MIPMANET - Mobile IP for Mobile Ad Hoc Networks

Ulf Jönsson*, Fredrik Alriksson*, Tony Larsson*, Per Johansson*, Gerald Q. Maguire Jr.†

*Ericsson Radio Systems AB, SE-164 80 Stockholm, Sweden
†Dept. of Teleinformatics, Royal Institute of Technology, SE-164 40 Stockholm, Sweden
Email: {ulf.jonsson, fredrik.alriksson, tony.g.larsson, per.johansson}@ericsson.com, maguire@it.kth.se

Abstract -**Mobile ad hoc networking allows nodes to form temporary networks and communicate beyond transmitter range by supporting multihop communication through IP routing. Routing in such networks is often reactive, i.e., performed on-demand, as opposed to Internet routing that is proactive. As ad hoc networks are formed on a temporary basis, any IP address should be allowed to appear in an ad hoc network.**

This paper presents MIPMANET, a solution for connecting an ad hoc network, in which on-demand routing is used, to the Internet. MIPMANET provides Internet access by using Mobile IP with foreign agent care-of addresses and reverse tunneling. This allows nodes to enjoy the mobility services of Mobile IP while at the same time the requirements on the ad hoc routing protocol are kept to a minimum.

Simulations of MIPMANET have been performed in Network Simulator 2. The Ad hoc On-demand Distance Vector (AODV) routing protocol has been used for routing within the ad hoc network. These simulations show that the ability to choose the closest access point to the Internet is worth extra work, as less traffic is generated in the network resulting in lower delays and fewer dropped packets.

Keywords - **MIPMANET, Mobile Ad Hoc Networks, Internet Access, Mobile IP, AODV**

I. Introduction

Mobility and IP are two strong trends nowadays. Cellular phones are becoming more and more widespread and people are getting used to the concept of mobility when it comes to telephony. The Internet has made information more available and easier to access and the desire for mobility concerning access to information on the Internet is increasing.

An especially hot area concerning IP mobility is *ad hoc networks*. Such networks are typically formed on a temporary basis, easy to set up, can operate without any preexisting infrastructure, and are characterized by untethered multihop communication. One motivation for such networks is to provide connectivity beyond the range of fixed and cellular infrastructures. Within the Internet Engineering Task Force (IETF [1]) there is a working group called Mobile Ad hoc Networks (MANET [2]) that is chartered to develop routing specifications. Many routing protocols have been proposed, including several using on-demand routing [3], [4].

The IP mobility that is provided by ad hoc networking is limited to the ad hoc network as such. The Mobile IP [5] protocol was developed (separately from ad hoc networking) to allow roaming between *different* networks. Since nodes in ad hoc networks are inherently mobile, it seems inevitable that some of these nodes will desire to roam between different ad hoc networks and to other parts of the Internet as well. Hence there is a need to utilize both Mobile IP and ad hoc networking.

Currently, most work concerning ad hoc networking has been concentrated on stand-alone ad hoc networks. Not much work has been done concerning the integration of ad hoc networks and the Internet. There are several issues that have to be considered, especially when on-demand routing is used within the ad hoc network. In this paper we have looked at how ad hoc networks in which on-demand routing is used can be connected to the Internet and how to provide nodes in the ad hoc network with the roaming services that Mobile IP enables. Previous work concerning Mobile IP in such ad hoc networks has been very limited, since key mechanisms of Mobile IP have been left out [6].

To alleviate the need for tedious configuration, it is assumed in this paper that any IP address may appear in an ad hoc network. A node should for example be able to use a preconfigured IP address that it has "inherited" from some other IP network, as long as that address is unique.

The solution proposed in this paper is called MIPMANET (Mobile IP for Mobile Ad Hoc Networks). MIPMANET has been analyzed by means of simulations using Network Simulator 2 (ns2 [7], [8]). In the simulations, the Ad hoc On-demand Distance Vector (AODV [4], [9]) routing protocol has been used within the ad hoc network.

The rest of the paper is organized as follows. Section 2 briefly describes Mobile IP and AODV. Section 3 discusses different issues concerning Internet access from an ad hoc network and Mobile IP in ad hoc networks. Section 4 presents MIPMANET while Section 5 describes the simulation environment and presents the simulation results. Related work is discussed in Section 6, whereas Section 7 concludes the paper. Finally, Section 8 outlines some future work.

II. Protocol Descriptions

This section gives a short description of the protocols used in MIPMANET and the simulation study.

0-7803-6534-8/00/$10.00 © 2000 IEEE

A. *Mobile IP*

Mobile IP [5], [10], [11], [12] is a proposed standard for location independent routing. It makes mobility transparent to applications and higher level protocols like TCP and UDP. Mobile IP allows mobile nodes to have seamless, untethered access to the Internet while roaming between different networks.

In order to maintain existing transport layer connections, such as TCP connections, while roaming every mobile node is assigned a *home address*. The home address enables the mobile node to always be able to receive data as if it was on its *home network*, i.e., the network to which it's home address belongs.

When the mobile node is attached to a network other than its home network (called a *foreign network*) it uses a *care-of address*. The care-of address is an IP address valid on the foreign network that the mobile node is visiting. Whenever a mobile node moves from one network to another it has to change to a new care-of address that is valid on the new network. A mobile node in a foreign network is called a *visiting node* (VN).

To be able to receive datagrams while visiting a foreign network, the visiting node has to register its current care-of address with its *home agent* (HA), representing the visiting node within its home network. To do this, the visiting node usually has to register through a *foreign agent* (FA), located in the foreign network. When the node has registered successfully with the home agent, every datagram sent to the mobile node's home address is intercepted by the home agent and tunneled to the care-of address, from whence the foreign agent forwards it to the mobile node. Each foreign agent keeps a *visitor list* in which information about visiting nodes currently registered through it is kept. This information includes (among other things) the link-layer addresses of the visiting nodes.

If the care-of address is that of the foreign agent, it is known as a *foreign agent care-of address*. If the node can acquire a care-of address by other means, the foreign agent is not needed. The Dynamic Host Configuration Protocol (DHCP [13]) could for example be used to acquire such an address. The home agent can then forward packets to the mobile node directly since the node's address is the care-of address. Such a care-of address is called a *co-located care-of address*.

By broadcasting *agent advertisements* periodically, foreign agents announce their presence and enable a mobile node to determine when it has a new point of attachment, i.e., that it needs a new IP address. There are several cell-switching algorithms that describe ways to choose between different foreign agents, e.g., Lazy Cell Switching (LCS) and Eager Cell Switching (ECS) [11]. In addition, a mobile node may broadcast *agent solicitations* to find foreign agents. A foreign agent that receives an agent solicitation should reply with a unicast agent advertisement.

B. *AODV*

AODV [4], [9] is a distance vector routing protocol that operates on-demand. There are no periodic routing table exchanges; routes are only set up when a node wants to communicate with some other node. Only nodes that lie on the path between the two end nodes keep information about the route.

Whenever a node wishes to communicate with a destination for which it has no routing information, it initiates route discovery. The aim of route discovery is to set up a bidirectional route from the source to the destination. Route discovery works by flooding the network with route request (RREQ) packets. Each node that receives the RREQ looks in its routing table to see if it is the destination or if it has a fresh enough route to the destination. If it does, it unicasts a route reply (RREP) message back to the source, otherwise it rebroadcasts the RREQ. The RREP is routed back on a temporary reverse route that was created by the RREQ.

Each node keeps track of its local connectivity, i.e., its neighbors. This is performed either by using periodic exchange of so-called HELLO messages, or by using feedback from the link-layer upon unsuccessful transmission. If a route in the ad hoc network breaks, some node along that route will detect that the next hop router is unreachable based upon its local connectivity management. If this node has any active neighbors that depend on the broken link, it will propagate route error (RERR) messages to all of them. A node that receives a RERR will do the same check and if necessary propagate the RERR further in order to inform all nodes concerned.

AODV uses sequence numbers to determine freshness of routing information, thereby preventing routing loops.

III. Internet Access

The characteristics of an ad hoc network differ substantially from those of the fixed Internet. Furthermore, connecting an ad hoc network to the Internet brings up several issues regarding routing and how to provide nodes within an ad hoc network with IP addresses that are routable to from the fixed Internet.

This section discusses some of these routing and addressing issues. Also, since the MIPMANET solution is based on Mobile IP using foreign agent care-of addresses, this section also examines the problems that arise when using Mobile IP within a multihop ad hoc network.

A. *Routing & Addressing*

Addressing in the Internet is hierarchical with IP addresses divided into a network ID and a host ID. All hosts on a certain network use the same network ID. In this way, each IP address is mapped to a physical location that can be derived by looking at the network ID of the IP address. This means that an Internet host does not have to keep track of routes to every Internet host. Instead, routing information can be aggregated; one entry in the routing table can handle all hosts that share the same network ID. Also, default routes can be used when no other route exists to a destination. The ability to use one route to an entire network instead of having one route per host and the ability to use default routes are two powerful features of Internet routing.

In ad hoc networks on the other hand, these features have not been required. The reason for this is that the traditional view of ad hoc networks has been as stand-alone networks temporarily formed by mobile nodes that can come and go as they wish. As such, the ad hoc network should be able to operate without any centralized control or configuration. Also, any set of nodes should be able to form an ad hoc network regardless of which addresses they use and without having to use any particular network ID. This implies that one no longer can decide if a node belongs to a particular network by looking at the network ID. In such an autonomous ad hoc network without the hierarchy that the network ID creates there is no meaningful use of default routes, since either the recipient is reachable within the ad hoc network or it is not reachable at all. As a result of this, routing in ad hoc networks is typically performed using only host specific routes.

Another thing that distinguishes an ad hoc network from a fixed LAN is the IP multihop communication within the ad hoc network. Nodes in an ad hoc network cannot expect to have link-layer connectivity with all other nodes in the ad hoc network. In order to reach a gateway between the ad hoc network and the fixed Internet, nodes must use IP layer routing. Today, many ad hoc routing protocols use an on-demand approach. This means that the routing protocol only operates when there are packets that demand to be routed. When there is a packet to send, the routing protocol tries to find a suitable route through the network on-the-fly. Several studies show that an on-demand approach has many advantages in such dynamic environments as ad hoc networks, e.g., [14], [15], [16].

If the traditional view of ad hoc networks should be preserved while additionally providing Internet access, several issues arise. Since nodes within an ad hoc network should not have to make any assumptions about their network ID's, it is not possible to decide whether a destination is located within the ad hoc network or not by simply looking at the destination's network ID. Also, when using on-demand routing, a node cannot expect to have routes to all hosts reachable within the ad hoc network beforehand since routes only are set up when needed. The fact that we do not have a host route to a host does not necessarily mean that it is not reachable within the ad hoc network. Thus, the route discovery mechanism of the ad hoc routing protocol has to search for the destination within the ad hoc network *before* it can decide whether the destination is within the ad hoc network or not.

Another problem is how to make a node in an ad hoc network reachable from the fixed Internet. To allow this, the node needs an IP address that is routable from the rest of the Internet. This could by accomplished by making use of the fact that there must be at least *one* node belonging to the ad hoc network that has a routable IP address — a node that resides on the border between the ad hoc network and the fixed Internet.

B. Mobile IP

Since Mobile IP was designed primarily for the fixed Internet and wireless leaf networks, several issues arise when applying it to mobile ad hoc networking. This section describes some of the problems that arise when using Mobile IP for Internet access in a multihop ad hoc network.

B.1 Implications of Multihop Communication

One of the key features of ad hoc networks is multihop communication. Mobile IP on the other hand was designed to have the foreign agent and the visiting node on the same link. When they have link-layer connectivity, packets to the visiting node are forwarded by the foreign agent using the link-layer address of the visiting node. In an ad hoc network, the foreign agent and a visiting node might not have link-layer connectivity, but instead have to use multihop communication. Thus, when applied to an ad hoc network, Mobile IP must rely on the network routing protocol used in the ad hoc network for *routing* packets between the foreign agent and the mobile node.

Another problem that arises when applying Mobile IP to ad hoc networks is that broadcasts are much more costly in a multihop ad hoc network than on a single link. A link-local broadcast is received by all hosts on a link, e.g., all hosts within a wireless LAN cell, but none of the recipients need to forward it further. A broadcast in an ad hoc network on the other hand floods the whole network, i.e., is both received and transmitted by every node in the ad hoc network. Such flooding costs a lot of bandwidth and energy, which are both typically limited resources in an ad hoc network. Hence, it is desirable to reduce the number of broadcasts.

The fact that an ad hoc network uses multihop communication also has impact on the movement detection mechanism supported by Mobile IP. A visiting node cannot determine if a foreign agent is reachable by using link-layer feedback anymore. It has to rely on the routing protocol to determine if there is a route to the foreign agent or not. It is also more difficult to decide between several possible foreign agents as the quality of the communication with each foreign agent may depend on the quality of several links.

B.2 Implications of On-Demand Routing

As said earlier, many promising routing protocols for ad hoc networks operate on-demand. Mobile IP on the other hand uses a proactive approach. The foreign agents announce their existence by broadcasting agent advertisements periodically regardless of whether someone wants the information or not. Thus, the basic design of the two are quite contradictory.

Adjusting Mobile IP to operate in a more on-demand fashion would have negative effects on several of Mobile IP's mechanisms (including agent discovery, movement detection and reachability) since the visiting nodes would receive less information about existing foreign agents. On the other hand, to provide the visiting nodes with as much information as in ordinary Mobile IP, other nodes that are not using Mobile IP would suffer because of the traffic that all agent advertisements and agent solicitations flooding the network would impose. This issue will be examined further in Section V, but before that MIPMANET will be presented.

IV. MIPMANET

MIPMANET is designed to provide nodes in ad hoc networks with access to the Internet and the mobility services of Mobile IP. The solution uses Mobile IP foreign agents as access points to the Internet in order to keep track of in which ad hoc network a node is located and to direct packets to the border of that ad hoc network. The ad hoc routing protocol is used to deliver packets between the foreign agent and the visiting node. A layered approach with tunneling is used for the outward data flow to separate the Mobile IP functionality from the ad hoc routing protocol. All this makes it possible for MIPMANET to provide Internet access with the ability for nodes to select and perform seamless switching between multiple access points.

In short, MIPMANET works as follows:

1) Nodes in an ad hoc network that want Internet access use their home address for all communication and register with a foreign agent.

2) To send a packet to a host on the Internet: Tunnel the packet to the foreign agent with whom you are registered.

3) To receive packets from hosts on the Internet: The packets are routed to the foreign agent by ordinary Mobile IP mechanisms. The foreign agent will then deliver the packets to the node in the ad hoc network.

4) Nodes that do not require Internet access will see the ad hoc network as a stand-alone network, i.e., they will not need any knowledge about routes to destinations outside of the ad hoc network.

The layering of Mobile IP and ad hoc routing functionality is illustrated in Fig. 1. By the use of tunneling, the ad hoc network becomes transparent to Mobile IP.

A. Foreign Agents & Tunneling

Using Mobile IP foreign agents as Internet access points is advantageous in many ways. A Mobile IP foreign agent can provide Internet access to an entire ad hoc network using a single IP address as care-of address in addition to the home addresses of each mobile that is to be reachable from the Internet. A node with arbitrary home address can attach to any ad hoc network and have Internet access as long as there is a foreign agent that is willing to serve in that network. When registered with a foreign agent, the node is routable by its home address. Mobile IP also provides seamless transparent roaming between different networks, including different ad hoc networks.

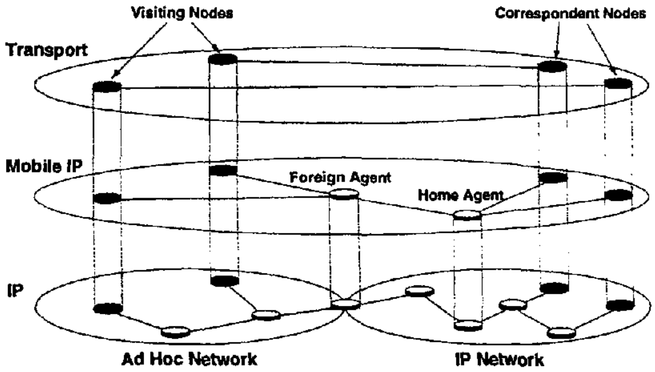


Fig. 1. A conceptional view of MIPMANET

If an ad hoc network does not have a network ID it is not possible to decide whether a destination is located within the ad hoc network or not by simply looking at the destination's network ID. Instead, MIPMANET lets the route discovery mechanism of the ad hoc routing protocol search for the destination within the ad hoc network before it can be decided whether the destination is within the ad hoc network or not.

By using tunneling, MIPMANET can incorporate the default route concept into on-demand ad hoc routing protocols like AODV and DSR [3] without incurring any major modifications. Packets addressed to destinations that are not found within the ad hoc network can simply be tunneled to the foreign agent (assuming that the node is registered with a foreign agent).

Since a node that wants Internet access has to register with a foreign agent, it knows the IP address of the Internet access point. It can then tunnel packets to that access point (i.e. the foreign agent) by encapsulating them with the IP address of the access point as the destination address in the outer IP header [17]. The ad hoc routing protocol then treats the encapsulated packet just as any other packet since both source and destination reside within the ad hoc network. Mobile IP does not have to be concerned with routing within the ad hoc network, this is handled by the ad hoc routing protocol. If a node does not have a route to the foreign agent the route discovery mechanism is used to find a route. If the node is not currently registered with any foreign agent, it considers the destination to be unreachable, since it does not know where to tunnel packets.

By using this solution only registered visiting nodes get Internet access; the only traffic that will enter the ad hoc network from the Internet is traffic that is tunneled to the foreign agent from a registered node's home agent and the only traffic that will leave the ad hoc network is traffic that is tunneled to the foreign agent from a registered node.

B. Adapting Mobile IP

As discussed in Section III-B, one issue when using Mobile IP foreign agents is that according to Mobile IP visiting nodes must have link-layer connectivity with their foreign agent. Since such link-layer connectivity cannot be expected in an ad hoc network, ad hoc routing has to be used between the foreign agent and the visiting node. Instead of using link-layer addresses as identifiers, network-layer identifiers, i.e., IP addresses have to be used. In this paper it is assumed that a mobile node that wants Internet access has been assigned a home address that is valid on the Internet. This home address can then be used on the ad hoc network as well.

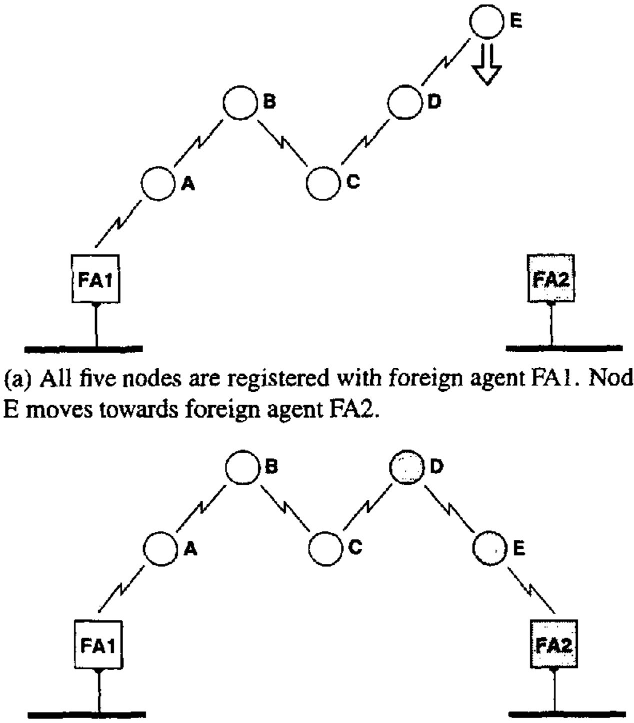
In the following sections the different Mobile IP mechanisms that are affected by MIPMANET will be discussed further.

B.1 Periodic Agent Advertisements

In ordinary Mobile IP the minimum time between two consecutive agent advertisements is one second. This is quite frequent for use in an ad hoc network, taking into consideration that every periodic advertisement involves flooding the ad hoc network. Although the exact beacon period to use has not been evaluated, a period of 5 seconds has been used in our simulations. By increasing the beacon period, the ad hoc network is flooded less often. However, this will also have some negative effects on mechanisms in Mobile IP, i.e., agent discovery, movement detection and reachability since information about available foreign agents is spread less frequently within the ad hoc network.

B.2 Movement Detection

Since there can be multiple hops between foreign agents and the visiting nodes, it is not as straightforward to choose between foreign agents in an ad hoc network as in ordinary Mobile IP enabled networks. Unfortunately none of the movement detection methods provided by Mobile IP is suitable. For example, Lazy Cell Switching (LCS) says that a node should stick to the same foreign agent as long as possible. However, because of the multihop nature of ad hoc networks, this decision might be very bad in many situations. The problem with Eager Cell Switching (ECS) is that it assumes movement along a straight line. Because of this it does not allow a visiting node within range of two different foreign agents to switch back and forth between them. The ability to do so might in fact be desirable, since the ranges of the foreign agents are extended by the multihop communication.



(a) All five nodes are registered with foreign agent FA1. Node E moves towards foreign agent FA2.

(b) FA2 has sent two agent advertisements into the ad hoc network. Nodes D and E have decided to switch to FA2.

Fig. 2. Illustration of the MIPMANET Cell Switching Algorithm

MIPMANET uses hop count as the metric to decide whether a visiting node should change foreign agent or not. The expectation is that the number of hops to the Internet access point is closely related to both delay and the fraction of packets received. The MIPMANET Cell Switching (MMCS) algorithm is as follows:

A registered visiting node should register with another foreign agent if it is at least two hops closer to this foreign agent than the foreign agent that it is currently registered through, for two consecutive agent advertisements.

MMCS is similar to ECS. The difference is that MMCS allows visiting nodes to switch back and forth between foreign agents in a somewhat controlled manner. MMCS prevents high frequent oscillations and decreases the probability of a visiting node registering with a foreign agent that is only temporarily better. MMCS will also help to spread the visiting nodes registrations among the available foreign agents. Fig. 2 illustrates MMCS in action.

According to Mobile IP a visiting node should always have a valid agent advertisement from the foreign agent through which it is currently registered, otherwise it should consider the contact with the foreign agent to be lost. As the lifetime of an agent advertisement is three times the beacon period, a node should be allowed to miss three consecutive agent advertisements.

If the visiting node considers the contact to be lost, but has received agent advertisements (that have not expired) from other foreign agents then the node will register with the closest known foreign agent. Otherwise it will send an agent solicitation. MIPMANET uses the hop count to each foreign agent as the metric to determine which foreign agent a visiting node should be registered with. The hop count can be acquired by for example letting all foreign agents use a well-known predetermined value in the time-to-live field of the IP header.

An agent advertisement beacon period of 5 seconds results in an agent advertisement lifetime of 15 seconds. In the worst case a node would wait 15 seconds before it would consider the contact with its foreign agent to be lost. To make the node detect the loss of contact faster, feedback from the underlying protocols is used. If a node wants to send a packet to the Internet it first has to tunnel it to the foreign agent. If the routing protocol cannot find a route it will send a destination unreachable message to Mobile IP. Mobile IP can then act as if it has lost contact with the foreign agent and start looking for a new foreign agent. In this way, the time it takes for a node to decide that it has lost contact with it's foreign agent is reduced down to the time it takes for the underlying protocol to decide that the foreign agent is unreachable.

B.3 Registration & Datagram Delivery

The registration procedure is almost the same as in ordinary Mobile IP with the exception that the registration request now may have to traverse multiple hops before reaching the foreign agent (and vice versa for the registration reply). What has to be modified is the way the foreign agent handles its visitor list and since reverse tunneling is used, the setup of the tunnel between the visiting node and the foreign agent.

In Mobile IP the foreign agent stores the link-layer address from which the registration request is received in its visitor list. If a visiting node uses multihop communication to reach the foreign agent, that link-layer address belongs to the first intermediate node (seen from the foreign agent). Thus, packets that are destined for the visiting node should instead be forwarded using information provided by the ad hoc routing protocol. If the link-layer address is used and the route to the visiting node changes, the entry in the visitor list has to be modified. If the routing table is used instead, the visitor list can remain unchanged as long as *some* route exists.

When a node registers with a foreign agent, Mobile IP sets up a default route to that foreign agent. In MIPMANET, the route discovery mechanism of the ad hoc routing protocol is used for all destinations. If the destination is not found within the ad hoc network, a host route is set up that tunnels packets to the foreign agent according to the default route. Packets destined to a correspondent node on the fixed Internet can then be tunneled to the foreign agent from where they can be delivered to the correspondent node by ordinary IP routing. When Mobile IP (in the visiting node) determines that it has lost contact with the foreign agent it was registered with, Mobile IP has to remove the default entry in the routing table as well as all host routes that use the tunnel, as the tunnel no longer should exist.

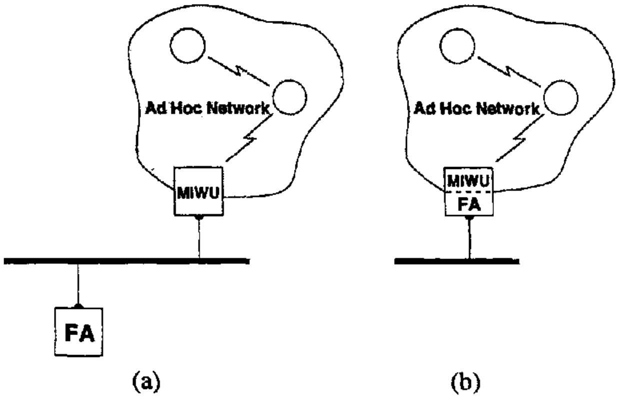


Fig. 3. The MIPMANET Interworking Unit (MIWU) is either on the same LAN as (a), or co-located with (b), the Foreign Agent (FA).

MIPMANET uses reverse tunneling as defined in RFC 2344 [18]. This means that packets from a registered visiting node should be tunneled all the way to the home agent. However, for MIPMANET to work properly, the only requirement is that packets that are destined to the fixed Internet are tunneled from the visiting node to the foreign agent. When the foreign agent receives a tunneled packet it could send the decapsulated packet to the correspondent node directly. Our reason for choosing reverse tunneling is that many Mobile IP implementations already include this mechanism.

C. *The MIPMANET Interworking Unit*

To be able to use the original code in the foreign agents all new functionality has been put in a separate interworking unit, the *MIPMANET Interworking Unit* (MIWU), that is inserted between the foreign agent and the ad hoc network. The MIWU can be put either in the foreign agent itself or in a host on the same link as the foreign agent, as shown in Fig. 3. From a foreign agent's point of view the MIWU will look like a visiting node that is registering different IP addresses, but with the same link-layer address. The MIWU transforms Mobile IP's link-layer communication into network layer communication that can be routed on the ad hoc network (and vice versa). All ad hoc routing functionality can be put in the MIWU.

V. Simulations

To be able to evaluate MIPMANET and study it's different mechanisms in more detail, MIPMANET has been implemented in Network Simulator 2 (*ns2* [7], [8]) using the mobility extensions [19] developed by the Carnegie Mellon University Monarch project. The AODV routing protocol has been used for routing inside the ad hoc network in the simulations.

The major mechanism studied with the simulations is the periodic agent advertisements.

As mentioned earlier, one way of adapting Mobile IP to an ad hoc network with on-demand routing could be to skip the periodic broadcast of agent advertisements. Mobile nodes would then have to use the agent solicitation mechanism to find foreign agents. As the periodic agent advertisements are used by Mobile IP to maintain reachability and perform movement detection, it might not be a good idea to skip them completely. Another solution could be to unicast them periodically to registered nodes only. This means that each foreign agent periodically unicasts agent advertisements only to mobile nodes that are registered through that particular foreign agent. This approach will be referred to as *the unicast approach*, whereas the approach described in Section IV will be referred to as *the broadcast approach.*

By using the unicast approach, a visiting node will only receive information from the foreign agent that it is currently registered with. The only way to receive information from other foreign agents is to use agent solicitations, but that is only performed when a node does not have contact with any foreign agent. This means for example that a node can be several hops closer to a foreign agent other than the one it is registered with without knowing about it. Because of this, the ability to switch between foreign agents is lost with the unicast approach. The visiting nodes will register with a foreign agent and stick with that foreign agent until it is no longer reachable. Then, and only then they will start looking for a better foreign agent. The expected gain with the unicast approach is that when there only is small percentage of visiting nodes in the ad hoc network, the Mobile IP overhead will be much lower, thus disturbing non-Mobile IP nodes less.

The simulation study presented in this section aims at evaluating the differences between the broadcast and the unicast approach.

A. *Simulation Setup*

The scenario studied considers 15 mobile nodes that move randomly over a rectangular (1000m x 500m) flat space for 900 seconds of simulated time, and two foreign agents, one on each side of the rectangle. Besides these 17 nodes, there are a number of wired nodes: home agents and correspondent nodes. Since MIPMANET's only modifications to Mobile IP concerns the communication between the foreign agents and visiting nodes, we will focus on the wireless part of the scenario.

The main parameter in the simulations is the number of visiting nodes in the network, i.e., how many of the 15 mobile nodes use Mobile IP.

The mobile nodes move according to the "random waypoint" model [3]. To quantify the mobility of the nodes, the *mobility* metric as defined in [15] has been used. This metric reflects the relative movement between nodes; parallel movement does not add to the mobility. The mobility in the simulations is about 1.5 m/s; the nodes themselves move at random absolute speeds below 8 m/s.

TABLE I
MIPMANET PARAMETERS

Parameter	Value
Beacon period time	5 s
Agent advertisement lifetime	15 s
Nominal time between two solicitations	2 s
Maximum time between two solicitations	
–broadcast approach	60 s
–unicast approach	16 s

Communication in the simulations is carried out between wireless visiting nodes and wired correspondent nodes. It is duplex; both the visiting nodes and their correspondent nodes are constant bit rate (CBR) sources. Each CBR source sends 5 packets per second containing 128 bytes of data. The time when a visiting node starts to send CBR packets is chosen randomly within the first ten seconds of the simulation. After this start time the node continues to send CBR packets for the duration of the simulation.

Mobility and traffic load have been selected not to stress AODV too much. The aim of our evaluation is *not to study AODV.*

As mentioned earlier, the AODV routing protocol has been used in the simulations. Except for the route reply wait time parameter, *RREP_WAIT_TIME*, the default values given in the AODV draft [9] have been used. A *RREP_WAIT_TIME* of one second has been used to enable nodes to detect a lost foreign agent faster. Also, link-layer feedback has been used to allow a more rapid response to route changes. No HELLO messages have been used.

Finally there are some MIPMANET specific parameters that have been used in the simulations. These parameters are compiled in Table I.

B. *Results*

Fig. 4 shows the difference in Mobile IP overhead between the broadcast and unicast approaches[1]. This overhead includes all agent advertisements, agent solicitations, registration requests and registration replies. The overhead is the sum for 900 s of simulated time and is counted on a per-hop basis, meaning that a packet that travels four hops is counted four times.

For both approaches, the registration request/replies should be approximately linear in number of visiting nodes. With

[1] The overhead is only calculated at the network level (IP level). No physical layer framing or MAC layer overhead has been included.

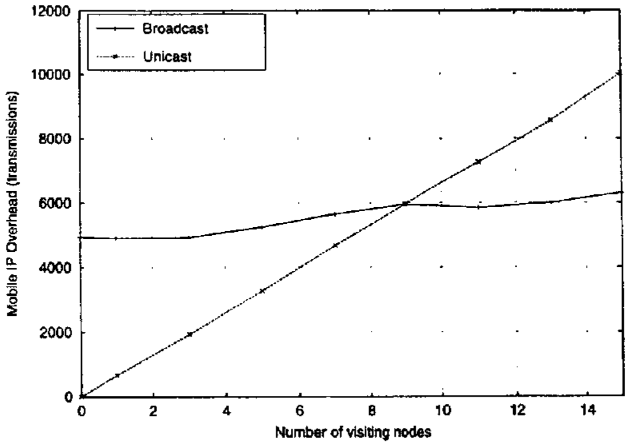


Fig. 4. Mobile IP overhead

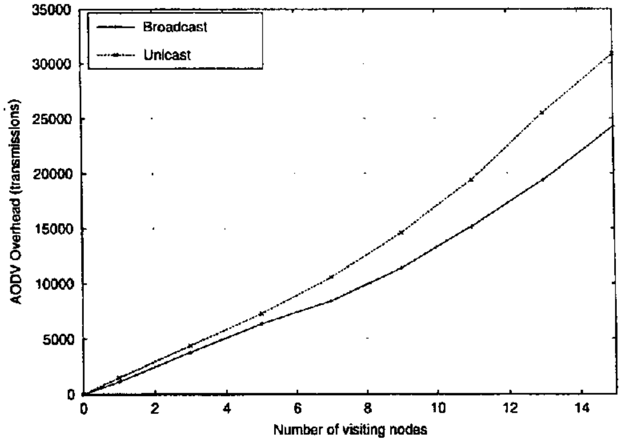


Fig. 5. AODV overhead

the broadcast approach the two foreign agents flood the network periodically with their agent advertisements, regardless of whether any node is interested in this information or not. Thus the Mobile IP overhead will have one part that is approximately constant. This can be seen in Fig. 4 where the overhead for the broadcast approach is almost constant, it only increases marginally as the number of visiting nodes increases.

With the unicast approach a foreign agent only sends agent advertisements to nodes that are registered through it. Thus the two foreign agents will not send any agent advertisements if no nodes are registered through them. For every node that is registered with some foreign agent the overhead will increase since a foreign agent has to unicast one agent advertisement to every registered node. This explains why the Mobile IP overhead with the unicast approach, shown in Fig. 4, is approximately linear with the number of visiting nodes.

The AODV overhead in total number of transmissions is shown in Fig. 5. The overhead starts at zero for both approaches as the periodic broadcasts do not cause any AODV control packets to be sent. Unicasting agent advertisements generates more AODV control packets than if broadcast is used. Accordingly, the unicast approach generates most AODV overhead.

If you were to only look at the Mobile IP overhead and the AODV overhead it seems as if the unicast approach is better than the broadcast approach if the percentage of visiting nodes is low. It is only when half or more of the nodes are visiting nodes that the broadcast approach generates less overhead than the unicast approach. However, considering the total number of transmissions performed in the ad hoc network gives a completely different picture. Fig. 6 shows that the broadcast approach generates less total transmissions than the unicast approach, *regardless of how many visiting nodes there are in the network*. It is only when there are *no* visiting nodes in the ad hoc network that the broadcast approach generates more traffic than the unicast approach.

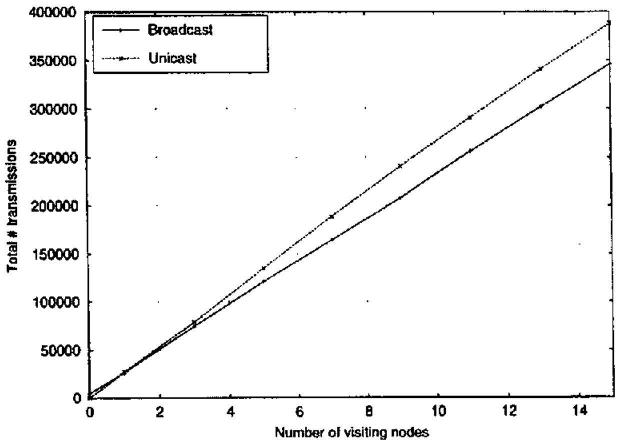


Fig. 6. Total number of transmissions

As shown in Fig. 7, the fraction of packets received is better with the broadcast approach than with the unicast approach. Since CBR traffic is used, a higher fraction of packets received implies a higher number of transmissions of data. In spite of that, the total number of transmissions is higher for the unicast approach. One explanation of this is that the protocol overhead is larger for the unicast approach. The loss of a packet may be the result of a broken link, and as shown in Fig. 5 the routing overhead is larger for the unicast approach. However, this difference in overhead only makes up a small part of the difference in total number of transmissions.

The larger part of the difference in total number of transmissions is instead that a visiting node in the broadcast approach is able to switch to the foreign agent that is closest. This switch is possible since it receives information from all available foreign agents in the ad hoc network. On the other hand, with the unicast approach a visiting node only receives information from the foreign agent it is currently registered with. Fig. 8 shows the average number of times a visiting node switches

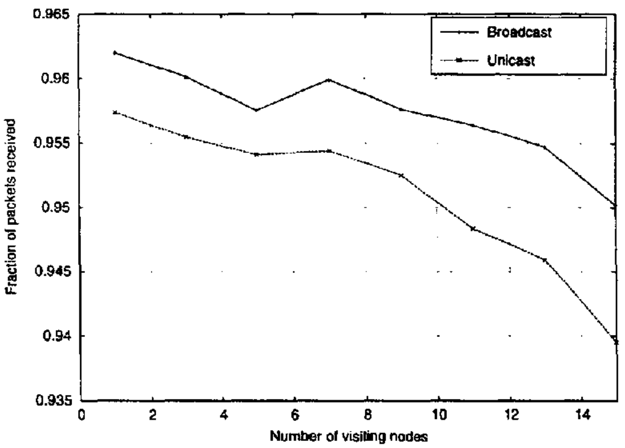


Fig. 7. Fraction of packets received

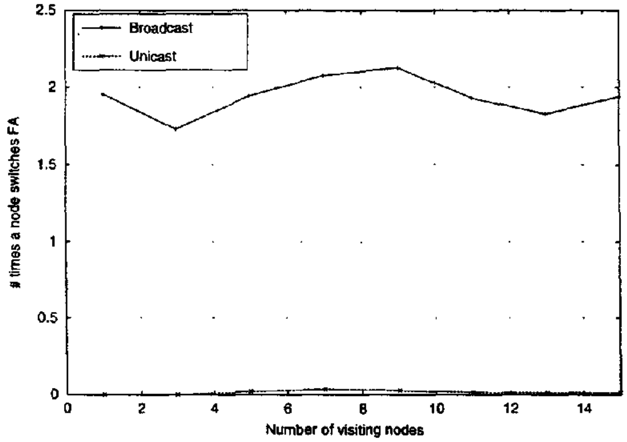


Fig. 8. Mobile IP reregistrations

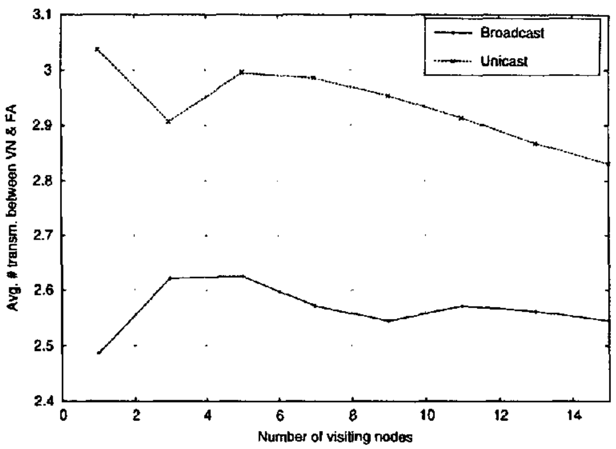


Fig. 9. Average number of transmissions to deliver data

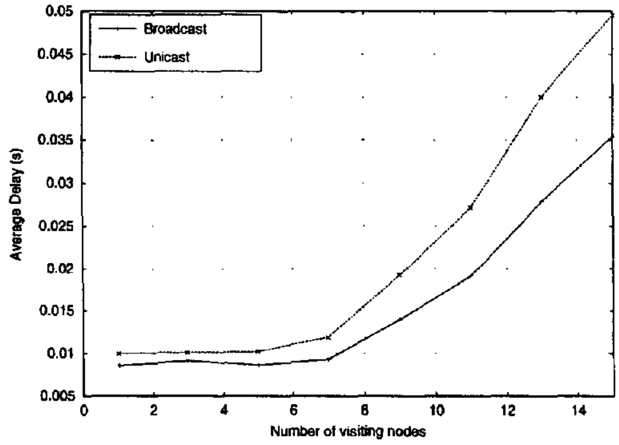


Fig. 10. Delay for data packets

to a foreign agent that is closer (using MMCS) in the two approaches. With the broadcast approach the nodes switch about 2 times on average whereas with the unicast approach they cannot reregister with a better foreign agent as they do not receive information about them.

The fact that a visiting node considers its foreign agent to be unreachable does not necessarily mean that the foreign agent considers the visiting node to be unreachable. Thus, in the unicast approach, the situation can occur where a foreign agent continues to unicast agent advertisements to a visiting node even though the visiting node has switched to the other foreign agent. This is why it sometimes happens that a visiting node reregisters with a closer foreign agent without first loosing contact with the foreign agent it is currently registered with.

The fewer number of hops a visiting node can be from its foreign agent, the fewer number of hops packets have to traverse between them. This can be seen in Fig. 9 that shows the total number of data transmissions divided by the total number of delivered data packets. A packet in the broadcast approach only needs to be transmitted on average about 2.5 times within the ad hoc network before it reaches the foreign agent and vice versa. A packet sent in the unicast approach needs about 3 transmissions to do the same thing. These figures cannot be interpreted as distance in number of hops as they include transmissions of packets that are dropped in between the visiting node and the foreign agent. Thus the actual distance in number of hops is slightly smaller than what Fig. 9 shows.

Another advantage of being able to switch to the closest foreign agent is that the delay for a packet to traverse between a visiting node and its foreign agent can be kept at a minimum. That is why the delay, shown in Fig. 10, in the broadcast approach is lower than the unicast approach. Fig. 10 also shows that the delay increases with extra visiting nodes, starting at about seven visiting nodes. This is probably due to congestion. As all traffic passes through either of the two foreign agents, the areas around them are likely to be congested as the number of visiting nodes increases.

To sum up, these results indicate that it is very important for a visiting node to be close to its foreign agent. This results in a lower traffic load in the ad hoc network and a lower delay for data packets. Hence, it is worthwhile distributing information about available foreign agents even though this means some extra cost in terms of broadcasting agent advertisements periodically.

VI. Related Work

There has not been much work published in the field of connecting ad hoc networks to the Internet and using Mobile IP in ad hoc networks, prior to this paper.

In "Ad Hoc Networking with Mobile IP" by Hui Lei and Charles E. Perkins. [20], a solution for using Mobile IP on top of a proactive routing protocol is described. The routing protocol that is used is said to be "a modified RIP". The idea is that every node within an ad hoc network should set up a default route to an available access point, i.e., foreign agent. However, this approach does not work in an ad hoc network where on-demand routing is used and where no assumptions about network ID has been made. The reason for this is, as discussed in Section III-A, that a node within the ad hoc network must have a host route to a destination in order to determine whether the destination resides within the ad hoc network or not. Hence, applied to an on-demand routing protocol the solution described in [20] would have the effect that every intermediate node in the path to the foreign agent would have to search for the destination within the ad hoc network.

In "Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks" by Josh Broch, David A. Maltz, David B. Johnson, Yin-Chun Hu, and Jorjeta Jetcheva [6], an initial design of an addressing architecture that among other things could be used to provide Mobile IP support within an ad hoc network is presented. The section that covers interworking between Mobile IP and ad hoc networking is however not very elaborate. The idea is that the mobile node piggybacks an agent solicitation on a route request. When the foreign agent receives the solicitation, it will unicast an agent advertisement in reply. Once the agent advertisement reaches the mobile node, the mobile node can register with the foreign agent. Most of the issues presented in this (MIPMANET) paper are however not even recognized in [6], e.g.,

- What happened with the periodic agent advertisements?
- What happens if there are several FAs to choose from?
- How can the mobile node detect that it has moved?
- How is handoff handled?

It should perhaps be noted that both the above papers use foreign agents to enable Mobile IP's services within ad hoc networks.

VII. Conclusion

This paper has presented a solution of how to interconnect an ad hoc network with the Internet called MIPMANET. Ad hoc networking enables IP mobility within a network whereas Mobile IP enables IP mobility between networks. By combining these two, MIPMANET allows mobile nodes to enjoy extended IP mobility.

Regarding Mobile IP in mobile ad hoc networks, our proposal includes a new movement detection scheme and the use of reverse tunneling to Internet access points. No major changes have to be made to the foreign agent, all interworking functionality can be put in an interworking unit between the foreign agent and the ad hoc network.

The simulation study has evaluated whether periodic broadcasts of agent advertisements should be unicast or broadcast. In the scenario used, broadcasting agent advertisements periodically is better than unicasting at all times except when there are *no* visiting nodes in the ad hoc network. The visiting nodes get more information and can make better choices of where to be registered (and thus which access point to use to reach the Internet). The simulations have shown that the ability to choose the closest access point to the Internet is highly valuable as that lessens the total load on the network.

The advantages of MIPMANET are:

- It separates the tasks of the routing protocol and Mobile IP and provides transparent interaction between the two.
- The changes to Mobile IP only concern the communication between the foreign agent and the mobile node *within* the ad hoc network. The behavior of Mobile IP on the Internet side is not affected.
- Only minor modifications have to be made in the on-demand routing protocol for interworking with the Internet.
- Nodes in the ad hoc network that are not using Mobile IP see the ad hoc network as a stand-alone network, i.e., they have no knowledge about the Internet.
- By the use of a separate module, called the MIPMANET Interworking Unit (MIWU), only minor modifications have to be made in the foreign agents to make our solution work.

VIII. Future Work

There are several areas related to Internet access and Mobile IP in ad hoc networks that might be the subjects of future work.

- Dynamic address allocation: If there were mechanisms for dynamic address allocation within ad hoc networks, Internet access could be provided in a quite simple manner. Access points could be assigned pools of addresses that can be allocated by nodes that desire Internet access. Nodes that desire the mobility services that Mobile IP offers can use the dynamically allocated addresses as co-located care-of addresses.

- Cooperating access points: By letting the access points cooperate, perhaps load-balancing could be performed and handover performance could be boosted.

- Cost in fixed network: In this simulation study, the cost of using an access point only takes the ad hoc network into account. The fixed network has not been considered. There could however be many reasons for taking the fixed network into account as well.

- Non-layered approach: MIPMANET uses a layered approach to separate Mobile IP and the ad hoc routing functionality. How would the performance of the system be affected if these two were integrated? Would it be much more efficient to integrate the agent discovery with the routing protocol, minimizing its overhead?

- Multicast: If multicast were implemented in an efficient way in ad hoc networks, that would alleviate the discussion of multiple unicasts vs. broadcast. Mobile IP's messages for agent advertisements and agent solicitations could be sent to a multicast group that only interested nodes participate in. Currently there is no detailed evaluation of different proposed multicast schemes; the cost of using multicast in ad hoc networks has not been explored.

- Mix between proactiveness and on-demand mechanisms: This paper shows that broadcasting agent advertisements in a proactive way has advantages. However, we have not examined what an optimal mix between proactiveness and on-demand mechanisms would be.

REFERENCES

[1] "The Internet Engineering Task Force (IETF)," Webpage, http://www.ietf.org/.

[2] Chairs: Joseph Macker and Scott Corson, "Mobile ad hoc networks, IETF working group," Webpage, http://www.ietf.org/html.charters/manet-charter.html.

[3] David B. Johnson and David A. Maltz, *Mobile computing*, chapter 5, pp. 153–181, Kluwer Academic Publishers, 1996.

[4] Charles E. Perkins and Elizabeth M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, Feb. 1999, pp. 90–100.

[5] Charles E. Perkins, "RFC 2002: IP mobility support," Oct. 1996, Updated by RFC2290. Status: PROPOSED STANDARD.

[6] Josh Broch, David A. Maltz, and David B. Johnson, "Supporting hierarchy and heterogeneous interfaces in multi-hop wireless ad hoc networks," in *Proceedings of the Workshop on Mobile Computing*. IEEE, June 1999.

[7] Kevin Fall and Kannan Varadhan, *ns Notes and Documentation*, The VINT Project, Work in progress.

[8] "UCB/LBNL/VINT Network Simulator - ns (version 2)," Webpage, http://www-mash.cs.berkeley.edu/ns/.

[9] Charles E. Perkins, Elizabeth M. Royer, and Samir R. Das, "Ad hoc on-demand distance vector (AODV) routing," Internet draft (work in progress), IETF Mobile Ad Hoc Networks Working Group, June 1999, draft-ietf-manet-aodv-03.txt.

[10] Charles E. Perkins, "Mobile IP," *IEEE Communications Magazine*, pp. 84–99, May 1997.

[11] Charles E. Perkins, *Mobile IP: Design Principles and Practices*, Addison-Wesley, 1998.

[12] James D. Solomon, *Mobile IP: The Internet Unplugged*, Prentice Hall, 1998.

[13] R. Droms, "RFC 2131: Dynamic host configuration protocol," Mar. 1997, Obsoletes RFC1541. Status: DRAFT STANDARD.

[14] Josh Broch, David A. Maltz, David B. Johnson, Yin-Chun Hu, and Jorjeta Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in *Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking*. ACM/IEEE, Oct. 1998, pp. 85–97.

[15] Per Johansson, Tony Larsson, Nicklas Hedman, Bartosz Mielczarek, and Mikael Degermark, "Scenario-based performance analysis of routing protocols for mobile ad-hoc networks," in *Proceedings of the Fifth Annual International Conference on Mobile Computing and Networking*, Aug. 1999.

[16] David A. Maltz, Josh Broch, and David B. Johnson, "The effects of on-demand behaviour in routing protocols for ad hoc networks," *IEEE Journal on Selected Areas of Communications*, 1999.

[17] Charles E. Perkins, "RFC 2003: IP encapsulation within IP," Oct. 1996, Status: PROPOSED STANDARD.

[18] G. Montenegro, "RFC 2344: Reverse tunneling for Mobile IP," May 1998, Status: PROPOSED STANDARD.

[19] The CMU Monarch Project, *The CMU Monarch Project's Wireless and Mobility Extensions to ns*, Aug. 1999.

[20] Hui Lei and Charles E. Perkins, "Ad hoc networking with Mobile IP," in *Proceedings of 2nd European Personal Mobile Communication Conference*, Sept. 1997.