Towards Self-organising Personal Networks

Mikko Alutoin and Sami Lehtonen
VTT
P.O.Box 1202
FIN-02044 VTT, Finland
mikko.alutoin@vtt.fi

Jeroen Hoebeke, Gerry Holderbeke and Ingrid Moerman
Ghent University - IMEC
Sint-Pietersnieuwstraat 41
B-9000 Ghent, Belgium
jeroen.hoebeke@intec.ugent.be

Luis Sanchez and Jorge Lanza
University of Cantabria
Avda los Castros s/n
Santander, Spain
lsanchez@tlmat.unican.es

Wajdi Louati and Djamal Zeghlache
GET-INT
rue Charles Fourier
91011 Evry, France
djamal.zeghlache@int-evry.fr

ABSTRACT

Personal Network (PN) is an emerging concept which combines pervasive computing and strong user focus. The idea is that the user's personal devices organise themselves in a secure and private personal network transparently of their geographical location. This paper studies a PN architecture where devices form *clusters* using shared key cryptography over short range radio links (or a local area network) and where the otherwise isolated clusters are interconnected over the IP infrastructure using dynamic tunnelling. True self-organisation of the PN requires establishing distributed consensus via a voting algorithm. Remarks on the linkage between the different voting algorithms and the ad hoc routing schemes are provided.

Categories & Subject Descriptors:

C. Computer Systems Organization
C.2 COMPUTER-COMMUNICATION NETWORKS
C.2.1 Network Architecture and Design
Subject descriptors: Wireless communication, Distributed networks

General Terms: Design, Security

Keywords: Personal Network, ad hoc routing, self-organisation

1. INTRODUCTION

Intelligence is being embedded everywhere these days in order to make our lives easier and more secure. Mobile phones are old news, as biosensors, RFID tags and handheld digital television are paving the way to the new era of pervasive computing. We are offered access to more and more information from our body as well as our surroundings. Some of the devices, which offer us this information, are portable, such as mobile phones or heart rate monitors. Others are more stationary and not always nearby. Nevertheless, one desires to communicate with these devices transparently of their location. From the user's point of view these personal devices form a Personal Network (PN) which is a new paradigm used to describe pervasive computing with strong focus on the person. The devices in the PN are referred to as Personal Nodes. Privacy and security are fundamental properties of the PN as well as ability to self-organise in ad hoc manner.

The topology of the PN is affected by mobility, devices running out of battery or being switched off. All the time the user should be presented with an up to date view of the PN, its capabilities, and services.

This paper discusses the PN self-organisation from the network layer point of view. The paper describes how personal nodes form clusters and how these clusters are interconnected using an IP network, such as the Internet. In Section 3 the requirements for PN addressing are described. In addition, we address cluster self-configuration and provide motivation for the cluster formation mechanism described in Section 4. In Section 5 intra-cluster routing is dealt with in more detail. Section 6 describes how clusters interconnect via the fixed IP infrastructure and Section 7 gives an idea about how cluster mobility is handled. Conclusions and further work are given in Section 8.

2. THE NETWORK ARCHITECTURE

The work presented in this paper is a continuation of previous work [1], which outlined the PN architecture developed in the IST MAGNET project [2] (see Figure 1 below).

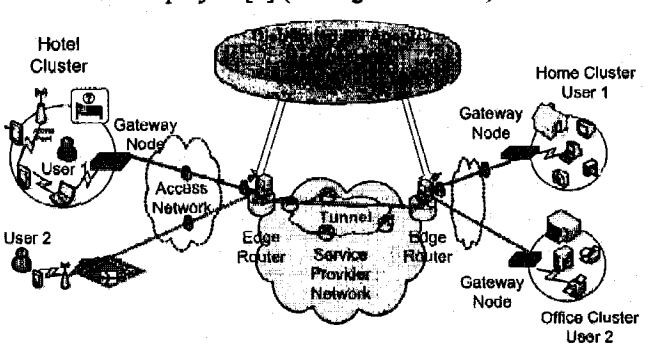

Figure 1. Clusters organised as personal networks.

The basic idea is that it is the network layer (i.e. IP) which glues the PN together. The personal nodes are organised as

DIN'05, September 2, 2005, Cologne, Germany.

clusters. If two personal nodes can communicate using a route that does not incorporate any non-personal nodes, then the nodes belong to the same cluster. A cluster can be a network at home, consisting of a PC, DVD recorder, refrigerator, burglar alarm, etc. Another cluster could be formed by the electronic devices in the user's vehicle. There is also a special cluster named Private Personal Area Network (P-PAN) which can be thought of as a wireless bubble around the user. It consists of portable devices which all have at least one radio interface, such as WLAN, Bluetooth or some other kind of WPAN interface.

The clusters are interconnected over the Internet using dynamic tunnelling. The gateway node is a special personal node via which a cluster has access to other clusters. The edge router, as depicted in Figure 1, is on the provider edge and it can alleviate the burden on the gateway node, provided that a sufficient trust relation can be established between the gateway node and the edge router [3]. The distributed PN Agent Management Framework keeps track of the clusters as they roam between network access points. Security and privacy between any two personal nodes is achieved via standard encryption and authentication mechanisms leveraging a pair-wise shared key. The encryption and authentication can be done either on a hop-by-hop basis (in link or network layer) or end-to-end in network layer. The nodes negotiate the long-term pair-wise shared key via a procedure called *imprinting* which is out of the scope of this paper, but is outlined in [4].

3. ADDRESSING IN THE PN

The network layer address of a personal node should be as static as possible. This is because changing the IP address always results in breaking the ongoing TCP connections. This is a well-known problem which has been tackled by multiple research initiatives over the last decade [5]. In the proposed PN architecture, it is the PN routing protocol together with a PN Agent Management Framework that handles mobility. The address of the personal node remains unchanged as the user roams from one network access point to another. When used like this, the IP address is more a host identifier than an interface identifier, as it is in traditional internetworking. In order to distinguish this difference, the IP address that is used for PN communications is referred to as PN address. A PN node has always exactly one PN address, even if it may have multiple network interfaces of which each can have multiple IP addresses. IPv6 is selected to be used for the PN plane communications because of its large address space.

3.1 PN Address Autoconfiguration

The self-configuration of the PN starts with PN address autoconfiguration for which there are two options: stateful autoconfiguration and stateless autoconfiguration. The challenge in the latter option is how to avoid duplicate addresses whereas the former option introduces a single point of failure. Thus, the stateless autoconfiguration would be a more viable solution, if the problem of duplicate addresses could be handled efficiently and reliably. The standard IPv6 stateless address autoconfiguration, developed for fixed networks, starts by generating a link-local address. It is generated by taking a well known prefix and appending a link dependent unique token called Interface ID to it [6]. The 64 bit Interface ID can be mapped from a 48 bit MAC address or it can be a random ID. Before the address can be used, its uniqueness on the link must be ensured through the Duplicate Address Detection (DAD) message exchange [7, 8].

There are a couple of issues in the standard IPv6 stateless address autoconfiguration, which deserve attention with respect to the proposed PN architecture. Firstly, the scheme is based on the notion of the well-defined link and IP subnet. These do not exist in multi-hop mobile ad hoc environment at all. As the collection of stations within the same radio coverage change continuously, DAD should also be performed frequently. The lack of clear subnets indicates that the scope of DAD should be at least the whole cluster if not the whole PN. Having a unique address prefix for PN nodes within each cluster (i.e. cluster prefix) would limit the scope of DAD inside the cluster, but would hinder merging of clusters when they are collocated. Therefore we have specified that the PN address consists of a concatenation of a 64 bit PN prefix and a 64 bit Interface ID which is mapped from a MAC address using the IEEE EUI-64 format [6]. This guarantees that the generated Interface ID is globally unique, without DAD. Each personal node can generate the Interface ID part of the PN address in isolation, but the PN prefix is same for all nodes in the PN.

Three options exist for PN prefix assignment: it can be statically configured (e.g. during the imprinting procedure [4]), it can be assigned by the PN Agent, or it can be agreed upon dynamically using a voting algorithm. The last option resembles the well known consensus problem [9] for which practical solutions are known. However, unlike in the classical consensus problem, the personal nodes might not know which other nodes are part of the decision making process. This variation of the problem is referred to as Consensus with Unknown Participants (CUP) [10]. It is for further study to find a practical voting algorithm that would require minimum a priori knowledge and at the same time tolerate discontinuity which can occur, e.g., due to cluster partitioning. It has been shown [10] that reaching consensus in a strongly connected cluster is substantially easier than in a cluster that allows asymmetric connections. To this end, the next section presents beacons to keep clusters strongly connected.

4. CLUSTER FORMATION

After having negotiated the long-term pair-wise shared key and a unique device identifier during the imprinting procedure [4], two personal nodes have all necessary knowledge to discover, identify and authenticate each other. Physically collocated personal nodes organise themselves in

clusters, i.e., strongly connected groups of personal nodes that can communicate with each other without using any non-personal node.

4.1 Neighbour discovery

In order to discover each other, the personal nodes broadcast periodic beacon messages on all network interfaces. The beacon interval could be dynamically adapted depending on the node context (e.g. mobility rate of the node or the cluster, remaining battery, etc.). The beacons are not encrypted and they contain the aforementioned unique device identifier of the sending node so that other nodes will know which long-term pair-wise key to use in order to establish a short-term security relationship to the newly discovered neighbour.

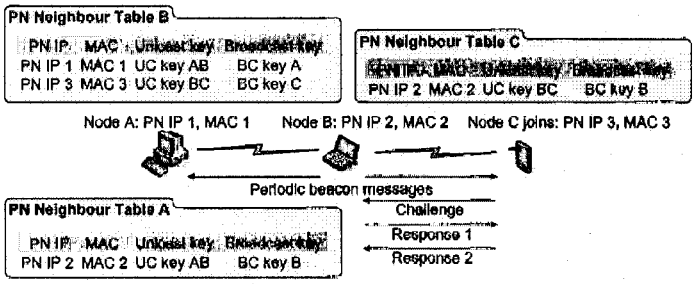

Figure 2. Cluster formation through three-way handshake.

Upon the reception of a beacon, the node will check whether an entry for the peer is found in the neighbour table. If so the entry will be updated by reinitializing the expiration timer. If the neighbour relationship does not exist, then the node initiates a three-way handshake procedure consisting of a mutual challenge-response authentication based on the pair-wise shared key. This handshake must at least ensure the authenticity and presence (to avoid replay) of both parties. Moreover, the process is used to exchange additional information, such as the derivation of a temporary link key (to avoid the use of main keys in all further communication) and exchange of per-node broadcast keys. After completion of the handshake, the personal nodes have established a trusted link between them. As this process is executed by all neighbouring personal nodes, the result is a cluster of trusted personal nodes. Periodic beaconing still continues, in order to detect additional personal nodes and link breaks to existing neighbours in the absence of link break detection mechanisms in the link layer. This beaconing process is also used to inform the ad hoc routing protocol about the immediate neighbours so that the mechanisms in the routing protocol in charge of this aspect can be disabled. The use of beacons might seem as an overhead, but most ad hoc routing protocols use beacons (in absence of more efficient link detection mechanisms in the link layer). In our solution, the beacons are just omitted from the ad hoc routing protocol and implemented on top of the link layer and not in the network layer.

4.2 Election of Cluster Master

The neighbour discovery mechanism resolves the problem of forming a secure cluster. In addition, the neighbour discovery feeds the routing process so that multi-hop intra-cluster routes can be built with either a reactive or proactive ad hoc routing protocol. Nevertheless, the cluster self-organisation involves also other types of functions which can not be carried out in a peer-to-peer manner, but require master election. These include, for example, the election of the Service Management Node (SMN) which maintains a list of services running within the cluster [11]. The algorithm that is used for SMN election is described in [12]. The algorithm depends on secure cluster wide broadcast which is enabled by the proactive cluster formation.

5. INTRA-CLUSTER ROUTING

Once trusted links have been established between neighbouring personal nodes, secure communication can take place within the cluster. As a cluster is an overlay network that uses its own internal IP addressing scheme and that comprises both wired and wireless communication interfaces, traditional routing mechanisms are not adequate to provide connectivity. Also, they assume subnet-based addressing and having each interface assigned one IP address, which does not fit our requirements. Additionally, these mechanisms are not able to deal with dynamics such as cluster splitting and merging. Therefore, as existing techniques are not adequate, a solution based on ad hoc routing techniques is proposed that meets the following requirements:

- Integration on top and joint optimisation with the underlying neighbour discovery mechanisms
- Low latency with limited protocol overhead
- Flexible extension to an efficient (low overhead, low latency) PN routing solution, which implies efficient propagation of gateway information within clusters
- Easy incorporation of QoS information

Based on the above requirements, we propose the use of a proactive ad hoc routing protocol, adapted to the specific characteristics of the PN environment. It fits the cluster formation process perfectly, as it propagates route updates only upon the detection of new links and/or link breaks (due to mobility or nodes being switched on or off). Furthermore, low latency is an inherent characteristic of proactive routing and gateway information can be easily propagated to all nodes in the cluster. Moreover, proactive routing allows wide collection of voting algorithms, because it provides a complete list of cluster members as a by-product. From the PN concept, it can be assumed that neither cluster size nor context will cause scalability problems. A roaming P-PAN is a small-size, battery-powered, network with a slowly changing composition and low internal mobility. The other, larger clusters mainly consist of static devices with both wired and wireless interfaces often connected to a power supply. These characteristics can be exploited to further reduce the overhead incurred by proactive protocols. Finally, all route updates are encrypted using the per-node broadcast key. The result of both the cluster formation process and the

intra-cluster routing protocol, is a self-organising and -maintaining network, in which each personal node has a secured proactive route to all other nodes within the cluster and a default route to gateway nodes providing access to remote clusters. Note that these concepts only apply to communication in the PN plane, characterised by the use of PN addresses, which is separated from traditional IP communication based upon IP (non-PN) addresses. Therefore, all other communication, e.g., connecting to a server in the Internet, uses standard IP routing mechanisms (see Figure 3).

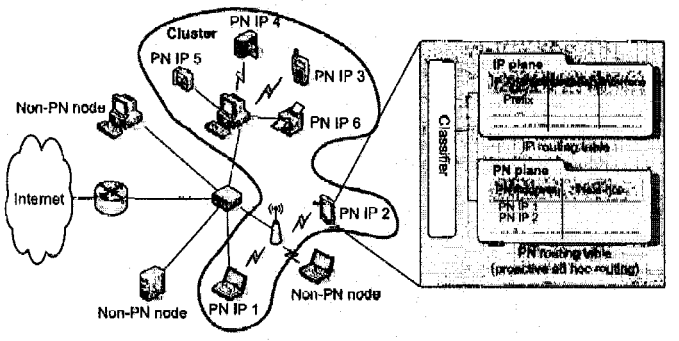

Figure 3. Cluster formation and IP plane vs. PN plane routing.

5.1 Cluster Wide Multicast

As mentioned earlier, SMN election depends on cluster wide multicast/broadcast. Link layer broadcast does not always reach all nodes within the cluster and therefore group communications need to be supported on higher protocol layers. Ad hoc routing protocols concentrate on unicast routes and do not usually support multicast/broadcast in the network layer which would be convenient for the application developers. In order to implement cluster wide broadcast in the network layer, we have defined a multicast address format to be used in the personal network. It consists of a triplet of a special PN prefix, multicast group identifier and the scope of the multicast (e.g. cluster wide vs. PN wide scope). The actual flooding algorithm, used for cluster wide broadcasting, is for further work. So far the identified options are a unicast based flooding algorithm and a flooding algorithm utilising link layer broadcasting. In both cases, the neighbour table can be exploited to make the flooding more efficient.

6. INTER-CLUSTER ROUTING

After cluster formation, the clusters gain access to the infrastructure through the gateway nodes, locate each other and establish secure tunnels between each other. This results in a virtual overlay network that encompasses all the devices of the person (i.e. the Personal Network). Low latency deployment and management, transparently to the end user, are of prime importance in order for the PN concept to succeed. It is advantageous not only to offload complexity from the user, but also to make the protocols implementation in the end user devices as lightweight as possible. This is achieved by shifting complexity to the service providers. Assuming a trust relationship can be established between users and providers, the deployment and management of the inter-cluster overlay can be outsourced to a service provider. To this end, edge routers have been introduced. These are powerful nodes that can reside anywhere in the access network. The edge routers provide the virtual links (i.e. tunnels) which the clusters use for inter-cluster connectivity. The cluster functionality is then reduced and consists only of discovery of the edge router, establishing a secure communication path to the edge router, and registering with the edge router. All this is handled by the gateway node(s) which the other nodes locate via the intra-cluster routing protocol. The gateway in turn discovers the edge router via a DHCP message exchange with the network access point, for example.

It is important to note that the PN concept can also be realised in the absence of the edge routers. In that case it is the gateway node that provides the virtual links between the clusters. Whether edge routers are used or not, a prerequisite to continue the PN formation process is the availability of cluster location information (i.e. the Internet address of the edge router or the gateway node). The distributed *PN agent management framework* (see Figure 1) stores this information. After a successful registration of a new cluster to the PN agent management framework, the corresponding edge router will install a Virtual Router (VR) instance for the specific PN that the cluster belongs to. When proactive intra-cluster routing is used, the gateway node can provide the edge router with the PN addresses of all the personal nodes within the cluster. These addresses are stored by the VR. The VR establishes tunnels to its peers and exchanges routing information with them. As a result, each VR has a list of all nodes belonging to that PN and it knows the virtual link through which each node can be reached. Upon changes in the composition (not the topology!) of a cluster, the gateway node will send a route update to its VR, upon which the VRs update and exchange the new routing information amongst each other. The only overhead for the clusters to run the proactive intra-cluster routing protocol within the limited size cluster network.

7. SESSION CONTINUITY

Session continuity must be ensured while a cluster roams between edge routers. Assume that a P-PAN has connectivity to an edge router through a gateway node and that a communication session with a remote personal node is ongoing, as shown in Figure 4 below. Due to mobility, the P-PAN looses its connectivity to the serving edge router. As soon as the P-PAN has registered itself to an alternative edge router, a new VR is installed in this router and a dynamic tunnel is established between the new and the remote edge router. Once the routing information has been exchanged, over the newly created virtual link, communication can continue. As an internal PN addressing scheme is used, the ongoing communication session will not break, but will only

experience a short delay (depending on the time to regain access and the time to setup the new virtual link). The edge routers can assist session continuity by buffering P-PAN terminated pending packets and fast forwarding context information.

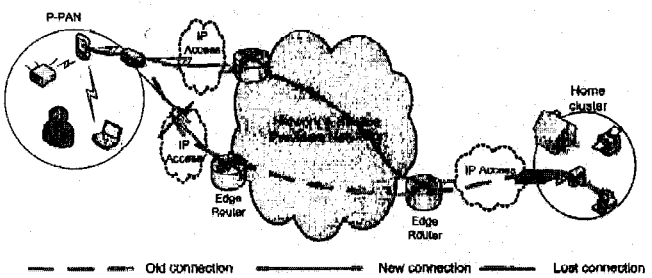

Figure 4. Mobility scenario.

8. CONCLUSIONS AND FUTURE WORK

Self-organisation and mobility management are key capabilities of Personal Networks (PN). This paper outlines an adaptive PN as an overlay network on top of the Internet. It is explained how personal nodes organise themselves in clusters and how these clusters remain interconnected over the Internet. The idea of a proactive cluster formation protocol for building secure clusters is put forward in this paper. The protocol consists of neighbour discovery and authentication using pair-wise shared keys. The cluster formation protocol removes the security concerns from the intra-cluster routing protocol.

When it comes to the PN self-organisation a voting algorithm can be used to reach consensus. It is anticipated that a proactive intra-cluster routing protocol allows a wider collection of voting algorithms than a reactive one, because it provides a list of cluster nodes as a by-product. This in turn restores the self-organisation problem to the classical consensus problem for which many practical solutions are known. If a reactive intra-cluster routing protocol is used instead, then the participants of the voting process are unknown to the triggering process and need to be therefore determined during the execution of the algorithm. This variation of the consensus problem is referred to as Consensus with Unknown Participants (CUP). The CUP problem has not been studied extensively. It is for further work to find viable voting algorithms to be used with both proactive and reactive intra-cluster routing as well as analyse their performance and their effect on the stability of the system.

ACKNOWLEDGMENTS

This work was mainly conducted in the IST MAGNET project (IST 507102). The authors would like to thank the members of the project.

REFERENCES

[1] IST MAGNET Project, "A Network Architecture for Personal Networks", To be published in the Proceedings of IST Mobile and Wireless Communications Summit, 19-23 June 2005.

[2] IST MAGNET project, http://www.ist-magnet.org/

[3] IST MAGNET Project, "Networking in Personal Networks", To be published in the Workshop on Applications and Services in Wireless Networks (ASWN 2005), June 29th - July 1st 2005.

[4] IST MAGNET Project, Deliverable 4.3.2, "Final version of the Network-Level Security Architecture Specification", http://www.ist-magnet.org/publications.html#WP4, Feb. 2005.

[5] Wesley M. Eddy, "At What Layer Does Mobility Belong?", IEEE Communications Magazine, Vol. 42, Issue 10, pp. 155-159, October 2004.

[6] R. Hinden, S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", IETF RFC 3513, http://www.ietf.org/rfc/rfc3513.txt, April, 2003.

[7] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", IETF RFC 2461, http://www.ietf.org/rfc/rfc2461.txt, Dec. 1998.

[8] S. Thomson, T. Narter, "IPv6 Stateless Address Autoconfiguration", IETF RFC 2462, http://www.ietf.org/rfc/rfc2462.txt, Dec. 1998.

[9] Michael J. Fischer, "The Consensus Problem in Unreliable Distributed Systems (a Brief Survey), In M. Karpinsky, editor, Foundations of Computation Theory, Vol. 158 of Lecture Notes in Computer Science, pp. 127-140, Springer-Verlag, 1983.

[10] David Cavin, Yoav Sasson, André Schiper, "Consensus with unknown participants or fundamental self-organization", Third International Conference on Ad hoc Networks and Wireless (ADHOC-NOW 2004), Vancouver, 22-24 July 2004.

[11] IST MAGNET project, Deliverable 2.2.1, "Resource and Service Discovery: PN Solutions", http://www.ist-magnet.org/publications.html#WP2, Dec. 2004.

[12] IST MAGNET project, "Self-organization and mobility in Personal Networks", To be published in the Symposium on Wireless Personal Multimedia Communications (WPMC) 2005, Aalborg, Denmark, Sep. 2005.

Towards self-organising personal networks

Full text Pdf (1.02 MB)

Source **International Conference on Mobile Computing and Networking** archive
Proceedings of the 1st ACM workshop on Dynamic interconnection of networks table of conte
Cologne, Germany
SESSION: Selfconfiguration of interconnecting networks table of contents
Pages: 12 - 16
Year of Publication: 2005
ISBN:1-59593-144-9

Authors
Mikko Alutoin VTT, Finland
Sami Lehtonen VTT, Finland
Jeroen Hoebeke Ghent University - IMEC, Ghent, Belgium
Gerry Holderbeke Ghent University - IMEC, Ghent, Belgium
Ingrid Moerman Ghent University - IMEC, Ghent, Belgium
Luis Sanchez University of Cantabria, Santander, Spain
Jorge Lanza University of Cantabria, Santander, Spain
Wajdi Louati GET-INT, Evry, France
Djamal Zeghlache GET-INT, Evry, France

Sponsors ACM: Association for Computing Machinery
SIGMOBILE: ACM Special Interest Group on Mobility of Systems, Users, Data and Computing

Publisher ACM Press New York, NY, USA

ABSTRACT

Personal Network (PN) is an emerging concept which combines pervasive computing and strong user focus. The idea is that the user's personal devices organise themselves in a secure and private personal network transparently of their geographical location. This paper studies a PN architecture where devices form clusters using shared key cryptography over short range radio links (or a local area network) and where the otherwise isolated clusters are interconnected over the IP infrastructure using dynamic tunnelling. True self-organisation of the PN requires establishing distributed consensus via a voting algorithm. Remarks on the linkage between the different voting algorithms and the ad hoc routing schemes are provided.

↑ REFERENCES

Note: BCR errors may be found in this Reference List extracted from the full text article. ACM has opted to expose the complete List rather than only correct and linked references.

1 IST MAGNET Project, "A Network Architecture for Personal Networks", To be published in the Proceedings of IST Mobile and Wireless Communications Summit, 19-23 June 2005.

2 IST MAGNET project, http://www.ist-magnet.org/

3 IST MAGNET Project, "Networking in Personal Networks", To be published in the Workshop on Applications and Services in Wireless Networks (ASWN 2005), June 29th - July 1st 2005.

4 IST MAGNET Project, Deliverable 4.3.2, "Final version of the Network-Level Security Architecture Specification", http://www.ist-magnet.org/publications.html#WP4, Feb. 2005.

5 Wesley M. Eddy, "At What Layer Does Mobility Belong?", IEEE Communications Magazine, Vol. 42, Issue 10, pp. 155-159, October 2004.

6 R. Hinden, S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", IETF RFC 3513, http://www.ietf.org/rfc/rfc3513.txt, April, 2003.

7 T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", IETF RFC 2461, http://www.ietf.org/rfc/rfc2461.txt, Dec. 1998.

8 S. Thomson, T. Narter, "IPv6 Stateless Address Autoconfiguration", IETF RFC 2462, http://www.ietf.org/rfc/rfc2462.txt, Dec. 1998.

9 Michael J. Fischer, "The Consensus Problem in Unreliable Distributed Systems (a Brief Survey), In M. Karpinsky, editor, Foundations of Computation Theory, Vol. 158 of Lecture Notes in Computer Science, pp. 127-140, Springer-Verlag, 1983.

10 David Cavin, Yoav Sasson, André Schiper, "Consensus with unknown participants or fundamental self-organization", Third International Conference on Ad hoc Networks and Wireless (ADHOC-NOW 2004), Vancouver, 22-24 July 2004.

11 IST MAGNET project, Deliverable 2.2.1, "Resource and Service Discovery: PN Solutions", http://www.ist-magnet.org/publications.html#WP2, Dec. 2004.

12 IST MAGNET project, "Self-organization and mobility in Personal Networks", To be published in the Symposium on Wireless Personal Multimedia Communications (WPMC) 2005, Aalborg, Denmark, Sep. 2005.

↑ INDEX TERMS

Primary Classification:

C. Computer Systems Organization

↳ **C.2** COMPUTER-COMMUNICATION NETWORKS

↳ **C.2.1** Network Architecture and Design

↳ **Subjects:** Wireless communication

Additional Classification:

C. Computer Systems Organization

↳ **C.2** COMPUTER-COMMUNICATION NETWORKS

↳ **C.2.1** Network Architecture and Design

↳ **Subjects:** Distributed networks

General Terms: