DESIGN AND SIMULATION OF AN EFFICIENT UNICAST ROUTING PROTOCOL IN MOBILE ADHOC NETWORKS (MANETS)

By

Ghania Quddus

Rabia Khan

Waqas Ahmed

Submitted to Faculty of Computer Science, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment for the requirements of BE Degree in Computer Software Engineering

April 2006

ABSTRACT

DESIGN, IMPLEMENTATION AND SIMULATION OF AN EFFICIENT UNICAST ROUTING PROTOCOL IN MOBILE ADHOC NETWORKS (MANETS)

A mobile ad hoc network differs from wired networks in several respects. Routing protocols are challenged by high mobility, low bandwidth, limited computing capability and limited energy which are the key characteristics of mobile nodes. The protocols for these networks must be designed to keep up with the drastically and unpredictably changing network topology, with minimized message exchanges and utilization of scarce network resources in an efficient manner.

Ad-hoc on demand Distance Vector Routing Protocol (AODV) is intended for use by mobile nodes in an ad hoc network. The dynamism of a route makes it less stable and hence less suitable for a network. The focus has been on enhancing the performance of Ad Hoc on Demand Distance Vector (AODV) routing protocol by choosing Route Fragility Coefficient (RFC) as its metric. This metric causes AODV to find a stable route. The stable route is characterized as the one which has less dynamism and in which nodes stay close to each other. Simulation results are provided to demonstrate improvement in throughput and reduction in routing protocol overhead with increased mobility. The performance metrics are measured by varying the maximum speed of the nodes and size of the network.

DECLARATION

No portion of the work presented in this dissertation has been submitted in support of any other award or qualification either at this institution or elsewhere.

DEDICATION

In the name of Allah, the Most Merciful, the Most Beneficent

To our parents, without whose unflinching support and unstinting cooperation, a work of this magnitude would not have been possible

ACKNOWLEDGMENTS

We wish to thank Almighty Allah who gave us the vigor and determination to complete this project. We gratefully recognize the continuous supervision and motivation provided to us by our Project Supervisor, Head of Department, Col. Raja Iqbal. We would also like to thank Lecturer Ahmad Raza Shahid, for his ever-extended moral and technical support. We deeply treasure the unparallel support and forbearance that we received from our friends for their critical reviews and useful suggestions that helped us in completion of this project. We are also deeply obliged to our families for their never ending patience and support for our mental peace and to our parents for the strength that they gave us through their prayers.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

1 Introduction

A *Mobile Ad-Hoc Network* (MANET) is a decentralized network of autonomous mobile nodes able to communicate with each other. There are several routing schemes that have been proposed and several of these have been extensively simulated or completely implemented as well. Ad-hoc networks are primarily used in improvised environments where communication can be rapidly established between the nodes without requiring any fixed infrastructure.

1.1 Background

Mobile Ad Hoc Networks emerge in a spontaneous manner when a node is within the transmission range of one or more nodes. Unlike conventional wireless networks one may find in offices, universities, communities or homes there is no central entity that controls how, when and where, packets are delivered to each recipient. All communication takes place in an ad hoc manner, which means on the fly and all the nodes in the network participate in relaying packets or messages to each other whenever it is possible for each node to do so. There are several ad hoc routing algorithms at present that have been designed, and many of them also implemented, to make routing decisions at each node [1].

High mobility in MANETs results in major issues like frequent link breakages, packet drops and dynamic topology changes, low channel bandwidth and limited battery power.

Ad-hoc On-Demand Distance Vector Routing Protocol (AODV) is inherently a distance vector routing protocol that has been optimized for ad-hoc wireless networks. It is an on-demand protocol as it finds the routes only when required and is hence also reactive in nature. When mobility routing protocols like DSR [2], DSDV [3], AODV [4] and TORA [5] were evaluated based on the metrics like packet delivery ratio (ratio of the number of packets received to the number of packets sent) and routing overhead (number of routing control packets sent), [6] it concluded that on-demand protocols such as DSR and AODV performed better than table driven ones such as DSDV at high mobility rates. Furthermore, a comparison study of the two on-demand routing protocols: DSR and AODV, using the performance metrics of packet delivery ratio and end to end delay showed that AODV outperforms DSR at heavy traffic load and high mobility.

1.2 Wireless Networks

A wireless network is a flexible data communications system, which uses wireless media such as radio frequency technology to transmit and receive data over the air, minimizing the need for wired connections Wireless networks are used to augment wired networks and are most commonly used to provide last few stages of connectivity between a mobile user and a wired network. Wireless networks use electromagnetic waves to communicate information from one point to another without relying on any physical connection. Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver. The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end. Once data is superimposed

(modulated) onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier. Multiple radio carriers can exist in the same space at the same time without interfering with each other if the radio waves are transmitted on different radio frequencies. To extract data, a radio receiver tunes in one radio frequency while rejecting all other frequencies. The modulated signal thus received is then demodulated and the data is extracted from the signal.

Wireless networks offer the following productivity, convenience, and cost advantages over traditional wired networks:

Mobility: provide mobile users with access to real-time information so that they can roam around in the network without getting disconnected from the network. This mobility supports productivity and service opportunities not possible with wired networks.

Installation speed and simplicity: installing a wireless system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.

Reach of the network: the network can be extended to places which can not be wired

More Flexibility: wireless networks offer more flexibility and adapt easily to changes in the configuration of the network.

Reduced cost of ownership: while the initial investment required for wireless network hardware can be higher than the cost of wired network hardware, overall

installation expenses and life-cycle costs can be significantly lower in dynamic environments.

Scalability: wireless systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations can be easily changed and range from peer-to-peer networks suitable for a small number of users to large infrastructure networks that enable roaming over a broad area.

1.2.1 Mobile Ad-hoc Networks

A Mobile Ad-Hoc Network (MANET) is an infrastructure less collection of mobile nodes that can arbitrarily change their geographic locations such that these networks have dynamic topologies which are composed of bandwidth constrained wireless links.

MANET nodes are equipped with wireless transmitters and receivers. At a given time depending on the nodes positions and their transmitter and receiver coverage patterns and transmission power levels, a wireless connectivity in the form of a random, multi hop graph or ad-hoc network exists between the nodes. This ad-hoc topology may change with time as the nodes move or change their transmission and reception parameters [1].

The possible applications of MANETs are in scenarios with little or no communication infrastructure such as defense operations, emergency search-and-rescue operations, meetings and conventions and other scenarios where quick sharing of information is desired without any fixed infrastructure available [1].

1.2.2 Cellular Networks

A cellular radio network is a radio network made up of a number of radio cells (or just cells) each served by a fixed transmitter, normally known as a base station. These cells are used to cover different areas in order to provide radio coverage over a wider area than the area of one cell. They can be thought of networks that are based on a wired back-bone which connects the base-stations. The base-station nodes have at least one network interface for the wired network and one or more wireless network interfaces to provide communication to the mobile nodes.

Cellular Networks offers number of advantages:

Increased capacity

Reduced power usage

Better coverage

The primary requirement for a network in the cellular concept is a way for each distributed station to distinguish the signal from its own transmitter from the signal from other transmitters. There are two common solutions to this, frequency division multiple access (FDMA) and code division multiple access (CDMA).

Practically every cellular system has some kind of broadcast medium. This can be used directly for distributing information to multiple mobiles, commonly, for example, in mobile telephone systems; the most important use of broadcast is to set up channels for one to one communication between the mobile transceiver and the base station.

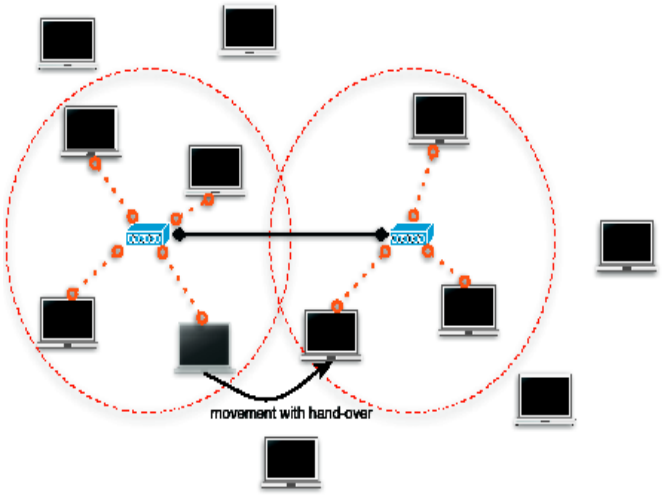

Figure 1-1: Cellular Network

The communication of the mobile node is only possible over a one-hop link to base-station. Direct links between nodes or multi-hop links to the base-station are not possible. The transmission range of the base-stations limits the size of a cellular network. If the node is out of the transmission range of the base-stations, no communication is possible. Inside the area covered by the base-stations it may move without losing connection and if it leaves the transmission range of the current base-station, a hand-over to a another base-station will let the node communicate seamlessly.

1.2.3 Multi-hop Cellular Network

In multi-hop cellular networks the two concepts described before are combined. On one hand there is a cellular network; on the other hand there are mobile nodes with additional routing facilities.

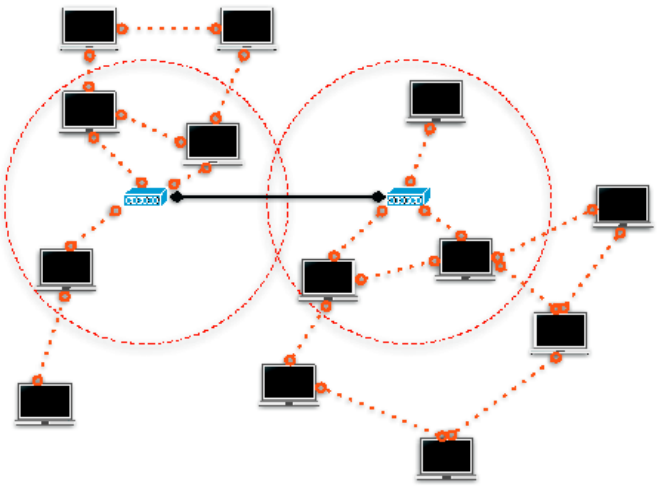

Figure 1-2: MultiHop Cellular Network

With this approach it is possible to have multiple hops between a mobile node and a base-station. The idea is to benefit from existing infrastructure and to gain more efficiency out of it, to cover wider areas with less fixed antennas and base-stations and to reduce power consumption due to shorter hop distances.

1.3 MANET

With recent performance advancements in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly widespread use and application, much of which will involve the use of the Internet Protocol (IP) suite. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly changing, random, multi-hop topologies, which are likely composed of relatively bandwidth-constrained wireless links.

A Mobile Ad-Hoc Network (MANET) is a decentralized network of autonomous mobile nodes able to communicate with each other over wireless links. Due to the mobility of the nodes, the topology of the network may rapidly be changing, making it impossible to use conventional routing tables maintained at fixed points (routers). Instead, each node is required to determine the best route to a given destination node by itself.

Given their dynamic nature, route discovery in a MANET differs significantly from the more or less static routes in wired networks: Not all nodes in a MANET necessarily have the same capabilities. Two nodes, even if they are direct neighbors, may differ with respect to signal strength, available power, reliability etc.

These differences require much more complicated and particularly more active routing protocol in order to maintain an accurate picture of the networks topology, while at the same time providing scalability for potentially large (and ever-growing) networks. At the same time, route discovery must not use up the majority of the often limited bandwidth available to mobile devices.

A wireless routing protocol in a MANET is the methodology or algorithm by which routes are created often with the help of routing tables in intermediate nodes in order to enable nodes to send packets to each other in a manner that is as efficient, reliable and error free as possible.

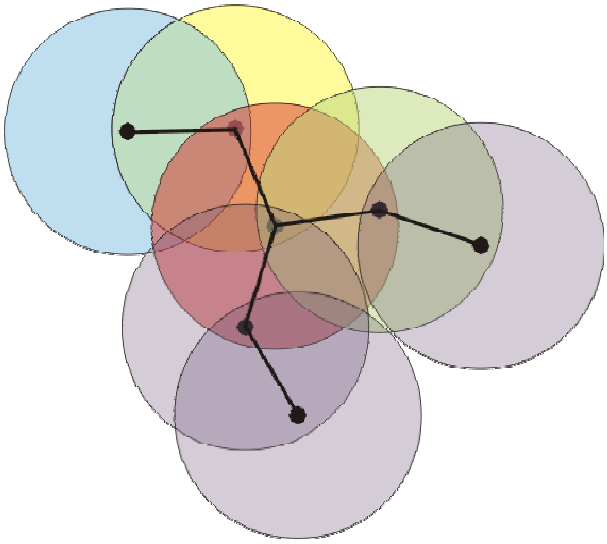

Figure 1-3: Mobile Adhoc Network

A MANET may operate in isolation, or may have gateways to and interface with a fixed network [6]. MANET nodes are equipped with wireless transmitters and receivers using antennas that may be omni-directional (broadcast), highly directional (point-to-point), possibly steerable, or some combination thereof. They are assumed to be mobile and communicate with each other wirelessly. The nodes in a MANET can be just about anything from micro-sensor equipped nodes to Personal Digital Assistants (PDAs) to laptops or even computer systems embedded in vehicles. If one node needs to send a message to another node, it often has to send the message through multiple hops or intermediate nodes which themselves may be moving, thus causing frequent disconnections in the communication network.

MANETS have proved popular in new and exciting applications for three basic reasons; (a) They can be deployed easily in several situations (nodes could possibly drop into place by hand or by an airplane), (b) They can be deployed quickly and hopefully with economies of scale, cheaply as well and (c) They can lead to

decreased dependence on prior or fixed infrastructure or provide alternative infrastructure in areas where current infrastructures fail.

1.4 Unicast Vs Multicast:

A routing protocol is the mechanism by which user traffic is directed and transported through the network from the source node to the destination node. Objectives include maximizing network performance form the application point of view - application requirements- while minimizing the cost of network itself in acordance with its capacity . The application requirements are hop count, delay, throughput, loss rate, stability, jitter, cost, etc; and the network capacity is a function of available resources reside at each node and number of nodes in the network as well as its density, frequency of end-to-end connection (i.e. number of communication), frequency of topology changes (mobility rate).

1.4.1 Unicast Routing Protocols:

Most high-level network protocols (such as the ISO Transport Protocols or TCP or UDP) only provide a unicast transmission service. That is, nodes of the network only have the ability to send to one other node at a time

All transmission with a unicast service is inherently point-to-point. If a node wants to send the same information to many destinations using a unicast transport service, it must perform a replicated unicast, and send N copies of the data to each destination in turn[7].

1.4.2 Multicast Routing Protocols:

A better way to transmit data from one source to many destinations is to provide a multicast transport service. With a multicast transport service, a single node can send data to many destinations by making just a single call on the transport service.

For those applications that involve a single node sending to many recipients, a multicast facility is clearly a more natural programming paradigm than unicast. However, the benefits of multicast are more than just logical. Many underlying transmission media (such as Ethernet) provide support for multicast and broadcast at the hardware and media-access level. When a multicast service is implemented over such a network, there is a huge improvement in performance. If the hardware supports multicast, a packet that is destined for N recipients can be sent as just a single packet [8].

Multicast is useful because it allows the construction of truly distributed applications, and provides important performance optimizations over unicast transmission. There are a number of applications for real-time audio and video conferencing that can make good use of a multicast service when it is available.

1.5 Classification of Routing Protocols

Routing protocols govern the routing mechanism in a network. Routing protocols are classified according to the routing mechanism. It depends on the way the routes are discovered and maintained by the nodes.

1.5.1 Proactive Routing Protocols

Proactive routing attempts to maintain routes to all destinations at all times, regardless of whether they are needed. All nodes should in theory, know the whole network. This results in a constant overhead of routing traffic, but no initial delay in communication. To support this, the routing protocol propagates information updates about a network's topology or connectivity throughout the network [9]. Information updates can be topology-driven, which are generated when connectivity in the network is detected or periodic which generates connectivity information at fixed intervals; or both.

Topology-driven updates provide optimal routes if network connectivity is stable, while periodic updates limit overhead deterministically at the expense of route optimality and responsiveness. These updates can be incremental (include only route changes) or full (include all route information). These frequent updates may consume large amounts of bandwidth that comes as a disadvantage associated with proactive routing protocols.

Traditional routing protocols such as Open Shortest Path First (OSPF), DSDV (Destination-Sequenced Distance Vector Routing) and OLSR (Optimized Link State Routing) are examples of proactive routing protocols [10].

1.5.2 Reactive Routing Protocols

Reactive routing protocols have seen much popularity in ad hoc networks research. This is due to several good reasons, including the battery savings achieved by not transmitting anything during idle periods. Reactive or on-demand routing protocols

determine routes only when there is data to send. If a route is unknown, the source node initiates a search to find one, which tends to cause a traffic surge as the query is propagated through the network. Nodes that receive the query and have a route to the requested destination respond to the query.

Data sent in networks using reactive protocols do tend to suffer a delay during the search for a route. Under highly dynamic link conditions, reactive protocols are expected to generate less overhead and provide more reliable routing than proactive routing, but at the cost of finding the optimal route. Examples of reactive protocols include Temporally-Ordered Routing Algorithm (TORA) and Ad Hoc On Demand Distance Vector (AODV) [11].

1.5.3 Hybrid Routing Protocols

Both a purely proactive or purely reactive approach to implement a routing protocol for a MANET has its disadvantages. Another approach that combines the advantages of both into a *hybrid* scheme, taking advantage of pro-active discovery within a node's local neighborhood, and using a reactive protocol for communication between these neighborhoods is known as Hybrid Routing Protocol. Example of Hybrid Routing Protocol is ZRP (Zone Routing Protocol).

The separation of node's local neighborhood from the global topology of the entire network allows for applying different approaches – and thus taking advantage of each technique's features for a given situation. These local neighborhoods are called zones (hence the name); each node may be within multiple overlapping zones, and each zone may be of a different size. The "size" of a zone is not determined by geographical measurement, but is given by a radius of length 'α' where α is the

number of hops to the perimeter of the zone. The nodes on the perimeter of a zone (with a hop-count= α) referred to as peripheral nodes and nodes with hop-count< α are interior nodes[12].

ZRP consists of two components. IARP (Intra Zone Routing Protocol) is meant for routing within the nodes of a zone. This protocol is used by a node to communicate with the interior nodes of its zone and as such is limited by the zones radius 'α' (the number of hops 'α' from the node to its peripheral nodes). IAPR is a proactive, table-driven routing protocol. The node continuously needs to update the routing information in order to determine the peripheral nodes as well as maintain a map of which nodes can be reached locally. When a global route search is needed, the IARP's routing zones can be used to efficiently guide route queries outwards (via bordercasting) rather than blindly relaying queries from neighbor to neighbor. The proactive maintenance of routing zones also helps improve the quality of discovered routes, by making them more robust to changes in network topology.

However, IERP takes up advantage of the known local topology of a node's zone and using a reactive approach enables communication with nodes in other zones. Route queries within the IERP are issued on demand that is only when a request for a route is made [12].

1.5.4 Geographical Routing Protocols

Geographical routing protocols make use of the geographical location of a node to make routing decisions. Such location information would generally be acquired either from GPS satellites, or from location interpolation given the positions of neighboring nodes. In addition to knowing its own geographical location, a node also needs to

know the locations of its neighbors, as well as the location of its intended destination. Dream (Distance Routing E_ect Algorithm for Mobility) [13] and Grid Location Service [14] are mechanisms for finding out the location of any given node in the network. In Dream, nodes periodically flood their location information throughout the network. However, as the flood travels away from the source, the speed with which updates are propagated is decreased, thereby drastically reducing the overall overhead of the protocol.

Geographic routing protocols include Greedy Perimeter State-less Routing (GPSR) and Location Aided Routing (LAR). GPSR greedily routes packets to the one-hop neighbor that is closest to the destination. Should an obstacle appear between source and destination, GPSR uses a planarized version of the network graph, and follows the ”right hand rule” to route around the obstacle.

However, geographical routing relies heavily on two assumptions: a) that each node knows its position, b) the geographical distance between nodes corresponds well to the distance between these nodes in the network topology. In many situations, these assumptions are unacceptable.

1.6 Applications of MANETS

Mobile Ad-Hoc Networks (referred to as MANETs), are impromptu wireless communication networks increasingly appearing in the Commercial, Military, and Private sector as portable wireless computers become more and more ubiquitous. Mobile Ad-Hoc Networks allow users to access and exchange information regardless of their geographic position or proximity to infrastructure. In contrast to the infrastructure networks, all nodes in MANETs are mobile and their connections are

dynamic. Unlike other mobile networks, MANETs do not require a fixed infrastructure. This offers an advantageous decentralized character to the network. Decentralization makes the networks more flexible and more robust.

Applications for MANETs are wide ranging and have use in many critical situations: An ideal application is for search and rescue operations. Such scenarios are characterized by the lack of installed communications infrastructure. This may be because all of the equipment was destroyed, or perhaps because the region is too remote. Rescuers must be able to communicate in order to make the best use of their energy, but also to maintain safety. By automatically establishing a data network with the communications equipment that the rescuers are already carrying, their job made easier.

A commercial application for MANETs includes ubiquitous computing. By allowing computers to forward data for others, data networks may be extended far beyond the usual reach of installed infrastructure. Networks may be made more widely available and easier to use.

Another application of MANETs is sensor networks. This technology is a network composed of a very large number of small sensors. These can be used to detect any number of properties of an area. Examples include temperature, pressure, toxins, pollutions, etc. The capabilities of each sensor are very limited, and each must rely on others in order to forward data to a central computer. Individual sensors are limited in their computing capability and are prone to failure and loss. Mobile ad-hoc sensor networks could be the key to future homeland security.

1.7 Problem Statement

"To design and simulate a uni-cast routing protocol for mobile ad-hoc networks that achieves a maximum packet delivery ratio (PDR) in any network topology, minimum end to end delay and using the results for analysis with other standard routing protocols for a regressive assessment of the work."

1.8 Project Domain

Routing protocols implement algorithms that tell routers the best paths through internetworks. Routing is a layer 3 function, thus, routing and routed protocols are network-layer entities. Development of a uni-cast routing protocol means working at the network layer which is the third layer of Open System Interconnection (OSI) model. Any new idea that is generated is first simulated to see how much it is successful. Where it can be improved and what should be changed to make it better. Mobile ad-hoc networks are currently in the research phase. New ideas are developed and then simulations are performed to check out the performance.

The aim was to do something inventive, generate new ideas and test them in a field that in the coming years would revolutionize the world. The importance of simulations and amount of learning one gets from using good simulators served as an inspiration to make a new routing protocol and then simulate it using the most famous simulator used in networking which is 'the network simulator NS-2'. Development of a routing protocol meant advanced study of already implemented routing protocols and their merits and demerits.

2 Research Objectives

2.1 Project Goals and Objectives

The objectives of the project were: (a) design a uni-cast routing protocol for MANETs which adjusts to the changing topology of the network, is scalable and has a maximum throughput and minimum end to end delay, (b) implement it in C++, (c) simulate it in the network simulator (NS-2) and (d) compare its performance with other standard uni-cast routing protocols.

2.2 Deliverables

The deliverables of the project are: (a) compiled C++ code of AODV_RFC, (b) mobility and traffic scenarios in OTcl, (c) awk script and (d) trace graph.

The scenario files and connection pattern files are created prior to execution of Network Simulator. These files are further used by the simulation script. The execution of the simulation script results in trace files with an extension '.tr' and nam files with an extension '.nam'. The NS-2 offers a tool called tracegraph that takes as an imput .tr file and delivers a tracegraph that can be analyzed for throuput. Similarly NAM tool takes .nam files as an input and results in an animation.

3 Literature Review

3.1 Introduction

The On demand routing algorithms find a route only when desired by a source node. Under highly dynamic link conditions, reactive protocols are expected to generate fewer overhead messages and provide a more reliable routing than proactive routing protocols. There is no updating of every possible route in the network instead it focuses on routes that are being used or being set up. AODV, ABR, DSR, SSA are the examples of On demand routing algorithms.

3.2 AODV (**A**dhoc **O**n demand **D**istance **V**ector Routing Protocol)

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner.

The operation of AODV is loop-free, and by avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link. One distinguishing feature of AODV is its use of a

destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number.

When a source node intends communicating with a destination node whose route is not known, it broadcasts a ROUTE REQUEST packet. Each ROUTE REQUEST packet contains an ID, source and the destination node IP addresses and sequence numbers together with a hop count and control flags. The ID field uniquely identifies the ROUTE REQUEST packet; the sequence numbers indicate the freshness of control packets and the hop-count maintains the number of nodes between the source and the destination. Each recipient of the ROUTE REQUEST packet that has not seen the Source IP and ID pair or doesn't maintain a fresher (with larger sequence number) route to the destination rebroadcasts the same packet after incrementing the hop-count. Such intermediate nodes also create and preserve a REVERSE ROUTE to the source node for a certain interval of time. When the ROUTE REQUEST packet reaches the destination node or any node that has a fresher route to the destination a ROUTE REPLY packet is generated and unicast back to the source of the ROUTE REQUEST packet. Each ROUTE REPLY packet contains the destination sequence number, the source and the destination IP addresses, route lifetime together with a hop count and control flags. Each intermediate node that receives the ROUTE REPLY packet, increments the hop-count, establishes a FORWARD ROUTE to the source of the packet and transmits the packet on the REVERSE ROUTE.

3.3 ABR (**A**nt **B**ased **R**outing Protocol):

The Associativity-Based Routing (ABR) protocol is free from loops, deadlock, and packet duplicates, and defines a new routing metric for ad-hoc mobile networks. This metric is known as the degree of association stability. In ABR, a route is selected based on the degree of association stability of mobile nodes. Each node periodically generates a beacon to signify its existence. When received by neighboring nodes, this beaconing causes their associativity tables to be updated. For each beacon received, the associativity tick of the current node with respect to the beaconing node is incremented.

Association stability is defined by connection stability of one node with respect to another node over time and space. A high degree of association stability may indicate a low state of node mobility, while a low degree may indicate a high state of node mobility. Associativity ticks are reset when the neighbors of a node or the node itself moves out of proximity. A fundamental objective of ABR is to derive longer-lived routes for ad-hoc mobile networks.

The three phases of ABR are:

Route discovery,

Route re-construction (RRC),

Route deletion.

The route discovery phase is accomplished by a broadcast query and await-reply (BQ-REPLY) cycle. A node desiring a route broadcasts a BQ message in search of mobiles that have a route to the destination. All nodes receiving the query (that are not the destination) append their addresses and their associativity ticks with their

neighbors along with QoS information to the query packet. A successor node erases its upstream node neighbors' associativity tick entries and retains only the entry concerned with itself and its upstream node. In this way, each resultant packet arriving at the destination will contain the associativity ticks of the nodes along the route to the destination. The destination is then able to select the best route by examining the associativity ticks along each of the paths. In the case where multiple paths have the same overall degree of association stability, the route with the minimum number of hops is selected. The destination then sends a REPLY packet back to the source along this path. Nodes propagating the REPLY mark their routes as valid. All other routes remain inactive and the possibility of duplicate packets arriving at the destination is avoided.

3.4 DSR (**D**ynamic **S**ource **R**outing Protocol)

The *Dynamic Source Routing* protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two mechanisms of *Route Discovery* and *Route Maintenance*, which work together to allow nodes to discover and maintain *source routes* to arbitrary destinations in the ad hoc network. The use of source routing allows packet routing to be trivially loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded, and allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use. All aspects of the protocol operate entirely *on-*

demand, allowing the routing packet overhead of DSR to scale *automatically* to only that needed to react to changes in the routes currently in use.

The DSR protocol allows nodes to dynamically discover a *source route* across multiple network hops to any destination in the ad hoc network. Each data packet sent then carries in its header the complete, ordered list of nodes through which the packet must pass, allowing packet routing to be trivially loop-free and avoiding the need for up-to-date routing information in the intermediate nodes through which the packet is forwarded. By including this source route in the header of each data packet, other nodes forwarding or overhearing any of these packets may also easily cache this routing information for future use.

The protocol consists of two major phases:

Route Discovery.

Route Maintenance.

When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it already has a 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 by broadcasting a route request packet. This route request contains the address of the destination, along with the source node's address and a unique identification number.

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 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 been seen by the mobile and if the A route reply is generated when either the route request reaches the destination itself, or when it reaches an intermediate node which contains in its route cache an unexpired route to the destination [4]. 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.

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. Route maintenance is accomplished through the use of route error packets and acknowledgments.

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 hop are truncated at that point. In addition to route error messages, acknowledgments are used to verify the correct operation of the route links. Such acknowledgments include passive acknowledgments, where a mobile is able to hear the next hop forwarding the packet along the route.

3.5 SSA (**S**ignal **S**tability-Based **A**daptive Routing Protocol)

The SSA protocol performs on-demand route discovery by selecting longer-lived routes based on signal strength and location stability. The signal strength criterion

allows the protocol to differentiate between strong and weak channels. Each channel is characterized as strong or weak by the average signal strength at which packets are exchanged between the hosts at either end of the channel. The location stability criterion biases the protocol toward choosing a channel which has existed for a longer period of time. Together, these two concepts form the signal stability criterion that chooses strong channels which have been in existence for a time greater than some threshold.

A source initiates a route discovery request when it has data to send to a destination that is not in the routing table. The route search is broadcast to all neighboring hosts. These hosts propagate the broadcast if it is received over a strong channel and the request has not been propagated previously (to avoid looping). The route search packet stores the address of each intermediate host in the route taken. The destination chooses the route recorded in the first arriving request, since this route is probably shorter and less congested than routes for slower-arriving requests. The destination returns the route reply along the selected route, and each intermediate node includes the new next-hop, destination pairs in its routing table.

Functionally, the SSA protocol consists of two protocols, the Forwarding Protocol (FP) and the Dynamic Routing Protocol (DRP), which utilize the extended device driver interface. This interface is responsible for making available to the routing protocols the signal strength information from the device. DRP maintains the routing table by interacting with the DRP on other hosts. FP performs the actual routing table lookup to forward a packet onto the next hop.

The Forwarding Protocol (FP) and Dynamic Routing Protocol (DRP) work together to route packets in the ad hoc network. Two tables are maintained to enable SSA routing: the Signal Stability Table and the Routing Table

Each host sends out a link layer beacon[1] to its neighbors once every time quantum, denoted by a *click*. Every host receiving this beacon records the *signal strength* at which the beacon was received in the Signal Stability Table (SST). Each host also classifies its neighbors as strongly connected (*SC*, hence belonging to the *SC set*) if the host has been receiving strong beacons from the neighbor for the past few clicks. The neighbor is otherwise classified as weakly connected (*WC*, hence belonging to the *WC set*). A host marked as SC in the SST also has an entry in the Routing Table (RT) which stores destination and next-hop pairs for each known route.

The FP functions by looking up the destination in the RT and forwarding the packet on the next hop for the destination. When there is no entry for the destination in the RT, the FP initiates a *route search* to find a route to this destination. The route search message has a hop list which records the path taken by the message. Each intermediate DRP uses this list to prevent loops and adds its own address to the hop list. Although the destination DRP may receive multiple copies of a route search message, it simply selects the route contained in the first arriving message and tunnels a *route reply* message on the reverse path to the source. The DRP at each intermediate host installs the appropriate next-hop entry for the destination and the source in its RT. When a route reply message is received, the DRP at the source updates the RT, and the FP routes the data via the next hop found in the RT.

A route may become unavailable due to migration of the hosts along the route. When a host moves out of range of its neighbors or shuts down, the neighbors will recognize that the host is unreachable since they no longer receive beacons from that host. The DRP will modify the SST and RT to reflect the changes. Any routes that have this unreachable host as the next hop will become invalid.

Route maintenance is triggered when a host has data to send over a failed link. Intermediate nodes send an error message to the source when such a failure occurs. The source host sends a route-search packet to find a new route and sends an erase message to remove the old route. The erase message should reach the intermediate host which discovered the failed next-hop.

4 Design

4.1 Introduction

The design specifies the assumptions that are assumed while designing the respective protocol. The assumptions are made to approximate the real world scenario. The Random Way Point Model selected for the routing protocol governs the movement of the nodes. Energy usage optimization is an important issue and a critical design factor for mobile ad hoc networks (MANETs). Free Space Path is used to predict the received signal power of each packet.

4.2 Assumptions

The protocol is designed for the mobile ad hoc networks and the network is assumed to consist of a set of mobile wireless nodes. The nodes move according to the "random waypoint" model. Each node moves in a piece-wise linear trajectory with a constant velocity that is chosen randomly. The nodes pause for a set time before changing direction. The power at which the nodes transmit is assumed to be constant. A Freespace path loss model is assumed to characterize the received power at a node.

In order to discover a route, each node is assumed to broadcast a route request packet. The route request packet is assumed to ripple through the network till it reaches the destination. The destination replies to one or more route requests.

It is assumed in this document that all nodes wishing to communicate with other nodes within the ad hoc network are willing to participate fully in the network. In particular, each node participating in the ad hoc network should also be willing to forward packets for other nodes in the network. The diameter of an ad hoc network is the minimum number of hops necessary for a packet to reach from any node located at one extreme edge of the ad hoc network to another node located at the opposite extreme. Packets may be lost or corrupted in transmission on the wireless network. It is assumed that a node receiving a corrupted packet can detect the error and discard the packet. Nodes within the ad hoc network may move at any time without notice, and may even move continuously, but it is assumed that the speed with which nodes move is moderate with respect to the packet transmission latency and wireless transmission range of the particular underlying network hardware in use. Wireless communication ability between any pair of nodes may at times not work equally well in both directions, for example due to differing antenna or propagation patterns or sources of interference around the two nodes. That is, wireless communications between each pair of nodes will in many cases be able to operate bidirectional, but at times the wireless link between two nodes may be only unidirectional, allowing one node to successfully send packets to the other while no communication is possible in the reverse direction. Bi-directional links are assumed in the protocol.

4.3 Overview

The routing metric specifies the measure on which the “goodness” of routes will be calculated. The route finally chosen depends on the value of this metric. Before

choosing a route the destination analyzes the values of metric for each route and picks the best route based on the value of the metric.

4.3.1 Routing Metric and Protocol Overview

The performance of routing protocols depends on the quality of the routes chosen in terms of route longevity, the manner in which route failures are handled and the protocol overhead introduced in the process. A protocol that discovers better routes also features a reduced rate of route failures and lesser route discovery traffic. Thus an important aspect of the decision process is to compare and pick the better route.

Intuitively, a route consisting of nodes that stay together while being mobile, will last longer. In other words, if the nodes in a route move such that they remain within the transmission range of the same neighbors for a longer duration, the route stays valid for a longer duration. The metric used in this protocol is Route Fragility Coefficient (RFC), a metric which describes how dynamic a route is. More static routes (which last longer) are represented by a lower value of RFC.

The computation of RFC proceeds in two steps. First, on receiving a Route Request (RREQ) packet, each node on the route computes the extent by which the link to its previous hop is contracting or expanding. Assuming a Freespace path loss model, we examine the received power of two successive packets. If the nodes are moving apart the second power measurement is lesser. The extent of expansion or contraction is captured by a function of the received power samples which represents the relative speed of the two nodes within proportionality constant. The result is then added to the counters in RREQ (one for expansion and the other for contraction).

Second, the destination collects multiple RREQs and employs a function of the number of hops and the value of RFC for the routes represented by each RREQ, to arrive at the best route. Employing a simple inequality to decide which metric is better, the destination chooses the RREQ representing the best route and replies to it.

4.3.2 Routing Metric

This section explains the metric used to describe the dynamic nature of a route. In order to compute this metric, estimation of the rate at which the separation between each adjacent pair of nodes in the route is increasing (expansion) or decreasing (contraction). A measure of such an expansion or contraction is given by the relative speed of the nodes. Consider a node n1 receiving packets from a node n2. Let t1 and t2 be the times at which the last two packets from n2 were receiv ed. Denote the received power for these packets as P1 and P2. We consider two possible situations, viz., the nodes are moving closer (P1 > P2) or are moving apart (P1 < P2).

Fig 4-1 indicates two nodes n1 and n2, with d1 and d2 being distances corresponding to the positions of node n2 at received powers of P1 and P2. To estimate the relative speed of the nodes, we do not need the exact position of the two nodes as shown below. This is indicated by the two circles which indicate all the possible positions in which n2.

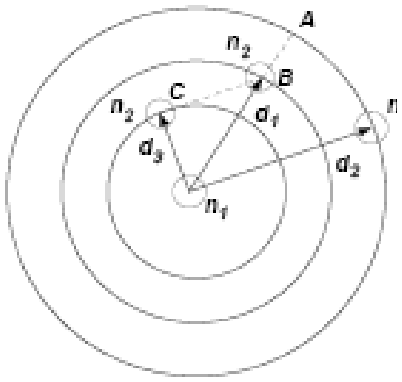

Figure 4-1: Schematic showing two positions of node n2 relative to n1

Assuming a free space path loss model, we have:

$$P_i = \frac{K}{d_i^2} \Rightarrow \frac{d_i}{\sqrt{K}} = \frac{1}{\sqrt{P_i}} \qquad \textbf{(4-1)}$$

Here K denotes a constant that depends on the antenna gains of the two nodes and the wavelength of the transmission. Since the nodes are assumed to be moving with a constant velocity in a piecewise linear manner, we can then write the following.

$$\frac{d_2 - d_1}{\sqrt{K}} = \frac{1}{\sqrt{P_2}} - \frac{1}{\sqrt{P_1}} \qquad \textbf{(4-2)}$$

$$\frac{v}{\sqrt{K}} = \frac{1}{(t_2 - t_1)} \left(\frac{1}{\sqrt{P_2}} - \frac{1}{\sqrt{P_1}} \right) \qquad \textbf{(4-3)}$$

Equation 4-1 thus allows us to compute the relative speed v, normalized by the constant K. For the case where P2 > P1, i.e., n2 is moving closer to n1, a similar analysis holds. In Figure 4-1 the circle of radius d3 represents the new position of n2 closer to n1. Hence in the following paragraph, the power measurement P2

corresponds to a distance of d3. Again we assume that the node moves in a straight line.

Note that the node n2 will stay in the range of n1 for a longer time if it moves along a radial direction. The worst-case scenario is when n2 starts moving away from n1 just after time t2. We then obtain the relative speed, v as

$$\frac{v}{\sqrt{K}} = \frac{\sqrt{d_1^2 - d_3^2}}{(t_2 - t_1)} = \frac{1}{(t_2 - t_1)}\sqrt{\frac{1}{P_1} - \frac{1}{P_2}} \qquad \textbf{(4-4)}$$

We thus have the means to compute an estimate of the relative speed (normalized by a constant) with just the received power measurements.

In order to obtain this combined metric, the following intuition is considered. Consider a pair of nodes n1 and n2 which are in each other's range at some point in time. Let d1 indicate the distance between the nodes when they are closest. We can divide the period in which they are within range, into two parts - one, comprising of the time when they drawing closer till d1; two, comprising of the time when they are moving apart. On the average we can consider these two distances to be equal. Thus, a contracting link eventually transforms into an expanding link, staying alive for approximately twice the time as compared to a link currently detected to be expanding. Hence we propose the following combined metric, which we call the "Route Fragility Coefficient" (RFC):

$$RFC = CCM + 2 * CEM \qquad \textbf{(4-5)}$$

4.4 Control Packets

The message types defined by the protocol are RREQ, RREP, and RERR. These message types are received via UDP, and normal IP header processing applies. So, for instance, the requesting node is expected to use its IP address as the Originator IP address for the messages. For broadcast messages, the IP limited broadcast address (255.255.255.255) is used. This means that such messages are not blindly forwarded.

4.5 Format of Control Packets

The format of the control packets i.e., Route Request, Route Reply and Route Error are shown below.

4.5.1 Route Request (RREQ) Packet

The format of Route Request is shown in Fig 4-2

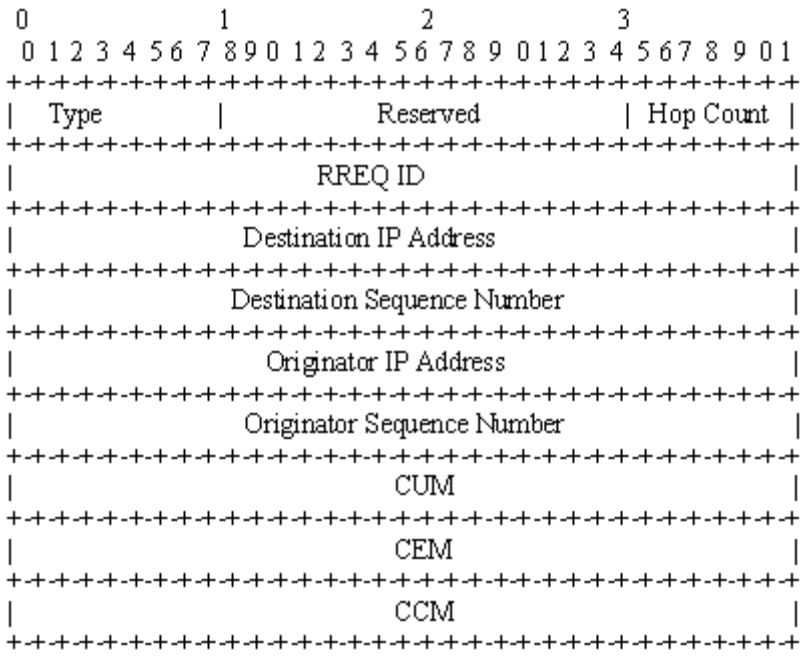

Figure 4-2: Format of RREQ Packet

The format of the Route Request message is illustrated above, and contains the following fields:

Type	Set to 1 for RREQ packet
Reserved	Set as 0; Ignored on reception
Hop Count	The number of hops from the Originator IP Address to the node handling the request.

RREQ ID	A sequence number uniquely identifying the particular RREQ when taken in conjunction with the originating node's IP address.
Destination IP Address	The IP address of the destination for which a route is desired.
Destination Sequence No	The latest sequence number received in the past by the originator for any route towards the destination.
Originator IP Address	The IP address of the node which originated the Route Request.
Originator Sequence No	The current sequence number to be used in the route entry pointing towards the originator of the route request.
CUM	Value of Cumulative Uncertainty Metric
CEM	Value of Cumulative Expansion Metric
CCM	Value of Cumulative Contraction Metric

Table 4-1: Fields in RREQ Message

4.5.2 Route Reply (RREP) Packet

The format of Route Reply Packet is shown in Fig 4-3.

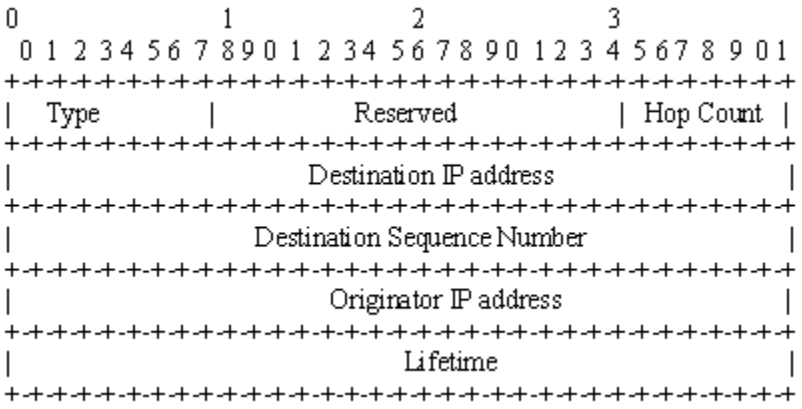

Figure 4-3: Format of RREP Packet

The format of the Route Reply message is illustrated above, and contains the following fields:

Type	Set to 2 for RREP packet
Reserved	Set as 0; Ignored on reception
Hop Count	The number of hops from the Originator IP Address to the Destination IP Address.
Destination IP Address	The IP address of the destination for which a route is supplied.
Destination Sequence Number	The destination sequence number associated to the route.
Originator IP Address	The IP address of the node which originated the RREQ for which the route is supplied.
Lifetime	The time in milliseconds for which nodes receiving the RREP consider the route to be

valid.

Table 4-2: Fields in RREP Message

4.5.3 Route Error (REER) Packet

The format of Route Error Packet is shown in Fig 4-4

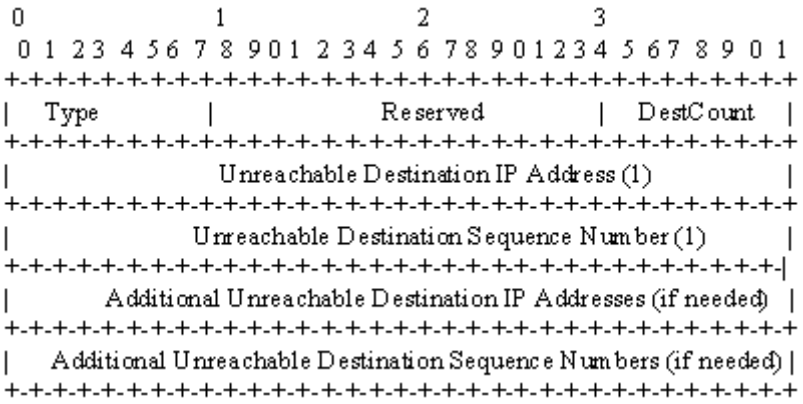

Figure 4-4: Format of RERR Packet

The format of the Route Error message is illustrated above, and contains the following fields:

Type	Set to 3 for RERR packet
Reserved	Set as 0; Ignored on reception
DestCount	The number of unreachable destinations included in the message; MUST be at least 1.
Unreachable Destination IP Address	The IP address of the destination that has become unreachable due to a link break.
Unreachable	The sequence number in the route table entry

Destination Sequence Number	for the destination listed in the previous Unreachable Destination IP Address field.

7Table 4-3: Fields in RERR Message

4.6 Route Discovery

4.6.1 Route Requests

When the source has data to send to some node in the network (called the destination node for that source) but no route information of the destination node is present in the routing table of the source, the node initiates a route discovery procedure. In this route discovery procedure the source broadcasts route request packets (RREQ) to the downstream nodes in the network. The RREQ packet initially contains the IP address of the source, the IP address of the destination of that source. Each intermediate node of the source forwards the packet to its downstream node until it reaches the destination.

4.6.1.1 Operation at Intermediate Nodes

When some downstream node receives the RREQ it considers whether it has heard this request before. If the node has heard the request before it discards the packet. But if the node has not heard the request it has to calculate the dynamism of the link with its upstream neighbor, and updates the CCM, CUM and CEM fields. To update the fields routing layer requires two power samples for the previous hop. These are obtained from the data packets and the recently received RREQ or RREP packets.

When a data packet is received at a node, the MAC layer records the received power for the source originating the packet. When a RREQ is received from a source, the

MAC layer passes the previous received power information for this source and the received power for the RREQ packet. Thus the routing layer obtains two power samples for the previous hop and the algorithm in Fig 4-5 in executed at the node.

```
/* Algorithm to Update RREQ packets with
expansion or contraction information */

Input: A RREQ packet from node s
Input: Last two received power measurements P1,
P2, for node s

if No Power Samples then
   CUM ← CUM + 1 ;
   Return
end if

if P2 < P1 then
     Compute relative speed estimate v
     CEM ← CEM + v
end if

if P2 > P1 then
     Compute relative speed estimate v
     CCM ← CCM + v
End if
```

Figure 4-5: Algorithm to Update RREQ packet

4.6.1.2 Operation at Destination Node

When the RREQ packet reaches the destination, it processes the packet and sends a route reply packet in the reverse path. Thus the destination chooses a route for the source. In order to obtain the route with the best properties, the destination should not just reply to the first route request it receives. Instead, if it waits for a set amount of time and compares the RREQs it receives; it can do a much better job of choosing a good route. Thus a delay called the "Route Reply Latency" (RRL) is introduced.

Higher the value of RRL, higher the number of RREQs at the disposal of the destination and higher the end-to-end latency of obtaining a route at the source.

```
/* Procedure executed at destination on
receiving a RREQ packet */

Input: m*, N* - RFC for best route till now and
its hop-length
Input: CUM* - Cumulative Uncertainty Metric for
best route till now
Input: RREQ packet

Extract CCM, CEM, CUM and N (hop-length) from
the RREQ

if CUM > CUM* then
   /*Greater uncertainty; ignore this RREQ*/
   return;
end if

m ← CCM + 2*CEM
if m/N < m*/N* then
     /*Replace m as the best route till now*/
     m* ← m
     Save the RREQ packet
end if
```

Figure 4-6: Algorithm executed at Destination node

In Equation 4-5 demonstrates the means to obtain a single metric representative of the route and specified a strategy to compare two routes. The destination waits for a duration specified by RRL after the first RREQ, Algorithm shown in Figure 4-3 specifies the operation performed when each RREQ is received.

The route which does not have information about many of its constituent links is worse than a route about which there is information. The CUM value in the RREQ packet indicates the number of links about which there is no expansion or contraction

information. If the best route received till now has a CUM value that is less than that of the RREQ received, the RREQ is ignored. Otherwise, the RFC for this route is evaluated using the CCM and CEM values and compared with that of the best route seen till that time. At the end of the duration specified by RRL, the destination sends a reply to the RREQ packet representing the best route seen till then.

```
/* Handling of RREQ */
FOR each RREQ received {
IF RREQ has not been seen before {
          Obtain power of received packet and
          previously stored power for node s;

Update RREQ packet using Algorithm

          IF receiving node is Destination Node
          {
               Execute Algorithm 2;
               Send a unicast Reply to Source;
}
     Obtain power of this packet and update the
     power measurement for node s;
}
```

Figure 4-7: Pseudo Code for Handling Route Request

4.6.2 Route Replies

A node generates a RREP if either (a) it is itself the destination, or (b) it has an active route to the destination, the destination sequence number in the node's existing route table entry for the destination is valid and greater than or equal to the Destination Sequence Number of the RREQ (comparison using signed 32-bit arithmetic), and the "destination only" ('D') flag is NOT set.

When generating a RREP message, a node copies the Destination IP Address and the Originator Sequence Number from the RREQ message into the corresponding fields in the RREP message. Processing is slightly different, depending on whether the node is itself the requested destination, or instead if it is an intermediate node with an fresh enough route to the destination.

Once created, the RREP is unicast to the next hop toward the originator of the RREQ, as indicated by the route table entry for that originator. As the RREP is forwarded back towards the node which originated the RREQ message, the Hop Count field is incremented by one at each hop. Thus, when the RREP reaches the originator, the Hop Count represents the distance, in hops, of the destination from the originator.

4.7 Route Maintenance

Each forwarding node should keep track of its continued connectivity to its active next hops. A node can maintain accurate information about its continued connectivity to these active next hops, using link layer detection. The suitable link layer notification, provided by IEEE 802.11, is used to determine connectivity, each time a packet is transmitted to an active next hop. For example, absence of a link layer ACK or failure to get a CTS after sending RTS, even after the maximum number of retransmission attempts, indicates loss of the link to this active next hop.

Generally, route error and link breakage processing requires, invalidating existing routes, listing affected destinations, determining which, if any, neighbors may be affected, delivering an appropriate RERR to such neighbors. A Route Error (RERR) message may be broadcast, unicast, or iteratively unicast to all precursors. Even when the RERR message is iteratively unicast to several precursors, it is considered to be a

single control message for the purposes of the description in the text that follows. With that understanding, a node should not generate more than RERR_RATELIMIT RERR messages per second. A node initiates processing for a RERR message in three situations:

(a) if it detects a link break for the next hop of an active route in its routing table while transmitting data (and route repair, if attempted, was unsuccessful), or

(b) if it gets a data packet destined to a node for which it does not have an active route and is not repairing (if using local repair), or

(c) if it receives a RERR from a neighbor for one or more active routes.

5 Results and Simulation

5.1 Introduction

This section describes the network simulator 2 (NS-2), its tracing mechanism and especially the wireless model in NS-2.In order to test the protocol, an implementation in a network simulator is chosen. The alternative of an implementation in a real system (e.g., Linux) and testing it as experimentation would use too many resources and finally be too expensive. Furthermore, the implementation in a simulator offers more flexibility and variations, i.e., scenarios with much more nodes can be tested and adapted for the initial parameter tuning.

5.2 Implementation of Simulation Models

An implementation in real systems can be considered, if the verification with the help of the simulation is successful. A network simulator for the verification of the cooperation schemes should fulfill the requirements: (a) Simulation scenarios with 50 and more nodes, (b) Physical Layer model with Radio Propagation, (c) MAC Layer and Link Layer models, (d) Mobility of the nodes and (e) Enhanced tracing functionality.

There exist quite a number of network simulators today. Not all of them have a good reputation within the research community, and of those which have, most are expensive. Therefore, NS-2 is chosen, because it is open source software, freely

available and it is widely used in the research community. Besides, NS-2 meets perfectly the above mentioned requirements.

5.2.1 Implementation with Network Simulator II

NS-2 is a discrete event driven simulator. The source code and the documentation [15] are currently maintained by the Virtual Internet Test bed (VINT) at the Information Sciences Institute (ISI) of the University of Southern California (USC). The goal of NS-2 is to support networking research and education. It provides an environment for protocol design, traffic studies and protocol comparison. Its license model enables the sharing of code, protocols, models, and ensures that the work is given back to the community. It allows easy comparison of similar protocols. This collaborative environment and the big number of users should also increase the confidence in the results because more people look at the models in more situations than by using a closed source simulator.

5.2.2 Structure of NS-2

In NS-2 real world objects are modeled by objects in the simulation and programmed to react as much as possible as their correspondents in the real world would react. In the concept of event driven simulation, physical activities are translated to events. The events are stored in a queue. They are processed in the order of their scheduled occurrences. The time in the simulation progresses as the events are processed. Each event happens in an instant of simulated time, but takes an arbitrary amount of real time. NS-2 is built using object oriented methods in C++ and Otcl. The developers of NS-2 tried to combine fast iteration time with good run-time performance. This results in a mixed coding framework in C++ and Otcl, C++ serves as system

programming language in which all time consuming components, e.g., packet processing and routing algorithms, are implemented. OTcl is used as the configuration language for the simulation scenarios. It allows the quick setup of different simulation scenarios and an interactive simulation mode. OTcl and C++ share linked class hierarchies and the additional library Tclcl offers sharing of functions and variables. Objects in C++ are compiled and then made available to the OTcl interpreter through an OTcl linkage (Tclcl) which maps methods and member variables of the C++ object to methods and variables of the linked OTcl object. This system architecture facilitates the usage of NS-2 and its existing components, but it makes the development of new components complicated and time-consuming.

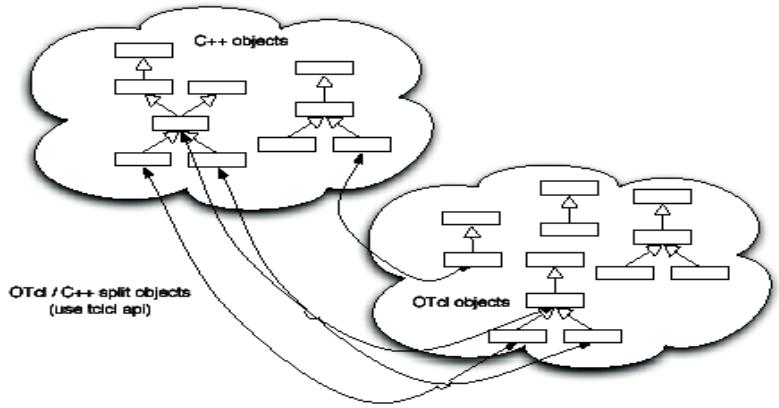

Figure 5-1: Duality of C++ and Otcl in NS-2

5.2.3 Internal Packet Representation

The internal packet representation of NS-2 is quite different from a packet in the real world. The packet in the simulator contains all headers that the simulator supports, e.g., UDP, TCP, MAC, IP etc., and not only the headers of the real world packet. Furthermore, a packet in the simulator has a common header which contains

important simulation information, e.g., the simulated packet size (size of the real world packet), the packet type, the flow direction, a unique packet ID and a time-stamp. Besides, the packet headers of NS-2 do not necessary correspond to the protocol headers defined in RFCs, e.g., header checksums are normally left out.

5.2.4 Simulation Process

The figure shows the simplified process for a simulation. The user has to set the different components, e.g. event scheduler objects, network components and setup module libraries, up in the simulation environment. This is done by a simulation script in OTcl. The script is processed by ns2 and delivers trace files that the user analyzes with the Network Animator (NAM) or custom scripts.

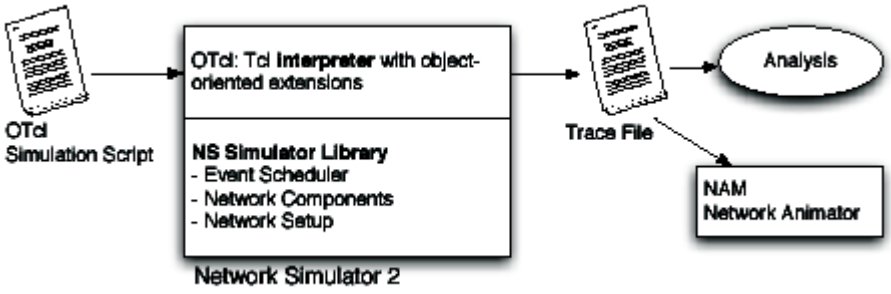

Figure 5-2: User View of NS-2

5.2.5 Wireless Model in NS-2

The wireless model in NS-2 is contributed from CMU's Monarch project (Wireless extension to NS-2). Various modules were added to ns2 to simulate node mobility and wireless networking, including (a) Mobile Node, (b) Base station Node, (c) Ad-hoc Routing Agents (DSR, DSDV, TORA, AODV, AODV+), (d) MAC 802.11, (e) Radio Propagation Model and (f) Channel.

5.2.6 Tracing

NS-2 offers tracing of all packets in the simulation. Furthermore, NS-2 enables the tracing of variables in C++ or OTcl and supports the monitoring of queues and flows (see [15] for detailed information). In this thesis only the packet tracing ability is used. There exist three different trace file formats (old, new wireless and NAM) for packet tracing. [16] gives a good overview of them.

5.3 Random Waypoint Mobility (RW) Model

The Random Waypoint model, as depicted by Figure 5-3, is most commonly used mobility model in research community. In the current network simulator (NS-2) distribution, the implementation of this mobility model is like this: at every instant, a node randomly chooses a destination and moves towards it with a velocity chosen uniformly randomly from $[0,V_{max}]$, where V_{max} is the maximum allowable velocity for every mobile node. After reaching the destination, the node stops for a duration defined by the 'pause time' parameter. After this duration, it again chooses a random destination and repeats the whole process again until the simulation ends. In this framework, the RW model acts as the 'baseline' mobility model to evaluate the protocols in Ad Hoc Network.

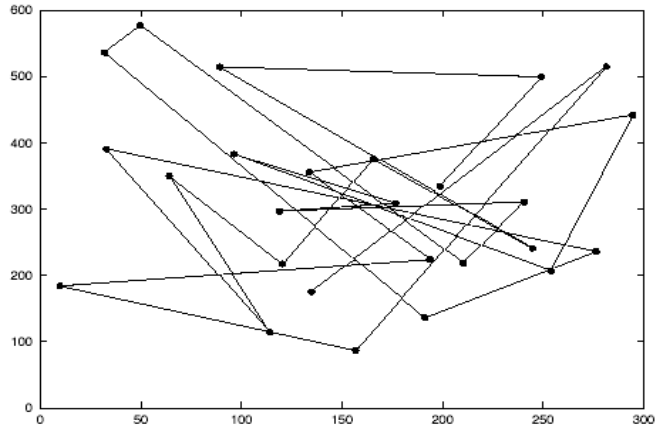

Figure 5-3: Traveling Pattern of the Node in Random Way Point Mobility Model

5.4 Free Space Path Loss Model

Free Space Model is a Radio propagation model. These models are used to predict the received signal power of each packet. At the physical layer of each wireless node, there is a receiving threshold. When a packet is received, if its signal power is below the receiving threshold, it is marked as error and dropped by the MAC layer.

The free space propagation model assumes the ideal propagation condition that there is only one clear line-of-sight path between the transmitter and receiver. H. T. Friis presented the following equation to calculate the received signal power in free space at distance d from the transmitter [17].

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \qquad \textbf{(5-1)}$$

where Pt is the transmitted signal power. Gt and Gr are the antenna gains of the transmitter and the receiver respectively. L($L \geq 1$) is the system loss, and λ is the wavelength. It is common to select Gt = Gr = 1 and L = 1 in *ns* simulations.

The free space model basically represents the communication range as a circle around the transmitter. If a receiver is within the circle, it receives all packets. Otherwise, it loses all packets.

5.5 Simulation Scenario

Used in the thesis is a detailed simulation model based on NS-2. The Monarch research group in CMU developed support for simulating multi-hop wireless networks complete with physical, data link and MAC layer models on NS-2. IEEE 802.11 [18] is used as the MAC layer. The radio model uses characteristics similar to a commercial radio interface, Lucent's WaveLAN [V]. WaveLAN is a shared-media radio with a nominal bit-rate of 2 Mb/sec and a nominal radio range of 250 meters. The random waypoint model is used to model mobility. The speed of nodes is varied between 20m/s to 50m/s. The mobile hosts are placed randomly within a 1000m x 500m area. Traffic is generated by CBR(constant bit rate)sources and User Datagram Protocol (UDP) is used on the transport layer. The source-destination pairs (sessions) are spread randomly over the network. The size of data packets is 512 bytes. Different mobility scenarios and traffic patterns are used for the various simulations done and each simulation scenario is run for 400 seconds.

5.5.1 Performance Metrics

The following metrics are used to assess the performance:

- *Packet Delivery Ratio*: The ratio of the data delivered to the destinations (i.e., throughput) to the data sent out by the sources.
- *Control overhead*: Total number of RREQ, RREP and RERR packets that are being propagated into the network.

- *Average End-to-End Delay:* Average time taken to transmit a packet from source to destination.

The performance of the protocols i.e., AODV, DSDV and AODV_RFC is compared by keeping in view the effects of mobility and scalability.

5.6 Effect of Mobility

The effect of mobility on the protocol has been studied by varying the pause time of the nodes from 1s to 100s.

5.6.1 Simulation Environment

For generating the results to measure the performance of the three protocols with changing mobility conditions, environment in NS-2 was set up as given in Table 5-2: Simulation Environment B

.

Simulation Parameters	**Values**
Num of nodes	75
Num of connections	10
Max speed	20m/s
Propagation	Free Space
Pause time (s)	1,25,50,75,100
Packet size	512 bytes
Sending rate :	10 packet/sec (CBR)
Transport layer	UDP

Mac layer	IEEE802.11
Antenna type	Omni atenna
Communication range	250 m
Bandwidth	2 Mbps

Table 5-1: Simulation Environment A

5.6.2 Effect on Packet Delivery Ratio

Figure 5-4 shows the performance of the three protocols with varying mobility conditions. A lesser pause time means greater mobility. AODV_RFC perform extremely well, and give a packet delivery ratio of more than 95% for different mobility conditions. DSDV, being a reactive protocol, gives a much lower packet delivery ratio, which deteriorates even further when mobility increases.

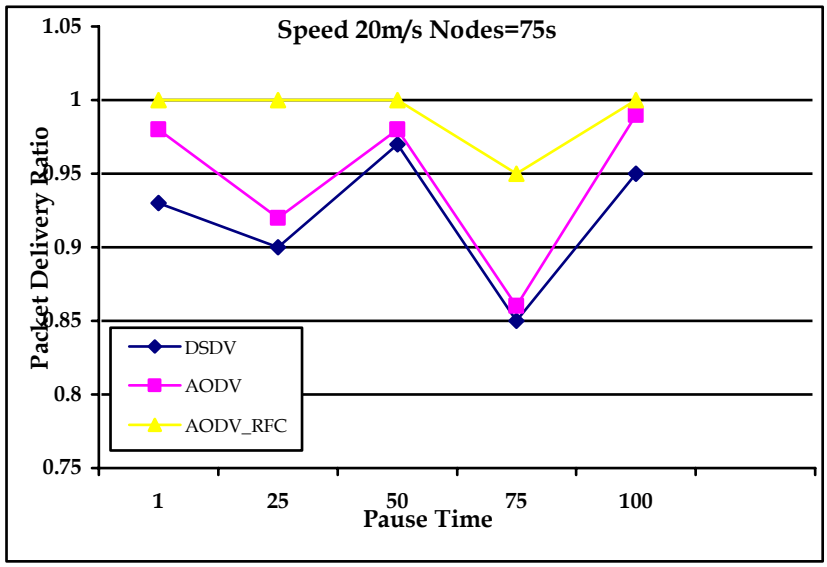

Figure 5-4: PDR VS Pause Time

The above graph shows that the Packet Delivery ratio of AODV_RFC is almost constant irrespective of the mobility. At high mobility (pause time 1s) the PDR is 1

and at low mobility (pause time 100s) the PDR is 1. This is because of the fact that irrespective of mobility the protocol always chooses a stable route which results in higher PDR. However the PDR of AODV and DSDV follow a zig-zag path which means that with mobility the PDR of both the protocols does not remain constant.

5.6.3 Effect on Control Overhead

Fig 5.5 shows the effect of mobility on the control overhead of the three protocols. The graph shows that with highest mobility (pause time=1s) the control overhead of DSDV is highest as the mobility decreases the control overhead of the protocol decreases. On the other hand the control overhead of AODV is lowest at high mobility but as the mobility increases the control overhead also increases. The control overhead of AODV_RFC is lower than that of AODV and DSDV.

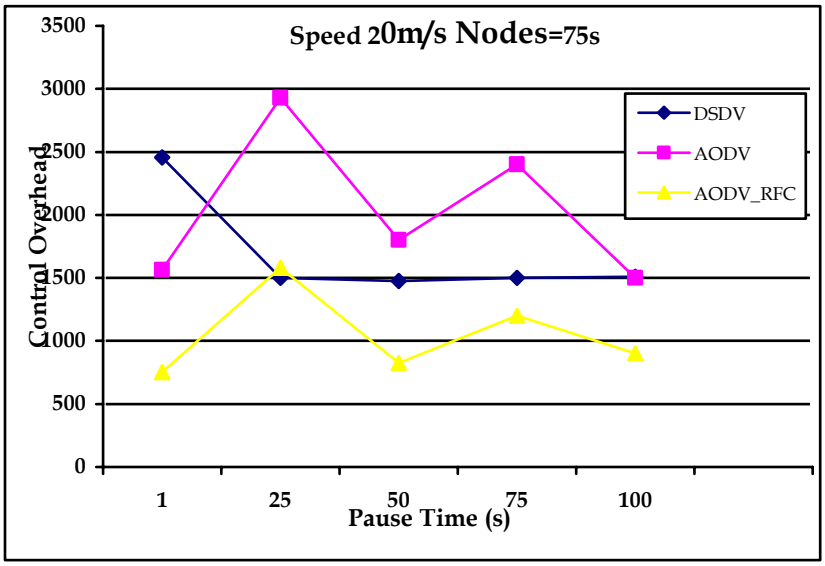

Figure 5-5: Control Overhead VS Pause Time

The overhead of AODV_RFC is less than that of the other two protocols because the protocol tends to find a stable route and so there are less link breakage in the route thus resulting in less route repair and discovery process which results in less overhead. So the control overhead of AODV_RFC is lesser than the DSDV and AODV.

5.6.4 Effect on Average End-to-End Delay

Fig 5.6 shows the effect of mobility on Average End-to-End delay of the data packets. The delay of all the three protocols is lowest at highest mobility (pause time 1s) and it increases after that.

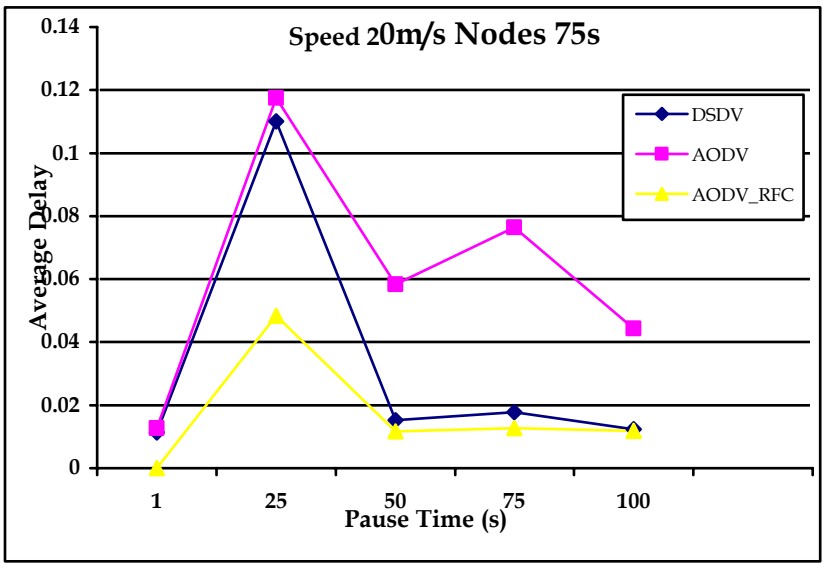

Figure 5-6: Average Delay VS Pause Time

5.7 Effect of Scalability

Scalability refers to how well a solution works to a given issue when the size of the issue increases. In a broader sense it is the ability to use a software environment on a whole series of different computers without changes i.e., to expand the software's area of application. In the present context the term refers to the possibility of increasing the size of the network by increasing the number of nodes and to analyze the effect of scalability on the throuput of the network.

5.7.1 Simulation Environment

For generating the results to measure the performance of the three protocols with changing mobility conditions, environment in NS-2 was set up as given in Table 5-2: Simulation Environment B

.

Simulation Parameters	**Values**
Num of nodes	50,75,100,125,150
Num of connections	10
Max speed	20 m/s
Propagation	Free Space
Pause time	1 sec
Packet size	512 bytes
Sending rate :	10 packet/sec (CBR)
Transport layer	UDP

Mac layer	IEEE802.11
Antenna type	Omni antenna
Communication range	250 m
Bandwidth	2 Mbps

Table 5-2: Simulation Environment B

5.7.2 Effect on Packet Delivery Ratio

First we check the scalability of the three protocols under high mobility. Figure 5.7 shows that when mobility is extremely high (pause time is 1s) and the number of nodes in the network is kept below 150, AODV-RFC has a very consistent PDR, which is also greater than DSDV and AODV. Although when the size of the network is 75 nodes the packet delivery ratio of AODV-RFC drops but it remains consistent otherwise. The performance of AODV is good when the number of nodes in the network is low but as the nodes increase the performance of AODV deteriorates. AODV-RFC performs better than AODV as the number of nodes increases beyond 75. This shows that AODV-RFC is more scalable to larger networks as compared to AODV. Whereas the performance of DSDV is initially not very good but as the network size increases the performance of the DSDV improves.

With DSDV there is a good PDR with increasing number of nodes because more nodes mean more routes to other nodes in the network and thus a route is available every time for the source to send data to the destination. With AODV the PDR decreases with an increase in the number of nodes because this places a lot of load on the intermediate nodes. So many nodes mean that the intermediate nodes must at all times be holding the routing information for these many nodes as well. With such

huge routing tables, intermediate nodes are over burdened and thus processing so many packets for so many sources whose data is queued in the buffers takes time, reducing PDR considerably.

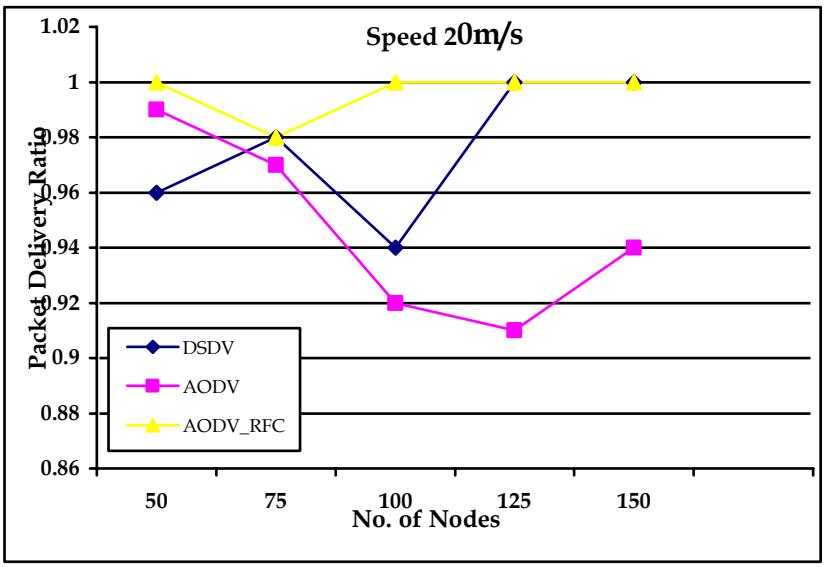

Figure 5-7: PDR VS No of Nodes

5.7.3 Effect on Control Overhead

Figure 5.8 shows the control overhead of the three protocols versus the varying network size. The pause time is 1s, which means that the nodes in the network are very mobile. The control overhead of AODV is greater than of DSDV and AODV-RFC when the network size is less than 125 nodes. As the nodes in the network are 125 or more the control overhead of AODV is lesser than that of DSDV but greater than AODV-RFC. The control overhead of AODV-RFC increases as the size of the network increases but it is always less than that of DSDV and AODV.

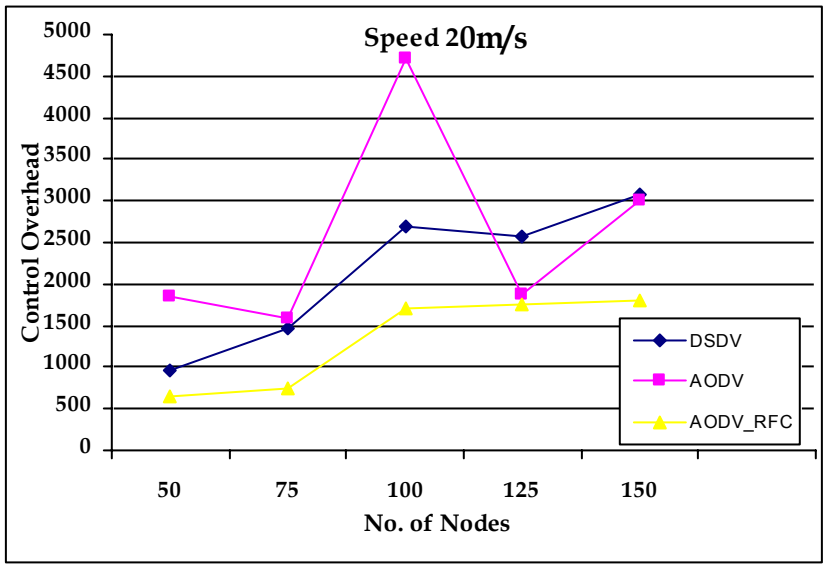

Figure 5-8: Control Overhead VS No of Nodes

The control overhead of DSDV increases as the network size increases because there are more nodes in the network and more control packets are transmitted in the network. Moreover there are more link breakages due to which more control packets are to be transmitted in the network. The performance of AODV_RFC is better than the other two protocols because the protocol always choose the route which is less

dynamic and hence it is more stable. By choosing the stable route the chances of route breakages are minimized and hence the control overhead also reduces.

5.7.4 Average End-to-End Delay vs. Scalability

Fig 5.9 shows the Average End-to-End delay of the three protocols with the increasing network size. The average delay of AODV is highest when the nodes in the network are 50. With the increasing nodes the delay decreases. The delay of AODV_RFC is least followed by DSDV and then AODV.

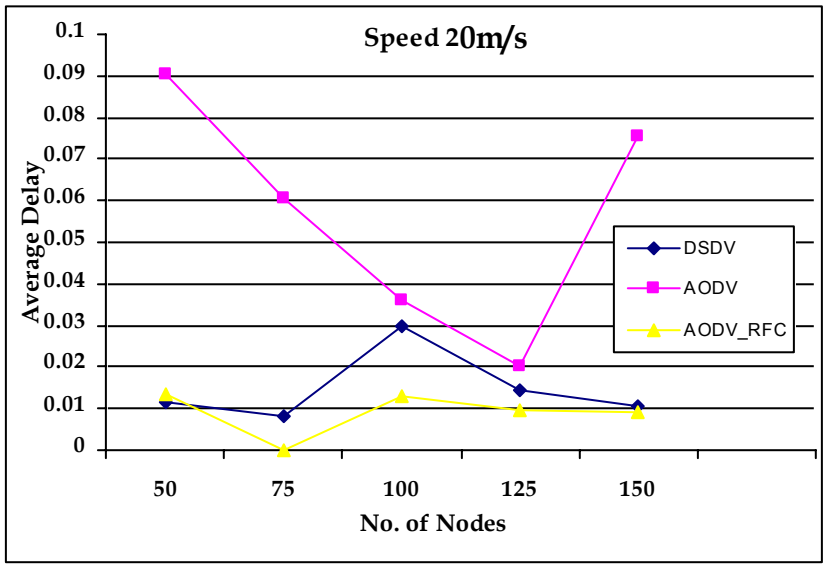

Figure 5-9: Average Delay VS No of Nodes

The delay of AODV_RFC is lesser than the other two protocols because with the formation of more stable links within routes, the probability of link breakages decreases. This reduces the frequency of route repairs and route re-quests and hence reduces the end to end delay during the transfer of data packets.

6 Conclusion and Future Work

6.1 Introduction

Ad hoc On-demand Distance Vector Routing protocol (AODV) was enhanced with the Route Fragility Coefficient as a metric. Simulation was performed with varying network characteristics, the results depicted gains in throughput in terms of packet delivery ratio and reduction in routing overhead. The protocol also reduced the end-to-end delay in the delivery of the data packets. This yields that the protocol adapts to the changing network parameters and performs well with varying speed of nodes and with increased size of the network.

6.2 Future Work

Presently the protocol has been studied with only Random Waypoint mobility model. In future the evaluation of the protocol based on different mobility models can be studied. Similarly the effect of using other radio propagation models can also be studied. The power values which are used in the design of the protocol are instantaneous power values. They values are taken as they are and inserted in the RREQ packet. But we can also use weighted values instead of instantaneous power values. The weights can be based on the contraction and expansion properties of the route, or other properties can also be incorporated into it.

The analysis done in this thesis is for CBR/UDP traffic only. The analysis should be done for TCP only and mixed traffic scenarios to get a better idea of how the protocol performs under varying traffic conditions.

The protocol can be extended to include battery power (BP) as an additional metric for the selection of the paths. In addition to appending the condition of link in the RREQ packets, the nodes would also append their respective battery power. The RREQ packet would have an additional field for storing the battery power. Three kinds of nodes would be identified, the sending nodes, the receiving nodes and the forwarding (intermediate) nodes.

6.3 Conclusion

The results were studied by changing the characteristics i.e., scalability and mobility of the network. The performance of the protocol was compared with a reactive and proactive protocol namely AODV and DSDV respectively. The comparison of results showed that the performance of AODV_RFC is better than the other two protocols when considered under varying mobility and network size. The protocol shows almost constant Packet Delivery Ratio under different mobility scenarios and with varying network size. The control overhead generated due to the protocol is also lesser than the other two protocols. With a significant decrease in network overhead caused by control packets, there is less congestion in the network. This leads to a higher packet delivery ratio since there is lesser contention for bandwidth between data and control packets.

APPENDIX A

FLOWCHARTS

This section explains the flowchart that explains the flow of events in AODV-RFC, its describes how various events arrive and how they are processed.

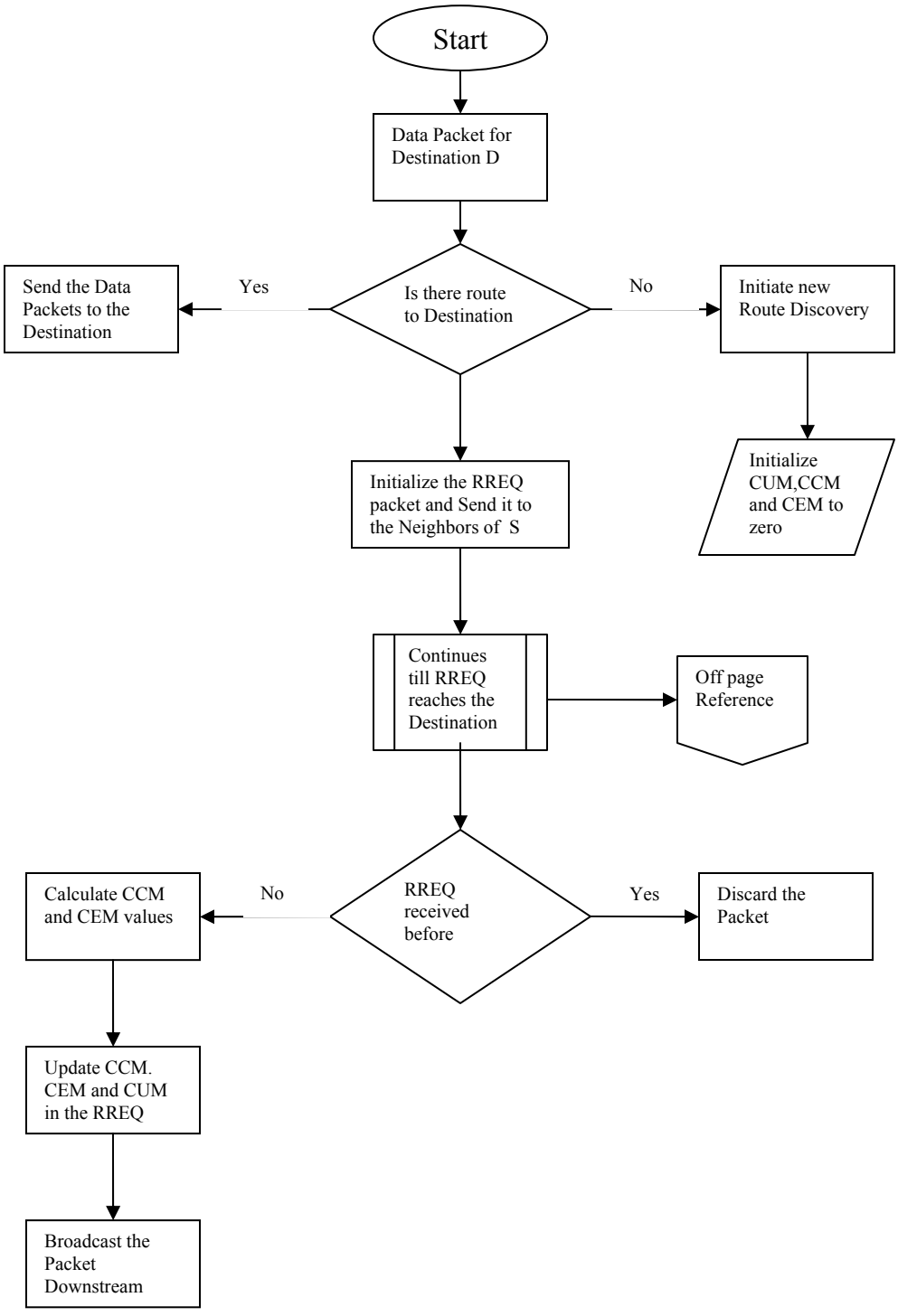

Figure A-1 Flow Chart (1/3)

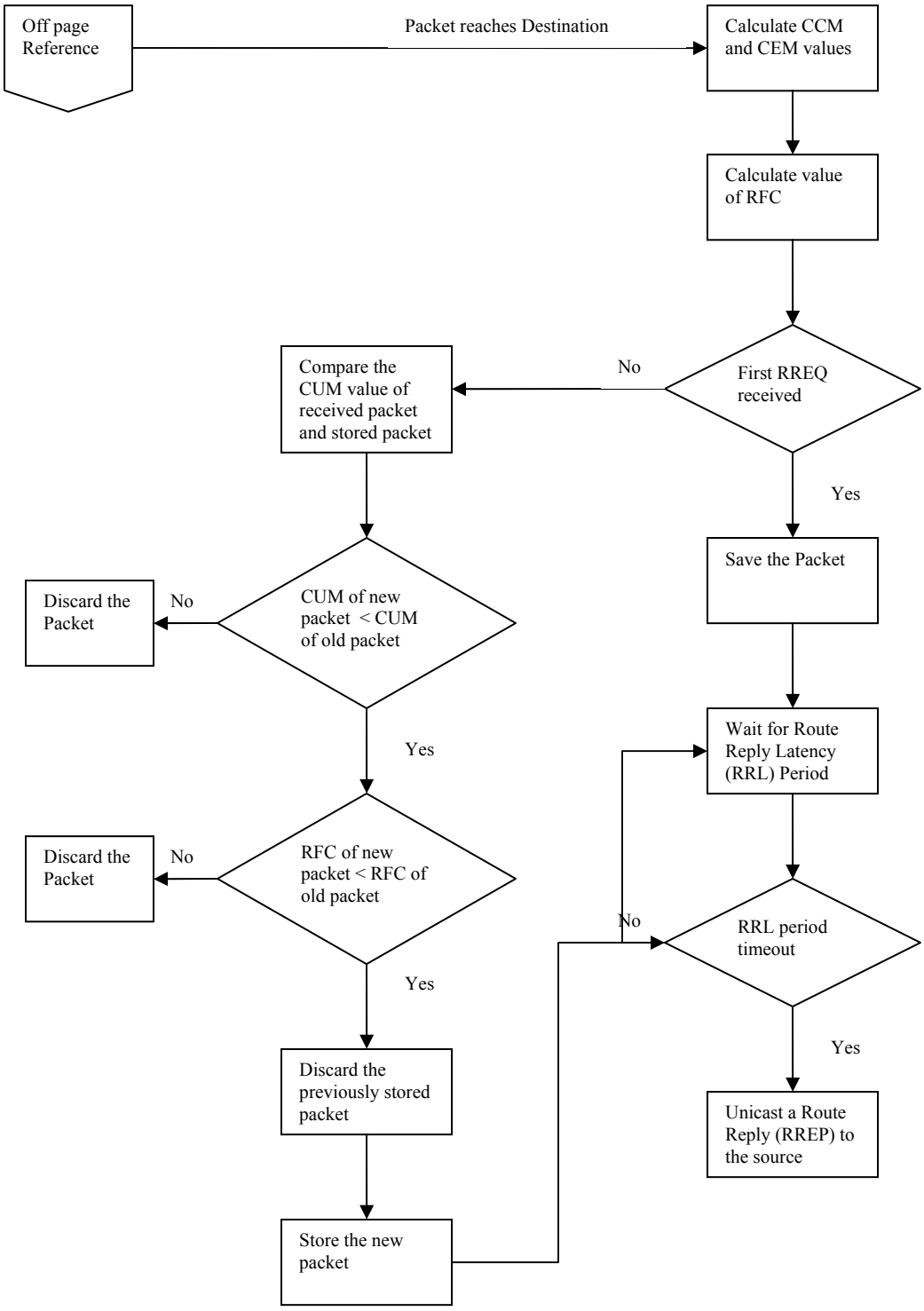

Figure A-1 Flow Chart (2/3)

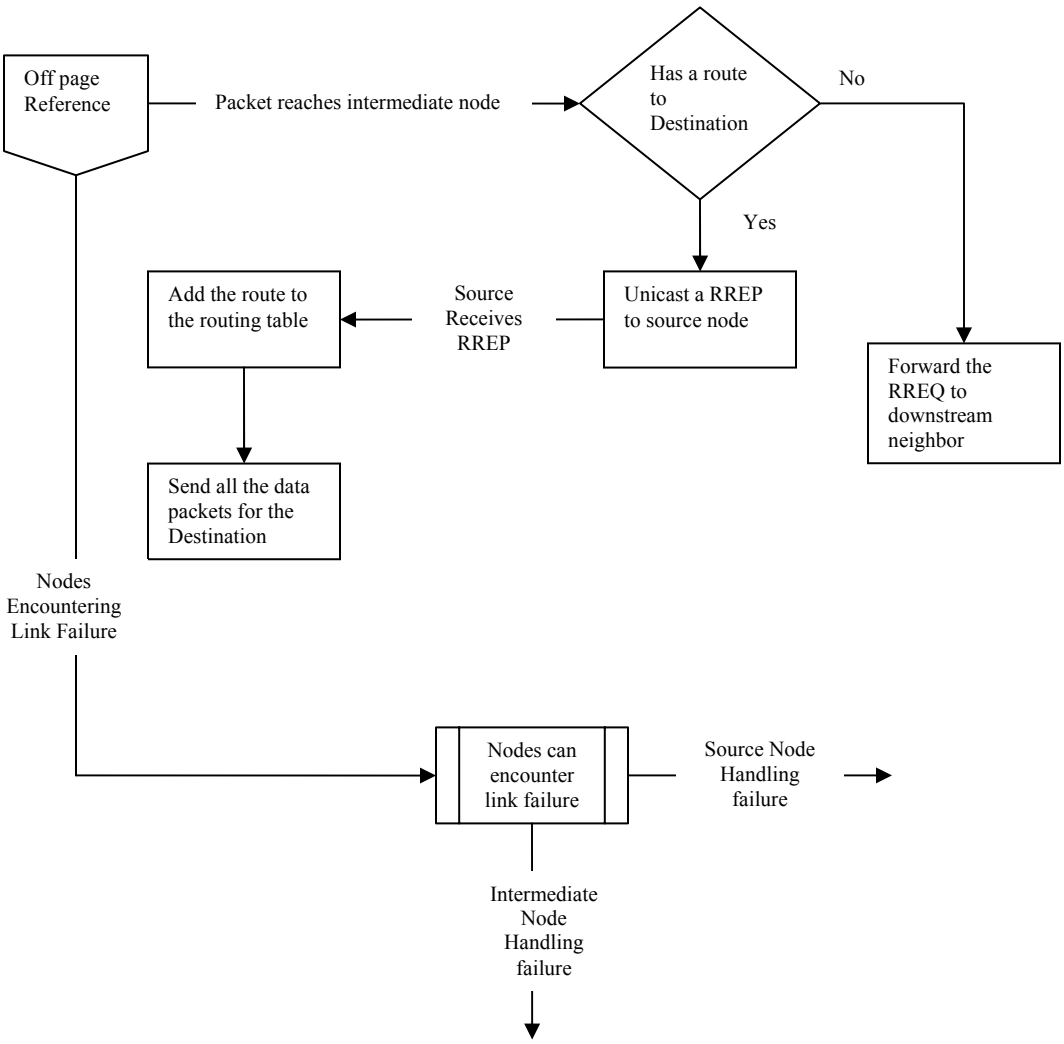

Figure A-1 Flow Chart (3/3)

APPENDIX B

DATA DICTIONARY

AODV	Ad Hoc On Demand Distance Vector Routing Protocol
DSDV	Destination-Sequenced Distance Vector Protocol
ABR	Ant Based Routing Protocol
SSA	Signal Stability-Based Adaptive Routing Protocol
DSR	Dynamic Source Routing Protocol
RREQ ID	Route Request ID
CUM	Cumulative Uncertainty Metric
CEM	Cumulative Expansion Metric
CCM	Cumulative Contraction Metric
P2	Power of the sample at time t2
P1	Power of the sample at time t1
v	Relative speed estimate
m	Route Fragility Coefficient

REFERENCES:

[1] Fan Bai, Narayanan Sadagopan, Ahmed Helmy, Univ. of Southern California, "A framework to systematically analyze the Impact of Mobility on Performance of RouTing protocols for Adhoc NeTworks", 2002, pp. 234–244.

[2] D. B. Johnson, D. A. Maltz, and J. Broch, ""DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks"," in Ad Hoc Networking, C. Perkins, Ed. Addison-Wesley, 2001, pp. 139–172.

[3] C. E. Perkins and P. Bhagwat, "Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers," in ACM SIGCOMM, 1994, pp. 234–244.

[4] C. Perkins, "Ad hoc on demand distance vector (AODV) routing, internet draft, draft-ietf-manet-aodv-00.txt."

[6] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking, ACM, October 1998.

[5] V. D. Park and M. S. Corson, "Temporally-ordered routing algorithm (TORA) version 1: Functional specification, internet-draft, draft-ietfmanet- tora-spec-01.txt," August 1998.

[6] Jan Schaumann, Analysis of the Zone Routing Protocol, December 8, 2002, pp. 4–5

[7] J. Moy, " Routing in Communications Networks" ed. M.E. Steenstrup (Prentice Hall, 1995) chapter 5, pp. 135–157.

[8] Mahesh K. Marina and Samir R. Das "On-demand multi-path distance vector routing in ad hoc networks (2001)". pp 210-233.

[9] S. Murthy and J.J. Garcia-Luna-Aceves," An efficient routing protocol for wireless networks, Mobile Networks and Applications" (1996), pp. 183–197.

[10] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol," RFC 3626, October 2003, pp. 245-266.

[11] Charles E. Perkins, Elizabeth M. Belding-Royer, Samir R. Das "Ad hoc On-Demand Distance Vector Routing", IEFT MANET Draft, February 2003 Charles E. Perkins, Ad Hoc Networking, ISBN 0-201-30976-9, pp.310-326.

[12] Jan Schaumann," Analysis of the Zone Routing Protocol", December 8, 2002, pp 189-227.

[13] S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A. Woodward. A distance routing e_ect algorithm for mobility (DREAM). In ACM/IEEE MOBICOM, 1998.

[14] J. Li, J. Jannotti, D. De Couto, D. Karger, and R. Morris. A scalable location service for geographic ad-hoc routing. In Proceedings of the 6th ACM International Conference on Mobile Computing and Networking (MOBICOM '00), pages 120–130, August 2000.

[15]"NS-2 notes and documentation" **http://www.isi.edu/nsnam/ns/ns-documentation.html**

[16] "NS-2 trace formats" **http://www.k-lug.org/~griswold/NS2/ns2-trace-formats.html**

[17]H. T. Friis. A note on a simple transmission formula. Proc. IRE, 34, 1946. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, ISO/IEC 8802-11; ANSI/IEEE Std 802.11, Aug.1999.

[18] Development of WaveLAN, an ISM Band Wireless LAN, AT&T Technical Journal, pp. 27-37, July/Aug. 1993