Use of Ad Hoc Networks for Wireless Internet Access

Jouni Mäenpää
jpmaenpa @ cc.hut.fi

1 Abstract

An ad hoc network consists of a collection of mobile wireless nodes that dynamically create a network among themselves without using any infrastructure or administrative support. Therefore, ad hoc networks have the potential to provide a free, non-operator controlled means of mobile communication. On the other hand, they also provide a low cost alternative to extend the reach of current wireless access networks. In this paper, the use of ad hoc networks for wireless Internet access is discussed. An overview of some proposed technical architectures and their challenges is provided. Also business models enabling the use of ad hoc networks and the challenges associated with the models are considered.

2 Introduction

An ad hoc network is a mobile or stationary collection of communication devices (nodes) that dynamically create a network among themselves. The nodes have no fixed infrastructure available, and have no pre-determined organization of available links [19]. Not all nodes in an ad hoc network can directly communicate with each other, meaning that nodes are required to relay packets on behalf of other nodes in order to ensure data delivery across the network. What makes ad hoc networking challenging is that rapid changes in network topology, connectivity and link characteristics are introduced due to node mobility and power control practices.

It has been argued that as applications grow hungrier for bandwidth, wireless architectures are likely to move away from cellular to ad hoc [19]. This is because more capacity requires higher communications bandwidth and thus better spatial spectral reuse. Further, higher bandwidth is found at higher frequencies where communication ranges are shorter. Finally, mobile devices need to minimize power consumption. All these factors support a shift from a single long wireless link to a mesh of short links used in ad hoc networks.

Ad hoc networks can play a disruptive role in the world of wireless communications [8]. First of all, ad hoc networks challenge the traditional ideas of wireless infrastructure and its ownership and control. Secondly, ad hoc networks have the potential to disrupt the existing approach to how wireless networks are used and how wireless applications are designed. Thirdly, ad hoc networks challenge the status quo because they have the potential to provide a free, non-cellular based, non-operator controlled means of mobile communication. Fourthly, ad hoc networks can have an impact on social order and behavior; as the infrastructure is less dependent on the operators, it becomes easier for groups of people to form wireless communities. Finally, ad hoc networks can also be physically disruptive in the wireless spectrum, since they may cause interference with each other and with e.g. Wireless Local Area Networks (WLANs) or Bluetooth networks. Ad hoc networks force a different view on network infrastructure, ownership and resource control. Ad hoc networks also remove the operator linkage and require the creation of alternative business models and applications.

Ad hoc networking is an increasingly important topic and has been regarded as one of the key features in beyond third generation (3G) systems [4]. In these heterogeneous and integrated environments, ad hoc networking is considered to be an important solution to extend the radio coverage of wireless systems and to extend the reach of multimedia Internet services to wireless environments.

The focus of this paper is on the question of how ad hoc networks can be used for wireless Internet access and what impact this has on business models. In Section 3, first the integration of the Internet and mobile ad hoc networks (MANETs), and then personal networking are described. Section 4 presents four business models regarding the use of ad hoc networks for wireless Internet access. In Section 5, some technical and business model related challenges are considered. Section 6 presents a brief overview of how ad hoc networks are used currently. Finally, conclusions are drawn in Section 7.

3 Internet Access through Ad Hoc Networks

In this chapter, technologies and architectures enabling the use of ad hoc networks for wireless Internet access are described.

3.1 Integration of Internet and Ad Hoc Networks

The goal of the integration of the Internet and mobile ad hoc networks (MANETs) is to provide mobile nodes in a MANET with wireless Internet access although they are multiple wireless hops away from the edge of the Internet. The problem of integrating MANETs and the Internet has been studied e.g. in [2], [5], [6] and [24]. Central to all of these approaches is the use of mobile gateways (MGs), which sit between the MANET and the

Internet. Another key feature is the use of Mobile Internet Protocol (IP) [21] for mobility management. The MG has two interfaces: the first interface is connected to the Internet so that normal IP routing mechanisms can be used when packets come in and out of the MANET, while the interface connected to the MANET uses some ad hoc routing protocol to route packets within the MANET. The gateway provides an illusion to the outside world that the MANET is simply a normal IP subnet. The gateways are multihomed, meaning that they can connect simultaneously to multiple access points acting as Mobile IP foreign agents (FAs). The access points can use different wireless access technologies and the gateway can switch between access points of different technology to obtain optimal service [5].

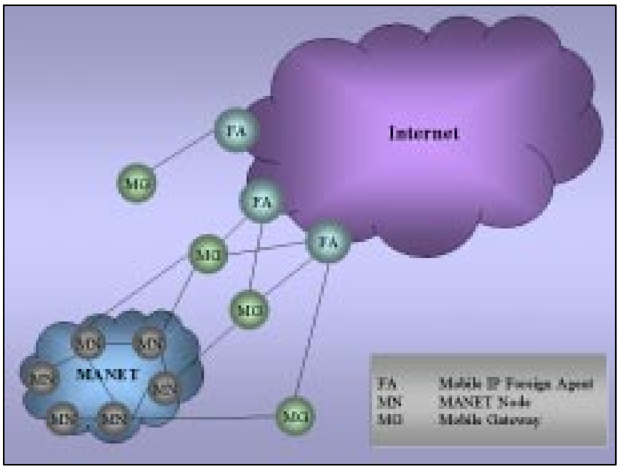

Figure 1 – Integrating MANETs and the Internet

The architecture for integrating MANETs and the global Internet is summarized in Figure 1. Mobile gateways (MGs) are responsible for providing Internet connectivity to MANET nodes (MNs). Mobile IP foreign agents (FAs) act as access points to the Internet and help MGs behave as mobile access points with respect to MANET nodes desiring Internet access. All MNs may not be within the reach of an MG, meaning that other MNs need to relay their traffic towards an MG.

Two principal ways in which ad hoc networks (either stationary or mobile) can be used to extend access networks are presented in [4]. In the first approach, the access network extension is planned. In this approach, which is also known as the cellular ad hoc network, special wireless access routers (WARs) are used for wireless interconnection. The WARs are either stationary or slow-moving and they are operated by legal entities or organizations, like universities or network providers. What makes the planned network extension an ad hoc installation is that the WARs can reach the fixed access points possibly multiple wireless hops away through other WARs. For this, an ad hoc routing protocol is used. Further, no central management is applied; if one WAR drops out, the other WARs will overtake its responsibilities.

The second approach is that of unplanned access network extensions. In this scenario, MGs are used to extend the access network. The MGs are simply normal terminals owned and operated by individual users. A user whose terminal acts as an MG can be seen as an auxiliary network provider, providing an extension of the access service of the access network provider (ANP) to other users. The planned and unplanned access network extension scenarios are depicted in Figure 2.

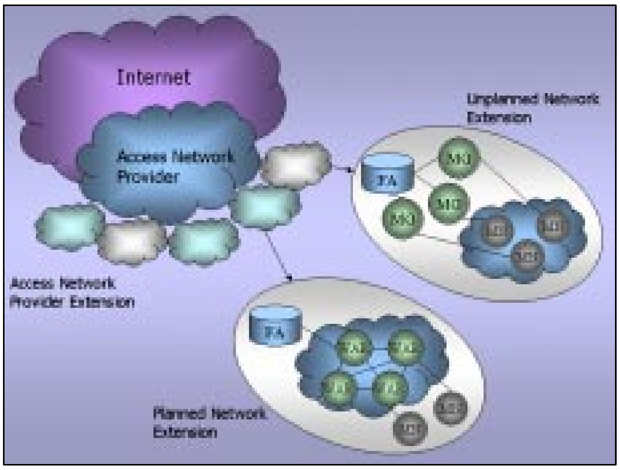

Figure 2 – Planned and Unplanned Extensions

Also a third approach, in which both planned and unplanned network extensions are used, is possible [4]. In this scenario, an MG can connect MNs to WARs when the MNs are out of the range of WARs.

In the most straightforward application of the planned and unplanned access network extension scenarios, the WARs are owned by the ANP and both the MNs and MGs are customers of the ANP. However, one can easily identify situations that are more complicated than this ANP centric scenario. First of all, the WARs and/or FAs could be owned by individual users providing open WLAN hotspots as described in [25]. Secondly, both in the planned and the unplanned access network extension scenarios, the MNs and also MGs might not have a customer relationship with the local ANP, meaning that they would be roaming users in the network of a foreign ANP.

3.2 Personal Networking

Another key concept besides ad hoc networking in beyond 3G networks is personal networking, which can be seen as an evolutionary and revolutionary step towards fourth generation (4G) networks [18]. Personal networks (PNs) introduce a shift from the technology centricity of current second generation (2G) and 3G networks towards greater user centricity. PNs are interesting from the viewpoint of this paper since ad hoc networking is one of their key features.

According to the definition of the European union funded My personal Adaptive Global NET (MAGNET) project, a PN includes a dynamic collection of personal nodes and devices around a user known as the Private Personal Area Network (P-PAN), and remote personal nodes and devices in different clusters, e.g. the home cluster, office cluster and car cluster. The P-PAN is a special cluster consisting of a small-area ad hoc network, and can be though of as a wireless bubble around the user. The PAN and clusters are connected to each other either through infrastructure networks like cellular networks and Internet, or in an ad hoc hop-by-hop manner. This is illustrated in Figure 3.

Figure 3 – The Layout of a Personal Network

The clusters of the PN are self-organizing. Routes inside a cluster can consist of multiple hops and are built with an ad hoc routing protocol [1]. In fact, the entire PN is dynamic in the sense that it is created, maintained and destructed in an ad hoc manner. For instance, when a user moves around a building, nodes and clusters become a part of the network and leave the network in a dynamic fashion. Within each cluster of a PN, there is a special personal node called the gateway node, which provides to the other personal nodes in the cluster access to devices in remote clusters. If a remote cluster can only be reached through the Internet, the gateway (i.e. an MG) can offer Internet connectivity to other personal nodes e.g. through the nearest WLAN hotspot.

4 Business Models

The following business models regarding the use of ad hoc networks for wireless Internet access are described in this section: (i) network provider centric model, (ii) third party authentication, authorization and accounting (AAA) service provider (SP) centric model, (iii) proxy access network provider (ANP) business model, and (iv) access network repeater business model. These four models were selected because they reflect the different authentication relationships between the MNs and MGs described in [23]. In the network provider business model, it is the home network provider that provides the authentication, while in the 3rd party AAA SP model, this is done by a trusted third party. In the proxy ANP model, the MNs and MGs have a pre-existing trust relationship and are authenticated by each other. Finally, in the access network repeater business model, there is no trust; the nodes are not authenticated.

4.1 Network Provider Business Model

In the network provider business model, which is illustrated in Figure 4, all the MNs and MGs have a customer relationship with the network provider. In addition, the infrastructure such as WARs and FAs are owned by the network provider. The end-users always use their home network provider; roaming to the networks of other network providers having overlapping coverage is not possible. Thus, there exists a tight coupling of the user and the network provider and its network. Ad hoc networks are used to extend the coverage of the network provider's wireless access network. The MGs and relay MNs act as auxiliary network providers, and are included as new players in the business model. The network provider business model could be used e.g. in the Unified Cellular and Ad hoc Network architecture (UCAN) [13], in which an operator's 3G network is extended with a WLAN based ad hoc network.

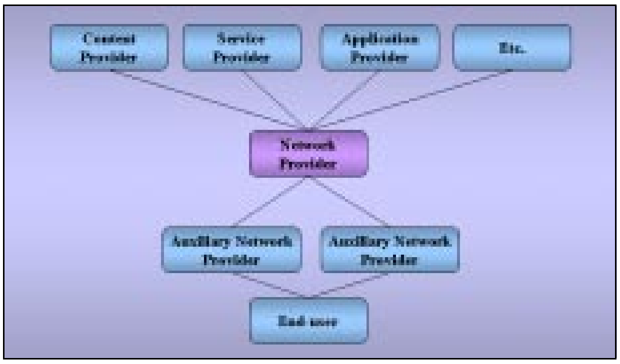

Figure 4 – Network Provider Business Model

Central to this model is that the network provider is in charge of the value network, delivering all different services and applications and controlling the contact to the end-users. Because of this central role, the network provider is dividing the revenue within the value network. The network provider also authenticates the auxiliary network providers and regular MNs and compensates the auxiliary network providers for the use of their resources for relaying the traffic of other users. In general, this model can be seen as a natural continuation of current 2G and 3G network provider business models described in [28] and [16]. However, there is also an aspect of a consumer to consumer business model present, since the auxiliary network providers are compensated for their efforts.

The main issues for the network provider business model include the design of a payment scheme that allows the compensation of the relay nodes, and willingness of users to share and offer infrastructure.

4.2 Third Party AAA Service Provider

In the third party AAA service provider (3P AAA SP) model proposed by the Academic Network on Wireless Internet Research in Europe (ANWIRE) project [4], the end-user is not tied to a single network provider, but can connect to different content providers, service providers and application service providers by using any ANP. Therefore, this model enables much more flexible service provisioning than the network provider centered model. Further, the home network provider is removed from its privileged position. The 3P AAA SP business model is illustrated in Figure 5.

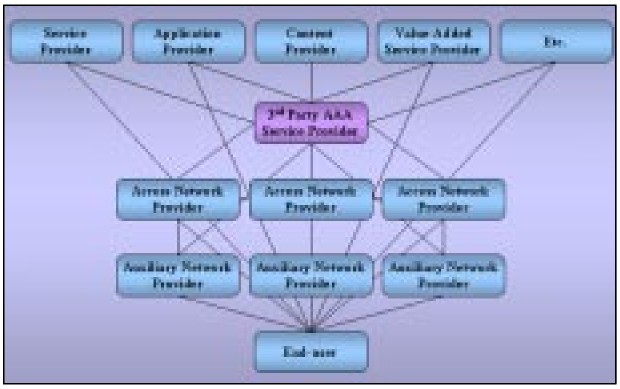

Figure 5 - Third Party AAA SP Business Model

In the 3P AAA SP business model [4], all the players have business agreements with the 3P AAA SP, which is a clearinghouse-like entity providing authentication, authorization and accounting of all the other players in the value network. The 3P AAA SP becomes therefore the central player of the model. All players have business agreements with the 3P AAA SP, whose task is to distribute the revenue within the value network. Also the auxiliary network providers are compensated and authenticated by the 3P AAA SP. Users have agreements with one or more 3P AAA SPs in the same way as they have one or more credit cards, and they receive one itemized bill for all services used through the 3P AAA SP. The 3P AAA SP business model could also include additional players not depicted in Figure 5 such as access brokers and access aggregators, which have been defined by the Ambient Networks project [20].

The main issues with the 3P AAA SP business model include that is likely to require regulatory and standardization support. Also a payment scheme is needed to compensate the intermediate nodes. Finally, the model is likely to face the resistance of current network providers.

4.3 Proxy Access Network Provider

The proxy access network provider (ANP) business model is based on the idea of there being a pre-existing trust relationship between the MNs (including the MGs) [23]. The MNs have a trust relationship for instance because they are all devices of a single user or devices of the members of the same family. The MNs can rely entirely on the MG to provide access to the network resources. Because of the special relationship between the nodes, there is no need to provide incentives for the MG to share its Internet connection or for the MNs to relay the traffic of other MNs. The MG can be seen as a proxy ANP, relaying traffic without compensation. As an example of the use of the proxy ANP model, members of a family could establish an ad hoc network between their terminals using Bluetooth and share a single Internet connection. In another, PN related example, the MG might be a gateway node in a PN cluster (e.g. the P-PAN or home cluster) and the MNs the other devices that belong to the same cluster.

In both of the examples above, the ad hoc set-ups do not need a business model, since the relay nodes offer their services for free. However, in the PN scenario, the business opportunity for the network provider lies in the interconnection of the ad hoc clusters constituting the PN. The idea is that although users can set up parts of the network infrastructure and construct and deliver the services themselves, they also need to interconnect and work together with commercial network providers for parts of the network and services [12]. In MAGNET, the remote clusters of the PN are interconnected using dynamic virtual private network (DVPN) tunnels [7]. DVPNs provide users with on-demand QoS, bandwidth, and security. In contrast to traditional VPNs, in MAGNET, DVPN management is placed into the hands of the user. The business opportunity for the network provider lies in the provisioning of the DVPNs. Of course, the success of this business model is tied to the success of the personal networking paradigm.

4.4 Access Network Repeater

When there is no trust relationship between the nodes of the ad hoc network, the intermediate nodes (i.e. MGs and relay MNs) can be seen as mere access network repeaters, as defined in [23]. The MG shares its connection and the relay MNs forward traffic without compensation. The connection can be free (e.g. through an open WLAN hot spot) or non-free (e.g. a 3G connection). The access network repeater scenario could occur e.g. in a campus area where nodes that are strangers to each other create an ad hoc network using a short range wireless technology such as Bluetooth. In addition to these nodes, also nodes that have both a WLAN connection to the Internet and a Bluetooth interface that connects them to the ad hoc network are needed. Such nodes act as MGs, sharing their Internet connections with the MNs of the ad hoc network. Naturally, if also the ad hoc network is constructed using WLAN links, MG nodes are not needed.

The most significant challenge for the access network repeater business model is the lack of authentication between the nodes and the resulting lack of security. In addition, the model provides no incentives for the intermediate nodes to relay the packets of other nodes or to share their Internet access. Therefore, it can be argued that this model will be very difficult to deploy in real life.

The different business models presented in this Chapter are summarized in Table 1.

Table 1 – Different Business Models Summarized

Model	**Auth. done by**	**Key player**	**Roaming between ANPs**	**Relays compensated**
Network provider	Network provider	Network provider	no	yes
3rd party AAA SP	3rd party AAA SP	3rd party AAA SP	yes	yes
Proxy ANP	Pre-existing trust relationship	User/ network provider	yes	no
Access network repeater	No auth.	User	yes	no

5 Challenges

In this chapter, the technical and business model related challenges concerning the use of ad hoc networks are discussed.

5.1 Technical Challenges

There are numerous open problems with ad hoc networking [19]. First of all, scalability is an issue; one problem for current ad hoc routing algorithms is that they cannot guarantee an acceptable level of service in the presence of a large number of nodes in the network. Quality of Service (QoS) is another problem, since radio frequency channel characteristics can vary unpredictably and since network partitions can be created because of dynamic topology changes. There are also issues in sharing the channel medium with many neighbors; technologies to enhance spectrum efficiency are required. All in all, end to end QoS is very difficult to achieve since routers may be continuously moving and links may go up and down all the time. Energy efficiency is an important problem, since in the absence of a fixed infrastructure nodes need to rely on the limited power of their batteries. A further problem for mobile ad hoc networks is how to maintain a sufficient density of wireless coverage to prevent the partitioning of the network [27]. If partitions exist, current ad hoc routing protocols will fail to deliver packets. Also node willingness is a problem [11]; due to selfish behavior, nodes may refuse to relay packets of other nodes. The reasons for this might include lack of trust, desire to save battery power, etc. One additional challenge is the interoperation between different ad hoc routing protocols. Finally, one of the most important problems is security [14]. As an example, relay nodes (MNs and MGs) can eavesdrop information, delete messages, inject erroneous messages, or impersonate a node. This violates availability, integrity, authentication and nonrepudiation. Compromised nodes can also launch attacks from within the network.

There are also challenges in the integration of MANETs and the Internet, including the mismatches regarding their infrastructure, topology and mobility management mechanisms [2]. Other problems include gateway discovery, selection of an optimal gateway and providing MANET nodes with globally routable IP addresses [3]. In addition, MGs need to perform dynamic access selection [22] and handle handovers between different access technologies.

5.2 Challenges for Business Models

There are two central issues a business model for ad hoc networks must address [8]. First of all, an alternative means of payment that does not rely on a prearranged trust scheme with the ANP is needed. Secondly, an incentive scheme is necessary for nodes relaying messages on behalf of other nodes. The intermediate nodes may need to be compensated for the use of their resources. One approach that attempts to address both of these issues is the multiparty micropayment scheme introduced in [26].

It should be noted that providing incentives to the intermediate nodes is likely to be necessary even though a pricing scheme such as flat rate was used, since the intermediate nodes participate in the provisioning of end to end QoS, and because relaying the traffic of other nodes consumes limited resources such as battery power, central processing unit (CPU) time and bandwidth that the intermediate nodes could have otherwise used themselves. An incentive scheme is also needed to prevent the tendency towards selfish behavior; a selfish relay node could temporarily refuse to forward traffic from other nodes to obtain a larger share of the bandwidth for its own traffic.

Other challenges include high costs and limited availability of spectrum, user acceptance and willingness to share infrastructure and resources, and challenges associated with assuring users of the security of ad hoc networks [23]. An important question is also how to price the service offered by the auxiliary network providers. Also the requirement of zero configuration is an important one; ad hoc Internet access should not result in increased complexity for the user. There are also regulatory uncertainties concerning the sharing of network connections and the lack of control over the transmitted content for the relay nodes. Finally, regulatory and standardization support is needed in order to enable more flexible business models like the 3P AAA SP model.

As a summary, there are a number of open problems that need to be addressed before the large-scale deployment of ad hoc networks and their use for wireless Internet access can become a reality. A failure to solve critical technical challenges such as end to end QoS, security and scalability, and business model related challenges like alternative means of payment, regulatory uncertainties and compensation of intermediate nodes can severely hinder the wide-scale deployment of ad hoc networks.

6 Current Use of Ad Hoc Networks

Traditional examples of the use of ad hoc networks are military and emergency situations. In fact, the initial development of ad hoc networks was mainly driven by military applications. However, many companies are starting to realize the commercial potential of ad hoc networks outside their original contexts of use, including companies such as Green Packet [10], PacketHop [17] and Firetide [9]. These companies are targeting e.g. law enforcement agencies, intelligent transport systems, community networking and home networks with their ad hoc networking solutions.

One example of the proxy ANP business model not including the personal networking aspects is when family members use the same General Packet Radio Service (GPRS) enabled handset as a modem for their laptops, utilizing one hop Bluetooth links. Another example is a solution called PacketHop Communication System offered by PacketHop, Inc. [17] to law enforcement agencies and fire fighters. In this solution, law enforcement personnel can create a mobile ad hoc network among themselves. The solution is interoperable with WLAN access points enabling thus also wireless Internet access through ad hoc networks.

The third party AAA service provider business model is not being applied at the moment and the use of the access network repeater business model is limited to few special cases. One such special case is the current opportunistic use of open WLAN hotspots by single terminals, which does not, however, involve the use of ad hoc networks, but rather one-hop wireless links. Finally, a special case of the network provider business model is possible e.g. in companies and universities if the planned access network extension scenario with a mesh network of WARs presented in Section 3.1 is used. In this case, the company operating its own WLAN access network would act as a network provider. The use of this model is possible, since commercial cable-free WLAN-based WARs are already available. One example is the Firetide Instant Mesh Network solution offered by Firetide, Inc. [9].

7 Conclusions

In this paper, the use of ad hoc networks for wireless Internet access was discussed. The proposed architecture for integrating MANETs and the Internet was described and the use of personal networking was discussed. Also four business models for providing wireless Internet access through ad hoc networks were presented. Finally, some challenges were listed and a brief overview of the current use of ad hoc networks was presented.

There are emerging factors supporting the use of ad hoc networks as part of wireless architectures. Further, ad hoc networking can be seen as a potentially disruptive force, since it challenges many current assumptions in the world of wireless communications. Ad hoc networking has also been considered as a key feature in beyond 3G systems. To integrate MANETs and the Internet, the use of mobile gateway nodes acting as a bridge between the MANET and the edge of the Internet has been proposed. Besides ad hoc networking, another key concept in beyond 3G systems is personal networking, in which ad hoc networks have a central role.

Four different business models supporting the use of ad hoc networks for wireless Internet access were considered in this paper. In the network provider centric business model, the network provider is in charge of the value network. To enable a shift from this model towards more flexible business models, regulatory support is likely to be needed. One way to relax the tight coupling of users and network providers is to make a trusted third party responsible for the user account, as is the case in the third party AAA service provider business model. The business opportunity in the proxy access network provider model is that although in personal networking users can setup parts of the network infrastructure themselves, they still need the services of commercial network providers for providing interconnection services. Finally, the access network repeater business model is unlikely to be widely deployable in real life due to its severe security concerns.

Also a number of barriers regarding the use of ad hoc networks for wireless Internet access were identified. In addition to a number of technical concerns, many business model related issues were discussed. The most important of these include the design of an alternative means of payment not relying on the network operator, and the design of an incentive scheme for relay nodes. Although ad hoc networks have the potential to change the wireless landscape, a failure to address the technical and business model related challenges can effectively hinder this potential and the wide-scale deployment of ad hoc networks.

8 References

[1] Alutoin, M. et al: Towards Self-organising Personal Networks. Proceedings of the ACM DIN’05, September 2, 2005.

[2] Ammari, H. M.: Using Group Mobility and Multihomed Mobile Gateways to Connect Mobile Ad Hoc Networks to the Global IP Internet, International Journal of Communications Systems, John Wiley & Sons, Ltd., 2006.

[3] Andreadis, G.: Providing Internet Access to Mobile Ad Hoc Networks, London Communications Symposium, Sept 2002.
[4] Armuelles, I. et al.: On Ad Hoc Networks in the 4G Integration Process, The Third Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc) 2004.
[5] Aust, S. et al.: Mobile Internet Router for Multihop Ad Hoc Networks, 6th International Symposium on Wireless Personal Multimedia Communications (WPMC 2003), Yokosuka, Kanagawa, Japan, October 2003.
[6] Broch, J. et al.: Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks, Proceedings of the Workshop on Mobile Computing, June 1999.
[7] Calin, D. et al: MAGNET: An Approach for Secure Personal Networking in Beyond 3G Wireless Networks, Bell Labs Technical Journal 11(1), 79-98, 2006.
[8] Doyle, L. et O'Mahony, D.: Ad-Hoc Networking: A Welcome Disruption, IST 2002 Event, Copenhagen, 2002.
[9] Firetide, Inc. http://www.firetide.com (Referred 22.10.2006)
[10] Green Packet, Inc. http://www.greenpacket.com (Referred 22.10.2006)
[11] Harras, K. A. et al.:. Delay Tolerant Mobile Networks (DTMNs): Controlled Flooding in Sparse Mobile Networks, In IFIP Networking, Waterloo, Canada, May 2005.
[12] Henten, A. et Saugstrup, D.: The PN Concept in a Business Modelling Perspective, Center for Tele-Information Working Papers, No. 95, 2004.
[13] Luo, H. et al.: UCAN: A Unified Cellular and Ad-Hoc Network Architecture, Proceedings of the ACM MobiCom'03, September 2003.
[14] Milanovic, N. et al.: Routing and Security in Mobile Ad Hoc Networks. IEEE Computer Society, February 2004.
[15] My personal Adaptive Global NET (MAGNET) http://www.ist-magnet.org/ (Referred 22.10.2006)
[16] Nurmiranta, P.: Social Optimality of Alternative Business Models, Seminar on Networking Business, TKK Networking Laboratory, 2006.
[17] PacketHop, Inc. http://www.packethop.com (Referred 22.10.2006)
[18] Prasad, R. et Olsen, R. L.: The Unpredictable Future: Personal Network Paving Towards 4G, Telektronikk, vol. 1, 2006.
[19] Ramanathan, R. et Redi, J.: A Brief Overview of Ad Hoc Networks: Challenges and Directions, IEEE Communications Magazine 50th Anniversary Commemorative Issue, May 2005.
[20] Raza, S. A.: Conceptual Frameworks for Interconnection of Heterogeneous Networks, Seminar on Networking Business, TKK Networking Laboratory, 2006.
[21] Perkins, C.: IP Mobility Support for IPv4, RFC 3344, August 2002.
[22] Rinta-aho, T.: Dynamic Selection of Optimal Wireless Access Service, Seminar on Networking Business, TKK Networking Laboratory, 2006.
[23] Robles, T. et al.: Usage Scenarios and Business Opportunities for Systems beyond 3G, Proceedings of the IST Mobile and Wireless Telecommunications Summit 2002, Thessaloniki, June 2002.
[24] Sun, Y. et al.: Internet Connectivity for Ad Hoc Mobile Networks, International Journal of Wireless Information Networks, special issue on Mobile Ad Hoc Networks (MANETs): Standards, Research, Applications, 9(2), April 2002
[25] Tallberg, M.: P2P-based Roaming Between Home WLAN Hotspots, Seminar on Networking Business, TKK Networking Laboratory, 2006.
[26] Tewari, H. et O'Mahony, D.: Multiparty Micropayments for Ad Hoc Networks, in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC) 2003, New Orleans, Louisiana, March 2003.
[27] Vahdat, A. et Becker, D.: Epidemic Routing for Partially-Connected Ad Hoc Networks. Technical Report CS-200006, Duke University, April 2000.
[28] Välimäki, J.: Change of Business Models for Wireless Internet Access, Seminar on Networking Business, TKK Networking Laboratory, 2006.