Internet Connectivity for Ad hoc Mobile Networks

Yuan Sun Elizabeth M. Belding-Royer
Department of Computer Science
University of California, Santa Barbara
{suny, ebelding}@cs.ucsb.edu

Charles E. Perkins
Communications System Laboratory
Nokia Research Center
charliep@iprg.nokia.com

Abstract

The growing deployment rate of wireless LANs indicates that wireless networking is rapidly becoming a prevalent form of communication. As users become more accustomed to the use of mobile devices, they increasingly want the additional benefit of roaming. The Mobile IP protocol has been developed as a solution for allowing users to roam outside of their home networks, while still retaining network connectivity. The problem with this solution, however, is that the deployment of foreign agents is expensive because their coverage areas are limited due to fading and interference. To reduce the number of foreign agents needed while still maintaining the same coverage, ad hoc network functionality can cooperate with Mobile IP such that multi-hop routes between mobile nodes and foreign agents can be utilized. In this work, we present a method for enabling the cooperation of Mobile IP and the Ad hoc On-Demand Distance Vector (AODV) routing protocol, such that mobile nodes that are not within direct transmission range of a foreign agent can still obtain Internet connectivity. In addition, we describe how duplicate address detection can be used in these networks to obtain a unique co-located care-of address when a foreign agent is not available.

1 Introduction

Wireless LANs are becoming a prevalent method for obtaining network connectivity because they have the desirable property of allowing users freedom of mobility. Wireless LANs are *infrastructured* wireless networks, whereby mobile nodes communicate directly with an access point to the wired network. This access point typically has both a wired and a wireless interface, and hence serves as a gateway between the two access media. As users continue to gain experience with wireless connectivity, they increasingly want the benefit of roaming. That is, they want to maintain open connections while not being restricted to certain physical areas. Users want the ability to seamlessly roam between domains without having to restart their open connections or obtain a new IP address.

The difficulty with roaming, however, is that normal IP routing is based on the hierarchical IP address assigned to nodes. Hence, when a node leaves the subnet from which its address is assigned, the node cannot be located using IP routing. Its IP address no longer accurately reflects its point of attachment to the network. The Mobile IP protocol [9, 10] allows mobile nodes that are away from their home network to register with a foreign agent and obtain a care-of address on the visited foreign network. This care-of address allows the mobile node to send and receive data packets from its new point of attachment. Mobile IP assumes that a mobile node is within direct transmission range of a foreign agent in order to register with that foreign agent, obtain a care-of address, and acquire Internet connectivity.

One of the biggest challenges to installing wireless LANs is creating coverage maps with no *dead zones*, or areas without coverage. Transmission phenomena such as multipath, fading, and obstacles can make it difficult to avoid such dead zones. Network designers typically expend considerable effort determining an optimum configuration for access points such that dead zones are avoided. This is expensive in terms of network hardware (i.e. access points), the labor required to determine the placement of access points, and

the labor needed to install the access points. The additional requirement of configuring certain nodes to be foreign agents adds to the overall network cost. Mobile nodes visiting a foreign network can only gain network connectivity if they are within the coverage area of a foreign agent. Installing enough foreign agents such that seamless connectivity with the network can be provided is a daunting task.

The alternative to infrastructured wireless networks are *ad hoc* (infrastructureless) wireless networks. An ad hoc network is comprised of mobile nodes that communicate solely over the wireless medium. The mobile nodes often have a limited transmission range. Hence, multi-hop paths are typically required to connect source/destination pairs. The Ad hoc On-Demand Distance Vector (AODV) protocol [11, 13] has been designed to discover and maintain multi-hop paths within an ad hoc network. AODV is a reactive routing protocol, meaning that routes are only discovered when they are needed. Once discovered, the routes are then maintained as long as needed by the source node.

In this work, we propose a method for enabling nodes within an ad hoc network to obtain Internet connectivity when one or more nodes within that network is within direct transmission range of an Internet gateway. Specifically, we describe how the Mobile IP and AODV routing protocols can cooperate to discover multi-hop paths between mobile nodes and foreign agents. These paths allow nodes that are multiple hops from a foreign agent to gain Internet connectivity. In addition, we describe a method for duplicate address detection, whereby a node can obtain a unique co-located care-of address when a foreign agent is not available for the assignment of care-of addresses.

The remainder of this paper is organized as follows. Section 2 presents related work in the area of integrating ad hoc network and infrastructured wireless network technology. Then, section 3 provides an overview of both the Mobile IP and AODV routing protocols. Section 4 describes the method for obtaining a unique *co-located* care-of address on a foreign network. The details of the cooperation between Mobile IP and AODV are presented in section 5. The performance of our protocol is evaluated in section 6. Finally, section 7 concludes the paper.

2 Related Work

One of the earliest approaches for facilitating Internet connectivity for ad hoc networks is described in [7]. In this work, a method for integrating the ad hoc routing protocol daemon with the Mobile IP routing daemon (*mipd*) to manipulate the kernel IP routing table is described. Connectivity within the ad hoc network is provided by *routed*, a modified version of the Routing Information Protocol (RIP) daemon, on each mobile node within the network. This protocol integration enables foreign agents to participate in the ad hoc network routing. For mobile nodes not in the transmission range of foreign agent, *routed* relays agent advertisements or related messages to *mipd*. Each mobile node uses the foreign agent as its default router. A route table manager is used to coordinate the manipulation of the IP route table.

An initial design of integrating the Dynamic Source Routing protocol (DSR) [5] with Internet routing and Mobile IP networks is presented in [2]. In this technique, an addressing architecture for ad hoc networks is described. Individual nodes, working together as an ad hoc network, are assigned home addresses from a single IP subnet. Nodes within range of the foreign agent serve as gateways between the ad hoc network and the Internet. DSR is utilized for routing within the ad hoc network, while normal IP source routing applies to the wired network. In the integration of Mobile IP and DSR, foreign agents are responsible for forwarding packets between the ad hoc and wired networks.

An alternative solution, MIPMANET, is presented in [6]. In this approach, nodes in an ad hoc network that want Internet access register with the foreign agent and use their home address for all communication. Mobile nodes tunnel all packets destined for the Internet to the registered foreign agent. The foreign agent decapsulates the packets and forwards them to the destination. The AODV routing protocol is used to deliver packets between mobile nodes and the foreign agent. Additionally, MIPMANET utilizes a new algorithm,

called MIPMANET Cell Switching (MMCS), to determine when mobile nodes in the ad hoc network should register with a new foreign agent. In this solution, it is assumed that a mobile node that wants Internet access has been assigned a home address that is valid on the Internet.

3 Overview of Mobile IP and AODV

In the following sections overviews of the Mobile IP and AODV networking protocols are provided. Further detail on Mobile IP can be found in [10], and in [11] for AODV.

3.1 Mobile IP

The Mobile IP protocol [9, 10] is currently being standardized by the IP Routing for Wireless/Mobile Hosts (MobileIP) Working Group [1] of the Internet Engineering Task Force (IETF). Mobile IP provides transparent routing of IP datagrams to mobile nodes in the Internet, such that mobile users can connect to the Internet and maintain those connections while they are roaming within different networks.

Mobile IP defines the following functional entities:

- **Mobile Node**: A host that changes its point of attachment from one network or subnetwork to another.
- **Home Agent**: A router on a mobile node's home network that maintains location information for the mobile node and tunnel packets to the node while the node is away from its home network.
- **Foreign Agent**: A router on the mobile node's visited (foreign) network. The foreign agent cooperates with the mobile node's home agent to deliver packets to the mobile node.

Each mobile node has a unique *home address*. Because of the hierarchical nature of IP addressing and routing, the node must be addressable within its home network to receive data packets. In order to maintain existing transport layer connections, a mobile node should continue to use its home address to receive data, even when it leaves its home network. Mobile IP assigns the mobile node a *care-of address* while roaming. This address provides information about the mobile node's current point of attachment to the Internet so that the node can maintain Internet connectivity.

Home agents and foreign agents periodically broadcast *Agent Advertisements* to advertise their presence. Optionally, mobile nodes can send *Agent Solicitation* messages to determine whether any prospective agents are present in the network. A mobile node utilizes Agent Advertisement messages to determine whether it is on its home or foreign network. When a mobile node learns of the foreign agent's presence, it selects a care-of address on the foreign network from one of the advertised care-of addresses in the Agent Advertisement.

To receive data packets on the foreign network, the mobile node must register its current care-of address with its home agent. A *Registration Request* message is transmitted by the mobile node to the foreign agent; this message is then forwarded by the foreign agent to the home agent. Upon the reception of the Registration Request, the home agent records the care-of address of the mobile node and sends a *Registration Reply* back to the mobile node, thereby acknowledging a successful registration.

Data packets sent to the mobile node's home address are intercepted by its home agent. The home agent tunnels those packets to the mobile node's care-of address. The datagrams are received at the tunnel endpoint, decapsulated by the foreign agent, and forwarded to the mobile node.

3.2 AODV

The Ad hoc On-Demand Distance Vector (AODV) [11, 13] routing protocol is a reactive protocol that utilizes a route request/route reply query cycle for route discovery. Once discovered, a route is maintained as long as needed by the source. To guarantee loop freedom, AODV utilizes per-node sequence numbers. A node increments the value of its sequence number whenever there is a change in its local connectivity information.

Route discovery begins when a source node needs a route to some destination. It places the destination IP address and last known sequence number for that destination, as well as its own IP address and current sequence number, into a *Route Request* (RREQ). It then broadcasts the RREQ and sets a timer to wait for a reply.

When a neighboring mobile node receives the RREQ, it first creates a *reverse route entry* for the source node in its route table. It then checks whether it has an unexpired route to the destination node. In order to respond to the RREQ, the node must either be the destination itself, or it must have an unexpired route to the destination whose corresponding sequence number is at least as great as that contained in the RREQ. If neither of these conditions are met, the node rebroadcasts the RREQ.

On the other hand, if it does meet either of these conditions, the node then creates a *Route Reply* (RREP) message. It places the current sequence number of the destination, as well as its distance in hops to the destination, into the RREP, and then unicasts this message back to the source. Intermediate nodes along the path to the source node create a *forward route entry* for the destination node in their route table. Once the source node receives the RREP, it can begin using the route to transmit data packets to the destination.

If the source node does not receive a RREP by the time its discovery timer expires, it rebroadcasts the RREQ. It attempts discovery up to some maximum number of times. If no route is discovered after the maximum number of attempts, the session is aborted.

An active route is defined as a route which has recently been used to transmit data packets. When a link break in an active route occurs, the node *upstream* of the break invalidates all its routes that utilized that link. It creates a *Route Error* (RERR) packet, and places in that packet the IP address of each destination which is now unreachable, due to the link break. The node then broadcasts the RERR message to its neighbors.

When a neighboring node receives the RERR, it in turn invalidates each of the routes listed in the packet, *if* that route used the source of the RERR as a next hop. If one or more routes are deleted, the node then creates and broadcasts its own RERR message. Once a source node receives the RERR, it invalidates the listed routes as previously described. If it determines that it still needs any of the expired routes, it then re-initiates route discovery for that route.

4 Care-of Addresses

Mobile nodes running Mobile IP can acquire care-of addresses in two ways. In the first method, a foreign agent must be available on the foreign network. This agent advertises one or more care-of addresses in its Agent Advertisements. Mobile nodes can then use one of those care-of addresses to obtain Internet connectivity. Agent Advertisement broadcasts within an ad hoc network are discussed further in section 5.2.

The other method for a mobile node to obtain Internet connectivity is to acquire a *co-located* care-of address. This type of care-of address is used when a foreign agent is not available on the network. At minimum, a gateway between the wired and wireless networks must be configured to advertise network prefixes that are routable on the given network. When such a gateway is available, mobile nodes can use the advertised prefix to configure their own care-of addresses.

To obtain a unique care-of address, a mobile node must select a unique identifier to append to the advertised network prefix. A mobile node does not necessarily know the care-of addresses of the other mobile nodes within the wireless network. Hence, it must perform *duplicate address detection* to ensure that its selected address is unique. The following method is based on that described in [12].

When a node requires a unique IP address, it first selects a random host ID from the range $2048 - (2^{(32-n)} - 1)$, where n is the number of significant bits in the advertised network prefix. The node then appends that host ID to the prefix advertised by the Internet gateway. This is the IP address for which it performs duplicate address detection. The node then selects a random, temporary host ID in the range $0 - 2047$ and appends this value to the advertised network prefix. This ID serves as a source IP address for

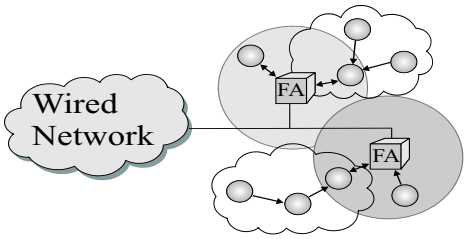


Figure 1: Ad hoc Network with Internet Connectivity.

the short period while the node performs duplicate address detection. The node creates an Address Request (AREQ) by placing its randomly selected source IP address, as well as its temporary IP address, in the AREQ and broadcasts this request to its neighbors.

When a mobile node receives an AREQ message, it creates a *reverse route* entry for the node indicated by the temporary IP address in the AREQ. The node then checks whether its own IP address matches the requested address in the AREQ. If the node's IP address does not match the requested address, it rebroadcasts the packet to its neighbors.

On the other hand, if the node has the same IP address as that requested by the AREQ, then the source node is requesting an IP address that is already in use. In this case, the node with the duplicate IP address creates an Address Reply (AREP) packet. It places the requested IP address in this message, and unicasts this packet to the node that requested the address. The reverse route that was created by the AREQ broadcast is used to route the AREP back to the source node.

When a node originates an AREQ, it sets a timer to wait for the reception of an AREP message. If no AREP is returned for the selected address within a timeout period, the node retries the AREQ up to some maximum number of times. If, after all retries, no AREP is received, the node assumes that the address is not already in use, and that the address can safely be taken for its own.

On the other hand, if the node does receive an AREP within the discovery period, and if the requested IP Address included in the AREP matches the address it was requesting, then this indicates that another node within the ad hoc network is currently using that IP address. In this case, the node randomly picks another host ID from the same $2048 - (2^{(32-n)} - 1)$ range, and begins the duplicate address detection again.

5 Global Internet Connectivity

The Mobile IP and AODV networking protocols can work together to create an environment where multi-hop wireless paths exist between mobile nodes and foreign agents, such as that shown in figure 1. These paths eliminate dead zones and extend the coverage range of the foreign agents. To enable multi-hop Internet connectivity, the proposed method utilizes the AODV routing protocol for the discovery and maintenance of routes within the ad hoc network. The Mobile IP protocol is utilized such that mobile nodes may obtain care-of addresses, and hence Internet connectivity, through a multi-hop path to a foreign agent.

The method proposed here conforms with the Mobile IP [10] and AODV [11] protocols to the largest extent possible. All message types, data structures, and configuration parameters specified within this paper are used unmodified, unless otherwise noted. The following sections describe how Mobile IP and AODV can work together to provide global connectivity for ad hoc networks.

5.1 Data Structures

A foreign agent maintains a Mobile Node Registration List in which it records the IP address of all mobile nodes for which it has received valid registrations. Mobile node registrations have lifetimes, whereby each

mobile node must periodically re-register with its foreign agent to indicate it is still within the ad hoc network. Mobile node registrations that are not periodically refreshed expire and are deleted; an expired registration indicates the mobile node has either left the ad hoc network, or else no longer desires Internet connectivity. The selection of an appropriate lifetime value is determined as specified in the Mobile IP specification [10].

A Foreign Agent List is maintained by each mobile node to record the IP address of foreign agents from which an Agent Advertisement has been received. When a mobile node receives an Agent Advertisement from a new foreign agent, it creates an entry for the foreign agent in its Foreign Agents List and inserts the IP address of that foreign agent. Associated with the entry for the foreign agent is a sequence number, a foreign agent lifetime, and a registration lifetime. The sequence number is the set to the sequence number indicated in the Agent Advertisement. The foreign agent lifetime represents the minimum frequency that the mobile node must receive Agent Advertisements from the foreign agent. This lifetime is a function of the foreign agent's Agent Advertisement transmission rate, and can generally be set to three times this interval. Each time a mobile node receives an Agent Advertisement from the indicated foreign agent, it updates the lifetime and sequence number associated with that entry. If a mobile node has not received an Agent Advertisement from the indicated foreign agent within the specified lifetime, the mobile node must assume it is no longer within multi-hop connectivity of that foreign agent. It therefore removes that entry from its Foreign Agent List. When a mobile successfully registers with a foreign agent, it sets a flag in the entry of the foreign agent with which it has registered, indicating that is its assigned foreign agent.

The registration lifetime in the Foreign Agent List entry indicates the period for which the mobile node's registration is valid at the foreign agent. For foreign agents with which the mobile node is not registered, this timer equals zero. Before the expiration of this timer for valid registrations, the mobile node must refresh its registration at the foreign and home agents by sending a new Registration Request to that foreign agent.

When a mobile node receives an Agent Advertisement from a foreign agent, the AODV module on that node creates a route table entry for the foreign agent. The mobile node then registers with the foreign agent, according to the methods described in sections 5.4 and 5.6. If the mobile node does not actively use the route to the foreign agent, that route will time out according to the specifications of the AODV protocol. Hence it is possible for a mobile node to be registered with a foreign agent but not have a current route to that agent.

5.2 Agent Advertisements

Foreign agents periodically advertise their presence through Agent Advertisement messages. When a mobile node receives an Agent Advertisement, it records the IP address of the foreign agent, together with the sequence number of the Agent Advertisement, in its Foreign Agents List. It then assigns that entry a lifetime. Recording this information serves the dual purpose of tracking the foreign agents from which the mobile node has received Agent Advertisements, as well as preventing re-processing of duplicate Agent Advertisements. If the mobile node later receives the advertisement as it is rebroadcast by the node's neighbors, the mobile checks the foreign agent IP address and advertisement sequence number and does not reprocess the packet. When a node receives duplicate Agent Advertisement messages, it discards the duplicates.

Mobile nodes also use the Agent Advertisement to update their route information to the foreign agent. If the mobile's route to the foreign agent has expired, or if this Agent Advertisement has arrived along a shorter path than the recorded route, the mobile node updates its route information for that foreign agent to indicate the new path.

After processing the Agent Advertisement, the mobile node rebroadcasts the packet on its interfaces. This allows mobile nodes that are not within direct transmission of the foreign agent to receive the Agent Advertisements. Mobile nodes randomize their rebroadcasting of the Agent Advertisement message so that synchronization and subsequent collisions with other nodes' rebroadcasts can be avoided.

5.3 Foreign Agent Discovery

When a mobile node wishes to proactively discover a foreign agent, it may do so by issuing a RREQ. The RREQ has the destination IP address set to 224.0.0.11, the *All Mobility Agents* multicast group address [8]. The mobile cannot put the IP address of the foreign agent into the RREQ because it does not know the foreign agent's address. The mobile node then broadcasts this RREQ to its neighbors.

When a neighboring mobile node receives this RREQ, it first checks its Mobile IP Foreign Agent List to determine whether it has received Agent Advertisements from a foreign agent. If the node does not support Mobile IP, then it does not have a Foreign Agent List, and so it simply rebroadcasts the request. If the mobile node has one or more foreign agents in its Foreign Agent List, then it checks its route table to determine whether it has a current route to one of those foreign agents. Priority is given to the foreign agent with which the node is registered. If the mobile node does not have a current route to a foreign agent, then it rebroadcasts the request. Otherwise, if it does have a current route to the foreign agent, it creates a route reply message, and it appends a Foreign Agent extension to the RREP. The Foreign Agent extension indicates the IP address of the foreign agent. The foreign agent group IP address (224.0.0.11) is placed in the *Destination IP Address* field of the RREP. The RREP is then unicast back to the source node.

When the source node receives a RREP for a foreign agent, it can then use that route to unicast an Agent Solicitation message to the foreign agent. Upon receiving the Agent Solicitation message, the foreign agent unicasts an Agent Advertisement back to the mobile node. After receiving the Agent Advertisement message, the mobile node then proceeds as described in the previous section, by selecting one of the advertised care-of addresses to be its own care-of address. The following section describes the registration procedure for mobile nodes.

5.4 Registration

A node needing Internet connectivity must register with a foreign agent. Because mobile nodes that do not need Internet connectivity do not have to register with the foreign agent, the foreign agent may not know the identity of every node within the ad hoc network.

To register with the foreign agent after receiving an Agent Advertisement, the node creates a Registration Request. The node places its home address, home agent address, and care-of address into the Registration Request, and then unicasts the message to the foreign agent. In the event that the mobile node's route to the foreign agent has become invalid, the node can initiate a route discovery procedure to find a new route to the foreign agent.

The foreign agent and home agent process the Registration Request as specified in [10] by recording the new care-of address for the mobile node. When the FA receives the Registration Reply from the HA, the FA unicasts this reply along the (possibly multi-hop) path back to the mobile node. Upon reception of the Registration Reply, if the foreign agent's route to the mobile node has timed out or been invalidated, the foreign agent can utilize the AODV route discovery procedure to rediscover a route to the mobile node.

Once the mobile node receives the Registration Reply, it marks the corresponding entry in its Foreign Agent List, thereby signifying its registration with the foreign agent. It also sets the registration lifetime associated with that entry according to the lifetime value returned in the Registration Reply.

5.5 Route Discovery

A mobile node that needs a route to a destination does not initially know whether the destination node is within the ad hoc network, or whether it is reachable through the wired interface of the foreign agent. It therefore must first search the ad hoc network for the destination. The AODV protocol is utilized for route discovery. If a route to the destination is not discovered within the ad hoc network, the mobile can conclude that the destination is not in the ad hoc network; instead it is likely to be found in the wired Internet.

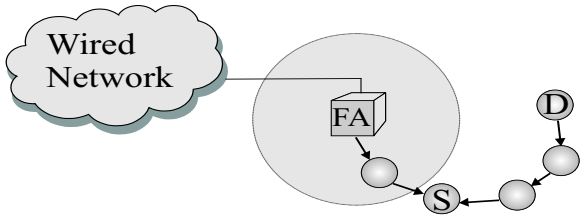


Figure 2: Path Selection with FA-RREPs.

To begin the search for the destination, the mobile node creates a RREQ packet and broadcasts this packet to its neighbors. A mobile node receiving the RREQ checks its route table for a valid route to the destination node. If such a route exists, it returns a RREP message to the source. The source node waits a discovery period to receive RREP messages. If the destination exists within the ad hoc network, a RREP is returned to the source node, and the source can begin data packet transmissions to that destination. If a RREP is not received, the source node attempts route discovery for the destination node up to some maximum number of attempts.

The foreign agent has specialized processing of route request messages. When a foreign agent receives a RREQ, it checks its route table to determine whether it has an explicit route entry for the destination node. The foreign agent may have such an entry if the destination is a registered mobile node within the ad hoc network. If a valid route table entry for the destination exists, then the foreign agent follows the standard reply procedure by creating a route reply and unicasting it back to the source node. On the other hand, if the foreign agent does not have a route table entry for the destination node, then it assumes that the destination is a node in the Internet that is reachable through its wired interface. In this case, it creates a special route reply with the Foreign Agent flag set. The destination sequence number of the RREP is set equal to that in the RREQ, and the hopcount of the RREP is set to a large value (i.e., 2^7). The foreign agent then unicasts this route reply back to the source node. This route reply is hereafter referred to as an FA-RREP.

If the source node receives an FA-RREP, it stores this route but it does not use this route immediately. This route reply indicates that the foreign agent believes the destination node is located in the wired Internet. It is possible for the mobile to receive an FA-RREP from the foreign agent before it receives a route reply from the destination node within the ad hoc network, if the mobile node is located closer to the foreign agent than it is to the destination. This scenario is illustrated in figure 2. Therefore, the mobile node should retain this route, and utilize it only after it has concluded that the destination is not located in the ad hoc network.

If the source node does not receive a RREP without the Foreign Agent flag set after a maximum number of attempts, it is concluded that the destination node is not in the ad hoc network. The mobile node then determines whether it has received an FA-RREP in response to its route request. If it has, it then enters this route into its route table and utilizes it for the transmission of data packets to the destination node. These data packets are transmitted using standard IP forwarding to the foreign agent. Once the foreign agent receives the data packets, it also uses standard IP forwarding to route the data packets to their intended destinations. Note that tunneling within the ad hoc network is not needed.

5.6 Multiple Foreign Agents

When an ad hoc network cloud is within range of multiple foreign agents, mobile nodes within that cloud can receive Agent Advertisement messages from each of the foreign agents. When nodes receive Agent Advertisements from more than one foreign agent, they need to decide when to handoff from the current foreign agent to a new one. To define when a mobile node should handoff between foreign agents, a modified version of the MIPMANET Cell Switching (MMCS) algorithm, defined in [6] is used. According to this algorithm, a node should register with a new foreign agent when it is at least two hops closer to this foreign

agent than to its current foreign agent, for two consecutive agent advertisements. For our approach, we modify the MMCS algorithm by removing the "two consecutive agent advertisements" restriction. Because a mobile node may oscillate around a position equidistant from multiple foreign agents, a mobile node should not register with a new foreign agent as soon as there is a shorter path to the new agent than to its current agent. Doing so would potentially create frequent re-registrations between pairs of foreign agents, resulting in unnecessary bandwidth overhead and congestion.

The other event that causes a mobile node to register with a new foreign agent is when it loses connectivity with its old foreign agent. Foreign agent lifetimes in the Foreign Agent List are typically set to a multiple of the foreign agent Agent Advertisement interval. This potentially results in lengthy delays between mobile node disconnections with a foreign agent, and a subsequent re-registration with a new foreign agent. Hence, a mobile node should register with a new foreign agent when it receives an Agent Advertisement from a new foreign agent, if both of the following conditions hold:

- The mobile node has not heard from its registered foreign agent for more than *one* beacon interval.
- The mobile node's route to the foreign agent has become invalid (either due to route expiration or node movement).

These specifications allow nodes that have moved from multi-hop communication with one foreign agent into multi-hop communication with another foreign agent to register with the new foreign agent in a timely manner.

In the event that a mobile node has an active route through a foreign agent and the route through the foreign agent breaks, the mobile initiates a route discovery procedure for the destination node. If the only reply for that destination is an FA-RREP received through a new foreign agent, then the mobile node registers with the new foreign agent in order to maintain Internet connectivity and continue its data session.

6 Performance Evaluation

The goal of the following simulations is to evaluate the performance of the protocol in a wide range of scenarios. The protocol was implemented in the NS-2 [4] simulator with mobility extensions. Unless otherwise noted, the parameter values for Mobile IP and AODV are the same as those suggested in [10] and [11], respectively.

The protocol is evaluated using the following performance metrics:

- **Packet delivery fraction**: The number of data packets received by the destination compared with the number of data packets generated by the source.
- **End-to-end packet delivery latency**: The average delivery delay of the data packets from the source to the destination. This includes all delays due to buffering during route discovery time, queueing at the interface queue, and retransmission latency at the MAC layer, as well as propagation and transmission time.
- **Normalized Mobile IP overhead**: The number of Mobile IP control packet transmissions per data packet delivered to the destination. Each hop-wise forwarding of a Mobile IP control packet is counted as one transmission.
- **Normalized AODV overhead**: The number of routing packets transmitted per data packet delivered to the destination. Each hop-wise transmission of a routing packet is counted as one transmission.

6.1 Experimental Setup

Networks of three different sizes are evaluated. For the scenarios described in section 1, the ad hoc component is envisioned to be relatively small, on the order of 10 or 20 nodes. However, to understand the operation of

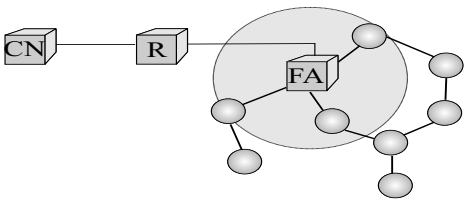


Figure 3: Simulation Scenario.

the protocol in larger networks, ad hoc networks as large as 50 nodes are simulated. As the number of nodes in the ad hoc network is increased, the size of the simulation area is increased so that a consistent node density is maintained. The network sizes utilized are as follows:

- 330m×330m simulation area with 10 mobile nodes
- 670m×670m simulation area with 20 mobile nodes
- 1000m×1000m simulation area with 50 mobile nodes

In the first two sets of simulations, there is one foreign agent node running both AODV and Mobile IP. This node acts as a gateway in providing Internet access to the mobile nodes. There is one correspondent node (CN) on the wired network connected to the foreign agent through a router. Figure 3 illustrates this network configuration. The third set of simulations has two foreign agents, which are each connected through the wired network to the CN.

There are five constant bit rate (CBR) traffic sources distributed randomly within the ad hoc network. The destination of each of the data sessions is the correspondent node in the wired network. The CBR data packets are 512 bytes and the sending rate is 10 packets per second. All mobile nodes move according to the random waypoint mobility model [3]. Node speeds are randomly distributed between zero and some maximum, where the maximum speed varies between 0 and 20 m/s. The pause time is consistently 10 seconds. All simulations are run for 900 simulated seconds. Each data point represents an average value of 10 runs with the same traffic models, but different randomly generated mobility scenarios.

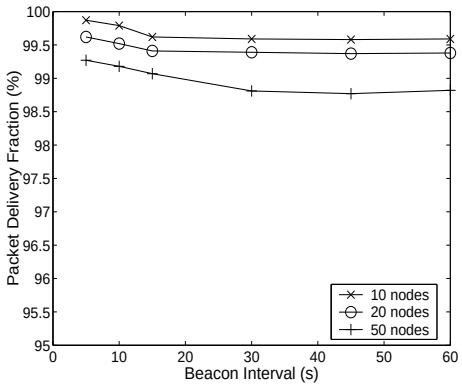
In the following simulations, the effects of different Agent Advertisement beacon intervals, node mobility, and number of foreign agents are evaluated. In the first set of simulations, the foreign agent beacon interval is varied. Next, the protocol performance with varying mobility, using a consistent beacon interval, is evaluated. In each of these scenarios, there is only one foreign agent with which the mobile nodes can communicate. Finally, the performance of the protocol with two foreign agents is evaluated.

6.2 Results

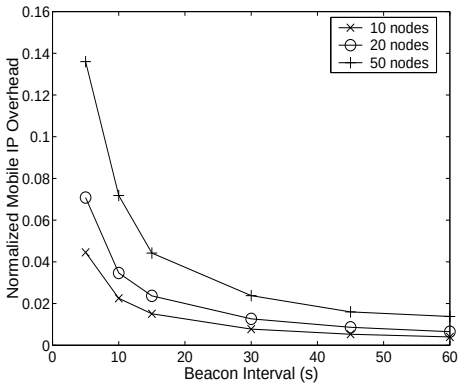
The protocol performance is first evaluated with different Agent Advertisement beacon intervals. Figure 4 shows the result with beacon intervals between 5 and 60 seconds. In these scenarios, nodes move randomly with maximum speed 20 m/s.

As the beacon interval is increased, fewer beacon messages are flooded within the network. The infrequent beacons result in less recent information, at the mobile nodes, about the route to the foreign agent. With high node mobility (20 m/s), route changes happen more frequently, and hence there are more route discoveries for the foreign agent within the ad hoc network with the larger beacon interval.

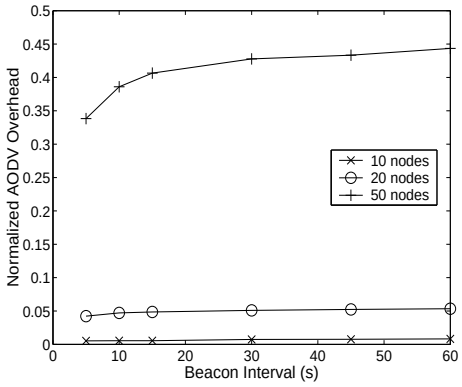
Figure 4(a) shows that the packet delivery fraction decreases slightly as the beacon interval increases. As described in sections 5.2 and 5.4, the mobile node updates its route to the foreign agent when it receives Agent Advertisements. When the interval increases, route updates for the foreign agent are performed less frequently. Source nodes are consequently more likely to initiate route discoveries for the foreign agent. After a link break in an active path, the source continues to send data packets until it is notified of the link break by



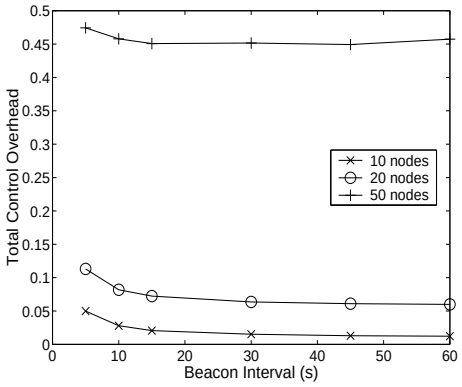
(a) Throughput.



(b) Normalized Mobile IP Overhead.



(c) Normalized AODV Overhead.



(d) Normalized Total Control Overhead.

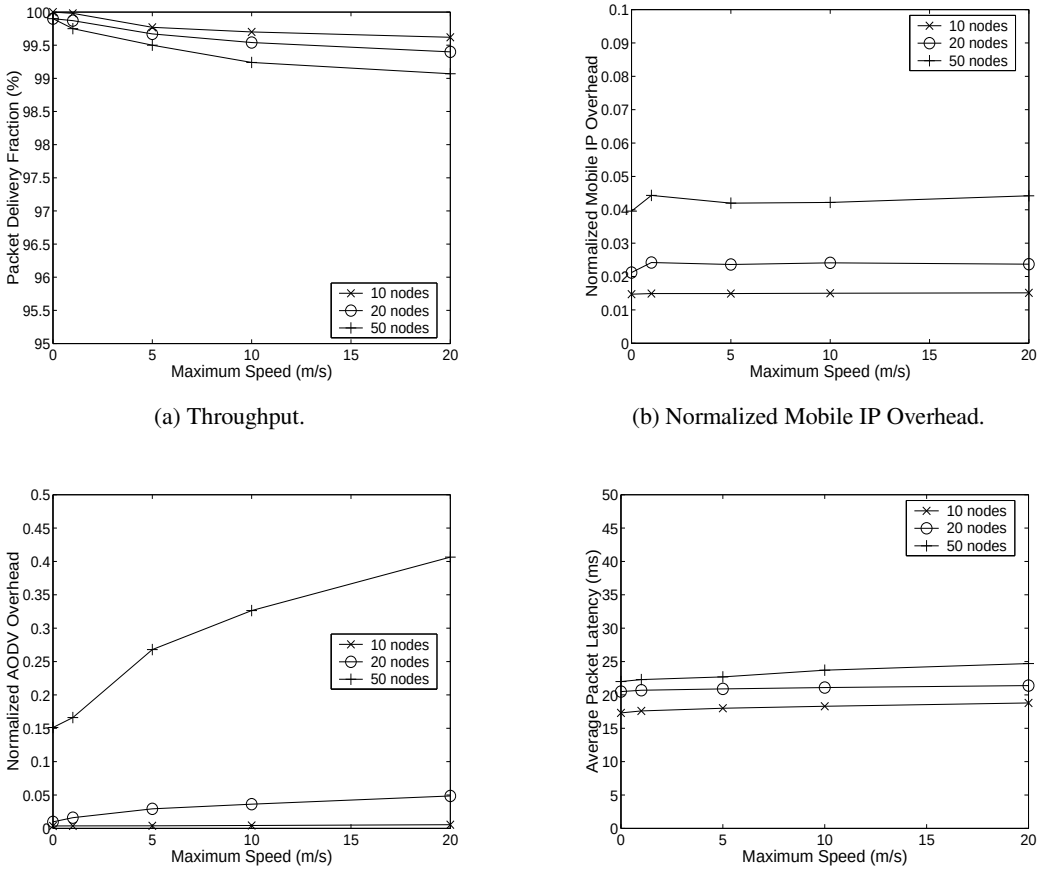
Figure 4: Effects of Varying Beacon Intervals.

a RERR. As a result, data packets can be lost before the RERR is received. When the beacon interval is short, the Agent Advertisement message plays an important role in keeping the routes between the mobile nodes and the foreign agent fresh. When the interval increases, these messages have much less effect on the route updates.

The Normalized Mobile IP overhead is shown in figure 4(b). The Mobile IP overhead is dominated by Agent Advertisements. Hence, this overhead decreases as the beacon interval increases; the values are inversely proportional to each other.

Figure 4(c) illustrates the normalized AODV overhead. AODV control overhead increases as the beacon interval increases. This is due to less frequent route updates from Agent Advertisements. For 50 nodes, the normalized AODV overhead is larger than 10 and 20 nodes, and the increase of AODV overhead for 50 nodes is also more rapid than in the other two scenarios. This is due to the fact that the average path length is greater for 50 nodes. In the 50 node network, there are more hop-wise RREQ and RREP message transmissions, as well as more frequent link breaks in active routes. Hence there are more route discoveries than in the other two scenarios. This also contributes to the throughput decrease with increasing number of nodes, as shown in figure 4(a).

The normalized total control overhead with increasing beacon intervals is shown in figure 4(d). At first, the total control overhead decreases when the interval increases, indicating that the decrease of Mobile IP over-



(a) Throughput.

(b) Normalized Mobile IP Overhead.

(c) Normalized AODV Overhead.

(d) Delay.

Figure 5: Effects of Varying Mobility.

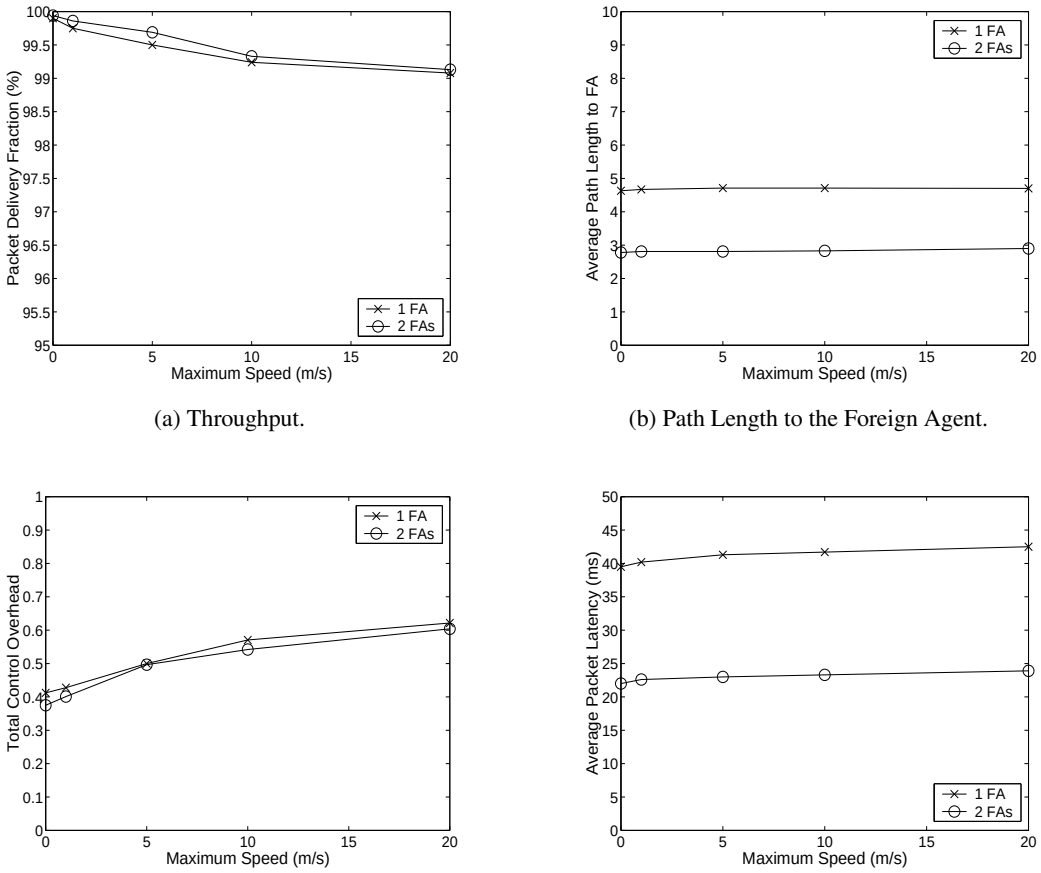
head is dominant. When the interval increases to a certain value, the increase of AODV overhead counteracts the Mobile IP overhead decrease. Hence the total overhead remains fairly constant.

To summarize the effects of varying beacon intervals, the Mobile IP overhead decreases as the beacon interval increases. Due to the route expirations and link breaks, there is more AODV control overhead in these scenarios, and thus the packet delivery fraction decreases. The total control overhead initially decreases as the beacon interval increases; once the beacon interval reaches 20 seconds, the control overhead decreases much less rapidly.

Based on these results, a beacon interval of 15 seconds is selected for the remainder of the experiments. A 15 second beacon interval offers a good balance between the control overhead and the data throughput. The effect of mobility on the protocol performance is now investigated. Figure 5 illustrates the results for different maximum movement speeds, varying between 0 and 20 m/s.

The packet delivery fraction is shown in figure 5(a). The throughput drops as the node mobility increases. High mobility results in more frequent link breaks and routing path changes. In general, however, the Mobile IP/AODV combination results in a very high packet delivery rate of more than 99%.

The normalized Mobile IP overhead is not significantly effected by mobility, as shown in figure 5(b), because it is dominated by Agent Advertisements. However, the increasing number of nodes results in an increase in Mobile IP overhead. As the number of nodes increases, more beacon messages are rebroadcast



(a) Throughput.

(b) Path Length to the Foreign Agent.

(c) Total Control Overhead.

(d) Delay.

Figure 6: Effects of Two Foreign Agents.

across the network, resulting in higher overhead.

As the mobility increases, the AODV overhead also increases. This result is shown in figure 5(c). As the mobility increases, links break more frequently and hence route discoveries occur more often. This results in an increase in RREQ, RREP and RERR traffic overhead.

Figure 5(d) shows the average packet latency for varying mobility. This is the end-to-end delay from the source node to the destination node. The delay includes the packet traversal time within the ad hoc network from the source node to the foreign agent, and the transmission time from the foreign agent to the wired destination node. As the network size increases, the average path length grows. Hence, the larger network sizes have longer delays due to the longer path lengths. Additionally, the latency increases slightly as the node mobility increases. This is primarily caused by the buffering during route discovery time.

With a fixed beacon interval, the packet delivery fraction drops slightly and the average packet latency increases as the node mobility increases. The normalized Mobile IP overhead remains fairly constant while the AODV overhead increases with higher mobility. This results in an increase in total control overhead.

The third set of experiments evaluates the protocol performance with multiple foreign agents. In these experiments, 50 nodes move around a 1000m$\times$1000m network with a maximum speed between 0 and 20 m/s. There are two simulation scenarios. In the first scenario, there are two foreign agents at opposite corners of the simulation area. Each foreign agent transmits beacons every 15 seconds. The two foreign agents are located

on the same subnet and are both connected to the correspondent node in the same number of hops. In the second scenario, one foreign agent is located at the corner of the network. This node also sends beacons every 15 seconds. In each scenario, there is one mobile node that moves between the two corners of the simulation area. This node is the CBR traffic source; the destination is the correspondent node in the wired network, as in the previous scenarios.

Figure 6(a) shows that the packet delivery fraction with two foreign agents is slightly greater than with one foreign agent. With two foreign agents, the mobile node switches to a new foreign agent if that foreign agent becomes two hops closer than its current foreign agent, as described in section 5.6. Consequently, as figure 6(b) indicates, the path length with two foreign agents is almost half of that with one foreign agent. With longer path lengths, paths break more frequently, resulting in greater packet loss.

Figure 6(c) shows the total control overhead of the two scenarios. The Mobile IP overhead with two foreign agents is slightly greater than with one foreign agent. With two foreign agents, the number of Agent Advertisements transmitted by foreign agents is doubled. However, this does not result in a doubling of Mobile IP overhead. When a mobile node receives an Agent Advertisement, it only rebroadcasts the advertisement if it is registered with the foreign agent that initiated it. This prevents Agent Advertisements sent by multiple foreign agents from being flooded across the ad hoc network, thereby reducing control overhead and saving resources. In contrast to the Mobile IP overhead, the AODV overhead is greater when there is only one foreign agent. With one foreign agent, the path lengths are longer. Link breaks, and therefore route discoveries, occur more frequently, resulting in an increase in AODV overhead. When the Mobile IP and AODV overhead is combined, the total overhead is slightly smaller when two foreign agents are used. Hence, with two foreign agents, better throughput can be achieved while control overhead is reduced.

Because the average path length is smaller when there are two foreign agents, the average packet delivery latency is also reduced in these scenarios. The average packet latency in these scenarios is shown in figure 6(d). Although there is additional delay due to the hand-off, the latency is shorter with two foreign agents because of the decrease in path length.

7 Conclusions

The Mobile IP and AODV routing protocols can work together to create a hybrid ad hoc/infrastructured network in which mobile nodes can discover multi-hop paths to foreign agents, thereby gaining Internet connectivity. AODV is utilized for the discovery and maintenance of routes within the ad hoc network, while Mobile IP is used for care-of address assignment and registration with the home agent. When a foreign agent is not available, duplicate address detection can be used for a mobile node to obtain a co-located care-of address that is unique within the ad hoc cloud.

Through simulation, we have shown that our protocol combination achieves excellent results in networks of varying sizes and configurations. In all cases, the throughput of the networks is high, while the relative control overhead is quite low. Data packet delay can be reduced through the installation of multiple foreign agents, such that the average path length is reduced. In these scenarios, the network performance can be improved while the overall control overhead does not significantly increase. In scenarios where multiple foreign agents are not possible, however, longer path lengths can be utilized to provide the ad hoc cloud with Internet connectivity.

There are many benefits for creating multi-hop paths between mobile nodes and foreign agents. Such a scheme allows nodes which are not within direct transmission range of a foreign agent to obtain Internet connectivity. By allowing multi-hop connectivity between mobile nodes and foreign agents, the installation of Mobile IP networks is made easier because fewer foreign agents are necessary. Additionally, dead zones are eliminated, and the coverage area of the foreign agent can be extended into areas in which the deployment of

such agents is not feasible. As wireless communication becomes increasingly prevalent, we envision hybrid ad hoc/infrastructured wireless networks becoming a viable networking solution.

References

[1] Internet Engineering Task Force (IETF) IP Routing for Wireless/Mobile Hosts (MobileIP) Working Group Charter. http://www.ietf.org/html.charters/mobileip-charter.html.

[2] J. Broch, D. Maltz, and D. Johnson. Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks. *Proceedings of the* 4^{th} *International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN'99)*, pages 370–375, Perth, Australia, June 1999.

[3] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva. A Performance Comparison of Multihop Wireless Ad Hoc Network Routing Protocols. *Proceedings of the* 4^{th} *ACM/IEEE International Conference on Mobile Computing and Networking (MobiCOM'98)*, pages 85–97, October 1998.

[4] K. Fall and K. Varadhan. ns Manual. The VINT Project. http://www.isi.edu/nsnam/ns/doc/.

[5] D. B. Johnson and D. A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. T. Imielinski and H. Korth, editors, *Mobile Computing*, pages 153–181. Kluwer Academic Publishers, 1996.

[6] U. Jonsson, F. Alriksson, T. Larsson, P. Johansson, and G. Q. Maguire Jr. MIPMANET - Mobile IP for Mobile Ad Hoc Networks. *Proceedings of the* 1^{st} *Workshop on Mobile Ad hoc Network and Computing (MobiHOC'00)*, pages 75–85, Boston, Massachusetts, August 2000.

[7] H. Lei and C. E. Perkins. Ad Hoc Networking with Mobile IP. *Proceedings of the* 2^{nd} *European Personal Mobile Communications Conference*, pages 197–202, Oct. 1997.

[8] C. Perkins. IP Mobility Support. Request for Comments (Proposed Standard) 2002, Internet Engineering Task Force, Oct. 1996.

[9] C. E. Perkins. Mobile IP. *IEEE Communications Magazine*, 3(5), pages 84–99, May 1997.

[10] C. E. Perkins. IP Mobility Support for IPV4, Revised. *IETF Internet Draft, draft-ietf-mobileip-rfc2002-bis-08.txt*, September 2001.

[11] C. E. Perkins, E. M. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. *IETF Internet Draft, draft-ietf-manet-aodv-09.txt*, November 2001. (Work in Progress).

[12] C. E. Perkins, J. T. Malinen, R. Wakikawa, E. M. Belding-Royer, and Y. Sun. Ad hoc Address Autoconfiguration. *IETF Internet Draft, draft-ietf-manet-autoconf-01.txt*, November 2001. (Work in Progress).

[13] C. E. Perkins and E. M. Royer. Ad-hoc On-Demand Distance Vector Routing. *Proceedings of the* 2^{nd} *IEEE Workshop on Mobile Computing Systems and Applications*, pages 90–100, New Orleans, LA, February 1999.