Theses and Dissertations

Student Graduate Works

3-2-2007

Effective Mobile Routing Through Dynamic Addressing

HeungSoon Park

Follow this and additional works at: https://scholar.afit.edu/etd

Part of the Digital Communications and Networking Commons

EFFECTIVE MOBILE ROUTING THROUGH DYNAMIC ADDRESSING

THESIS

Heungsoon Park, Captain, ROKA

AFIT/GCS/ENG/07-09

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/GCS/ENG/07-09

EFFECTIVE MOBILE ROUTING THROUGH DYNAMIC ADDRESSING

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science

Heungsoon Park, BS

Captain, ROKA

March 2007

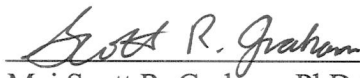APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

EFFECTIVE MOBILE ROUTING THROUGH DYNAMIC ADDRESSING

Heungsoon Park, BS

Captain, ROKA

Approved:
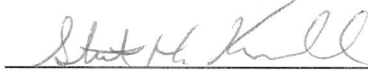
(signature)	2 Mar 07
Maj Scott R. Graham, PhD (Chairman)	Date
(signature)	2 Mar 07
Dr. Kenneth M. Hopkinson (Member)	Date
(signature)	2 Mar 07
Lt.Col Stuart Kurkowski, PhD (Member)	Date

AFIT/GCS/ENG/07-09

Abstract

Military communications has always been an important factor in military victory and will surely play an important part in future combat. In modern warfare, military units are usually deployed without existing network infrastructure. The IP routing protocol, designed for hierarchical networks cannot easily be applied in military networks due to the dynamic topology expected in military environments. Mobile Ad-hoc Networks (MANETs) represent an appropriate network for small military networks. But, most ad-hoc routing protocols suffer from the problem of scalability for large networks. Hierarchical routing schemes based on the IP address structure are more scalable than ad-hoc routing but are not flexible for a network with very dynamic topology. This research seeks a compromise between the two; a hybrid routing structure which combines mobile ad-hoc network routing with hierarchical network routing using pre-planned knowledge about where the various military units will be located and probable connections available.

This research evaluates the performance of the hybrid routing and compares that routing with a flat ad-hoc routing protocol, namely the Ad-hoc On-demand Distance Vector (AODV) routing protocol with respect to goodput ratio, packet end-to-end delay, and routing packet overhead. It shows that hybrid routing generates lower routing control overhead, better goodput ratio, and lower end-to-end packet delay than AODV routing protocol in situations where some *a-priori* knowledge is available.

Acknowledgments

    I would like to express my sincere appreciation to my thesis advisor, Maj. Scott Graham, for all that he taught me in the classroom and his kind guidance. I could not have completed this research without his support and concerns.

<div align="right">Heungsoon Park</div>

Table of Contents

List of Figures

List of Tables

EFFECTIVE MOBILE ROUTING THROUGH DYNAMIC ADDRESSING

I. Introduction

1.1. Background

A network consists of two or more hosts connected together over wired or wireless links to communicate and share resources [1]. The most well-known network, the Internet, is enormous and manifests a high degree of interconnection. A military network must meet various requirements for a military operation in order to ensure military victory. A key factor is keeping connections active, with minimal packet losses between sender and receiver, despite battlefield events.

In multi-hop networks, intermediate nodes must forward packets toward the destination nodes, according to rules, which are typically stored in routing tables for quick lookup. These forwarding rules are determined by routing protocols, which are responsible for forming a network connection between two end points. Diverse routing protocols have been implemented in various ways to establish the connection and communication between two nodes. A specific routing protocol may be more suitable than another protocol in a particular network environment.

Hierarchical routing relies on a fixed hierarchical topology in which the address of a node gives some indication of where in the network it is connected. A hierarchical routing scheme, based on the Internet IP structure, simplifies the complex routing

problem for a large network by reducing the size of the forwarding tables. The hierarchy allows entries to be grouped into large entries, resulting in much smaller tables. Moreover, because hierarchal based systems are composed of relatively static nodes, (i.e., they may fail, but when they return to service, they maintain the same address and topological location in the network) the routing control traffic can be greatly reduced. Hierarchical routing requires significantly less routing control overhead than a MANET, better scalability and faster routing decision-making [2].

Mobile Ad-hoc Networks (MANET) are self-configuring networks of mobile wireless nodes that also act as routers. MANET's possess no dedicated infrastructure. In the ad-hoc network, the nodes are usually mobile and have finite transmission ranges. Hence, the network topology of a MANET may change unpredictably, frequently and rapidly. As a result, MANET's typically employ a flat routing protocol, which allows any node to be connected anywhere in the network, but must maintain an entry for every single destination serviced, requiring much larger routing tables for a similar sized network. As a result, flat routing protocols simply do not scale well.

Military communication is required in hostile surroundings where unpredictable environmental factors abound and interruptions from enemies occur. The network will likely be bandwidth-constrained, with variable capacity links and dynamic topology [3].

1.2. Problem Statement

One of the trends in military communications is that the individual links are beginning to be integrated into one global network in which the network infrastructure itself must adapt to the change in its surroundings. Military units must keep its network connected despite the changes in available media and various other environmental factors.

The MANET is initially very attractive for military communication due to its fault tolerance and adaptability. However, with potentially very large node populations, limited resources and dynamic topologies, the scalability issue quickly manifests itself as a major problem, causing excessive routing control message overhead.

The MANET routing protocol and the hierarchical routing are complementary to each other for the problems mentioned above. Thus, one way to solve the issues for the military communication is to implement a hybrid routing which combines the salient features of the two routing schemes.

1.3. Research Objectives

The objective of this research is to evaluate a hybrid routing approach which combines hierarchical routing based on pre-planned knowledge, with flat ad-hoc routing as a fault-tolerant backup. The analysis of the hybrid routing will compare it to an existing flat ad-hoc routing protocol, Ad-hoc On-demand Distance Vector (AODV) routing protocol with respect to goodput ratio, end-to-end packet delay, and routing

control overhead. The research will also identify the strengths and weaknesses of the hybrid routing in dynamic topology.

In order to meet the purpose of this research, the major research question is "How does the hybrid routing work and what are the advantages and disadvantage of the routing compared to Ad-hoc On-demand Distance Vector (AODV) routing?"

1.4. Methodology

This research methodology follows a systematic approach. The hybrid routing scheme is defined as dynamic addressing with a prescribed military plan for traffic demands. The hybrid routing protocol uses a dynamic address, based upon hierarchical routing, to "guess" the location of the receiving node, reverting to the reactive routing scheme only in the event of a failure in the prediction. To allow dynamic addressing in the OPNET simulation environment, all interfaces are based on version 6 of the Internet Protocol (IPv6), which allows nodes to change their IP addresses dynamically throughout the simulation scenario.

The performance metrics observed are goodput ratio, node pair end-to-end delay, and routing packet overhead in order to evaluate the performance of the hybrid routing scheme.

1.5. Assumptions/Limitations

This research assumes that all traffic demands generated by senders are already prescribed according to an assumed plan. While unreasonable in many scenarios, this

assumption is plausible in a military environment in which the operation is planned in advance. While it is true that the operation may deviate from the plan, the original plan can still serve as the basis for the communication network routing. The implication of this assumption is that sender's already know where in the network the intended receivers are supposed to be at some point in time, and can thus forward messages "toward" the receivers without having to first search the network for where the receiver is (as is done in reactive routing such as AODV). Thus, all traffic demands are dependent on prescribed plans in the simulation of this research. It is understood that this approach is limited to scenarios in which pre-planned data exists.

1.6. Thesis Preview

This chapter briefly introduces the issues of military communications and the characteristics of MANETs and hierarchical routing. It also presents motivations for this research. The remainder of the paper is organized as follows. Chapter 2 presents a literature review of hierarchical routing, MANET routing protocols, and IPv6. Chapter 3 describes the methodology used to conduct this research. Chapter 4 presents a detailed analysis of the hybrid routing and the results. Chapter 5 draws conclusions based on the research results and provides recommendations for future work.

II. Literature Review

2.1. Overview

The purpose of this chapter is to provide common understanding of hierarchical routing, IPv6, and mobile ad-hoc network routing. Hierarchical routing and mobile ad-hoc network are explained as the basis of the research concept. AODV and the IPv6 addressing structure are explained in detail because they form an integral part of this research simulation.

2.2. Hierarchical Address Routing

The following describes hierarchical addressing. The complicated routing problems on large networks can be resolved by reducing the problem into smaller-scale networks. The entire network is divided into several levels of hierarchy. Each level is accountable for its own routing [4]. The Internet is based on the hierarchical addressing. The primary advantage of hierarchical routing is that routing updates can be reduced because routers in a same layer of hierarchy need to know only about other routers within the same domain. The resulting routing mechanisms are very small and simple.

On the other hand, there is also drawback of the hierarchical routing structure. When nodes which have to communicate are mobile, the nodes may move topologically with respect to one another, disrupting the hierarchical routing scheme. To maintain the hierarchy, the nodes must adopt a new address, derived from their topological location in the network. While some protocols, such as Mobile IP support

a mechanism for roaming within the hierarchical addressing network, it must be understood that these represent limited mobility at the edge of the network. A mobile node and its related agents (a home agent and a foreign agent in case of IPv4) must maintain the mobile node's care-of-address and register that address whenever the mobile node changes its point-of-attachment to the Internet [5]. Mobility at the core requires a fundamentally different approach.

In military communication, hierarchy is inherent. All military units are deployed in accordance with military operational plans and military hierarchy. Each military group has responsibility for its operational area. Thus, the most popular way of building hierarchical communication in military environments is to group all nodes geographically and to assign related network address to each node.
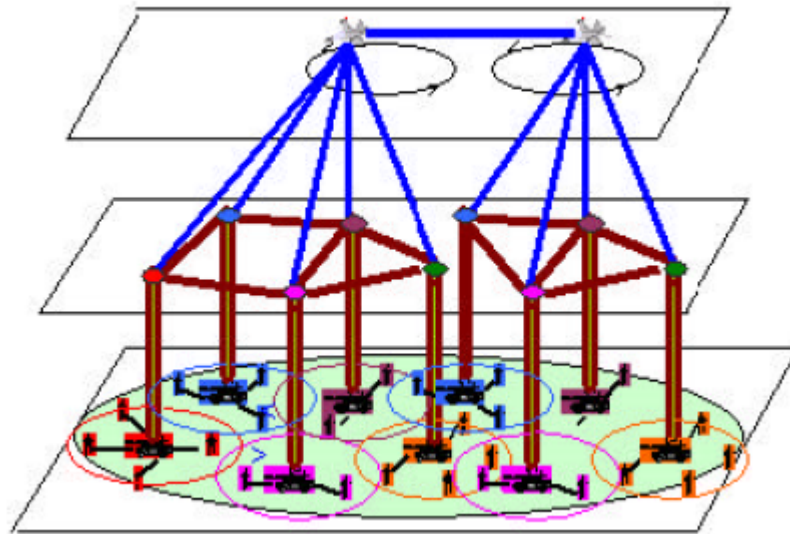
Figure 2.1 Multi-level Hierarchical Network [6]

2.3. Mobile Ad-hoc Network (MANET)

2.3.1. Overview

Wireless telecommunication continues to grow in popularity. One of the primary attributes gained by wireless communication is mobility. Currently world trends in communications issues are related to and driven by the mobile communications. We make a distinction between an infrastructured mobile network and infrastructureless mobile network [7].

The infrastructured network consists of mobile edge nodes, with access points and existing infrastructure linking them. In this network type, whenever mobile nodes travel from an access point to another access point, a handoff mechanism is needed for seamless network integration. But the access points themselves remained topologically fixed within the network hierarchy.

In stark contrast, mobile ad-hoc network (MANET)'s do not need (or assume) any preinstalled infrastructure network as mentioned. The goal of MANETs is to support mobile wireless networks [8], making it appropriate for small military communication or emergency systems. However, MANETs to date have not produced efficient transfer of information [9].

2.3.2. Features of MANETs

Most characteristics of MANETs are a result of node mobility.

(1) Dynamic topology caused by node mobility: Nodes in the MANET can move randomly and unpredictably, with resulting changes in the network topology.

(2) Energy-constrained network: Nodes in a MANET are usually battery-driven

hence they are typically energy limited.

(3) Bandwidth-constrained: Wireless links have lower capacity than wired links.

Their capacity is affected by interference, fading and noise, etc.

(4) Limited physical security: MANETs have more physical security threats than

wired networks due to the ease of intercepting a wireless link.

2.3.3. Routing Protocols in MANETs

Numerous routing protocols have been developed for mobile ad-hoc networks. Currently, MANET routing protocols are categorized into three categories: flat routing, hierarchical routing and geographic position assisted routing. This classification is shown in Figure 2.2.
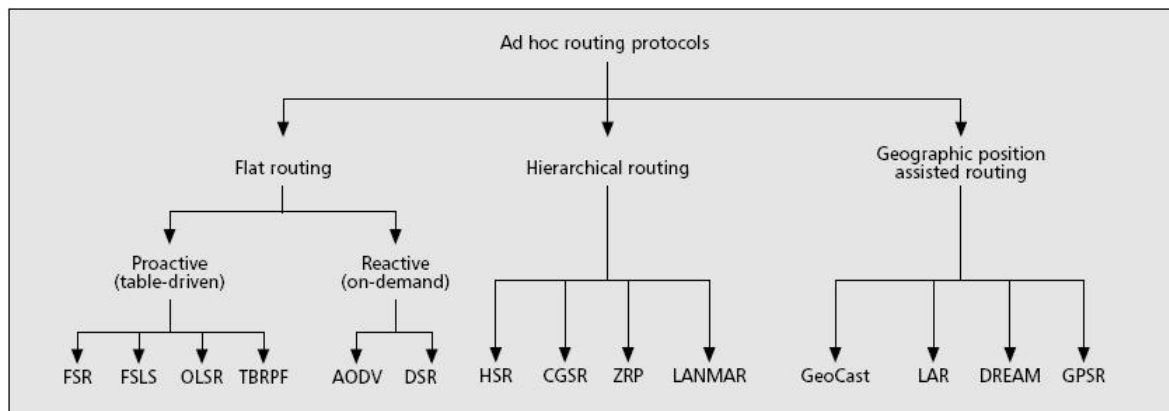
Figure 2.2 Classification of Ad-hoc Routing Protocols [10]

Flat routing is the traditional routing approach in MANETs. All nodes fulfill equivalent roles. If hierarchical routing is used, some nodes must adopt special roles.

Although hierarchical routing may be used, it does not imply a hierarchical addressing scheme. I.e., addresses are really just globally unique identifies, not addresses in the sense that routing can be inferred from portions of the address. Geographic position assisted routing is a routing protocol which considers the physical position of the node, usually with assistance from the Global Positioning System (GPS). In this paper, flat routing protocols are reviewed in detail.

2.3.4. Flat Routing Protocols

Flat routing protocols in MANETs are either proactive (table-driven) or reactive (on-demand). Conventional routing protocols use either link-state based or distance-vector based algorithms. Many proactive routing protocols use link-state routing, which maintains global network routing information by flooding routing information periodically. On the other hand, reactive protocols only perform routing activities as needed, i.e., on demand. Thus, no periodic routing information is maintained at each node.

Proactive routing protocols include Fisheye State Routing (FSR), Fuzzy Sighted Link State (FSLS), Optimized Link State Routing (OLSR), and Topology Broadcast, based on Reverse Path Forwarding (TBRPF). The common feature of proactive routing protocols is periodic routing information flooding in spite of no communication. Thus, nodes in proactive routing protocols constantly maintain routing entries for all nodes in the network. If node population is small, this is acceptable.

However, if the number of nodes is large, the routing table size becomes unmanageable. The message overhead also increases [10].

Reactive routing protocols include Ad-hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Temporally Ordered Routing Algorithm (TORA). The general characteristic of reactive routing protocols is that communication exists between nodes only as needed. When a node needs a route, the node invokes a route discovery phase. Route requests are broadcast into the network until the route is found or all possible paths are searched. Because reactive protocols must discover the routes, they typically suffer longer delays. However, unlike the proactive routing protocols, the routing overhead in reactive protocols is limited to maintenance of the routes currently in use. Thus, reactive protocols with large network populations are acceptable if the network has low mobility and light traffic with a small number of "conversations", i.e., communicating pairs. However, if node mobility

	FSR	OLSR	TBRPF	AODV	DSR
Routing philosophy	Proactive	Proactive	Proactive	On-demand	On-demand
Routing metric	Shortest path	Shortest path	Shortest path	Shortest path	Shortest path
Frequency of updates	Periodically	Periodically	Periodically, as needed (link changes)	As needed (data traffic)	As needed (data traffic)
Use sequence numbers	Yes	Yes	Yes (HELLO)	Yes	No
Loop-free	Yes	Yes	Yes	Yes	Yes
Worst case exists	No	Yes (pure LS)	No	Yes (full flooding)	Yes (full flooding)
Multiple paths	Yes	No	No	No	Yes
Storage complexity	$O(N)$	$O(N)$	$O(N)$	$O(e)$	$O(e)$
Comm. complexity	$O(N)$	$O(N)$	$O(N)$	$O(2N)$	$O(2N)$

Figure 2.3 Comparisons of Flat Ad-hoc Routing Protocols [10]

increases or the number of "conversations" grows, then routing overhead grows unacceptably large [10]. A comparison of flat routing protocols is shown in Figure 2.3.

2.4. Ad-hoc On-Demand Distance Vector Routing

2.4.1. Overview

The ad-hoc on-demand distance vector (AODV) routing is an on-demand routing protocol or reactive routing protocol. Routes to destinations are only established as required by a source node. The source and intermediate nodes maintain a route to the destination as long as it is needed. Hence, AODV routing protocol reduces the number of broadcasts for route discovery, only storing information for needed routing entries. The AODV routing protocol allows mobile nodes to enable dynamical multi-hop routing for new connections. More information on the ad-hoc on-demand distance vector routing protocol is found in [11].

2.4.2. Destination_Sequence_Number

As mentioned above, each AODV node maintains a routing table which includes the latest information for a particular destination. In the routing table, the Destination_Sequence_Number, is incremented whenever a node receives a new AODV routing control packet (RREQ, RREP, or RERR messages) which has a higher number than its current sequence number. The Destination_Sequence_Number is used to maintain the latest routing information in the ad-hoc network and to ensure all routes are loop free. This mechanism is explained below in detail.

2.4.3. Routing Table Management

Each routing table entry includes the following information: destination IP address, next hop node, Hop_Count (metric), Destination_Sequence_Number, list of precursors, and lifetime for the routing table entry.

When a node receives any AODV routing control packet, the node checks its own routing table entries related to the destination address in the routing control packet. If there is no entry for the destination address, the node creates a new routing entry for that destination. Otherwise, the routing entries are examined for possible update.

If the incoming Destination_Sequence_Number contained in the control packet is greater than the existing Destination_Sequence_Number in the routing table. If the incoming Destination_Sequence_Number is equal to the existing sequence number but the Hop_Count is smaller than the existing Hop_Count in the routing table, the table is updated with the new information contained in the control packet.

Each routing entry has a lifetime field. A routing entry expires when the node has not received any packet for that destination within the ACTIVE_ROUTE_TIMEOUT (The default value is 3,000 milliseconds). A routing entry is marked invalid after a route has expired or a link breaks.

2.4.4. Route Request (RREQ) Message

Route discovery occurs when a source node needs to send packets to a destination node and the source node doesn't have a routing entry for that destination.

The route discovery process continues until a route to the destination is found or when all possible routes have been checked. The route discovery process begins by broadcasting a route request (RREQ) packet. The format of a route request message is shown in Figure 2.4.

The Type field stands for AODV control packet types. The Hop_Count is set to zero initially, and incremented before nodes rebroadcast the RREQ to neighbor nodes in order to find path to the destination. The RREQ_ID is maintained by all individual nodes. The RREQ_ID is incremented whenever the node broadcasts a RREQ message. The pair of Originator_IP_Address field and RREQ_ID uniquely identifies a RREQ. When a node receives a RREQ already received with the same RREQ_ID and Originator_IP_Address, the node just drops the unnecessary RREQ message.

0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Type	J|R|G|D|U	Reserved	Hop Count
RREQ ID			
Destination IP Address			
Destination Sequence Number			
Originator IP Address			
Originator Sequence Number			
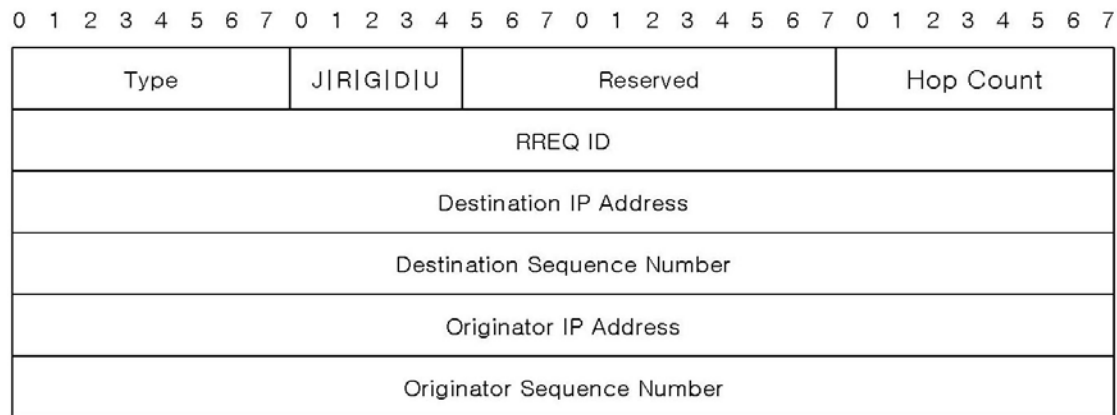
Figure 2.4 Route Request Message Format [11]

The last known Destination_Sequence_Number from the related routing table entries is contained in the Destination_Sequence_Number field. The source node generates an

Originator_Sequence_Number, used to maintain the latest information for the reverse path to the originator [12].

2.4.5. Route Reply (RREP) Message

If a RREQ message reaches the destination or an intermediate node which has a route to the destination, then that node sends a Route Reply (RREP) message back to the source node along the reverse path recorded as the RREQ messages flood the network. If the network does not support symmetric links, the destination node begins route discovery to the originator. The format of a route reply message is described in Figure 2.5.

0 1 2 3 4 5 6 7	0 1	2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Type	R|A	Reserved	Prefix Sz	Hop Count
Destination IP Address				
Destination Sequence Number				
Originator IP Address				
Originator Sequence Number				
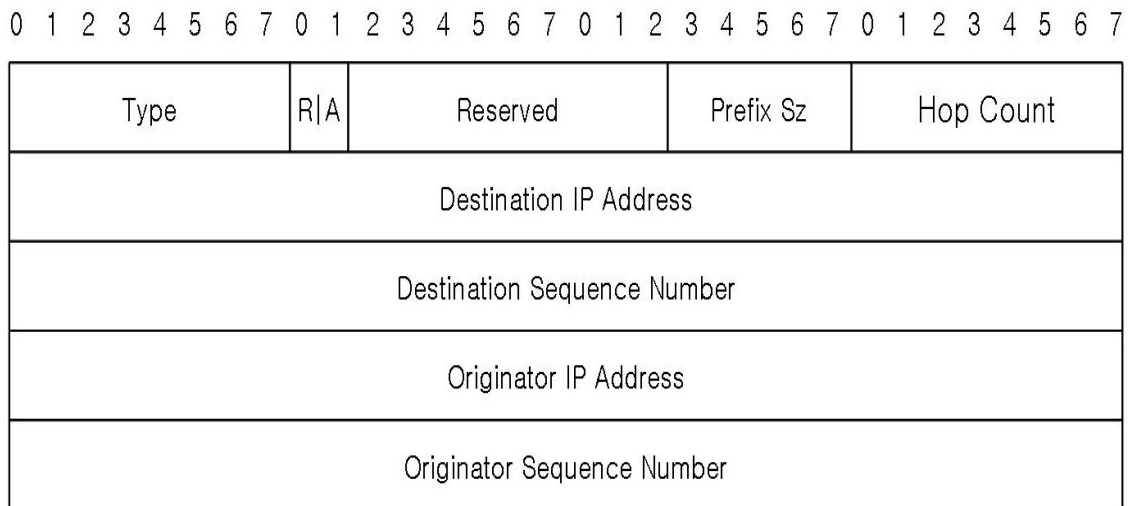
Figure 2.5 Route Reply Message Format [11]

Flag 'A' stands for requiring a route reply acknowledgement if a network link is unstable. A RREP message may be sent from the destination, or from an intermediate node which has a known route to the destination.

The destination sets Hop_Count to zero before it sends a RREP message to the originator. The Hop_Count is increment in the same as a RREQ message. The Destination IP Address field and Originator_IP_Address are copied from the RREQ message received. Before a RREP message is sent back to the originator, the destination checks its sequence number and the Destination_Sequence_Number field in the RREQ message. The destination updates its own sequence number and puts that number into a RREP message before sending the RREP message back to the originator if the Destination_Sequence_Number of the RREQ message is greater. The Lifetime field is set to MY_ROUTE_TIMEOUT by the destination. The default MY_ROUTE_TIMEOUT is 2 * ACTIVE_ROUTE_TIMEOUT.

When an intermediate node which has a routing entry to the destination receives a RREQ message, the node sets the Destination_Sequence_Number field to the number in its own routing table entry. The Hop_Count field is also set to the Hop_Count in the routing table in the same way. The Lifetime is the remaining lifetime of the route to the source of the RREQ.

Like the RREQ message, when an intermediate node receives the RREP messages, it sets up a forward path to the destination in the routing table. Every time the path is utilized, the lifetime of the route is reset. If the route is not used within the specified lifetime, it is removed.

2.4.6. Route Maintenance

When a network topology changes, immediate nodes which detect the link breakage broadcast a Route Error (RERR) message to its neighbor nodes. RERR messages are also broadcasted when a node receives a RERR message from a neighbor node. There are three ways to detect a link breakage: periodic Hello messages, link-layer ACK and failure to send a packet to the next hop. The format of Route Error (RERR) message is shown in Figure 2.6.

The DestCount field includes the number of destinations listed in the packet which generates a RERR message. The Unreachable Destination entries are marked as invalid. The entries will be deleted after DELETE_PERIOD time. The DELETE_PERIOD is K * max (ACTIVE_ROUTE_TIMEOUT, HELLO_INTERVAL) where K = 5 is recommended value. The HELLO_INTERVAL is explained later.

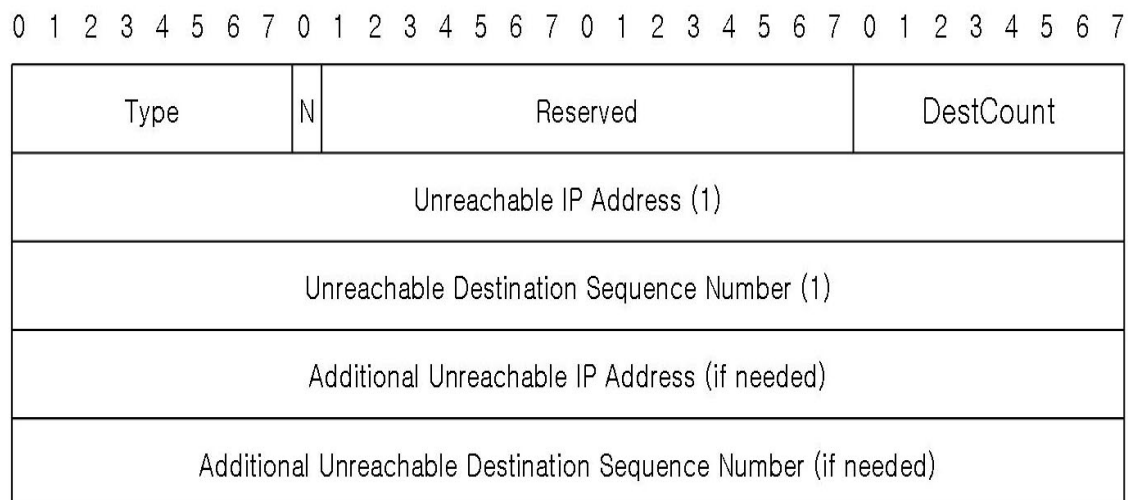| 0 1 2 3 4 5 6 7	0	1 2 3 4 5 6 7 0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Type	N	Reserved	DestCount
Unreachable IP Address (1)			
Unreachable Destination Sequence Number (1)			
Additional Unreachable IP Address (if needed)			
Additional Unreachable Destination Sequence Number (if needed)			

Figure 2.6 Route Error Message Format [11]

If a node detects a link breakage, the upstream node of the break broadcasts RERR messages with Hop_Count of infinity to all active upstream nodes. The RERR messages are broadcasted until all active source nodes are notified. After that, the originator restarts a new route discovery process as needed and broadcasts a RREQ message again.

2.4.7. Local Connectivity Management

A node maintains its neighbors by listening for HELLO messages from each node. HELLO messages are used to maintain connectivity of neighbor nodes. Each node checks if the node has broadcasted RREQ messages or other traffic every HELLO_INTERVAL times. (The default HELLO_INTERVAL value is 1,000 milliseconds.) If no message has been sent, the node broadcasts a Hello message with TTL = 1. If a node which does not have routes from the sender receives a Hello message, it creates new routing entry. If a route already exists, the lifetime of the routing entry is incremented accordingly to ALLOWED_HELLO_LOSS*HELLO_INTERVAL where the default value for the ALLOWED_HELLO_LOSS is 2.

2.5. Internet Protocol Version 6 (IPv6)

2.5.1. Overview

This description of the Internet Protocol version 6 (IPv6) is derived from [13]. The Internet has been based on the Internet Protocol version 4 (IPv4) but there are

some limitations expected for continuous growth of the Internet. One of the problems is that IPv4 addresses are exhausted rapidly and the number of hosts connected to the Internet is increasing by geometric progression. Routers in the Internet are overloaded since network fragmentations also increase in order to allocate insufficient IPv4 addresses to more networks. Thus, the Internet Protocol version 6 (IPv6) is designed as the successor to IP version 4 (IPv4).

2.5.2. Features of IPv6

The most remarkable difference between IPv4 and IPv6 is the length of the IPv6 address, which is extended to 128bits (from 32bits in IPv4). The following is a list of the principle new features of IPv6.

(1) Expanded address space: IPv6 increases the address space from 32bits to 128 bits in order to provide a large number of addressable nodes and more levels of addressing hierarchy. Figure 2.7 presents the IPv6 packet header structure.

(2) Packet size extension: The size of packets in IPv4 is limited to 64kB of payload. But, when the IPv6 option of "jumbograms" is used, specific hosts can transmit larger packets over this limit. Thus, it can support the improvement to use large bandwidth network efficiently.
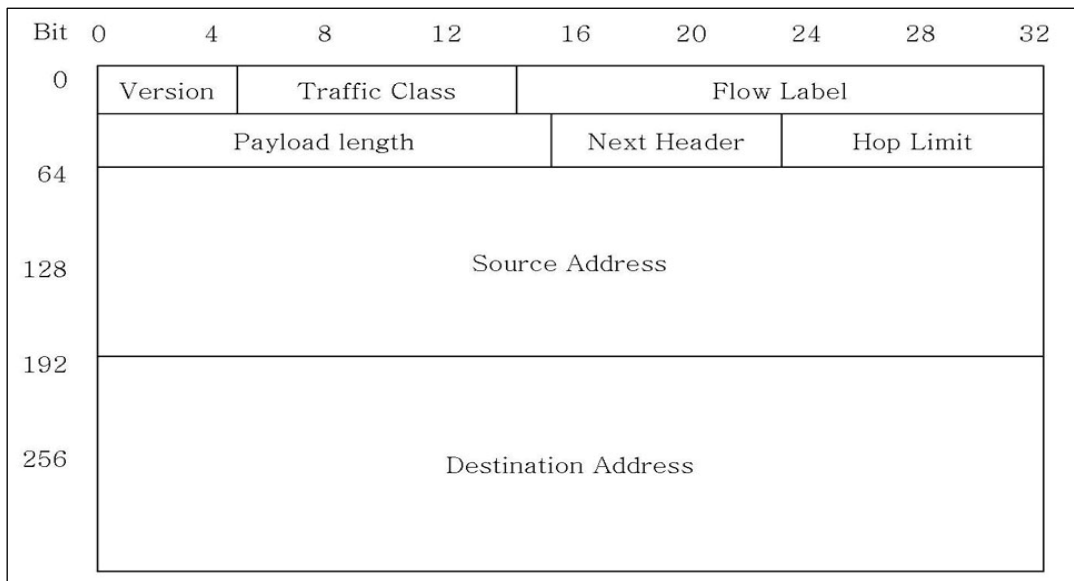
Figure 2.7 Structure of an IPv6 Packet Header [14]

(3) Stateless auto-configuration of hosts: IPv6 hosts can be configured automatically when it is connected to an IPv6 network.

(4) Flow labeling capability: This function is to enable the labeling of packets belonging to particular traffic flows to support quality of service guarantees, such as "real-time" service.

(5) Mobility support: IPv6 continues to support mobility (at the edge) through Mobile IPv6 (MIPv6), which operates similarly to Mobile IPv4.

2.5.3. IPv6 Addressing Architecture

The IPv6 addressing architecture is defined in [14]. The Internet Protocol version 6 addresses are 128-bit identifiers for interfaces. There are three kinds of addresses.

(1) Unicast: The unicast address is an identifier for a particular interface. A message transmitted to a unicast address is sent to the interface acknowledged by that address.

(2) Anycast: The anycast address is an identifier for a set of interfaces. Messages transmitted to an anycast address are sent to any one of the interfaces identified by that address.

(3) Multicast: The multicast address is also an identifier for a set of interfaces. Messages sent to a multicast address are delivered to all interfaces identified by that address.

An interface can be assigned multiple IPv6 addresses of any type (unicast, anycast, and multicast), but must have at least one link-local unicast address.

2.5.4. IPv6 Address Representation

IPv6 addresses can be represented as text strings in three ways.

(1) The basic form is x:x:x:x:x:x:x:x. Each 'x' represents a 16-bit number, typically written in hexadecimal.

(2) The longest string of zeros can be left out. For example, 0:0:0:0:0:0:0:1 and 0:0:0:0:0:0:0:0 may be represented as ::1 and :: .

(3) In a mixed network of IPv4 and IPv6, IPv4 address may be embedded into IPv6 address. For example, an IPv4 address of 13.1.68.3 can be embedded into an IPv6 datagram using the following address: 0:0:0:0:0:0:13.1.68.3 or ::13.1.68.3 .

2.5.5. Unicast Address Type

This research only uses unicast addresses. Thus, anycast and multicast address are not explained in any further detail. There are two types of unicast addresses in IPv6, link-local unicast address and global unicast address.

Link-local addresses are used for communicating with nodes directly connected. Link-local unicast address format is shown in Figure 2.8.

10 bits	54 bits	64 bits
1111111010	0	Interface ID

Figure 2.8 Link-Local IPv6 Unicast Address Format [14]

As shown above, the link-local addresses must start with the prefix 1111111010, which is FE80::/10 in Classless Inter-Domain Routing (CIDR) notation. The link-local address is used for the purposes of auto-configuration and neighbor discovery. Notice that any packets with link-local addresses must not be routed by routers.

Global unicast addresses are used for globally communicating with nodes. Global unicast address format is shown in Figure 2.9. The global unicast address starts with prefix 001.

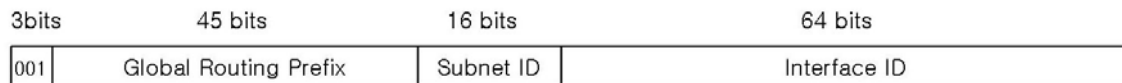| 3bits	45 bits	16 bits	64 bits
001	Global Routing Prefix	Subnet ID	Interface ID

Figure 2.9 Global IPv6 Unicast Address Format [14]

2.6. Summary

This chapter provides background information on hierarchical routing and mobile ad-hoc routing concepts. The Ad-hoc On-demand Distance Vector (AODV) routing protocol is explained in detail as it used in this research. Lastly, the Internet Protocol version 6 is introduced.

III. Methodology

3.1. Problem Definition

3.1.1. Goals and Hypothesis

Military communication systems for C^4I (Command, Control, Communications, Computers, and Military Intelligence) continue to require greater integration, principally achieved by interconnecting various elements through computer networks. While mobile ad-hoc networks (MANETs) represent one appropriate class of networks for these systems, the feasible network population supported by traditional MANET routing protocols is small compared to the number of nodes required for C^4I systems. For a large network, the excessive routing control message overhead is unsupportable and must somehow be reduced [10].

In contrast, a hierarchical routing scheme, based on hierarchical addressing, has lower routing overhead in a large-scale wireless network. However, it requires extra address management for mobile nodes. Thus, our goal is to find a way to combine flat ad-hoc routing protocols and hierarchical protocols to achieve a scalable routing scheme for large military networks.

In a military environment, hierarchical addressing related to military hierarchy and prescribed traffic plan by military orders may be exploited. A prescribed traffic plan, perhaps called a Communications Tasking Order, or a Network Tasking Order, might detail the messages one sender may send to a particular receiver and the receiver's expected movement (and thus the expected topological location) at any

particular time. This paper defines a plan to use such pre-planned knowledge. While hierarchical routing based on prior knowledge will certainly be efficient, it is clear that it will not be inherently robust, and mechanisms to support deviations from the plan must exist. For this research, we have chosen to use AODV to handle exceptional cases. Reactive routing protocols are more appropriate in this case because we expect to use them relatively rarely and do not wish to flood the network with numerous routing messages.

The goal of this research is to create and then analyze the performance of such a hybrid routing scheme. Hybrid routing utilizes hierarchical routing whenever possible, and reverts to a reactive ad-hoc routing protocol, AODV, whenever the hierarchical approach fails. Furthermore, this research compares the effectiveness of the hybrid routing to AODV routing protocol behavior.

In a large military system, the hybrid routing ought to experience lower routing overhead due to the fact that much of the routing information is known a priori. Routing overhead only occurs in exceptional cases, which we expect to be limited in number. We therefore expect "goodput" ratio to be high compared to any flat ad-hoc routing protocols. For packet end-to-end delay, the hybrid routing approach should also have better performance.

3.1.2. Approach

To analyze the hybrid routing scheme, we implemented it using the OPNET simulation tool. The hybrid routing mechanisms will be implemented as follows:

(1) All interface addresses of routers and hosts in the simulation area are assigned hierarchically and geographically in accordance with a military scenario. The Figure 3.1 presents how to assign addresses. All mobile receivers may be assigned multiple subnet prefixes (Network ID) with a unique interface ID for moving around in the simulation area.
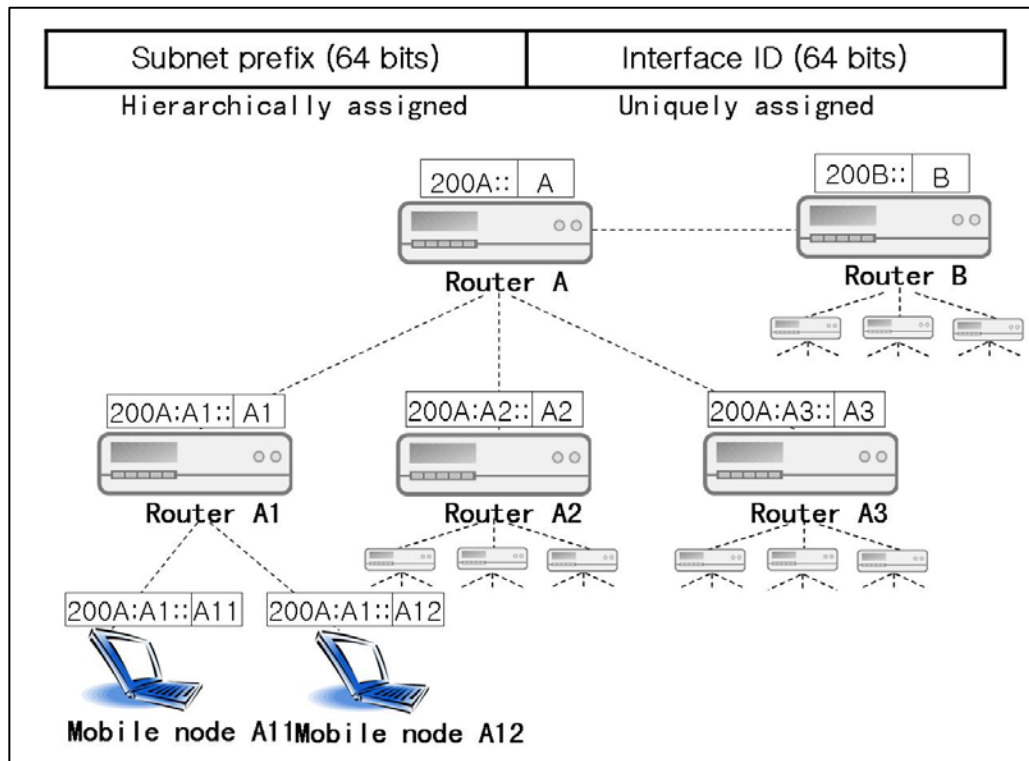

Figure 3.1 Interface Addresses Assignments

(2) All interface addresses are based on IPv6.

(3) All interfaces run the hierarchical static routing and AODV.

(4) Messages are first routed to receivers according to the pre-planned data.

(5) If the receivers do not follow the prescribed routes, hierarchal routing will fail, and AODV will recover the connection between senders and receivers.

The mechanism is explained specifically in (6) and (7).

(6) If the receiver does not follow the pre-planned paths, the router which expected to have the receiver connected will discover that the receiver is not connected, and will, in turn, generate an AODV Route Request message (RREQ) to discover a route to the receiver. After a connection is established between the router and the receiver (at its actual location, vs the pre-planned location), the message will be forwarded to the receiver. We refer to that as the recovered connection.
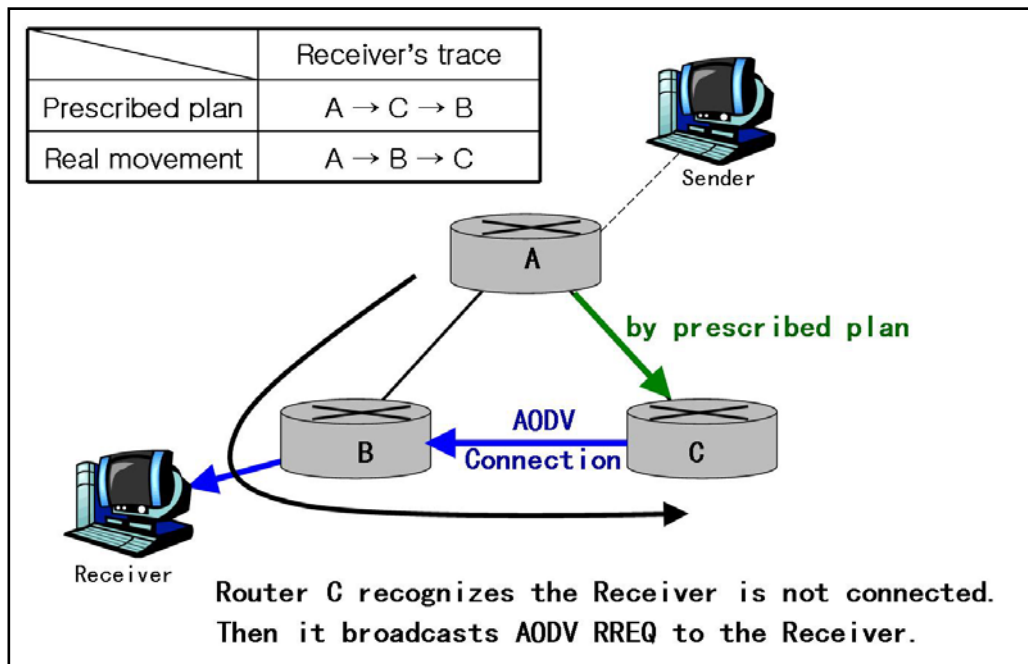

Figure 3.2 Recovered Connection

(7) An alternative method is that the receiver, knowing that it is not in the prescribed location, notifies the sender by sending AODV RREQ packets from its current location. Of course, this assumes that the receiver knew that the sender had messages to send to it. There are two ways to let the receiver broadcast RREQ to the sender. One is a trigger message generated by the router which discovers that the receiver is not at the pre-planned location. Whenever the receiver gets the trigger message from the router it sends a RREQ to the sender. Note that this approach was simulated in the experiments presented in Chapter 4. Another is that the receiver broadcasts RREQs if expected messages are not received by the prescribed time. After the connection is established, the traffic is transmitted directly to the receiver. This is shown in Figure 3.3.
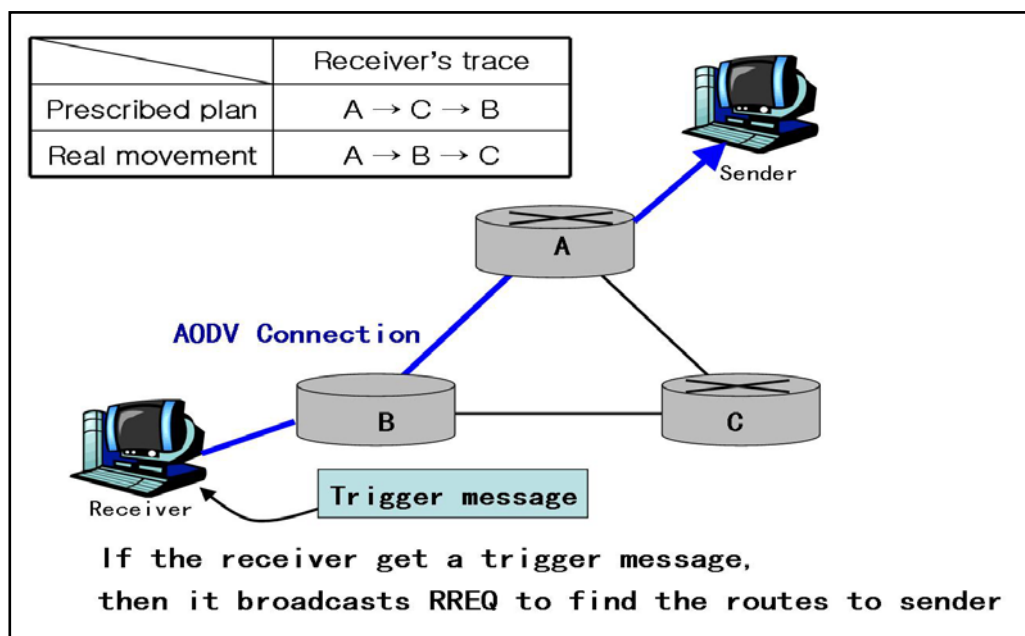

Figure 3.3 Receiver's Broadcast

(8) In this research, we assume that the receiver knows the time at which the messages generated by senders are intended to reach the receiver. The receiver generates AODV RREQs in order to discover the routes to the sender at that time. If the routes are established by AODV processes, then all messages generated by the sender are routed via AODV routing entries instead of static routing entries.

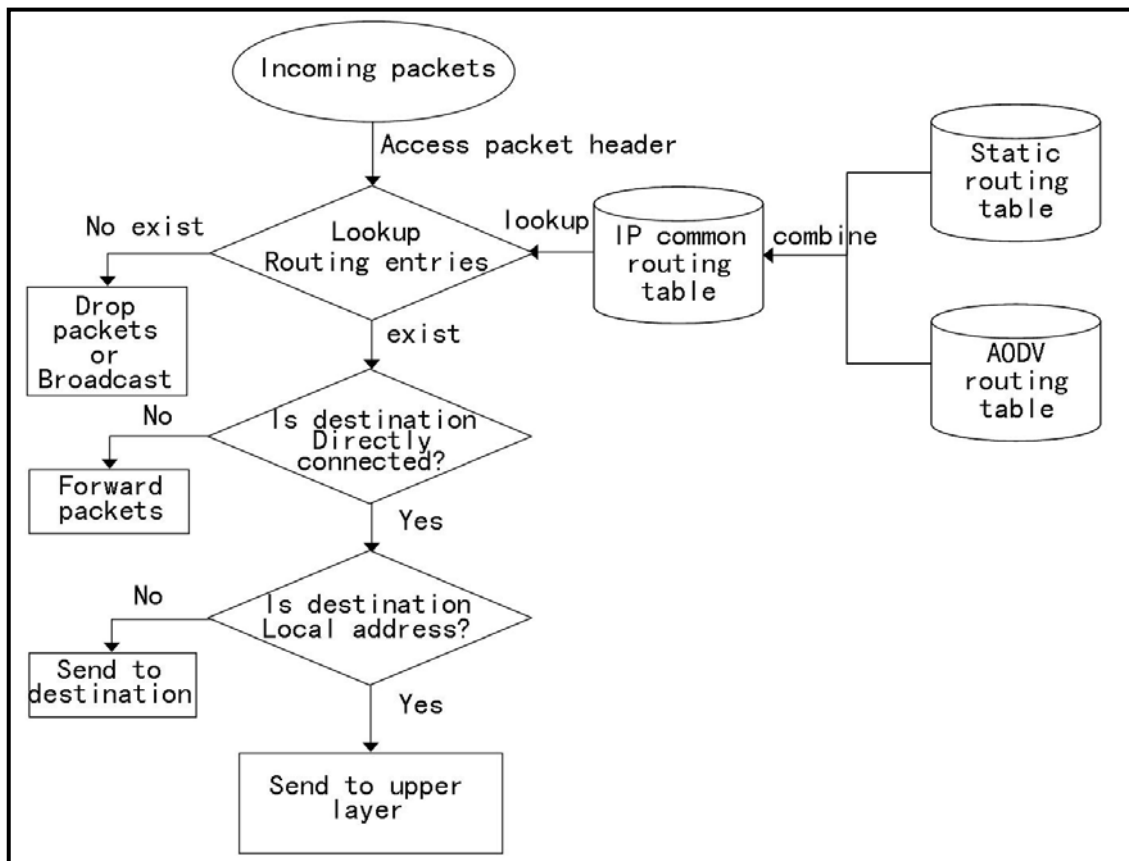(9) Packet processing on routers is as shown in Figure 3.4.

Figure 3.4 Packet Processing on Routers

Each router has a common routing table which combines AODV routing entries and static routing entries. For packet forwarding, a router searches the common routing table to find the appropriate outbound link to use. Note that if a match to the unique ID (second half of the IPv6 address) is made, the router uses that entry, which is derived from the AODV routing protocol. If no unique ID match is found, the search continues using the longest prefix matching scheme.

(10) The lookup method for a hybrid routing table is explained with an example in Figure 3.5. There are three simple subnets, A, B, and C. Routers which have two interfaces are directionally linked with each other. And each subnet has a network ID starting with 200A:x:x:x, 200B:x:x:x, and 200C:x:x:x, respectively. A receiver is expected to move from A to C via B based on a prescribed plan. The receiver will be assigned three different network IDs corresponding to the three subnets, each of which will include a unique ID. Every node can identify the receiver through the unique ID. Router A forwards packets generated by the sender through static routing entries if there is no AODV routing entry. If there is an AODV routing entry of the receiver, router A uses that AODV routing entry. Initially, all messages, according to pre-planned data are forwarded by the static entries. As failures occur, messages will be forwarded via AODV entries generated by the system because AODV entries have higher forwarding priority.
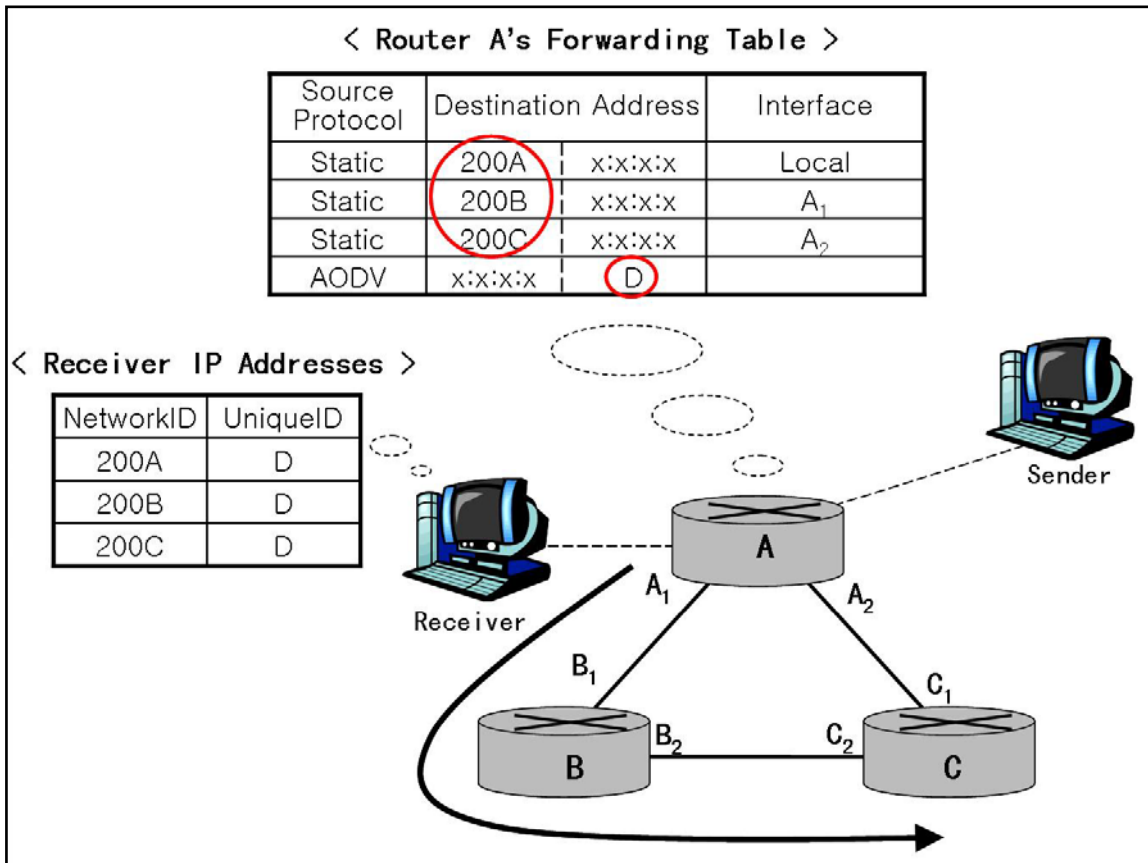
Figure 3.5 Lookup Hybrid Routing Table

To evaluate the hybrid routing, simulations are performed and statistics are collected. To compare the hybrid routing to a pure AODV routing protocol, three different networks using a military scenario are modeled.

3.2. System Boundaries

  The system under test (SUT) for this research contains mobile nodes within the mobile ad-hoc network. The components under test (CUT) include the AODV routing protocol, hierarchical routing, simulation area and mobility. The system under test is shown in Figure 3.6.

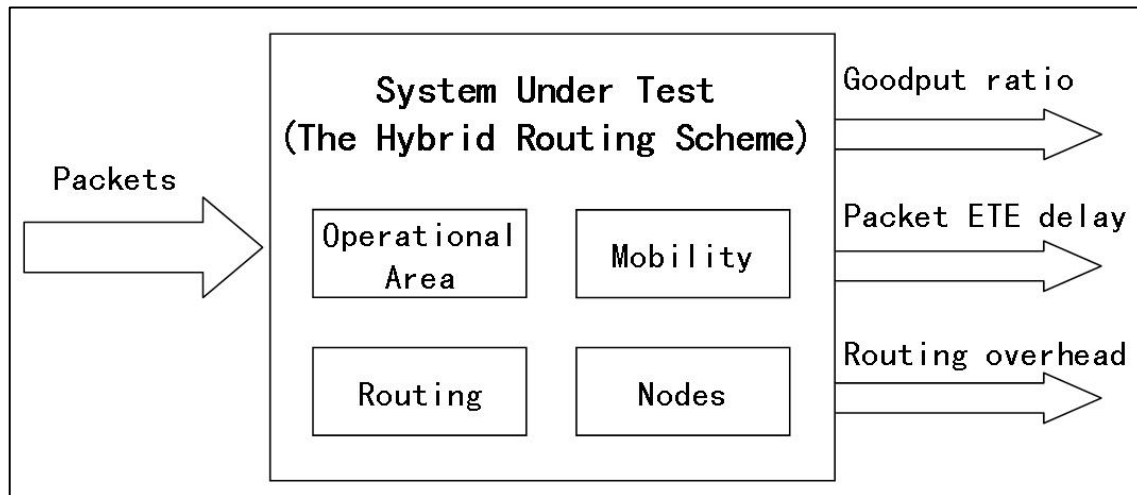Figure 3.6 System Under Test

3.3. System Services

  The system provides services of transmitting packets from sources to destinations. The outcomes of these services are successful packet transmission and failed packet transmission. Successful packet transmission is that the packet generated by a sender can reach a receiver without any error. Failed packet transmission is when the packet is dropped.

There are a number of causes for delivery failures. First is a result of a node moving out of another node's transmission range. If mobile nodes move frequently and rapidly, the network can become partitioned. Second, a wireless link may receive interference from other wireless devices. Third, due to limited link bandwidth, if too many packets flood the network, packets may be dropped.

3.4. Workload

The workload for this system is the packets transferred between mobile nodes and routers in a simulation network. These packets include payload (data) and routing protocol control information. Payload is the actual information for the user communication. In this research, traffic demands are generated from senders for user data. All traffic demand is generated according to a pre-planned scenario. Routing control information is used to discover new routes to destinations and to maintain connections. In this system, routing control traffic is generated by the AODV routing protocol processes.

3.5. Performance Metrics

The following performance metrics are used to evaluate the hybrid routing scheme and to compare that routing scheme to the performance of the AODV routing protocol.

(1) Goodput ratio: "Goodput" ratio is a ratio of successfully received data packets on the receivers to transmitted data packets and routing packets. The goodput ratio is defined as $Goodput = \dfrac{DPR}{DPT}$, where DPR is the number of data packets received by the receivers and DPT is the number of data and routing packets transmitted.

(2) Node pair end-to-end (ETE) delay (sec): Node pair end-to-End delay is the elapsed time from when a packet arrives at the originator to when the packet is received at the destination. Node pair ETE delay is the average time of all packet delays between a source and a destination.

(3) Routing traffic rate (bits/sec): This performance metric is used for measuring routing packet overhead. The routing traffic rate is defined as the number of routing control bits transmitted on all nodes per a second.

3.6. Parameters

The following parameters affect performance of the system under test (SUT).

3.6.1. System

(1) Link connection type: The network connections are bi-directional links. Although the AODV routing protocol prefers bi-directional links for discovering routes smoothly, it is not a requirement. In the simulation, it assumes all wired links between routers are bi-directional point-to-point

wireless links. The propagation delay of each link is set to one second.

(2) Node transmission range: The transmission range (radius) of all nodes in simulations is 540 meters. The transmission range is associated with node mobility and network contentions. If the transmission range of a mobile node is extended as wide as the entire network, the mobile node is not affected by disconnection caused by mobility.

(3) Node movement trajectory: In this research, all receivers follow traces based on a priori data. While the simulation injects errors in the pre-planned routes, the actual node trajectories are identical in all instances; only the predictions vary. In the simulations, a receiver (A2) moves from router A2 (R_A2) to router A3 (R_A3). The receiver node's trajectory is (R_A2)-(R_B1)-(R_B2)-(R_B3)-(R_C3)-(R_C2)-(R_C1)-(R_A3).   The   receiver starts to move at R_A2 and is intended to receive traffics from a stationary sender while moving among the other edge routers. (R_B1 to R_A3). The trajectory is shown later in Figure 3.7.

(4) Routing protocol: As mentioned in the previous section, the goal of this study is comparison of the hybrid routing scheme to AODV routing protocol. Thus, the simulations run two routing schemes separately.

(5) Node speed: The node speed affects the degree of the network topology changes. If the node speeds are higher, the network topology changes suddenly and rapidly. If the node speeds are lower, the topology of the network will change slowly. The rapid topology change causes poor goodput ratio and large routing overhead in AODV networks. In this simulations, a receiver moves at about 111 m/s to cause lots of traffic disconnections.

(6) Number of nodes: The number of nodes affects the degree of network congestion. In this research, 9 hosts and 12 routers are deployed. There is only one source node (sender) and a single destination node (receiver).

(7) Simulation area: The size of the simulation area is also related to the degree of traffic congestion with the number of nodes. In this research, the simulation area is 12x18 kilometers.

3.6.2. Workload

(1) Packet arrival rates: Packet arrival rates affect the performance metrics of throughput and routing overhead. A source node sends user data at a rate of 10 packets / sec in the simulations.

(2) Size of packets: Packet sizes of all traffic demands generated by source

nodes are 1024 bytes. Routing control message sizes vary. AODV routing

control packet sizes are defined in [11].

(3) Number of senders: The number of senders also affects the performance of

the network with packet arrival rate.

3.7. Factors

A key factor in this experiment is the correctness of pre-planned knowledge. The first simulation scenario is a network only based on AODV routing protocol. In the scenario, a source sends packets to a mobile receiver using AODV routing protocol only. The remaining scenarios are based on hybrid routing scheme with different percentages of correct predictions. Each percentage is the ratio of the amount of time that the receiver is located where the plan indicates. The 0% correctness of a priori means that the receiver does not follow prescribed routes at all. I.e., it is never where it is supposed to be. Hence, the receiver will not receive any packets unless the recovery is initiated by the AODV routing protocol. A 100% correct prediction means that the receiver can receive packets from sender without any help from the AODV routing protocol.

3.8. Evaluation Technique

There are three evaluation techniques: measurement, simulation and analytical model. The measurements have the most accurate and believable results. But, it is hard to measure directly due to environmental and outside factors. And measurements have the problems of flexibility and costs. The analytical model is also infeasible because MANET environment is too complicated to formulate. The most reasonable evaluation technique for this research is simulation. This research is evaluated by simulations in OPNET 12.0.

Figure 3.7 Network Scenario in OPNET
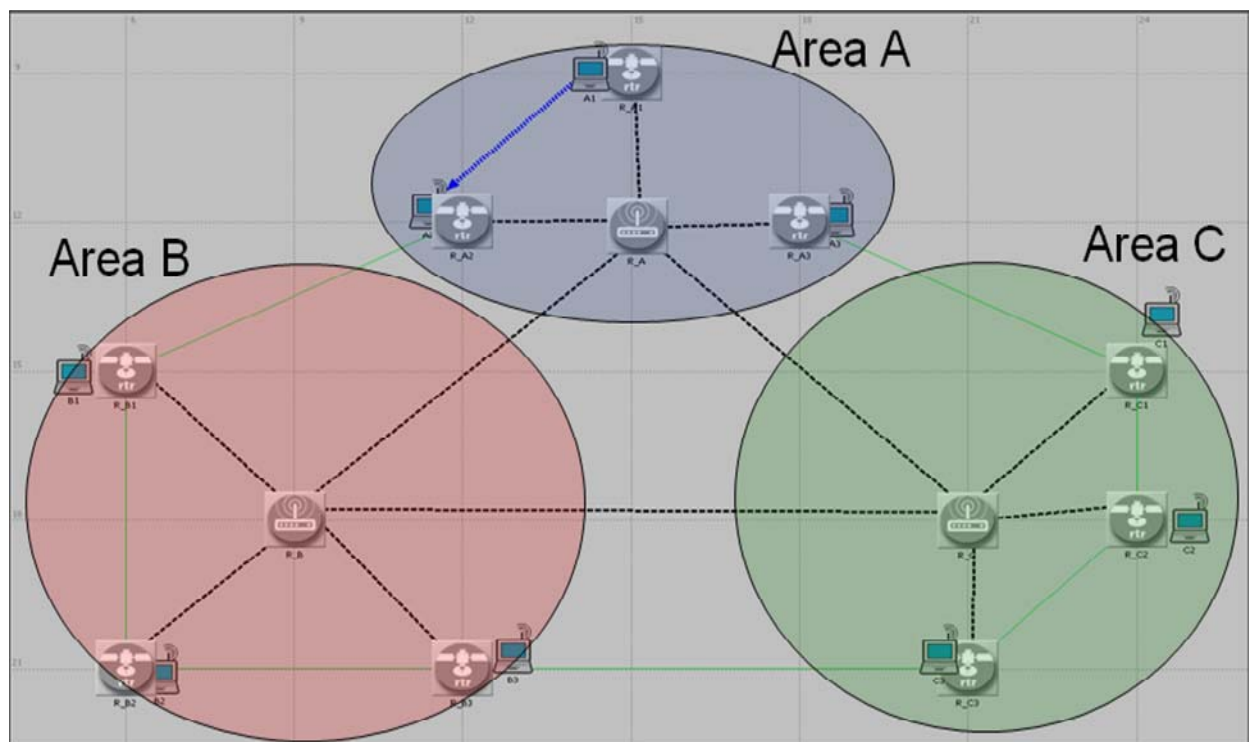
OPNET 12.0 has built in functions to implement a mobile ad-hoc network with typical MANET routing protocols such as AODV, DSR, TORA, OLSR and etc. It also supports mobility, defining trajectories for mobile nodes with a fixed speed. Figure 3.7 shows the network scenario in OPNET.

3.9. Experimental Design

For this experiment, there is only one factor used, namely the percentage of correct predictions. It requires 12 experiments (0%, 3%, 6%, 10%, 25%, 50%, 75%, 90%, 94%, 97%, 100%, and AODV only). No replication is required because the simulation is deterministic.

3.10. Summary

This chapter defines a methodology to evaluate the performance of the hybrid routing scheme and to compare it to the performance of a flat ad-hoc routing protocol, AODV. The major goal of this research and hypotheses are described in first part of this chapter. The essential part of the hybrid routing scheme is explained in this section. The formulation of this methodology section follows a systematic approach.

IV. Analysis and Results

4.1. Overview

This chapter includes results of this research and analyses of those results. The first three sections show network performances for different scenarios, AODV only, hybrid routing with 50% correct predictions, and hybrid routing with perfect prediction. The following sections contain an analysis of goodput ratio, node pair end-to-end delay, and routing traffic overhead.

4.2. AODV-Only Network Performance Analysis

4.2.1. Settings for AODV Implementation

In order to verify correct AODV behavior implemented in OPNET, AODV parameters which play important roles in AODV behaviors should be based on the most public description of AODV [11]. All simulations with different factors use the same settings of AODV parameters shown in Table 4.1.

Table 4.1 Settings of Major AODV Parameters

Parameter	Setting
Route Request Retries	5
Route Request Rate Limit (pkts/sec)	10
Active Route Timeout (sec)	3
Net Diameter	35
Node Traversal Time (sec)	0.04
Packet Queue Size (packets)	10

All AODV parameters follow the default OPNET implementation except Route_Request_Retries and Packet_Queue_Size parameters. The Route_Request_Retries and Route_Request_Rate_Limit are related to route discovery patterns. If route discovery takes a long time or fails, the packet may be dropped. The OPNET default setting allows more route request retries. The Route_Request_Rate_Limit is the same as [11] but Route_Request_Retries is 5 although [11] uses 2. There is no description about Packet_Queue_Size parameter in [11]. In simulations, 10 packet sizes are used.

A long Active_Route_Timeout causes a large number of stale routes. Thus, a packet sent by a stale route should be resent after the fresh routes are discovered or may be dropped.

4.2.2. Goodput

Figure 4.1 shows goodput for the network with only AODV routing protocol. The left graph and right graph show the transmitted traffic from a sender and received traffic by a correspondent, respectively. The wide blank spaces between large spikes in the graph of traffic received are caused by node mobility and wireless transmission range. It shows a large amount of packet loss if the receiver moves fast. The performance of AODV routing protocol is used for comparative criterion.
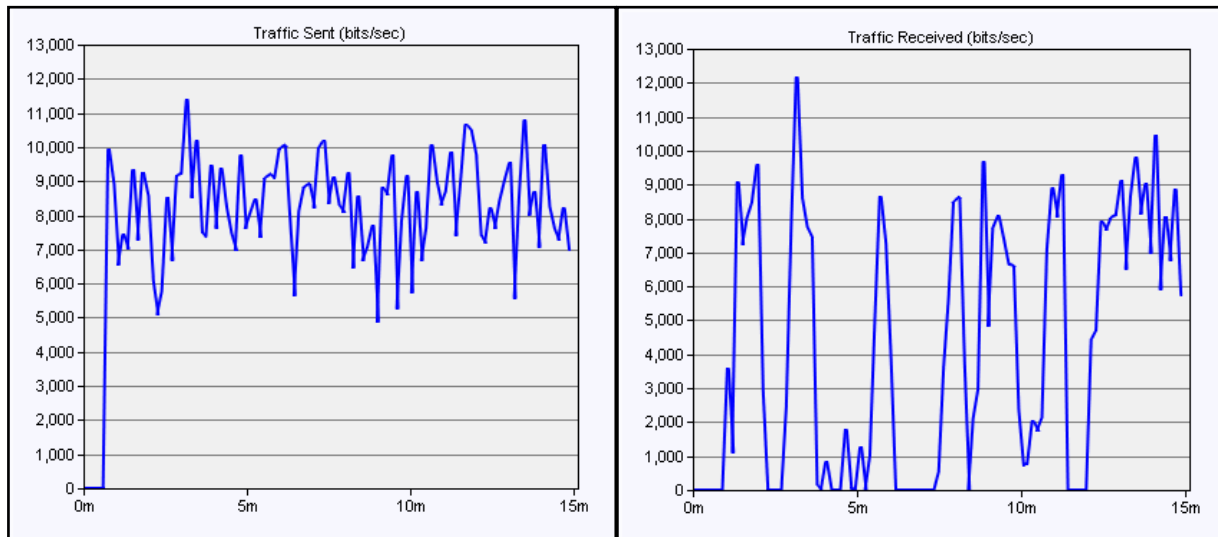
Figure 4.1 Goodput for AODV Routing Protocol Only

4.2.3. Node Pair End-to-End Delay

The packet end-to-end delay for a simulation using AODV only is shown in

Figure 4.2. The horizontal lines indicate normal packet end to end delay.
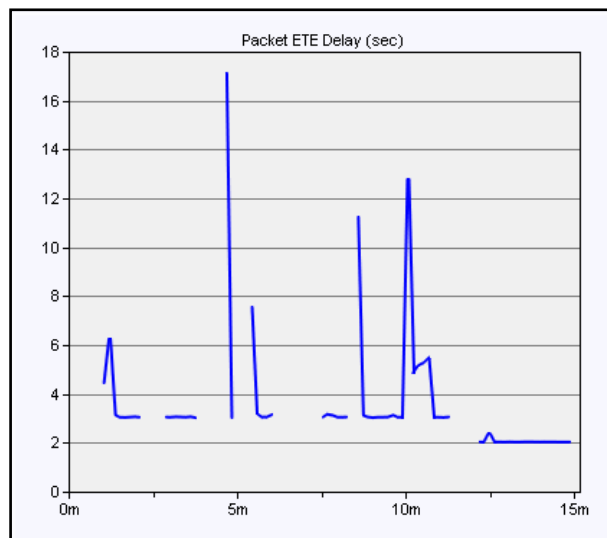

Figure 4.2 Node Pair ETE Delay for AODV Routing Protocol Only

4-3

Normally, the packet end to end delay is from 2 seconds to 3 seconds according to system propagation delay. The delay spikes above 3 seconds indicate that the route discovery mechanism increased the packet end to end delay to be longer. Note that these graphs show a time averaged end to end delay. Over time, as subsequent packets are able to utilize the discovered routes, the time-averaged delay approaches the delays expected via propagation. The AODV packet queue can hold the user traffic until the routes to the destination are found. But, after the fixed amount of time to discover the routes, all packets in the AODV queue are dropped.

4.2.4. Routing Packet Overhead

Figure 4.3 provides the routing packet overhead for the result using AODV routing protocol only. Routing packet overhead is measured by collecting the number of routing control bits transmitted on all nodes in the simulation area.
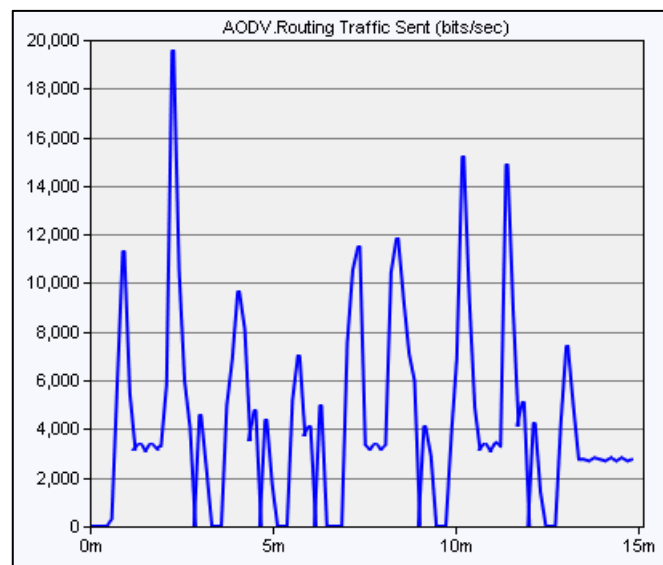

Figure 4.3 Routing Packet Overhead for AODV Routing Protocol Only

As seen in Figure 4.3, AODV routing traffic is transmitted for the entire simulation time. The AODV routing traffic is sent throughout the entire simulation due to frequent node movement.

4.3. Hybrid Routing with Perfect Prediction Performance Analysis

4.3.1. Goodput

Figure 4.4 shows goodput for the hybrid routing with 100% correct a priori. As seen the left graph of Figure 4.4., all traffics generated from the originator are fragmented at seven times because the receiver cannot receive any traffic when it is out of transmission range from wireless routers and the prescribed plan is the receiver moves through seven routers as mentioned in methodology. The only reason why the two graphs are different is caused by node transmission range and propagation delay.

Figure 4.4 Goodput for Hybrid Routing with Perfect Prediction

4.3.2. Node Pair End-to-End Delay

Figure 4.5 shows the packet end to end delay for the hybrid routing with perfect prediction. The graph indicates precisely the expected link propagation delays, which dominate the miniscule processing and queuing delays. As no recovery is needed in this baseline case, only link propagation delay affects the end-to-end delay in the perfect prescribed plan. The first six groups of end to end delays require three hops (hence 3 secs of propagation delay) and the last group indicates two hops, which is in accordance with the simulation setup.
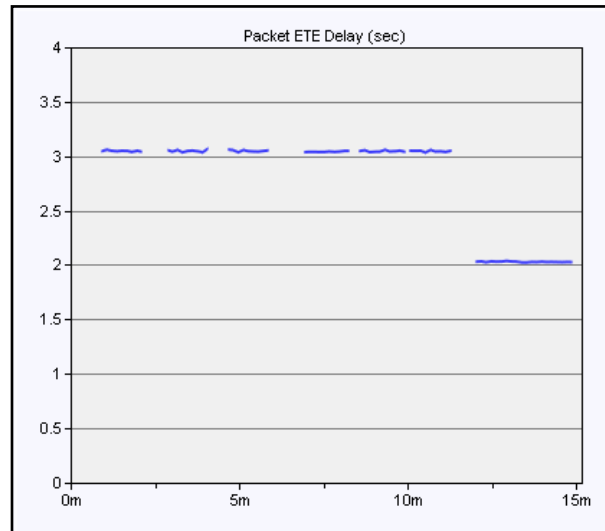

Figure 4.5 Node Pair ETE Delay for Hybrid Routing with Perfect Prediction

4.3.3. Routing Packet Overhead

Figure 4.6 shows the routing packet overhead for the network with the hybrid routing with 100% correct prediction. In this case, the sender does not send any traffic to the receiver via AODV routing entries. And the receiver also does not generate

RREQ messages because there is no exceptional case. But there are seven spikes in the graph because intermediate routers and the rest of hosts broadcast hello messages periodically for local link connectivity. The network topology changes slightly whenever the receiver connects a leaf router. Then, all intermediate nodes broadcasts connectivity information to the entire network.
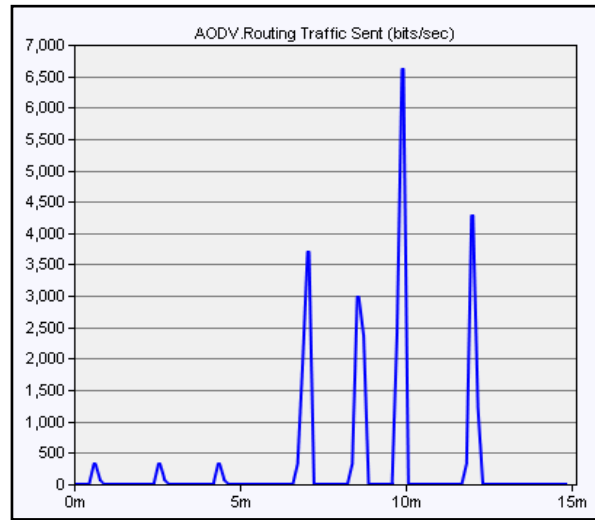

Figure 4.6 Routing Packet Overhead for Hybrid Routing with Perfect Prediction

4.4. Hybrid Routing with 50% Prediction Performance Analysis

4.4.1. Goodput

Figure 4.7 shows goodput for the hybrid routing with 50% prediction correctness, meaning that the source node sends traffics to incorrectly predicted locations for 50% of the simulation time, while correctly predicting the locations for

the other half of the simulation time. It assumes the receiver cannot receive the parts of planned traffics from first, third, fifth, and seventh routers (R_B1, R_B3, R_C2, and R_A3) in the simulation. The first spike of the traffic received graph means that AODV routing processes hold packets until route is discovered because the receiver is not on planned location.
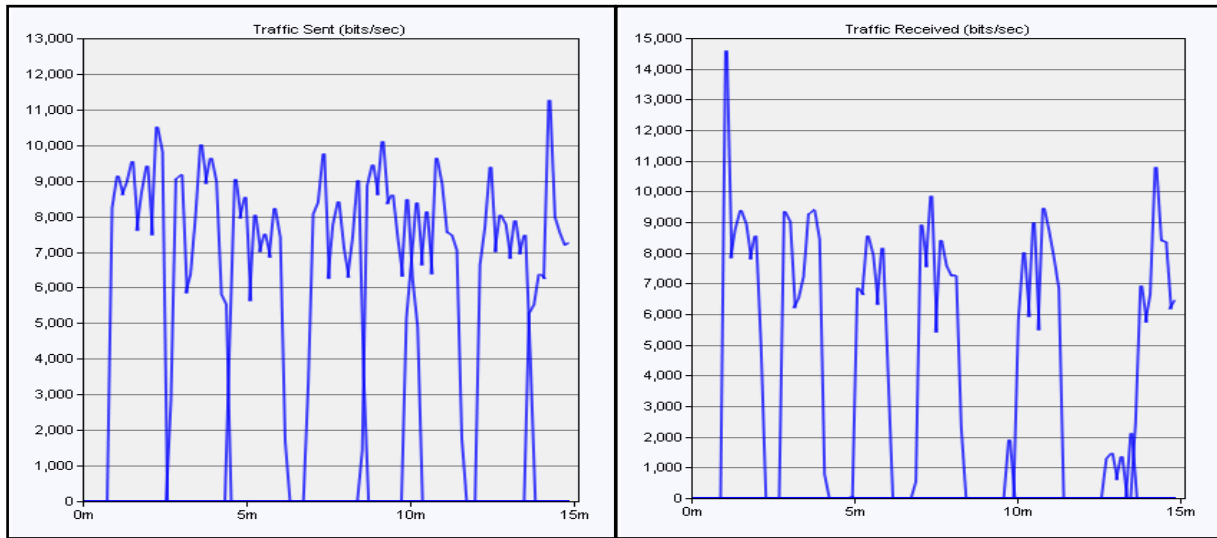

Figure 4.7 Goodput for Hybrid Routing with 50% Correct Prediction

4.4.2. Node Pair End-to-End Delay

Figure 4.8 shows the packet end to end delay for the hybrid routing with 50% correctly predicted destination locations. The horizontal lines indicate that the destination node is on the planned route. The spikes of this graph are caused by AODV route discovery processes. It holds the data packets until a route to the destination is discovered. The spaces between lines show packet losses caused by the node being out of transmission range or because the AODV route discovery fails.
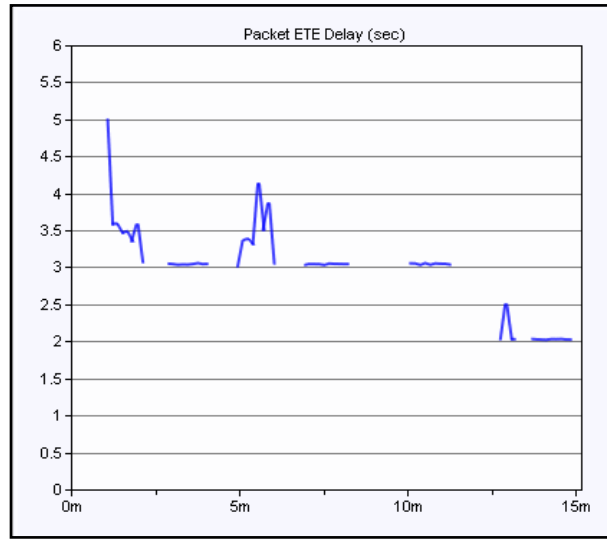
4-8

Figure 4.8 Node Pair ETE Delay for Hybrid Routing with 50% Correct Prediction

4.4.3. Routing Packet Overhead

Figure 4.9 shows the routing packet overhead for the network with the hybrid routing with 50% correct prediction.
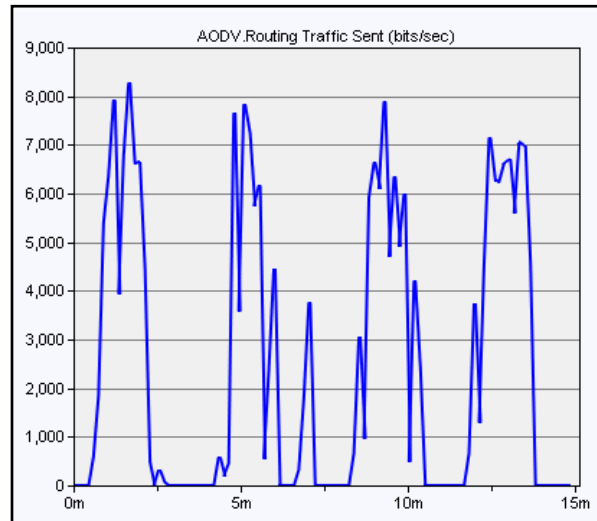

Figure 4.9 Overhead for Hybrid Routing with 50% Correct Prediction

In this case, the receiver tries to discover routes to the sender at first, third, fifth, and seventh routers in order to receive the generated messages from the sender. Thus, Figure 4.9 indicates a large amount of AODV routing traffic sent to locate the receiver.

4.5. Goodput Ratio Analysis

Goodput ratio measures the ratio of user data bits successfully received on a mobile receiver relative to bits transmitted on a sender. Figure 4.10. shows goodput ratio for AODV routing protocol and the hybrid routing protocol. As seen in Figure 4.10, the hybrid routing models with more than 25% correct a priori have significantly higher goodput than AODV routing protocol.
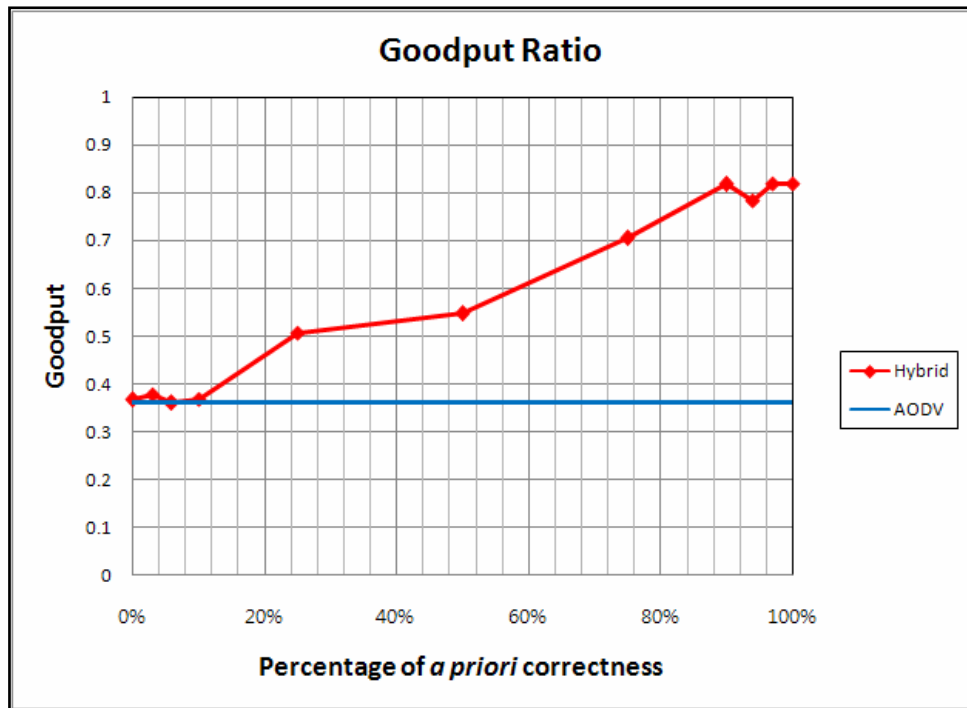

Figure 4.10 Comparison of Goodput Ratio

The traffic forwarded by pre-planned hierarchical static routing table may reach the wrong destination if the receiver follows the routes based on incorrect predictions. Then, the receiver generates AODV RREQ packets to find the routes between the sender and the receiver. Thus, if a significant amount of predictions are wrong, lower than 10% correctness of a priori, goodput ratio is the same (or perhaps worse) than the network with AODV only. The well-planned traffic demands and fast route recovery mechanisms when the receivers are on a wrong way are two critical parts in this hybrid routing scheme.

4.6. Node Pair End-to-End Delay Analysis

Node pair end-to-end delay measures the time it takes to transmit packets between a source and a destination. Figure 4.11 shows packet ETE delay for AODV routing protocol and the hybrid routing scheme

As seen in Figure 4.11., the hybrid routing models with more than 25% correct predictions have lower end-to-end delay than the AODV only routing protocol because the major parts of traffics are transmitted via hierarchical static routing tables. It doesn't need to be delayed to transmit packets. If no recovery is required, only the propagation delay influences the packet end-to-end delay.
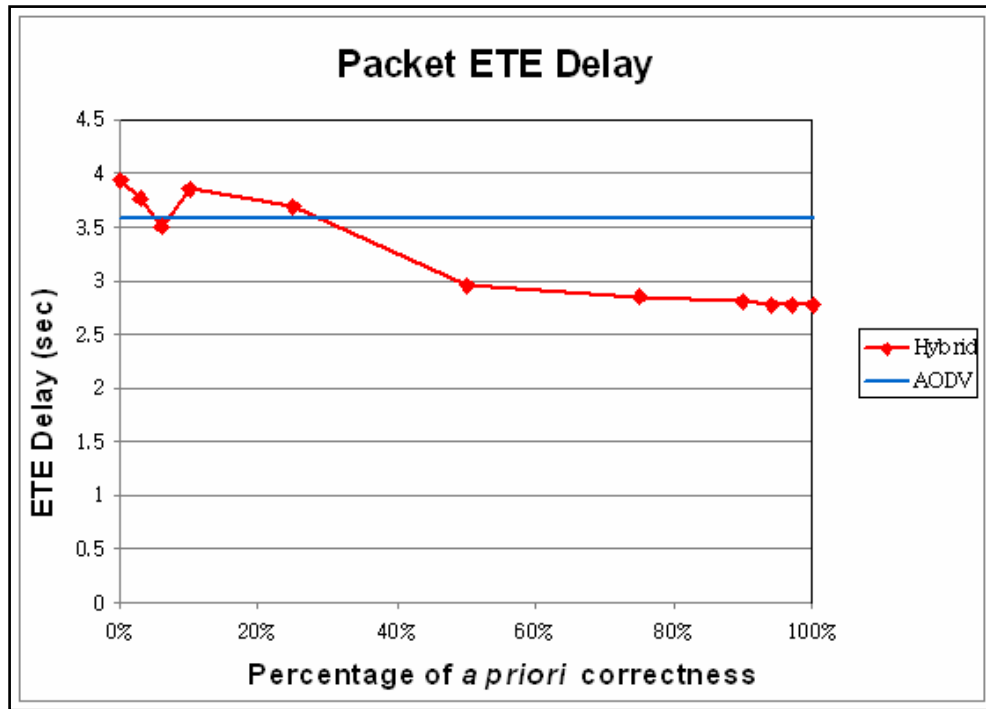
Figure 4.11 Comparison of Node Pair ETE Delay

4.7. Routing Packet Overhead Analysis

Routing packet overhead is the AODV routing control packets transmitted by all nodes in the network. Figure 4.12 presents routing packet overhead for the AODV routing protocol and the hybrid routing scheme.

The hybrid routing scheme with higher percentage of correct prescribed plan generates lower routing traffic overhead. A plot for 6% correctness is residual. However, the entire hybrid routing schemes with any different correctness of a priori have lower routing traffic overhead than an AODV only network.

In conclusion, the hybrid routing scheme can transmit packets to the destination with minimum packet losses and packet delay using significantly lower routing overhead if a priori knowledge is well planned.
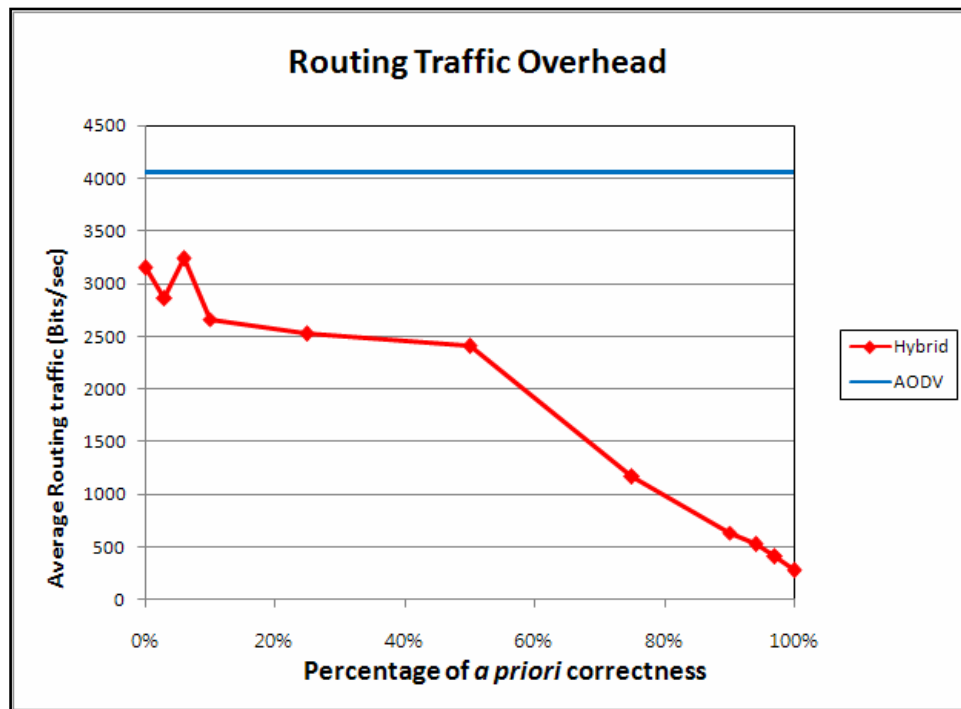

Figure 4.12 Comparison of Routing Packet Overhead

4.8. Summary

This chapter provides the performance of AODV only network and the hybrid routing with 100% and 50% correctness of a priori data. Next, the results of performance metrics with various percentages of a priori correctness are presented and compared to AODV performance.

V. Conclusions and Recommendations

5.1. Overview

This chapter provides a summary of the research problem, the research conclusion and significance, and the recommendations for future research.

5.2. Problem Summary

To implement a large mobile ad-hoc network for military communication, there is a scalability issue concerned with excessive routing control overhead due to inherent limitations of MANETs, low bandwidth and energy constrained. A hierarchical routing scheme, based on hierarchical addressing, has a major solution for the scalability problem of MANETs. But it has also disadvantages for dynamic topologies. To solve the scalability issue for the large military communication is to implement a hybrid routing which combines the salient features of the two routing schemes. In order to implement the hybrid routing scheme, *a priori* knowledge is prerequisite element. Since a priori data is the core of the hybrid routing scheme, tests should use different correct portions of a priori knowledge as a factor.

5.3. Conclusions of Research

The performance of the hybrid routing scheme is dependent on *a priori* knowledge. The hybrid routing scheme with 25% or more correctness of a priori knowledge has better performance metrics than Ad-hoc On-demand Distance Vector

routing protocol for goodput ratio and end-to-end delay. But, the routing traffic overhead of the hybrid routing scheme is always lower than AODV.

5.3. Significance of Research

This research is a new attempt to combine a hierarchical routing scheme and a MANET routing scheme for a specific network environment. The new hybrid routing scheme is a robust and effective routing way for large military networks compared to a flat ad-hoc network routing.

5.4. Recommendations for Future Research

This research has some limitations. All network cores which are intermediate routers are fixed each other due to difficulty to implement wireless directional links based on the node mobility. In this simulation, only network edges are mobile. This is not realistic because all nodes should be mobile in military networks.

There is a source node and a destination node is used in the simulation. And the mobility pattern is also simple. Future works should consider different mobility pattern like group mobility. And future experiments should be extended to significantly large network sizes with large amount of traffics.

Lastly, there are many ways to recover the incorrectly predicted cases as mentioned in Chapter 3. This research assumed the receiver knows the time at which the receiver generates RREQ messages. But, it should be generated by a trigger message or different recovery mechanisms. Future research should discover the optimal recovery mechanism as mentioned above or from new idea.

5.5. Summary

System integration is one of the trends for computer communications. There is no exception in military networks. MANETs are a suitable scheme for networks with restricted resources and special requirements such as military networks. However, there are scalability issues for a large mobile ad-hoc network. This research presents one effective way to solve the scalability issue as implementing a hybrid routing scheme.

Bibliography

[1] David Groth, Toby Skandier, "Network Study Guide, Fourth Edition," SYBEX Inc., 2005.

[2] L. Kleinrock and F. Kamoun, "Hierarchical Routing for Large Networks: Performance Evaluation and Optimization," Computer Networks, Vol. 1, pp. 155-174, 1977.

[3] Kelvin Fall, "A delay-tolerant network architecture for challenged Internets," SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, pp. 27-34, 2003.

[4] G. Malkin, T. LaQuey Parker, "Internet User's Glossary," Internet informational RFC 1392, January 1993.

[5] C. Perkins, "IP Mobility Support for IPv4," Network Working Group, Request for Comments 3344, August 2002.

[6] K. Xu, X. Hong, M. Gerla, H. Ly, and D. L. Gu, "LANDMARK ROUTING IN LARGE WIRELESS BATTLEFIELD NETWORKS USING UAVS," 2001.

[7] Elizabeth. M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," IEEE personal Communications, April 1999.

[8] S. Corson, J. Macker, "Mobile Ad-hoc Networking (MANET) : Routing Protocol Performance Issues and Evaluation Considerations," Network Working Group, Request for Comments 2501, January 1999.

[9] Gupta, P. and P.R. Kumar. "The capacity of wireless networks," Information Theory, IEEE Transactions, 46(2): 388-404 (March 2000).

[10] Xiaoyan Hong, Kaixin Xu, and Mario Gerla, "Scalable Routing Protocols for Mobile Ad-Hoc Networks," IEEE Network, July/August 2002.

[11] C. Perkins, E. Belding-Royer, and S. Das, "Ad-hoc On-Demand Distance Vector (AODV) Routing," Network Working Group, Request for Comments 3561, The Internet Society, July 2003.

[12] Charles E. Perkins, Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector Routing,"wmcsa, p.90, Second IEEE Workshop on Mobile Computer System and Applications, 1999.

[13] S. Deering, R. Hinden "Internet Protocol, Version 6 (IPv6) Specification", Network Working Group, Request for Comments 2460, December 1998.

[14] R. Hinden, S. Deering "IP Version 6 Addressing Architecture", Network Working Group, Request for Comments 4291, February 2006.

Vita

      Captain Heungsoon Park was born in Seoul, Korea. After completing his work at Jang-Hoon High School, Korea in 1998, he went on to the Korea Military Academy in Seoul, Korea where he received his Bachelor of Science in Computer Sciences in March 2002. He has been a member of Republic of Korea Army (ROKA) since his graduation. For the next three years he pursued a career in computer science, managing for C4I systems and networks in Korea. In August 2005 he entered the Air Force Institute of Technology at Wright Patterson Air Force Base in Dayton, Ohio.

1. REPORT DATE (DD-MM-YYYY) 22-03-2007	2. REPORT TYPE Master's Thesis	3. DATES COVERED (From – To) Aug 2005 – Mar 2007

4. TITLE AND SUBTITLE EFFECTIVE MOBILE ROUTING THROUGH DYNAMIC ADDRESSING	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Park, HeungSoon, Captain, ROKA	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management(AFIT/EN) 2950 Hobson Way, Building 640 WPAFB OH 45433-8865	8. PERFORMING ORGANIZATION REPORT NUMBER AFIT/GCS/ENG/07-09

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Dr. David R. Luginbuhl (703) 696-6207 AFOSR 876 North Randolph Street Arlington, VA 22203-1768 David.luginbuhl@afosr.af.mil	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Military communications has always been an important factor in military victory and will surely play an important part in future combat. In modern warfare, military units are usually deployed without existing network infrastructure. The IP routing protocol, designed for hierarchical networks cannot easily be applied in military networks due to the dynamic topology expected in military environments. Mobile ad-hoc networks (MANETs) represent an appropriate network for small military networks. But, most ad-hoc routing protocols suffer from the problem of scalability for large networks. Hierarchical routing schemes based on the IP address structure are more scalable than ad-hoc routing but are not flexible for a network with very dynamic topology. This research seeks a compromise between the two; a hybrid routing structure which combines mobile ad-hoc network routing with hierarchical network routing using pre-planned knowledge about where the various military units will be located and probable connections available.

This research evaluates the performance of the hybrid routing and compares that routing with a flat ad-hoc routing protocol, namely the Ad-hoc On-demand Distance Vector (AODV) routing protocol with respect to goodput ratio, packet end-to-end delay, and routing packet overhead. It shows that hybrid routing generates lower routing control overhead, better goodput ratio, and lower end-to-end packet delay than AODV routing protocol in situations where some *a-priori* knowledge is available.

15. SUBJECT TERMS
Mobile Ad-hoc Network, Hierarchical addressing, Dynamic addressing, Mobility

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Scott Graham , Major, USAF (ENG)
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U	UU	71	19b. TELEPHONE NUMBER (Include area code) (937) 255-6565, ext 4918 (Scott.Graham@afit.edu)