MICRO-MOBILITY MANAGEMENT

IN AD-HOC ACCESS NETWORKS

by

Wenping Yang

A thesis submitted to the Faculty of Graduate Studies
in partial fulfillment of the requirement for the degree of

Master of Science

in Information and Systems Science

Department of Systems and Computer Engineering

Carleton University

1125 Colonel By Drive, Ottawa

Ontario, K1S 5B6, Canada

August 2002

The undersigned recommend to the Faculty of Graduate Studies and Research

acceptance of the thesis

MICRO-MOBILITY MANAGEMENT

IN AD-HOC ACCESS NETWORKS

Submitted by

Wenping Yang

In partial fulfillment of the requirements
for the degree of
M.Sc. of Information & System Science

_____

Professor T. Kunz, Thesis Supervisor

_____

Chair, Department of Systems and Computer Engineering

Carleton University

August, 2002

Abstract

Much effort and progress has been made toward solving the problem of routing packets inside an ad hoc network, or from single hop wireless networks to the wired Internet, but there are presently few proposals for connecting ad hoc networks with the Internet and little is known about the actual performance of these proposals. This thesis is the first work to demonstrate the employment of micromobility protocols for the integration of ad hoc networks with the Internet and to provide a performance comparison of two key micromobility management protocols. The simulation results for the Hierarchical Mobile IP and HAWAII protocols are based on an ad hoc network of 50 wireless mobile nodes moving about and communicating with a corresponding wired host within the same subnet or in a different subnet, or with a wireless mobile node of another ad hoc network, using the Destination-Sequenced Distance-Vector (DSDV) ad hoc routing protocol. For simulating different speeds of a mobile user under different communication scenarios, three different node movement speeds and four different simulation scenarios have been studied. As mobile users frequently change the access point while moving within one WLAN to a different WLAN, three subnets were used for the simulation, and handoff performance as well as wandering nodes effect are investigated in this work. The performance of each micromobility protocol is analyzed and explained from its design decisions. The detailed simulation results presented in this thesis illustrate the relative performance of HAWAII and Hierarchical Mobile IP in terms of packet delivery ratio, ad hoc routing protocol overhead and control message overhead.

Acknowledgement

I would like to thank Prof. Thomas Kunz for accepting to supervise this work and for his invaluable guidance, consistent support from the start to the end of this thesis. I am grateful for his willingness to listen to my opinions and to encourage me to pursue my ideas. I will always remember this pleasant experience.

I would like to thank all the faculty and staff at the Department of Systems and Computer Engineering and the School of Computer Science for the knowledge I acquired and for the services I received in the past few years. I also thank Mr. Liang Qin for his help and suggestions for using Network Simulator in this work.

Finally, I leave my special thanks to my family for their love, support and encouragement in my life.

Table of Contents

List of Figures

List of Tables

Chapter 1. Introduction

A Mobile Ad Hoc Network (MANET) is a dynamically reconfigurable, autonomous wireless network, which is self-organizing and does not rely on existing infrastructure or central administration. Ad hoc network applications range from collaborative, distributed mobile computing to disaster recovery (fire, flood, earthquake), law enforcement (crowd control, search and rescue) and digital communications. Ad hoc networks can also play an important role in civilian forums such as electronic classrooms, convention centers and construction sites. With such a broad scope of applications, it is not difficult to envision ad hoc networks operating over a wide range of coverage areas, node densities and node velocities. However, nodes in these networks move arbitrarily, thus network topology changes frequently and unpredictably. Due to the limited radio propagation range of wireless devices, routes are often multihop. Moreover, bandwidth and battery power are limited. These constraints in combination with the dynamic network topology make the applications of ad hoc networks within themselves limited. In order to deploy the applications of ad hoc networks, MANET is required to be able to connect to different types of external networks, such as the Internet. By extending the global communication infrastructure to the ad hoc networks, nodes in the ad hoc networks will be able to link to huge numbers of computers and users connected by the Internet, sharing the large amount of useful resources on the Internet.

As computers become smaller, more affordable and global networking ubiquitous, the demand to provide network access to the mobile users will grow rapidly. One can image a scenario of using ad hoc networking in a campus environment, students and professors may use laptop computers to participate in an interactive lecture, or to access the Internet

through the access points provided in each building while walking or driving in the campus. The main function of access points is to form a bridge between the wireless and wired network. By integrating the ad hoc networks with the Internet, people would be able to download files, browse the web or talk on the Internet phone while on the move on campus. As people may move frequently between the buildings on campus, they need to frequently change the access point (handoff) within one wireless LAN or across different wireless LANs during a communication session. In order to deploy ad hoc networks in these scenarios, ad hoc network needs to be able to connect to the Internet.

Existing Internet protocols such as basic Mobile IP are designed primarily to provide transparent packet redirection to non-real time TCP applications running on conventional network hosts. This results in disruption to user traffic during handoff, and high control overhead due to frequent notifications to the home agent. With Route Optimization in Mobile IP, packets are forwarded from the old foreign agent to the new foreign agent to reduce disruption during handoff. Still, the mobile device's care-of-address changes each time the user moves between neighboring base stations, resulting in undesirable notifications to the home agent and the correspondent hosts on every handoff. In order to extend Mobile IP to overcome these limitations, IP micromobility protocols are designed for environments where mobile hosts change their point of attachment to the network so frequently that the base Mobile IP mechanism introduces significant network overhead in terms of increased delay, packet loss, and signaling. In these micromobility protocols, the Mobile IP is the basis for mobility management in wide-area inter-domain mobility, and the micromobility protocol is used to handle the local (intra-domain) mobility.

However, existing protocols such as Mobile IP, Mobile IP Route Optimization and micromobility protocols are all designed for single hop wireless networks, i.e., cellular networks and wireless LANs, and all the research efforts on performance evaluation were conducted on single hop wireless networks such as a cellular network architecture. However, these structures did not necessarily take into account the unique aspects of the ad hoc wireless environment and fundamental differences exist between the wireless networks with infrastructure support and the ad hoc network.

In wireless networks with infrastructure support, cells are well defined. In each defined cell, a base station is responsible to communicate with all mobile hosts in its cell. Mobile hosts can change cells while communicating. Hand-off occurs when a mobile host starts communicating via a new base station (Figure 1 [1]).

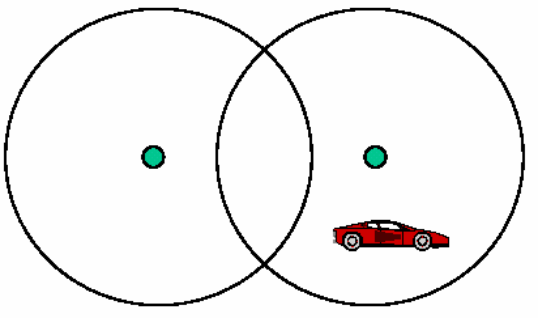

Figure 1: Example of Single Hop Cellular Network

However, this is not always the case in ad hoc network. A destination node might be out of range of a source node transmitting the packet. Thus, routing is needed to find a path between the source and destination nodes and to forward the packet appropriately. As a result, in ad hoc network, each node must be able to forward packet for other nodes, and team collaboration of large numbers of mobile nodes is very important. Some important characteristics of ad hoc networks are summarized below:

• Dynamic topology: The mobile nodes might move as shown in Figure 2 [1] (at one moment mobile node A and B can reach each other through one intermediate node; at another moment they can reach each other through two intermediate nodes), or medium characteristics might change, which leads to frequent change in the topology. Therefore, the network topology, which is typically multihop, may change randomly and rapidly at unpredictable times.

• Frequent route breakage: Mobility of nodes results in frequent route breakage

• Variable capacity wireless links: Wireless links are bandwidth-constrained. Moreover, since wireless links have lower capacity than hardwired links, traffic congestion is typical rather than atypical.

• Power constrained operation: Power conservation is crucial in mobile wireless systems since these networks typically operate with power-limited sources, which dictate whether a network is operational or not.

• Physical security: Mobile networks are more vulnerable to physical security threats such as eavesdropping and jamming attacks.

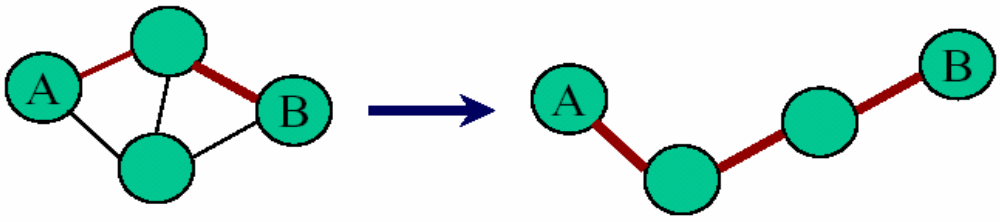

Figure 2: Example of Ad Hoc Network

Therefore, the applications of MANET are constrained by its inherent characteristics, and routing of packet/data is one of the most difficult issues in ad hoc networks. It is unlikely that a single routing protocol will be optimal for all scenarios. A given protocol will

execute efficiently in those networks whose characteristics are in accordance with the mechanisms used by the protocol.

Although a significant body of research has been done on ad hoc routing protocols, these protocols do not scale well to the Internet. Until now, there are few proposals for connecting ad hoc networks together to form larger networks, or for integrating them with the Internet. Gateway Model and Cluster Gateway Model are the only two related techniques proposed in the literature. However, little is known about the actual performance of these proposals, since no simulation results have been published to demonstrate the performance of these proposals. Herein lies the motivation for this work.

The goal of this work is to employ the micromobility management protocols for the integration of ad hoc networks with the Internet. Among all the micromobility management protocols presented in the literature, Hierarchical Mobile IP, HAWAII and Cellular IP represent the most important ones. Based on the similarity between HAWAII and Cellular IP in handling handoff, as well as the availability of the Columbia IP Micromobility Software (CIMS) NS-2 extension, which includes NS implementations for Cellular IP, HAWAII and Hierarchical Mobile IP, two different micromobility protocols, Hierarchical Mobile IP and HAWAII, are chosen for this work.

As for the ad hoc routing protocol, the Destination-Sequenced Distance-Vector (DSDV) is selected in this work. This choice is not based on its routing performance, but on its enhanced features implemented in CIMS, in which the DSDV routing protocol is provided with additional capacities such as mobile IP encapsulation/decapsulation functions, and base station nodes participating in the routing protocol. These enhanced features are necessary for connecting the ad hoc networks with the Internet.

This work is the first to sucessfully implement the integration of ad hoc networks with the Internet, and provide a quantitative analysis comparing the performance of the micromobility protocols for the integration of ad hoc networks with the Internet. The results presented in this thesis are based on the Columbia IP Micromobility Software NS-2 extension. Each simulation includes an ad hoc network of 50 wireless mobile nodes moving about and communicating with a corresponding wired host within the same subnet or in a different subnet, or with a wireless mobile node of another ad hoc network. For simulating different speeds of a mobile user under different communication scenarios, three different node movement speeds and four different simulation scenarios have been studied. As mobile users frequently change the access point while moving within one WLAN to a different WLAN, three subnets were used for the simulation, and handoff performance as well as wandering nodes effect are investigated in this work.

The performance of each micromobility protocol in terms of packet delivery rate, ad hoc routing protocol overhead and signaling overhead is analyzed and explained from its design decisions. The detailed simulation results presented in this thesis demonstrate the relative performance of HAWAII and Hierarchical Mobile IP in terms of the performance metrics.

The remainder of the thesis is structured as follows. Chapter 2 presents an overview of the Mobile IP and micromobility management protocols that are related to this work. The simulation environment and methodology are described in Chapter 3, followed by simulation experimental design decisions in Chapter 4. Simulation results and performance comparison of micromobility protocols are discussed in Chapter 5. Conclusions and future work are summarized in Chapter 6.

Chapter 2. Mobility Management Protocols Review

In this chapter, the basic concept of mobility management, as well as the basic Mobile IP protocol, and the related micromobility protocols, such as Hierarchical Mobile IP, HAWAII and Cellular IP, are reviewed in terms of their design and performance comparison. Finally, two proposals for connecting ad hoc networks with the Internet, the Gateway Model and the Cluster Gateway Model, are reviewed.

2.1. Mobility Management Overview

Wireless mobility management provides an alerting function for packet delivery in IP network to a wireless terminal, monitors wireless link performance to determine when an automatic link transfer is required, and coordinates link transfers between wireless access interfaces. Mobility management contains two components [2]: location management and handoff management.

2.1.1. Location Management

The location management is a two-stage process that enables the network to discover the current attachment point of the mobile user for packet delivery, as shown in Figure 3 [2]. The first stage is location registration, in which the mobile terminal periodically notifies the network of its new access point, allowing the network to authenticate the user and revise the user's location profiles. The second stage is call or packet delivery, in which the network is queried for the user location profiles and the current position of the mobile host is found. Current techniques for location management involve database architecture design and the transmission of signaling messages between various components of the

signaling network. As the number of mobile subscribers increases, new or improved schemes are needed to effectively support a continuously increasing subscriber population. Figure 3 associates some research issues with their respective location management operation, such as security, dynamic database updates, querying delays, terminal paging methods and paging delays.

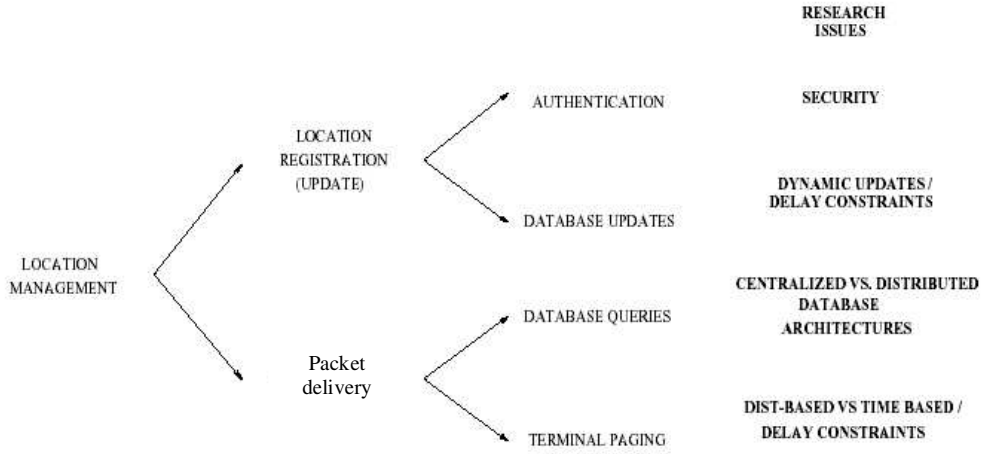

Figure 3: Location Management Operations

2.1.2. Handoff Management

The handoff management is a three-stage process that enables the network to maintain a user's connection as the mobile host continues to move and change its access point to the network. The first stage involves initiation, where the user or a network agent or changing network conditions identifies the need for handoff. The second stage is new connection generation, where the network must find new resources for the handoff connection and perform any additional routing operations. The final stage is data flow control, where the delivery of the data from the old connection path to the new connection path is maintained according to agreed-upon service guarantees.

In handoff management (Figure 4 [2]), on-going communication sessions are modified under two conditions: signal strength deterioration and user mobility. Deterioration of the radio channel results in intra-cell or inter-cell handoff. User mobility always results in inter-cell handoff. In each case, the mobile terminal's connections may be passed to the new base station without interrupting communication with the old base station, which is called a soft handoff [3]. Otherwise, if the connections are interrupted at the old base station and then established at the new base station, the process is called a hard handoff.

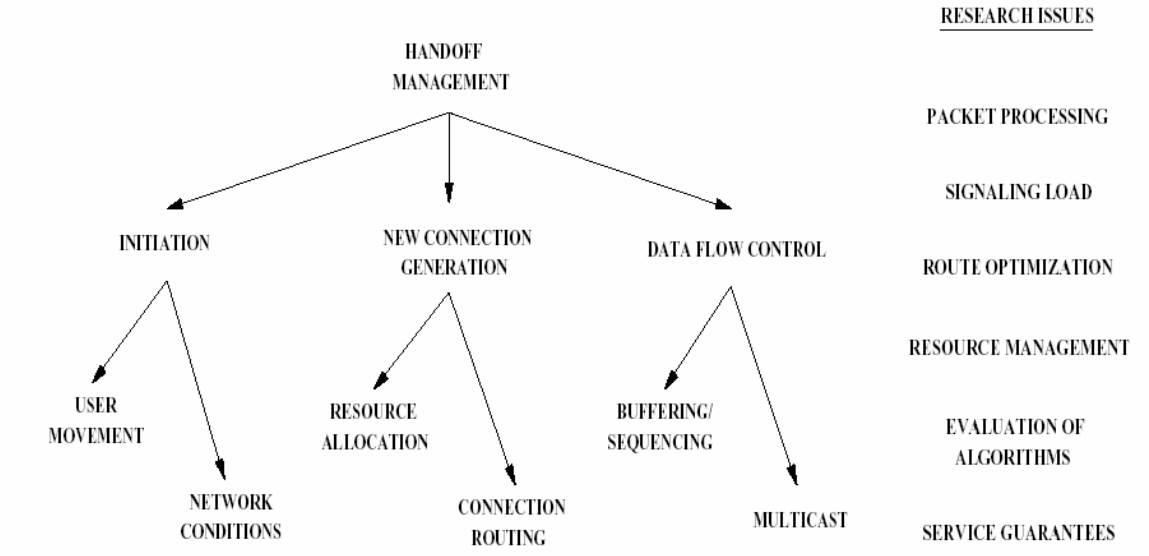

Figure 4: Handoff Management Operations

Figure 4 lists the research issues for the handoff management operations such as: efficient and expedient packet processing, minimizing the signaling load on the network, optimizing the route for each connection, efficient bandwidth re-assignment, evaluating existing methods for standardization, and refining quality of service for wireless connections.

The following section describes several mobility management protocols for location and handoff management according to the type of backbone network.

2.2. Mobility Management for Mobile IP

Mobile IP (RFC 2002) [4], a standard proposed by a working group within the Internet Engineering Task Force, provides transparent routing of packets to a mobile host and requires no modification to existing routers or correspondent hosts.

2.2.1. Basic Mobile IP Protocol Overview

Mobile IP defines protocols and procedures by which packets can be routed to a mobile node, regardless of its current point-of-attachment to the Internet, and without changing its IP address. Mobile IP was designed to allow the mobile node to use two IP addresses: a fixed home address and a care-of address (COA) that changes at each new point of attachment. Mobile IP involves two kinds of mobility agents in order to achieve the transparent mobility. These agents are the home agent (HA) and the foreign agent (FA). The home agent has the same function as the mobile home router, which is the destination where the packets go if a host's location is unknown or the rest of the system does not understand the mobile protocol. Foreign agents are not necessary but usually one or more foreign agents are present in the foreign subnets. The agents periodically advertise their presence by broadcasting agent advertisements in their local subnets.

The home address is static and identifies the connection. The home address points to the home network, where every host has a home agent. Each mobile host is assigned a unique home address in the same way as any other Internet host, within its home network. Hosts communicating with a mobile host are known as correspondent hosts and may, themselves, be either mobile or stationary.

The care-of address can be the address of a foreign agent. The foreign agent is the router, which is closest to the host. This is also referred to as the point of attachment. The care-of

address may also be a unique local address (co-located care-of address), which makes it possible to process the necessary functions inside the mobile host, without any foreign agent. This is especially useful in networks which have not deployed a foreign agent [5].

In sending an IP packet to a mobile host, a correspondent host always addresses the packet to the mobile host's home address, regardless of the mobile host's current location. At the home network, the mobile node's home agent intercepts such packets and tunnels them to the mobile node's most recently reported care-of address. At the endpoint of the tunnel, the inner packets are decapsulated and delivered to the mobile node. In the reverse direction, packets originated by mobile nodes are routed to their destination using standard IP routing mechanisms.

2.2.2. Location Management

A home agent keeps a list of registered mobile nodes. The registrations are called bindings and are defined as triplet (home address, care-of address, and lifetime). A binding holds an association between the permanent local home address and a temporary foreign address and is valid only for a given period of time. The home agent intercepts the packets destined for home addresses that it has a binding for and tunnels them to their corresponding COA. A mobile node may at any time update its associated binding and thus cause the packets to be tunneled into another foreign subnet.

Each foreign agent maintains a list known as a visitor list, which identifies those mobile hosts that are currently registered with it. An entry in this list is the mobile host's home address and the current location. The binding between a mobile host and a foreign agent is tagged by a logical timestamp, which is generated by the mobile host by incrementing its previous timestamp value each time it attempt to register with a foreign agent.

When establishing service with a new foreign agent, a mobile host must register with that foreign agent, and must also register with its home agent to inform it of its new COA. When instead establishing a new temporarily assigned local IP address as a COA, a mobile host must likewise register with its home agent to inform it of this new address. Finally, when a mobile host returns to its home network, it must register with its home agent to inform it that it is no longer using a COA.

To register with a foreign agent, a mobile host sends a registration request message to the foreign agent, which includes the address of the mobile host and the address of its home agent. The foreign agent forwards the request to the home agent, which returns a registration reply message to the foreign agent. Finally, the foreign agent forwards the registration reply message to the mobile host. When registering directly with its home agent, either when the mobile host has returned home or when using a temporarily assigned local IP address as its COA, the mobile host exchanges the registration request and reply messages directly to its home agent.

Each registration with a home agent or foreign agent has associated with it a lifetime period, negotiated during the registration. After this lifetime period expires, the mobile host's registration is deleted. In order to maintain continued service from its home agent or foreign agent, the mobile host must re-register within this period. The lifetime period may be set to infinity, in which case no re-registration is necessary. When registering with its home agent on returning to its home network, a mobile host registers with a zero lifetime and deletes its current binding, since a mobile host needs no services of its home agent while at home.

Home agents and foreign agents periodically advertise their presence by multicasting an agent advertisement message on each network to which they are connected and for which they are configured to provide service. Mobile hosts listen for agent advertisement messages to determine which home agents or foreign agents are on the network to which they are currently connected. If a mobile host receives an advertisement from its own home agent, it deduces that it has returned home and registers directly with its home agent. Otherwise, it chooses whether to retain its current registration or to register with a new foreign agent from among those it knows of.

While at home or registered with a foreign agent, a mobile host expects to continue to receive periodic advertisements from its home agent or from its current foreign agent, respectively. If it fails to receive a number of consecutive expected advertisements, the mobile host may deduce either that it has moved or that its home agent or current foreign agent has failed. If the mobile host has recently received other advertisements, it may attempt registration with one of those foreign agents. Otherwise, it may multicast an agent solicitation message onto its current network, which should be answered by an agent advertisement message from each home agent or foreign agent on this network that receives the solicitation message.

2.2.3. Handoff Management

When a mobile host migrates, the COA changes while the home address remains static. All the traffic to the roaming mobile host comes to the COA as encapsulated IP packets. In Figure 5 the correspondent host is any host in the Internet, with which the mobile host exchanges information. In this case the correspondent host is not aware of the exact location of the mobile host and the packets are sent via the home agent.

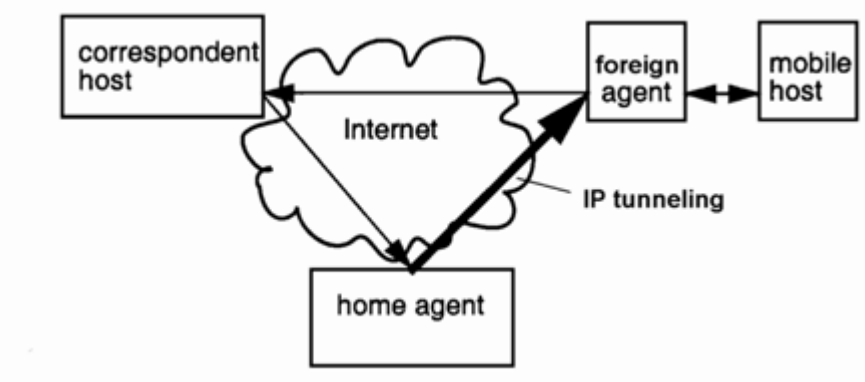

Figure 5: Mobile IP Routing

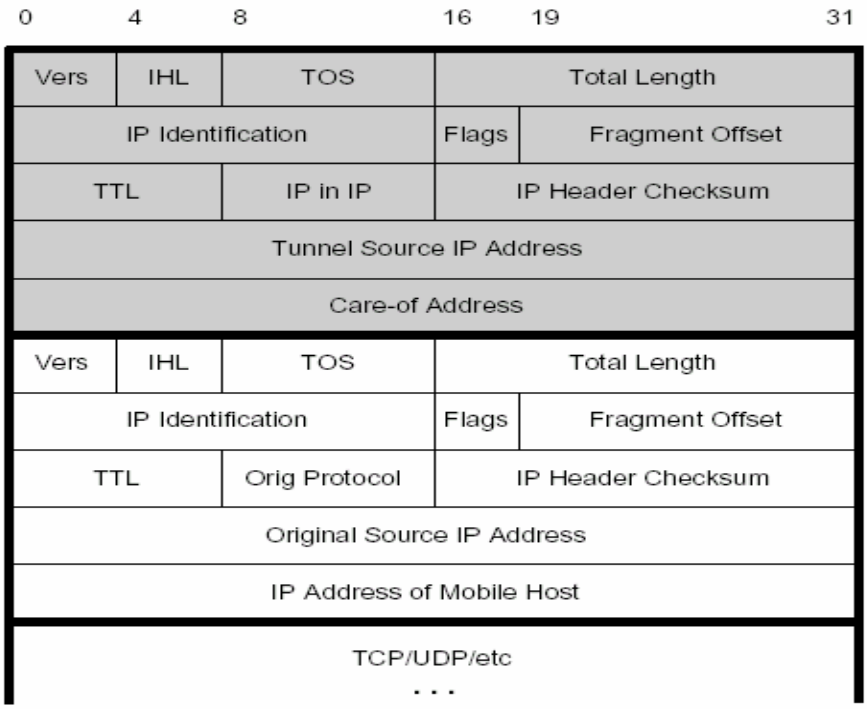

Figure 6: Mobile IP tunneling using "IP in IP" encapsulation

In a basic mobile IP operation, packets sent by the correspondent host to the mobile host are always sent to the mobile host's home network first, and then forwarded by the home agent to the mobile host's current COA. Packets originating from the mobile host are sent

directly to the correspondent host, thus forming a triangular route. These packets use the mobile host's home address as their source address to preserve their home identity. The packets forwarded by the home agent to the COA are encapsulated in another IP packet.

The protocol requires support for "IP in IP" encapsulation (Figure 6 [6]) for tunneling. In this method, to tunnel an IP packet, a new IP header is wrapped around the existing packet. The source address in the new IP header is set to the address of the node tunneling the packet (the home agent), and the destination address is set to the mobile host's COA. The new header added to the packet is shaded in gray in Figure 6. This type of encapsulation may be used for tunneling any packet, but the overhead for this method is the addition of an entire new IP header (20 bytes) to the packet.

The advantages of Mobile IP are its simplicity and its compatibility with wired networks since only mobile agents and mobile nodes have to be modified. However, it has several limitations. First, the triangle routing of IP packets to mobile nodes through a home agent is not optimal. For example, while a mobile host is away from its home network, all packets for the mobile host must follow the path shown in Figure 5. Each packet is routed through the Internet to the mobile host's home network and must then be tunneled by the mobile host's home agent to the mobile host's current location. This indirect routing through the home agent in general causes unnecessary overhead on the home network and on the portion of the Internet leading to and from the home network, and causes unnecessary latency in the delivery of each packet to the mobile host. Second, the COA of a mobile node at the home agent changes whenever it moves from one IP subnet to another. This could lead to frequent registrations with the home agent, which cause significant packet drop and throughput reduction.

2.3. Micromobility Management Protocols

In the basic Mobile IP, mobile nodes have to report their every movement in the foreign network to their home networks. This causes a huge amount of signaling traffic and latency during handoffs. Because of these problems, several micromobility proposals have been defined to solve this so-called micromobility problem. Micromobility protocols [7] are designed for environments where mobile hosts change their point of attachment to the network so frequently that the basic Mobile IP protocol tunneling-mechanism introduces network overhead in terms of increased delay, packet loss and signaling. In all of these micromobility solutions the home network does not have to know the exact location of the mobile node. Instead the home network only has to know in which visited network the mobile node is located and the local micro mobility is managed inside the visited network. This has the benefit of reducing delay and packet loss during handoff and eliminating registration between mobile hosts and possibly distant home agents when mobile hosts remain inside their local coverage areas. Eliminating registration in this manner reduces the signaling load experienced by the network in support of mobility. Another important characteristic of micromobility protocols is their ability to reduce the signaling overhead related to frequent mobile migrations taking into account a mobile host's operational mode (i.e., active or idle). Support for "passive connectivity" to the wireless Internet balances a number of important design considerations. For example, only keeping the approximate location information of idle users requires significantly less signaling and thus reduces the load over the air interface and in the network. Reducing signaling over the air interfaces in this manner also has the benefit of preserving the power reserves of mobile hosts. To

minimize signaling overhead and optimize mobility management performance, micromobility protocols support IP paging.

The following section reviews and compares some important micromobility proposals found in the literature.

2.3.1. Hierarchical Mobile IP

Hierarchical approaches have been studied in order to reduce registrations with the home agent while roaming. There are several protocol suggestions that have the same basic idea of a hierarchical structure of the visited networks. In all these proposals, Mobile IP is extended by arranging foreign agents in a hierarchy. The top of the hierarchy is rooted at the edge of the access network and is defined by the care-of address registered with HAs. Upon reception of a packet, the foreign agent at the top of the hierarchy interacts with a local database to determine to which lower-level foreign agent located in the access network to forward the packet to. This procedure may be repeated, depending on the depth of the routing hierarchy. The basic idea for all these proposals is that the mobile node does not have to inform its home agent of every movement it performs inside the visited network. Instead there is a network element that takes care of the mobile node's registrations.

(a) Regional Tunnel Management

In regional tunnel management [8], the mobile node can move inside a visited domain without informing its home agent about every movement. When a mobile node first arrives at the visited network, it performs normal registration with its home agent. After that the mobile node is doing regional registrations inside the visited network. Figure 7 [8] illustrates the basic idea of hierarchical Mobile IP.

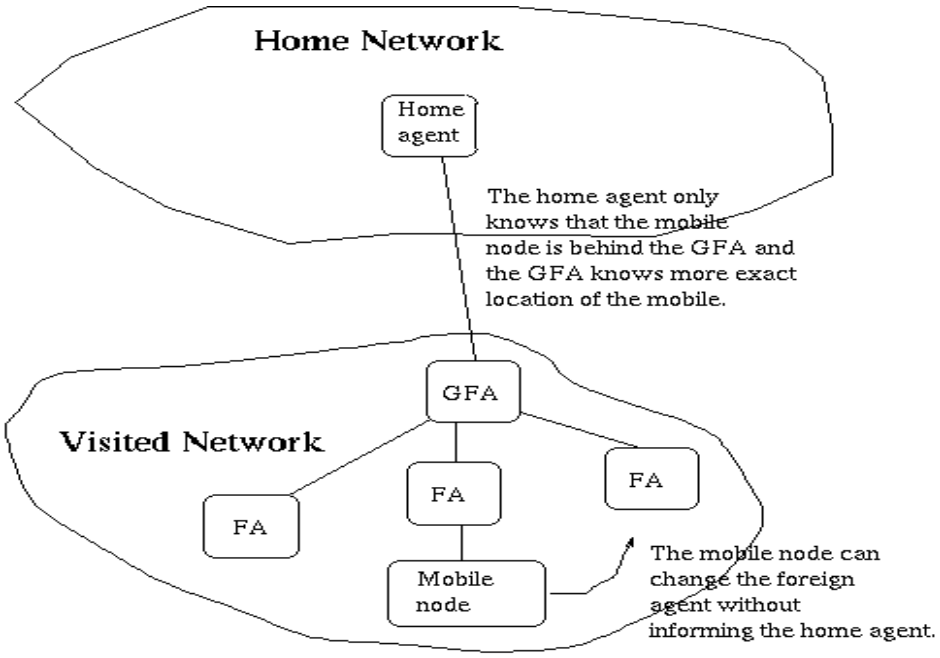

Figure 7: Regional Tunnel Management

If the foreign network supports regional tunnel management, there is a special kind of foreign agent called a gateway foreign agent (GFA). The mobile node uses the GFA's IP address as its COA when it registers with the home agent. This COA does not change when the mobile node moves between the foreign agents that are located under the same GFA. After first registration, the mobile node makes its registrations with the GFA. Registrations are not done with the home agent as long as it is moving under the same GFA. If the mobile node changes GFA, within or between visited domains, it must again register with the home agent. Because the binding of the mobile node must not expire at the home agent, there also has to be regular registrations with the home agent.

(b) Hierarchical Foreign Agent

Foreign agents are organized into a hierarchy according to the region topology [9]. The home agent serves as the “universal root” and the current foreign agent is a leaf node in

the hierarchy. Registration requests are sent to the foreign agent at the lowest level in the hierarchy that remains the same across a handoff. IP packets for a mobile node are sent to the home agent and then tunneled down through the hierarchy of foreign agents to the mobile node.

(c) Redirection Agent

Cho and Marshall [10] present a method that exploits the locality properties of a host's pattern of movement and access history. Two concepts, "local region" and "patron service" are introduced based on the locality features. A local region is defined for each mobile node by including those subnetworks among which the mobile node often moves. Patrons are the hosts from which the majority of traffic for the mobile host originated. These are used to confine the effects of a host moving, so location updates are sent only to its local area, and to those source hosts which are most likely to call again.

A hierarchy of redirection agents is used to intercept IP datagrams for mobile nodes within a region and send them directly to current locations of mobile nodes. Movements within a region do not have to be announced to nodes outside of a region. Correspondent nodes outside the local region of a mobile node can use inaccurate location information because redirection agents can intercept IP datagrams and tunnel them to the current location of the mobile node. This scheme has the advantages of limiting location updates, and providing optimal routing, whilst increasing network and host scalability.

(d) Regional Aware Foreign Agent

The Regional Aware Foreign Agent model [11] introduces the following new architectural entities:

- Regional Aware Foreign Agent (RAFA)

A host or router on a mobile node's visited routing domain that provides local registration service for a mobile node during handoff. It cooperates with the local foreign agents to allow the home agent to have incomplete knowledge of the mobile node 's true point of attachment. It may be the tunnel endpoint of datagrams from the home agent. It either extracts the datagrams and then tunnels datagrams to the local foreign agent for delivery to the mobile node, or just acts as a simple router within a large routing domain. It therefore provides tunneling, registration and routing services to the mobile node while registered.

- Local Foreign Agent (LFA)

The LFA has the same functionality as the foreign agent in the base protocol. It is a router on a mobile node's visited network, which provides routing service to the mobile node while registered. It extracts and forwards datagrams to the mobile node. It has a security association with the regional aware foreign agent, and there is a slight modification in the way it relays registration packets from the base protocol.

In this model, the RAFA is the proxy LFA, known by the home agent, while the LFA provides the point of access. The mobile node can register with the RAFA through the LFA instead of always registering with the home agent. Compared to base Mobile IP, this proposed extension can reduce frequent distant registrations during handoffs, also reduce the number of trusted entities in the network and hence enable us to minimize the key management problem. Importantly, the above advantage can be obtained without requiring any changes in the base protocol implemented at the mobile node.

(e) Surrogate Agent

McCann et al. [12] suggested a distribution of the foreign agent functionality with a new type of specialized mobility agents called surrogate agent. These agents create link layer tunnels to foreign agents before any Mobile IP signaling, thus making the distributed functionality and the hierarchy invisible to the mobile node. Additionally, the Transparent Hierarchical Mobility Agents (THEMA) draft discusses distributing the home agent functionality. This works both in the foreign network where the surrogate agents reply to the registration requests and in the home network where the home agent may connect to a home link via surrogate agents. The home link then provides an access point for the mobile node and keeps the mobile node and the home agent connected.

(f) Distributing Mobility Agent

In the Dynamic – HUT Mobile IP [13], the functionality of the home agent is distributed into the foreign network. This is a hierarchical version of Mobile IP that distributes the role of the mobile agent. The mobility bindings are cached in the access network and the system protects their use with a session key protocol. This enables secure localized location updates with efficient signaling. The agent advertisement and the registration request contain only the address of the hierarchical foreign agent (HFA), and the registration request travels only to the closest foreign agent that can candle the routing change. This results in a scalable system and enables the use of private addresses between intermediate and lowest foreign agents.

2.3.2. Intra-Domain Mobility Management Protocol (IDMP)

The Intra-Domain Mobility Management Protocol [14] developed by Telcordia and University of Texas aims to reduce handoff latency and signaling overhead of frequently roaming hosts by localizing mobility-related management within a wireless access domain. IDMP supports fast handoff with minimal packet losses and paging for reduced signaling, which uses a hierarchical structure with a mobility agent at the top of the hierarchy with several child sub-network foreign agents interconnected to it. The top-level mobility agent functions as a gateway to the Internet. No global registration is necessary as long as hosts move within the agent's administrative domain. The home agent only needs to be updated when the mobile host changes administrative domains. Figure 8 [14] depicts the functional layout of IDMP. The Mobility Agent (MA) acts as a domain-wide point for packet redirection. A Subnet Agent (SA) is similar to a Mobile IP FA and provides subnet-specific mobility services.

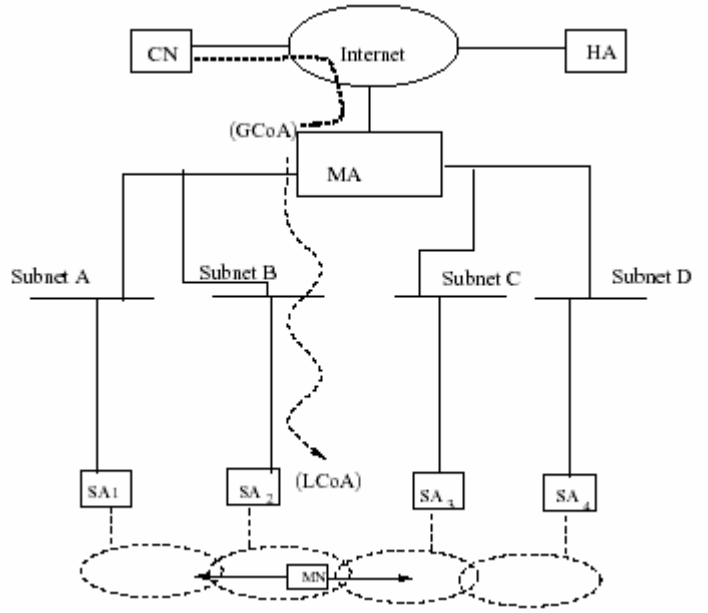

Figure 8: IDMP Logical Elements & Architecture

Under IDMP, a mobile node obtains two concurrent COAs. The local Care-of Address (LCOA) is similar to the Mobile IP's COA in that it identifies the MN's present subnet of attachment, but the LCOA in IDMP only has domain-wide local scope. By updating its MA of any changes in the LCOA, the mobile node ensures that packets are correctly forwarded within the domain. The global care-of address (GCOA) resolves the mobile node's current location only up to a domain-level granularity and hence remains unchanged as long as the mobile node stays within a single domain. By issuing global binding updates that contain this GCOA, the mobile node ensures that packets are routed correctly to its present domain.

Two enhancements to the base IDMP solution have been presented in [15]. To minimize packet loss during intra-domain handoffs, a time-bound localized 'multicasting' approach is proposed. By proactively informing its associated MA of an impending change, a mobile node enables the MA to multicast packets for a limited duration to a set of neighboring subnets. Specific nodes on those subnets (SAs/designated routers) buffer such multicast packets for a short while. If the mobile node enters its subnet, such a node is able to immediately forward these packets to the mobile, significantly eliminating packet loss and delays. This localized 'multicasting' idea is also extended to provide paging support under IDMP. In this approach, each subnet would be associated with one or more Paging Areas (PA). A non-active mobile node would perform intra-domain location updates only when it changes its PA. To determine the exact location of a mobile node within its current PA, the MA would 'multicast' a paging packet to all subnets to this PA. Unlike other suggested IP-based paging schemes, this mechanism does not assume a tree-like topology and allows easy configuration of variable-size PAs.

2.3.3. Handoff-Aware Wireless Access Internet Infrastructure (HAWAII)

HAWAII [16] is proposed by Lucent Technologies to handle intra-domain mobility. It is a domain-based approach for supporting mobility in wide-area wireless networks. The design goals of HAWAII were scalability, efficient routing, limited disruption, QoS support, and reliability. Essentially, HAWAII attempts to do this by making the assumption that most of the mobility is within a single logical administrative domain, and then taking steps to optimize the system for that type of environment.

HAWAII uses a hierarchical strategy, segregating the network into a hierarchy of domains, loosely modeled on the autonomous system hierarchy used in the Internet. The network architecture is illustrated in Figure 9 [16].

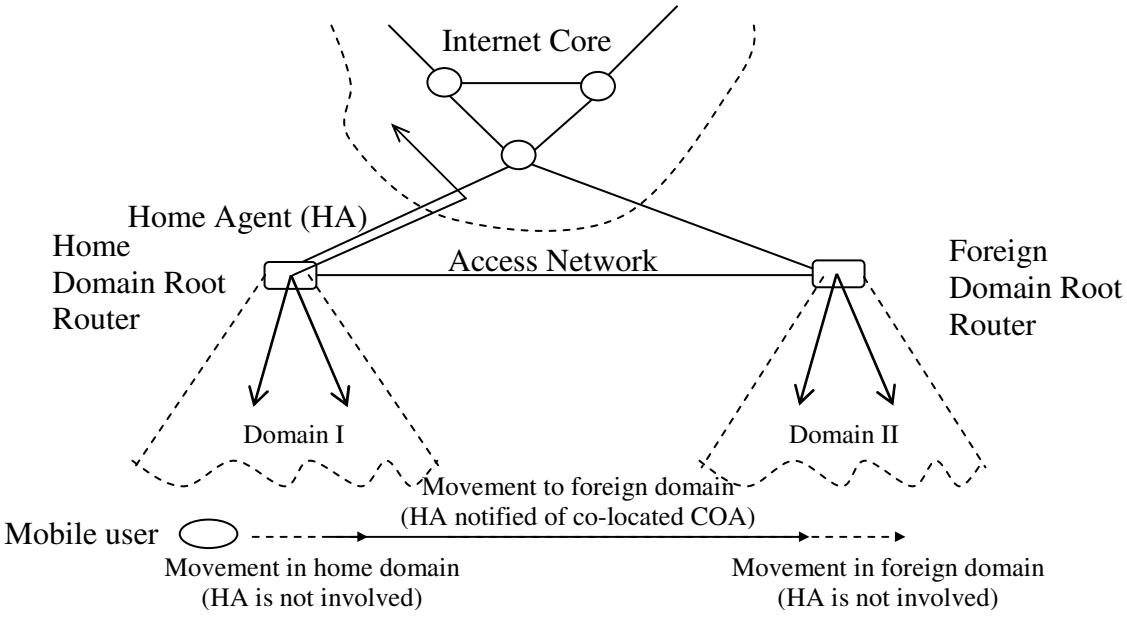

Figure 9: Hierarchy using Domains in HAWAII

In HAWAII, a domain is a logical aggregation of networks, which sit behind a common router called domain root router. When a mobile host is no longer in its home domain,

then standard Mobile-IP routing occurs from the home agent to the domain root router. The HAWAII protocol operates inside the domain, between the domain root router and the mobile host. Each host is assumed to have an IP address and a home domain. While moving in its home domain, the mobile host retains its IP address. Packets destined to the mobile host reach the domain root router based on the subnet address of the domain and are then forwarded over special dynamically established paths to the mobile host.

When the mobile host moves into a foreign domain, it is reverted to traditional Mobile IP mechanisms. If the foreign domain is also based on HAWAII, then the mobile host is assigned a co-located care-of address (CCOA) from its foreign domain. Packets are tunneled to the COA by a home agent in its home domain. When moving within the foreign domain, the mobile host retains its COA, and connectivity is maintained using dynamically established paths.

HAWAII uses path setup messages to establish and update host-based routing entries for the mobile hosts in the selective routers in the domain, so packets arriving at the domain root router can reach the mobile host. It operates over the following types of messages:

- Path setup power-up message: for constructing a route between the mobile host and the domain router. This state information is only known to the domain router, and all routers on the path.
- Path setup update message: for updating the necessary routers when a mobile host has moved within the domain. The routers that receive this message are determined by the path setup scheme.

- Path refresh message: The routing state in HAWAII is soft, so the mobile host must periodically send these messages so that the routers know that it is still alive, and that its state should be kept.

When the mobile host powers up, it sends a Mobile-IP registration message to its nearest base station, which then propagates a HAWAII path setup update message to the domain root router using a configured default route. Each router in the path between the mobile host and the domain root router adds a forwarding entry for the mobile host. Finally, the domain root router sends back an acknowledgement to the base station, which then sends a Mobile-IP registration reply to the mobile host. At this time, when packets destined for the mobile host arrive at the domain root router based on the subnet portion of the mobile host's IP address, the packets are routed within the domain to the mobile host using the host-based forwarding entries just established. These host-based forwarding entries are soft-state entries that are kept alive by periodic hop-by-hop refresh messages. Note that other routers in the domain have no specific knowledge of this mobile host's IP address. In the case of mobile to mobile communication, packets arriving at a router that has no specific host-based entry are routed using a default route. The packets eventually reach an upstream router (in the worst case, the domain root router) which has a forwarding entry for the mobile host.

When the topology has multiple paths between the base station and the domain root router, the base station and routers will have multiple routes for the domain root router (or multiple default routes). Each base station and router can choose any of these routes to forward the path setup message for a particular mobile host that has powered up. In this case, the base station or router must ensure that subsequent refreshes for a given

mobile host always go through the same route. Thus, all the packets for a particular mobile host will arrive on the same path from the domain root router resulting in no re-ordering. At the same time, multiple paths between the domain root router and the base station are utilized for different users attached to a base station.

The HAWAII handoff procedures are only activated when the mobile host's next hop IP node is changed during the handoff. A tree-based topology is assumed for the discussion, although the path setup schemes work with any arbitrary topology. Here, crossover router is defined as the router closest to the mobile host that is at the intersection of two paths, one between the domain root router and the old base station, and the second between the old base station and the new base station.

In HAWAII, there are two path setup schemes used to re-establish path state when the mobile host moves from one base station to another within the same domain. The path setup schemes are classified based on the way packets are delivered to the mobile host during a handoff. In both path setup schemes, forwarding entries during handoff are added so that packets are either forwarded from the old base station or diverted from the crossover router to the new base station. This property ensures us against the possibility of persistent loops after the handoff update.

(a) Forwarding Schemes

In the forwarding schemes, packets are first forwarded from the old base station to the new base station before they are diverted at the crossover router. There are two variants of the Forwarding scheme:

- Multiple Stream Forwarding (MSF): This scheme uses the standard IP routing infrastructure in order to divert packets from the old base station to the new base

station. This method can transmit multiple out-of-order streams to the mobile host, and can be subject to transient routing loops.

- Single Stream Forwarding (SSF): This scheme uses interface-based forwarding, a modification to the IP routers that allows packets sent to the old base station to be diverted to the new base station in a single stream. While SSF performs slightly better than MSF, this slight gain comes at the expense of a more complex implementation.

(b) Non-Forwarding Schemes

In the non-forwarding schemes, as the path setup message travels from the new base station to the old base station, data packets are diverted at the cross-over router to the new base station, resulting in no forwarding of packets from the old base station. There are two variants of the Non-Forwarding scheme, motivated by two types of wireless networks:

- Unicast Non-Forwarding (UNF): Optimized for networks in which the mobile host can listen to multiple base stations simultaneously. When the crossover router detects that the mobile host has moved, it automatically routes packets destined for the old base station to the new one.
- Multicast Non-Forwarding (MNF): Optimized for networks where the mobile host is able to listen/transmit to only one base station. It uses a custom designed "dual-casting" scheme, which is suited for networks that force the mobile host to communicate with one base station only. This scheme is similar to UNF, except that the crossover router will multicast packets to both base stations for a short time.

2.3.4. Cellular IP

The Cellular IP [17]-[18] proposal from Columbia University and Ericsson is optimized to support local mobility but efficiently interworks with Mobile IP to provide wide area mobility support. It combines the capability of cellular networks to provide smooth fast handoff and efficient location management of active and idle mobile users with inherent flexibility, robustness and scalability found in IP networks. Figure 10 illustrates the basic structure of the Internet containing networks implementing the cellular IP protocol. In Cellular IP, a mobile host's home agent is only informed when the host moves into a new access network and is unaware of the hosts' mobility within an access network.

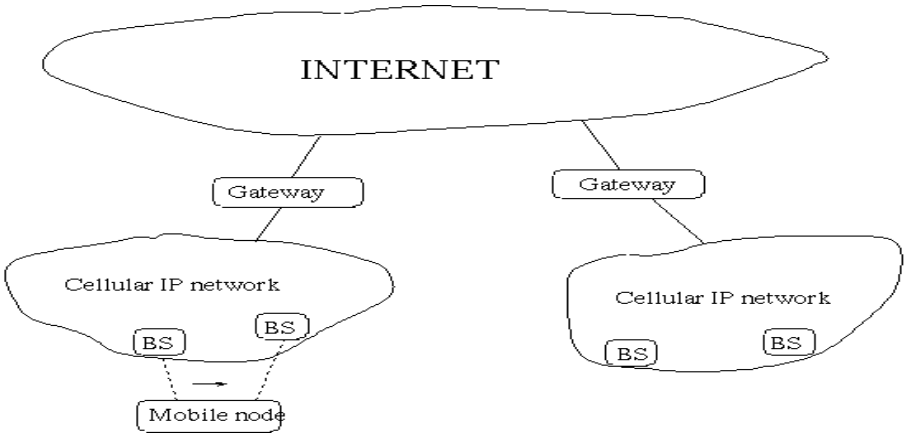

Figure 10: Micro Mobility with Cellular IP

The universal component of a Cellular IP network is the base station which serves as a wireless access point but at the same time routes IP packets and integrates cellular control functionality traditionally found in Mobile Switch Centers and Base Station Controllers. The base stations are built on regular IP forwarding engines, but IP routing is replaced by Cellular IP routing and location management. The cellular IP network is connected to the Internet via a gateway router. Mobility between gateways is managed by Mobile IP while

mobility within access networks is handled by Cellular IP. Mobile hosts attached to the network use the IP address of the gateway as their Mobile care-of address. Assuming the basic Mobile IP, packets will be first routed to the host's home agent and then tunneled to the gateway. The gateway "detunnels" packets and forwards them towards base stations. Inside the Cellular IP network, mobile hosts are identified by their home address and data packets are routed without tunneling or address conversion. Actually, Cellular IP routing protocol ensures that packets are delivered to the host's actual location. Packets transmitted by mobile hosts are first routed to the gateway, then on to the Internet.

The Cellular IP gateway periodically broadcasts a beacon packet that is flooded in the access network. Base Stations use this beacon to record the interface, which will be used to route packets toward the gateway. All packets transmitted by mobile hosts regardless of their destination address are routed to the gateway using these routes. Each base station maintains a routing cache (RC). When a data packet originated by a mobile host enters a base station, the local RC stores the IP address of the source mobile host and the interface over which the packet enters the node. This mapping remains valid for a system specific time, which is renewed by each data packet that traverses the same interface from the same mobile host. As long as the mobile host is regularly sending data packets, base stations along the path validate the entries in their RC. Packets addressed to the same mobile host are routed on a hop-by-hop basis using the established RC. In order to maintain its RC mappings even though there are no data packets to transmit, the mobile host sends route-update packets at regular route-update intervals. Route-update packets are empty data packets addressed to the gateway, and have the same effect on RC as normal data packets, but do not leave the Cellular IP access networks.

Cellular IP supports two types of handoff schemes: hard handoff and semisoft handoff. Cellular IP hard handoff is based on a simple approach that trades off some packet loss for minimizing handoff signaling rather than trying to guarantee zero packet loss. Cellular IP semisoft handoff exploits the notion that some mobile hosts can simultaneously receive packets from the new and old base stations during handoff, which improves handoff performance by minimizing packet loss.

Handoff in Cellular IP is always initiated by mobile hosts. As the host approaches a new base station, it redirects its data packets from the old to the new base station. The first of these redirected packets will automatically configure a new path of RC mappings for the host to the new base station. For a time equal to the timeout of RC mappings, packets addressed to the mobile host will be delivered at both the old and new base stations. If the host's radio device is capable of listening to two logical channels, the handoff will be soft; otherwise, the performance of hard handoff will depend on the radio device. After a while, the path to the old base station will time out and clear, while packets will continue to be delivered to the host at its current location via the new base station.

This handoff process is simple, transparent and automatic. If the old and new paths take the same route, the old mappings are automatically reused, rendering the search for an optimal crossover point unnecessary. In addition, if the old and new cells overlap, there is little interruption or disturbance in communications. If at handoff the mobile host is temporarily out of radio contact while moving between two cells, the upper layers may notice a delay and some packets may be lost, but communication is resumed as soon as the host appears in the new cell. This also applies to hosts becoming temporarily unreachable due to reasons other than handoff. If a host reappears before the RC timeout,

service continues without any further delay. If RCs have timed out, they are reconfigured by the first packets transmitted by the host which does not even have to know about the disruption or notice whether it reappeared in the same or in another cell. Note that the handoff process is valid for data packets as well as for route-update packets, since route-update packets have the same effect as data packets.

While this process would normally result in smooth handoff, in some cases handoffs can occur quickly or the mobile host can flip-flop between two base stations when it is on the border of two cells. To ensure continuous communication in these situations, the mobile host maintains a RC route to both base stations by sending its data packets to one and sending, in parallel, route-update packets to the other base station. In this case, the network is prepared for the handoff, and data transmission will be continuous if the host suddenly becomes unreachable by one of the base stations. The same method can be used for idle mobile hosts, which can send paging-update packets to two or more base stations in parallel, instead of just one base station. Cellular IP can use these strategies to enhance reachability and handoff quality in exchange for network efficiency.

Cellular IP defines an idle mobile host as one that has not received data packets for a system specific time (active-state-timeout). In this respect, idle mobile hosts allow their respective soft-state routing cache mappings to time out. These hosts transmit paging-update packets at regular paging-update-time intervals. The paging-update packet is an empty IP packet addressed to the gateway on a hop-by-hop basis, which is distinguished by its IP type. Base stations may optionally maintain a paging cache (PC), which has the same format and operation as a RC except for two differences: PC mappings have a longer timeout period and can be updated by any packet sent by mobile hosts including

paging-update packets. In contrast, RC mappings are updated by data and route-update packets sent by mobile hosts. This results in idle mobile hosts having mappings only in paging caches, and active mobile hosts have mappings both in paging caches and routing caches. Packets addressed to a mobile host are normally routed by routing cache mappings. Paging occurs when a packet is addressed to an idle mobile host and the gateway or base stations find no valid routing cache mapping for the destination. Idle mobile hosts that receive a packet move from idle to active state, start their active-state-timer and immediately transmit a route-update packet. This ensures that routing cache mappings are established quickly, potentially limiting any further flooding of messages to the mobile host. The paging cache is used to avoid broadcast search procedures found in cellular systems. If the base station has no paging cache, it will forward the packet to all its interfaces except for the one the packet came through. Using paging caches, the network operator can restrict the paging load in exchange for memory and processing cost.

2.3.5. Performance Comparison of Micromobility Protocols

A comparison of a number of key micromobility protocols that have been designed and implemented over the past several years has been presented by Campbell et al. [19] Micromobility protocols complement Mobile IP with fast, seamless, local handoff control. Despite the different design approaches, the operational principles that govern them are largely similar. Separate programming models for Cellular IP, HAWAII, and Hierarchical Mobile IP have been developed in CIMS [20] NS-2 extension.

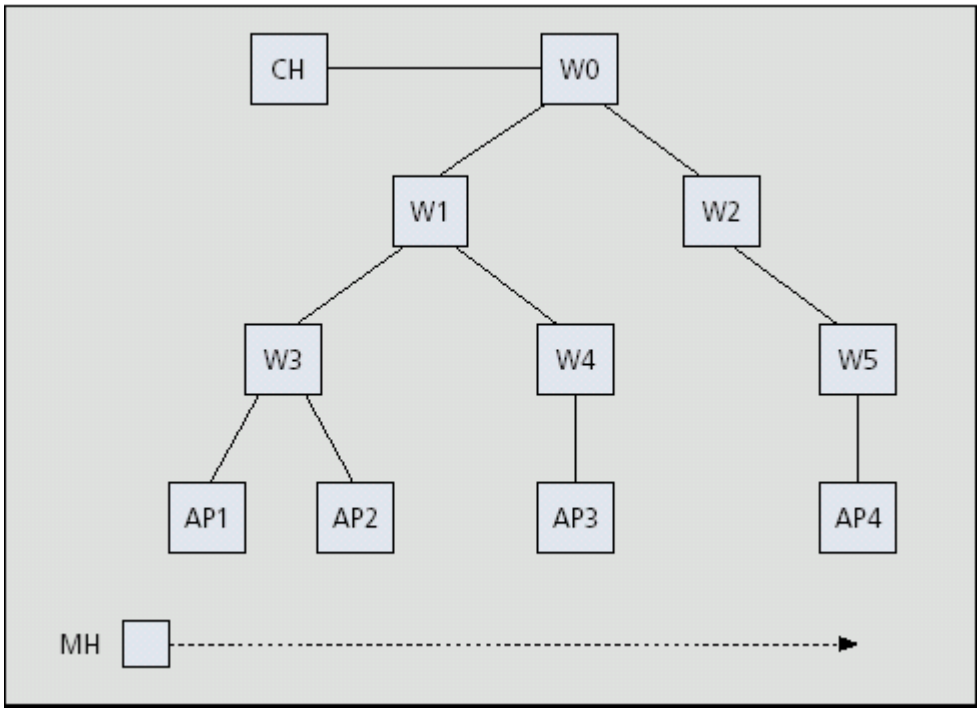

Figure 11: The Simulated Network Topology

All simulations are performed using the network topology shown in Figure 11 [19]. In Cellular IP simulations each Wi and APi corresponds to Cellular IP nodes where W0 acts as a gateway to the Internet. In HAWAII simulations all Wis and APis are HAWAII-enabled routers, and W0 is the domain root router. When simulating Hierarchical Mobile IP, the GFA function is implemented by W0, while W1–W5 represent mobility-unaware routers, the FAs are collocated with the APis. During simulation, a mobile host moves periodically between neighboring access points (APs) at a speed of 20 m/s. The circular areas covered by neighboring access points have an overlap region of 30 meter. The simulation network accommodates using both UDP and TCP traffic. The average number of packets lost during handoff for each protocol is counted for measuring handoff delay. Simulations were performed for three different scenarios with various crossover distances

(i.e., the number of hops between the crossover node and new AP). The crossover distance is 1, 2, or 3 hops when the mobile host moves between AP1-AP2, AP2-AP3, and AP3-AP4, respectively.

The simulation results for the basic (hard) handoff performance for Cellular IP hard handoff and HAWAII UNF are very similar. In both cases handoff delay is related to the packet delay between the APs and the crossover node. When the mobile host moves between AP1 and AP2 the delay is small. If the crossover distance is larger, the handoff delay increases with an extra packet delay of 2 ms for each additional hop. The results are a direct consequence of the similarity between these two protocols, particularly in the way in which the protocols build up the route between a crossover node and the new AP. In contrast, Hierarchical Mobile IP updates routing only when registration messages reach the GFA. Therefore, Hierarchical Mobile IP cannot benefit from the fact that a crossover node is topologically close to the APs. This phenomenon is illustrated in the results where the handoff delay for Hierarchical Mobile IP is shown to be independent of the crossover distance, and is equal to the handoff performance in the case of the maximum crossover distance for Cellular IP and HAWAII.

For route control messaging, the operation is similar in Hierarchical Mobile IP and HAWAII. However, the crossover node is always at the GFA for Hierarchical Mobile IP, which accounts for the additional delay. The operation of Cellular IP and HAWAII is different when the network topology is not a tree. In HAWAII, path setup messages are directed toward the old access point, while Cellular IP route update packets are sent toward the gateway. For non-tree topologies this difference will often result in different nodes being used as the crossover point. In HAWAII the crossover node lies at the

intersection of the old downlink path and the shortest path between the old and new access points. As a result, the new downlink path will not necessarily be the shortest path between the domain root router (i.e., gateway) and the new access point. This sub-optimal routing problem represents a generic trade-off associated with handoff control signaling in micromobility protocols. If handoff control messages reach the gateway, it will have to deal with a potentially large number of messages causing performance bottlenecks. Keeping routing update messaging close to access points seems reasonable because in most cases the old and new downlink paths overlap, and routing entries do not have to be updated along the common section of the paths. By discarding update messages at the crossover node, nodes higher up the hierarchy do not have to process these messages, hence minimizing the signaling load at those nodes. In HAWAII, for example, a node that receives an update message referring to a mobile host that already has a valid entry assumes it is the crossover node. However, Cellular IP cannot identify the crossover node, thus has no ability to safely discard update messages before the gateway.

Two enhanced handoff schemes such as Cellular IP semi-soft handoff and HAWAII MSF have been also compared in this work [19]. A number of similarities between the performances of these two enhanced handoff schemes have been observed. Both enhancements buffer packets for some time. In both cases, the amount of time data packets are buffered influences handoff performance. Both are capable of totally eliminating packet loss at the expense of packet duplication. However, Cellular IP semi-soft handoff [21] allows a mobile host to set up routing to the new access point prior to handoff, while HAWAII MSF operates after handoff. The only performance difference is

that HAWAII's forwarding scheme introduces packet reordering in addition to duplication. The performance of HAWAII MSF handoff is somewhat lower than that of Cellular IP semisoft handoff. This difference is because the TCP protocol reacts adversely to the level of packet reordering introduced by the HAWAII MSF scheme.

The disruption performances of the four HAWAII path setup schemes and two Mobile-IP schemes are investigated by R. Ramjee et al. [16]. They were simulated using the HARVARD simulator [22]. The transfer of a packet in the simulated network is achieved through execution of real TCP/UDP/IP code in the kernel. In order to compare the disruption caused during a handoff by the various schemes quantitatively, consider the operation of an interactive audio application. The application typically uses a playout delay to overcome network jitter. The packet playout time at the receiver is set to packet-send-time + playout delay. If the packet arrives after its playout time, it is dropped. The total packet loss, including packets dropped due to late arrival as well as packets lost in the network, are investigated. While one would expect the HAWAII schemes which operate locally to outperform the basic Mobile-IP scheme, the performance differences between the HAWAII schemes and the Mobile-IP Route Optimization (RO) scheme is less clear. In the Mobile-IP RO scheme [23], packets are forwarded from the old FA to the new FA to reduce disruption during handoff. Still, the mobile device's COA changes each time the user moves between neighboring base stations, resulting in undesirable notifications to the HA and the correspondent hosts on every handoff. While in HAWAII, local update results in packets being quickly redirected to the new base station.

It is observed that at higher value of playout delay, the Mobile-IP RO scheme results in comparable total loss as HAWAII; while at lower value of playout delay, the localized

HAWAII schemes result in smaller disruption to audio/video traffic compared to the Mobile-IP schemes. This is because the HAWAII schemes switch over very quickly to the new route, while in Mobile-IP RO scheme, the home agent and then the correspondent host must be notified before packets use the new route. Among the HAWAII schemes, UNF performs best for mobile hosts that can listen to two base stations simultaneously, while MNF performs best for mobile hosts that can listen to only one base station at any given time. SSF and MSF are lossless and deliver good performance but require slightly larger values of playout delay. The forwarding schemes (SSF and MSF) have slightly lower performance than the non-forwarding schemes. Between SSF and MSF, SSF slightly outperforms MSF; the difference is due to the creation of multiple flows in the MSF scheme that results in older packets getting delayed beyond their playout time. For higher values of playout delay, the forwarding schemes outperform the MNF scheme. It is also reported that HAWAII's approach to managing mobility locally results in almost ten times lower processing overhead at the most heavily loaded router as compared to using a non-hierarchical approach based on Mobile-IP. Even if the processing time for a Mobile-IP registration is optimized to a much lower value, the total number of control messages received by a home agent is still almost three times the number of messages received by a domain root router in HAWAII. The reason is because the home agent has to perform several actions when processing a Mobile-IP registration: authenticate the message, enable proxyarp for the mobile host, remove the old entry from the home list, and add the new care-of address for the mobile host.

2.4. Mobility Management Proposals for the Integration of MANET with Internet

Existing Internet protocols or one-hop solutions such as Mobile IP, which are designed for single hop wireless networks, do not necessarily take into account the unique aspects of the wireless environment. Although a significant body of research has been done on ad hoc routing, these protocols do not scale well to the Internet. Until now, there are only few complete proposals for connecting ad hoc networks together to form larger networks, or for integrating them with the Internet. Gateway Model and Cluster Gateway Model are the only two related techniques proposed in the literature. However, no simulation results have been published to demonstrate the performance of these proposals.

2.4.1. Gateway Model

J. Broch, D. Maltz, and D. Johnson have proposed a Gateway Model [24] to integrate ad hoc networks into the hierarchical Internet and support the migration of mobile nodes from the Internet into and out of ad hoc networks via Mobile IP.

The addressing scheme inside the ad hoc network is designed to be flat. Each node participating in the ad hoc network selects a single IP address, which is referred to as the node's home address. The assignment of home addresses can use many different mechanisms, subject to the basic requirement that the addresses be globally unique. Since each node is known to other nodes by a single IP address, thus a unique interface index is required to distinguish between the multiple network interfaces a node might carry. With the exception of several reserved indices, these index values are local to each node, and unique to the network interface. This eliminates the need to globally agree on a mapping

between interface indices and interface types and allows nodes to encode extra information that is locally significant into the index value.

Routing within the ad hoc network is flat, and routing within the Internet is hierarchical. Local delivery within the ad hoc "subnet" is accomplished using the DSR protocol while standard IP routing mechanisms decide which packets should enter and leave the subnet.

Figure 12 [24] depicts how an ad hoc network can be connected to the Internet. Node **G1** is a gateway between the ad hoc network and the Internet. Routing on **G1**'s interface internal to the ad hoc network is accomplished using Dynamic Source Routing (DSR), while its interface connected to the Internet is configured to use normal IP routing mechanisms.

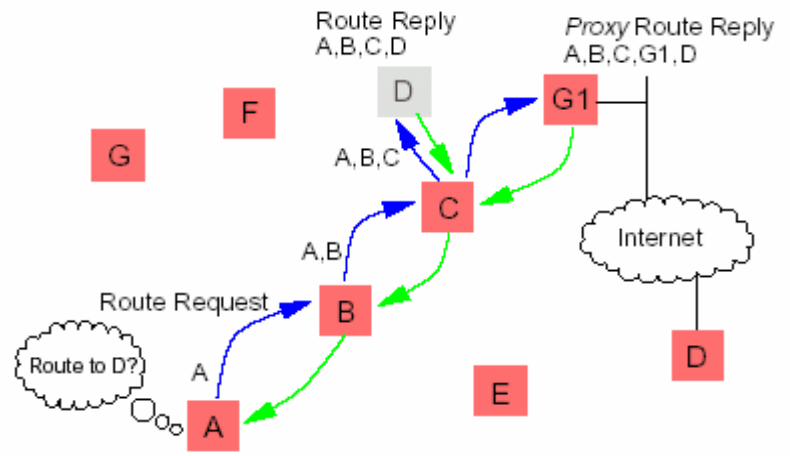

Figure 12: A Route Request for D Being Answered by D and by the Gateway

In order for node **A** (within the ad hoc network) to communicate with node **D** (outside of the ad hoc network), **A** simply initiates Route Discovery for **D**. As the ROUTE REQUEST from **A** targeting **D** propagates, it is eventually received by the gateway node **G1**. If **G1** believes **D** is reachable outside the ad hoc network, it sends a proxy reply listing itself as the second-to-last node in the route and **D** as the last node in the route.

When generating a proxy reply, the reserved gateway interface index (253) is used to distinguish this reply from normal route replies.

When node **A** subsequently originates a data packet for node **D**, the source route on the packet will be **A/1->B/1->C/1->G1/253->D** (the number denotes the interface). When node **G1** receives the packet for **D** it will notice the reserved gateway interface index in the source routing header, remove the source routing header from the packet, and transmit the packet on its interface to the Internet. This packet will have an IP source address of **A** and an IP destination address of **D,** which is identical to a packet that **A** would send to node **D** if it were attached to a normal IP subnet instead of a DSR ad hoc network. If the target node **D** is actually inside the ad hoc network (Figure 12), then node **A** will receive a ROUTE REPLY from both **G1** and **D**. Since the REPLY from **D** will not contain a gateway interface index, **A** can prefer the direct route when sending packets to **D**.

The primary mechanism used to support visiting mobile nodes is Mobile IP. For example, if an external node **D** would like to communicate with a node in the ad hoc network, it will transmit a Mobile IP AGENT SOLICITATION piggybacked on a ROUTE REQUEST targeting the IP limited broadcast address. When the gateway node **G1** receives the SOLICITATION, it will reply with an AGENT ADVERTISEMENT, allowing the external node **D** to register with it in order to provide Mobile IP foreign agent services. Once the registration is complete, the external node **D**'s home agent will use Mobile IP to tunnel packets destined for **D** to foreign agent **G1** and **G1** will deliver the packets locally to the mobile node using DSR.

Figure 13 [24] shows three different ad hoc clouds, a shaded cloud, a white cloud, and a striped cloud, each connected to the other clouds using long-range radios. Suppose node **A** in **G1** is performing Route Discovery for node **B** in **G2**. The Route Discovery would propagate throughout the entire ad hoc network, bothering nodes in all three clouds. However, if the home addresses are assigned such that each cloud is a distinct IP subnet, the multi-homed Gateways (**G1**, **G2**, and **G3**) can be configured not to forward ROUTE REQUEST packets into their cloud if the REQUEST targets an address not in their subnet. In this example, the ROUTE REQUEST would be contained to the three gateways (**G1**, **G2**, and **G3**) and the white and shaded clouds; it would not needlessly be propagated into the striped cloud.

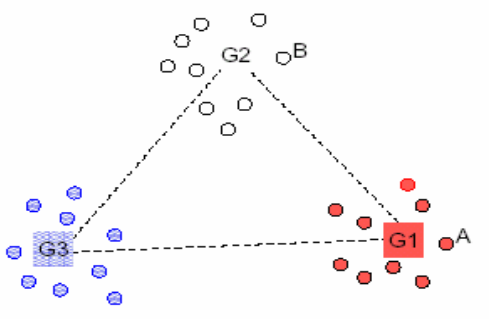

Figure 13: Hierarchical Routing in the Absence of Wired Infrastructure

Furthermore, each gateway can proxy reply for nodes in their cloud, which will decrease the latency of Route Discovery. When a packet from node **A** to node **B** arrives at **G2**, **G2** will take responsibility for delivering the packet to **B**, performing Route Discovery as necessary. This is extremely advantageous because topological change in the white cloud is then completely hidden from node **A**, meaning that **A** will not need to perform Route Discovery simply because **B** is moving around inside of its cloud.

2.4.2. Cluster Gateway Model

Cluster Gateway (CG) [25] is proposed as a protocol-independent Internet gateway for ad hoc networks, which provides Internet access by acting as both a service access point and a Mobile IP Foreign Agent for ad hoc networks. The CG model provides a framework, which is independent of the underlying ad hoc routing protocol while providing a uniform set of services to nodes on the ad hoc network. The CG model works together with existing ad hoc routing protocols (The Source Initiated Routing Protocol, etc.) as well as Mobile IP to provide seamless Internet access for mobile nodes on Autonomous Wireless Local Area Network (AWLAN).

The CG model consists of two modules:

- Application Module: for routing packets between the AWLAN and the Internet.
- Node Support Module: for connecting the node to the CG application, registration with the CG node, location queries, and data forwarding to the CG.

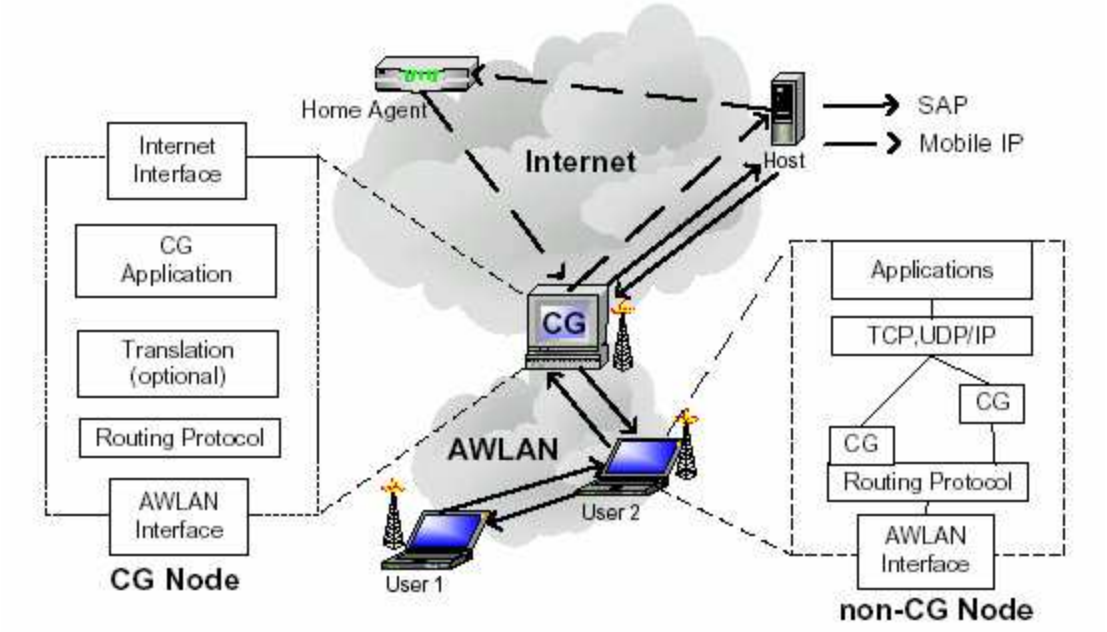

Figure 14: Internet Access via the Cluster Gateway

For packets from the Internet side (Figure 14 [25]) of the CG node, the CG application module is responsible for promiscuously monitoring, responding, and forwarding the appropriate packets to the AWLAN. For packets from the AWLAN side of the CG node, the CG application module is responsible for monitoring a specific type of packets (registration messages, advertisement solicitations, location requests, and encapsulated data packets) as outlined by the services offered by the CG. The actual translation of the routing protocol messages to CG messages takes place in the CG node support module. Thus, the CG application module and the services offered by the CG are kept independent of the routing protocol.

The CG node support module may be implemented in a variety of fashions depending upon the underlying routing protocol, the behavior of nodes in the network and the type of services required. It may be built into the actual routing protocol module (dependent) or constructed on top of the routing protocol module (independent):

- Dependent case: a translation is done at the CG node between the routing protocol messages and CG messages, which reduces the CG messages across the AWLAN and reduces the requirements of non-CG nodes for CG support
- Independent case: CG messages flow across the AWLAN like normal data messages with minimal changes to the routing protocol, which requires a separate CG module at each node that is location-aware since no translation occurs at the CG node.

Since an AWLAN can be dynamic, it may or may not posses a route to a CG. All non-CG nodes are expected to try to find potential CGs. Once a CG is detected, all nodes in the AWLAN should attempt to register with it, which allows the CG to appropriately allocate resources and to perform location resolution in a routing protocol independent manner.

Under the CG model, a node may select two broad classes of service:

- Service Access Point (SAP) service: CG acts as a simple Internet access point whereby packets are intelligently translated and forwarded to the Internet.
- Mobile IP service: CG acts as a Foreign Agent through Mobile IP support.

SAP service offered by the CG is a lightweight service for nodes that desire simple Internet access. This service is offered for nodes that desire one of the following features:

- The node does not want to implement Mobile IP
- The node desires to eliminate the triangle routing of Mobile IP

For this service, the CG will perform a Network Address Translation (NAT) for all outgoing packets from the node in order to assure proper routing from the global Internet, thus all connections must be initiated by nodes inside the AWLAN. Another important reason for using the SAP service is to eliminate the triangle routing aspect of Mobile IP. Although it is possible under Mobile IP for nodes to eliminate the triangle routing through route optimization, this is currently unavailable for the majority of Internet hosts. Such optimizations will probably not be deployed on a large scale until IPv6, due to the inclusion of authentication requirements in IPv6. Thus, by selecting the SAP service, the traffic or connection for the AWLAN node is routed directly between the host and the node due to the NAT done by the CG.

The Mobile IP service is offered to nodes with Mobile IP clients, especially for companies or institutions that desire a higher level of security. These nodes may desire additional authentication, mobile access to company resources, or the ability for remote accessibility from the Internet. In the Mobile IP service mode, the CG node acts as a Foreign Agent for the node on the AWLAN. The FA component of the CG may be

independent of the CG application itself. Thus, the registration with the CG is entirely independent from the Mobile IP registration. Although Mobile IP was originally intended for a single hop environment, it can be extended to ad hoc networks by the support for several key components of Mobile IP.

2.5. Summary

Mobility management and micromobility management protocols have been reviewed in this chapter. As described previously, Mobile IP is designed primarily to provide transparent packet redirection to non-real time TCP applications running on conventional network hosts. The triangle routing of IP packets to the mobile nodes through home agent results in disruption to user traffic during handoff. The change of the COA of a mobile node at the home agent whenever it moves from one access point to another leads to frequent registrations with the home agent and causes significant high control overhead. With Route Optimization in Mobile IP, packets are forwarded from the old foreign agent to the new foreign agent to reduce disruption during handoff. Still, the mobile node's COA changes each time the user moves between neighboring base stations, resulting in undesirable notifications to the home agent and the correspondent hosts on every handoff. IP micromobility protocols are designed to overcome these limitations in Mobile IP. They are suitable for environments where mobile hosts change their point of attachment to the network so frequently that the base Mobile IP mechanism introduces significant network overhead in terms of increased delay, packet loss and signaling. In these micromobility protocols, the Mobile IP is the basis for mobility management in wide-area inter-domain mobility, and the micromobility protocol is used to handle the local (intra-domain) mobility. IP micromobility protocols complement Mobile IP by offering fast and

seamless handoff control in limited geographical areas, and IP paging in support of scalability and power conservation.

From the review of a number of key micromobility protocols (Hierarchical Mobile IP, HAWAII and Cellular IP), despite the difference in the design approach, the fundamental operating principles that underpin these protocols are similar. Especially between HAWAII and Cellular IP, a number of similarities in the operation are observed. Table 1 [7] shows a simple comparison of Hierarchical Mobile IP, HAWAII and Cellular IP.

Table 1: Simple Comparison of Cellular IP, Hawaii and Hierarchical Mobile IP

	Cellular IP	Hawaii	Hierarchical MIP
OSI Layer	L3	L3	"L3.5"
Nodes Involved	all CIP nodes	all routers	FAs
Mobile Host ID	home addr	c/o addr	home addr
Intermediate Nodes	L2 switches	L2 switches	L3 routers
Means of Update	data pkt	signalling msg	signalling msg
Paging	implicit	explicit	explicit
Tunneling	no	no	yes
L2 Triggered Handoff	optional	optional	no
MIP Messaging	no	yes	yes

The most important difference between these protocols is the choice of protocol layer at which per-host location information is stored and maintained. If the protocol is implemented at layer 3, mobile hosts are most logically identified by IP addresses, as in Cellular IP and HAWAII. In contrast, if the protocol layer is implemented at layer 3.5, the involved nodes are tunneling endpoints, as in Hierarchical Mobile IP. Thus, the choice of the protocol layer determines the type of the mobile host identifier, the protocol layer associated with intermediate nodes, and the type of involved nodes.

The similarity between HAWAII and Cellular IP is also observed in the way that the protocols build up the route between a crossover node and the new access point. In contrast, Hierarchical Mobile IP updates routing only when registration messages reach GFA.

Based on the similarity between HAWAII and Cellular IP in handling handoff, as well as the availability of Columbia IP Micromobility Software (CIMS) NS-2 extension, which includes NS implementations for Cellular IP, HAWAII and Hierarchical Mobile IP, two different micromobility protocols, Hierarchical Mobile IP and HAWAII, are chosen for this work.

As described earlier in this chapter, much effort and progress has been made for single hop wireless networks (i.e., cellular networks and wireless LANs) by using these micromobility protocols [19, 21], but they do not necessarily take into account the unique aspects of the ad hoc wireless environment. Although a significant body of research has been done on ad hoc routing protocols, these protocols do not scale well to the Internet. Until now, there are few proposals for connecting ad hoc networks together to form larger networks, or for integrating them with the Internet. The Gateway Model [24] and the Cluster Gateway Model [25] are the only two related techniques proposed in the literature. However, little is known about the actual performance of these proposals, since no simulation results have been published to demonstrate the performance of these proposals. This introduces the necessity and importance of this work: investigating the feasibility of the micromobility protocols for the integration of ad hoc networks with the Internet.

Chapter 3. Simulation Environment

This chapter provides a detailed description of the simulation environment, such as the network simulator (NS) and the Columbia IP Micromobility Software (CIMS) [20], which includes NS implementations of relevant micromobility protocols. The design and implementation decisions in CIMS for Hierarchical Mobile IP and HAWAII that are used in this work are also presented.

3.1. Network Simulator (NS) Overview

This section briefly introduces the general structure and architecture of the network simulator (NS) [26], which is the simulation tool used for all the simulations in this work. NS is an event driven network simulator developed at UC Berkeley that simulates a variety of IP networks. It implements network protocols such as TCP and UPD, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and more. NS also implements multicasting and some of the MAC layer protocols for LAN simulations. NS also includes tools for simulation results display, analysis and converters that convert network topologies generated by well-known generators to NS formats. The current version NS-2 (version 2) is written in C++ and OTcl (Tcl script language with Object-oriented extensions developed at MIT).

As shown in Figure 15 [27], in a simplified user's view, NS is an Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries, and network setup module libraries. To setup and run a simulation

network, a user should write an OTcl script that initiates an event scheduler, sets up the network topology using the network objects and the plumbing functions in the library, and tells traffic sources when to start and stop transmitting packets through the event scheduler. The term "plumbing" is used for a network setup, because setting up a network is plumbing possible data paths among network objects by setting the "neighbor" pointer of an object to the address of an appropriate object. The power of NS comes from this plumbing.

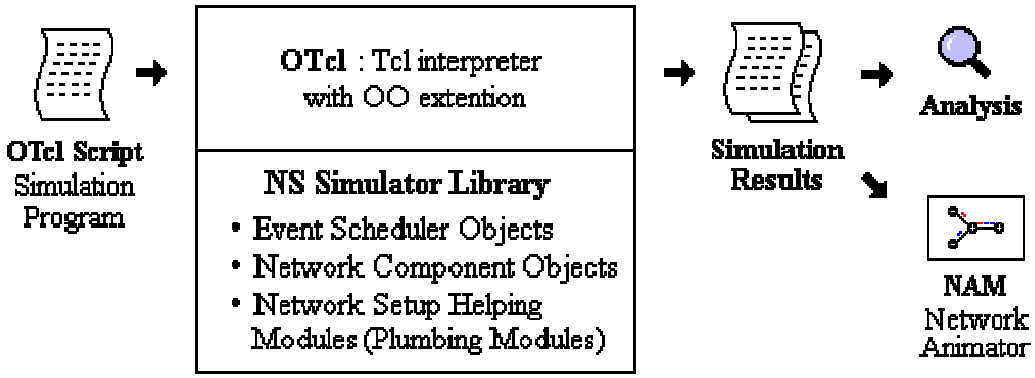

Figure 15: Simplified User's View of NS

Another major component of NS beside network objects is the event scheduler. An event in NS is a packet ID that is unique for a packet with scheduled time and the pointer to an object that handles the event. In NS, an event scheduler keeps track of simulation time and fires all the events in the event queue scheduled for the current time by invoking appropriate network components, which usually are the ones who issued the events, and let them do the appropriate action associated with the event. Network components communicate with one another passing packets, however this does not consume actual simulation time. As using the abstract model of the object, there is no processing delay for processing a message. If a the network component needs to spend some simulation

time handling a packet (i.e. needs a delay), it then use the event scheduler by issuing an event for the packet and waiting for the event to be fired to itself before doing further action handling the packet. Another use of an event scheduler is as timer. For example, TCP needs a timer to keep track of a packet transmission timeout for retransmission (transmission of a packet with the same TCP packet number but different NS packet ID). Timers use event schedulers in a similar manner to delay. The only difference is that a timer measures a time value associated with a packet and does an appropriate action related to that packet after a certain time goes by, and does not simulate a delay.

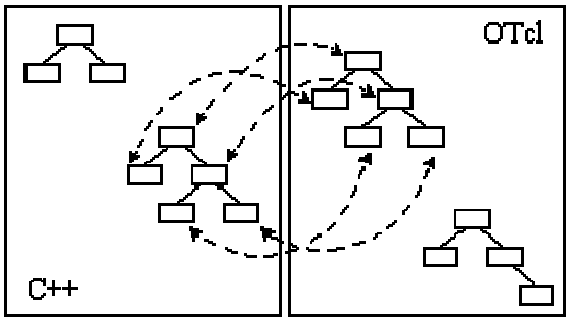

Figure 16: C++ and OTcl: The Duality

NS is written not only in OTcl but in C++ also. For efficiency reasons, NS separates the data path implementation from control path implementations. In order to reduce packet and event processing time (not simulated time), the event scheduler and the basic network component objects in the data path are written and compiled using C++. These compiled objects are made available to the OTcl interpreter through an OTcl linkage that creates a matching OTcl object for each of the C++ objects. The control functions and the configurable variables specified by the C++ object act as member functions and member variables of the corresponding OTcl object. In this way, the controls of the C++ objects are given to OTcl. It is also possible to add member functions and variables to a C++

linked OTcl object. The objects in C++ that do not need to be controlled in a simulation or internally used by another object do not need to be linked to OTcl. Likewise, an object can be entirely implemented in OTcl. Figure 16 [27] shows an object hierarchy example in C++ and OTcl. Its is shown that for C++ objects that have an OTcl linkage forming a hierarchy, there is a matching OTcl object hierarchy very similar to that of C++.

Figure 17 [27] shows the general architecture of NS. In this figure a general user, not an NS developer, can be thought of as standing at the left bottom corner, designing and running simulations in Tcl using the simulator objects in the OTcl library. The event schedulers and most of the network components are implemented in C++ and available to OTcl through an OTcl linkage that is implemented using tclcl, which is a Tcl/C++ interface used by NS to glue C++ over OTcl. The whole package together is NS, which is an OO extended Tcl interpreter with network simulator libraries.

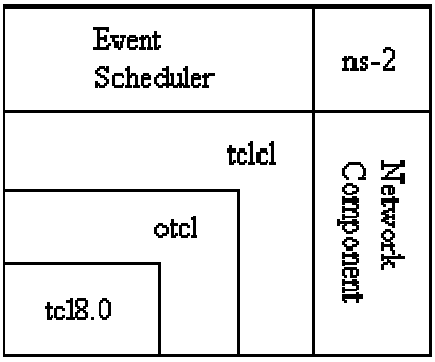

Figure 17: Architectural View of NS

As shown in Figure 15, when a simulation is finished, NS produces one or more text-based output files that contain detailed simulation data, if specified to do so in the input Tcl (or more specifically, OTcl) script. The data can be used for simulation analysis or as an input to a graphical simulation display tool called Network Animator (NAM). NAM has a nice graphical user interface, and also has a display speed controller. Furthermore,

it can graphically present information such as throughput and number of packet drops at each link, although the graphical information cannot be used for accurate simulation analysis.

3.2. NS2-extension: Columbia IP Micromobility Software (CIMS)

The Columbia IP Micromobility Software (CIMS) [20] v1.0 release includes NS implementations of Cellular IP, HAWAII, and Hierarchical Mobile IP. These micromobility protocols aim to support fast handoff control with minimum or zero packet loss, and to minimize signaling through the introduction of paging techniques, thereby reducing registration to a minimum. The Cellular IP implementation supports hard and semi-soft handoff, and IP paging. The HAWAII implementation supports Unicast Non-Forwarding (UNF) and Multiple Stream Forwarding (MSF) schemes. HAWAII's IP paging capability is currently not supported in CIMS. In addition, the CIMS implementation of Hierarchical Mobile IP currently does not support IP paging.

This section presents the design and implementation details in CIMS for Hierarchical Mobile IP and HAWAII micromobility protocols that are used in this work.

3.2.1. Hierarchical Mobile IP (HFA)

The Hierarchical Mobile IP protocol [28] from Ericsson and Nokia employs a hierarchy of Foreign Agents (FAs) to locally handle Mobile IP registration. In this protocol mobile hosts send Mobile IP registration messages with appropriate extensions to update their respective location information. Registration messages establish tunnels between neighboring FAs along the path from the mobile host to a Gateway Foreign Agent

(GFA). Packets addressed to the mobile host travel in this network of tunnels, which can be viewed as a separate routing network overlay on top of IP.

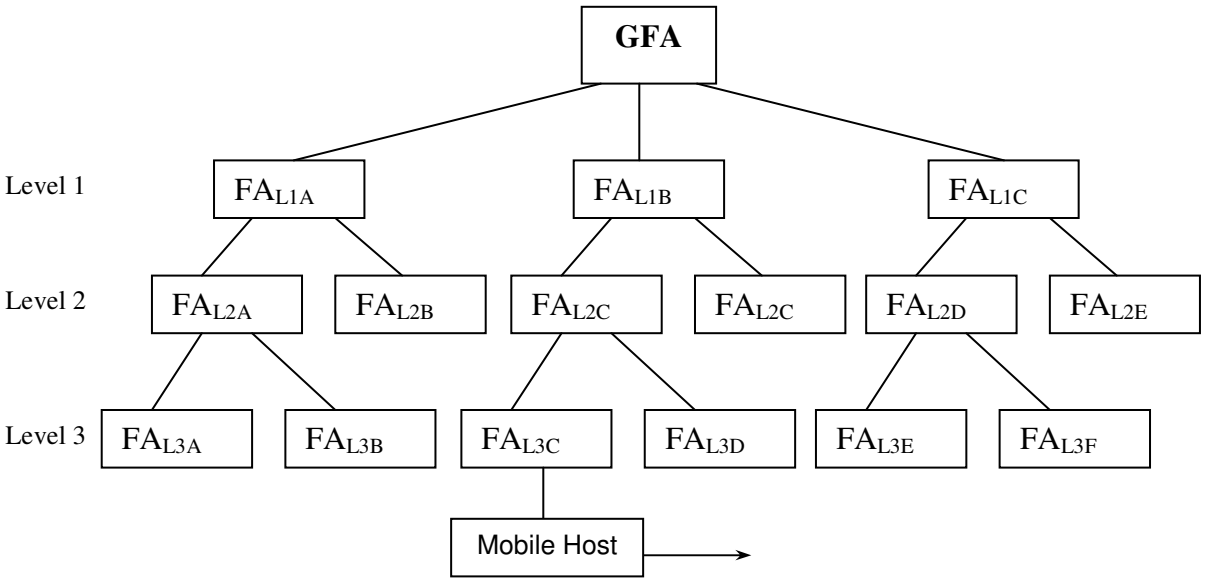

Figure 18: Hierarchy of Foreign Agents

Each FA reads the incoming packet's original destination address and searches its visitor list for a corresponding entry. If the entry exists, it contains the address of the next lower-level FA. The sequence of visitor list entries corresponding to a particular mobile host constitutes the mobile host's location information and determines the route taken by downlink packets. Entries are created and maintained by registration messages transmitted by mobile hosts. Hierarchical tunneling schemes rely on a tree-like structure of FAs (Figure 18). Encapsulated traffic from a HA is delivered to the root FA. Each FA on the tree decapsulates and then reencapsulates data packets as they are forwarded down the tree of FAs toward the mobile host's point of attachment. The use of tunnels makes it possible to employ the protocol in an IP network that carries non-mobile traffic as well. Typically one level of hierarchy is considered where all FAs are connected to the GFA.

This design decision is motivated by the desire to reduce the number of mobility-aware nodes in the network [19]. In this case, direct tunnels connect the GFA to FAs that are located at access points, which is very similar to the traditional Mobile-IP mechanism.

In CIMS, the FA function is implemented in the base station node. A mobile node is created with permanent IP address along with an assigned GFA as its HA. This permanent IP address is also the mobile node's home address. While roaming within its home network, the mobile node performs Mobile IP registration to its home agent (i.e., GFA) to update its current COA.

If the mobile node moves to another network, the address of the GFA in the visiting network should be the mobile node's COA address, the home agent should not be informed of the movements of mobile node inside the visiting network. Hence, signaling overhead is greatly reduced for out of home network (inter-network) mobility. However, this feature is not yet implemented in CIMS.

While moving in its home network, the mobile nodes need to perform Mobile IP registration to update their respective current location information. At this registration, the home agent registers the care-of address (COA) of the mobile node, which is the IP address of the current base station for the mobile host. There can be more than one base station on a network, but each mobile host connects to only one base station at a time, and for each mobile host, only one base station address is recorded as the COA maintained by the mobile host's home agent. Each base station node maintains a list recording the IP address of each visiting mobile host currently registered with it, and also records each mobile host's previous COA and the time of registration. Since a binding between the HA and its COA is valid only for a given period of time, the mobile node

must send the MIPT_REG_REQUEST messages at a regular registration interval to renew the validity of the binding. When roaming, if the mobile node receives a MIPT_ADS (Agent Advertisement) from a different base station node, it sends a MIPT_REG_REQUEST to the new base station node. Upon receiving a registration request (MIPT_REG_REQUEST) from a mobile node, the base station node generates a control message including the requesting COA that propagates toward its home agent, i.e., gateway node. After receiving a MIPT_REG_REQUEST of a mobile node, the gateway node acknowledges this mobile node by sending a MIPT_REG_REPLY message through the intermediate wired nodes and the current FA (the base station node). All the constants used for Mobile IP in ns-2.1b6a are listed in Table 2. Here, the lifetime of the base station advertisement is the maximum length of time that the advertisement is considered valid in the absence of further advertisements. The lifetime of the mobile host registration is the duration for which a binding is valid.

Table 2: Constants used for Mobile IP in ns-2.1b6a

Lifetime of the base station advertisement	2 s
Lifetime of the mobile host registration	2 s
Registration interval of the mobile host	1 s

3.2.2. HAWAII

The HAWAII protocol [16] from Lucent Technologies proposes a separate routing protocol to handle intra-domain mobility. HAWAII relies on Mobile IP to provide wide-area inter-domain mobility. In CIMS, the HAWAII implementation supports Unicast Non-Forwarding (UNF) and Multiple Stream Forwarding (MSF) schemes. An appropriate path setup scheme is selected depending on the operator's priorities between eliminating packet loss, minimizing handoff latency and maintaining packet ordering. HAWAII assigns a unique address for each mobile host that is retained as long as the mobile host remains within its current domain. HAWAII uses path setup messages to establish and update host-based routing entries for the mobile hosts in selective routers in the domain so that packets arriving at the domain root router can reach the mobile host.

The protocol contains three types of messages for path setup: power-up, update and refresh. Path setup update messages are sent by the mobile host during power up and following a handoff. The HAWAII handoff procedures are only activated when the mobile host's next hop IP node is changed during the handoff.

Power Up Processing

When the mobile host powers up, it sends a path setup update message to its nearest base station. This message propagates to the domain root router. Each router on the path between the mobile host and the domain root router adds a forwarding entry for the mobile host. Finally, the domain root router sends back an acknowledgement to the mobile host. At this time, when packets destined for the mobile host arrive at the domain root router based on the subnet portion of the mobile host's IP address, the packets are

routed within the domain to the mobile host using the host-based forwarding entries just established.

While routers process only HAWAII messages, base stations have the additional responsibility of implementing the Mobile-IP foreign agent functionality (without the decapsulation function) and originating HAWAII messages for processing within the domain. The base stations periodically issue agent advertisement messages, and reply to agent-solicitation messages.

On receipt of a registration request from a mobile host, the base station generates HAWAII power-up or handoff update messages based on whether the previous COA exists, and the HAWAII power-up message is forwarded by the base station for registering with the home agent.

Refresh Processing

The mobile host infrequently sends periodic path refresh messages to the base station to which it is attached to maintain the host based entries, failing which they will be removed by the base station. The base station and the intermediate routers, in turn, send periodic aggregate hop-by-hop refresh messages towards the domain root router.

Handoff Processing

Each mobile host in HAWAII is associated with a home domain and the Mobile-IP Home Agent is involved only when the mobile host is visiting a foreign domain. However, even while the mobile host is moving in the HAWAII home domain, the mobile host is required to send registrations to the base station on every handoff so that the HAWAII host-based entries are re-established locally. Whenever the host detects a change of base

station it MUST issue a Mobile IP registration request to the new base station. These registrations are used to trigger HAWAII path setup schemes inside the domain.

Another issue is the need for a mobile host to acquire a co-located care-of address when the host is in a HAWAII foreign domain and use its home address in the HAWAII home domain. However, this feature is not yet implemented in CIMS.

The basic processing of an update message at a router is fairly simple. On receiving the message, modify the forwarding entry for the mobile host in the kernel and forward the update message towards the new or the old base station depending on whether the Forwarding or Non-Forwarding schemes are used.

HAWAII handoff processing for Multiple Stream Forwarding (MSF) scheme

In the forwarding scheme, packets are first forwarded from the old base station to the new base station before they are diverted at the crossover router. The crossover router is defined as the router closest to the mobile host that is at the intersection of two paths, one between the domain root router and the old base station, and the second between the old base station and the new base station.

If the handoff is intra-domain (mobile host's HA matches the domain router's address), the new base station sends a HAWAII_Update message to old base station. Else, if the handoff is inter-domain, the new base station sends the new COA registration to the home agent, and sends a HAWAII_Update message to the old base station only after receiving the approval by the home agent. However, the functions to handle the inter-domain handoff for HAWAII MSF are not yet implemented in CIMS.

The MSF scheme is illustrated in Figure 19. The forwarding table entries are shown adjacent to the routers. These entries are prepended with a message number indicating

which message was responsible for establishing the entry (a message number of zero indicates a pre-existing entry). The letters denote the different interfaces.

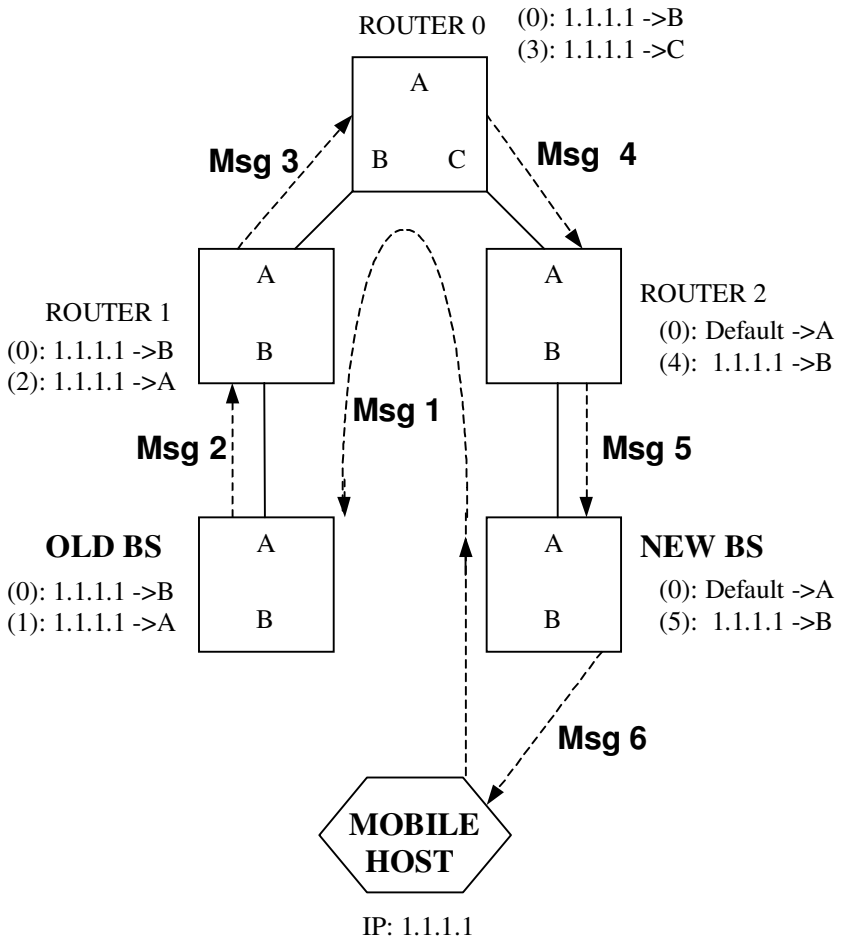

Figure 19: HAWAII Multiple Stream Forwarding (MSF) Path Setup Scheme

Upon receiving a registration request from a mobile host with a different previous COA, the new base station generates a HAWAII_Update message, which is sent directly to the old base station (Message 1). After receiving the HAWAII_Update message, the old base station performs a routing table lookup for the new base station, and determines the interface, interface A, and next hop router, Router 1. The base station then adds a forwarding entry for the mobile host's IP address with the outgoing interface set to interface A. It then forwards Message 2 to Router 1. Router 1 performs similar actions

and forwards the message to Router 0. Router 0, the crossover router in this case, adds forwarding entries that result in new packets being diverted to the mobile host at the new base station. It then forwards the message towards the new base station. Eventually Message 5 reaches the new base station that changes its forwarding entry and sends an acknowledgement of the path setup message to the mobile host, shown as Message 6 [29]. Note that only the new and old base stations, and the routers connecting them, are involved in processing the path setup message. Also, only routers on the path between the new base station and the domain root router will receive the periodic refresh messages. Therefore, the entries in Router 1 and the old base station, which are no longer on this path, will timeout, while the entries in Routers 0 and 2, and the new base station will get refreshed.

HAWAII handoff processing for Unicast Non-Forwarding (UNF) scheme

In the Non-forwarding schemes, as the path setup message travels from the new base station to the old base station, data packets are diverted at the cross-over router to the new base station, resulting in no forwarding of packets from the old base station.

If handoff is intra-domain, the new base station obtains the mobile node's information (IP address, old base station address and timestamp). Else, if the handoff is inter-domain, the new base station sends a COA registration to the home agent, and records the mobile node's information only when the registration is accepted and acknowledged by the home agent. Again, the functions to handle the inter-domain handoff for HAWAII UNF are not yet implemented in CIMS.

The UNF scheme is illustrated in Figure 20. Upon receiving a registration request from a mobile host with a different previous COA, the new base station generates the path setup

message, and adds a forwarding entry for the mobile host's IP address with the outgoing interface set to the interface on which it received this message. It then performs a routing table lookup for the old base station and determines the next hop router, Router 2. The new base station then forwards Message 2 to Router 2. This router performs similar actions and forwards Message 3 to Router 0. At Router 0, the crossover router in this case, forwarding entries are added such that new packets are diverted directly to the mobile host at the new base station. Eventually Message 5 reaches the old base station that then changes its forwarding entry and sends an acknowledgement, Message 6, back to the mobile host through the new base station.

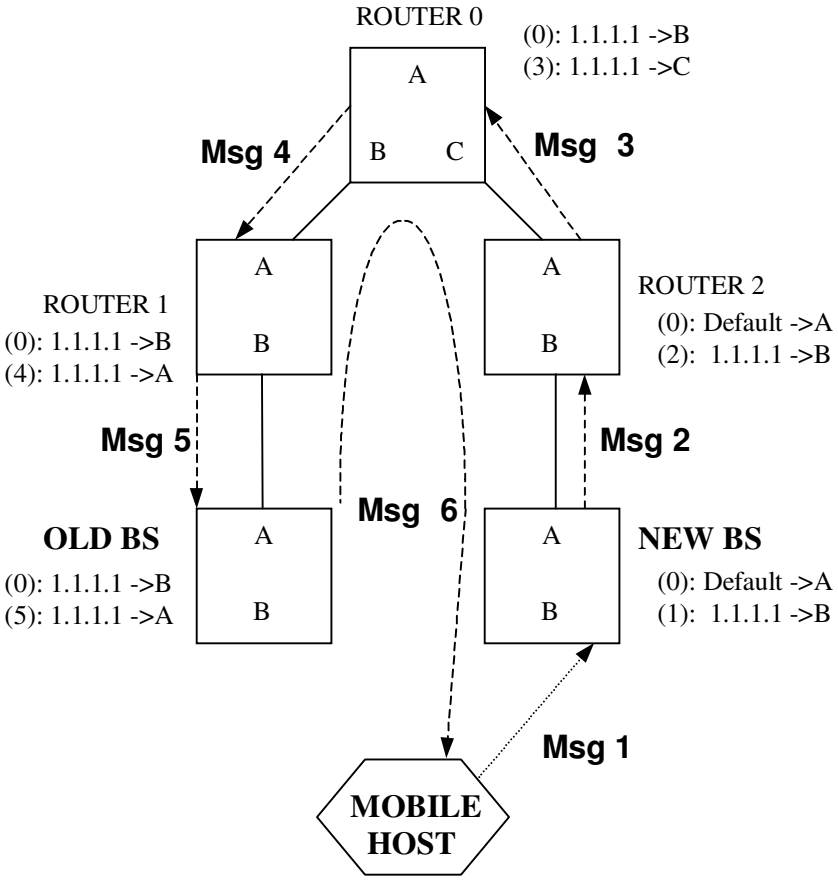

Figure 20: HAWAII Unicast Non-Forwarding (NUF) Path Setup Scheme

Chapter 4. Simulation Experimental Design

This chapter provides the detailed description of the simulation experimental design decisions such as network topology, physical and data link model, hierarchical address and address resolution, packet buffering, ad hoc routing protocol, node movement model and connection mode, scenario characteristics and metrics for performance evaluations of the micromobility protocols.

4.1. Network Topology

All simulations in this work are performed using the network topology shown in Figure 21. This topology has been proposed and used in [19] to compare the performances of IP micromobility protocols, such as Cellular IP, HAWAII and HFA. This structure provides multiple access points for the mobile nodes, as well as allows us to identify the difference in the crossover node selection between the micromobility protocols.

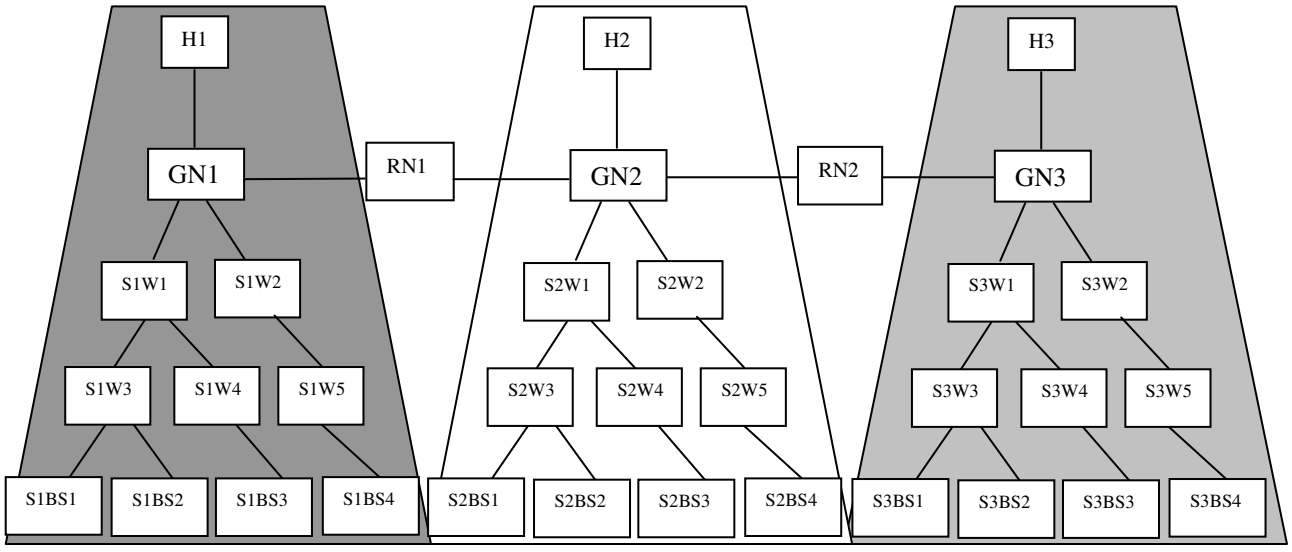

Figure 21: Network Topology

Three subnets are used for the simulations. In each subnet, there is one node acting as a gateway node (GN) to the Internet, four base station nodes (BS) acting as the access points for the ad hoc nodes to the gateway node, and five wired nodes (WN) acting as the routers from the base station nodes to the gateway node. The base station node is the router that connects the ad hoc network to the rest of the Internet.

In HAWAII simulations, the gateway node is the domain root router, and each base station node and wired node is a HAWAII-enabled HAWAIIRouter of its home domain root router. When simulating HFA, GFA function is implemented in the gateway node, all the wired nodes (SiW1-SiW5) represent mobility-unaware routers with collocated base station nodes as FAs. Two subnets are connected by one router node (RN), as node RN1 between subnet 1 and subnet 2 and node RN2 between subnet 2 and subnet 3. These RNs are ordinary wired nodes and they do not belong to any subnet.

4.2. Physical and Data Link Model

Radio engineers typically use a model that attenuates the power of a signal as $1/r^2$ at short distances (r is the distance between the antennas), and as $1/r^4$ at longer distances. The crossover point is called the reference distance d_c. At near distances ($d < d_c$), Friis free-space attenuation ($1/r^2$) is used; at far distance ($d > d_c$), Two-ray ground ($1/r^4$) reflection model is used. In NS-2 implementation [30], these models are used to predict the received signal power of each packet. At the physical layer of each wireless node, there is a receiving threshold. When a packet is received, if its signal power is below the receiving threshold, it is marked as error and dropped by the MAC layer. The approximation assumes specula reflection off a flat ground plane. The crossover point is

calculated to be 86.14 meters. The link layer of our simulator implements the complete IEEE 802.11 standard Medium Access Control (MAC) protocol.

4.3. Hierarchical Address and Address Resolution

In order to use hierarchical routing, the hierarchy of the topology as well as hierarchical addressing of each node need to be defined. In flat routing, every node knows about every other node in the topology. In hierarchical routing, each node knows only about those nodes in its level. For all other destinations outside its level, it forwards the packets to the border router of its level. Thus the routing table size is reduced significantly.

In order to create a topology with 3 subnets defined in Section 4.1, 5 domains are designed to reflect the topology:

- D1 for subnet1
- D2 for router node (RN1)
- D3 for subnet2
- D4 for router node (RN2)
- D5 for subnet3

Since the routing protocols all operate at the network layer using IP addresses, an implementation of ARP [31], was included in the simulation and used to resolve IP addresses to link layer addresses.

4.4. Packet Buffering

Each node has a queue for packets awaiting transmission by the network interface that holds up to 50 packets and is managed in a drop-tail fashion, which implements FIFO scheduling and drop-on-overflow buffer management.

4.5. Ad Hoc Routing Protocol: Destination-Sequenced Distance-Vector (DSDV)

The Destination-Sequenced Distance-Vector Routing protocol [32] allows a collection of mobile nodes, which may not be close to any base station or not within range for direct communication, to exchange data. In addition, it remains compatible with operation in case where a base station is available.

4.5.1. Basic Mechanisms

Each DSDV node maintains a routing table listing all reachable destinations and number of hops to each. Each entry is marked with a sequence number assigned by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, thereby avoiding the formation of routing loops.

Each node in the network advertises a monotonically increasing even sequence number for itself. When a node **B** decides that its route to a destination **D** has broken, it advertises the route to **D** with a metric of ∞, and a sequence number one greater than its sequence number for the route that has broken (resulting in an odd sequence number). Sequence numbers defined by the originating mobile nodes are defined to be even number, and the sequence numbers generated to indicate ∞ metrics are odd numbers. This causes any node **A** routing packets through **B** to incorporate the infinite-metric route into its routing table until node **A** hears a route to **D** with a higher sequence number.

Routing information is advertised by broadcasting or multicasting the packets which are transmitted periodically throughout the network in order to maintain table consistency. The DSDV routing protocol requires each mobile node to advertise, to each of its current

neighbors, its own routing tables by broadcasting its entries. In a wireless medium, broadcasts are limited in the range by the physical characteristics of the medium. Routes received in broadcasts are also advertised by the receiver, when it subsequently broadcasts its routing information; the receiver adds an increment to the metric before advertising the route.

When any new or substantially modified route information is received by a mobile node, the new information will be retransmitted soon. When a link to the next hop has broken, which qualifies as a substantial route change, such modified routes are immediately disclosed in a broadcast routing information packet.

New route broadcasts contain the address of the destination, the number of hops to reach the destination, the sequence number of the information received regarding the destination, as well as a new sequence number unique to the broadcast. Routes with more recent sequence numbers are always preferred as the basis for making forward decisions. Of the paths with the same sequence numbers, those with the smallest metric is used.

To help alleviate the potentially large amount of network traffic that such updates can generate, route updates can employ two possible types of packets:

- Full dump: packet carries all available routing information.
- Incremental: packet carries only that information which has changed since the last full dump.

To prevent fluctuation of route table entry advertisement, mobiles also keep track of the settling time of routes, or the weighted average time that routes to a destination will fluctuate before the route with the best metric is received. By delaying the broadcast of a routing update by the length of the settling time, mobiles can reduce network traffic and

optimize routes by eliminating those broadcasts that would occur if a better route was discovered in the very near future. In order to bias the dumping mechanism in favor of recent events, the most recent measurement of the settling time of a particular route must be counted with a higher weight factor than the less recent measurements.

In order to enable the mobile nodes to be used in conjunction with base stations, it is necessary to allow them to exchange data with other nodes connected to the wired network. Therefore, base station nodes are participating in the DSDV protocol, which can extend their coverage beyond the range imposed by their wireless transmitters. When a base station node participates in DSDV, it is shown as a default route in the tables transmitted by a mobile station. In this way, mobile stations within range of a base station can cooperate to effectively extend the range of the base station to serve other stations outside the range of the base station, as long as those other stations are close to other mobile stations that are within range.

4.5.2. DSDV Implementation Decision in NS Version 2.1b6a

In ns-2.1b6a, the DSDV implementation uses both full and incremental updates as required by the protocol's description. If 30% of the entries of the route table are changed, a full update will be transmitted, else only a partial update will be triggered.

DSDV can be categorized based on the mechanisms of the triggered updates:

- DSDV-SQ (Sequence Number): receipt of a new sequence number for a destination should trigger an update
- DSDV: the update is triggered only upon the receipt of a new metric, and the receipt of a new sequence number is not sufficiently important to incur the overhead of propagating a triggered update

The advantage of the first approach is that the broken links will be detected and routed around as new sequence numbers propagate around the broken links and create alternate routes. It was found that [35], while DSDV-SQ is much more expensive in terms of overhead, it provides a much better packet delivery ratio in most cases. The second scheme (DSDV) is much more conservative in terms of routing overhead, however, since link breakages are not detected as quickly, more data packets are dropped. For all the simulations in this work, simple DSDV was used and all the constants used for DSDV simulation in ns-2.1b6a are listed in Table 3.

Table 3: Constants used for DSDV Routing Protocol in ns-2.1b6a

Periodic route update interval	15 s
Periodic updates missed before link declared broken	3
Initial triggered update weighted settling time	6 s
Weighted settling time weighting factor	7/8
Route advertisement aggregation time	1 s
Maximum packets buffered per node per destination	5

4.6. Node Movement Model

The movement scenario files used for each simulation are characterized by a pause time. Each node begins the simulation by remaining stationary for pause time seconds. It then selects a random destination and moves to that destination at a speed distributed uniformly between 0 and some maximum speed. Upon reaching the destination, the node pauses again for pause time seconds, selects another destination, and proceeds there as previously described, repeating this behavior for the duration of the simulation.

Two types of nodes were defined:

1. Normal nodes: move within the same subnet (a 500m x 500m space)

2. Wandering nodes: move within two adjacent subnets (1000 x 500m space)

Simulation results were obtained using a group of 50 wireless nodes forming an ad hoc network, continuously moving within a subnet (500m x 500m) at a speed that could be varied during the simulation. To observe the wandering node effect, 10 wandering nodes were included among the 50 wireless nodes.

Parameters used for the movement files are:

- Each simulation ran for 900 seconds of simulated time.
- Pause time: 20 seconds.
- Maximum speed: 1 m/s, 10 m/s and 20 m/s.

The simulation time is fixed at 900 seconds. This insures that network stability is achieved. This choice also makes it possible to compare the simulation results with previous ones obtained in this research group [33]-[34] and those found in the literature [35]. Preliminary studies showed no effect of pause time on simulation results. Three different maximum speeds were experimented with in order to observe the impact of node movement speed on the performance of micromobility protocols.

4.7. Traffic Model

As the goal of the simulation is to compare the performance of the micromobility protocols, the traffic source is chosen to be constant bit rate (CBR) sources. The following parameters are used for the communication model, which are used widely in the literature [35].

- sending rates: 4 packets per second;
- Number of CBR sources: 20;
- Packet sizes: 64 bytes.

All communication patterns were chosen to be peer to peer, and connections were started at times uniformly distributed between 0 and 180 seconds. Two connection patterns were combined with six movement patterns, providing a total of 12 different scenario files for each simulation result. Therefore, all micromobility protocols were run on the same 12 scenario files for each simulation result. Each simulation result presented in this work is the average value of 12 simulation results.

4.8. Scenario Characteristics

Table 4 lists the average number of link connectivity changes that occurred during each simulation run (900 second) for each node movement speed. Whenever a node goes into or out of direct communication range with another node, the link connectivity change, and the resulting route change, are counted.

Table 4: Average Number of Link Connectivity Changes during each Simulation as a Function of Node Movement Speed

Maximum speed (m/s)		Number of Unreachable Destinations	Number of Link Changes	Number of Route Changes
1	No wandering nodes	0	1291	1526
	20 % wandering nodes	188	1207	2383
10	No wandering nodes	0	7910	9389
	20 % wandering nodes	743	6978	14454
20	No wandering nodes	0	12963	15977
	20 % wandering nodes	964	11240	23774

4.9. Metrics

To compare the performance of HFA and HAWAII protocols, the following three metrics were used:

- Packet delivery ratio: The ratio between the number of packets sent by the sender and the number of packets received by the destination node.
- DSDV routing overhead: The ratio between the number of control messages sent or forwarded by the DSDV agent and the number of packets sent by the sender.
- Control message overhead: The number of control messages sent by each network component, such as the gateway nodes, wired nodes, base station nodes and router nodes.

Packet delivery ratio is important as it describes the loss rate that will be seen by the transport protocols. Since the same ad hoc routing protocol (DSDV) was used, the packet delivery ratio represents the maximum throughput that the network can achieve, which is determined by the micromobility protocol. This metric characterizes both the correctness and efficiency of the micromobility protocol and ad hoc routing protocol.

The goal of this work is to compare the micromobility protocols with each other, not only in terms of network performance but also in terms of cost. The routing overhead caused by the DSDV routing protocol was also evaluated in order to investigate the ad hoc routing effect on the network managed by the micromobility protocol.

Finally, the control message overhead caused by the micromobility protocol at each network component is also investigated. The control message overhead is an important metric for comparing micromobility protocols, since it measures the scalability of a protocol, the degree to which it will function in congested or low-bandwidth environments, and its efficiency in terms of consuming node battery power. Protocols that send large numbers of control message packets can also increase the probability of packet collisions and may delay data packets in network interface transmission queues.

Chapter 5. Simulation Results and Performance Comparisons

This chapter first provides the descriptions of the simulation scenarios, followed by the simulation results obtained by Hierarchical Mobile IP and HAWAII micromobility protocols. Finally, their performances are compared.

5.1. Simulation Scenarios

In order to enable the communication between an ad hoc node with any other node on the Internet, four different scenarios were investigated. These scenarios are described in the following paragraphs.

5.1.1. Wired hosts to ad hoc nodes

Subnet1 (500mx500m) GN1 (host1)	Subnet2 (500mx500m) GN2 (host2)	Subnet3 (500mx500m) GN3 (host3)

For each connection, a randomly selected wired host (host1, host2 and host3) sends data packets to a randomly selected ad hoc node moving in the subnet2 (the striped area).

5.1.2. Ad hoc nodes to wired nodes

Subnet1 (500mx500m) GN1 (host1)	Subnet2 (500mx500m) GN2 (host2)	Subnet3 (500mx500m) GN3 (host3)

For each connection, a randomly selected ad hoc node moving in subnet2 (the shaded area) sends packets to a randomly selected wired host (host1, host2 and host3).

5.1.3. Ad hoc nodes to ad hoc nodes in separate subnets

Subnet1 (500mx500m) GN1 (host1)	Subnet2 (500mx500m) GN2 (host2)	Subnet3 (500mx500m) GN3 (host3)

For each connection, a randomly selected ad hoc node moving in subnet1 (the shaded area) sends packets to a randomly selected ad hoc node moving in subnet3 (the striped area). In this scenario, the sender nodes and the receiver nodes are not in communication range of each other.

5.1.4. Ad hoc nodes to ad hoc nodes in adjacent subnets

Subnet1 (500mx500m) GN1 (host1)	Subnet2 (500mx500m) GN2 (host2)	Subnet3 (500mx500m) GN3 (host3)

For each connection, a randomly selected ad hoc node moving in subnet1 (the shaded area) sends packets to a randomly selected ad hoc node moving in subnet2 (the striped area). In this scenario, the sender nodes and the receiver nodes may be in communication range of each other, if they are moving along the border of the adjacent subnets.

5.2. Hierarchical Mobile IP Simulation Results

As described above, simulations are conducted with four different simulation scenarios:

A: wired hosts to ad hoc nodes;

B: ad hod nodes to wired hosts;

C: ad hoc nodes to ad hoc nodes in separate subnets;

D: ad hoc nodes to ad hoc nodes in adjacent subnets.

For each scenario, three different maximum node movement speeds are considered. The simulation results for Hierarchical Mobile IP are presented in this section.

5.2.1. Packet Delivery Ratio

Table 5 shows the packet delivery ratio as a function of node mobility rate for all simulation scenarios. This ratio is defined as the total data packets received by destination nodes over the total data packets sent by the source nodes.

Table 5: Packet Delivery Ratios (%) for Hierarchical Mobile IP Protocol

Maximum speed (m/s)	Scenario A	Scenario B	Scenario C	Scenario D
1	73.74	70.67	53.58	63.00
10	85.05	83.33	75.30	33.16
20	83.58	83.79	72.28	32.02

For simulation scenarios A and B, data packets are delivered through heterogeneous interfaces, and all the packets are routed through the gateway node in order to reach the destination nodes, as illustrated in Figure 22 (circles represent the ad hoc nodes). When comparing the delivery ratios, any difference less than 1% is considered insignificant, while a difference of more than 5% is considered significant. Table 5 shows a significant increase in packet delivery rate when node maximum movement speed increases from 1 to 10 m/s, but no significant change was observed when the speed increases from 10 to

20 m/s. These observations can be explained by the behavior of the DSDV routing protocol employed for the ad hoc network.

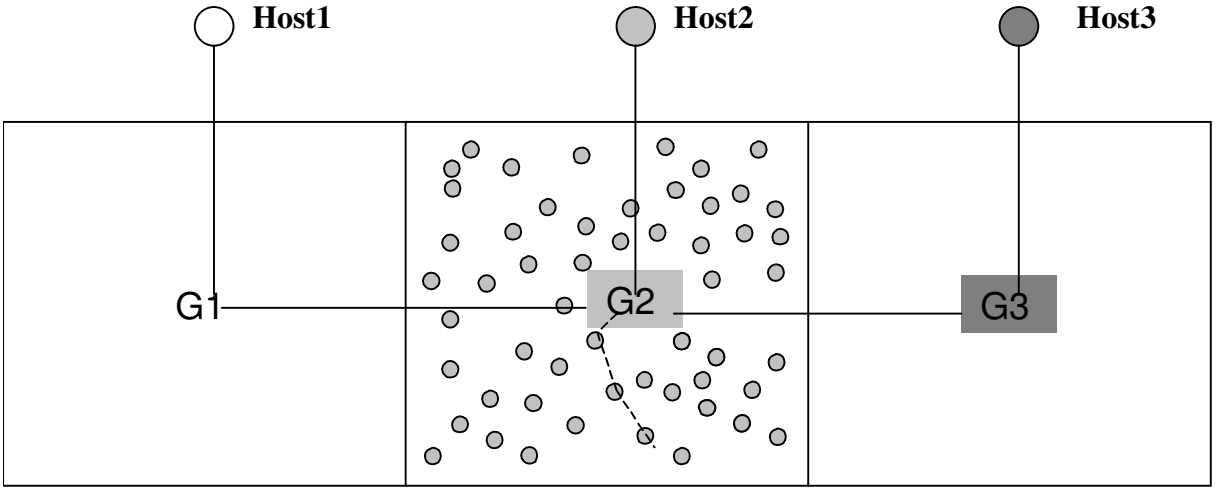

Figure 22: Packets Delivery through Heterogeneous Interfaces (Scenario A and B)

Analysis of the distributions of packet loss for these two scenarios (A and B) shows that the packet loss can occur either in the ad hoc network or between the heterogeneous interfaces. Each packet dropped in the ad hoc network is due to a broken link without an alternate route. When packets are sent from wired hosts to ad hoc nodes, the delivery failure between the heterogeneous interfaces is either due to the absence of an available route from the base station to any of the ad hoc nodes or handoff failure. When packets are sent from ad hoc nodes to a wired host, this delivery failure is due to the absence of an available route to the base station. In this case, the packet is freed (discarded but not traced) by the routing agent if no route to base station is available.

The number of packet loss caused by link failure among the ad hoc nodes can be obtained by counting the “Drop” packets (discarded and traced) marked by the DSDV routing agent in the trace file. The number of packet loss due to an unknown route to the base station node can be counted from the “Free” packets freed by the DSDV routing agent.

However, there is no way to distinguish the no-route loss or the handoff loss among the total lost packets between the heterogeneous interfaces when packets are sent from wired hosts to ad hoc nodes.

The simulation results have shown that when the node movement speed is very slow (speed ≤ 1 m/s), most packet losses (over 80 %) occur when packets are delivered between the heterogeneous interfaces. This observation comes from the behavior of the DSDV routing protocol. DSDV maintains only one route per destination, and is refreshed by a periodical update or a triggered update caused by route change. When the node movement speed is slow (≤ 1m/s), most of the lost packets are freed because a stale routing table is unable to find a route to the base station. The reason is that at lower speed, the update triggered by route change is less frequent than at higher speed. At lower movement speed, the nodes may stay longer in a state where it cannot find an available route to the base station than at higher movement speed. More packets may be dropped at lower movement speed due to the limit of maximum packets buffered per node per destination defined in the DSDV routing protocol (Table 3). When the node movement speed is higher, most of the dropped packets are lost due to broken links caused by high node movement speed. These observations are the same for the simulation scenarios A (Table 6) and B (Table 7).

Table 6: Distribution of Packet Loss (%) in Simulation Scenario A

Maximum speed (m/s)	Packet Drop due to broken links among ad hoc nodes	Packet Drop between the heterogeneous interfaces
1	18	82
10	78	22
20	93	7

Table 7: Distribution of Packet Loss (%) in simulation scenario B

Maximum speed (m/s)	Packet Drop due to broken links among ad hoc nodes	Packet Drop due to no route to BS
1	10	90
10	65	35
20	87	13

Scenario C (packets are sent from ad hoc nodes to ad hoc nodes in separate subnets) is simply a combination of Scenario B (packets are sent from ad hoc nodes to wired nodes) and Scenario A (packets are sent from wired nodes to ad hoc nodes). In this scenario, as shown in Figure 23, when a white node (in subnet1) transmits a data packet to a shaded node (in subnet3), it will not be able to find a route to any of the shaded nodes in its routing table, therefore it will forward the packet to its gateway node G1. In this environment, all the packets are routed through its gateway node towards that of the destination node to reach the destination node.

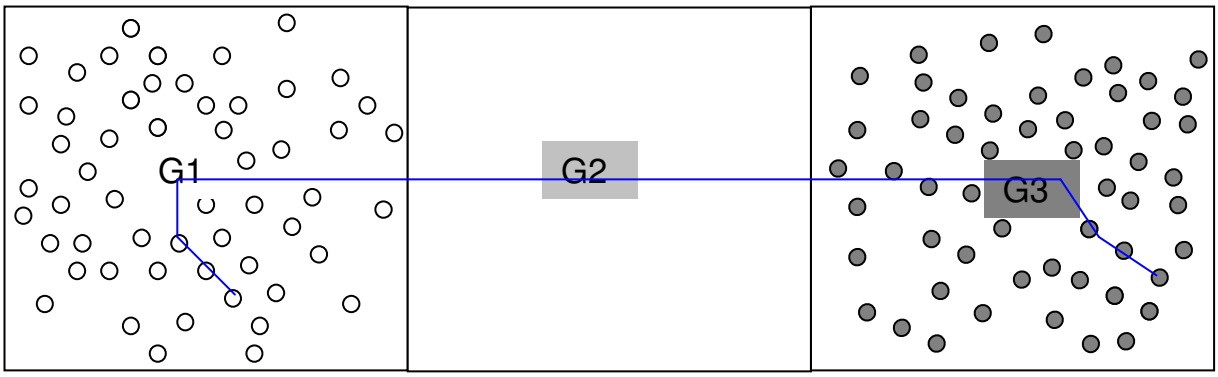

Figure 23: Ad Hoc Nodes Send Packets to other Ad Hoc Nodes in Separate Subnets

Next, in the simulation scenario D (packets are sent from ad hoc nodes to ad hoc nodes between adjacent subnets), more complications are involved as shown in Figure 24. In this environment, some nodes from subnet1 (white nodes) and subnet2 (shaded nodes)

are in communication range of each other. If any of these nodes broadcasts its routing information, this information will also be received by its neighboring nodes that are not in the same subnet. As implemented in DSDV, this information will then be forwarded to its neighboring nodes within this subnet. If a white node transmits a data packet to a shaded node, the white node will first consult its routing table. If it finds a route entry for this destination, it will send the packet along this path (as shown by the dashed line); otherwise it will route the packet to the gateway node in order to reach the destination node (as shown by the solid line).

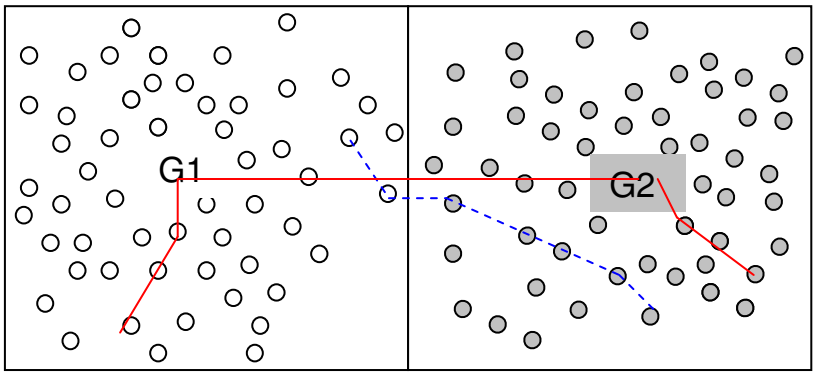

Figure 24: Ad Hoc Nodes Send Packets to other Ad Hoc Nodes in Adjacent Subnets

Table 8: Average Ratio of Packets Received at the Sender's Gateway Node over Packets Received at the Destination Nodes

Maximum speed (m/s)	Simulation Scenario C	Simulation Scenario D
1	140 %	56 %
10	115 %	61 %
20	118 %	51 %

The above discussion is confirmed by analyzing the trace files. The average ratio of packets received at the gateway node over that received at the destination nodes is listed in Table 8. In scenario C, it is found that there are more packets received at the sender's

gateway node G1 than those received at the destination nodes because of the packet loss in the receiver's subnet, indicating that all the packets are routed through the gateway node. While in scenario D, only 50-60 % packets (on average) are routed through the gateway node, showing that the packets received at the gateway node G1 are fewer than those received at the destination node.

This observation can also explain the deterioration of packet delivery ratio with increasing node movement speed in scenario D. At higher node movement speed, the ad hoc node path, which is built by nodes along the border of the adjacent subnets (as shown by the dashed line in Figure 24), is more frequently broken.

5.2.2. DSDV Routing Overhead

Table 9 shows the DSDV routing overhead, defined as the ratio of total DSDV routing messages sent and forwarded over total packets sent.

Table 9: DSDV Routing Overhead for Hierarchical Mobile IP Protocol

Maximum speed (m/s)	Simulation Scenario A	Simulation Scenario B	Simulation Scenario C	Simulation Scenario D
1	5.18	5.28	9.27	18.43
10	10.40	10.35	19.93	24.13
20	10.63	10.62	20.85	24.99

As expected, when the node movement speed increases, the route-change frequency increases in the ad hoc network (shown in Table 4). This results in increased triggered updates, and the subsequent advertisements of new route information in the entire ad hoc network. At higher node movement speed, to prevent fluctuations of routing table entry advertisements, a settling-time table is used for each node. The settling time is calculated

by maintaining a running, weighted average over the most recent updates of the routes, for each destination. This parameter must be selected so that it can indicate how long a route has to remain stable before it is considered as truly stable and advertised to the others. In ns-2.1b6a, advertising of the new route information are limited by the minimum time between triggered updates (defined as 1.0 second), which is used to eliminate the excessive advertisements and insure a truly stable route before it is advertised. This is why increasing the speed from 10 to 20 m/s does not result in increased routing overhead.

For simulation scenarios A and B, the same ad hoc network with the same network topology is involved (Figure 22). The simulation results for both scenarios are obtained with the same node movement patterns and different senders/receivers. Since the routing overhead is only related to the ad hoc network, this explains the identical routing overhead for simulation scenarios A and B.

For simulation scenario C (Figure 23), two ad hoc networks are involved. They are located in subnet1 and subnet3, respectively. Consequently, the routing overhead is roughly doubled in this case compared to the previous scenarios (A and B).

For simulation scenario D (Figure 24), some nodes moving along the border of adjacent subnets are in communication range with each other. If any of these nodes broadcasts its routing information, this information will also be received by its neighborhood nodes that are not in the same subnet. These neighborhood nodes will then forward this information within its subnets. Consequently, the number of routing packets sent greatly increases in this scenario, because there are more destinations to which the nodes must maintain

working routes. This is why the routing overhead is much higher in scenario D than in scenario C.

5.2.3. Control Message Overhead

In this section, the control message overhead consumed on the fixed infrastructure is investigated. For each individual network component, such as gateway nodes (GNs), base station node (BSs), intermediate wired nodes (WNs) between gateway and base station nodes and router nodes (RNs) between gateway nodes, the control messages sent and received are investigated. Reported in Figure 26 (scenario A), Figure 27 (scenario B), Figure 28 (scenario C), Figure 29 (scenario D) are the 95% Confidence Interval values and the average values for the numbers of control message sent at each network component.

Using Hierarchical Mobile IP, a mobile node registers with its home agent (gateway node) each time it changes its care-of address. Each FA (base station node) maintains a location database recording the visiting ad hoc nodes, which register its COA as the FA's address. Upon receiving a registration request from a mobile node, the base station node generates a control message that propagates toward its home agent, i.e., gateway node, which acknowledges the request by sending a message back to the foreign agent.

The control messages sent by the base station nodes (BSs) are used for responding to each MIPT_REG_REQUEST of the ad hoc nodes, and they are sent to the gateway nodes through two intermediate wired nodes (WNs) according to the network topology. Upon receiving a COA of a mobile node, the gateway node (GN) acknowledges this mobile node by sending a MIPT_REG_REPLY message through the intermediate wired nodes

and the current FA (the base station node). So the number of control messages sent by the intermediate wired nodes (WNs) is four times of that sent by the base station nodes.

Table 10: Average Number of Messages Sent by the Base Station Nodes in HFA

Maximum speed (m/s)	1	10	20
Scenario A	26273	25654	25691
Scenario B	26372	25770	25847
Scenario C	50335	50654	49178
Scenario D	54181	51882	52161

Table 11: Average Number of Handoffs Processed in HFA

Maximum speed (m/s)	1	10	20
Scenario A	260	605	792
Scenario B	309	611	848
Scenario C	225	836	1337
Scenario D	670	1486	1962

As explained, the number of control messages sent by the base station nodes is equal to that of MIPT_REG_REQUEST messages received by the base station nodes. It is observed (Table 10) that the total number of MIPT_REG_REQUEST messages received by the base station nodes slightly decreases when the node movement speed increases from 1 to 10 m/s, due to higher node movement speed. At higher node movement speed, the total number of MIPT_REG_REQUEST messages received by the base station nodes becomes stable. In order to keep the binding between the mobile node's HA and its COA, the mobile node keeps sending the MIPT_REG_REQUEST messages at a regular registration interval. If the binding is not renewed within the registration lifetime, the mobile node needs to power up again to set up the new binding information. From the

average number of handoffs processed for each scenario (Table 11), it can be deducted that there are only a maximum of 4% control messages that are used for handling the handoff. Thus, most of the control messages are used to keep the binding between the home agent and mobile host's COA valid.

The control messages, sent by the intermediate router nodes (RNs) between the gateway nodes, are the messages exchanged between the gateway nodes. This happens only when an ad hoc node registers its COA with a base station node not in its home subnet. As depicted in Figure 25, when nodes are moving along the border of the subnets, they may handoff to the base station node of a neighboring subnet. For simulation scenarios A and B, nodes moving in subnet2 can handoff from the base station node in its home domain to S3BS1 or to S1BS4. For simulation scenario C, nodes moving in subnet1 or subnet3 can handoff to S2BS1 or S2BS4. For simulation scenario D, nodes moving in subnet1 can handoff to S2BS1, and nodes moving in subnet2 can handoff to S1BS4 or S3BS1.

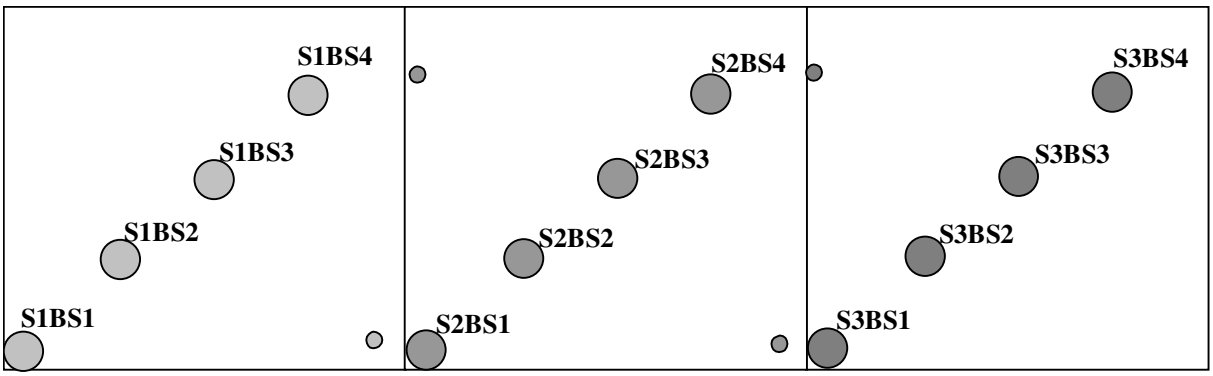

Figure 25: Inter-Domain Handoff

Note that there are the same amount of control messages received at each network component, since a gateway node acknowledges each received message, which causes a large number of control messages in the entire network.

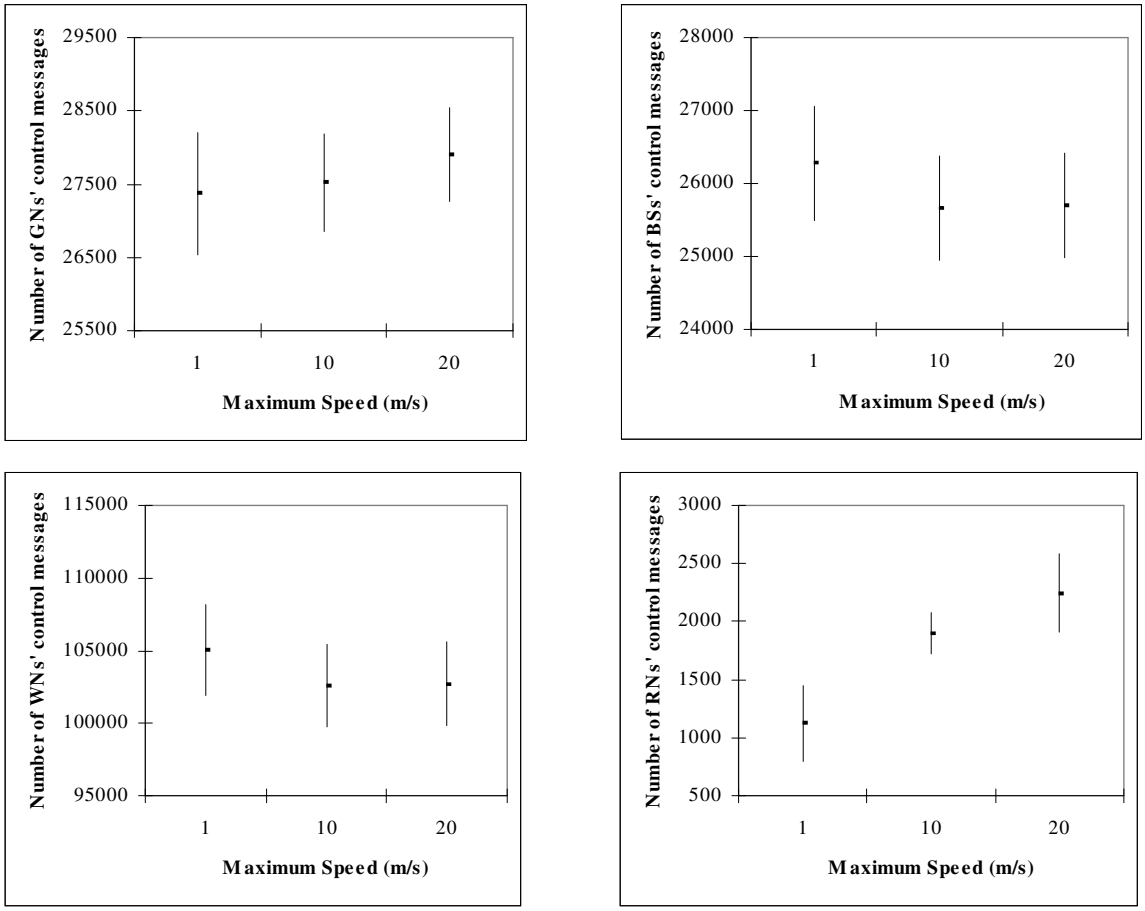

Figure 26: Control Message Detail in Scenario A for HFA

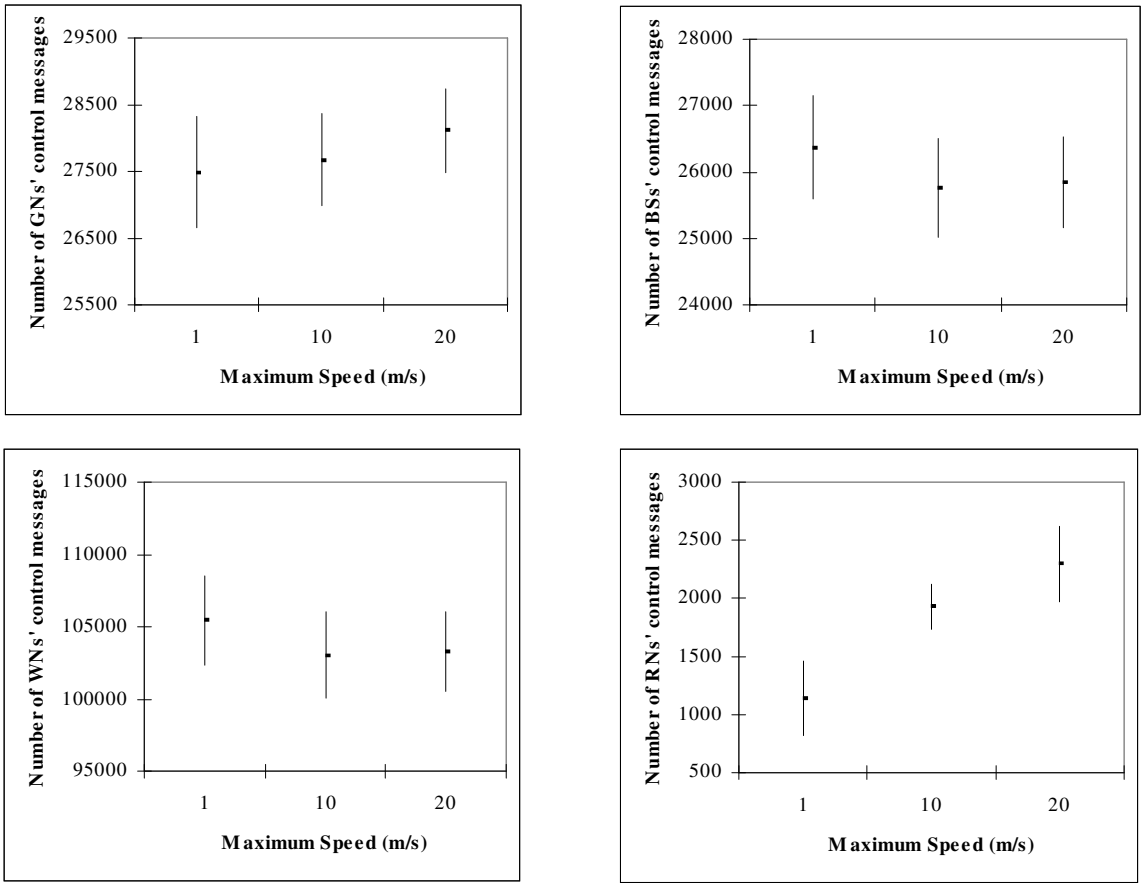

Figure 27: Control Message Detail in Scenario B for HFA

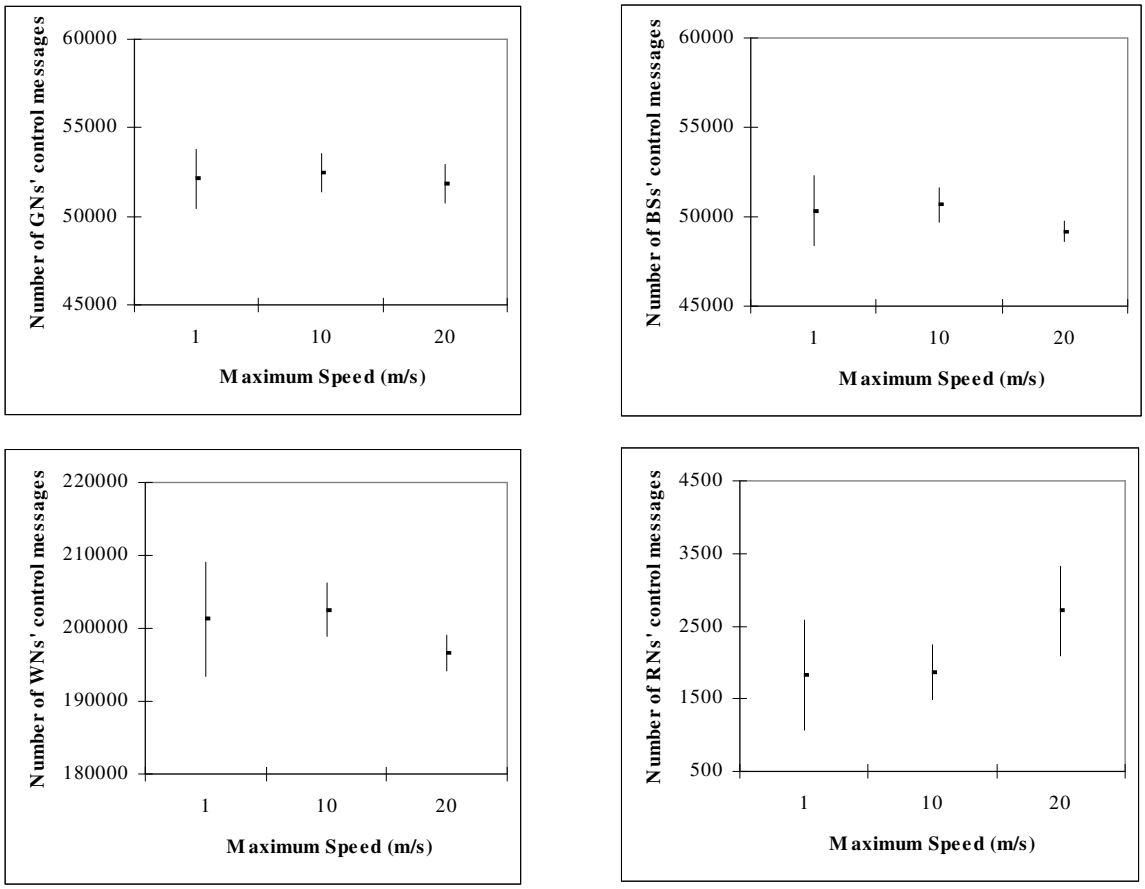

Figure 28: Control Message Detail in Scenario C for HFA

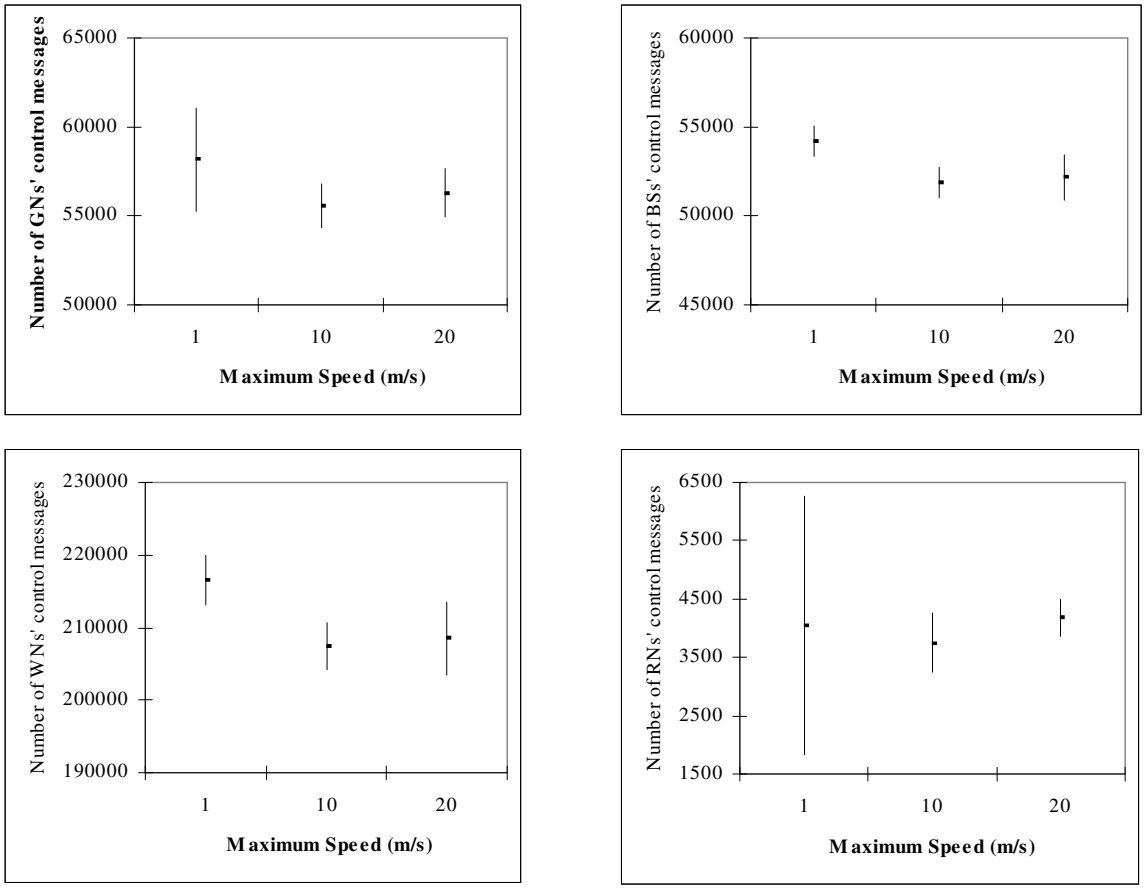

Figure 29: Control Message Detail in Scenario D for HFA

5.2.4. Wandering Nodes Effect

This section investigates the influence of the wandering nodes among the ad hoc network. As described in Section 4.6, wandering nodes are moving within two adjacent subnets rather than one restricted subnet. Similarly, simulations are conducted with four different simulation scenarios as following:

A: wired hosts to ad hoc nodes:

Subnet1 (500mx500m) GN1 (host1)	Subnet2 (500mx500m) GN2 (host2)	Subnet3 (500mx500m) GN3 (host3)

In this scenario, normal ad hoc nodes are moving in the subnet2 (the shaded area), wandering nodes are moving within subnet1 and subnet2.

B: ad hod nodes to wired hosts:

Subnet1 (500mx500m) GN1 (host1)	Subnet2 (500mx500m) GN2 (host2)	Subnet3 (500mx500m) GN3 (host3)

The same as the previous scenario, normal ad hoc nodes are moving in the subnet2 (the shaded area), wandering nodes are moving within subnet1 and subnet2.

C: ad hoc nodes to ad hoc nodes in separate subnets:

Subnet1 (500mx500m) GN1 (host1)	Subnet2 (500mx500m) GN2 (host2)	Subnet3 (500mx500m) GN3 (host3)

In this scenario, two groups of ad hoc nodes are involved. Among the sender nodes, normal ad hoc nodes are moving in subnet1 (the shaded area), wandering nodes are moving within subnet1 and subnet2. For the receiver nodes, normal ad hoc nodes are moving in the subnet3 (the shaded area), wandering nodes are moving within subnet2 and subnet3. In this scenario, there are wandering nodes in subnet2, which is sandwiched between the sender's and receiver's subnets.

D: ad hoc nodes to ad hoc nodes in adjacent subnets.

Subnet1 (500mx500m) GN1 (host1)	Subnet2 (500mx500m) GN2 (host2)	Subnet3 (500mx500m) GN3 (host3)

Similar to scenario C, two groups of ad hoc nodes are involved here. Among the sender nodes, normal ad hoc nodes are moving in subnet1 (the shaded area), while wandering nodes are moving within subnet1 and subnet2. For the receiver nodes, normal ad hoc nodes are moving in subnet2 (the shaded area), with wandering nodes moving within subnet1 and subnet2. In this scenario, wandering nodes move from subnet1 to subnet2 and vice versa.

The simulation results (Table 12) are obtained with the above four simulation scenarios, in the presence of 10 wandering nodes for each group of 50 ad hoc nodes. For the wandering nodes, the home gateway node remains their home agent, and the base station node in the visiting subnet acts as a foreign agent. This allows the wandering nodes to continue communication as if they were still connected to their home subnet.

Table 12: Influence of Wandering Node on Packet Delivery Ratio (%) for HFA

Maximum speed (m/s)		Scenario A	Scenario B	Scenario C	Scenario D
1	no wandering nodes	73.74	70.67	53.58	63.00
	20% wandering nodes	*79.40*	*76.69*	*60.04*	*76.82*
10	no wandering nodes	85.05	83.33	75.30	33.16
	20% wandering nodes	*81.36*	*80.64*	*48.81*	*48.01*
20	no wandering nodes	83.58	83.79	72.28	32.02
	20% wandering nodes	*73.59*	*74.50*	*39.05*	*41.00*

Table 13: Influence of Wandering Node on DSDV Routing Overhead for HFA

Maximum speed (m/s)		Scenario A	Scenario B	Scenario C	Scenario D
1	no wandering nodes	5.18	5.28	9.27	18.43
	20% wandering nodes	*3.52*	*3.48*	*7.79*	*21.11*
10	no wandering nodes	10.40	10.35	19.93	24.13
	20% wandering nodes	*6.59*	*6.71*	*14.40*	*25.35*
20	no wandering nodes	10.63	10.62	20.85	24.99
	20% wandering nodes	*7.55*	*7.63*	*16.44*	*25.21*

For simulation scenarios A and B, in the presence of wandering nodes, the path to the gateway node is no longer the only way to route the packet to a destination node. Packets could now be routed through the wandering nodes to the adjacent subnet to reach a destination node (shown as solid line in Figure 30). For this to happen, this path must exist, otherwise the packets are directed to the gateway node to reach the destination node (shown as dashed line in Figure 30). The simulation results show that the packet delivery ratio increases in the presence of the wandering nodes at lower node movement speed (maximum speed =1 m/s); while at higher node movement speed (maximum speed > 1 m/s), the packet delivery performance deteriorates. This performance deterioration is

caused by increased link failure along the ad hoc node path through the adjacent subnets at higher node movement speed. This discussion is in agreement with the distribution of packet loss. It is observed that more packets are lost due to the link failure among the ad hoc nodes when the node movement speed increases (Table 14, Table 15). Besides, the presence of the wandering nodes mostly increases the packet loss due to link failure.

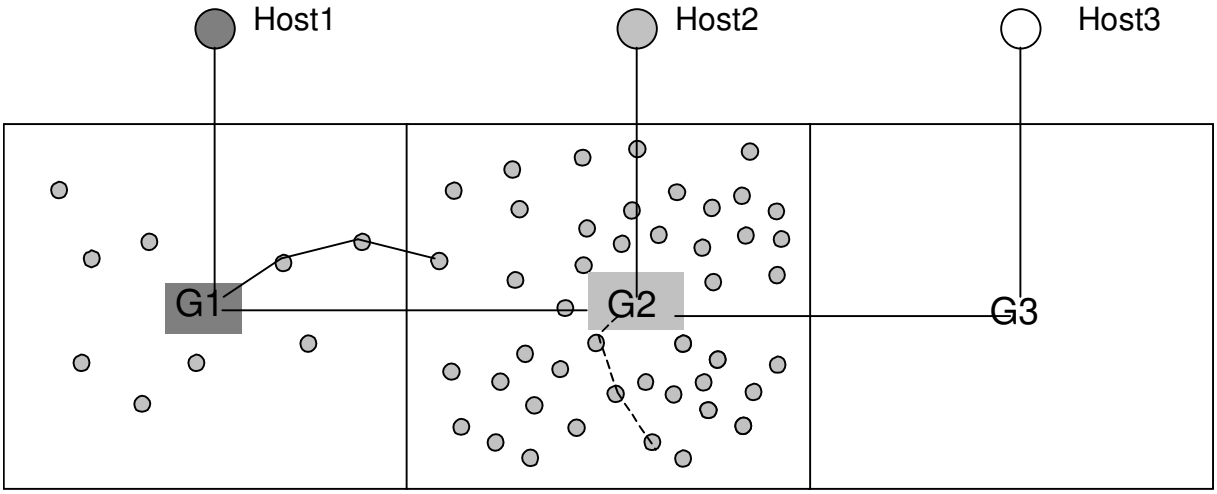

Figure 30: Packet Delivery Through Heterogeneous Interfaces (Scenario A and B) in the Presence of Wandering Nodes

Table 14: Fraction of Packet Loss (%) Due to Link Failure as a Function of Node Movement Speed for Scenario A

Number of wandering nodes	0	10
maximum speed = 1 m/s	18	27
maximum speed = 10 m/s	78	90
maximum speed = 20 m/s	93	95

Table 15: Fraction of Packet Loss (%) Due to Link Failure as a Function of Node Movement Speed for Scenario B

Number of wandering nodes	0	10
maximum speed = 1 m/s	10	16
maximum speed = 10 m/s	65	75
maximum speed = 20 m/s	87	84

For simulation scenario C, the situation is similar to that of scenarios A and B. In the presence of wandering nodes, the sender can route the packets either to the gateway node (shown as solid line in Figure 31), or through the wandering nodes to reach the destination node (shown as dashed line in Figure 31). For the same reason given above, packet delivery performance improves at lower node movement speed (s = 1 m/s), but deteriorates when node movement speed increases.

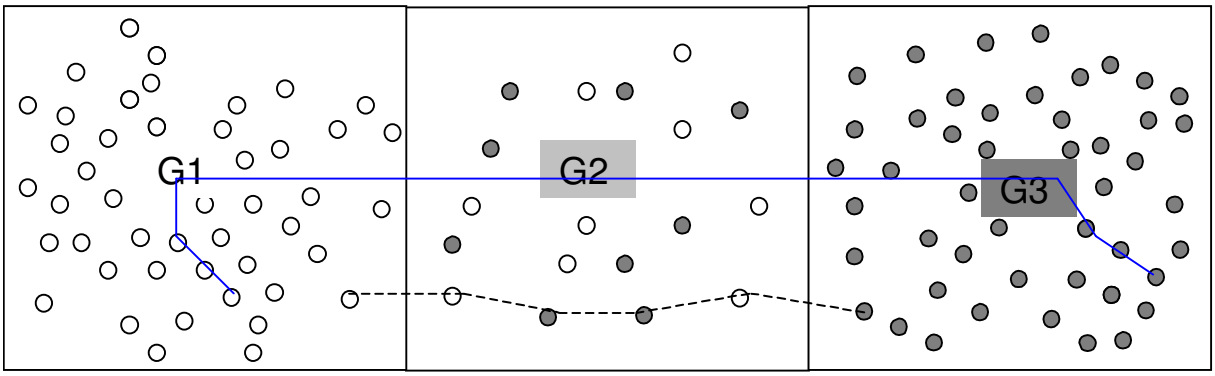

Figure 31: Packet Delivery between Ad Hoc Nodes through Separate Subnets in the Presence of Wandering Nodes

For simulation scenario D in the presence of wandering nodes, when packets are sent from ad hoc nodes to ad hoc nodes in adjacent subnets, packet delivery performance improves regardless of node movement speed. In this environment, some nodes have wandered into the adjacent subnet, participating in the neighbor's ad hoc network.

The result can be explained from the distribution of mobile nodes in the simulation area by the random waypoint model [36]. This model describes the movement behavior of a mobile network node in a two-dimensional system area. In this model, a node randomly chooses a destination point in the area and moves with constant speed to this point; after waiting a certain pause time, it chooses a new destination, moves to this destination, and so on. This description is the same as our node movement model used for all the

simulations, as given in Section 4.6. As shown in Figure 32 [36], this mobility model does not result in a uniform node distribution, with higher node density in the middle of the area and lower node density at the edges or borders of the simulation area. The reason for this behavior is that nodes located at the edges or borders of the simulation area are very likely to move back toward the middle of the area.

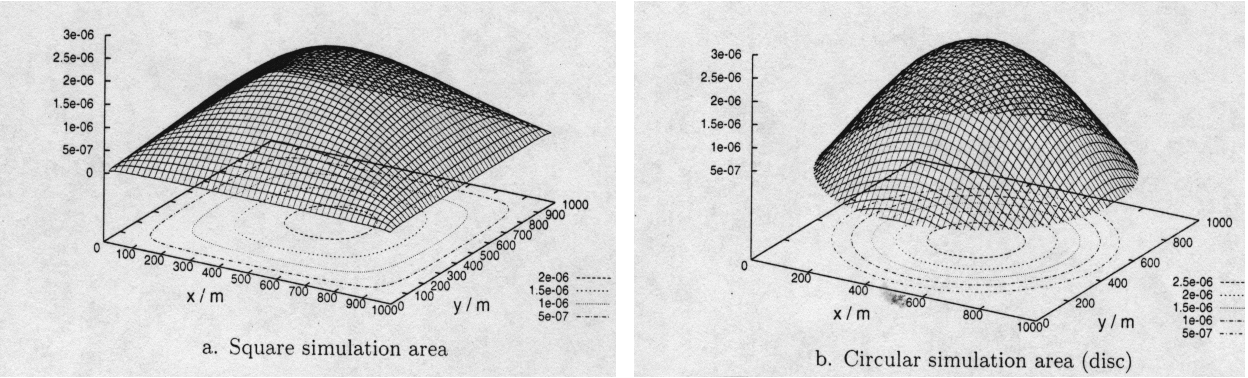

Figure 32: Spatial node distribution resulting from the random waypoint mobility model (simulation results)

With the presence of wandering nodes, the node density along the border of the adjacent subnets should be significantly increased by the node movements across the adjacent subnets. As discussed previously, the mobile nodes located along the border of the adjacent subnets are beneficial for building up paths between the subnets and exchanging routing information between the adjacent subnets. As implemented in the DSDV routing protocol, routing information exchanged between the neighborhood nodes will then spread through the two ad hoc networks. This is the reason that this scenario is the only one to show the DSDV routing overhead to increase, because more destinations are listed in the routing table for each node. If a white node transmits a data packet to a shaded node, it first consults its routing table. If a route entry for this destination is found, it will

then send the packet along this path (as shown by the dashed line in Figure 33); otherwise it will route the packet to the gateway node to reach the destination node (as shown by the solid line in Figure 33).

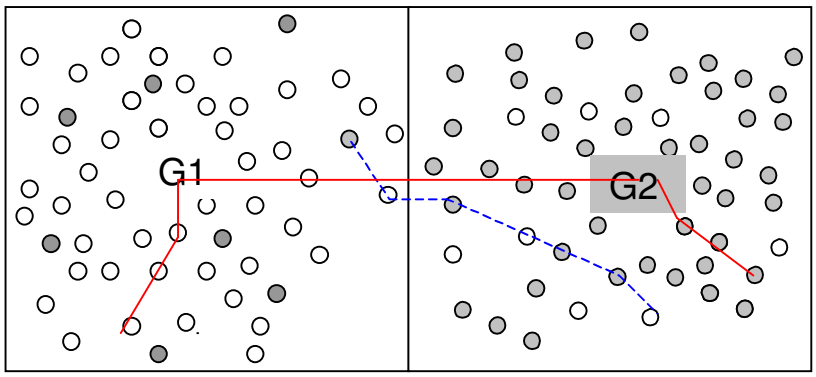

Figure 33: Packet Delivery between Ad Hoc Nodes through Adjacent Subnets in the Presence of Wandering Nodes

For all other simulation scenarios (A, B and C), the DSDV routing overhead decreases in the presence of wandering nodes, because the presence of the wandering nodes disperses the ad hoc nodes in the subnet. Some of the wandering nodes may not be reachable by the rest of the nodes in its home subnet, as shown in Table 4 which summarizes the scenario characterization. For each ad hoc node, the routing table may have fewer entries for reachable destinations, which results in reduced overhead. When the number of the wandering nodes increases, this observation is still valid (Table 16). However, a high dispersion will not favor the packet delivery performance (Table 17), as it leads to a high number of unreachable destinations among the ad hoc network. The further investigations on increasing number of wandering nodes are only conducted on scenario A and B, which show the same results. No further study is conducted on scenario C, since similar results are expected.

Table 16: Routing Overhead as a Function of Wandering Node Number (maximum speed =1 m/s)

Number of wandering nodes	0	10	17	33	50
Scenario A	5.18	3.52	2.96	2.52	2.41
Scenario B	5.28	3.48	3.00	2.46	2.38

Table 17: Packet Delivery Ratio (%) as a Function of Wandering Node Number (maximum speed =1 m/s)

Number of wandering nodes	0	10	17	33	50
Scenario A	73.74	79.40	71.29	71.49	67.03
Scenario B	70.67	76.69	68.56	68.95	63.02

For all the simulation scenarios, the presence of wandering nodes causes the control message overhead to increase at the gateway node. This contributes to the increased location updating of the wandering nodes over two subnets, consequently increasing the control message overhead at the router nodes. The situations at the base station nodes are different. Here, the number of control messages sent by a base station node depends on the total number of MIPT_REG_REQUEST messages received by the base station nodes. As expected, the presence of wandering nodes causes higher number of handoffs, and the packet delivery performance inside the ad hoc network itself deteriorates with increasing node movement speed. Therefore, at higher node movement speed with the presence of wandering nodes, fewer packets can arrive at the base station node caused by increased link failure along the longer path, consequently less control messages are sent by the base station nodes to reply to the MIPT_REG_REQUEST messages of the ad hoc nodes.

Table 18: Comparing Control Message Overhead in Simulation Scenario A for HFA

Maximum speed (m/s)		Gateway Nodes	Base Station Nodes	Wired Nodes	Router Nodes
1	No wandering nodes	27372	26273	105037	1127
	20% wandering nodes	32505	27111	108385	5424
	Change	+ 19%	+ 3%	+ 3%	+ 381%
10	No wandering nodes	27521	25654	102562	1895
	20% wandering nodes	32642	26081	104266	6591
	Change	+ 19%	+ 2%	+ 2%	+ 248%
20	No wandering nodes	27901	25691	102690	2247
	20% wandering nodes	31113	24660	98575	6486
	Change	+ 12%	- 4%	- 4%	+ 189%

Table 19: Comparing Control Message Overhead in Simulation Scenario B for HFA

Maximum speed (m/s)		Gateway Nodes	Base Station Nodes	Wired Nodes	Router Nodes
1	No wandering nodes	27482	26372	105432	1139
	20% wandering nodes	32569	27155	108562	5443
	Change	+ 19%	+ 3%	+ 3%	+ 378%
10	no wandering nodes	27672	25770	103027	1929
	20% wandering nodes	32813	26173	104633	6670
	Change	+ 19%	+ 2%	+ 2%	+ 246%
20	no wandering nodes	28110	25847	103312	2300
	20% wandering nodes	31238	24736	98872	6537
	Change	+ 11%	- 4%	- 4%	+ 184%

Table 20: Comparing Control Message Overhead in Simulation Scenario C for HFA

Maximum speed (m/s)		Gateway Nodes	Base Station Nodes	Wired Nodes	Router Nodes
1	no wandering nodes	52112	50335	201240	1828
	20% wandering nodes	61873	50556	202123	11367
	Change	+ 19%	+ 0.4%	+ 0.4%	+ 522%
10	no wandering nodes	52459	50654	202505	1860
	20% wandering nodes	62949	51158	204511	11852
	Change	+ 20%	+ 1%	+ 1%	+ 537%
20	no wandering nodes	51821	49178	196575	2709
	20% wandering nodes	59905	49333	197197	10638
	Change	+ 16%	+ 0.3%	+ 0.3%	+ 293%

Table 21: Comparing Control Message Overhead in Simulation Scenario D for HFA

Maximum speed (m/s)		Gateway Nodes	Base Station Nodes	Wired Nodes	Router Nodes
1	no wandering nodes	58187	54181	216625	4056
	20% wandering nodes	65612	53748	214885	11917
	Change	+ 13%	- 0.1%	- 0.1%	+ 194%
10	no wandering nodes	55578	51882	207415	3752
	20% wandering nodes	68223	53696	214653	14590
	Change	+ 23%	+ 3%	+ 3%	+ 289%
20	no wandering nodes	56282	52161	208513	4183
	20% wandering nodes	63910	50721	202757	13251
	Change	+ 14%	- 3%	- 3%	+ 217%

5.3. HAWAII Simulation Results

For HAWAII, simulations were conducted using the same movement patterns and connection patterns as for Hierarchical Mobile IP. Similarly, four different simulation scenarios were investigated:

A: wired hosts to ad hoc nodes;

B: ad hod nodes to wired hosts;

C: ad hoc nodes to ad hoc nodes between separated subnets;

D: ad hoc nodes to ad hoc nodes between adjacent subnets.

For each scenario, three different maximum node movement speeds (1 m/s, 10 m/s and 20 m/s) were considered.

5.3.1. Packet Delivery Ratio

In HAWAII, two different path setup schemes, Multiple Stream Forwarding (MSF) and Unicast Non-Forwarding (UNF), were investigated. The simulation results are presented for each scheme. The average packet delivery ratios as a function of node movement speed for all simulation scenarios are given in Table 22 for HAWAII MSF and in Table 23 for HAWAII UNF.

Table 22: Packet Delivery Ratios (%) for HAWAII MSF

Maximum speed (m/s)	Simulation Scenario A	Simulation Scenario B	Simulation Scenario C	Simulation Scenario D
1	70.63	*37.51*	53.08	62.42
10	74.30	*42.41*	66.47	31.76
20	72.89	*42.49*	65.89	30.43

Table 23: Packet Delivery Ratios (%) for HAWAII UNF

Maximum speed (m/s)	Simulation Scenario A	Simulation Scenario B	Simulation Scenario C	Simulation Scenario D
1	71.97	*69.51*	53.23	62.11
10	75.66	*84.17*	65.65	30.52
20	70.38	*84.23*	61.90	28.34

It can be seen that the results for MSF and UNF are very similar, except for scenario B, which is the only case in which the destination nodes are the wired hosts. This difference is a direct consequence of the design of the MSF forwarding scheme, which is used uniquely for handling the handoff of mobile hosts. During a handoff handled by MSF, if the destination node is not a mobile node, the path setup message is discarded at the old base station node. So, the mobile host will not be acknowledged for setting up the path with the new base station, it then should send power up message in order to establish the path with the new base station. Therefore, all the packets are lost before the path is established. Consequently, the MSF is not suitable for delivering packets to wired destination nodes. In this scenario (scenario B), packets are dropped during the handoff, showing lower packet delivery ratio. However, MSF performs as well as UNF when the destination nodes are mobile hosts, as shown in scenarios A, C and D. Moreover, at higher node movement speed, the packet delivery ratio of MSF is slightly higher than that of UNF due to its forwarding scheme. In MSF, during handoff, packets are first buffered at the old base station, and forwarded to the new base station only after the new path is established. However, in UNF, there is no buffer at the old base station, therefore packets can be lost before the new path is established.

As in HFA, for simulation scenarios A, B and C, the packet delivery ratio increases when node movement speed increases from 1 to 10 m/s, but slightly decreases when the speed increases from 10 to 20 m/s. For simulation scenario D, the packet delivery ratio deteriorates when node movement speed increases. As explained previously, this deterioration is caused by an increasing number of link failures among the ad hoc node path (shown by the dashed line in Figure 24), which is built by the nodes moving along the border of the adjacent subnets.

5.3.2. DSDV Routing Overhead

The DSDV routing overhead results (defined as the ratio of total DSDV routing messages sent and forwarded over total packets sent) are given in Table 24 for HAWAII MSF, and in Table 25 for HAWAII UNF, respectively. As expected, these results are identical, because the routing overhead is only related to the ad hoc routing protocol DSDV.

Table 24: DSDV Routing Overhead for HAWAII MSF

Maximum speed (m/s)	Simulation Scenario A	Simulation Scenario B	Simulation Scenario C	Simulation Scenario D
1	5.22	5.27	9.58	18.37
10	10.39	10.38	19.97	24.17
20	10.63	10.68	20.87	24.99

Table 25: DSDV Routing Overhead for HAWAII UNF

Maximum speed (m/s)	Simulation Scenario A	Simulation Scenario B	Simulation Scenario C	Simulation Scenario D
1	5.00	5.45	9.74	18.57
10	10.35	10.46	19.97	24.11
20	10.60	10.66	20.82	24.97

The variation of the routing overhead relative to the node movement speed in each scenario is the same as that observed in HFA. As explained previously, the routing overhead is only related to the ad hoc network and the routing protocol, and no micromobility protocol is involved.

5.3.3. Control Message Overhead

In HAWAII, the control message overhead on the fixed infrastructure is investigated for both path setup schemes: MSF and UNF. For each individual network component, such as gateway nodes (GN), base station nodes (BS), intermediate wired nodes (WN) between gateway and base station nodes and router nodes (RN) between gateway nodes, the control messages sent and received are investigated. Reported in Figure 34 (scenario A), Figure 35 (scenario B), Figure 36 (scenario C), Figure 37 (scenario D) are the 95% Confidence Interval values and the average values for the numbers of control messages sent at each network component.

In HAWAII, control messages sent by the gateway nodes (GNs) and the base station nodes (BSs) are mostly used for path setup during the handoff. Each handoff is always handled by two base station nodes (old and new base station nodes), but the gateway node is only involved for inter-domain handoff. Besides the power up of mobile nodes, no COA update registration to the gateway node is necessary when the mobile node remains inside its home domain.

The first observation of the results is that the number of control messages sent is much lower for the UNF scheme than for the MSF scheme. Another important observation is that the number of control messages sent and received at the router nodes (RNs) are not the same for both path set up schemes (Table 26 and Table 27).

Table 26: Control Messages Sent and Received at the Router Nodes for HAWAII MSF

Maximum Speed (m/s)		Scenario A	Scenario B	Scenario C	Scenario D
1	**sent**	1161	1165	956	2606
	received	2321	2328	1911	5202
10	**sent**	3073	3280	3281	5707
	received	6136	6373	6547	11386
20	**sent**	2847	2958	2861	5457
	received	5677	5898	5688	10875

Table 27: Control Messages Sent and Received at the Router Nodes for HAWAII UNF

Maximum Speed (m/s)		Scenario A	Scenario B	Scenario C	Scenario D
1	**sent**	2	2	3	3
	received	1161	1163	956	2615
10	**sent**	10	10	15	27
	received	3090	3281	3276	5695
20	**sent**	13	15	25	36
	received	2865	2939	2876.58	5521

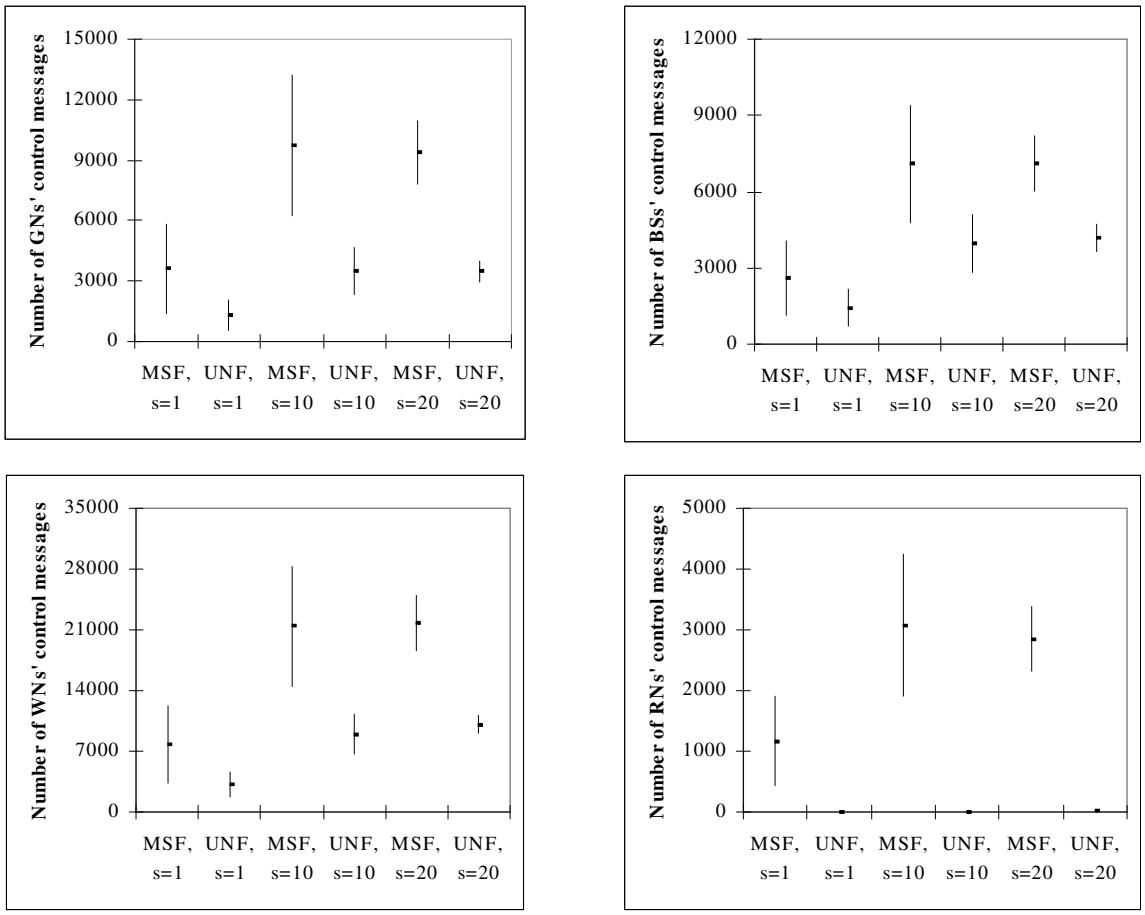

Figure 34: Comparison of Control Message Overhead for HAWAII MSF and UNF in Scenario A

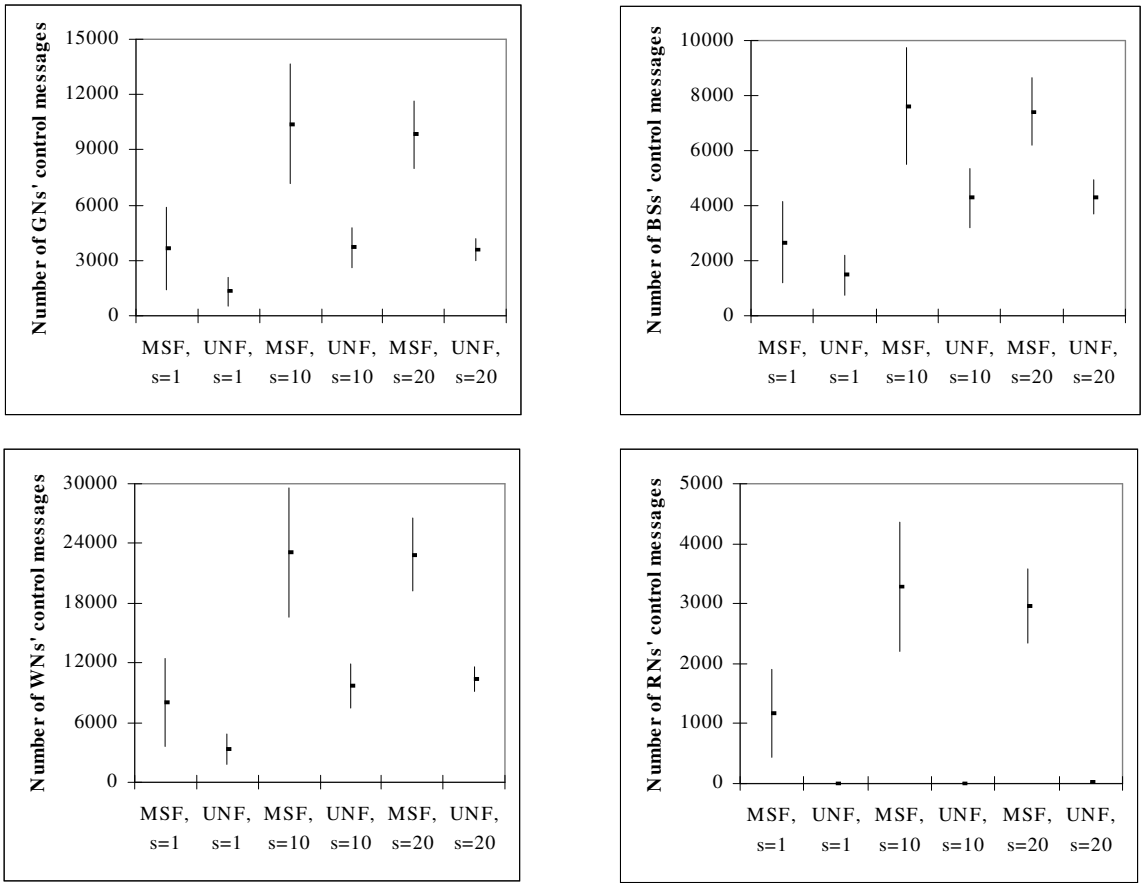

Figure 35: Comparison of Control Message Overhead for HAWAII MSF and UNF in Scenario B

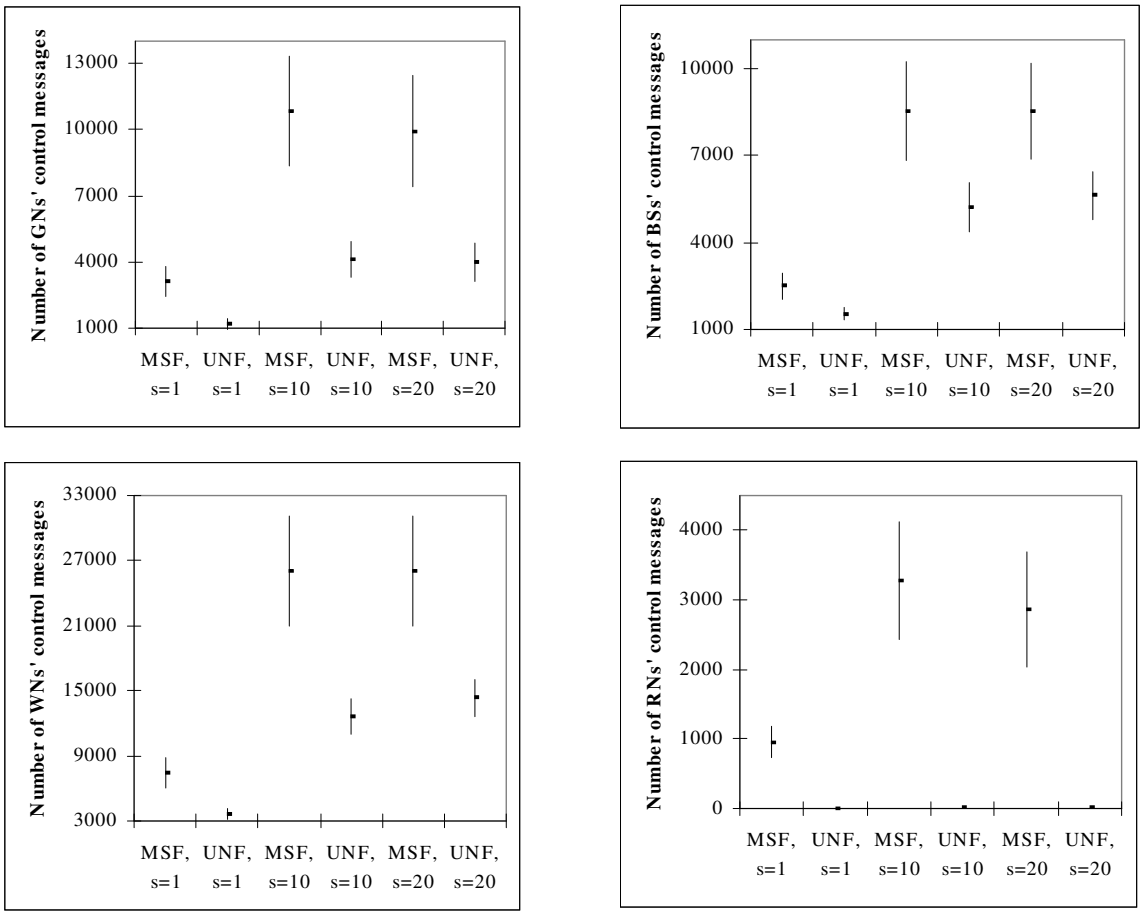

Figure 36: Comparison of Control Message Overhead for HAWAII MSF and UNF in scenario C

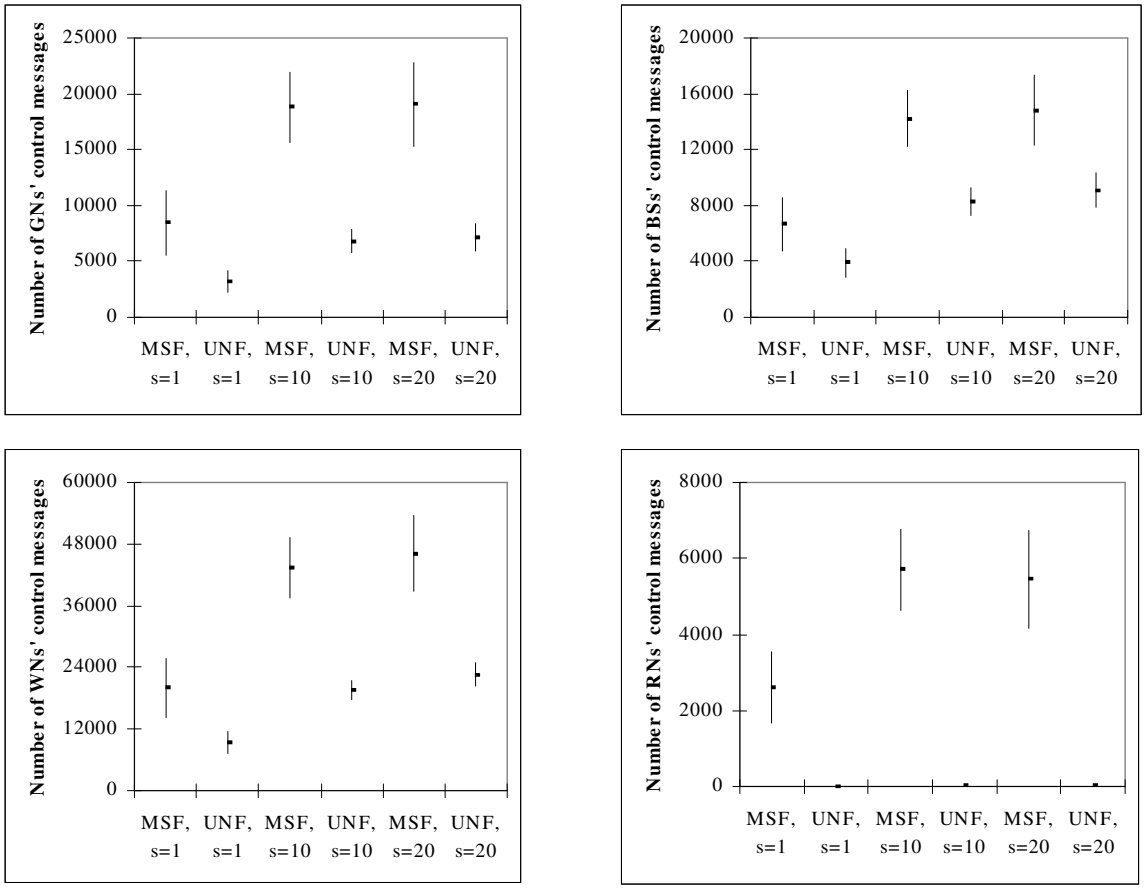

Figure 37: Comparison of Control Message Overhead for HAWAII MSF and UNF in scenario D

These observations seem surprising, since the two path setup schemes are quite similar, and differ only in the order of path update during handoff. When a base station node receives a MIPT_REG_REQUEST from a mobile host with a different previous COA, it generates a HAWAII_Update message. In UNF, the new base station initiates the path setup procedure immediately, the new path is then updated hop by hop by the HAWAIIRouters to the old base station, which acknowledges back to the new base station by a HAWAII_Ack message. After receiving the HAWAII_Ack message, the new base station node sends a MIPT_REG_REPLY to the mobile node, acknowledging the successful handoff with a new COA. In MSF, the new base station first forwards the HAWAII_Update message hop by hop to the old base station, and it is the old base station who initiates the path setup procedure hop by hop to the new base station. After the path setup is done on the new base station node, it sends a MIPT_REG_REPLY to the mobile node, acknowledging the successful handoff with a new COA.

Since the most important difference between the two path setup schemes is the control message overhead at the router nodes (RNs) between the gateway nodes, it indicates that the two schemes handle the inter-domain handoff differently. As explained in the case of HFA (Section 5.2.3), the control messages sent by the RNs are the messages exchanged between the gateway nodes. This happens only when an ad hoc node handoffs to a base station node that is not in its home subnet (as depicted in Figure 25).

To confirm that the difference of control message overhead between these two path setup schemes comes solely from the inter-domain handoff, simulations without any inter-domain handoff involved are required. For this purpose, a series of simulations were performed using only one subnet with the same network topology described in Section

4.1. Only scenario A was investigated to observe the handoff effect, and the same node movement patterns and connection patterns were used. But, the destination node is the only wired host in the subnet, not the three wired hosts of three subnets. In this environment, all handoffs are intra-domain. Since only one subnet exists, no inter-domain handoff is involved.

Table 28: HAWAII UNF and MSF Results of One Subnet for Scenario A

Maximum Speed (m/s)		Delivery Ratio (%)	Routing Overhead	GN' Control Msg	BSs' Control Msg	WNs' Control Msg
1	**UNF**	69.63	4.38	192	339	1094
	MSF	69.57	4.54	195	379	1167
10	**UNF**	86.56	9.61	513	1027	3318
	MSF	86.84	9.49	536	1077	3447
20	**UNF**	82.78	9.74	600	1371	4324
	MSF	82.52	9.72	605	1417	4445

The results of this series of simulations show that the packet delivery ratio as well as the control message overhead at each network component are the same for HAWAII UNF and MSF (Table 28), which confirms that UNF and MSF handle the intra-domain mobility equally. The difference in control message overhead is then only attributed to the inter-domain handoff.

By carefully studying the implementation details of each path setup scheme in CIMS, it is found that neither UNF nor MSF can update the new path during the inter-domain handoff between two different domains, as no functions were implemented for the inter-domain handoff in CIMS. This is the reason for the higher packet delivery ratio when no inter-domain handoff is involved (Figure 38). This is especially the case for higher node movement speed when a higher number of handoffs occur.

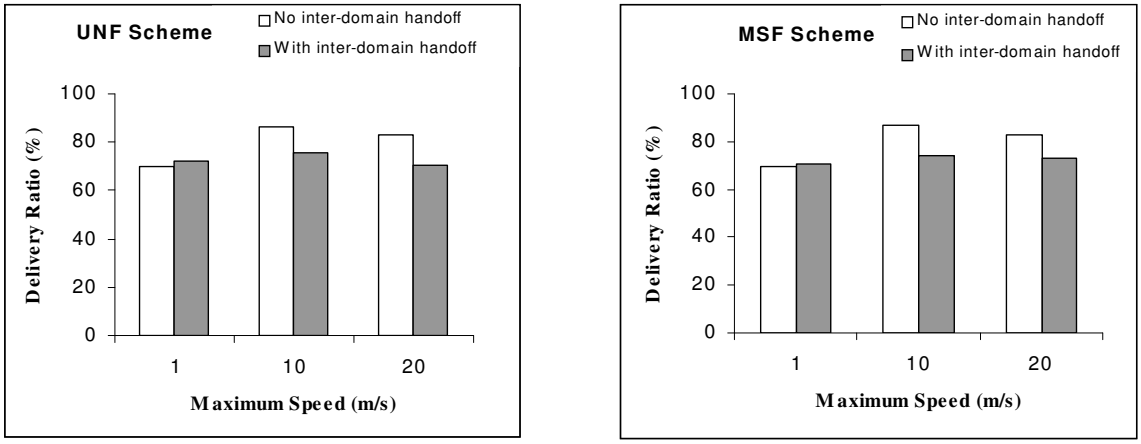

Figure 38: Comparison of Packet Delivery Performance with and without Inter-Domain Handoff for Simulation Scenario A

The cause of the failure to establish path setup during inter-domain handoff is the router node between the gateway nodes. Recall that in Section 4.1, the intermediate router nodes (RNs) between the subnets are ordinary wired nodes, which do not belong to any subnet. Therefore, a RN is not a HAWAIIRouter of any particular subnet. However, in the UNF or MSF scheme, the path setup messages are processed by the new base station node, the old base station node and the related wired nodes (WNs) connecting them. Each of them is a HAWAIIRouter, which updates its forwarding entry according to the path setup message. When path setup proceeds in two different domains, the router node (RN) between the gateway nodes becomes the crossover router. Since the router node cannot participate in the path setup as a HAWAIIRouter, it discards all the path setup messages. In this case, the old base station node still acts as the foreign agent (FA) for the mobile node, and the packets are continuously forwarded to the current domain, where the mobile node remains. In case the timestamp in its FA expires for the mobile host, it registers with the base station node by the power up procedure.

For MSF, the messages sent by the RNs are the HAWAII_Update messages forwarded from the new base station node to the old base station node. Upon receiving a HAWAII_Update message, the old base station node sends the path setup message hop by hop to the new base station, which is discarded at the router node. This explains why the number of control messages received at the RNs is double of that sent by the RNs (Table 26). For UNF, the few messages sent by the RNs are the power up messages. If a mobile node initiates a power up message through a base station node of the neighboring subnet, the gateway node of this neighboring subnet will send the location information to the node's home agent (its home gateway node) through the router node. The messages received at the RNs are the path setup messages, which are then discarded.

In order to investigate the effect of inter-domain handoff, the number and type of handoffs during each simulation is investigated for scenarios A (Table 29) and B (Table 30). The results for HAWAII UNF demonstrate that about 30-40% handoffs are inter-domain handoffs, however only 10-20% of overall handoffs are successfully processed and acknowledged, indicating that most of the handoff messages are unnecessary. The results obtained with one subnet, where the packet delivery ratio is higher when no inter-domain handoff is involved, clearly shows that the inter-domain handoff is not necessary for the normal node movement within one subnet.

The first explanation for the unnecessary handoffs is the behavior of the mobile node. Upon receiving a MIPT_AD with a different COA, the mobile node sends a MIPT_REG_REQUEST message immediately to the base station node. Note that before the handoff is acknowledged, the mobile node will continuously send a MIPT_REG_REQUEST message for each MIPT_AD received with a different COA.

The immediate response of a mobile node to the agent advertisement with a different COA produces excessive handoff messages, which in turn initiates the numerous unnecessary path setup procedures. The second explanation for the unnecessary handoffs is the overlapping area. As in wide-area wireless networks where cell coverage usually overlaps (in CIMS, the overlapping area is defined as 30 m), a mobile node can be connected to either of two base station nodes in this overlapping area. While moving in the overlapping area, the mobile node can needlessly handoff from one to another until it loses the connection with either of them. This is why only 10-20% of handoffs are successfully processed and acknowledged. The above observations are also true for the HAWAII MSF scheme.

Table 29: Average Number of Handoffs for Scenario A for HAWAII UNF

Maximum speed (m/s)	Average number of handoffs processed	Ratio (%) of inter-domain handoffs	Ratio (%) of successful handoffs
1	1246	43	12
10	3479	32	13
20	3434	42	20

Table 30: Average Number of Handoffs for Scenario B for HAWAII MSF

Maximum speed (m/s)	Average number of handoffs processed	Ratio (%) of inter-domain handoffs	Ratio (%) of successful handoffs
1	1278	42	14
10	3706	30	14
20	3562	40	21

5.3.4. Wandering Nodes Effect

This section investigates the influence of the wandering nodes among the ad hoc network. The same simulation scenarios as described in Section 5.2.4 for HFA are used. Simulations are conducted for two path setup schemes: MSF and UNF. The influence of wandering node on packet delivery performance is given in Table 31 for HAWAII MSF and in Table 32 for HAWAII UNF.

Table 31: Effect of Wandering Node on Packet Delivery Ratio (%) for HAWAII MSF

Maximum speed (m/s)		Scenario A	Scenario B	Scenario C	Scenario D
1	no wandering nodes	70.63	*37.51*	53.08	62.42
	20% wandering nodes	*70.38*	*41.09*	*57.30*	*74.33*
10	no wandering nodes	74.30	*42.41*	66.47	31.76
	20% wandering nodes	*66.64*	*41.96*	*42.59*	*47.05*
20	no wandering nodes	72.89	*42.48*	65.89	30.43
	20% wandering nodes	*58.97*	*37.43*	*31.60*	*40.09*

Table 32: Effect of Wandering Node on Packet Delivery Ratio (%) for HAWAII UNF

Maximum speed (m/s)		Scenario A	Scenario B	Scenario C	Scenario D
1	no wandering nodes	71.97	69.51	53.23	62.11
	20% wandering nodes	*72.99*	*76.79*	*57.32*	*76.07*
10	no wandering nodes	75.66	84.17	65.65	30.52
	20% wandering nodes	*69.45*	*80.58*	*38.77*	*44.78*
20	no wandering nodes	70.38	84.23	61.90	28.34
	20% wandering nodes	*59.95*	*74.37*	*29.27*	*37.50*

The results are similar for MSF and UNF schemes. For simulation scenarios A, B and C, packet delivery performance improves at lower node movement speed (s = 1 m/s), but deteriorates when node movement speed increases. This deterioration is not related to the failure of handling the inter-domain handoff, since the presence of 20 % wandering nodes does not increase the ratio of inter-domain handoff, even if the total number of handoffs increases (see Table 33 and Table 34). As in HFA, this deterioration is attributed to the increased link failure along the ad hoc node path, which is made up of wandering nodes moving across adjacent subnets. For simulation scenario D, the presence of wandering nodes improves packet delivery performance regardless of node movement speed. This improvement comes from spreading routing information through two ad hoc networks with the help of wandering nodes in each other's network.

Table 33: Average Number of Handoffs in Scenario A for HAWAII UNF

Maximum speed (m/s)		Average number of total handoffs	Ratio (%) of inter-domain handoffs	Ratio (%) of successful handoffs
1	no wandering nodes	1246	43	12
	20% wandering nodes	*2921*	*23*	*5*
10	no wandering nodes	3479	32	13
	20% wandering nodes	*5953*	*30*	*8*
20	no wandering nodes	3434	42	20
	20% wandering nodes	*6730*	*25*	*10*

Table 34: Average Number of Handoffs in Scenario B for HAWAII UNF

Maximum speed (m/s)		Average number of total handoffs	Ratio (%) of inter-domain handoffs	Ratio (%) of successful handoffs
1	no wandering nodes	1278	42	14
	20% wandering nodes	*2937*	*24*	*5*
10	no wandering nodes	3706	30	14
	20% wandering nodes	*6112*	*29*	*7*
20	no wandering nodes	3562	40	21
	20% wandering nodes	*6785*	*25*	*10*

Table 35: Effect of Wandering Node on DSDV Routing Overhead for HAWAII MSF

Maximum speed (m/s)		**Scenario A**	**Scenario B**	**Scenario C**	**Scenario D**
1	no wandering nodes	5.22	5.27	9.58	18.37
	20% wandering nodes	*3.50*	*3.55*	*7.76*	*20.84*
10	no wandering nodes	10.39	10.38	19.97	24.17
	20% wandering nodes	*6.65*	*6.75*	*14.39*	*25.42*
20	no wandering nodes	10.63	10.68	20.87	24.99
	20% wandering nodes	*7.65*	*7.69*	*16.49*	*25.22*

Table 36: Effect of Wandering Node on DSDV Routing Overhead for HAWAII UNF

Maximum speed (m/s)		**Scenario A**	**Scenario B**	**Scenario C**	**Scenario D**
1	no wandering nodes	5.00	5.45	9.74	18.57
	20% wandering nodes	*3.51*	*3.52*	*7.74*	*21.18*
10	no wandering nodes	10.35	10.46	19.97	24.11
	20% wandering nodes	*6.73*	*6.67*	*14.41*	*25.44*
20	no wandering nodes	10.60	10.66	20.82	24.97
	20% wandering nodes	*7.59*	*7.69*	*16.48*	*25.20*

The influence of wandering nodes on DSDV routing overhead for HAWAII MSF and UNF are investigated (Table 35, Table 36). The results are the same for both path setup schemes. For the simulation scenarios A, B and C, the DSDV routing overhead decreases in the presence of the wandering nodes. The reason is that the presence of the wandering nodes to the neighboring subnet disperses the ad hoc nodes in their home subnet, therefore reduces the number of entries in a routing table, which leads to reduced overhead. By contrast, in simulation scenario D, the presence of the wandering nodes in each other's subnet increases the node density along the border of the adjacent subnets. The numerous nodes located along the border of the subnets help to exchange routing information between the adjacent subnets, therefore increase the number of entries in a route table, which result in increasing DSDV routing overhead.

Reported in Table 39 and Table 40 are the ratios of the number of control messages sent with 20% wandering nodes over that without wandering nodes. For all the simulation scenarios, the presence of the wandering nodes causes the control message overhead to increase at each network component. As mentioned in Section 5.3.3, the control messages in HAWAII are used for path set up during the handoff, therefore the increasing control message overhead is attributed to the increasing number of handoffs caused by the wandering nodes (Table 33, Table 34). The presence of the wandering nodes leads to an increase in the number of handoffs, which proportionally increases the number of control messages. For simulation scenarios A and B, the average control message ratio (CMwandering/CMno_wandering) at each network component is essentially the same as average handoff number ratio ($HandoffNUM_{wanderingNode}/HandoffNUM_{NoWanderingNode}$) in Table 37 (scenario A) and Table 38 (scenario B).

Table 37: Average Handoff Number Ratio for Scenario A

Maximum speed (m/s)	$\frac{HandoffNumber_{20\%WanderingNode}}{HandoffNumber_{NoWanderingNode}}$
1	2.34
10	1.71
20	1.96

Table 38: Average Handoff Number Ratio for Scenario B

Maximum speed (m/s)	$\frac{HandoffNumber_{20\%WanderingNode}}{HandoffNumber_{NoWanderingNode}}$
1	2.30
10	1.65
20	1.90

Table 39 : Average Control Message Ratio (CMwandering/CMno_wandering) for HAWAII MSF

Simulation Condition		**Gateway Nodes**	**Base Station Nodes**	**Wired Nodes**	**Router Nodes**
scenario A	1 m/s	2.4	2.3	2.3	2.5
	10 m/s	1.8	1.7	1.7	1.8
	20 m/s	2.1	1.9	1.9	2.2
scenario B	1 m/s	2.4	2.2	2.2	2.5
	10 m/s	1.7	1.6	1.6	1.8
	20 m/s	2.0	1.9	1.8	2.1
scenario C	1 m/s	3.4	3.0	3.0	3.6
	10 m/s	2.5	2.2	2.2	2.6
	20 m/s	3.1	2.7	2.6	3.4
scenario D	1 m/s	1.9	1.8	1.8	2.1
	10 m/s	1.9	1.7	1.7	1.9
	20 m/s	2.0	1.8	1.8	2.2

Table 40: Average Control Message Ratio (CMwandering/CMno_wandering) for HAWAII UNF

Simulation Condition		Gateway Nodes	Base Station Nodes	Wired Nodes	Router Nodes
scenario A	1 m/s	2.3	2.2	2.0	3.0
	10 m/s	1.7	1.6	1.6	1.2
	20 m/s	2.0	1.8	1.6	1.2
scenario B	1 m/s	2.3	2.1	2.0	2.7
	10 m/s	1.7	1.6	1.5	1.3
	20 m/s	1.9	1.7	1.6	1.1
scenario C	1 m/s	3.1	2.6	2.4	2.9
	10 m/s	2.3	2.0	1.9	1.5
	20 m/s	2.8	2.3	2.1	1.3
scenario D	1 m/s	1.8	1.7	1.6	3.4
	10 m/s	1.7	1.6	1.5	1.3
	20 m/s	1.8	1.6	1.5	1.1

5.4. Performance Comparison of HAWAII and HFA

As noted in Chapter 4, simulations are conducted using three different node movement speeds: maximum node movement speeds of 1, 10 and 20 m/s for each of four different simulation scenarios described in Section 5.1. In this section, simulation results obtained with HAWAII and HFA are compared in terms of packet delivery ratio, DSDV routing overhead and control message overhead for each simulation condition.

5.4.1. Packet Delivery Ratio Comparison

The simulation results of average packet deliver ratios obtained with HAWAII are compared with those of HFA in Figure 39. The important observation is that HFA slightly outperforms the HAWAII for all the simulation scenarios except scenario B, which is the only case where the destination nodes are the wired hosts.

For simulation scenario B, the packet delivery ratios of HFA and HAWAII UNF are identical. HAWAII MSF fails to converge because of its forwarding scheme for the mobile hosts. Since the destinations are the wired nodes, the handoff scheme of each micromobility protocol does not play any important role in packets delivery. For HFA and HAWAII UNF, once the packet is routed among the ad hoc network to reach one of the base station nodes, it can be successfully delivered to the corresponding wired host. Therefore, the packet delivery ratio is unaffected by the micromobility protocol in this scenario.

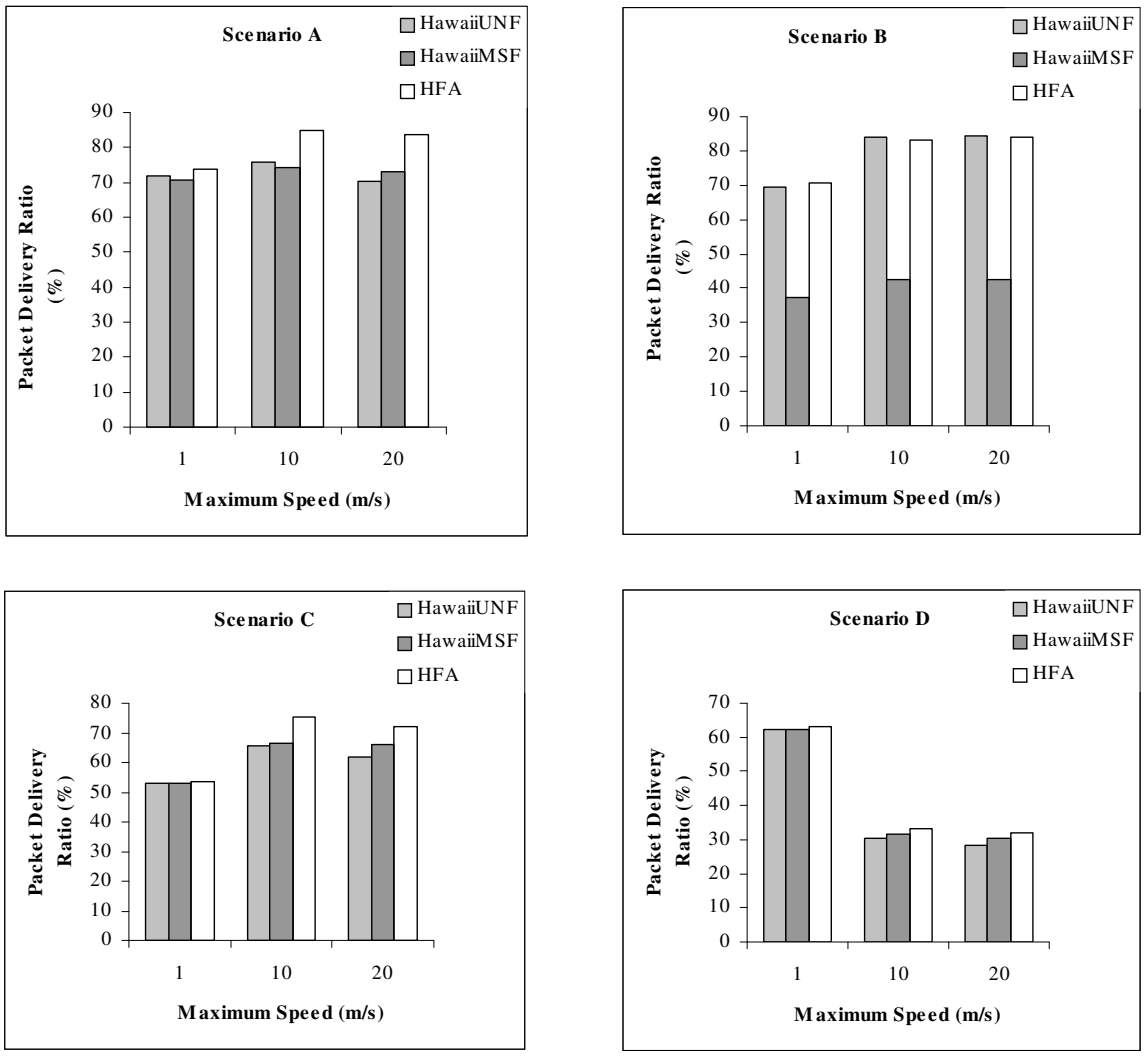

Figure 39: Comparison of Delivery Ratios of HAWAII and HFA

When packets are sent from wired hosts to ad hoc nodes (scenario A), the micromobility protocol is used to handle the handoff during the packet delivery. The results show that Hierarchical Mobile IP outperforms HAWAII, especially at higher node movement speed. In this environment, the packet loss can be caused by one of the following reasons:

1. Link failures among the ad hoc nodes
2. Delivery failures due to unknown route to base station nodes
3. Handoff.

By investigating the details of packet loss, it is found that the number of the packet loss due to link failures among the ad hoc nodes is identical for HFA and HAWAII. This observation is obvious, since the same node movement patterns and connection patterns are used for the simulations of both micromobility protocols. Thus, the probability for a node to find an available route to one of the base station nodes is the same for both micromobility protocols. As such, the difference in packet delivery performance is likely only attributed to the handoff scheme employed by each micromobility protocol.

As in the previous section, it has been demonstrated that both path setup schemes in HAWAII fail to establish path setup during the inter-domain handoff between two domains because of the router node between the gateway nodes. It then can be reasoned that the slight inferiority of delivery performance of HAWAII is due to its failure in inter-domain handoff. To confirm this suggestion, the same series of simulations on one subnet were conducted in HFA under the same conditions as those performed in HAWAII, and the simulation results are compared with that obtained in HAWAII (Figure 40).

These results show that HAWAII UNF and HAWAII MSF perform equally well as the HFA on packet delivery in one subnet, when no inter-domain handoff is involved. Therefore, the difference in packet delivery performance of HFA and HAWAII is only attributable to the failure of handling inter-domain handoff in HAWAII. In CIMS, no functions were developed for handling inter-domain handoff in HAWAII. However, due to time constraint, this problem remains unsolved in this work. As proposed in HAWAII, a mobile node needs to acquire a co-located care-of address (CCOA) when it is in a foreign domain. When the mobile node is in its home domain, the mobile must register with the base station using the advertised (non co-located) COA; otherwise, the mobile

host must register with the base station using a co-located COA. The HAWAII processing is required if the host is within the domain, and Mobile IP processing when it is roaming in a foreign domain.

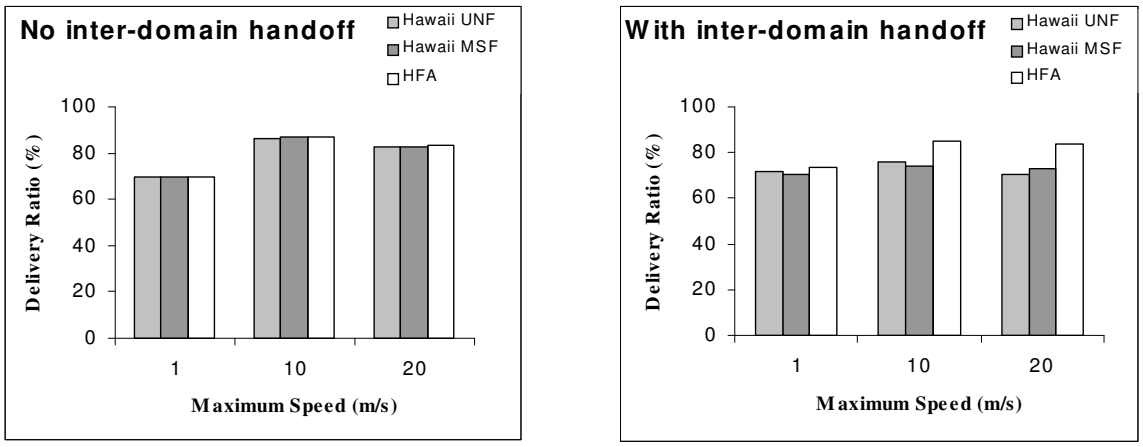

Figure 40: Comparison of Delivery Ratios of HAWAII and HFA for Scenario A without Inter-Domain Handoff (on 1 subnet) and with Inter-Domain Handoff (on 3 subnets)

5.4.2. DSDV Routing Overhead Comparison

The results for the DSDV routing overhead for HAWAII UNF, HAWAII MSF and HFA are summarized in Figure 41. It is clear that the DSDV routing overhead is unaffected by the micromobility protocol. With the network topology and the ad hod network defined in this work, DSDV routing overhead increases with the node movement speed. This increase is caused by the higher number of route changes in the ad hoc network with higher node movement speed, which in turn results in increased triggered updates, and the subsequent advertisements of new route information in the entire ad hoc network.

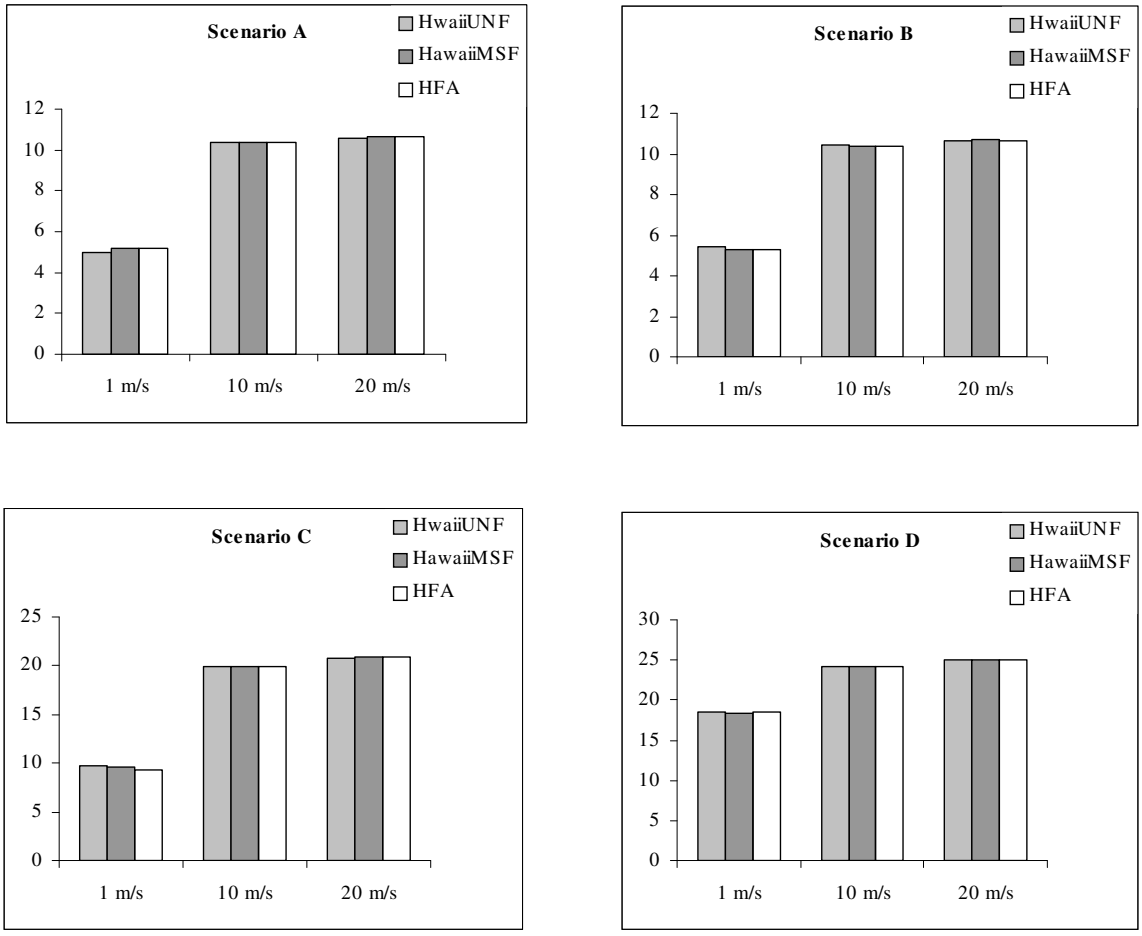

Figure 41: Comparison of DSDV Routing Overhead for HAWAII and HFA

5.4.3. Control Message Overhead Comparison

In the previous sections, the packet delivery performance and DSDV routing overhead of HAWAII and HFA have been compared. Results for HAWAII and HFA are similar, given that the micromobility protocols operate under the same network topology. In this section, the control message overhead is compared to observe the cost of each protocol to achieve comparable delivery performance.

The control message overhead is compared between HFA and HAWAII MSF, which has higher overhead than HAWAII UNF. The ratios of the number of control messages sent at each network component in HFA over that in HAWAII MSF are given in Table 41 for simulation scenario A, in Table 42 for scenario B, in Table 43 for scenario C, and in Table 44 for scenario D. It is shown that the control message overhead is much higher (by at least two times) in HFA than in HAWAII for each network component, except the router nodes (RNs) between the gateway nodes.

Table 41: Ratio of Control Message Overhead CM_{HFA}/CM_{HAWAII_MSF} for Scenario A

Maximum speed (m/s)	Gateway Nodes	Base Station Nodes	Wired Nodes	Router Nodes
1 m/s	7.6	10.1	13.4	1.0
10 m/s	2.8	3.6	4.8	0.6
20 m/s	3.0	3.6	4.7	0.8

Table 42: Ratio of Control Message Overhead CM_{HFA}/CM_{HAWAII_MSF} for Scenario B

Maximum speed (m/s)	Gateway Nodes	Base Station Nodes	Wired Nodes	Router Nodes
1 m/s	7.5	9.9	13.2	1.0
10 m/s	2.7	3.4	4.5	0.6
20 m/s	2.9	3.5	4.5	0.8

Table 43: Ratio of Control Message Overhead CM_{HFA}/CM_{HAWAII_MSF} for Scenario C

Maximum speed (m/s)	Gateway Nodes	Base Station Nodes	Wired Nodes	Router Nodes
1 m/s	16.8	20.1	27	1.9
10 m/s	4.8	5.9	7.8	0.6
20 m/s	5.2	5.8	7.6	0.9

Table 44: Ratio of Control Message Overhead CM_{HFA}/CM_{HAWAII_MSF} for Scenario D

Maximum speed (m/s)	Gateway Nodes	Base Station Nodes	Wired Nodes	Router Nodes
1 m/s	6.9	8.1	10.9	1.6
10 m/s	3.0	3.6	4.8	0.7
20 m/s	3.0	3.5	4.5	0.8

Recall that, the control messages in HFA are sent in response to each MIPT_REG_REQUEST from the ad hoc nodes; while the control messages in HAWAII are only sent for power up or path setup during a handoff.

In HAWAII, the control messages sent by the router nodes (RNs) between the gateway nodes are used only for handling the inter-domain handoff. In HFA, the control messages sent by the RNs are used for responding to each COA registration request from the mobile nodes to the base station nodes that are not in their home subnet. Also, the control messages sent by the RNs consist of two parts: one from the gateway node of the adjacent subnet to the mobile host's home gateway node to inform it of the inter-domain handoff; the other from the mobile node's home gateway node to the mobile node through the gateway node of the adjacent subnet to approve and acknowledge the new COA. One would expect the total number of inter-domain handoffs occurring during each simulation to be close for HFA and HAWAII, since the same node movement patterns and

connection patterns are used for the simulations of both micromobility protocols. However, the control message overhead at RNs is lower for HFA than for HAWAII. One possible explanation is the channel availability. Due to the high amount of control messages sent in the entire network in HFA, each handoff request can not be processed immediately as the case in HAWAII, therefore the total number of handoffs processed in HFA is lower (see Table 11 and Table 45).

The first reason for the higher control message overhead of HFA is due to the difference in the location update mechanism between the two micromobility protocols. In HFA, packets are forwarded from the old base station to the new base station just like the forwarding path setup schemes in HAWAII. The important difference lies in the fact that in HFA, the HA and the corresponding host need to be notified before packets go directly to the new base station. Moreover, the binding between the mobile node's HA and its current COA needs to be kept by periodically sending the registration request and reply messages within the registration lifetime. In HAWAII, mobile nodes retain their network address while moving within a domain, thus the HA and any corresponding hosts are unaware of the mobile node's mobility within this domain.

The second reason comes from the selection decision of the crossover router during the location update procedure. In HAWAII, only the new and old base stations and the intermediate wired nodes (WNs) connecting them are involved in processing the path setup messages during handoff. This local update (keeping routing update messaging close to base stations and not to the gateway node) dramatically decreases the control messages in the entire network. The location updating operation is similar in HFA, but the crossover router is always at the gateway node, which accounts for the additional

control message overhead. In HFA, sending all handoff update messages to the gateway causes a high number of control messages in the entire network.

For packet delivery between heterogeneous sender and receivers (scenarios A and B), the identical location of ad hoc nodes leads to the same number of control messages, which results in the same ratio of control message overhead at each network component. The increase in the ratio of control message overhead from 1 to 10 m/s is due to the increased number of handoffs (Table 45). This ratio is stabilized at higher node movement speed, which is in agreement with the variation of the number of handoffs (Table 45).

Table 45: Average Number of Handoffs Processed in HAWAII UNF

Simulation Scenario	S = 1 m/s	S = 10 m/s	S = 20 m/s
A	1246	3479	3434
B	1278	3706	3562
C	1158	3964	4065
D	3172	6811	7358

For packet delivery between ad hoc nodes (scenarios C and D), one would expect that the control message overhead to be doubled compared to that in scenarios A and B, since two groups of ad hoc nodes are involved. However, this is only true for HFA, but not for HAWAII. In HFA, it is also observed that the number of control messages sent in scenario D is slightly higher than that in scenario C. In HAWAII, the number of control messages sent in scenario C is comparable to that in scenarios A and B, but is doubled in scenario D. These observations result in higher ratios of control message overhead in scenario C (Table 43) than in scenario D (Table 44).

The higher control message overhead observed in scenario D compared to scenario C is due to the difference between the location of the ad hoc networks. As discussed in the previous section for HAWAII, control messages sent by the gateway nodes (GNs) and the base station nodes (BSs) are mostly used for path setup during the handoff. Among the total number of handoffs, 30-40% is due to inter-domain handoff for simulation scenarios A and B, where ad hoc nodes are located in the subnet2, sandwiched between subnet1 and subnet3. As for scenario C, even if two groups of ad hoc nodes are involved in the simulation, they are located separately in subnet1 and subnet3, and the chance to have inter-domain handoff for each group of ad hoc nodes is reduced by half. This is why, compared to scenarios A and B, the total number of handoffs does not increase significantly. Similarly, in scenario D, two groups of ad hoc nodes are involved in the simulation, but they are located in subnet1 and subnet2, which cause the total number of handoffs to increase significantly compared to that in scenarios A and B (Table 45). In HAWAII, the location of the ad hoc nodes in scenario C results in the lower control message overhead compared to that of scenario D. This is why the ratio of control message overhead is much higher (Table 43) in scenario C than that observed in other scenarios (Table 41, Table 42 and Table 44).

5.4.4. Wandering Nodes Effect Comparison

The wandering nodes effect has been investigated in Section 5.2.4 for HFA and in Section 5.3.4 for HAWAII. The effects of wandering nodes on packet delivery performance, DSDV routing overhead and control message overhead are similar for both micromobility protocols.

Packet delivery performance improves at lower node movement speed for simulation scenarios A, B and C, but deteriorates when node movement speed increases. However, the improvement is more pronounced in HFA than in HAWAII for scenario A. This difference is attributed to the fact that HAWAII fails to handle the inter-domain handoff between two domains. The improvement in packet delivery performance at the lower node movement speed is due to the additional paths created by the wandering nodes between the adjacent subnets in order to reach a destination node. The deterioration at higher node movement speed is attributed to the increased link failures along the ad hoc node path built by the wandering nodes. For simulation scenario D, the presence of wandering nodes improves packet delivery performance regardless of node movement speed. This improvement comes from additional paths between the adjacent subnets, and spreading the routing information through two ad hoc networks with the help of higher number of mobile nodes located along the border of the adjacent subnets.

Since the DSDV routing overhead is only related to the ad hoc network and the routing protocol, the variation of the DSDV routing overhead in the presence of wandering nodes in each scenario is the same for HFA and HAWAII. For simulation scenarios A, B and C, the DSDV routing overhead decreases in the presence of wandering nodes, because the presence of the wandering nodes disperses the ad hoc nodes in the subnet. Simulation

scenario D is the only scenario to show the DSDV routing overhead increase, because of spreading routing information between the adjacent subnets by higher number of nodes located along the border of the subnets, which results in increasing number of entries in the routing table.

The presence of the wandering nodes leads to an increase in the number of handoffs and subsequent location updating. In HAWAII, the control messages are used only for power up and path set up during the handoff, therefore the control message overhead is proportionally increased at each network component with the increase in the number of handoffs. In HFA, the presence of wandering nodes increases the control message overhead at the gateway nodes (GNs). This is attributed to the increased location updating of the wandering nodes over two subnets, consequently increasing the number of control messages sent by the router nodes (RNs). The situations at the base station nodes are different. Here, the number of control messages sent by a base station node depends on the total number of MIPT_REG_REQUEST messages received by the base station nodes. As explained previously, the presence of wandering nodes causes a higher number of handoffs, and the packet delivery performance inside the ad hoc network itself deteriorates with increasing node movement speed. Therefore, at higher node movement speed with the presence of wandering nodes, fewer packets can arrive at the base station node caused by increased link failure along the longer path, consequently less control messages are sent by the base station nodes trigged by the MIPT_REG_REQUEST messages of the ad hoc nodes.

Chapter 6. Conclusions and Future Work

In this work, two different types of micromobility protocols, Hierarchical Mobile IP (HFA) and HAWAII, were successfully employed for the integration of ad hoc networks with the Internet. For HAWAII, two different path setup schemes, Multiple Stream Forwarding (MSF) and Unicast Non-Forwarding (UNF), were investigated. A series of simulations were conducted with the network simulator NS version 2.1b6a and its extension CIMS (Columbia IP Micromobility Software) to illustrate the performance of the micromobility protocols. Simulation results were obtained in an ad hoc network of 50 mobile nodes moving about and communicating with a corresponding host within the same subnet or in a different subnet, or with a wireless mobile node of another ad hoc network. Three maximum node movement speeds (1 m/s, 10 m/s and 20 m/s) and four different communication scenarios for each movement speed were studied:

A: wired hosts to ad hoc nodes

B: ad hod nodes to wired hosts

C: ad hoc nodes to ad hoc nodes in separate subnets

D: ad hoc nodes to ad hoc nodes in adjacent subnets

The performance of HFA, HAWAII UNF and HAWAII MSF was compared in terms of packet delivery ratio, ad hoc routing protocol overhead and control message overhead.

Under the defined network topology with three subnets involved and the designated simulation environment, HFA, HAWAII UNF and HAWAII MSF handle the packet delivery equally within one subnet for all the simulation scenarios by using Destination-Sequenced Distance-Vector (DSDV) routing protocol. Due to the fact that HAWAII is a micromobility protocol for handling the intra-domain mobility and no functions were

developed for handling inter-domain mobility in CIMS, HFA slightly outperforms the HAWAII when three subnets are involved. When node maximum movement speed increases from 1 to 10 m/s, a significant increase in packet delivery rate was observed but no significant change was observed when the speed increases from 10 to 20 m/s. These observations have been demonstrated to result from the behavior of the DSDV routing protocol.

The DSDV routing overhead was observed to be unaffected by the micromobility protocol. At higher node movement speed, DSDV routing overhead increases. This increase arises from the higher number of route changes in the ad hoc network, consequently leading to increased triggered updates, which in turn lead to the subsequent advertisements of new route information in the entire ad hoc network.

The advantage of HFA lies in its simplicity in design and implementation, but the drawback is its higher control message overhead (by at least two times) compared to HAWAII. The difference in control message overhead between HFA and HAWAII comes from the difference in their location management mechanism and the crossover router selection in the handoff scheme.

Finally, the effects of wandering nodes have been observed for each micromobility protocol. The presence of wandering nodes provides additional paths from the source node to the destination node through the wandering nodes in the adjacent subnet, but it leads to an increase in the number of handoffs and subsequent location updating. For the simulation scenario where packets are sent from ad hoc nodes to ad hoc nodes in adjacent subnets, the presence of wandering nodes provides more reachable destinations in the ad hoc networks due to higher density of mobile nodes located along the border of subnets,

improving the packet delivery performance regardless of node movement speed at the expense of increased DSDV routing overhead. For all other simulation scenarios, the presence of wandering nodes disperses the ad hoc nodes in its home subnets, thus decreases the DSDV routing overhead and improves packet delivery performance at lower node movement speed. At higher node movement speed, the packet delivery deteriorates due to the increased link failures along the ad hoc node path built by the wandering nodes. In HAWAII, the control messages are used only for power up and path setup during the handoff, therefore the control message overhead is proportionally increased at each network component with the increase in the handoff number. While in HFA, the presence of wandering nodes increases the control message overhead mostly at the gateway nodes and the router nodes between the gateway nodes due to the increased location updates of the wandering nodes over two subnets.

It can be concluded through all the simulation and implementation measurements in this work that HAWAII is a better solution than Hierarchical Mobile IP for intra-domain mobility support and it can work with Mobile IP to support wide-area user mobility. With comparable packet delivery performance as HFA, HAWAII has the advantage of much lower signaling overhead. This lower signaling overhead is due to the elimination of the registrations between mobile hosts and possibly distant home agents when mobile hosts remain in their home domain. Besides, the local update scheme of HAWAII, which keeps routing update messaging close to base stations but not to the gateway node, also contributes to its lower signaling overhead. Therefore, HAWAII is better suited than HFA for integration of ad hoc network with the Internet, providing reduced signaling

overhead (which may result in reduced packet delay), more efficient routing and better scalability.

Due to time constraint, one of unsolved problems in this work is to handle the inter-domain handoff in HAWAII. As proposed in HAWAII, a mobile node needs to acquire a co-located care-of address (CCOA) when it is in a foreign domain. When moving within the foreign domain, the mobile host retains its COA, the home gateway node acts as the HA and is not notified of these movements. Therefore, HAWAII processing is required if the host is within the domain, and Mobile IP processing when it is roaming in a foreign domain. The protocols should coordinate with each other to maintain forwarding entries for the mobile host so that interleaved arrival of protocol messages do not leave the forwarding tables in an inconsistent state. After the home gateway node has processed the Mobile IP registration message indicating that the host has moved from its home domain to a foreign domain, HAWAII must ignore any refresh messages for this mobile host from downstream routers; these are stale refresh messages and will eventually be timed out. Similarly, when the host has moved back from the foreign domain to its home domain, the home gateway node should process the HAWAII update; in the meantime, Mobile IP should process any subsequent de-registration messages from the mobile host to remove its internal state without affecting the forwarding entries.

Similarly, more enhancement needs to be implemented in HFA. If a mobile node moves out of its home network, the address of the GFA in the visiting network should be its COA address, the mobile node's home agent should not be informed of any movement of mobile node within the visiting network. Hence, signaling overhead is greatly reduced for out of home network (inter-network) mobility. In order to be able to deliver packets to

any mobile node residing in its network, each GFA must be aware of the exact location of each mobile node in its area, since all the intermediate nodes in HFA are location-unaware. Therefore, each GFA must be informed of any movement of a mobile node within its network.

Since this is the first work on the integration of ad hoc network with the Internet, there is still much more work to be done in terms of performance evaluation of the micromobility protocols. Additional measurements on packet delivery delay and handoff latency, which are also good indications of performance evaluation, would be necessary. Also, the influence of different packet playout delays, network load, traffic sources (such as TCP) could be investigated to explore the performance of the micromobility protocols for different traffic conditions and applications. Finally, simulations with different ad hoc routing protocols, such as Ad Hoc On Demand Distance Vector (AODV) and Dynamic source routing (DSR), would allow us to observe the impact of ad hoc routing protocols on the performance of micromobility protocols.

References

[1] J. Thompson, “Mobile Ad Hoc Networks”, <www.nycwireless.net/presentation/jt_adhoc_tutorial.pdf>

[2] I. F. Akyildiz, J. McNair, J. Ho, H. Uzunalioglu and W. Wang, “Mobility Management in Next Generation Wireless Systems”, Proceedings of the IEEE, Vol. 87, pp. 1347-1384, August 1999.

[3] G. Fleming, A. Hoiydi, J. de Vriendt, G. Nikolaidis, F. Piolini, and M. Maraki, “A Flexible Network Architecture for UMTS”, IEEE Personal Communications Magazine, Vol. 5, No. 2, pp. 8-18, April 1998.

[4] C. Perkins, “IP Mobility Support”, INTERNET RFC 2002, <http://www.ietf.org/rfc/rfc2002.txt>, October 1996.

[5] J. Solomon, “Applicability Statement for IP Mobility Support“, INTERNET RFC 2005, <http://www.ietf.org/rfc/rfc2005.txt >, October 1996.

[6] D. B. Johnson, "Scalable Support for Transparent Mobile Host Internetworking", Wireless Networks, Vol. 1, pp. 311-321, October 1995.

[7] A. T. Campbell and J. Gomez, "IP Micro-Mobility Protocols", ACM SIGMOBILE Mobile Computer and Communication Review, Vol. 4, No. 4, pp. 45-53, October 2001.

[8] E. Gustafsson, A. Jonsson and C. Perkins, “Mobile IP Regional Tunnel Management”, INTERNET DRAFT, <http://comet.ctr.columbia.edu/micromobility/pub/draft-ietf-mobileip-reg-tunnel-04.txt>, March 2001.

[9] C. Perkins, “Mobile-IP Local Registration with Hierarchical Foreign Agents”, INTERNET DRAFT, <http://www.iprg.nokia.com/~charliep/txt/hierfa/hierfa.txt>, February 1996.

[10] G. Cho and L. Marshall, "An Efficient Location and Routing Scheme for Mobile Computing Environments", IEEE Journal on Selected Areas in Communications, Vol. 13, pp. 868-879, June 1995.

[11] S. Foo and K. Chua, “Regional Aware Foreign Agent (RAFA) for Fast Local Handoffs”, INTERNET DRAFT, <http://mip.ee.nus.edu.sg/paper/draft-chuafoo-mobileip-rafa-00.txt>, November 1998.

[12] P. McCann, T. Hiller, J. Wang, A. Casati, C. Perkins and P. Calhoun, “Transparent Hierarchical Mobility Agents (THEMA)”, INTERNET DRAFT, <http://www.ietf.org/proceedings/99mar/I-D/draft-mccann-thema-00.txt>, March 1999.

[13] D. Forsberg, J. T. Malinen, J. K. Malinen, T. Weckström and M. Tiusanen, “Distributing Mobility Agents Hierarchically under Frequent Location Updates”, Sixth IEEE International Workshop on Mobile Multimedia Communications (MOMUC'99), pp.159-168, San Diego, CA, November 1999.

[14] A. Misra, S. Das, A. Mcauley, A. Dutta and S. K. Das, “IDMP: An Intra-Domain Mobility Management Protocol using Mobility Agents”, INTERNET DRAFT, <http://comet.ctr.columbia.edu/micromobility/pub/draft-misra-mobileip-idmp-00.txt>, January 2000.

[15] A. Misra, S. Das, A. Dutta, A. McAuley and S. Das, "IDMP-based Fast Handoffs and Paging in IP-based Cellular Networks", in 3GWireless 2001, pp. 6-12, San Francisco, CA, May 2001.

[16] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan and S.Y. Wang, “HAWAII: A Domain-based Approach for Supporting Mobility in Wide-area Wireless networks”, in Proceedings of IEEE International Conference on Network Protocols, pp. 283-292, Toronto, Canada, October 1999.

[17] A. G. Valkó, “Cellular IP: A New Approach to Internet Host Mobility”, ACM Computer Communication Review, Vol. 29, No. 1, pp. 50-65, January 1999.

[18] A. G. Valkó, A. T. Campbell, J. Gomez, “Cellular IP”, INTERNET DRAFT, <http://comet.ctr.columbia.edu/cellularip/pub/draft-valko-cellularip-00.txt>, November 1998.

[19] A. T. Campbell, J. Gomez, S. Kim, Z. Turanyi, C-Y. Wan and A, Valko "Comparison of IP Micro-Mobility Protocols", IEEE Wireless Communications Magazine, Vol. 9, No. 1, pp. 1-12, February 2002.

[20] Micromobility home page, http://comet.columbia.edu/micromobility

[21] A. T. Campbell, J. Gomez, S. Kim, Z. Turanyi, C-Y. Wan and A, Valko, “Design and Performance of Cellular IP Access Networks”, IEEE Personal Communications, Special Issue on IP-Based Mobile Telecommunications Networks, pp. 42-49, June/July 2000.

[22] S. Y. Wang and H. Kung, “A Simple Methodology for Constructing an Extensible and High-Fidelity TCP/IP Simulator”, in Proceedings of INFOCOM99, pp. 1134-1143, New York, NY, March 1999.

[23] C. E. Perkins and D. B. Johnson, “Route Optimization in Mobile IP,” INTERNET DRAFT, <http://comet.ctr.columbia.edu/micromobility/pub/draft-ietf-mobileip-optim-10.txt >, November 2000.

[24] J. Broch, D. Maltz, and D. Johnson, “Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks", in Proceedings of the Workshop on Mobile Computing held in conjunction with the International Symposium on Parallel Architectures, Algorithms, and Networks, pp. 370-375, Perth, Australia, June 1999.

[25] A. Striegel, R. Ramanujan, J. Bonney, “A Protocol Independent Internet Gateway for Ad-Hoc Wireless Networks”, in Proceedings of Local Computer Networks (LCN’2001), pp. 1-15, Tampa, FL, November 2001.

[26] http://www.isi.edu/nsnam/ns

[27] http://nile.wpi.edu/NS/overview.html

[28] E. Gustafsson, A. Jonsson and C. Perkins, “Mobile IP Regional Registration”, INTERNET DRAFT, <http://www.mobile-ip.com.cn/draft/draft-ietf-mobileip-reg-tunnel-03.txt>, July 2000.

[29] S. Mohan and R. Jain, “Two User Location Strategies for Personal Communications Services”, IEEE Personal Communications, Vol. 1, No. 1, pp. 42-50, January 1994.

[30] http://www.isi.edu/nsnam/ns/ns-documentation.html

[31] D. C. Plummer, “An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Addresses for Transmission on Ethernet Hardware”, INTERNET RFC 826, <http://www.faqs.org/rfcs/rfc826.html>, November 1982.

[32] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers”, in Proceedings of the SIGCOMM ‘94 Conference on Communications, Architectures, Protocols and Applications, pp. 234-244, London, UK, August 1994.

[33] E. Cheng, "On-demand Multicast Routing in Mobile Ad Hoc Networks", M.Eng. Thesis, Carleton University, 2001.

[34] L. Qin, "Pro-Active Route Maintenance in DSR", M.Sc.(ISS) Thesis, Carleton University, 2001.

[35] J. Broch, D. A. Maltz, D. Johnson, Y-C. Hu and J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols", in Proceedings of the Conference on Mobile Computing and Networking (MOBICOM’98), pp. 85-97, Dallas, TX, October 1998.

[36] C. Bettstetter, “On the Minimum Node Degree and Connectivity of a Wireless Multihop Network”, in Proceedings of 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC’02), pp. 80-91, Lausanne, Switzerland, June 2002.