# WIRELESS MULTIHOP INTERNET ACCESS: GATEWAY DISCOVERY, ROUTING, AND ADDRESSING

Jin Xi and Christian Bettstetter
Technische Universität München, Institute of Communication Networks, 80290 Munich, Germany
Jin.Xi@ei.tum.de or Christian.Bettstetter@ei.tum.de, http://www.lkn.ei.tum.de

*Abstract*—**This paper investigates the interworking between wireless ad hoc networks and the Internet. In other words, we consider access to the Internet via a multihop wireless network. The heterogenous communication is established with the help of specific access routers, which serve as gateways between the two kinds of networks. We describe the network scenario and its basic protocol architecture. The main part of the paper is a discussion of issues on access router discovery, IPv6 address autoconfiguration of the mobile ad hoc devices, and the routing and addressing procedure in the heterogeneous scenario.**

*Keywords*—**Wireless ad hoc networking, wireless Internet access, interworking, convergence of wireless and Internet, heterogeneity, addressing, Mobile IPv6, autoconfiguration**

## I. INTRODUCTION AND MOTIVATION

With the advances in wireless communication and mobile computing technologies, wireless multihop networking (ad hoc networking) is expected to play an important role in mobile communications beyond third generation systems. Because of its independence on pre–existing network infrastructure and its distributed organization, ad hoc networking enables the spontaneous establishment of communication between network–enabled electronic devices (e.g., mobile phones, personal digital assistants). Especially in applications where information must be distributed quickly and is only relevant in the area around the sender, ad hoc communication has major advantages compared to "conventional" wireless systems, such as GSM and UMTS. For example, cars involved in an accident can send warning messages back over a defined number of other vehicles, thus avoiding a motorway pileup [1]. In this vehicular scenario, we can also imagine transmission of information about bad traffic or street conditions (e.g., icy roads, obstacles), or wireless communication of closed user groups (e.g., emergency teams).

For many applications, however, it is desired that a self–organizing ad hoc network is somehow connected to a "conventional" network, in particular to the world–wide Internet and to cellular networks. In this case, interworking functionality between the protocols in the ad hoc network and the "conventional" network is needed. In a vehicular environment, such interworking functionality could also extend the range of info stations [2]. These stations are positioned along streets and at city entrances to inform car drivers and passengers, in a drive–by fashion, about nearby restaurants, the current traffic situation, and cultural events. With ad hoc networking capabilities, cars in the transmission range of these stations could then forward this information in a multihop fashion to other cars that have no direct wireless link to the info station.

This paper addresses the interworking between ad hoc networks and Internet Protocol (IP)–based networks, where we restrict our view to IPv6 [3]. To achieve this network interconnection, the installation of *gateways* that understand the protocols of the ad hoc network and the IP suite is needed. From the point of view of the ad hoc network, these gateways act as *access routers* to the Internet.

While much research been done on protocols for autonomous (stand–alone) ad hoc networks during the last few years [4], the practically important heterogenous environment, as discussed in this paper, has not been regarded much (also see "areas for future work" in [5]). Only a few papers can be found on this topic (e.g. [6][7][8]), and, after submission of this paper, a related Internet draft [9] appeared.

The remainder of this paper is organized as follows: In Section II, we give an overview of the interworking system, including the basic protocol stack. Section III discusses the problems for gateway discovery. Section IV investigates IP address autoconfiguration in our scenario. Different routing and addressing mechanisms are discussed and compared in Section V. This raises an interesting "path selection" problem (i.e., how to choose the destination IP address for optimal routing). A countermeasure for this problem is discussed in Section VI. Finally, Section VII concludes this paper and defines topics for further research.

## II. SYSTEM DESCRIPTION

Figure 1 shows a group of *mobile nodes* (MNs) that form a wireless ad hoc network. The communication between the nodes is established through wireless multihop paths. Some MNs in this ad hoc network want to access the Internet. The *access routers* (ARs) are connected to the Internet and communicate with ad hoc nodes via wireless transceivers.

The basic protocol stacks for MNs and ARs are shown in Fig. 2. In the physical and data link layer, a mobile ad hoc

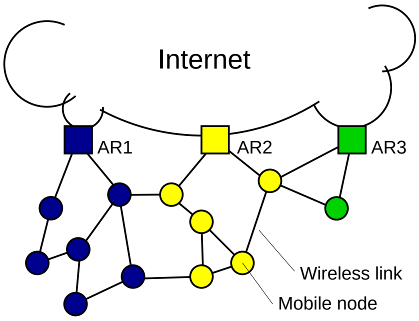

Fig. 1. Illustration of the interworking scenario

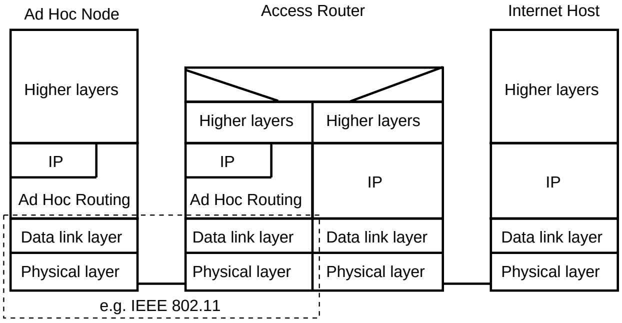

Fig. 2. Protocol architecture

node runs protocols that have been designed for wireless channels and are capable of decentralized direct mode operation. Extended versions of the Wireless LAN standards IEEE 802.11, HIPERLAN/2, or Bluetooth could serve this purpose. In the network layer, either an IP–based ad hoc routing protocol (e.g., Ad hoc On Demand Distance Vector (AODV) routing [10], Dynamic Source Routing (DSR) [11]) is used, or this layer is divided into two sublayers, namely the usual IP layer over a non–IP–based ad hoc routing protocol that transports the IP packets in the ad hoc network in an encapsulated manner. In higher layers, additional IP–based protocols are located (e.g., Transmission Control Protocol (TCP) for wireless channels, Service Location Protocol (SLP)).

The AR contains protocols of the fixed Internet and the wireless ad hoc network. On the Internet side, it runs the usual Internet protocols. On the ad hoc side, it sends and receives packets using an ad hoc routing algorithm. Two different routing tables are used. The AR may also contain protocols in higher layers, in case there is a need for translation in these layers (e.g., conversion of usual TCP to TCP for wireless channels).

In this paper, we take a closer look at the network layer. In order to be able to communicate with Internet hosts, each MN must configure an IP address with the prefix of a reachable AR. With this location–dependent address, IP packets can be received from and sent to hosts in the Internet. When an MN moves and selects a different AR, it should configure a new IP address with the new prefix. With this configuration, all MNs attached to the same AR form an IP subnet; i.e., an entire ad hoc network (fully connected or not) is logically divided into several clusters (see Fig. 1).

How does an MN configure its location–dependent address? Basically, it (1) configures an initial IP address which is routable in the ad hoc network, (2) discovers all reachable ARs in its surrounding and learns their prefix, (3) selects one AR out of the set of reachable ARs, and (4) forms a globally routable IP address with the prefix of the selected AR. These principles for access router discovery and IP autoconfiguration are discussed in Sections III and IV.

Furthermore, we use Mobile IPv6 [12] to make the mobility of MNs between different ARs transparent to higher layers. The location–dependent IP address is used as *care–of address*. In addition, we assume that each MN has a permanent IPv6 *home address*, which has the prefix of its home network and serves as a consistent and unique identifier for the MN. Whenever an MN configures a new care–of address, it registers its current care–of address with its *home agent* on its home network, using a BINDING UPDATE message. This home agent stores the mapping between an MN's home address and care–of address in a so–called *binding cache* and acts as a proxy for the MN. Packets addressed to a node's home address are received by the home agent and forwarded (tunneled) to the MN's care–of address according to the mapping information.

In summary, we can say that Mobile IPv6 is used to support macromobility between different ARs, and an ad hoc routing protocol is employed for micromobility management. The complete routing procedure between mobile ad hoc nodes and Internet hosts is described in Section V.

## III. ACCESS ROUTER DISCOVERY

Upon initialization, a mobile node should discover the existence of all access routers in its reachability and then select one access router out of these candidates. This problem is well–known for systems with only direct (single hop) connections between mobile nodes and access routers (see, e.g., [13]), but the multihop environment makes the discovery algorithm more complicated.

In general, AR discovery can be initiated by the mobile node (*active discovery*) or the access router (*passive discovery*). In the active discovery method, a mobile node sends out an ACCESS ROUTER REQUEST message. This request can be broadcasted in the ad hoc network (with a hop limit) or sent to a specific *Access Router Multicast Address* (i.e., an IP address for the group of all Internet gateways in an ad hoc network). When an access router receives this request it replies via a unicast ACCESS ROUTER RESPONSE message, which contains the router's IP address. Such a discovery should be performed upon initialization of a mobile node and if the multihop connection to an AR breaks or degrades (e.g., too many hops). It can also be performed periodically.

In the passive discovery method, an AR periodically sends out ACCESS ROUTER ADVERTISEMENTS to indicate its existence and inform nodes about its IP address including the prefix. These messages are received by all nodes within the transmission range of the AR. The multihop environment allows for a useful extension to this approach: the receiving ad hoc MNs could forward the advertisements to neighbors that are located beyond the range of the AR. Typically, an AR has a larger transmission range than an MN, which yields a disadvantage of the passive discovery method: It is not necessarily guaranteed that an ad hoc node receiving an ACCESS ROUTER ADVERTISEMENT *from* the gateway does have a multihop path *to* the gateway.

In practice, both discovery methods can be combined and run in parallel. This leads to a *hybrid* method for AR discovery. The access router periodically sends out advertisements, and all nodes in its radio range store this information. An active ACCESS ROUTER REQUEST, which was broadcasted by a mobile node that is not in the radio range of a gateway, can now be answered by any intermediate node with stored AR information, thus reducing the signaling traffic. Intermediate MNs cannot reply, if the active ACCESS ROUTER REQUEST was sent to the *Access Router Multicast Address.*

If an MN receives, within a certain time, more than one ACCESS ROUTER RESPONSE or ADVERTISEMENT from different ARs, it selects one AR according to a certain metric (e.g., received signal level from access router, hop count, capacity, security issues, load of AR, or combinations of these criteria). This is denoted as *access router selection.*

## IV. ADDRESS AUTOCONFIGURATION

IPv6 defines two fundamental principles for autoconfiguration: *stateful* and *stateless autoconfiguration*. Stateful address autoconfiguration can be implemented by a DHCP server [14] residing in the AR. It automatically assigns addresses to requesting MNs and manages the address space. The MNs learn the IP address of the DHCP server from the AR discovery.

Let us now consider stateless autoconfiguration. In fixed IPv6 networks, a node first forms a *link–local address* to obtain IP–level connectivity with neighboring nodes [15]. This temporary address is a combination of the reserved link–local prefix FE80::0 and the node's equipment identifier (EUI). Using this initial address, the node learns the prefix of its router, and can then form a global or site–local address. This autoconfiguration method must be slightly modified to work in our multihop scenario because link–local addresses may not be applicable for multihop communication. Instead of using the link–local prefix FE80::0, mobile ad hoc nodes must use a different reserved prefix (e.g. the *MANET Initial Prefix* [16]) to generate a temporary address. The uniqueness of the address can be validated by a protocol for *duplicate address detection* (DAD), e.g., as described in [16]. After a successful DAD of this initial address, a node can communicate with other nodes in the ad hoc network and is therefore able to send and receive messages for AR discovery. From received ACCESS ROUTER ADVERTISEMENT and RESPONSE messages, it learns the prefix information that identifies each candidate AR. After selecting one AR, the MN combines the prefix of this AR and the EUI to generate a *globally routable IP address*. The initial address should time out in all routing tables after a short period of time.

Instead of forming a temporary initial address for AR discovery, a node could also use its IPv6 home address to start the autoconfiguration process. However, this creates problems when using hierarchical routing in the ad hoc network (see Section V).

## V. ROUTING AND ADDRESSING IN THE HETEROGENEOUS ENVIRONMENT

This section describes and compares different approaches for flat and hierarchical routing and address assignment in our heterogeneous scenario.

### *A. Flat Routing in the Ad Hoc Network*

Let us first consider the case in which a flat routing protocol is used in the ad hoc network. Such protocols regard the ad hoc network as a number of nodes without subnet partitioning. The communication in this environment can be categorized into two scenarios: (1) routing between an Internet host and an ad hoc node and (2) routing between two ad hoc nodes with the same AR or with different ARs.

If a *proactive* routing protocol is used in the ad hoc network, a mobile sender should have an entry for the destination in its routing table, which is either a route in the ad hoc network or a link to the default AR if the destination is not reachable through the ad hoc network. If a *reactive* protocol is used, such as AODV or DSR, the ad hoc sender must first discover a route to the destination. To perform this route discovery, it sends out a ROUTE REQUEST message [4]. If the destination is located in the ad hoc network and is reachable via a multihop path, it will answer, and the source node will receive a ROUTE REPLY. The AR will also reply, if it knows a path to the destination's home agent. The

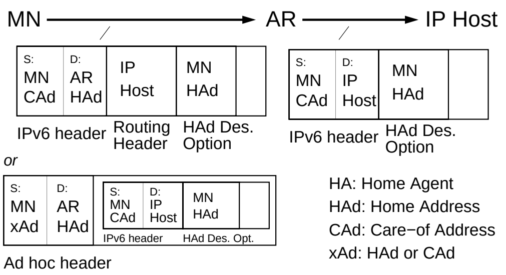

Fig. 3. Routing from an MN in an ad hoc network to an IP host

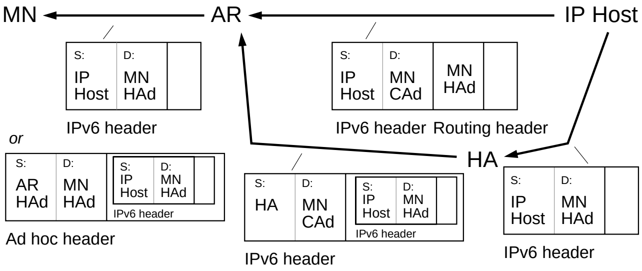

Fig. 4. Routing example from an IP host to an MN in an ad hoc network

source MN chooses the best path according to a certain metric. Even if the source and destination nodes have selected different ARs, there is no partitioning into different IP subnets. If an ad hoc node sends a packet to an Internet node, it also generates a ROUTE REQUEST message looking for a path to this destination. Because the IP host is not located in the ad hoc network, only the AR responds with a ROUTE REPLY.

*Communication btw. ad hoc MN and Internet host* — After obtaining a route to the destination, an MN can tunnel IPv6 packets through the ad hoc network to the AR, which then forwards them to the Internet host. There are two methods to realize this tunneling (see Fig. 3). One method is that the MN encapsulates each IPv6 packet (i.e., it adds an *ad hoc header* with the AR as destination address). Another method is possible, if the ad hoc network employs an IPv6–based routing protocol. The sending MN can then use an *IPv6 extension header*. The *routing header* of this extension header contains the final destination address, i.e., the address of the Internet host, and the destination field of the *IPv6 header* contains the AR address [3]. Only a network node with an IP address mentioned in the destination field of the IPv6 header of an IPv6 packet can examine the routing header of this packet [3]. The *home address destination option* of Mobile IPv6 [12] is used to inform the correspondent IP host about the home address of the MN. In case encapsulation is used, either the home or care–of address of the MN can be used as source address. The AR decapsulates incoming packets from the MN, or it reads the routing header and puts the address of the IP host into the destination field of the IPv6 header (see Fig. 3). The resulting packet is then routed through the Internet to the IP host.

We now consider traffic from the Internet host to the MN (see Fig. 4). If the IP host already knows the care–of address of the MN, it puts the MN's care–of address in the IPv6 destination address field and the MN's home address in the routing header of the outgoing IP packet [12]. If the IP host has no binding information about the MN, it sends a usual IPv6 packet to the MN's home address. The home agent intercepts this packet and must tunnel it to the MN's current care–of address using IPv6 encapsulation [12]. In the remaining routing process, we can distinguish two design options:

- All ad hoc MNs of a single subnet have been assigned the same care–of address from the AR, e.g., by stateful autoconfiguration. The AR possesses two IPv6 addresses: A home address that identifies the AR uniquely and a second address that is given as care–of address to the MNs. Both addresses have the same prefix. With this address assignment, incoming IP packets that are addressed to an MN's care–of address can be processed by the AR, i.e., the AR can decapsulate the packets or examine the routing header, respectively. It then forwards the packets to the MN. The home address of the MNs is used in ad hoc routing, i.e., the AR uses the MN's home address as destination address (see Fig. 4).
- Each MN has been assigned a different care–of address with the prefix of the corresponding AR using stateful or stateless autoconfiguration. This address or the home address can be used in ad hoc routing, where the location information of the care–of address is not used. The content of packets from the MN to an IP host (outgoing traffic) is the same as in the previous case (Fig. 3). In case of incoming traffic, the AR does not decapsulate packets or examine routing headers that are addressed to the care–of address of MNs.

*Communication btw. ad hoc MNs* — In order to send an IPv6 packet to another MN in the ad hoc network, the MN originates an IPv6 packet with the address of the destination MN in the IPv6 header. No IPv6 routing header is required in this case. If the ad hoc routing protocol is not based on IP, the IPv6 packet must be tunneled to the destination MN using encapsulation with an ad hoc header.

### B. Hierarchical Routing with Care–Of Address

Using hierarchical routing, the ad hoc network is logically separated into subnets (i.e., clusters). When an MN receives a packet, it checks the destination address. If itself is the destination, it processes the packet for further operation. If the MN is not the destination and the prefix of the source is different than its own prefix, the MN ignores this packet. Inter–subnet information exchange is only possible via the access router. In this case, a hierarchical address structure is also needed for routing in the ad hoc network, and therefore an MN's care–of address is the right choice for addressing in the ad hoc routing protocol, since it contains the prefix of the AR that a node is registered with. It is required that each MN obtains a unique care–of address.

The communication in this heterogeneous environment can be categorized into three scenarios: routing between (1) an Internet host and an ad hoc node, (2) two ad hoc nodes registered with the same AR, (3) two ad hoc nodes registered with different ARs.

*Communication btw. ad hoc MN and Internet host* — If an MN wants to send data packets to an Internet host, it knows from the prefix of the destination address that this host does not belong to its own subnet. Thus, it sends the data packets to the AR using the ad hoc routing protocol. If a proactive routing protocol is used within the subnet, the MN should have the route to the AR in its routing table; if a reactive protocol is used, it sends out a ROUTE REQUEST for the AR. Once the AR receives the data packets, it forwards them to the Internet host. In the other direction, the Internet host either addresses packets to the MN's home address or directly to its care–of address. In the first case, the MN's home agent re–addresses the packets to the MN's care–of address. Only the care–of address is used for routing from the access router to the MN.

*Communication btw. ad hoc MNs in same subnet* — If an ad hoc node wants to communicate with another ad hoc node that has attached to the same access router, the sending MN learns from the prefix of the destination's care–of address, that the destination is located in the same IP subnet. Thus, the sender initializes the route discovery or follows its routing table as usual. If the sender knows only the home address of the destination, the ROUTE REQUEST will be answered by the AR and packets will be routed to the home agent of the destination. The home agent then informs the sender about the destination's care–of address, and future communication can go through the direct path in the ad hoc network.

*Communication btw. ad hoc MNs in different subnets* — The sender learns from the IP prefix, that the destination is located in a different IP subnet. Thus, the packets are routed toward its serving AR, and the source AR routes the packets to the destination AR via the fixed IP network. The destination AR forwards the packets to the destination using ad hoc routing. In the whole procedure, the packets are sent with the MN's care–of address as destination.

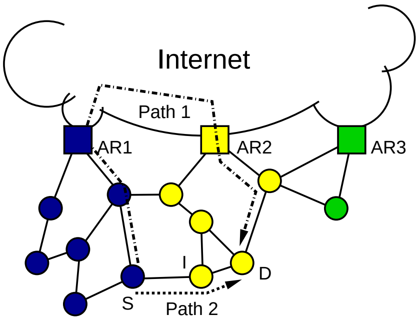

Fig. 5. Path selection problem

### C. Comparison

A hierarchical approach in the ad hoc network continues the hierarchical architecture of the Internet. Moreover, it limits some signaling traffic to the subnet of an AR. On the other hand, an advantage of the flat approach is that it is not required that each node forms a care–of address.

For communication between MNs and Internet hosts as well as between MNs of the same subnet, the routing path optimality is similar for both approaches. For communication between MNs in different IP subnets, the route optimality depends on the distance between two MNs: In case the source and destination are close to each other, the optimal path is the flat wireless multihop path between them. In case the MNs are far away from each other, the traffic between two IP subnets should be transported via a hierarchical routing path through the fixed network.

## VI. EXTENDED HIERARCHICAL ROUTING

### A. The Path Selection Problem

Fig. 5 gives an example in which strict hierarchical routing is inefficient. Two mobile nodes, *S* and *D*, reside in a connected ad hoc network. After AR discovery, node *S* selects AR1 and generates a care–of address with AR1's prefix. Node *D* obtains a care–of address with AR2's prefix. The distance between the two nodes is only two hops, but they belong to different IP subnets. If *S* sends packets to *D* using hierarchical routing, the packets are routed from *S* to AR1. AR1 forwards the packets to AR2 in the fixed network. AR2 then forwards the packets to *D* in the wireless ad hoc network (Path 1 in the figure). Using flat routing, packets are routed directly through wireless hops (Path 2). Obviously, the hierarchical path is much longer than the flat path and wireless resources are wasted.

### B. Introduction of a Prefix Cache in the Mobile Nodes

To optimize the hierarchical routing and to avoid this negative effect, we propose to add a *prefix cache* into each mobile ad hoc node. The MN stores the prefix for its subnet, and also collects prefixes of neighboring subnets. In dense ad hoc networks, it is likely that destination nodes with these prefixes are reachable via a wireless multihop path.

After this modification, a sender first checks whether the prefix of the destination address exists in its prefix cache. If so, it tries to find a path to the destination node inside the ad hoc network (ROUTE REQUEST) instead of sending them immediately to its access router. Also the intermediate nodes do not ignore packets arriving from a different subnet, but they check the source prefix in their prefix cache and forward the packet if the prefix is stored in their cache. For example, node $I$ in Fig. 5 receives the packets from node $S$ with destination address $D$. Without using a prefix cache, node $I$ would discard this packet because it was sent out from a different subnet. But after the modification, node $I$ finds the prefix of node $S$ in its own prefix cache and forwards the packet to $D$ (Path 2). The inter–subnet communication is now no longer only a task of the access router but also a task of *border nodes* to other subnets.

A key point for the performance of the modified hierarchical routing is the method by which a prefix cache is built up and maintained. First, the ad hoc nodes themselves may collect prefix information. During AR discovery, a node may receive several ACCESS ROUTER ADVERTISEMENTS and RESPONSES from more than one ARs. Its stores all received information in its prefix cache for a certain amount of time (e.g., using a *prefix expiration timer*), even if it only selects the most suitable access router. If nodes are mobile, they will anyway come into the radio range of different ARs and can receive the ADVERTISEMENTS or perform active access router discovery. Second, the access routers may collect information about all neighboring access routers through the fixed network and distribute this information with ADVERTISEMENTS. This method would save processing power of the ad hoc nodes. However, an algorithm for access router discovery over the fixed network in needed in this case.

## VII. CONCLUSIONS

In this paper we considered the Internet access of mobile devices in a wireless ad hoc network via specific access routers. We described problems and approaches to solutions for access router discovery, addressing, and routing. For the path selection problem, we proposed a prefix cache in each node that allows the node to optimize the routing path to ad hoc nodes in adjacent subnets of the ad hoc network.

Topics for further research include the investigation of proper methods for *access router selection*. Furthermore, *location updating* and *multihop handover* schemes must be designed and evaluated. As the MNs of the ad hoc network move around, they must switch to different ARs from time to time and obtain a new care–of address. The home agent and correspondent nodes of this MN must be informed about the new address using a BINDING UPDATE message. An interesting aspect in such a scenario is that delayed packets arriving at the old AR can still be forwarded via intermediate nodes to the destination node if the latter has a multihop connection to its old AR. This allows for a smoother handover with reduced packet losses.

## ACKNOWLEDGMENTS

This work is funded by the German research foundation DFG in the program AKOM (Adaptability in heterogenous communication networks with wireless access).

## REFERENCES

[1] W. Kellerer, C. Bettstetter, C. Schwingenschlögl, P. Sties, K.-E. Steinberg, and H.-J. Vögel, "(Auto)Mobile communication in a heterogeneous & converged world," *IEEE Personal Comm. Mag.*, Dec. 2001.

[2] R. H. Frenkiel, B. R. Badrinath, J. Borras, and R. D. Yates, "The infostation challenge: Balancing cost and ubiquity in delivering wireless data," *IEEE Personal Comm. Mag.*, Apr. 2000.

[3] S. Deering and R. Hinden, "IPv6 specification." RFC 2460, Dec. 1998.

[4] C. E. Perkins, *Ad hoc networking*. Addison Wesley, 2001.

[5] M. S. Corson, J. P. Macker, and G. H. Cirincione, "Internet-based mobile ad hoc networking," *IEEE Internet Computing*, Aug. 1999.

[6] H. Lei and C. E. Perkins, "Ad hoc networking with Mobile IP," in *Proc. Europ. Pers. Mobile Com. Conf. (EPMCC)*, (Bonn, Ger.), Sept. 1997.

[7] J. Broch, D. A. Maltz, and D. B. Johnson, "Supporting Hierarchy and Heterogeous Interfaces in Multi–Hop Wireless Ad Hoc Networks," in *Proc. Wrkshp. on Mobile Computing, in conj. Intern. Symp. on Parallel Architectures, Algorithms, and Networks*, (Perth, Australia), June 1999.

[8] U. Jönsson, F. Alriksson, T. Larsson, P. Johansson, and G. Q. Maguire, "MIPMANET: Mobile IP for mobile ad hoc networks," in *Proc. Wrkshp on Mobile Ad Hoc Netw. & Comp. (MobiHoc)*, (Boston, USA), 2000.

[9] R. Wakikawa, J. T. Malinen, C. E. Perkins, A. Nilsson, and A. J. Tuominen, "Global connectivity for IPv6 mobile ad hoc networks." Internet Draft, Nov. 2001. Work in progress.

[10] C. E. Perkins, E. M. Royer, and S. Das, "Ad hoc on demand distance vector (AODV) routing." Internet draft, Mar. 2001. Work in progress.

[11] D. B. Johnson, D. A. Maltz, Y.-C. Hu, and J. G. Jetcheva, "The dynamic source routing protocol for mobile ad hoc networks." Internet draft, Mar. 2001. Work in progress.

[12] D. B. Johnson and C. E. Perkins, "Mobility support in IPv6." Internet draft, July 2000. Work in progress.

[13] D. Trossen, G. Krishnamurthi, H. Chaskar, and J. Kempf, "Issues in candidate access router discovery for seamless IP handoffs." Internet draft, July 2001. Work in progress.

[14] J. Bound, M. Carney, C. Perkins, and R. Droms, "Dynamic host configuration protocol for IPv6 (DHCPv6)." Internet draft, June 2001. Work in progress.

[15] S. Thomson and T. Narten, "IPv6 stateless address autoconfiguration." RFC 2462.

[16] C. E. Perkins, J. T. Malinen, R. Wakikawa, E. M. Belding-Royer, and Y. Sun, "IP address autoconfiguration for ad hoc networks." Internet Draft, Nov. 2001. Work in progress.