Ad Hoc Federation of Networks (FedNets) – Mechanisms and Requirements

N.I. Cempaka Wangi, R.V Prasad, I. Niemegeers, S. Heemstra de Groot
Delft University of Technology
Mekelweg 4, 2628 CD
Delft, The Netherlands
{n.i.cempaka wangi, vprasad, i.niemegeers, s.heemstra.de.groot}@ewi.tudelft.nl

***Abstract*— We have been witnessing developments of many innovative applications in the field of ad hoc wireless networks as well as many projects in the area of user-centric, context aware and ambient assisted networks. This paper introduces a novel framework called FedNets that bridges user centric networks to form an ad hoc federation to achieve group cooperation. Our preliminary study of all the mechanisms, requirements and potential techniques that need to be addressed in this regard is presented. We describe a roadmap towards a fully networked co-operative interaction. We believe that this paper will serve as the basis for our next stages of development, as well as for other similar works in the field of wireless ad hoc networks.**

Keywords- Group networking, Pervasive computing, Ad hoc networks.

I. INTRODUCTION

The research and development in the area of microelectronics and RF communication is making a huge difference to the way we interact with the world. Each device is capable of storing a huge amount of data, communicating with its surroundings and making intelligent decisions based on various aspects. A range of wireless communication techniques has also contributed to this new trend in innovative applications. Besides, further miniaturization and provision of self-powering capabilities to wireless sensors and actuators together with inexpensive processing devices are providing the basis to create environments that are smart and reactive.

While the Internet offers mostly a permanent connectivity, we are witnessing a complete ad hoc and dynamic miniature networks enabling the interactions with the surroundings at the edge of the Internet infrastructure. The physical environment of a person, e.g., his or her home, office, car, public places he or she visits, and public transportation, will exhibit intelligence, become smarter, more responsive, and more accommodating to the individual needs. Future technologies would provide location and context dependent services and introduce new levels of personal comfort and safety. One important example of such an effort is Personal Networks (PNs), which are person-centric networks connecting personal devices and artifacts regardless of geographical location [1]. As illustrated in Fig. 1, the connection between devices will physically be made via infrastructure-based networks, vehicle area networks, a home network or mobile ad hoc networks (MANET). A PN provides its owner a global presence and supports and/or follows him everywhere.

While we think it is inevitable that individuals need to network their devices, we cannot forget the basic need of any human – the social networking. We envisage that at no point of time an individual would be satisfied with only a network of his/her devices. Thus, there is a strong need to go beyond person centric systems such as PNs. FedNet [2][1] is an ad hoc federation that allows these person-centric systems to support ad hoc group applications. For convenience, we call these systems networks, but they are actually distributed environments. Even though our work is concerning the development of FedNets formed by several PNs, other networks such as PANs, on-board networks of a vehicle could also become constituents of such FedNets.

In the early stage of our research, we need to identify mechanisms that are needed, requirements from each mechanism and how to satisfy such requirements. We notice that several protocols which are partially comparable to our design have emerged, especially in the area of ubiquitous and pervasive computing environment. We examine and compare the techniques used by protocols as potential alternatives for our solution. Regarding our proposal, we have to identify the techniques that might be useful, and which are still missing from the protocol or the one that needs further modification. This paper summarizes our preliminary studies on such aspects, in order to bring FedNets into reality.

The rest of this paper is structured as follows. In Section 2 we present our study on related works. In Section 3 and Section 4 we introduce the concept of PNs and FedNets respectively. In Section 5 we present several mechanisms that are needed to establish a FedNets together with their requirements and discuss different strategies proposed by existing protocols. Finally, in Section 6 we conclude.

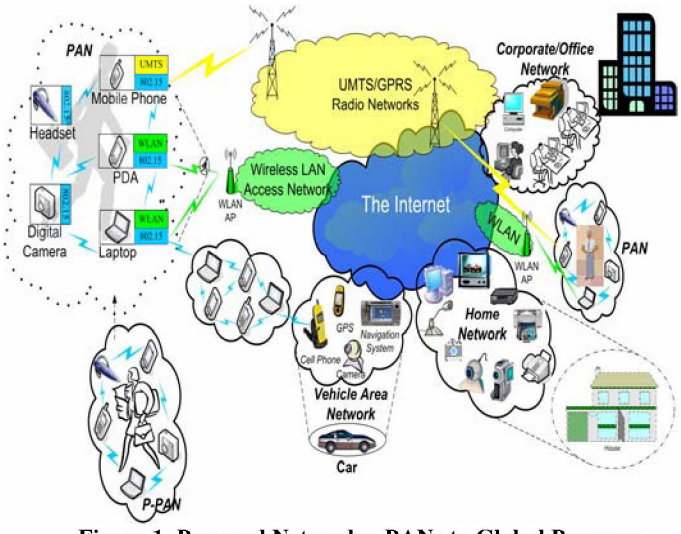

Figure 1. Personal Networks: PANs to Global Presence

[1] MagnetBeyond Project [3] is currently developing solutions for PN federation by considering all possible infrastructure and ad hoc cases [5]. The work presented in this paper focuses on PN federations that occur in ad hoc networks.

II. Related Works

In a proposal from the University of Illinois at Urbana-Champaign and the Mobius project [4], devices in close vicinity are grouped together to form so called Mobile Grouped Devices (MOPEDs). Each MOPED is connected to a proxy (some kind of home agent) via an infrastructure connection. MOPED differs from PNs in its dependency on the proxy and the infrastructure. Furthermore, MOPED does not address direct ad-hoc communication with other person's MOPED and is therefore too limited in scope to support the vision of group communications.

The concept of federation is not new in the distributed systems. In 1994, the ANSA consortium on open dependable distributed computing has defined federation as "facilitating co-operation between autonomous organizations for the purpose of sharing services and resources". The principal federation issue is seen as the problem of dealing with establishing heterogeneous authority in a large distributed system spanning boundaries of authority, while maintaining local control [5]. The ANSA approach until now has not been adopted widely, but contains potentially useful ideas for FedNets.

The idea of federation has come up again in the context of networks and grid computing. These developments aim at access control [6], resource allocation [7], load management [8] and security [9]. They are distinct from our approach in the sense that they are based on a (single) service-user service-provider paradigm, while our view is that of autonomous systems cooperating to achieve a common goal.

III. The Concept of Personal Networks

Personal Networks (PN) is an emerging concept related to pervasive computing with a strong user-focused view. PN extends a person's Personal Area Network (PAN) that surrounds him with devices and services farther away (see Fig. 1).

To distinguish between personal devices and devices belonging to someone else, the owner has to personalize his devices in a so-called imprinting procedure, which is done once for each device a person likes to add to his PN. In this process, a shared secret key is generated for securing communication between personal devices. Next, devices that are in close vicinity would automatically form a personal cluster and clusters would globally connect to each other using interconnecting networks. PNs consist of a mix of wired and wireless devices, with different networking technologies (e.g. 802.11 and all its variants, Bluetooth), and capabilities (e.g. memory space, power consumption and processing capability). Thus, a more powerful device should be elected in each cluster as a gateway to bridge communication with other clusters belonging to the same person as well as with nodes belonging to others.

The key to a successful PN realization is bridging different technologies and offering a homogeneous and a clear view to the end-user. To manage various services and resources within a PN, an entity called Service Management Node (SMN) is introduced in each cluster. Furthermore, a person's PN is configured to support his/her needs by taking into account the context, location and communication possibilities. For this purpose, Context Management Node (CMN) is introduced in each cluster. SMNs and CMNs will communicate with each other via gateway nodes in a private and secure way using the tunneling mechanisms. For more detailed explanation about PNs we refer to [3, 29].

IV. FedNets – Concepts and Examples

FedNet is an ad-hoc federation of networks created for achieving tasks that a group wants to carry out. Constituents of FedNets are PNs, PANs, distributed robotic systems and on board vehicle networks. In principle, FedNets use only a subset of the resources of its constituents and allows each other to access specific services or resources to perform the task.

Figure 2 illustrates an emergency situation where fire fighters, policemen, medical personnel, environmental specialists, civilians etc., spontaneously collaborate in a rescue team. Each individual has a diversity of devices which are part of their PNs, such as sensors, cameras and communication equipments, to assist them in monitoring and observing. By creating a FedNets, each of them will be able to share their devices to enhance their capabilities, e.g. to give the policeman or medical personnel a view of the situation inside a burning building by using helmet-mounted cameras of firemen.

We envisage that various other applications will run on top of the FedNet such as family networks, emergency services for elderly people, battlefield operation, collaboration works in rural area, gaming amongst group of people in proximity, resource sharing applications etc. The design thus has to cope with different applications possibly with different scenarios. It should be formed on purpose when the need for achieving a common task arises or when the opportunity to federate appears, e.g., when PNs or PANs of people with strong common interests detect each other and see opportunities to interact. Depending on the context and applications, FedNets need to be established for a short or long period of time. It is even more challenging since the following aspects need to be considered:

- The dynamics and unpredictable topology
- The mobility of constituent networks and their components
- The heterogeneity of the underlying link technologies
- The large variety of applications and the demands
- The variety of energy, processing and storage constraints of the involved devices
- The lack of infrastructure support
- The need for self-organization and fast localization of devices and services
- The security and privacy of members

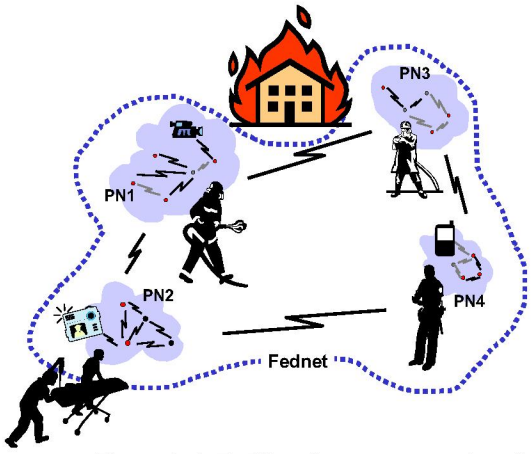

Figure 2. A FedNets for emergency situation

V. Mechanisms

In this section we will discuss several mechanisms that are needed for enabling group networking together with their requirements. Although each mechanism poses special requirements which most likely differ with others, we advocate that in general, mechanisms should have following prerequisites:

- **Autoconfiguration:** Solutions should require a minimal user involvement.

- **User transparency:** The complexity of FedNets mechanisms should be hidden to the users, requiring self-organization.
- **Autonomous:** The operation should not require support from infrastructure as well as other third party.
- **Efficient:** Due to the characteristics of wireless networks and devices, the developed solution should be efficient.
- **Scalable:** The solution must independent of the size of the network.
- **No additional skill to form a FedNet:** Procedures that are needed to establish a FedNets should not require any professional skills from owners as anyone should be able to create a FedNet anytime and anywhere.
- **Providing the security and privacy to the owners:** In every aspect, security and privacy concerns must not be neglected. For example, depending on the context and application, full identity and location should only be revealed after a sufficient level of trust has been established.

A. Network Layer Addressing

Unlike wired networks, addresses of mobile or wireless devices change from time to time. DHCP [10] is the most popular method that is used to assign temporary IP addresses for mobile nodes. However, access to DHCP servers is not always available or reachable. The solution developed by IETF ZeroConf [11] can handle local address configuration without the help of a network administrator. Yet, such protocol relies on the assumption that every node can reach all the others by link layer broadcast or multicast. Nevertheless it is not true in many ad hoc networking cases. Therefore, a different protocol is required for our proposal, which fulfill these requirements:

- **Guarantee the uniqueness of address:** The assigned address should uniquely represent a node, either locally or globally (if possible).
- **Supporting network events:** The addressing scheme should consider mechanism to handle dynamic network events of joining, leaving, partitioning and merging.
- **Integration with global connectivity:** If the global connectivity is available, the autoconfiguration protocol should handle the global addressing in addition to the local addressing.

To interact with other PNs, not all PN devices must obtain IP addresses. Depending on the type of architecture that is used to establish FedNets (explained in Section H), only PN gateways or the devices involved in a FedNet are required to participate in the addressing protocols. Further, a number of address autoconfiguration protocols for MANET like [12-14] have been proposed. From the protocol structure view, some protocols employ centralized assignment where one participant voluntarily acts as a leader to assign a unique address to each new node. Others employ distributed assignment, which are carried out in several ways; tentatively picking a random address and verifying it using Duplicate Address Detection (DAD) mechanism or splitting half of the address blocks of an existing node to be transferred to a new node.

Similarly when a node joins (merging), conflicting addresses is the main problem when two ad hoc clouds merge. As the result, packets destined to a recipient may not be transmitted correctly since another node is currently using a same address. Again, the protocols proposed different strategies to handle this problem. Centralized protocols typically require communication between leaders to detect duplicated addresses, so that only nodes using same addresses need to reconfigure. Some distributed protocols require all nodes in one partition to reconfigure, while others may keep their addresses. In the worst case, all nodes from both partitions have to reconfigure their addresses.

Most IPv6-based protocols proposed integration between local and global addressing. Here, several nodes acting as gateways to the Internet will provide topologically correct network prefixes for other nodes in the ad hoc network. When multiple gateways are present, an efficient method of gateway discovery and selection is needed.

Furthermore, a cross layer optimization technique, like the one proposed in [12], is a good alternative to reduce overhead of the protocol. That is, using information from existing routing protocol traffic to support the addressing protocol and vice versa. To provide flexibility, the integrated scheme should not be bounded to only one routing protocol, but also to other widely used protocols.

One of the major security issues in addressing protocols is Denial of Service (DoS) attacks. Without adequate protection, any device can easily mask itself, join the network and intrude the protocol by sending false information to block the use of certain addresses. While security is still an issue for addressing protocols in wireless ad hoc networks, we notice that only a little progress has been made such in [14]. Furthermore, exposing MAC addresses especially in an unfamiliar network could lead to breach of privacy since they can be used to track the current location of the users.

From our study on various addressing protocols, we observe that each protocol has its own advantages and disadvantages, while trying to achieve a level of optimization in a particular aspect. Further, we believe that the choice of a proper protocol will depend on many factors such as the routing protocol, the size of the network, various metrics such as packet loss, network type – hybrid or standalone, and particularly the applications running on it. Besides, security and privacy issues are left open. We intend to bring them together with investigation of the applicability of those techniques to develop an optimal solution for our FedNets proposal.

B. Naming

Generally, knowing the addresses of shared devices could be sufficient to establish a FedNet. However, since the constituent networks are likely to have a dynamic addressing, knowing the exact IP address of the peers is probably difficult to achieve.

Since FedNets could cover a wide variety of applications, assignment of names may be different depending on the task that the members need to accomplish. Still, we attempt to list all possible requirements for FedNets as follows.

- **Locally unique:** Since FedNets operate in an ad hoc mode, names do not need to be globally unique. However, if the global connectivity is available, resources may have both global and local names.
- **Transient:** Names of users, services or resources can be dynamically changed according to the context and application. For example, resources, files or devices can be based on the task/project.
- **Anonymous:** Names of resources should give no clue about the identity of the owner. However, in some applications indication as to who the owner is may be useful. In the above example, while viewing a camera feed, it is useful for the policeman to know the person who is sending the feed.

Along with the emerging service discovery protocols in the pervasive environments area, different approaches for resource naming have been proposed [15]. Usually, protocols have two kinds of service identifiers: one being user-friendly names and the other being machine friendly names. To provide expressiveness for various services and easiness for introducing new services, protocols like Salutation [16] and Jini [17], define a template for service names and attributes. Like network layer address, names related to resources need also to be unique. Yet, designed for a limited administrative domain such as home networks or enterprise networks, we notify that protocols like mentioned above still require pre-configuration and

professional assistance to assign unique names, especially when the mobility of devices is taken into account. Apple Bonjour [18] is a newly developed protocol to support spontaneous and mobile sharing applications without prior configuration. It uses DNS format to assign a unique name to a device or a service to the local network. Although access to DNS servers is not necessary, yet, Apple Bonjour assumes the existence of multicast or broadcast links to carry out many procedures including verifying the uniqueness of local names. Similar to the address configuration problems, the multi hop nature do not guarantee that each node can be reached through one-hop transmission, thus Bonjour will not work well in the case of multi hop networks. To avoid ambiguity, the uniqueness of the names should be verified at all participating entities across the multi-hop ad hoc network, possibly by using the techniques similar to addressing protocols.

C. Name Resolution

While the naming technique provides a means to identify resources, the name resolution deals with finding the actual address of a given name for invocation of an address like IP number. DNS [19] is a well known name resolution system in the Internet. Dynamic DNS [20] is a modified version of DNS aiming at handling node mobility i.e. update the binding information when the IP address is dynamically assigned to a node. Since the existence of such entities cannot be assumed in FedNets, a new protocol is needed. Besides the general prerequisites explained in the beginning of this section, the resolution protocol should satisfy the following requirements.

- **Timely:** The protocol should react to queries in a timely manner. The node should be aware if the queried named is no longer available, either with notifications or time-out approach.
- **Adapt to changes:** Mapped information about a device name to its location e.g. IP address should be dynamically maintained.

Solutions for ad hoc resolution protocols can be roughly categorized as non-overlay (physical) or overlay based solutions. The former deals with actual physical mapping, while the latter uses logical topology that is not necessarily mapped to the physical topology.

The non-overlay solutions can have a fully-distributed, centralized or hybrid structure. In the fully-distributed structure, when the caching mechanism is not applied, nodes have to flood name queries throughout the network. The node having that name should reply to the querying node returning the IP address of the service. When the caching is applied, nodes exporting services may proactively announce names and IP addresses of services to be cached by other nodes in the network. The advantage of this approach is that the resolution would be faster; however, periodical advertisement of all nodes throughout the network will cause broadcast storm problem and nodes have to allocate their memory space for binding storage. Alternatively, nodes may cache only advertisements from one-hop neighbors. When a node needs a service that is located beyond its physical coverage, it should send queries throughout the network to find the service. Although central entities are no longer available in the ad hoc network, a centralized approach can still be implemented. Using this approach, a node of a PN or a P-PAN should be elected as a leader to store bindings the names and IP addresses of nodes in the and respond to queries. Nevertheless, if this entity suddenly goes down or unreachable, the leader needs to be re-elected and the service registration has to be restarted.

The choice between the centralized and distributed approach will likely depend on the network size. The distributed resolution should work well in small network while the centralized approach should be more suitable for large networks. Besides the network size consideration, the choice will also depend on the underlying protocol being used. The combination of the centralized approach with proactive routing protocols and the decentralized approach with reactive routing protocols will naturally achieve a better efficiency than other combinations. Again, to reduce excessive traffic from resolving algorithms, the cross layering approach will be very useful.

Using the overlay approach, first nodes should build virtual connections on top of the physical network to connect each other. Although it is possible to have a centralized or hybrid structure, the distributed structure is used commonly by protocols like [21]. To join an overlay, a new node should find an existing node to be attached to. Based on the availability of the caching, names can be resolved either by a flooding (if the caching mechanism is not applied) or gossiping (if the caching is applied) technique.

Compared to that of non-overlay, the dependency of underlying protocols such as networking technology (e.g. variants of IEEE 802.11 protocol or Bluetooth) and ad hoc routing (e.g. proactive or reactive routing protocols) makes this P2P solution more flexible to be implemented over heterogeneous networks and devices. Nonetheless, the physical link-independency can also make a protocol inefficient. Following a logical topology, messages from two nearby nodes often have to be routed through some intermediate nodes. Therefore, the key of a good performance is building an effective overlay that takes in to account the physical topology. Typically, a node should continuously monitor states of neighboring nodes and possibly react when some significant changes happen. Again, since the ad hoc network pose a dynamic nature of frequently joining and leaving nodes, keeping the overlay stability and efficiency could be difficult and expensive. For example, a leaving node might cause their neighbors totally separated from the whole network. On other hand, a newly coming node may cause a significant change to the logical topology.

Trade off between two types of solution should be further analyzed. The performance of both types of solution should be fairly compared e.g. by considering different network settings, various routing protocols and several FedNet scenarios. It seems that due to the privacy concern, the distributed structure will be a better option for FedNets name resolution. In this approach, PNs do not necessarily expose their information to the third entity. To increase the efficiency and to get faster results, several 'powerful' devices in a cluster may perform coordination under SMN's control, to store as much useful information as possible from its surroundings.

D. User/Resource/Service Discovery

Like the name resolution protocol, the discovery protocols can be categorized as directory (centralized), directory-less (distributed) or hybrid infrastructure. Similarly, in the directory-less infrastructure, caching mechanisms can be applied fully, partially or not applied at all. From this point of view, the discovery protocol will have similar structure to the protocol presented in Section C. Therefore, in this subsection we will not repeat the explanation given in that section; rather focus on the other related issues.

While the resolution protocol is intended to locate a specific name that relates to a resource, the discovery protocol is intended to locate a generic name that relates to some available resources or services. Therefore, it should cover more advanced search than the resolution such as matching, browsing, searching based on context, etc. Requirements of the protocol are:

- **Integration between user, resource and service discovery:** PNs should not only able to find services and resources but also people in the close proximity.
- **Rich description:** Besides names, the descriptors should be enriched with other contextual information, e.g. location, capability, etc.

- **Accept fuzzy descriptions:** Fuzzy requests should be acceptable since users may not know exactly what are available in the vicinity.
- **Ability to rank information:** To help the user in selecting an optimal service or resource, the system should be able to rank all available services.

The user discovery for FedNets adopt similar concepts to IETF Presence protocols [22] of gaining knowledge about a user; whether he is logging in or last time he was seen. It can be further extended to disclose more information like current activity, location or other contextual information that might be useful to trigger FedNets. Presence protocols strongly rely on servers to cache presence information such as status and contact, and distribute information to interested parties, which again does not exist in the ad hoc networks. Here, interested parties should individually search the network to find others. Usually, a user will announce its presence to an existing community to subsequently get presence information of other users in vicinity. Again, the privacy and security of the users become important considerations for this protocol.

The limitation of wireless devices often hinder proposed ad hoc discovery protocols like [23] to occupy more advanced techniques for user's contentment. For instance, because of limited computational ability and energy, the description of ad hoc services typically cannot be as rich as in the Web protocols. The system cannot handle various types of service and users do not have adequate information to help them in selecting the most appropriate services. As described in Section 2, being composed from a collection of a person's devices, PNs and particularly SMNs would have sufficient capabilities to handle more complex procedures. Expressive service descriptions using XML like the one used by several pervasive protocols can be used to allow a more powerful semantic matching of PN discovery.

Exploiting context information would be useful to enhance the discovery protocol since the initiative of FedNets establishment could be triggered by the context. In the previous example, the policeman PDA may proactively search the camera of a fireman as soon as he arrives at the location. Context information could also be used to rank matched queries before finally returning the results. Since coexisting PNs may produce a large amount of context information by various means, an efficient method needs to be developed to exchange, filter and process this information.

F. Policy and Rules

Policies and rules are needed to guarantee that any security, privacy or any other concerns are not violated deliberately during cooperation. We enlist some of the requirements as follows.

- **Membership management:** The composition of the members and their resources can change over time.
- **Access Control:** Many resources that are shared in a federation can be restricted only to particular members.
- **Fairness:** Cooperation is done by considering fairness among involved members.

Our plan is to develop a template for FedNets profile to define, configure, manage and store this membership information. For example, the amount of members can be limited up to a maxima, or not restricted at all. Different types of membership authority could be developed to manage newly joining members. For instance the authority can be hold by all members, several members or delegated to a single node. Different levels of security could also be developed, e.g. during authentication process the new node must be successfully authenticated with all existing members, only to several members, or in the least level, a successful authentication with one member would be sufficient. Similarly, access to shared devices can be democratic, i.e. some members control the rights, or dictatorial, i.e. one member controls and has exclusive rights to those resources. To provide confidentiality, a mechanism to enforce such policies should be developed including how to give penalty to those violating the defined policy. Next, the term of fairness should be clearly defined, i.e., in what aspect it is applied and what kind of fairness that is going to be applied. For example, in network load problem, does fairness mean every node will have equal load or more powerful nodes will be loaded more than less powerful nodes?

G. FedNet Agent

To help owners in managing a FedNets, we envisage an entity called FedNet agent that is present in each PN. This entity is responsible for all necessary issues in the federation, for instance, being aware of the resources and services that the network is willing to engage in a federation, negotiate and process incoming requests to federate, maintain and enforce the policy rules etc. In this case, the agent should coordinate with SMNs and CMNs to complete the tasks.

We envisage that the agent functionality should not be delegated to an entity residing in an infrastructure (such as a home agent in Mobile IP [24]). As we look at this entity more as functionality than a unit residing in a device, it can also be distributed to several nodes located in several clusters. Next, to achieve multi agent interaction, a protocol is necessary to define common agent communication language (syntax and semantic), a common format for the content of communication and a common ontology, potentially using a similar concept described in [25].

H. Architecture

In this subsection we will describe two possible approaches of building the FedNets architecture.

In the first approach end to end IP connectivity is established between the communicating peers. This requires each personal node to configure a valid local address and search for potential neighbors to interact. Before starting the communication, the personal node should ask its gateway to check the authenticity of such nodes. Subsequently the node may send packets, e.g. to exchange service and context information to those nodes via the gateway.

While in the above approach devices communicate using peer to peer interaction, another way is to assume client server interaction in the service level. Using this approach, it is not necessary to have direct IP connectivity between end nodes. Instead, to bridge the communication to the outside world, gateway nodes may act as service proxies to make personal services available for others and vice versa. To use services from outside a PN, the service proxy in the gateway node forwards the service calls from a client device inside a PN to the external service and sends back replies from that service to the client.

From the security point of view, the second approach seems to offer a better solution since the gateway nodes can control the services that are exported and the ones that are not. Some heavy tasks, e.g. authorization and access control can be done by proxies so that even the weakest node inside a PN can take the support of the proxies and can export its services. However, the drawback of this approach is that the applications may experience a longer delay since the communication between the client and the server should be mediated by the proxies. A combined approach could be a good option to solve this problem. That is, using the first approach to import service from foreign nodes and the second approach to export services to foreign nodes.

J. Cognitive Techniques in FedNets

To provide transparency for users as stated in the general requirements, the system requires context awareness and the ability

of self-organization. As FedNets will be dynamic in composition, configuration and connectivity depending on the time, place and circumstances, the resources required and the partners that owners want to interact with, PNs have to be smart enough to acquire and apply knowledge to learn owner's preferences and to proactively behave accordingly. The cognitive technique thus plays important role for FedNets. Following are required from the cognitive system to support context awareness in FedNets.

- **Uniform context representation:** A uniform and understandable representation is necessary to express heterogeneous context information produced by various devices.
- **Supporting interaction between entities:** To obtain necessary information, PNs should be able to interact to exchange data and access each others services.
- **Ability to filter and manage information:** Since a large amount of information would be produced by internal and external devices, PNs have to filter and manage necessary information to be processed using learning and reasoning techniques.
- **Ability to make rational decisions:** Based on learning activity, PNs should be able to reason, make a rational decision and act upon it accordingly.
- **Ability to receive user interruption:** Although the cognitive technique would help owners to simplify many procedures, still, it has to be able to receive user interruption, e.g. canceling certain automatic actions as results of the learning activity.

Our focus will be on where, when and how cognitive techniques should be applied to hasten FedNets configuration and adaptation process. After that, we need to identify the information that needs to be sensed and the context it consists of. Currently, various types of learning algorithm have been proposed to complete different tasks with different knowledge [27]. For example, some of them are designed to get the past knowledge, e.g. user routine, while others are intended for infer future situation based on the current condition. Therefore, we should be able to decide the algorithm that is suitable for the respective applications. Applying cognitive techniques to FedNets seems to be more complicated than in PNs [28], since the decision is influenced by others' devices which affects personal devices too. Policy and rules of each federation should be taken into account in determining the final decision.

VI. Conclusions

We have presented here the issues that are to be addressed for enabling co-operative group communications. We started from the PNs and enhanced it to a FedNets to support group communications while keeping the user-centric nature intact. While defining requirements that will be needed for this purpose, we notice that different techniques may serve as potential alternatives for FedNets solution. After examining and analyzing those alternatives with different usage scenarios, we aim at further development and implementation of the protocols.

We think that in the near future secure user-centric networks are the order of the day. In turn, they will have to interact with similar networks forming social networking in the form of on-demand, ad hoc, and opportunistic group communications like FedNets.

ACKNOWLEDGMENTS

This research is funded partially by Schlumberger Foundation through Faculty for the Future Program and EU funded Magnet Beyond Project. The thoughts presented in this paper however do not necessarily reflect the views of Magnet Beyond.

References

[1] Niemegeers I. and Heemstra de Groot (editors), S. Personal Wireless Communications. Proceedings IFIP TC6 9th International Conference, PWC 2004, 478 pages, Delft, the Netherlands, September 21-23, 2004, Springer, ISBN 3-540-23162-5.

[2] Niemegeers IGMM and Heemstra-de Groot SM, FEDNETS: Context-aware ad-hoc network federations, *Wireless Personal Communications, Vol. 33, Springer 2005, ISSN 0929-6212, pp. 305-318.*

[3] Magnet Beyond Project. http://www.ist-magnet.org

[4] Kravets, R. et at. Cooperative Approach to User Mobility. *ACM Computer Communications Review*, Volume 31, Pages 57-69, Oct, 2001.

[5] Edwards,N.J. An ANSA Analysis of Open Dependable Distributed Computing. *ANSA*, Cambridge, UK, 1994.

[6] Furmento, N. et al. Building *Computational Communities* from Federated Resources. In R. Sakellariou et al. (eds.), Euro-Par 2001, *LNCS 2150, Springer Verlag, 2001*, pp.855-863.

[7] AuYoung, A. et al. Resource Allocation in Federated Distributed Computing Infrastructures. *In Procs of the 1st Workshop on Operating System and Architectural Support for the On-Demand IT.* Oct. 2004.

[8] Balazinska, M. et al. Contract-Based Load management in Federated Distributed Systems. *MIT Computer Science and Artificial Intelligence Lab*, nms.lcs.mit.edu/projects/medusa, 2003.

[9] Fox, G., and Pierce, M. Federated Grids and their Security. Draft 0.4, eprints.ecs.soton.ac.uk/archive, 2003.

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

[11] Guttman, E. Autoconfiguration for IP Networking: Enabling Local Communication. IEEE Internet Computing, June 2001.

[12] Weniger, K. PACMAN: Passive Autoconfiguration for Mobile Ad hoc Networks. In IEEE JSAC, Dec.2004.

[13] S. Nesargi and R. Prakash, "MANETconf: Configuration of hosts in a mobile ad hoc network," *In Proc. of INFOCOM*, 2002.

[14] P. Wang, et.al. "Secure Address Auto-con.guration for Mobile Ad Hoc Networks," mobiquitous, 2005.

[15] Zhu, et al. "Service Discovery in Pervasive Computing Environments," IEEE Pervasive Computing, vol. 4, pp. 81-90, 2005.

[16] http://www.salutation.org

[17] http://www.jini.org

[18] http://images.apple.com/macosx/pdf/MacOSX_Bonjour_TB.pdf

[19] Mockapetris, P. Domain names – concepts and facilities. *IETF RFC 1034*, November 1987.

[20] Vixie, P., et al. Dynamic Updates in the Domain Name System (DNS UPDATE). *IETF RFC 2136*, April 1997

[21] Doval, D. and O'Mahony, D. Nom: Resource Location and Discovery for Ad Hoc Mobile Networks. In Procs of Medhoc –Net, 2002.

[22] M. Day, et al. Instant Messaging/Presence Protocol Requirements. IETF RFC 2779, February 2000.

[23] Ververidis, C., et al. Routing Layer Support for Service Discovery in Mobile Ad Hoc Networks. In the Procs of Percom Workshop 2005.

[24] Perkins, C., Woolf, B., and Alpert, S. Mobile IP Design Principles and Practices. Prentice Hall PTR, 1998.

[25] http://www.fipa.org/repository/aclspecs.html

[26] Jacobsson. M., et al. Architectural Solutions for Foreign Communication in Personal Networks. Med-Hoc-Net'06 June, 2006.

[27] T. Dietterich and P. Langley. Machine learning for cognitive networks: Technology assessment and research challenges. Tech. report, Oregon State University, May 2003.

[28] Y Wu and I Niemegeers, "A Cognitive Architecture for Personal Networks", to appear in the First IFIP Autonomic Networking Conference, Paris, France, 2006.

[29] R. V. Prasad, Martin Jacobsson, Sonia Heemstra de Groot, Anthony Lo, Ignas Niemegeers, "Architectures for Communication in Personal Networks", PerNets, Mobiquitous, SanJose, 2006.