Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 9, September 2014, pg.148 – 156

RESEARCH ARTICLE

A SECURE PROTOCOL FOR IMPULSIVE WIRELESS ADHOC NETWORK

Sana Shireen Ismail, Research Scholar, G.Narayanamma Institute of Technology & Science

V. Usha, Assistant Professor, G.Narayanamma Institute of Technology & Science

Abstract: An ad hoc network is a wireless network that is of self configuring and self governing network which transfers the data from one node to another node without any infrastructure. The data transmission can be done by using some of the routing protocols securely without any data loss. In this paper we develop a secure protocol for spontaneous wireless ad hoc network which contains a balanced scheme and trust between the nodes in order to exchange the secret keys that are used to encrypt the data and exchange the information securely. We also propose to develop the network and sharing the resources in devices with limited licensed resources. Method for network creation stage is detailed and communication, protocol messages and network management are explained. Our protocol has been implemented in order to test the protocol procedure and performance.

1. Introduction

In recent years the wireless network technology has a rapid growth in the field of communication. The growth is mainly due to mobility offered to the users, providing an easy access of information at any time, easy deployment. In order to communicate with large numbers in different places simultaneously sharing resources, services and computing time. The network management should be transparent in order to communicate securely. An impulsive network is a special type of ad hoc networks usually does not have any dependence

on centralized administration. An impulsive network can be a wired or wireless. In this paper, we mainly deal with a wireless impulsive network for the integration of services and devices in the same environment. We use impulsive networks in the PDAs, mobile phones, laptops and many more wireless devices which use a lightweight protocol, manage new methods to control and integrate them.

Configuration services in impulsive networks depend significantly on network size, the nature of participating nodes, running applications. An impulsive network usually performs tasks based on user identification, authorization, address assignment, name service, operation and safety methods in order to define a efficient and user friendly security, mechanism. Security should be based on required confidentiality, node cooperation, anonymity and privacy. Generally exchanging pictures between two friends require less security than exchanging confidential document between two organizations. Energy constraints, node variability and node authorization in Manet, key exchange mechanism for node authorization and user authentication can be achieved by impulsive network. The literature shows a several secure methods such as pre distribution key algorithms, symmetric and asymmetric algorithms, intermediate node methods and hybrid methods. A secure impulsive network protocol is based on trust that provides authenticity, integrity checking and privacy. This paper proposes and establishes a secure self configured environment for data distribution, resources and services sharing among the users. The network management is also distributed in an impulsive method. In this method an asymmetric cryptography usually contain a public private key pair for node identification where as symmetric cryptography is used to exchange a session key between nodes.

The rest of the paper is organized as follows: section 2 presents the related work on impulsive network and shows the well known security mechanisms that can be applied to them. Section 3 describes how an impulsive network can be created with a network overview how a new node joins the network and discovers the services. Section 4 describes the how the impulsive network implementation has been done which explains all the operations performed. Section 5 shows the performance analysis of impulsive network and section 6 describes the conclusion.

2. Related Work

In Latakoski[1] explain a communication architecture concept for impulsive systems, integrating and application level spontaneous group communication and adhoc network together. Liu [2] showed how network nodes can automatically support and cooperate with each other in a peer to peer manner to quickly discover and reconfigure any services available in adaptability for monitoring the relief. Back storm [3] developed the first real spontaneous network that offers the services dynamically. Untz [4] propose a light weight protocol and efficient inter connection protocol suitable for spontaneous edge networks. Fenney [5] presented a prototype implementation of an interconnection node for impulsive edge network's. Danzeisan [6] apply the regular security mechanism used in a wireless LAN's available by default in IEEE 802.11. Rekimolo [7] introduced the concept of synchronous user operation, described a user interface technique for establishing network connection between digital devices. Deal with multiple over

lapping connection requests by detecting collision situations and ensure network security by exchange public key information upon establishing a connection. Diffie hellman [8] introduced public keys are used to calculate a shared secret session key for encrypted communication.

3. Secure Impulsive Network

3.1 Network Overview:

Impulsive protocol helps in the creation of nodes, management and decentralized impulsive network with integration of different devices like PDA's, mobiles etc. Cooperation between the devices allows provision and access to different services such as group chats, collaboration in data delivery, security etc. The network members and services vary because devices are free to join or leave the network.

Joining Procedure:

This method explains the joining of a new node in the network. It is described as an algorithm:

Step 1: Start and Generate a Network Key

Step 2: Is there any network Connection,

If Yes Go To Step3 Else

Go To Step 2

Step 3: Exchange Identity Card

Step 4: Authentication and session key agreement

Step 5: Agree transmission Protocols and speed

If Yes Go To Step 6

Else Go To Step 2

Step 6: IP assignment

Step 7: IP Duplication

If Yes Go To Step 2

If NO End the process

At First a network key should be generated for a new network. If there is any new network, an Identity Card (ID card) exchange should be done between the node that join the network. Then an authentication and session key agreement is given to the node that wants to join the network. If the node is being trusted an access for the authentication and session key

agreement is done and IP address is assigned to that node. If the node is not trusted then it looks for another trusted network. If the IP address allotted is a unique then it is confirmed that a new node has been joined in the network and if there is any IP duplication then the node is not been trusted and it checks for a other network that allows to join the network.

3.2 Service Discovery:

The services between the nodes and network can be discovered by web services description language. A user node can ask other devices in the network in order to know available services. If there is any trusted agreement, then the nodes are allowed to access and share the data between the two nodes. The nodes are automatically integrated and used in the network and maintenance, management of these nodes is complex matter.

3.3 Establishing a trusted Chain and changing the Trust Level:

There are two trust levels in the system If a node A trusts or does not trust another node B but due to software application installed node B has to trust the node A when it receives an Identity Card (IDC) from node B. There is a true relationship and the trust level is an asymmetric. The other system is if the node A did not have trust level with the node B directly, then node A trusts node C and node C trust node B, then the node A may trust node B based on mutual relationship. If there is no trust in any node, then the trust chain does not exist.

4. Network Creation

In the network formation and implementation, first a network should be created and the nodes are to be joined. And the impulsive approach is used to apply for the nodes to provide security and that approach discovers the authorized nodes with a Logical Identity (IDC) and at last a session key is invoked with both the nodes that are authorized.

4.1 Network Creation:

At first a network should be created in order to know whether an impulsive approach works better. The nodes in the network created should perform a mutual exchange of information and security using the mechanism of authentication with IDC. Thus network created by information provided by the user's must be identified by unique IP address, services shared using TCP connections. A network should be built according to the IEEE 802.11 standards. After authentication, the nodes should mutually exchange a public key. And information should be updated between the nodes in regular sessions. And each node created should verified uniquely with a Certificate from Certificate Authority.

Joining New Members:

The nodes in the network are connected through short link technology which provides flexibility and ease of detection, selection of nodes.

Further to establish a trust and to join a new member the following steps should be followed:

Step 1: Start a network selection and List the network selection menu

Step 2: Create a new network with a session key

Step 3: Start the network service

Step 4: start the authentication service to add the new nodes

Step 5: search for an authentication device after creating a new node

Step 6: if **NO** new device is found move to step 1

Else if **Yes** a new device is found then choose that particular device

Step 7: Send authentication request to the new node that has joined the network by selecting a device

Step 8: If Authentication is not successful then generate a Authentication Error and proceed to step 1

If Authentication is successful then a Certificate will be generated by Certificate Authority

Step 9: Then give the trust to the node and send the request

Step 10: Authenticate the request and response to that node is created and data is saved

4.2 Protocol operation and implementation:

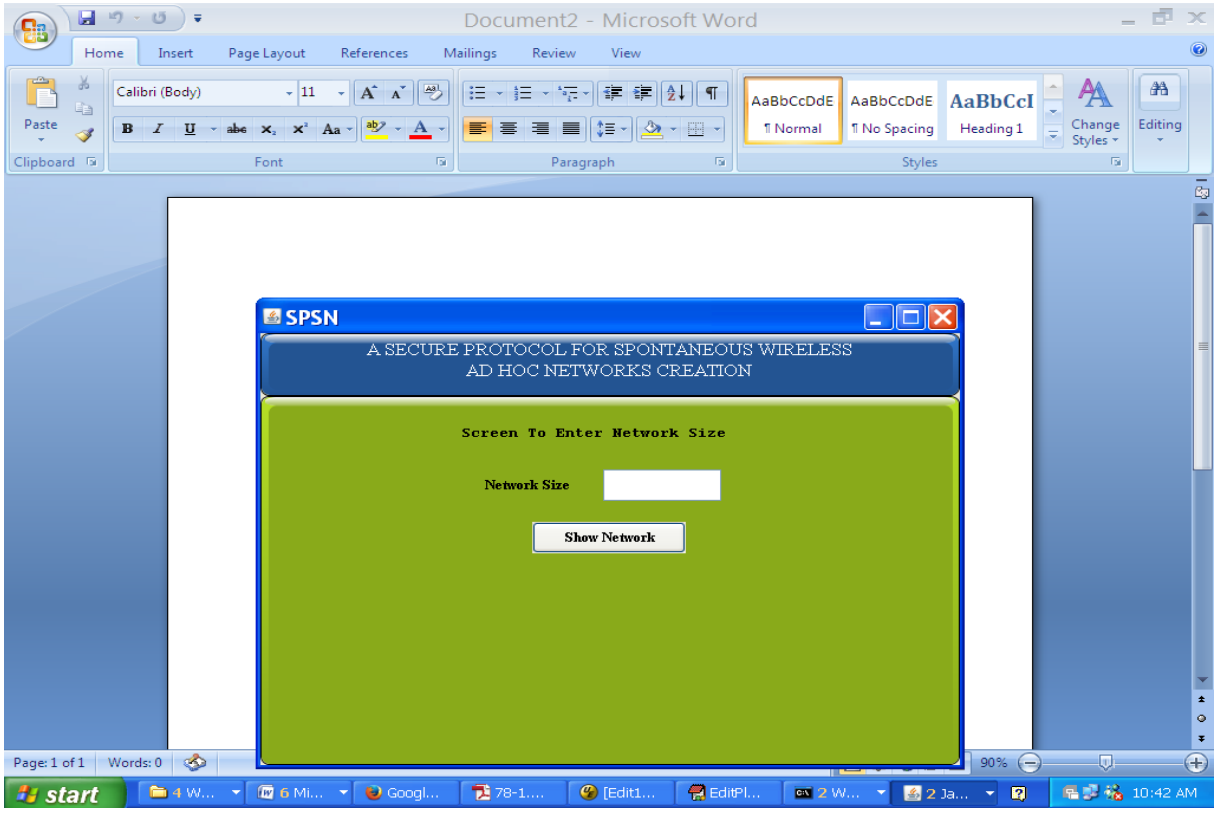
The impulsive protocol should be applied on the nodes in order to find the importance that particular protocol with respect to other protocols. The operations that are performed after the authentication procedure is successful are:

1. Show nodes in the network and modify the trust
2. The node which joins the network have to update the information with every single user, to all the nodes in a group and has to get the certificate from Certificate Authority
3. After receiving the certificate an authentication request is processed and the response information is taken
4. If the user node requests for the information from the sender, then the data should be send by the server. The data may be in the form of Encrypted format.
5. An authenticated node may even send the data to all the nodes without encryption of the data or with encryption of the data.
6. The node may even broadcast the request to get the information.
7. By receiving the information from neighbor nodes, the node can even modify the certificate, own data and password
8. After the communication, the node leaves the network when the session key is expired.

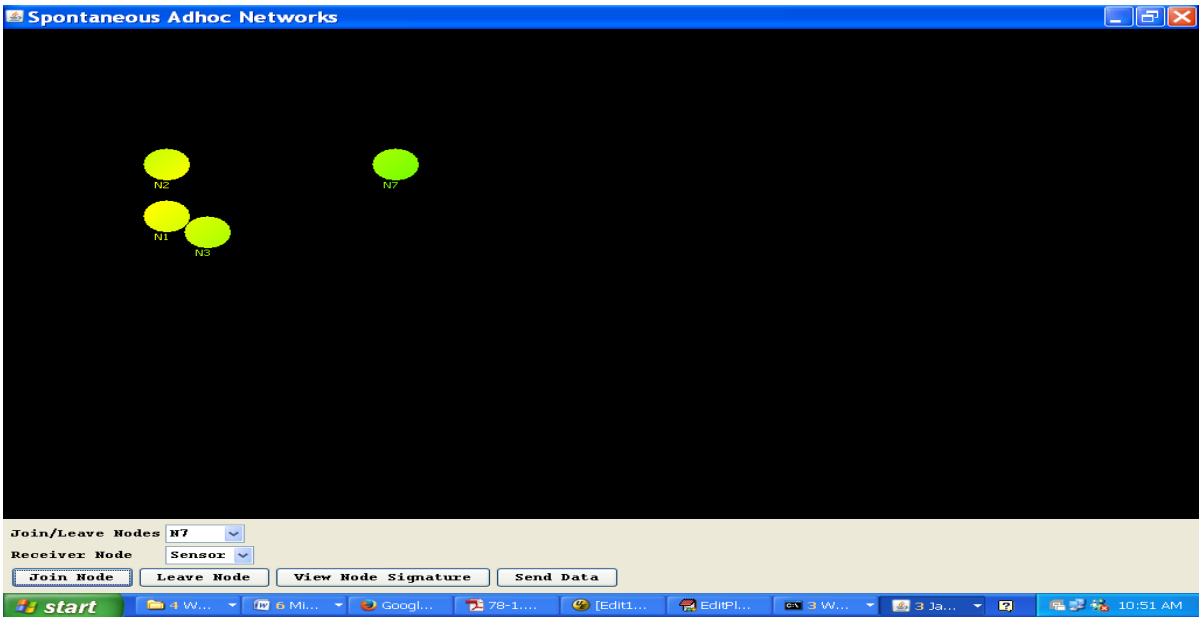
4.3 Session Key Revocation: A session key should be generated to each and every node that joins the network. The session should be generally given to a trusted node. The session key cannot be given to the nodes that are not valid.

5. Performance Analysis

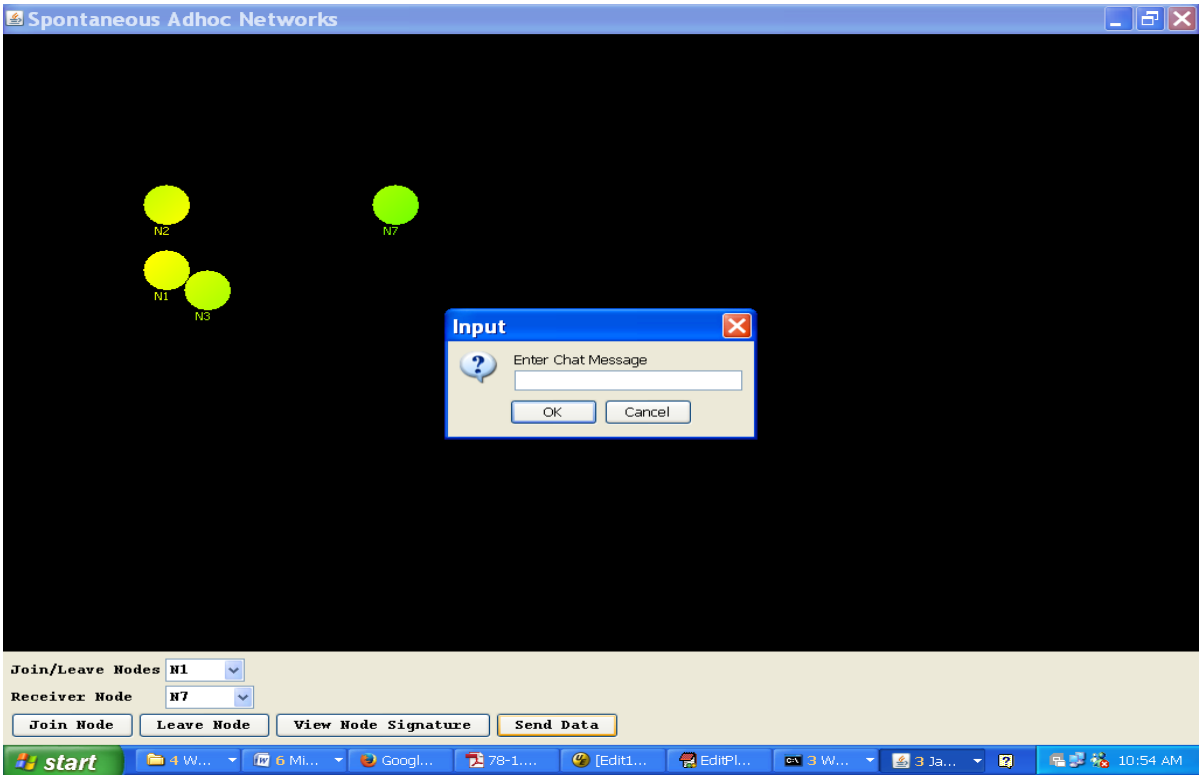
In this section we briefly show our network creation with new nodes. We implement an impulsive protocol on the new nodes for the communication. At first authenticated user should be logged on to create a network. After authenticating, the user has to define the number of nodes to define and create a new network.



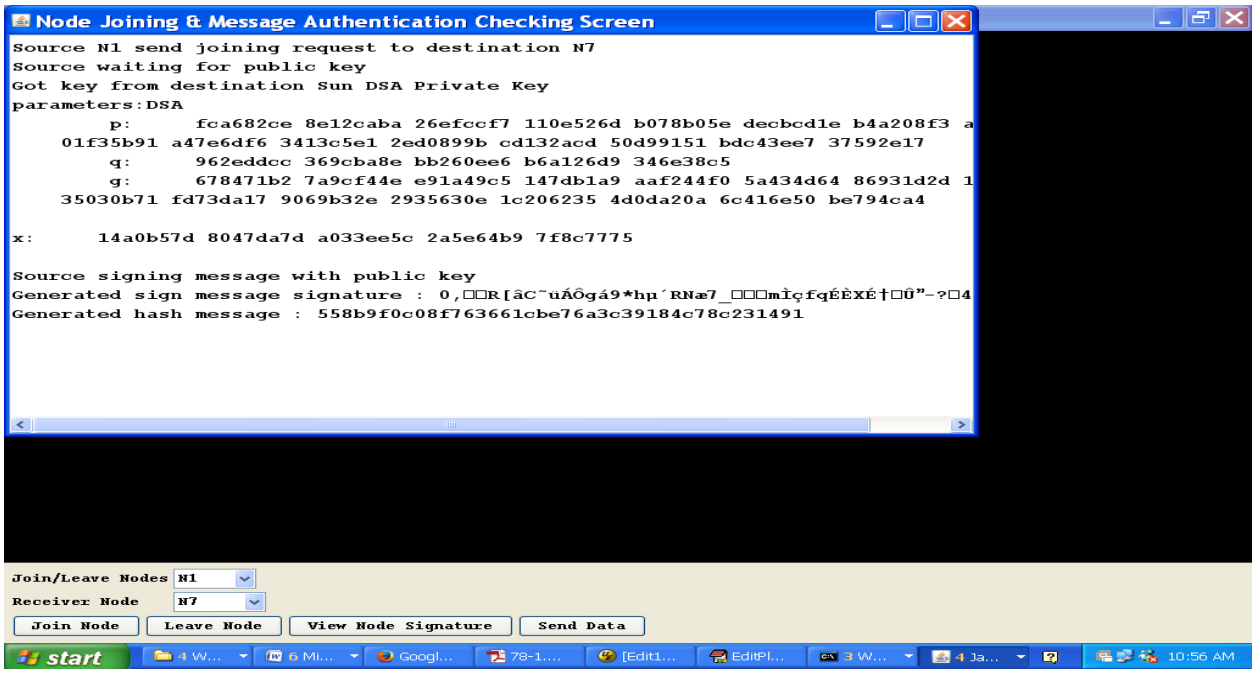
By using the approach we create a manual buttons for the new nodes to join the network and leave the network. It also shows the digital signature of each node and the rate of data that user can send. And click on the join node to create a new node.



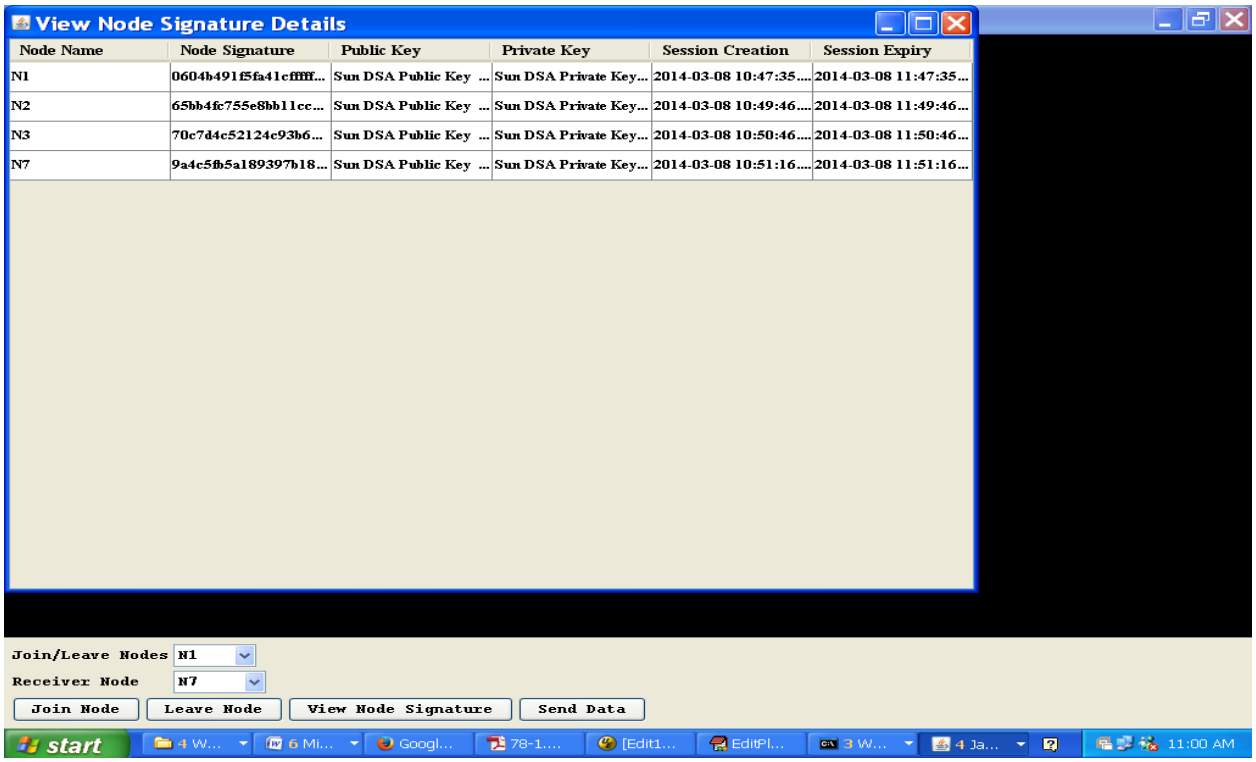
After creating the nodes, select the sender node and destination node. And then join the nodes and create a path. After authenticating then send a chat message.



After sending the node, you can view the data that is being sent from one node to another node. The data is sent in the form of an encrypted format.



To remove a node from network, select any node, here N2 and click on leave node, then the following screen is displayed.



By using this protocol we can create a new network and the user can create any number of nodes. The data which is sent from one node to another node, it is converted in the encrypted for at the time of sending the data.

6. Conclusion

In this paper, we show the design of a protocol that allows the creation and management of a impulsive wireless ad hoc network. Thus each node in the network will work to maintain the network, improve the services offered and provide information to other network users. By using this protocol each node is assigned with a unique IP address to each device, DNS can be managed effectively by using the impulsive approach. In the future we intend to add some more features like sharing other types of resources etc. We also plan to maintain an Intrusion Detection system mechanism and a Distributed domain name service using the IP of the nodes.

References:

1. J. Latvakoski, D. Pakkala, and P. Paakkonen, "A Communication Architecture for Spontaneous Systems," IEEE Wireless Comm., vol. 11, no. 3, pp. 36-42, June 2004.
2. L. Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu, "Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems," Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 107-132, 2012.
3. S. Gallo, L. Galluccio, G. Morabito, and S. Palazzo, "Rapid and Energy Efficient Neighbor Discovery for Spontaneous Networks," Proc. Seventh ACM Int'l Symp. Modeling, Analysis and Simulation of Wireless and Mobile Systems, Oct. 2004.
4. J. Ba¨ckstro¨m and S. Nadjm-Tehrani, "Design of a Contact Service in a Jini-Based Spontaneous Network," Proc. Int'l Conf. and Exhibits on the Convergence of IT and Comm., Aug. 2001.
5. V. Untz, M. Heusse, F. Rousseau, and A. Duda, "Lilith: an Interconnection Architecture Based on Label Switching for Spontaneous Edge Networks," Proc. First Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous '04), Aug. 2004.
6. L.M. Feeney, B. Ahlgren, A. Westerlund, and A. Dunkels, "Spontnet: Experiences in Configuring and Securing Small Ad Hoc Networks," Proc. Fifth Int'l Workshop Network Appliances, Oct. 2002.
7. M. Danzeisen, T. Braun, S. Winiker, D. Rodellar, "Implementation of a Cellular Framework for Spontaneous Network Establishment," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.
8. J. Rekimoto, "SyncTap: Synchronous User Operation for Spontaneous Network Connection," Personal and Ubiquitous Computing, vol. 8, no. 2, pp. 126-134, May 2004.

