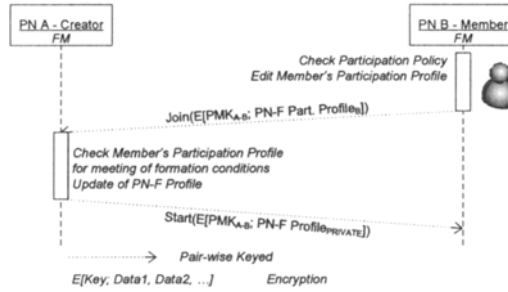

Fig. 6. Join step

Fig. 6 shows the primitives exchange during the Join step. The *JOIN* primitive contains information on the Member's PN-F Participation Profile as follows:

- Identifier of the PN-F for which this Participation Profile corresponds
- A Point of Contact for the Member containing the Identifier by which it can be recognized in the PN-F and an address where further negotiation concerning the PN-F can continue.
- Set of resources the participant intends to share with all other participants.
- Rules, policies for accessing these services (optional).

Once the Creator receives the *JOIN* message it will check if the Candidate fulfils the PN-F Participation rules. If they are, then the Creator can send the *START* primitive to the Member. However, it can occur that the general formation rules may not have been fulfilled yet, for example the federation use starts in two hours time, or certain participants have not joined yet, etc, so that the federation cannot start immediately. In this case, two options have been identified:

- Only when the federation can be started, the creator creates and sends the *START* primitive to all the registered Members
- The Creator sends the *START* primitive immediately and each of the Members is the responsible to enforce the general formation rules so that the PN-F is not used before.

In any of the cases, the *START* message will contain the **PN-F Profile$_{PRIVATE}$**.

4.3 PN-F Formation and Use phases

Once the new PN has fully joined the PN-F, it can proceed to the establishment of the PN-F with other surrounding members. In order to enable the communication between nodes belonging to different PNs, during the Formation phase, a network overlay is established among all the nodes of the PN-F members.

PN-F Addressing

Since a network overlay uses its own virtual addressing space, a PN-F addressing is defined (and this information is propagated as part of the PN-F profile) and every

involved node will obtain a unique PN-F IP address within this addressing space. These addresses will be used for all communication that takes place within the federation.

This virtual address space is separated from the public IP addressing space and from the private PN addressing space of the participating PNs and guarantees that all PN-F communication is confined within the PN-F already at the network level. In addition, at the network level, specific primitives (e.g. PN-F wide multicasting) can be offered to the higher layers in order to facilitate for example service provisioning.

As it will be described in Section 4.3.3, part of the security checks implemented within the GW node at UCL level, assures that only those nodes belonging to PNs that are member of the PN-F can use this addresses on the IP header. As such, only members of the same PN-F will be able to become part of this overlay and all their communication will be shielded from the outside world, any other PN-F communication or PN communication.

Establishment of a network

In the ad hoc case using overlays, the PN-F formation takes place both at connectivity and at network level.

The main requirements are:

- Self-configuration (or minimal user intervention, if defined in the PN-F policies)
- Independence from third party entities not part of any of the involved clusters.
- Establishment of secure network overlay.
- Support for spontaneous PN-F creation.

The first step in the formation of the federation is the establishment of a secure connection. As described in Section 3.2, neighboring nodes are authenticated and link session keys have to be exchanged for securing traffic. Based on this cryptographic material, at UCL level the privacy and origin authentication of the communications at the connectivity level are assured being the basis for authorization and access control , which is the main aspect of federations, on upper levels.

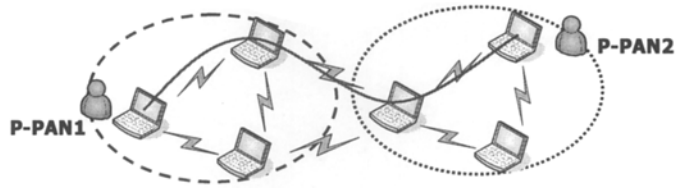

Fig. 7. Ad-hoc network establishment among cluster nodes

Once the connectivity level is assured, the network overlay can be established. As shown in Fig. 7, the routing protocol will provide end-to-end paths within the PN-F network. Different PN-Fs might require different routing alternatives. Nevertheless, reactive routing should be taken as the default choice since it fits better on the establishment of an on-demand network such as the PN-Fs would be in the majority of the cases. Route discovery process is authenticated since route response messages are unicast (protected by secure connectivity level).

Federation Use

The PN-F Use stage is triggered as soon as one of the nodes in any of the clusters involved in the PN-F request a service provided by some other node in a different

person's cluster. In this sense, within this phase, both the service discovery and provision phases are comprised.

Using the encryption capabilities provided by the UCL all the user data traffic sent is encrypted and signed to assure the integrity, authenticity and privacy of the information exchanged. Fig. 8 shows the procedure followed on the transmission function in the UCL for selecting the appropriate key to secure the communication.

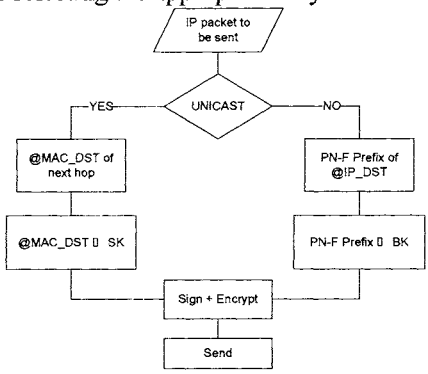

Fig. 8. Data transmission procedure.

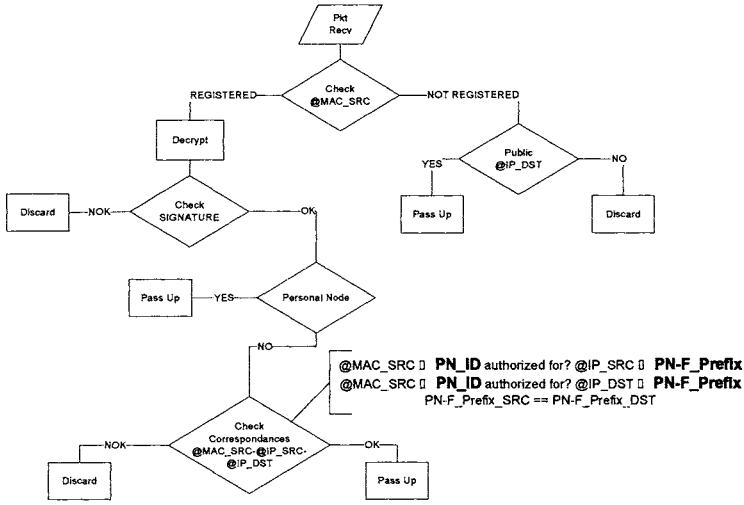

Fig. 9. Impersonation prevention procedure

Whenever a packet is received, the information on the datagram headers is checked to verify the authenticity of the information and to prevent impersonation as shown in Fig. 9. At the edges of the cluster, this conformance checks have to be reinforced in order to avoid misuse of the PN or PN-F resources. This allows upper layers to trust on the information contained on the packets and perform access control based on it.

In Fig. 10, a detailed description of the unicast and broadcast communications, both within the PN and under the auspices of a PN-F, is presented.

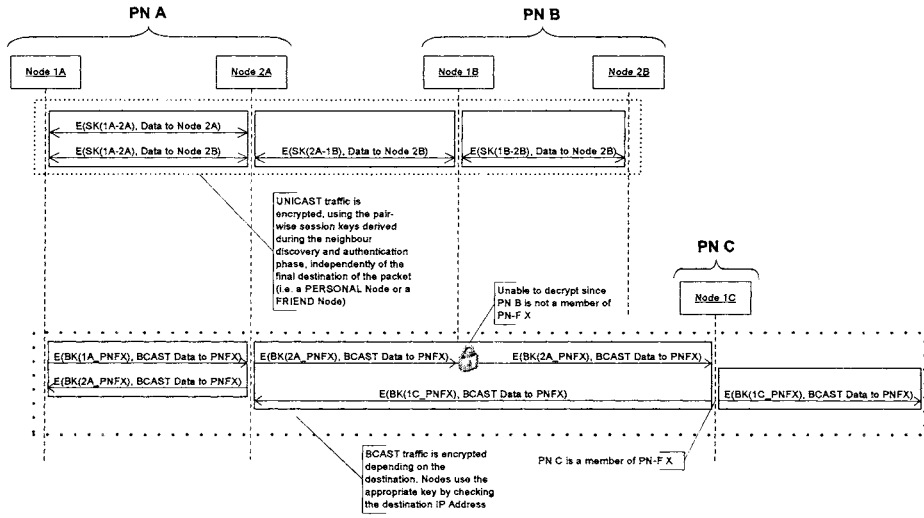

Fig. 10. Unicast and Broadcast communication encryption details

Finally, as shown in Fig. 11, the service discovery and provision is carried out.

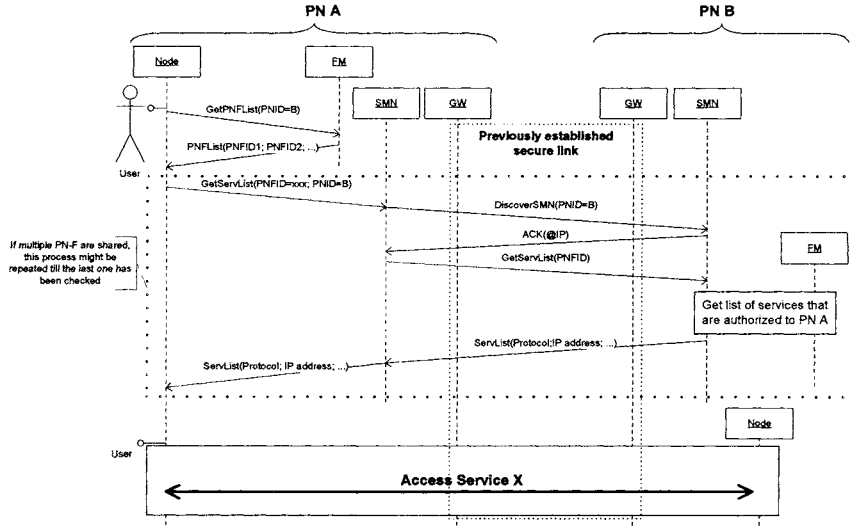

Fig. 11. Service discovery and access in ad hoc PN-F based overlays architecture

Whenever a node wants to know about the availability of services within the PN-F, it will direct its query to its cluster SMN. The SMN will first look for its counterpart in the other cluster and once it discovers the other SMN, redirects the query for available services. This query can try to discover all the authorized services (as shown in Fig. 11) or focus the search on specific ones. The SMN as the responsible for managing the services in the cluster is the one that has to check which of the complete list of available services the other person is authorized to access to. The information

stored in the different PN-F Participation profiles is checked to see whether the available services are authorized or not. Once it has the response, it sends it back to the originating SMN who forwards the information to the requesting node.

After the discovery phase, the requesting node initiates directly with the server node the service provision phase. The authorization mechanisms used in the discovery phase, do not prevent the use of further mechanisms to authenticate and authorize the user against the service.

5 Conclusions

In this paper we have presented a detailed specification of the mechanisms that allows the creation, formation and use of Personal Networks Federations over a heterogeneous peer-to-peer wireless scenario.

The main requirements in terms of security and self-configuration imposed by the federation concept, and the scenario selected for its creation and use have been identified, and the corresponding procedures that cope with them described in detail. In this sense appropriate mutual authentication algorithms have been described and pair-wise secrets leveraged to provide a secure connectivity and network level so that upper layers authorization and access control can be easily supported.

Additionally, specific multi-standard convergence procedure has been implemented in order to tackle the heterogeneity in terms of access technologies such that network overlay establishment can be done transparently and independently of the underlying radio domains that compose the connectivity level.

This detailed specification is the basis for an implementation that is being carried out over real platforms consisting of laptops and PDAs that will raise true interest of industry and end-users as well as support the identification of future optimizations that could be achieved by enhancing the collaboration between the different components comprising the whole system.

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), 175-186.
2. Charles Scott , Paul Wolfe , Mike Erwin, "Virtual private networks", O'Reilly & Associates, Inc., Sebastopol, CA, 1998
3. Sun Microsystems, "JXTA™ Technology: Creating Connected Communities", January 2004
4. J. Hoebeke, G. Holderbeke, I. Moerman, Bart Dhoedt, P. Demeester "Virtual Private Ad Hoc Networking", Wireless Personal Communications, Volume 38, Issue 1, June 2006, pp. 125-141
5. C. Kappler, P. Mendes, C. Prehofer, P. Pöyhönen and D. Zhou, "A Framework for Self-organized Network Composition", WAC 2004 (IFIP Workshop on Autonomic Communication), Berlin, Germany, October 2004.

6. L. Fan, N. Akhtar, K. A. Chew, K. Moessner and R. Tafazolli, "Network Composition: A Step towards Pervasive Computing", 3G 2004, London, UK, October 2004.
7. Elias C. Efstathiou, George C. Polyzos: "A peer-to-peer approach to wireless LAN roaming", Proc. 1st ACM Int. workshop on Wireless mobile applications and services on WLAN hotspots, San Diego, CA, 2003.
8. Kaler, Chris, et al. "Web Services Federation Language (WS-Federation)." Online article, 8 July 2003. IBM, Microsoft, RSA Security Inc., and VeriSign. 22 March 2004. http://msdn.microsoft.com/library/en-us/dnglobspec/html/ws-federation.asp
9. IST-507102 MAGNET/WP4.3/UNIS/D4.3.2/R/PU/002/1.0, "Final version of the Network-Level Security", March 3, 2005.
10. L. Sanchez, J. Lanza, L. Muñoz, J. Perez Vila, "Enabling Secure Communications over Heterogeneous Air Interfaces: Building Private Personal Area Networks", 8th International Symposium on Wireless Personal Multimedia Communications - Aalborg, September 2005.