석사학위 논문

An Efficient On-Demand Multipath Routing in Wireless Ad Hoc Network

제주대학교 대학원

전산통계학과

Abhijit Saha

2007 년 12 월

An Efficient On-Demand Multipath Routing in Wireless Ad Hoc Network

Abhijit Saha
(Supervised by Professor Gyung-Leen Park)

A thesis submitted in partial fulfillment of the requirement for the degree of
Master of Science

December 2007

The thesis of Abhijit Saha is approved:

Professor Cheol-Soo Kim, Chair

이윤정

Professor Yoon-Jeong Lee

Professor Gyung-Leen Park

Department of Computer Science and Statistics
Graduate School
Cheju National University

An Efficient On-Demand Multipath Routing in Wireless Ad Hoc Network

A thesis submitted in partial satisfaction
of the requirements for the degree of
Master of Science
In
Computer Science and Statistics
by
Abhijit Saha
(Supervised by Professor Gyung-Leen Park)

Department of Computer Science and Statistics
Graduate School
Cheju National University
December 2007

An Efficient On-Demand Multipath Routing in Wireless Ad Hoc Network

Abhijit Saha

ABSTRACT OF THE THESIS

An ad hoc network consists of a collection of wireless nodes that are capable to communicate with each other without any fixed based-station infrastructure and centralized management. All nodes can be mobile and the topology changes frequently. Each mobile node can operate as a host and as a router, indicating that all of them take equal roles.

In ad hoc networks, the responsibility of routing protocol includes exchanging the route information; finding a feasible path to a destination based on criteria such as hop length, minimum power required, and lifetime of the wireless link; gathering information about the path breaks; repairing the broken paths expending minimum processing power and bandwidth. Minimal control overhead, minimal processing overhead, quick route reconfiguration, and loop prevention are the major requirements of a routing protocol in ad hoc wireless networks.

This thesis proposes an on-demand Directional Node-Disjoint Multipath Routing (DNDMR) protocol for the wireless ad hoc network. Multipath routing inherently allows the establishment of multipath or multiple routes between a single source and single destination. The important components of the protocol, such as path accumulation with a novel directional method, reducing routing overhead by controlled propagation, and ensuring the node-disjoint paths automatically, are explained. DNDMR improves the reliability of data communication (i.e., fault tolerance) over the wireless ad hoc network. Because DNDMR significantly reduces the total number of Route Request (RREQ) Packets, this results in lower control traffic overhead, smaller end-to-end delays, and better throughput. We evaluate the performance of the proposed scheme with ns-2 simulator and compare its performance with existing unipath routing protocols (DSDV, DSR, and AODV), and multipath routing protocol (AOMDV). Control traffic overhead, end-to-end delay, and throughput metrics are considered for the evaluation. In case of control traffic overhead, the cumulative packets for all mentioned protocols at the end of simulation time are: DSDV (6000 packets), DSR (5000 packets), AODV (2600 packets), AOMDV (2700), and DNDMR (2300 packets), whereas DNDMR is comparatively less than the other protocols. In case of end-to-end delay, DNDMR is faster than DSDV (3.25 times), DSR (3 times), AODV (3.5 times), and AOMDV (2 times). Also, analysis shows that DNDMR throughput is better than the other mentioned protocols. The experimental results reveal that DNDMR has better performance and more reliable than the contemporary unipath and multipath routing protocols.

Keywords: Wireless Ad hoc Network, Routing Protocols, Unipath and Multipath Routing Protocols.

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Motivation

Wireless Networking is gaining large attention and becoming very popular these few years, due to its potential and possibilities. Infrastructure networks and mobile ad hoc networks are two main architectures of wireless networking. Infrastructure networks include cellular networks and wireless local area network. Users are connected via base stations/access points, and backbone networks. Ad hoc network is a recent developed part of wireless communication. The difference from traditional wireless networks is that there is no need for established infrastructure. Since there is no such infrastructure and therefore no preinstalled routers, which can forward packets from one host to another, this task has to be taken over by mobile nodes, of the network.

The main objective of ad hoc routing protocol is finding a short and optimized route from the source to the destination node without predetermined topology or centralized control. All nodes are mobile and topology changes frequently. Design issues for developing a routing protocol for wireless network is much complicated than those of wired network. Therefore, routing protocol is a challenging issue in wireless ad hoc network communication.

Routing protocols can be classified either as proactive or reactive. Reactive or on-demand routing protocols consume less bandwidth than proactive protocols. On-demand routing protocols have some limitation that all of them build and transmit on a unipath route for each data session. When there is a link break on the active route, all of them have to invoke a route discovery process. By establishing multiple paths between a source and a destination in a single route discovery, on-demand multipath routing protocols can alleviate these problems. Path rediscovery needs to initiate only when there is no path available from source to destination. In this thesis, an efficient on-demand Directional Node-Disjoint Multipath Routing (DNDMR) Protocol is proposed. DNDMR has two novel aspects compared with contemporary unipath and multipath routing protocols. It reduces the routing overhead significantly and achieves multiple node-disjoint routing paths efficiently.

1.2 Contributions

As the objective of this thesis, multipath routing of wireless ad hoc networks are addressed. The major contributions of this work can be summarized as follows:

- Get a general understanding of wireless ad hoc networks and wireless ad hoc networks routing.
- Directional Node-Disjoint Multipath Routing (DNDMR) protocol with very low control traffic overhead or routing overhead compared with contemporary unipath and multipath routing protocols is proposed. It has two novel aspects in that it reduces the routing overhead significantly and achieves multiple node-disjoint paths efficiently.
- Various techniques to enhance the performance of DNDMR are applied. These enhancements include controlling traffic overhead, end-to-end delay, and throughput.
- Study and compare the simulations performance of various schemes in wireless ad hoc networks by using ns-2 simulators.

1.3 Thesis Organization

Chapter 2 provides the general concepts of cellular and wireless ad hoc networks, and the major issues and application of wireless ad hoc networks. Each of the application is explained and also point out the issues of wireless ad hoc networks.

Chapter 3 gives a brief overview of routing in wireless ad hoc networks. This chapter describes related research efforts and existing problems in ad hoc routing protocols. Classification of ad hoc networking is also introduced.

Chapter 4 presents an on-demand Directional Node-Disjoint Multipath Routing (DNDMR) protocol with very low routing overhead. The important components of the protocol, such as path accumulation with a novel directional method, reducing routing overhead by controlled propagation and ensuring the node-disjoint paths automatically, are explained. This chapter also evaluates the performance of the proposed scheme using ns-2 simulator.

Chapter 5 summarizes the work in this thesis, demonstrates the conclusions, and also mentions the future work.

Chapter 2 Wireless Ad Hoc Networks

2.1 Background

This section provides the background of cellular and wireless ad hoc networks, and the major issues and application of wireless ad hoc networks. The application of wireless ad hoc networks include military applications, collaborative and distributed computing, emergency operations, wireless mesh network, sensor networks, and hybrid wireless architectures. Each of the application will be described briefly in section 2.1.2. The major issues of wireless ad hoc networks are also given.

2.1.1 Cellular and Wireless Ad Hoc Networks

There are two distinct approaches for enabling wireless communication between two stations. The first approach is to let the existing cellular network infrastructure carry data as well as voice. The presence of base stations simplifies routing and resource management in a cellular network as the routing decisions are made in a centralized manner with more information about the destination node. The major problems include the problem of handoff, which tries to handle the situation when a connection should be smoothly handed over from one base station to another without noticeable delay or packet loss. The networks based on the cellular infrastructure are limited to places where there exists such a cellular network infrastructure.

The second approach is to form an ad-hoc network among all users wanting to communicate with each other. This means that all users participating in the ad hoc network must be willing to forward data packets to make sure that the packets are delivered from source to destination. This form of networking is limited by the transmission range of the individual nodes and is typically smaller compared to the range of cellular systems. Ad hoc networks have several advantages compared to traditional cellular systems. These advantages include: on-demand setup, fault tolerance, and unconstrained connectivity.

A wireless ad hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multihop radio network and maintaining connectivity in a decentralized manner. Since the nodes communicate over wireless links, they have to contend with the effects of radio communication, such as noise, fading, and interference. In addition, the links typically have less bandwidth than in a wired network. Each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is in general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes. Hence, there is a need for efficient routing protocols to allow the nodes to communicate over multihop paths consisting of possibly several links in a way that does not use any more of the network "resources" than necessary. Some of these features are characteristic of the type of packet radio networks that were studied extensively in the 1970s and 1980s. Yet, research in the area of ad hoc networking is receiving much attention from academia, industry, and government. Since these networks pose many complex issues, there are many open problems for research and opportunities for making significant contributions.

Wireless ad hoc networks can be generally divided into two categories: quasi-static and mobile. In a quasi-static ad hoc network, nodes are static or portable. However, the resulting network topology may be dynamic due to power controls and link failures. A typical sensor network is an example of a quasi-static ad hoc network. In mobile ad hoc networks, the entire network may be mobile, and nodes may move quickly relative to each other. A major technical challenge in a wireless ad hoc network is the design of the efficient routing protocols to cope with the rapid topology changes.

There is much attention currently focused on the development and evaluation of ad-hoc routing protocols for wireless networks. Most of this evaluation has been performed with the aid of various network simulators (such as ns-2, GloMoSim and others) and synthetic models for mobility and data patterns.

As shown in Figure 2.1, wireless ad hoc networks are mainly peer-to-peer multihop mobile wireless networks where information packets are transmitted in a store-and-forward Style from source to destination, via intermediate nodes. As the nodes move, the resulting change in network topology must be made known to the other nodes so that prior topology information can be updated. Such a network may operate in a stand-alone fashion, or with just a few selected routers communicating with an infrastructure network.

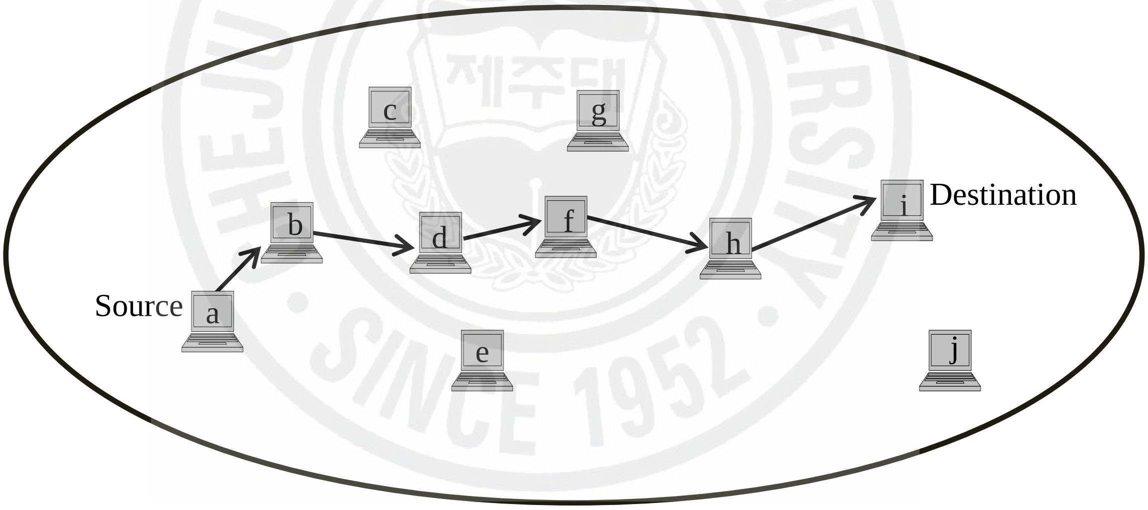

Figure 2.1 Illustration of a Wireless Ad Hoc Network

Each node is equipped with a wireless transmitter and a receiver with appropriate antenna, which may be omnidirectional, highly directional (point to point), possibly steerable, or some combination thereof. At a given point in time, depending on the nodes position and their transmitter and receiver coverage patterns, transmission power levels, and cochannel interface levels, a wireless connectivity in the form of a random and multihop graph or ad hoc network exists between the nodes. This network topology may change with time as the nodes move or adjust their transmission and reception parameters.

The major differences between cellular networks and wireless ad hoc networks are summarized in Table 2.1. The presence of base stations simplifies routing and resource managements in a cellular network as the routing decisions are made in a centralized manner with more information about the destination node. But in ad hoc wireless network, the routing and resource management are done in a distributed manner in which all nodes coordinate to enable communication among themselves. This requires each node to be more intelligent so that it can function both as network host for transmitting and receiving data and as a network router for routing packets from other nodes. Hence, the mobile nodes in wireless ad hoc networks are more complex than their counterparts in cellular networks.

Cellular Networks	**Wireless Ad Hoc Networks**
Fixed infrastructure-based	Infrastructure-less
Single-hop wireless links	Multi-hop wireless links
Guaranteed bandwidth (designed for voice traffic)	Shared radio channel (more suitable for best-effort data traffic)
Centralized routing	Distributed routing
Circuit-switched (evolving toward packet switching)	Packet-switched (evolving toward emulation of circuit switching)
Seamless connectivity (low call drops during handoffs)	Frequent path breaks due to mobility
High cost and time of deployment	Quick and cost-effective deployment
Reuse of frequent spectrum through geographical channel reuse	Dynamic frequency reuse based on carrier sense mechanism

Easier to achieve time synchronization	Time synchronization is difficult and consumes bandwidth
Easier to employ bandwidth reservation	Bandwidth reservation requires complex medium access control protocols
Application domains include mainly civilian and commercial sectors	Application domains include battlefields, emergency search and rescue operations, and collaborative computing
High cost of network maintenance (backup power source, staffing, etc.)	Self-organization and maintenance properties are built into the network
Mobile hosts are of relatively low complexity	Mobile hosts require more intelligence (should have a transceiver as well as routing/switching capability)
Major goals of routing and call admission are to maximize the call acceptance ration and minimize the call drop ratio	Main aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths
Widely deployed and currently in the third generation of evolution	Several issues are to be addressed for successful commercial deployment even though widespread use exist in defense

Table 2.1 Differences between cellular networks and wireless ad hoc networks

2.1.2 Applications of Wireless Ad Hoc Networks

Wireless ad hoc networks, due to their quick and economically less demanding deployment, find applications in several areas. Some of these include: military applications, collaborative and distributed computing, emergency operations, wireless mesh networks, wireless sensor networks, and hybrid wireless network architectures.

Wireless ad hoc networks can be very useful in establishing communication among a group of soldiers for tactical operations. Setting up a fixed infrastructure for communication among a group of soldiers in enemy territories or in inhospitable terrains can not be possible. In such environments, wireless ad hoc networks provide the required communication mechanism quickly. Another application in this area can be the coordination of military objects moving at high speeds such as fleets of airplanes or warships. Such applications require quick and reliable communication. Secure communication is of prime importance as eavesdropping or other security threats can compromise the purpose of communicating or the safety of personnel involved in these tactical operations. They also require the support of reliable and secure multimedia multicasting. For example, the leader of a group of soldiers may want to give an order to all the soldiers or to a set of selected personal involved in the operation. Hence, the routing protocol in these applications should be able to provide quick, secure, and reliable multicast communication with support for real-time traffic. In short, the primary nature of the communication required in a military environment enforces certain important requirements on wireless ad hoc networks, namely, reliability, efficiency, secure communication, and support for multicast routing.

Another domain in which the wireless ad hoc networks find applications is collaborative computing. The requirement of a temporary communication infrastructure for quick communication with minimal configuration among a group of people in a conference or gathering necessitates the formation of an ad hoc wireless network. For example, consider a group of researchers who want to share their research findings or presentation materials during a conference, or a lecture distributing notes to the class on the fly. In such cases, the formation of an ad hoc wireless network with the necessary support for reliable multicast routing can serve the purpose. The distributed file sharing applications utilized in such situations do not require the level of security expected in a military environment. But the reliability of data transfer is of high importance. Consider the example where a node that is part of an ad hoc wireless network has to distribute a file to other nodes in the network. Though this application does not demand the communication to be interruption-free, the goal of the transmission is that all the desired receivers must have the replica of the transmitted file. Other applications such as streaming of multimedia objects among the participating nodes in an ad hoc wireless network may require support for soft real-time communication.

Wireless ad hoc networks are very useful in emergency operations such as search and rescue, crowd control, and commando operations. The major factors that favor wireless ad hoc networks for such tasks are self-configuration of the system with minimal overhead, independent of fixed or centralized infrastructure, the nature of the terrain of such applications, the freedom and flexibility of mobility, and the unavailability of conventional communication infrastructure. In environments where the conventional infrastructure-based communication facilities are destroyed due to a war or due to natural calamities such as earthquakes, immediate deployment of wireless ad hoc networks would be a good solution for coordinating recues activities. Since the wireless ad hoc networks require minimum initial network configuration for their functioning, very little or no delay is involved in making the network fully operational. The above-mentioned scenarios are unexpected, in most cases unavoidable, and can affect a large number of people. Ad hoc wireless network employed in such circumstances should be distributed and scalable to a large number of nodes. They should also be able to provide fault-tolerant communication paths. Real-time communication capability is also important since voice communication predominates data communication in such situations.

Wireless mesh networks are wireless ad hoc networks that are formed to provide an alternate communication infrastructure for mobile or fixed nodes/users, without the spectrum reuse constraints and the requirements of network planning of cellular networks. The mesh topology of wireless mesh networks provides many alternate paths for a data transfer session between a source and destination, resulting in quick reconfiguration of the path when the exiting path fails due to node failures. Wireless mesh networks provide the most economical data transfer capability coupled with the freedom of mobility. Also, wireless mesh networks provide very high availability compared to the existing cellular architecture, where the presence of a fixed base station that covers a much larger area involves the risk of a single point of failure.

Sensor networks are a special category of wireless ad hoc networks that are used to provide a wireless communication infrastructure among the sensors deployed in a specific application domain. A sensor network is a collection of a large number of sensor nodes that are deployed in a particular region. The activity of sensing can be periodic or sporadic. The issues that make sensor networks a distinct category of wireless ad hoc networks are: mobility of nodes, size of the network, density of deployment, power constraint, data/information fusion, and traffic distribution.

One of the major application areas of wireless ad hoc networks is in hybrid wireless architectures such as multi-hop cellular networks (MCNs) and integrated cellular ad hoc relay (iCAR) networks. The major advantages of hybrid wireless networks are: 1) Higher capacity than cellular networks obtained by the better channel reuse provided by reduction of transmission power, as mobile nodes use a power range that is a fraction of the cell radius. 2) Increased flexibility and reliability in routing. The flexibility is in terms of selecting the best suitable nodes for routing, which is done through multiple mobile nodes or base stations or by a combination of both. The increased reliability is in terms of resilience to failure of base stations, in which case node can reach other nearby base stations using multi-hop paths. 3) Better coverage and connectivity in holes (areas that are not covered due to transmission difficulties such as antenna coverage or the direction of antenna) of a cell can be provided by means of multiple hops through intermediate nodes in the cell.

2.1.3 Issues in Wireless Ad Hoc Networks

This section points out the major issues and challenges that need to be considered when an ad hoc wireless system is to be designed. The deployment considerations for installation, operation, and maintenance of wireless ad hoc networks are also provided. The major issues that affect the design, deployment, and performance of an ad hoc wireless system are as follows:

- Medium access scheme
- Routing

- Multicasting
- Transport layer protocol
- Pricing scheme
- Quality of service provisioning
- Self-organization, security
- Energy management
- Addressing and service discovery
- Scalability
- Deployment considerations

Chapter 3 Routing in Wireless Ad Hoc Networks

3.1 Related Work

In this section, related research effort and existing problems in ad hoc routing protocol is described. These research efforts includes: classification of routing protocol, review of proactive routing protocols, review of reactive routing protocols, multipath routing protocol, and the problem with current multipath routing protocols.

3.1.1 Routing Protocols Classification

Routing in wireless ad hoc networks is clearly different from routing found in traditional infrastructure networks. The responsibilities of a routing protocol include exchanging the route information; finding a feasible path to a destination based on criteria such as hop length, minimum power required, and lifetime of the wireless link; gathering information about the path breaks; mending the broken paths expending minimum processing power and bandwidth; and utilizing minimum bandwidth. The major challenges for routing protocols are: mobility, bandwidth constraint, error-prone and shared channel, location-dependent contention, and other resource constraint. Designing issues for developing a routing protocol for wireless ad hoc networks are much more complicated than those for wired network. Minimum route acquisition delay, quick route reconfiguration, loop-free routing, distributed routing approach, minimum control overhead, scalability, provisioning of Quality of Service (QoS), support for time-sensitive traffic, security and privacy are the major requirements of a routing protocol in ad hoc wireless networks.

In ad hoc wireless networks, the communication range of a node is often limited and not all nodes can directly communicate with one another. Nodes are required to relay packets on behalf of other nodes to allow communication across the network. Since there is no such infrastructure and thus no preinstalled routers or predetermined topology, an ad hoc routing protocol is used to dynamically discover and maintain up-to-date routes between communication nodes.

In general, ad hoc network routing protocols are divided into two broad categories: proactive routing protocols and reactive (also known as on-demand routing) protocols according to their routing strategy. Next to the two described protocols there exist also hybrid protocols, which are a combination of the other two.

3.1.1.1 Proactive versus Reactive Approaches

Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating, proactively, route updates at fixed time intervals. The idea of such a protocol is to keep track of routes from a source to all destinations in the network. That way as soon as a route to a destination is needed it can be selected in the routing table. Advantages of a proactive protocol are that communication experiences a minimal delay and routes are kept up to date. Destination-Sequenced Distance-Vector (DSDV), Wireless Routing Protocol (WRP), Global State Routing (GSR), and Fisheye State Routing (FSR) are the well known proactive routing protocols in ad hoc network. On the other hand on-demand routing protocols established a route to a destination only when there is a demand for it, usually initiated by the source node through route discovery process within the network. When a route is needed by the source, it floods a route request packet to construct a route. Upon receiving route request, the destination selects the best route based on route selection algorithm. Route reply packet is then sent back to the source via the newly chosen route. In on-demand routing protocols, control traffic overhead is greatly reduced since no periodic exchanges of route tables are required. Numerous protocols of this type have been proposed.

Dynamic Source Routing (DSR), Ad-Hoc On-Demand Distance Vector (AODV) routing, and Temporally Ordered Routing Algorithm (TORA) are typical on-demand routing protocols. Proactive protocols have the advantage that new communications with arbitrary destinations experience minimal delay, but suffer the disadvantage of the additional control traffic overhead to update routing information at all nodes because that routes may break, as a result of mobility, before they are actually used or even that they will never be used at all, since no communication may be needed from a specific source to a destination. To cope with this shortcoming, reactive protocols adopt the inverse approach by finding a route to a destination only when needed. Reactive protocols often consume much less bandwidth than proactive protocols, but they will inevitably experience a long delay for discovering a route to a destination prior to the actual communication. However, because reactive routing protocols often broadcasts route requests, they may also generate excessive traffic if route discovery is required frequently.

3.1.2 Review of Proactive Routing Protocols

This section presents the brief description for several existing proactive routing protocols such as Dynamic Destination-Sequenced Distance-Vector (DSDV) Routing, and Wireless Routing Protocol (WRP).

3.1.2.1 Dynamic Destination-Sequenced Distance-Vector Routing

The Destination Sequenced Distance Vector (DSDV) protocol [7] is a proactive hop-by-hop distance vector routing protocol, requiring each node to broadcast routing updates periodically. Here, every MH in the network maintains a routing table for all possible destinations within the network and the number of hops to each destination. Each entry is the marked with a sequence number assigned by the destination MH. The sequence numbers enable the MHs to distinguish stale routes from new ones, thereby avoiding the formation of routing loops. Routing table updates are periodically transmitted throughout the network in order to maintain consistency in the tables.

To alleviate potentially large network update traffic, two possible types of packets can be employed: full dumps or small increment packets. A full dump type of packet carries all available routing information and can require multiple network protocol data units (NPDUs). These packets are transmitted less frequently during periods of occasional movements. Smaller incremental packets are used to relay only the information that has changed since the last full dump. Each of these broadcasts should fit into a standard-size NPDU, thereby decreasing the amount of traffic generated. The MHs maintain an additional table where they store the data sent in the incremental routing information packets. 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. The route labeled with the most recent sequence number is always used. In the event that two updates have the same sequence number, the route with the smaller metric is used in order to optimize (shorten) the path. MHs also keep track of settling time of the routes, or the weighted average time that routes to a destination could 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, MHs can reduce network traffic.

Note that if each MH in the network advertises a monotonically increasing sequence number for itself, it may imply that the route just got broken. For example, MH B in Figure.3.1 decides that its route to D with an infinite metric. This results in any node A, which is currently 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.

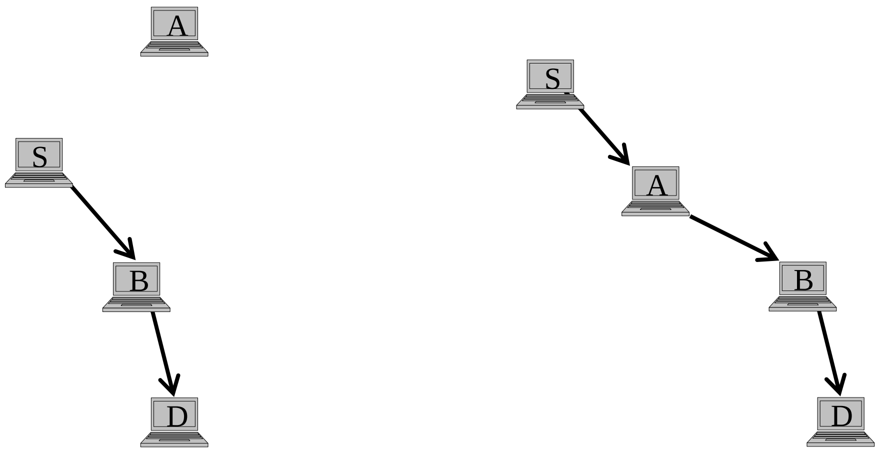

Figure 3.1 (a) MH S uses B to communicate with MH D

Figure 3.1 (b) Due to movement of MHs, S now uses A and B to reach D

Figure 3.1 Dynamic Destination-Sequenced-Vectors Routing

3.1.2.2 Wireless Routing Protocol

The Wireless Routing Protocol (WRP) [8] is a proactive distance-vector based protocol designed for ad hoc networks. The goal of this protocol is to maintain routing information among all nodes in the network. Each node in the network is responsible for maintaining four tables:

- Distance table
- Routing table
- Link-cost table
- Message retransmission list (MRL) table

Each entry of the MRL contains the sequence number of the update message, a retransmission counter, an acknowledgement-required flag vector with one entry per neighbor, and a list of updates sent in the update message. The MRL records which updates in a update message need to be retransmitted and which neighbors should acknowledge the retransmission.

Mobile informs each other of link changes through the use of update messages. An update message is sent only between neighboring nodes and contains a list of updates (the destination, the distance of the destination, and the predecessor of the destination), as well as a list of responses indicating which mobiles should acknowledge (ACK) the update. Mobiles send update messages after processing updates from neighbors or detecting a change in a link to a neighbor. In the event of the loss of a link between two nodes, the nodes send update messages to their neighbors. The neighbors then modify their distance table entries and check for new possible paths through other nodes. Any new paths are relayed back to the original nodes so that they can update their tables accordingly.

Nodes learn of the existence of their neighbors from the receipt of acknowledgements and other messages. If a node is not sending messages, it must send a hello message within a specified time period to ensure connectivity. Otherwise, the lack of messages from the node indicates the failure of that link; this may cause a false alarm. When a mobile receives a hello message from a new node, that new node is added to the mobile's routing table, and the mobile sends the new node a copy of its routing table information.

Part of the novelty of WRP stems from the way in which it achieves loop freedom. In WRP, routing nodes communicate the distance and second-to-last hop information for each destination in the wireless networks. WRP belongs to the class of path-finding algorithms with an important exception. It avoids the “count-to-infinity” problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbors. This ultimately (although not instantaneously) eliminates looping situations and provides faster route convergence when a link failure event occurs.

3.1.3 Review of Reactive Routing Protocols

In this section typical reactive routing protocols such as Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV) Routing are explained.

3.1.3.1 Dynamic Source Routing

The Dynamic Source Routing (DSR) protocol [9] is an on-demand routing protocol that is based on the concept of source routing. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned.

The protocol consists of two major phases: route discovery and route maintenance. Each node in the network keeps a cache of the source routes that it has learned. When a node has a packet to send to some destination, it first checks its route cache to determine whether it already has an up-to-date route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if the node does not have such a route, it initiates route discovery procedure by broadcasting a route request message to neighboring nodes. This route request message contains the address of the source and destination nodes, a unique identification number generated by the source node, and a route record to keep track of the sequence of hops taken by the route request message as it is propagated through the network. Each node receiving the packet checks whether it knows of a route to the destination. If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the request has not yet seen by the node and if the node's address does not already appear in the route record.

A route reply is generated when the route request reaches either the destination itself, or an intermediate node which contains in its route cache an unexpired route to the destination. By the time the packet reaches either the destination or such an intermediate node, it contains a route record yielding the sequence of hops taken. Figure 3.2(a) illustrates the formation of the route record as the route request propagates through the network. If the node generating the route reply is the destination, it places the route record contained in the route request into the route reply. If the responding node is an intermediate node, it will append its cached route to the route record and then generate the route reply. To return the route reply, the responding node must have a route to the initiator. If it has a route to the initiator in its route cache, it may use that route. Otherwise, if symmetric links are supported, the node may reverse the route in the route record. If symmetric links are not supported, the node may initiate its own route discovery and piggyback the route reply on the new route request. Figure 3.2(b) shows the transmission of the route reply with its associated route record back to the source node.

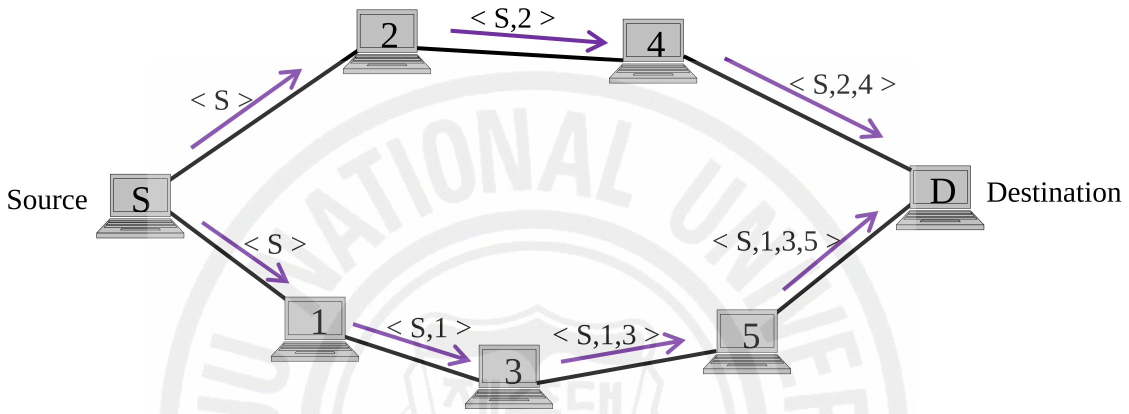

Figure 3.2 (a) Building Record Route

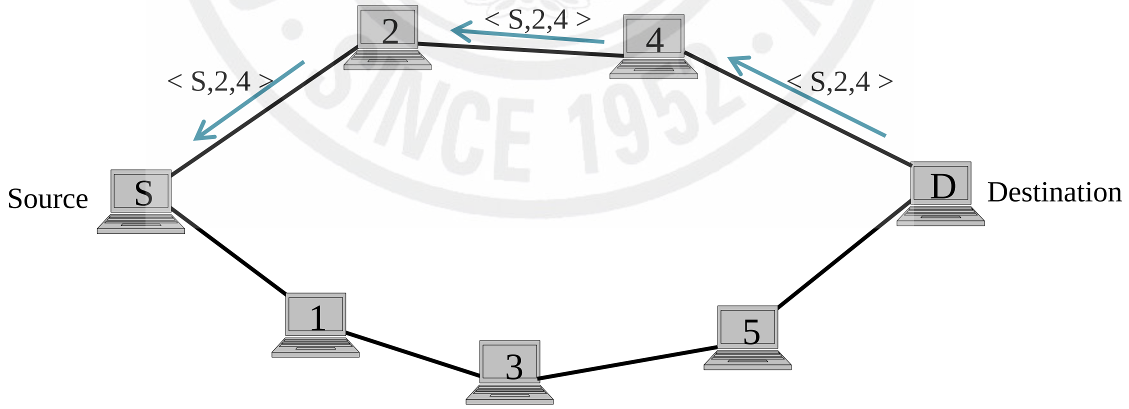

Figure 3.2 (b) Propagation of Route Reply

Figure 3.2 Route Discovery in DSR

Route maintenance uses route error messages and acknowledgement messages. Route error packets are generated at a node when the data link layer encounters a fatal transmission problem. When a route error packet is received, the hop in error is removed from the node’s route cache and all routes containing the hops are truncated at that point. In addition, to route error messages, acknowledgements include passive acknowledgements, where a node is able to hear the next hop forwarding the packet along the route. To reduce the route search overhead, an important optimization is allowing an intermediate node to send a route reply to the source node if it already has an up-to-date route to the destination.

3.1.3.2 Ad Hoc On-Demand Distance Vector Routing

The Ad Hoc On-Demand Distance Vector (AODV) routing [10] is a reactive protocol, even though it still uses characteristics of a proactive protocol. AODV takes the interesting parts of DSR and DSDV, in the sense that it uses the concept of route discovery and route maintenance of DSR and the concept of sequence numbers and sending of periodic hello messages from DSDV.

Routes in AODV are discovered and established and maintained only when and as long as needed. To ensure loop freedom sequence numbers, which are created and updated by each node itself, are used. These allow also the nodes to select the most recent route to a given destination node. AODV takes advantage of route tables. In these it stores routing information as destination and next hop addresses as well as the sequence number of a destination. Next to that a node also keeps a list of the precursor nodes, which route through it, to make route maintenance easier after link breakage. To prevent storing information and maintenance of routes that are not used anymore each route table entry has a lifetime. If during this the time the route has not been used, the entry is discarded.

When a source node wants to send a message to some destination node and does not already have a valid route to that destination, it initiates a route discovery process to locate the other node. It broadcast a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with an active route to the destination is located. Figure 3.3(a) illustrates the propagation of the broadcast RREQs across the network. AODV utilizes the destination sequence numbers to ensure all routes are loop-free and contain the most recent route information. Each node maintains its own sequence number, as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node’s IP address, uniquely identifies an RREQ. Along with its own sequence number and the broadcast ID, the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ.

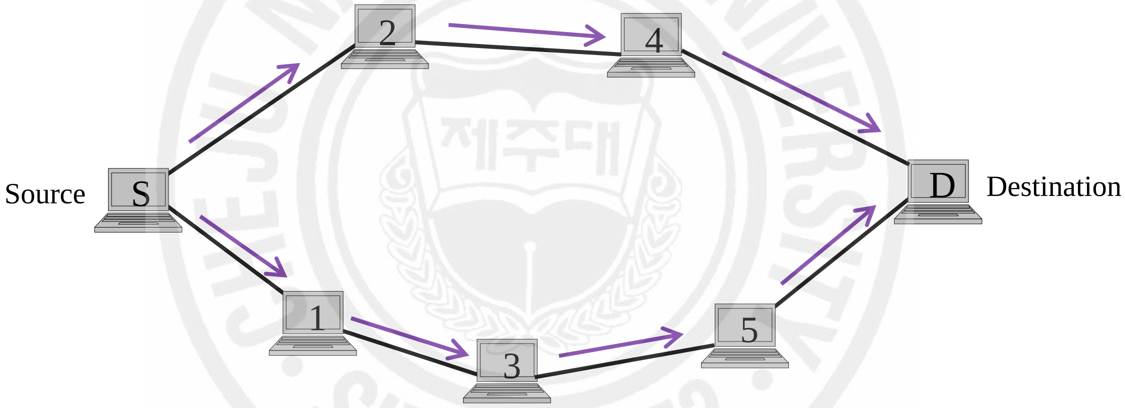

Figure 3.3 (a) Route Request Propagation

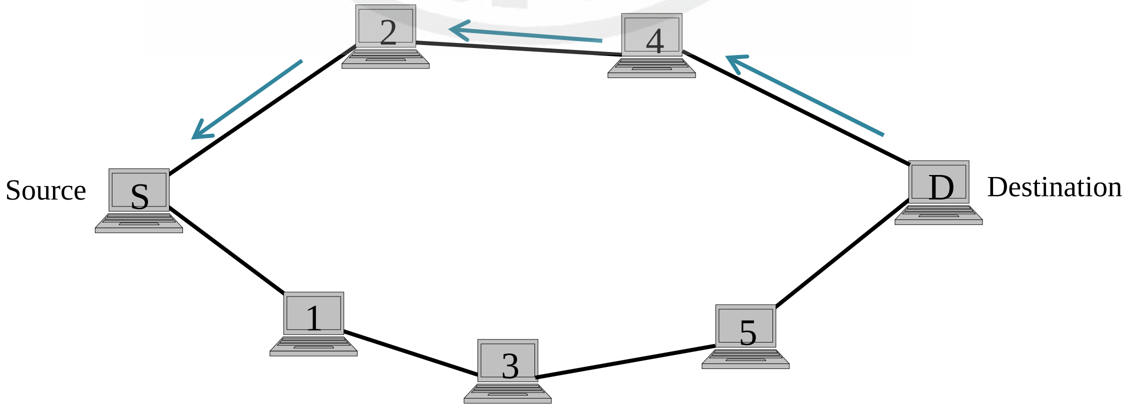

Figure3.3 (b) Route Reply Sent Back to Source

Figure 3.3 Route Discovery in AODV

During the process of forwarding route request, intermediate nodes record in their route tables the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. Once the RREQ reaches the destination or an intermediate node with an active route, the destination/intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ, shown in Figure 3.3(b). As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route tables which point to the node from which the RREP came. These forward route entries indicate the active forward route. Associated with each route entry is a route timer which will cause the deletion of the entry if it is not used within the specified life time. Because the RREP is forwarded along the path establishing by the RREQ, AODV only supports the use of symmetric links.

When a route has been established, it is being maintained by the source node as long as the route is needed. Movements of nodes effect only the routes passing through this specific node and thus do not have global effects. If the source node moves while having an active session and loses connectivity with the next hop of the route, it can rebroadcast an RREQ. If though an intermediate station loses connectivity with its next hop it initiates an Route Error (RERR) message and broadcasts it to its precursor nodes and marks the entry of the destination in the route table as invalid, by setting the distance to infinity. The entry will only be discarded after a certain amount of time, since routing information may still be used. When the RERR message is received by a neighbor it also marks its route table entry for the destination as invalid and sends again RERR messages to its precursors.

In the Figure 3.4(a), the node 4 moves to the node 4` and so node 2 cannot communicate with it anymore, connectivity is lost. Node 2 creates a RERR message and unicasts the message to source node. When the RERR is received at the source node and it still needs the route to the destination it reinitiates a route discovery. Figure 3.4(b), shows the new route from the source to the destination through node 5. Also if a node receives a data packet for a node which it does not have an active route too, it creates a RERR message and broadcasts it as described above.

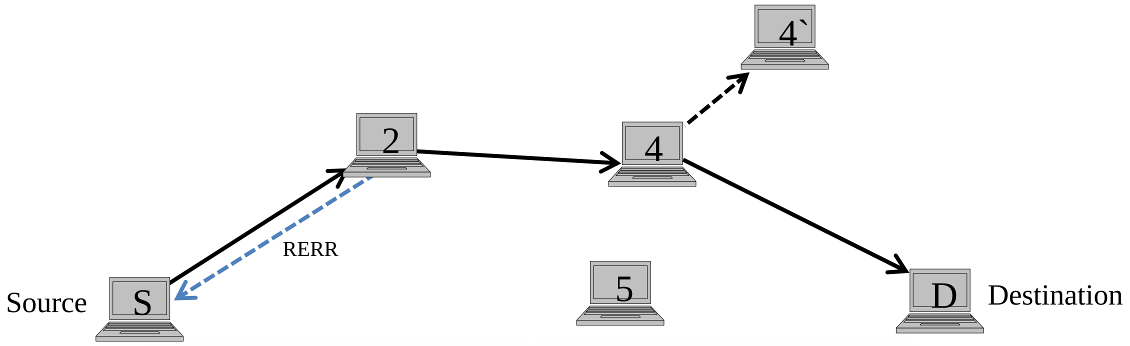

Figure 3.4 (a) Route Error Send to Source Node

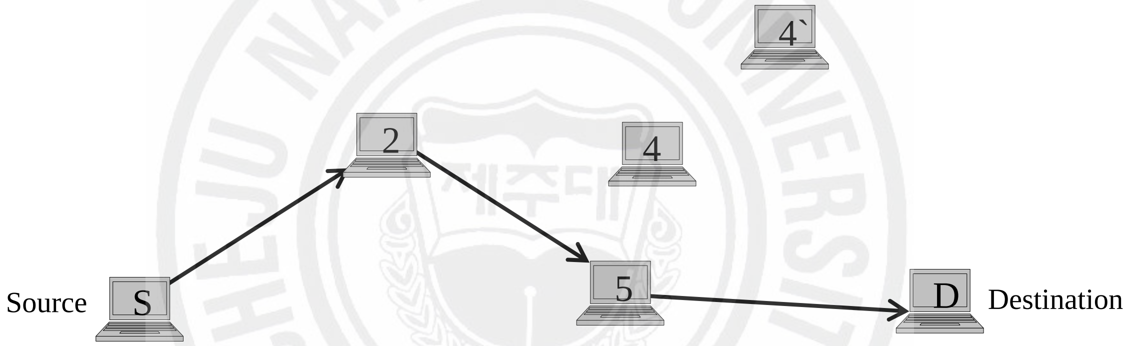

Figure 3.4 (b) New Route Discovered

Figure 3.4 Route Maintenance in AODV

If no broadcast has been send within, by default; one second, each node broadcasts Hello messages to its neighbors in order to keep connectivity up to date. These messages contain the nodes IP address and its current sequence number. So that these messages are not forwarded from the node’s neighbors to third parties the Hello message has a TTL value of one.

Table 3.1 shows and compares the unipath routing protocols for mobile ad hoc networks.

	DSDV	WRP	DSR	AODV
Routing Category	Proactive	Proactive	Reactive	Reactive
Beaconing	Yes	Yes	Yes	Yes
Periodic Update	Yes	Yes	No	No
Flood Control	No	No	Yes	Yes
TTL Limitation	No	No	Yes	Yes
QoS Support	No	No	No	No
Multicast Support	No	No	No	Yes
Power Management	No	No	No	No
Security Support	No	No	No	No

Table 3.1 Comparison of the unipath routing protocols

3.1.4 Multipath Routing

Multipath routing has been explored in several different contexts. Traditional circuit switched telephone networks used a type of multipath routing called alternate path routing. In alternate path routing, each source and destination node have a set of paths or multipath which consists of a primary path and one or more alternate paths. Alternate path routing was proposed in order to decrease the call blocking probability and increase overall network utilization. In alternate path routing, the shortest path between exchanges is typically one hop across the backbone network; the network core consists of a fully connected set of switches. When the shortest path for a particular source destination pair becomes unavailable due to either link failure or full capacity, rather than blocking a connection, an alternate path, which is typically two hopes, is used. Multipath routing has also been addressed in data networks which are intended to support connection-oriented service with quality of service (QoS).

Alternate or multipath routing has typically lent itself to be of more obvious use to connection-oriented networks; call blocking probability is only relevant to connection oriented networks. However, in packet-oriented networks, like the internet, multipath routing could be used to alleviate congestion by routing packets from highly utilized links to links which are less highly utilized.

3.1.5 Multipath Routing Protocols

Standard on-demand routing protocols in wireless ad hoc networks, such as AODV and DSR, are mainly intended to discover a single route between a source and destination node. When the route disconnects, nodes of the broken route simply drop data packets because no alternate path to the destination is available until a new route is established. Multipath routing is a useful technique for finding the multiple paths between a source and destination in a single route discovery. These multiple paths between source and destination can be used to compensate for the dynamic and unpredictable topology change in ad hoc networks. Recently, several different multipath routing mechanisms have been proposed. This section introduces some main characteristics of these multipath protocols. Split Multipath routing (SMR) and Multipath Source Routing (MSR) protocols are based on DSR routing protocol, where as Ad Hoc On-Demand Multipath Distance Vector (AOMDV) and Ad hoc On-Demand Distance Vector Multipath (AODVM) are based on AODV.

3.1.5.1 Split Multipath Routing

Split Multipath Routing (SMR) proposed in [12] is an on-demand multipath source routing protocol that builds multipath using a route request/reply cycle. SMR can find an alternative route that is maximally disjoint from the source to the destination. When the source nodes needs a route to the destination but no route is known, it floods the route request (RREQ) message to the entire network in order to find maximally disjoint paths, so the approach has a disadvantage of transmitting more RREQ packets. Because of this flooding, several duplicates traversed through different routes reach the destination. The destination node selects multiple maximally disjoint routes and sends route reply (RREP) packets back to the source via the chosen routes. In order to choose proper maximally disjoint route paths, the destination must know the entire path of all available routes. Therefore, SMR uses the source routing approach where the information of the nodes that compromise the route is included in the RREQ packet.

SMR is similar to DSR, and is used to construct maximally disjoint paths. Unlike DSR, intermediate nodes do not keep a route cache, and therefore, do not reply to RREQs. This is to allow the destination to receive all the routes so that it can select the maximally disjoint paths. Maximally disjoint paths have as few links or nodes in common as possible. Duplicate RREQs are not necessarily discarded. Instead, intermediate nodes forward RREQs that are received through a different incoming link, and whose hop count is not larger than the previously received RREQs. The proposed route selection algorithm only selects two routes. However, the algorithm can be extended to select more than two routes. In the algorithm, the destination sends an RREP for the first RREQ it receives, which represents the shortest delay path. The destination then waits to receive more RREQs. From the received RREQs, the path that is maximally disjoint from the shortest delay path is selected. If more than one maximally disjoint path exists, the shortest hop path is selected. If more than one shortest hop path exists, the path whose RREQ was received first is selected. The destination then sends an RREP for the selected RREQ.

3.1.5.2 Multipath Source Routing

Multipath Source Routing (MSR) [13, 14] is an extension of the on-demand Dynamic Source Routing DSR [9] protocol. It consists of a scheme to distribute traffic among multiple routes in a network. MSR uses the same route discovery process as DSR with the exception that multiple paths can be returned, instead of only one path.

When a source requires a route to a destination but no route is known, it will initiate a rote discovery process by flooding a RREQ packet throughout the network. A route record in the header of each RREQ records the sequence of hops that the packet passes. An intermediate node contributes to the route discovery by appending its own address to the route record. Once the RREQ reaches the destination, a RREP will reverse the route in the route record of the RREQ and traverse back through this route.

Each route is given a unique index and stored in the cache, so it is easy to pick multiple paths from there. Independence between paths very important in multipath routing, therefore disjoint paths are preferred in MSR. As MSR uses the same route discovery process as DSR, where the complete routes are in the packet headers, looping will not occur. When a loop is detected, it will be immediately eliminated.

Since source routing is used in MSR, intermediate nodes do nothing but forward the packet according to the route in the packet-header. The routes are all calculated at the source. A multiple-path table is used for the information of each different route to a destination. This table contains for each route to the destination: the index of the path in the route cache, the destination ID, the delay and the calculated load distributed weight of a route. The traffic to a destination is distributed among multiple routes. The weight of a route simply represents the number of packets sent consecutively on that path.

3.1.5.3 Ad Hoc On-Demand Multipath Distance Vector

Ad Hoc On-Demand Multipath Distance Vector (AOMDV) [16] is an extension to the AODV protocol for finding multiple loop-free and link disjoint paths. The protocol computes multiple loop-free and link-disjoint paths. Loop-freedom is guaranteed by using a notion of “advertised hopcount”. Link disjointness of multiple paths is achieved by using a particular property of flooding.

To keep track of multiple routes, the routing entries for each destination contain a list of the next-hops together with the corresponding hop counts. All the next hops have the same sequence number. For each destination, a node maintains the advertised hop count, which is defined as the maximum hop count for all the paths. This is the hop count used for sending route advertisements of the destination. Each duplicate route advertisement received by a node defines an alternative path to the destination. To ensure loop-freedom, a node only accepts an alternative path to the destination if it has a lower hop count than the advertised hop count for that destination. Because the maximum hop count is used, the advertised hop count therefore does not change for the same sequence number. When a node advertisement is received for a destination with a greater sequence number, the next-hop list and advertised hop count are reinitialized.

AOMDV can be used to find link-disjoint routes. To find disjoint routes, each node does not immediately reject duplicate RREQs. Each RREQ carries an additional field called first hop to indicate the first hop (neighbor of the source) taken by it. Also, each node maintains a first hop list for each RREQ to keep track of the list of neighbors of the source through which a copy of the RREQ has been received. In an attempt to get multiple link-disjoint routes, the destination replies to duplicate RREQs regardless of their first hop. To ensure link-disjointness in the first hop of the RREP, the destination only replies to RREQs arriving via unique neighbors. The trajectories of each RREP may intersect at an intermediate node, but each takes a different reverse path to the source to ensure link-disjoiness.

3.1.5.4 Ad Hoc On-Demand Distance Vector Multipath Routing

Ad Hoc On-Demand Distance Vector Multipath Routing (AODVM) [18] is an extension to AODV for finding multiple node disjoint paths. Instead of discarding the duplicate route request (RREQ) packets, intermediate nodes are required to record the information contained in these packets in the RREQ table. For each received copy of a RREQ message, the receiving intermediate node records the source that generated the RREQ, the destination for which the RREQ is intended, the neighbor that transmitted the RREQ, and some additional information in the RREQ table. Furthermore, intermediate relay nodes are precluded from sending an RREP message directly to the source.

When the destination receives the first RREQ packet from one of its neighbors, it updates its sequence number and generates an RREP packet. The RREP packet contains an additional field called “last hop ID” to indicate the neighbor from which the particular copy of RREQ packet was received. This RREP packet is sent back to the source via the path traversed by the RREQ. When the destination receives duplicate copies of the RREQ packet from other neighbor, it updates its sequence number and generates RREP packets for each of them. Like the first RREP packet, these RREP packets also contain their respective last hop nodes IDs.

When an intermediate node receives an RREP packet from one of its neighbors, it deletes the entry corresponding to this neighbor from its RREQ table and adds a routing entry to its routing table to indicate the discovered route to the originator of the RREP packet (the destination). The node, then, identifies the neighbor in the RREQ table via which, the path to the source is the shortest, and forwards the RREQ message to that neighbor. The entry corresponding to this neighbor is then deleted from the RREQ table. In order to ensure that a node does not participate in multiple paths, when nodes overhear any node broadcasting an RREP message, they delete the entry corresponding to the transmitting node from their RREQ tables.

Intermediate nodes make decisions on where to forward the RREP messages (unlike in source routing) and the destination, which is in fact the originator of these messages, is unaware as to how many of these RREP messages that it generated actually made it back to the source. Thus, it is necessary for the source to confirm each received RREP message by means of Route Confirmation Message (RRCM). The RRCM message can, in fact, be added to the first data packet sent on the corresponding route and will also contain information with regards to the hop count of the route, and the first and last hop relays on that route.

3.1.6 Problem with Current Multipath routing protocols

Previous section introduces simply routing mechanisms and benefits of several existing multipath protocols. Although these protocols can build on-demand multiple routing paths, all of them will encounter a broadcast storm of routing packets in the process of looking for multiple disjoint routing paths.

In the case of multipath routing, discovering the multiple routing paths from source to destination is very crucial task. As studied the related works, intermediate node(s) can take the duplicate RREQ over condition or can avoid the duplicate RREQ, depending on the routing discovery approach. When a source in these multipath routing protocols needs a route to a destination but no route information is known, it floods the route request (RREQ) message to the entire network. In order to ensure that the destination can select disjoint paths, all the four multipath routing protocols take the duplicate RREQs at intermediate nodes. But all of them are not considered organized propagation for finding the disjoint paths. As a result, all the approaches lead to dramatic increase of routing overhead in the ad hoc network. Because bandwidth in wireless ad hoc network is limited, how to reduce routing overhead has to be considered when designing a routing protocol. In our case, intermediate nodes take the duplicate path and transmit the RREQ directionally, which results in the discovery of preeminent node-disjoint paths. We reduce the routing overhead by controlled propagation of routing packet through the network. The routing packets thus received at the destination node automatically form node-disjoint paths. In the next chapter, Directional Node-Disjoint Multipath Routing (DNDMR) protocol with low control traffic overhead is explained in details. This is a novel approach with improved efficiency in terms of routing overhead, end-to-end delay, and fault tolerance.

Table 3.2 compares the main characteristics of exiting multipath routing protocols.

	SMR	**MSR**	**AOMDV**	**AODVM**
Routing Category	Reactive	Reactive	Reactive	Reactive
Loop-free Paths	Yes	Yes	Yes	Yes
Node-disjoint Paths	Possibly	Yes	Possibly	Yes
Complete Routes Known	Yes	Yes	No	No
Control Routing Overhead	No	No	No	No
Multiple Complete Paths	Yes	Yes	Yes	Yes
Node-disjoint Path Ensured	No	No	No	No
Path Used Simultaneously	Yes	Yes	Yes	Yes
TTL Limitation	Yes	Yes	Yes	Yes
Implementation	DSR	DSR	AODV	AODV

Table 3.2 Comparison of multipath routing protocols

Chapter 4 Directional Node-Disjoint Multipath Routing

4.1 Introduction

An ad hoc network consists of a collection of wireless nodes that are capable of communicating with each other without any base station and infrastructure support. All nodes can be mobile and the topology changes frequently. Therefore, routing protocols play an important role in ad hoc network communication.

Design issues for developing a routing protocol for wireless ad hoc networks are much more complicated than those for wired networks. Ad hoc networks include resource-poor devices, limited bandwidth, high error rates and a continually changing topology. Among the available resources, battery power is typically the most constraining. Minimal control overhead, minimal processing overhead, dynamic topology maintenance and loop prevention are the typical design goals for the ad hoc network routing protocols. With these goals in consideration, the routing protocol should be able to work in a distributed manner, self starting, and self organizing. Mobile hosts have a limited range and send message to another host, which is not in the sender's host transmission range. The message must be forwarded through the network using other hosts which will be operated as routers for delivering the message throughout the network.

The goal of the routing protocol is finding a short and optimized route from the source to the destination node. Routing protocols can be classified either as proactive or reactive. The idea of proactive protocols is to keep track of routes from a source to all destinations in the network, so that when a packet needs to be forwarded, the route is already known and can be immediately used. On the other hand, reactive protocols or also called on-demand protocols use the concept of getting information about routing only when needed. With proactive and reactive protocols there exist also Hybrid protocols, which are a combination of these two.

Also, the protocols can be either unipath or multipath protocols based on the number of routers discovered between source and destination. Most of the currently proposed routing protocols for ad hoc networks are unipath routing protocols. In this routing protocol, only a unipath or single route is used between a source and destination node. Dynamic Source Routing (DSR) and Ad hoc On-demand Distance Vector (AODV) protocols are the most popular and widely used protocols belonging to the on-demand protocols. On the other hand, Multipath routing consists of finding multipath or multiple routes between a source and destination node. These multiple paths between source and destination node pairs can be used to compensate for the dynamic and unpredictable nature of ad hoc networks.

The multipath routing is more effective than the single path routing because multipath can provide load balancing, fault-tolerance, and higher aggregated bandwidth. Multipath routing protocols in ad hoc networks have been proposed in [12-23]. Although these protocols build multiple routes on-demand, most of them discuss non-disjoint or link-disjoint paths; very few works are done for node-disjoint path, where node-disjoint routes offer the highest degree of fault-tolerance. In addition, all of them flood Route Request (RREQ) packets to the entire network in order to discover multiple routing paths.

We present Directional Node-disjoint Multipath Routing (DNDMR) protocol that builds node-disjoint paths by using a new directional process in the entire network. In DNDMR, the best and shortest delay multiple paths are discovered on-demand. The performance evaluation shows that DNDMR is more efficient and more reliable than the contemporary unipath and multipath routing protocols.

4.2 Directional Node-Disjoint Multipath Routing

The Directional Node-Disjoint Multipath Routing (DNDMR) Protocol proposed here is a novel approach. It reduces the routing overhead significantly and achieves multiple node-disjoint routing paths efficiently. This section shows the protocol mechanism in details.

4.2.1 Route Discovery

Directional Node-disjoint Multipath Routing (DNDMR) Protocol is an on-demand routing protocol which builds the multiple node-disjoint routes from the source to the destination by using Route Request (RREQ) and Route Reply (RREP) messages. When a source requires a route to the destination but no route is known, it will initiate a route discovery by flooding a RREQ packet directionally throughout the entire network. Because of this flooding, several duplicate packets traverse through the multiple node-disjoint routes to the destination in direction-wise fashion. Once the RREQ reaches the destination, a RREP will reverse the route in the route record of the RREQ and traverse back through this route.

4.2.2 Route Request (RREQ) Propagation

The main goal of DNDMR is to build multiple node-disjoint paths with a very low routing overhead. To achieve this goal in on-demand routing, the destination node must know the entire path of all available routes so that it can select the node-disjoint paths. Therefore, we use the source routing approach where node information of route is included in the RREQ packet. When the source node has data packets to send to the destination, but does not have the route information, it broadcast the RREQ packet. Every node knows its one hop neighbor through neighbor discovery. Every node periodically broadcasts HELLO packets to its one-hop neighbors. This knowledge of one-hop neighbors is utilized while deciding the next hop of RREQ packet during the route discovery process. The packet contains source id and a sequence numbers that uniquely identify the packet. For propagation of RREQ in DNDMR, we propose a novel directional approach. Before broadcasting a packet, every node checks its one-hop neighbor nodes, and after that it floods the packet in its left-right-up-down direction. After receiving RREQ from the source node, intermediate node(s) rebroadcast the packet respectively. Intermediate node can not rebroadcast the RREQ from which side it received the packet.

Moreover, when a node receives the same RREQ from a different incoming link than the link from the first RREQ is received and if packets current hop count is not greater than the first received RREQ it is considered as the duplicate.

For finding the node-disjoint multiple paths in DNDMR, the intermediate node takes the duplicate RREQ and retransmits both RREQ in the entire network. Figure 4.1 shows the propagation process of DNDMR. When an intermediate node first receives a RREQ packet from its neighbor, it checks how many nodes there are in its one-hop neighborhood and then it decides whether duplicate RREQ can be received from another neighboring node or not. If it finds that duplicate RREQ could be received from another neighboring node, the responding node, from which side it received the packet, retransmits the packet only to the opposite node (if the node is not available in opposite side, it will be discarded automatically).

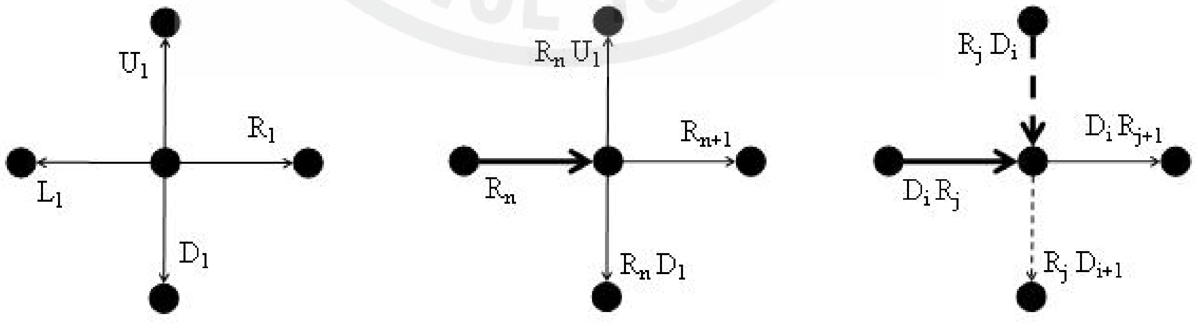

Figure 4.1(a) Source node

Figure 4.1(b) Intermediate node

Figure 4.1 Propagation Process in DNDMR

The direction of the propagation of RREQ is decided on the basis of relative position of the one-hop neighbors of the router node. Every node periodically broadcasts its position to its one hop neighbors and every node maintains a neighbor table. When RREQ is received by an intermediate node it decides the left, right, up and down nodes in its neighborhood and based on this notion of left, right, up and down, it sends the RREQ in the suitable direction. This controlled forwarding of RREQ packets is important in the sense that when RREQ packets reach the destination, node-disjoint paths are automatically ensured. Unlike the traditional node-disjoint protocols wherein node-disjoint paths are decided either at the source node or at the destination node, our protocol does not depend on any such mechanism. Instead control propagation of the RREQ packets automatically guarantees the formation of node-disjoint paths.

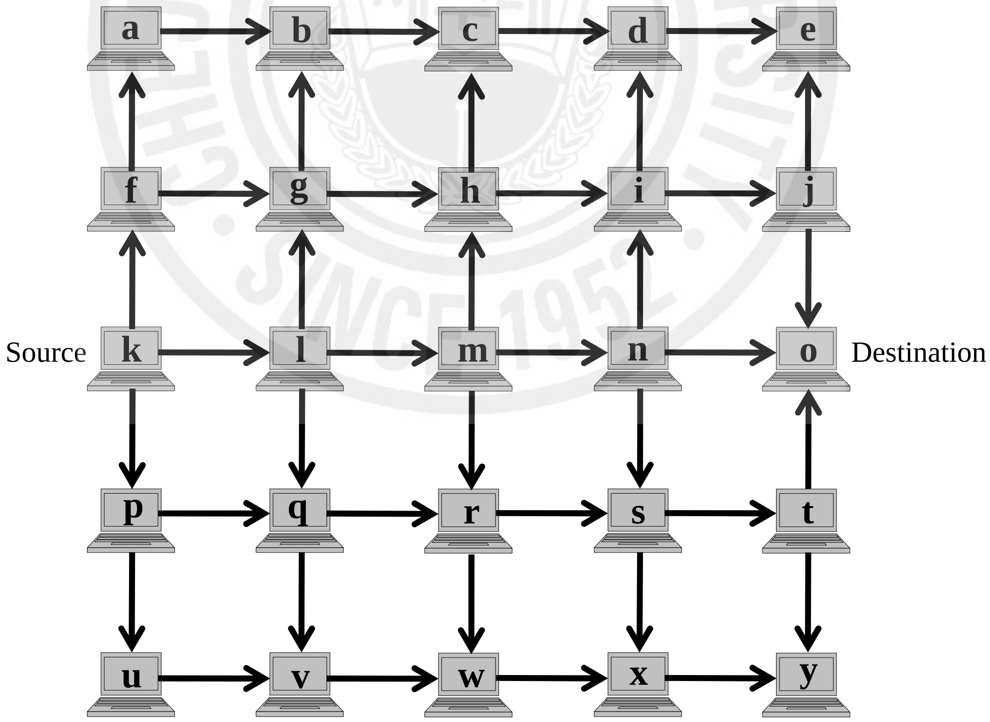

Figure 4.2 Network Topology

For example, in Figure 4.2, *node g* can be received first RREQ from its down node (l) or left node (f). Suppose that, *node g* received the first RREQ from its down node (l). After receiving the RREQ, it found three (f, h and b) more neighboring nodes in its one-hop range. *Node g* can guess that it could receive the duplicate RREQ from its left node (f). Therefore, *node g* rebroadcast the receiving first RREQ to the opposite side that means from down node (l) to up node (b) and when *node g* will receive the duplicate RREQ from left node (f), it rebroadcast the packet to its opposite side that means its right node (h). With this process, DNDMR discovers the route paths to the destination. By using this method, not only routing overhead reduced methodically but also multiple node-disjoint paths reached in the destination automatically.

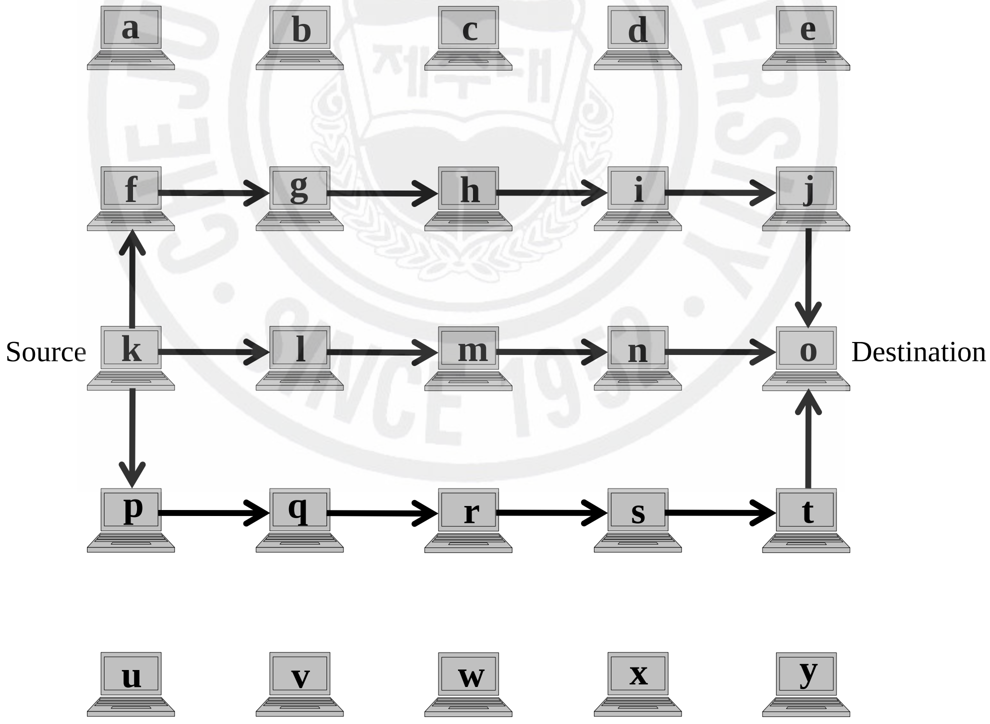

Figure 4.3 Node disjoint paths discovered

4.2.3 Node-Disjoint Path Selection

In DNDMR, first received two route paths by destination are always node-disjoint route paths. For example of DNDMR, in Figure 4.3, three node-disjoint route paths are received by destination: k-l-m-n-o, k-f-g-h-i-j-o and k-p-q-r-s-t-o. In most of the cases only two node-disjoint paths are received by the destination in DNDMR. Therefore, we limit the number of node-disjoint route paths to two in DNDMR. When the destination node first receives the RREQ, it records the entire path and sends the route reply (RREP) to the source by using that route. RREP packet includes the nodes id of the entire path and using this information, intermediate node can forward the packet. After this process, when the destination node receives the second RREQ, it sends another RREP to the source via the second route.

4.2.4 Route Maintenance

In the fault tolerance perspective, more reliable paths should be selected to reduce the chance of route failures. However because of the mobility, the congestion, and the packet collisions, route links can be broken often in ad hoc networks. In DNDMR, link can be disconnected when a node fails to send the packet to the next hop of the route. In this case responsible node will sends a Route Error (RERR) packet to the upstream direction of the route. The RERR message contains the route to the source and the immediate upstream and downstream nodes of the broken link. After receiving this RERR packet, the source node removes every entry from its route table that uses the broken link. If only one of the two route node-disjoint paths invalidated during the transmission, remaining valid route will be used for transmitting data packet. If all of the two routing paths are invalid, the source node initiates the route discovery process again. The summary of the pseudo code is revealed in the next section.

4.2.5 Pseudo code

```
PROCEDURE SendDataPacket(Packet p)
BEGIN
    IF (this is source node)
        IF (no path available)
            Discover Node-Disjoint-Paths Routes(Dest)
        IF (primary path available)
            Call SendPacket(Primary Path)
        ELSE IF (secondary path 1 available)
            Call SendPacket(Secondary Path)
    ELSE
        Result = ForwardPacket(Path)
        IF (result is link failure)
            Send error info to source
END

PROCEDURE ForwardPacket(Path)
BEGIN
    IF (Dest is equal to Current Node)
        Call ReceivePacket(Packet)
    ELSE
        Send Packet to the next node
END

PROCEDURE DiscoverNeighbors(Node)
BEGIN
    Send Hello Packets to Neighbors
```

```
END

PROCEDURE Discover Node-Disjoint-Paths(Dest)
BEGIN
    IF (Current node is not Dest)
    {
        Decide Next hop from the Neighbor Table
        Send Packet to the Next hop
    }
    ELSE (Current node is Dest)
    {
        Send the route to the source
    }
END

PROCEDURE Main()
BEGIN
    Discover Neighbors
    Discover Node-Disjoint-Paths
    Transmit data on suitable path
END
```

4.3 Performance Evaluation

In order to demonstrate the effectiveness of DNDMR, we evaluate the proposed protocol and compare its performance with that of DSDV, DSR, AODV and AOMDV. The metrics considered for the evaluation are routing traffic overhead, throughput, and end-to-end delay. We have implemented

DNDMR using the ns-2 simulator [24]. As a first step we have assumed a static network topology consisting of 49 nodes. The environment settings are explained in Table 4.1.

We have used TCP application as traffic generating source. The TCP packets are continuously transmitted and various performance metrics are measured in case of DSDV, DSR, AODV, AOMDV and DNDMR.

Antenna type	Omnidirectional
Propagation model	TwoRayGround
Transmission range	100m
MAC protocol	802.11 with RTS/CTS
MAC bandwidth	1 Mbit
Interface queue type	Drop-tail priority queue
Max. IFQ length	50
Propagation delay	1 ms
Node count	49
Network size	700m × 700m
Simulation time	130s

Table 4.1 The setup parameters used for the ns2 simulations

Control traffic overhead or routing overhead illustrated the cumulative sum of routing packets generated in order to route data packets form the source to the destination throughout the duration of the simulation. Figure 4.4 shows the routing overhead in case of DNDMR is significantly lower than

DSDV, DSR, AODV and AOMDV. The reason is that route discovery mechanism in DNDMR is highly optimized and the destination is discovered by the transmission of minimum packets throughout the network. From Figure 4.4, the cumulative packets at the end of simulation time is 6000 for DSDV, 5000 for DSR, 2700 for AOMDV, 2600 for AODV, whereas in case of DNDMR it is 2300 packets which is comparatively less than the other mentioned protocols.

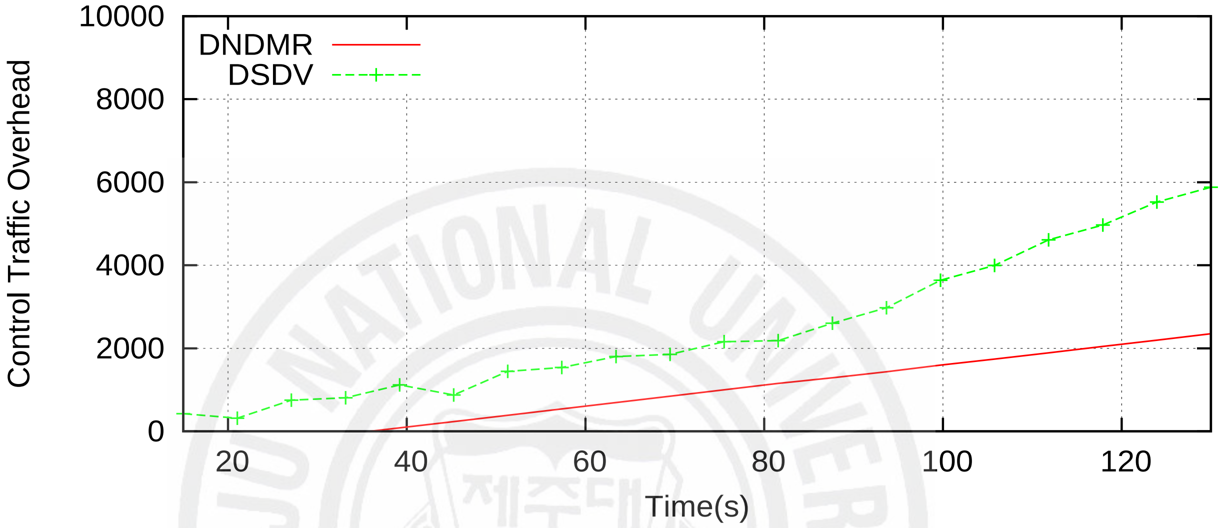

Figure 4.4(a) Control Traffic Overhead: DNDMR vs. DSDV

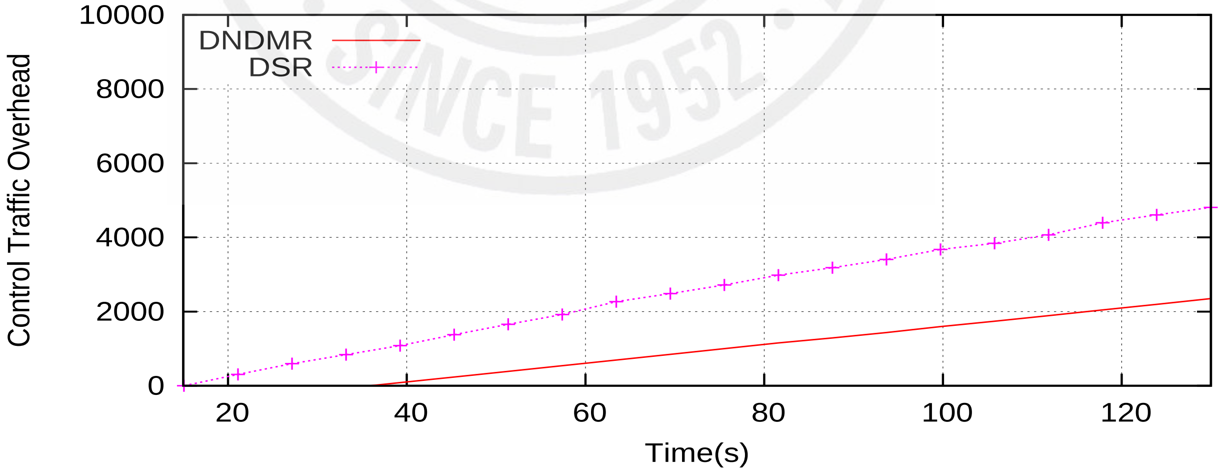

Figure 4.4(b) Control Traffic Overhead: DNDMR vs. DSR

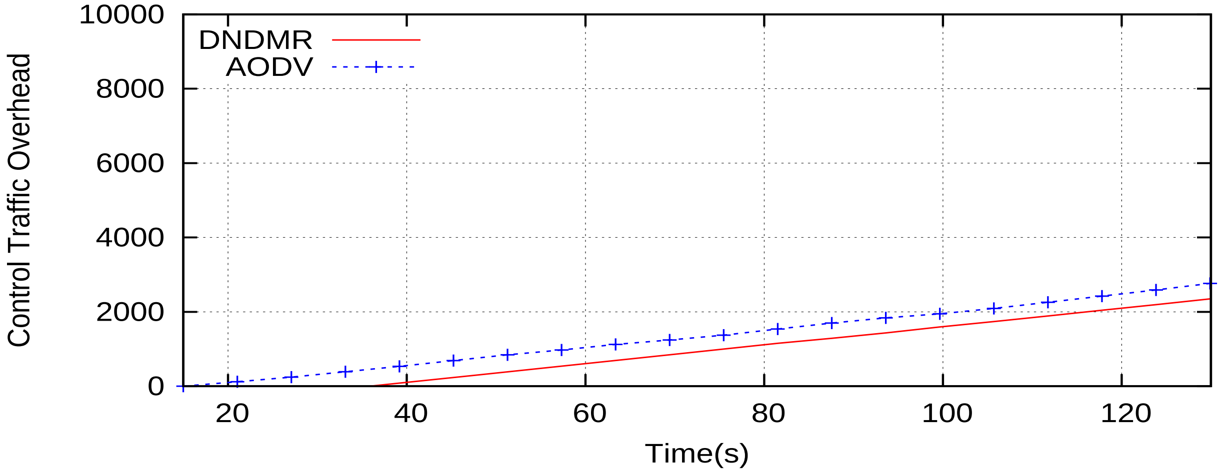

Figure 4.4(c) Control Traffic Overhead: DNDMR vs. AODV

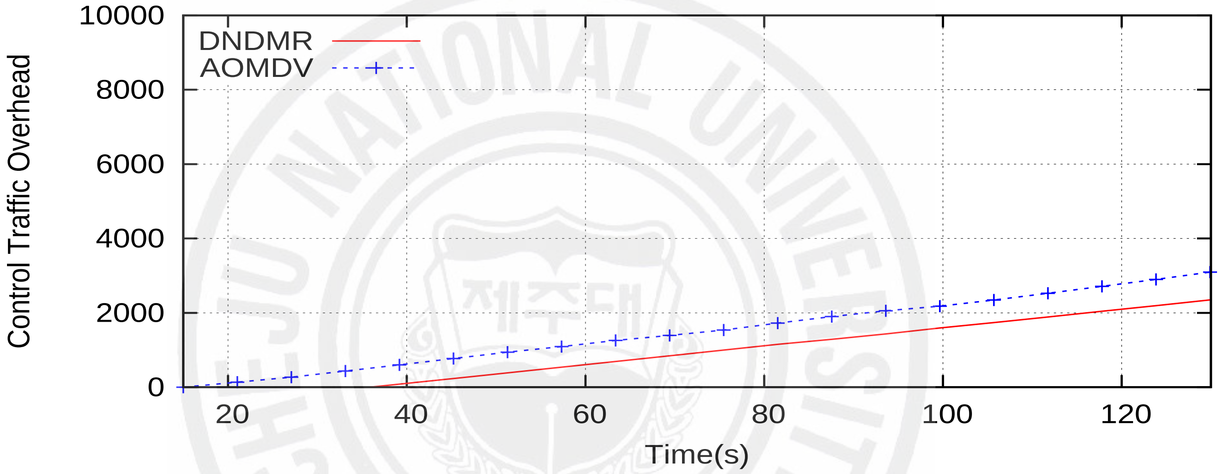

Figure 4.4(d) Control Traffic Overhead: DNDMR vs. AOMDV

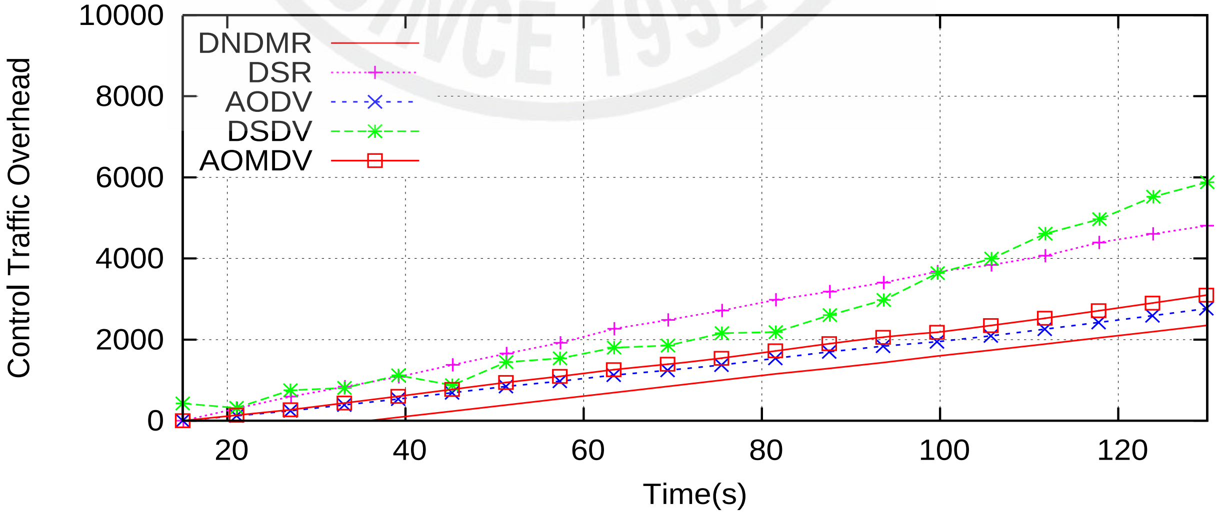

Figure 4.4 Comparative Control Traffic Overhead

End-to-End delay characteristics of DNDMR are analyzed in comparison to DSDV, DSR, AODV and AOMDV. DSDV, DSR and AODV are unicast routing protocols. If the route fails, route needs to be rediscovered which results in longer end-to-end delays. On the other hand, AOMDV is disjoint multipath and DNDMR is node-disjoint multipath routing protocol. If one path fails, the traffic can be re-routed on the remaining path. Path rediscovery needs to initiate only when there is no path available from source to the destination. Therefore, end-to-end delay is relatively less compared to DSDV, DSR, AODV and AOMDV. As seen in Figure 4.5, average end-to-end delay for DNDMR is 20ms, 40ms incase of AOMDV, 65ms incase of DSDV, 60ms incase of DSR and 70ms for AODV. Therefore, DNDMR is 2 times faster than AOMDV, 3 times faster than DSR, 3.25 times faster than DSDV and 3.5 times faster than AODV.

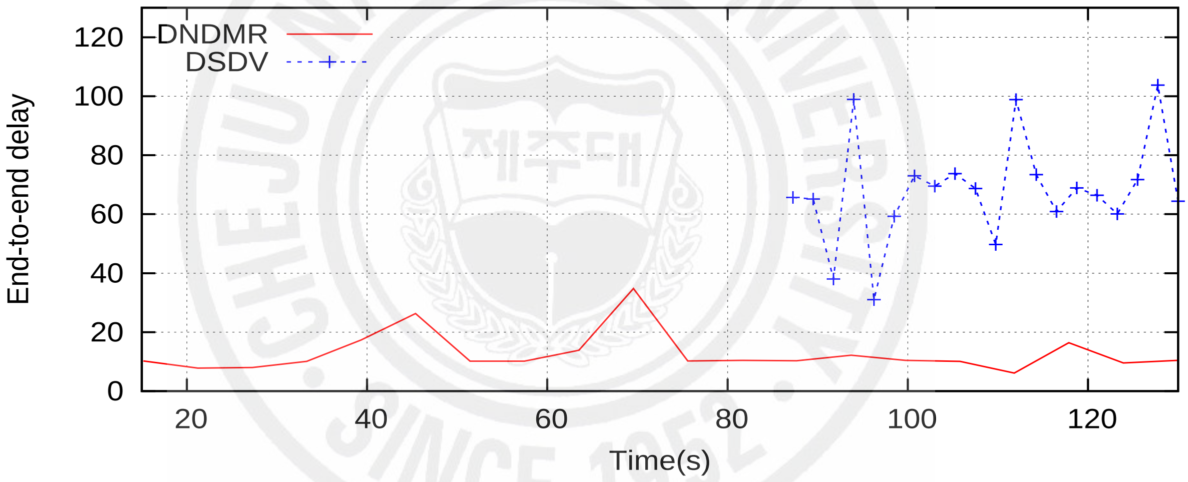

Figure 4.5(a) End-to-End Delay: DNDMR vs. DSDV

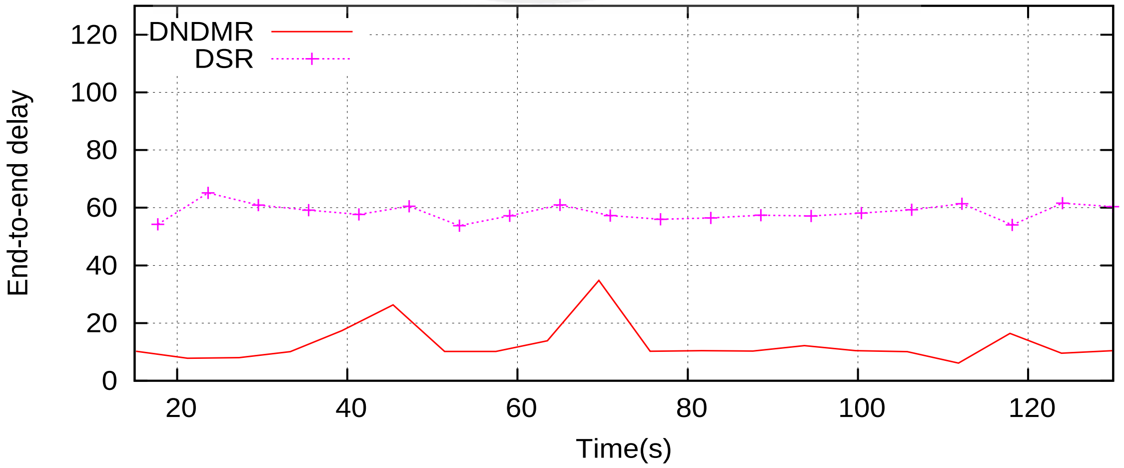

Figure 4.5(b) End-to-End Delay: DNDMR vs. DSR

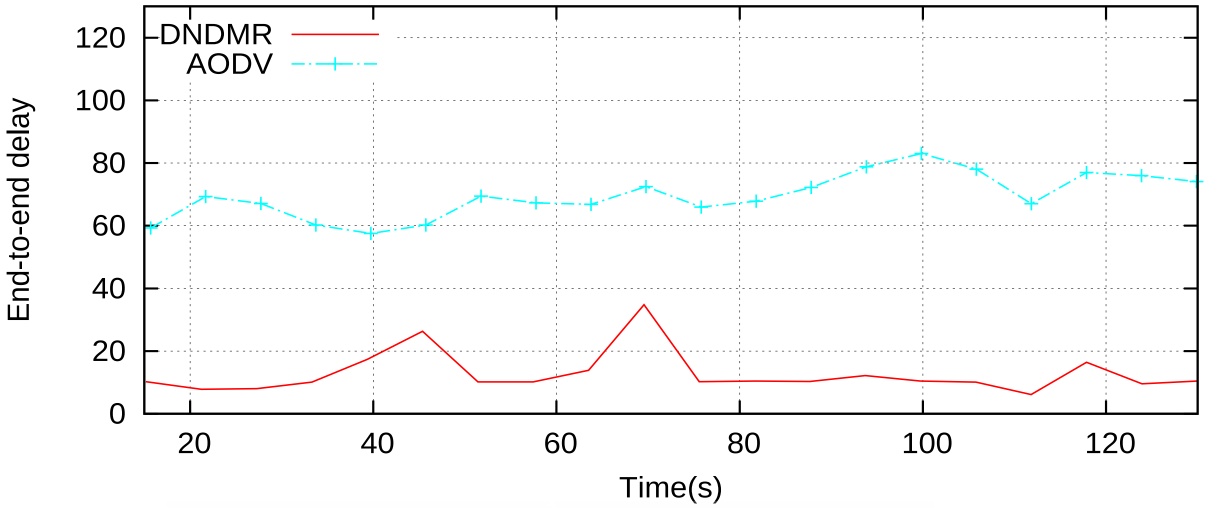

Figure 4.5(c) End-to-End Delay: DNDMR vs. AODV

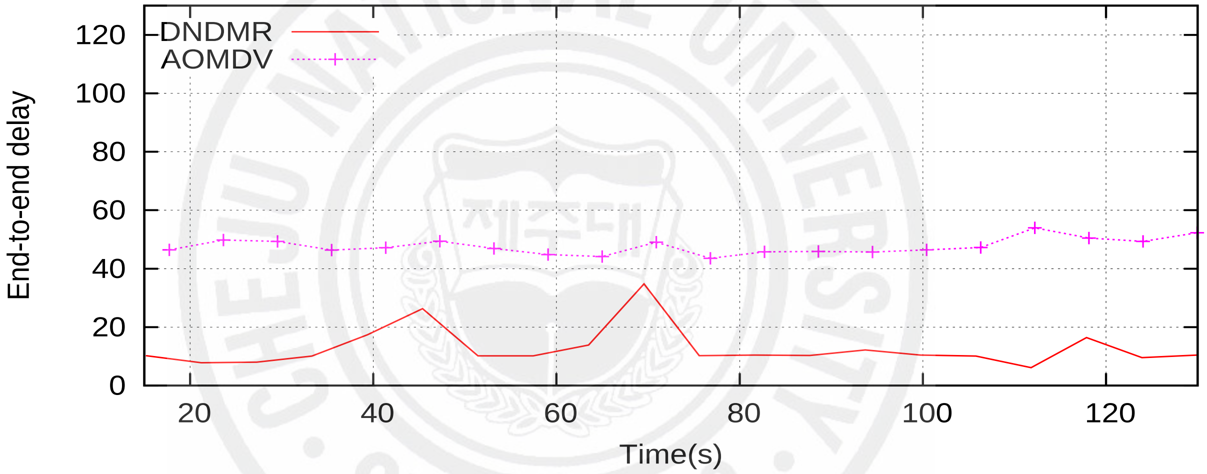

Figure 4.5(d) End-to-End Delay: DNDMR vs. AOMDV

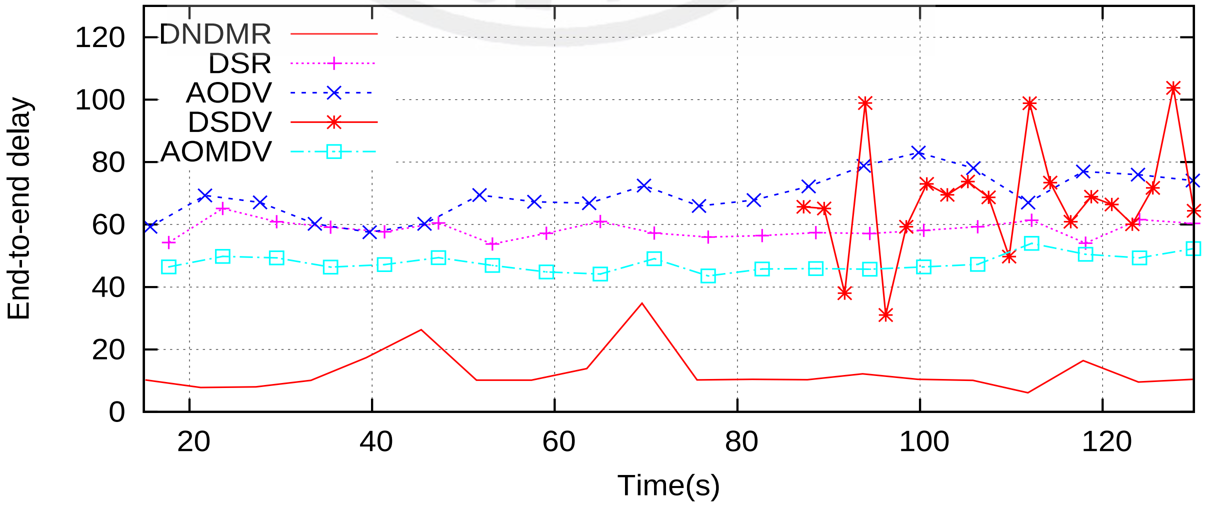

Figure 4.5 End-to-End Delay Comparative

We calculate the throughput as the number of bytes transferred per 5 seconds. The comparative analysis shows that DNDMR throughput is better than that of unipath routing protocols DSDV, DSR, AODV and that of disjoint multipath routing protocol AOMDV as shown in Figure 4.6. The proposed algorithm will perform better in dynamic environments. DNDMR is more fault-tolerant due to the presence of alternate node-disjoint routes. In case of node failure, DNDMR can re-route the traffic on any of the existing alternate paths instead of starting the process of new route discovery. This improves significantly the control traffic overhead, end-to-end delay, and throughput.

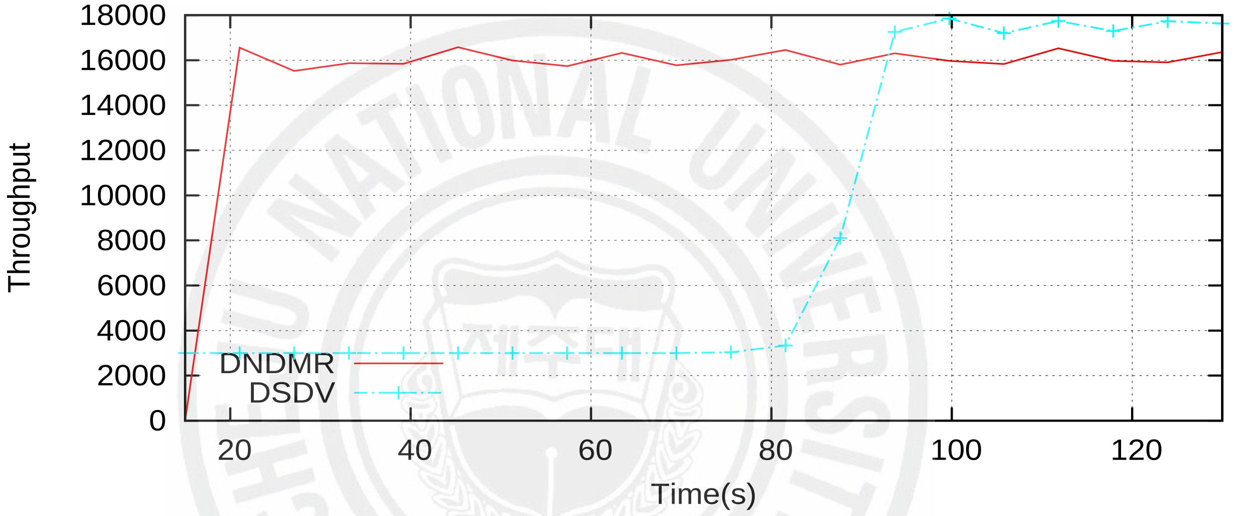

Figure 4.6(a) Throughput: DNDMR vs. DSDV

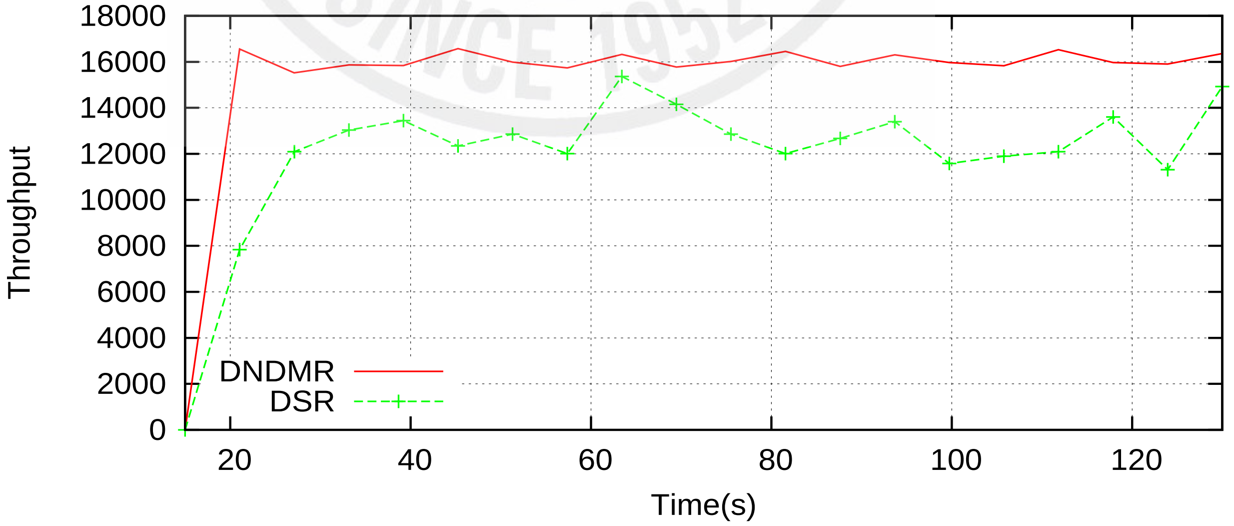

Figure 4.6(b) Throughput: DNDMR vs. DSR

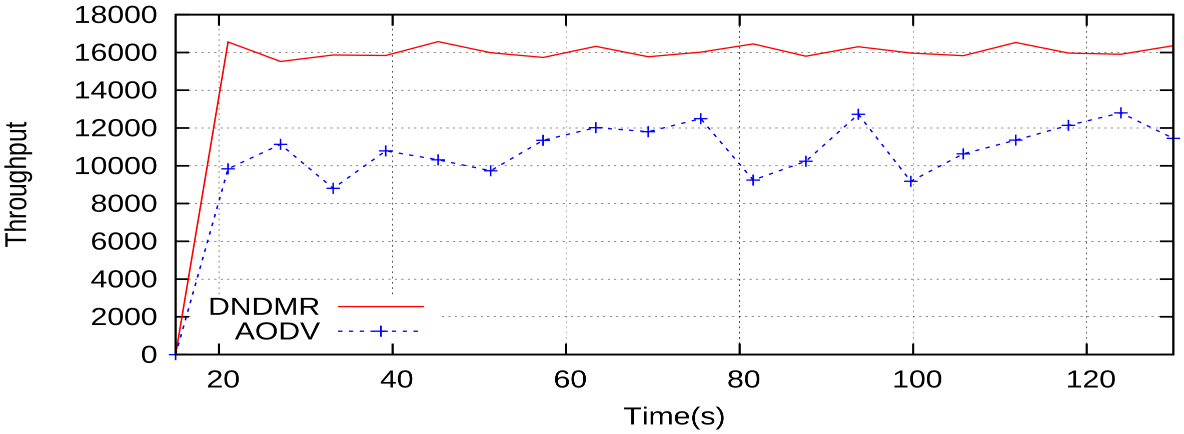

Figure 4.6(c) Throughput: DNDMR vs. AODV

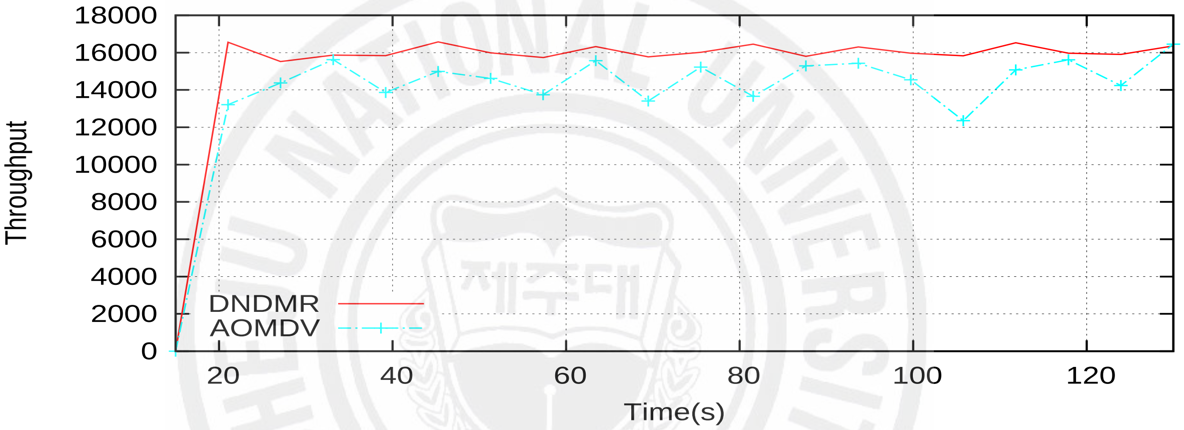

Figure 4.6(d) Throughput: DNDMR vs. AOMDV

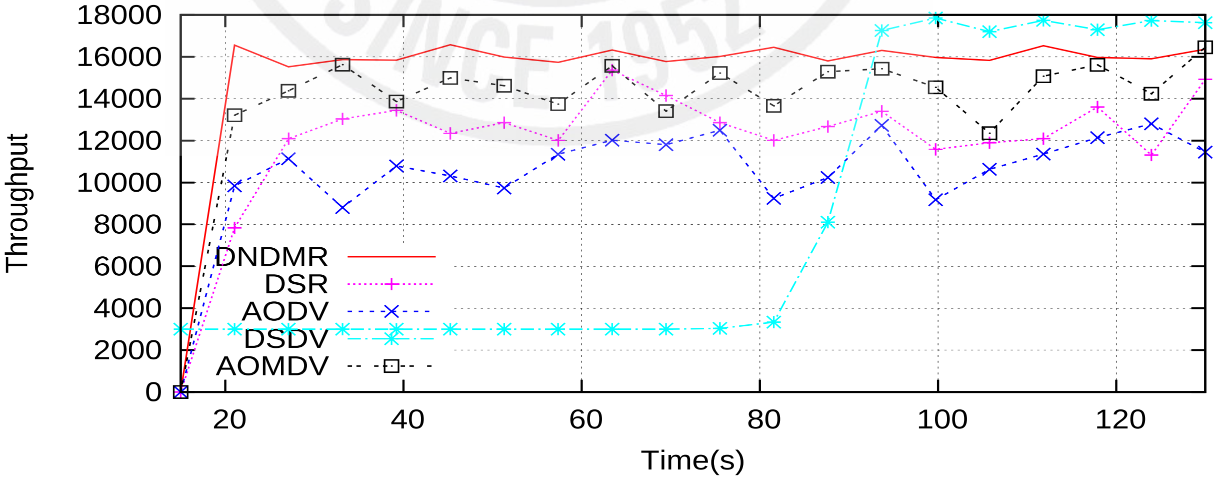

Figure 4.6 Comparative Throughput

Chapter 5 Conclusions

5.1 Conclusions

An ad hoc wireless network is a collection of mobile nodes that communicate with each other by forming a multihop radio network and maintaining connectivity management without an existing network infrastructure. Such networks are expected to play increasingly important roles in future civilian and military applications. Design of efficient and reliable routing protocols in such network are challenging issues. The goal of this research is to explore efficient multipath routing in wireless ad hoc networks.

In chapter 4, we have proposed a novel Directional Node-disjoint Multipath routing (DNDMR) protocol which is an on-demand routing protocol for wireless ad hoc networks. The protocol discovers the two best node-disjoint routes. We evaluate the performance of the proposed protocol using ns-2 simulator. Simulation results show that DNDMR route discovery and packet delivery is more efficient than DSDV, DSR, and AODV, which are the most popular unipath routing protocols, and AOMDV, which is the disjoint multipath routing protocol. The reason is that the proposed protocol discovers node-disjoint routes with minimum control traffic overhead. Also, the availability of more than one alternate path improves reliability. The improvement of the reliability further decreases the end-to-end delay.

5.2 Future Work

Ad-hoc networking is a rather absorbing concept in computer communications. This means that there is much research going on and that many issues remains to be solved. Due to limited time, research work only focuses on node-disjoint multipath routing with very low routing overhead. However there are many issues that could be subject to future studies.

At first, the simulation environment could be improved. These are just some of the improvements that could be made:

- More routing protocols with the dynamic topology
- Measurement of computing complexity

Secondly, there are many issues related to ad hoc networks that could be subject to further studies:

- Multicast: Multicast is the process of sending packets from a transmitter to multiple destinations identified by a single address. The packets of each multicast group are forwarded according to a multicast tree. Multicast routing in mobile ad hoc network is also hard since the network topology changes quite frequently. Therefore frequent maintenance of the multicast tree will result in a substantial amount of control overhead. How to reduce routing overhead has to be considered when designing multicast routing.

- Security: A very important issues that has to be considered is the security in an ad-hoc network. Routing protocols are prime targets for impersonation attacks. Because ad hoc networks are formed without centralized control, security must be handled in a distributed fashion.

- Distributed Power Control: Most wireless devices are battery-powered and hence it is desirable that protocols for wireless networking should be energy efficient. A distributed power control scheme should be taken into account to reduce energy consumption of nodes so that the battery life can be extended longer.

- Quality of Service (QoS): what are the needs for Quality of Service in an ad hoc network? This is related to what the networks actually will be used for.

- Effect of quality of wireless links: The network topology changes frequently, because nodes move in and out of each other’s range. The dynamic nature of the networks combined with poor wireless link’s effects, raises issues that are not easy to address. In the physical layer, some techniques are needed to adapt to rapidly changing channel characteristics to make wireless link quality less sensitive to node performance.

References:

[1] Internet Engineering Task Force (IETF) Mobile Ad Hoc Networks (MANETs) Working Group Charter. http://www.ietf.org/html.charters/manet-charter.html.

[2] Z. J. Haas and S. Tabrizi, “On Some Challenges, and Design Choices in Ad hoc Communications,” *Proc. IEEE, Military Communications Conference (MILCOM)*, Bedford, MA, Oct. 1998, 187-192.

[3] J. Jubin and J. D. Tornow, “The DARPA Packet Radio Network Protocols,” *Proc. IEEE*, 75, 1, Jan. 1987, 21-32.

[4] Y. D. Lin and Y. C. Hsu, “Multi-Hop Cellular: A New Architecture for Wireless Communications,” *Proc. IEEE INFOCOM 2000*, March 2000, 1273-1282.

[5] A. N. Zadeh, B. Jabbari, R. Pickholtz, and B. Vojcic, “Self-Organizing Packet Radio Ad Hoc Networks with Overlay,” *IEEE Communication Magazine*, 40, 6, June 2002, 140-157.

[6] R. Ananthapadmanabha, B. S. Manoj, and C. Siva Ram Murthy, “Multi-Hop Cellular Networks: The Architecture and Routing Protocol,” *Proc. IEEE PIMRC 2001*, 2, Oct. 2001, 78-82.

[7] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” *Comp. Commun. Rev.*, Oct. 1994, 234-244.

[8] S. Murthy and J.J. Garcia-Luna-Aceves, “An Efficient Routing Protocol for Wireless Networks,” *ACM Mobile Networks and App. J.*, Special Issue on Routing in Mobile Communication Networks, Oct. 1996, 183-197.

[9] D. B. Johnson and D. A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” *Mobile Computing*, T. Imielinski and H. Korth, EDS., Kluwer, 1996, 153-181.

[10] Charles E. Perkings, Elizabeth M. Belding-Royer, S. R. Das, “Ad hoc On-Demand Distance

Vector (AODV) Routing," *http:// www.ietf.org/internet-drafts/draft-ietf-manet-aodv-13 .txt, IETF internet draft,* July 2004.

[11] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," *Proc. INFOCOM'97,* Apr. 1997.

[12] S.-J. Lee and M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," *Proc. IEEE Int'l Conf. Comm.,* June 2001, 3201-3205.

[13] L. Wang, Y. Shu, M. Dong, L. Zhang and O. Yang, "Adaptive Multipath Source Routing in Ad Hoc Networks," *IEEE ICC 2001*, 3, june 2001, 867-871.

[14] L. Wang, Y. Shu, Z. Zhao, L. Zhang and O. Yang, " Load Balancing of Multipath Source Routing in Ad Hoc Networks", *Proc. IEEE ICCC'02,* 5, April 2002, 3197-3201.

[15] S.-J. Lee and M. Gerla, "AODV-BR: Backup Routing in Ad hoc Networks," *Proc. IEEE Wireless Communications and Networking Conference (WCNC),* 2000, 1311-1316.

[16] M. K. Marina and S. R. Das, "On-Demand Multipath Distance Vector Routing in Ad Hoc Networks," *Proc. IEEE Int'l Conf. Network Protocols (ICNP),* Nov. 2001, 14-23.

[17] A. Nasipuri and S.R. Das, "On-Demand Multipath Routing for Mobile Ad Hoc Networks," *Proc. IEEE Int'l conf. computer comm. And networks (IC3N),* Oct. 1999.

[18] Z. Ye, S.V. Krishnamurthy and S.K. Tripathi, "A Framework for Reliable Routing in Mobile Ad Hoc Networks," *Proc.IEEE INFOCOM 2003,* 1, Apr. 2003, 270-280.

[19] A. Nasipuri, R. Castaneda and S.R. Das, "Performance of Multipath Routing for On-demand protocols in Mobile Ad Hoc Networks," *ACM/Baltzer Mobile Networks and Applications J. (MONET), 6,* 2001, 339-349.

[20] Kui Wu and Janelle Harms, "On-Demand Multipath Routing for Mobile Ad hoc Networks," *Proc. European Personal Mobile Communication Conference (EPMCC),* Vienna, Austria, Feb 2001.

[21] Y. Xue and K. Nahrstedt, "Fault Tolerant Routing in Mobile Ad Hoc Networks," *Proc. IEEE Wireless Communications and Networking Conference, 2,* March 2003, 1174-1179.

[22] Xuefei Li and Laurie Cuthbert, "Stable Node-Disjoint Multipath Routing with low overhead

in mobile Ad Hoc Networks," *Proc. IEEE Computer Society's 12th Annual Int'l Symposium on Modeling, Analysis and Simulation of Computer amd Telecommunicatons Systems*, Oct. 2004, 184-191.

[23] S. Mueller and D. Ghosal, "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges," *in LNCS, 2965*, 2004.

[24] K. Fall and K. Varadhan, "ns Notes and documentation," *Technical Report, VINT project, UC Berkeley and LBNL*, 1997.

[25] R. Leung, E. Poon, A. C. Chan and B. Li, "MP-DSR: A Qos-aware Multi-path Dynamic Source Routing Protocol for Wireless Ad-Hoc Networks," *26th Annual IEEE International Conference on Local Computer Networks (LCN2001)*, Tampa, FL, United States, Nov. 2001, 132-141.

[26] J. Chen, P. Druschel and D. Subramanian, "An Efficient Multipath Forwarding Method", *Proc. IEEE INFOCOM'98*, San Francisco, CA, Mar. 1998.

[27] J. Raju and J.J. Barcia-Luna-Aceves, "A New Approach to On-demand Loop-Free Multipath Routing," *Proc. Int'l conf. computer comm. And networks (IC3N),*1999, 522-527.

[28] Abhijit Saha, Shafqat Ur Rehman, Gyung-Leen Park, and Junghoon Lee, "Directional Node Disjoint Multipath Routing in Wireless Ad Hoc Network," *Proc. Of the 19th IASTED International Conference on Parallel and Distributed Computing and Systems (PDCS)*, Cambridge, Massachusetts, USA, November 2007, 19-21.

초록

애드혹 네트워크는 기구축된 통신 하부구조나 집중화된 관리 기능이 없이 서로간에 통신할 수 있는 무선 노드들로 구성된다. 이 네트워크에서 각 노드들은 이동성을 가지고 있기 때문에 네트워크 위상이 고정되지 않고 시간에 따라 급격히 변화하게 되며 이에 따라 각 노드들은 하나의 호스트 기능뿐만 아니라 라우터의 기능까지도 수행할 수 있다.

애드혹 네트워크에서 경로배정 프로토콜은 다음과 같은 기능을 수행한다. 첫째, 경로 정보를 교환하고; 홉의 길이, 최소 요구 전력, 무선링크의 생명주기 등과 같은 요구사항과 제약조건을 기반으로 목적지까지의 효율적인 경로를 찾는다. 둘째, 경로 단절여부에 대한 정보를 수집하고, 최소의 프로세싱 파워와 대역폭으로 단절된 경로를 복구한다. 결국, 무선 애드혹 네트워크에서 경로배정 프로토콜은 최소의 제어 오버헤드와 최소의 프로세싱 오버헤드, 빠른 경로 재구성, 루프 발생 방지 등과 같은 요구사항을 갖는다.

본 논문은 무선 애드혹 네트워크에서 주문형 방향성 Node-Disjoint 다중경로배정 프로토콜(DNDMR; Directional Node-Disjoint Multipath Routing) 기법을 제안한다. 일반적으로 다중경로 경로배정 프로토콜은 단일 소스와 단일 목적지간 하나 이상의 경로를 설정하는데 본 논문에서 제안하는 프로토콜의 가장 큰 특징은 1) 방향성을 고려한 독창적인 진행경로 축적기법, 2) 경로 정보 전파 과정에서 노드위치기반 제어에 의한 경로배정 오버헤드 최소화, 3) 자동적인 node-disjoint 경로의 보장 등이다. DNDMR 은 무선 애드혹 네트워크상에서 데이터 통신의 신뢰성을 향상시킬 수 있을 뿐 아니라 총 경로 요청 패킷(RREQ)의 수를 현저히 줄임으로써, 제어 트래픽 오버헤드와 양단간 통신시간을 축소시키고 궁극적으로 통신에 있어서의 처리량을 개선한다. 제어 트래 픽 오버헤드와 양단간 통신시간, 처리량을 고려하여

Ns-2 시뮬레이터로 제안 방법의 성능을 평가하고, 단일경로 배정 프로토콜(DSDV, DSR, AODV)과 다중경로 배정 프로토콜(AOMDV)과의 성능을 비교한다. 시뮬레이션 결과, 각 프로토콜의 제어 트래픽 오버헤드(패킷수)는 DSDV(6000), DSR (5000), AODV (2600), AOMDV (2700), and DNDMR (2300) 이며, DNDMR 이 다른 프로토콜들에 비해 비교적 적다. 양단간 통신지연시간은 DNDMR 이 DSDV(3.25 배), DSR(3 배), AODV(3.5 배), AOMDV(2 배) 보다 빠르다. DNDMR 의 처리량 또한, 다른 프로토콜보다 좋다. 이는 DNDMR 이 기존의 단일경로와 다중경로 배정 프로토콜보다 더 개선된 성능과 신뢰성을 가진다는 것을 나타낸다.

Acknowledgements

There are not enough words of admiration of my advisor Prof. Gyung-Leen Park. I thank him for leading me into this exciting research area and giving me help whenever I need. I am grateful for his constant encouragement, support, supervision and guidance during my M.Sc. in Cheju National University. I would like to extend my sincere gratitude towards Prof. Junghoon Lee for his always encouraging behavior, guidance, precious advices, and extremely helpful attitude. He guided me to think and solve the problems in the academic way, which would be very helpful in my future work and study.

I wish to express my warm and sincere thanks to Prof. Cheol-Soo Kim and Prof. Yoon-Jeong Lee for their useful suggestions and important comments during the process of thesis. I am also grateful to other professors of my department: Prof. IIk-Chan Kim and Prof. Bong-Kyu Lee for their encouragement and guidance during my M.Sc. studies.

I would also like to thank Prof. Khi-Jung Ahn, Prof. Wang-Cheol Song (Dept. of Computer Engineering), Prof. Han-il Kim (Dept. of Computer Education) and Prof. Kyung-Yoon Kim (Dept. of Electronic Engineering) for their help, useful suggestion and continuous support.

I am also grateful of my department staff members. My thanks to Young-Ok Noh for making sure I stay out of trouble. I greatly acknowledge my current and former IT Research Center members: Dr. In-Hye Shin, Dr. Mi-Kyung Kang, Dr. Yong Moon Jin, Soon-Chol Kang, Yong-Ho Lim, Eui-Young Kang, Ji-Ae Kang, and other members Yeon-Ju Jin, Min-Jeong

Ko for their massive help, friendly manner and cooperation. I am extremely grateful to ITRC member Shafqat Ur Rehman for all his extensive help.

I would like to thank my friends at Cheju National University for the good time and the friendship. In particular, my thanks to Dr. Abu Affan, Md. Jasim Uddin, Md. Abu Morshed, Md. Safiqual Islam, Md. Rakib Mansur, Anil Kumar Khambampati, Anji Reddy, Shrikant Saini, A.V. Gunasekaran, Dr. Farrukh Aslam Khan, Dr. Yasantha Athul, Dr. Rohan Karawita, Sarath Senevirathne, Keun-Tak Yang, Jin Long, Sung Hyune, and many others.

This thesis is dedicated to my parents, my elder sister, her husband, and Sneha (my niece), who supported and encouraged me in my difficult time. Without their prayer, love, guidance and support, it would not have been possible to complete my M.Sc. degree in overseas. I thank my father for his wits that I chose this way of my life.

I would like to thank all those whom I have not mentioned above but helped me in numerous ways to success.

December 2007

Abhijit Saha