3-2001

Routing of Time-Sensitive Data in Mobile Ad Hoc Networks

Necdet Kilic

Recommended Citation

Kilic, Necdet, "Routing of Time-Sensitive Data in Mobile Ad Hoc Networks" (2001). *Theses and Dissertations*. 4644.
https://scholar.afit.edu/etd/4644

ROUTING OF TIME-SENSITIVE DATA IN MOBILE AD HOC NETWORKS

THESIS

Necdet KILIC, 1st Lt., TuAF

AFIT/GCE/ENG/01M-02

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

ROUTING OF TIME-SENSITIVE DATA IN MOBILE AD HOC NETWORKS

THESIS

Necdet KILIC, 1st Lt., TuAF

AFIT/GCE/ENG/01M-02

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
20 March 2001

2. REPORT TYPE
Master's Thesis

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
ROUTING OF TIME-SENSITIVE DATA IN MOBILE AD HOC NETWORKS

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Kilic, Necdet, 1st. Lt., TuAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 P Street, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT/GCE/ENG/01M-02

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Attn to: Mr. Ken Fore, Mr. Ron Price
DSN: 576-5472
Air Force Communication Agency
203 W. Losey, Scott AFB, IL

10. SPONSOR/MONITOR'S ACRONYM(S)
AFCA/ITAI

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
AFIT Technical POC: Major Rusty O. Baldwin, AFIT/ENG
rusty.baldwin@afit.edu

14. ABSTRACT

This research focuses on routing of time-sensitive data in mobile ad hoc networks. Routing protocols that were developed for ad hoc networks have been reviewed. Ad Hoc On-demand Distance Vectoring (AODV) routing protocol, which is a prominent routing protocol among these protocols have been implemented in OPNET, a discrete-event simulation tool. Taking AODV as a point of departure, a routing protocol named Real Time Routing Protocol (RTRP) has been developed and also implemented in simulation environment. The performance of these routing protocols have been observed by simulating them in various experiments where the workload has been chosen to be time-sensitive data. Results show that for lightly loaded networks, AODV and RTRP have similar performance. When the workload introduced to the network is increased, RTRP outperforms AODV significantly.

15. SUBJECT TERMS
RTRP, AODV, Mobile, Ad Hoc, Wireless, 802.11b, Routing Protocol, Time-Sensitive

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Major Rusty O. Baldwin, AFIT/ENG
U	U	U	UU	96	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636, ext 4582

AFIT/GCE/ENG/01M-02

ROUTING OF TIME-SENSITIVE DATA IN MOBILE AD HOC NETWORKS

THESIS

Presented to the Faculty
Department of Electrical and Computer Engineering
Graduate School of Engineering and Management
Air Force Institute of Technology
Air University
Air Education and Training Command
In Partial Fulfillment of the Requirements for the
Degree of Master of Science in Computer Engineering

Necdet KILIC, B.S.
1st. Lt., TuAF

March 2001

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AFIT/GCE/ENG/01M-02

ROUTING OF TIME-SENSITIVE DATA IN MOBILE AD HOC NETWORKS

Necdet KILIC, B.S.
1st Lt., TuAF

Approved:

Major Rusty O. Baldwin (Chairman)

6 Mar 01
Date

Major Richard A. Raines

6 Mar 01
Date

Dr. Michael A. Temple

6 Mar 01
Date

Acknowledgements

I would like to thank to those people whose support has helped me to complete this study here in AFIT. First of all, I want to thank my thesis advisor Maj. Rusty O. Baldwin, for his great support and encouragement he provided during the crises that took place on the way to the graduation. Without his guidance and encouragement, this thesis could not be completed. I also want to thank to my committee members, Maj. Richard A. Raines and Dr. Michael A. Temple for their precious guidance and opinions throughout this study. Last but definitely not least, I want to thank to my beloved wife Ebru, for the patience for sleepless nights that accompanied this research.

Table of Contents

1 INTRODUCTION 1

1.1 INTRODUCTION 1

1.2 RESEARCH OBJECTIVES 3

1.3 ORGANIZATION OF THE DOCUMENT 4

2 LITERATURE SURVEY 6

2.1 INTRODUCTION 6

2.2 AD HOC PROTOCOLS 8

2.2.1 Table Driven Routing Protocols 9

2.2.1.1 Destination-Sequenced Distance Vectoring Protocol 9

2.2.1.2 Wireless Routing Protocol 10

2.2.1.3 Cluster-head Gateway Switch Routing Protocol 11

2.2.2 Source-Initiated On-Demand Driven Routing Protocols 12

2.2.2.1 Dynamic Source Routing 13

2.2.2.2 Ad Hoc On Demand Distance Vectoring Routing Protocol 15

2.2.2.3 Temporally Ordered Routing Algorithm 17

2.2.2.4 Zone Routing Protocol 19

2.2.2.5 Associativity Based Routing 20

2.2.2.6 Signal Stability Routing 21

2.3 COMPARISON OF THE ROUTING PROTOCOLS 22

2.3.1 Table-driven Routing Protocols 22

2.3.2 Source-Initiated on Demand Routing Protocols *23*

2.4 SUMMARY 24

3 OBJECTIVES AND METHODOLOGY 26

3.1 OVERVIEW 26

3.2 OBJECTIVES AND SYSTEM BOUNDARIES 26

3.3 SYSTEM SERVICES 28

3.4 PERFORMANCE METRICS 28

3.4.1 Missed Deadline Fraction *28*

3.4.2 Mean End-to-End Delay *29*

3.4.3 Packet Delivery Fraction *29*

3.4.4 Routing Overhead *30*

3.5 SYSTEM AND WORKLOAD PARAMETERS 30

3.5.1 Data Rate *30*

3.5.2 Channel Bit Error Rate *30*

3.5.3 Workload *31*

3.5.4 Network Topology and Movement Models *31*

3.5.5 MAC Layer Parameters *31*

3.5.6 Routing Protocols and Parameters *32*

3.5.7 Number of Total and Source Nodes *32*

3.6 SYSTEM FACTORS 32

3.6.1 Number of Source Nodes *32*

3.6.2 Node Speeds *33*

3.6.3 Routing Protocols *33*

3.7 EVALUATION TECHNIQUE 33
3.8 WORKLOAD 34
3.9 DESIGN OF EXPERIMENTS 35
3.10 SUMMARY OF THE DEVELOPED MODEL 35
3.10.1 Number of Source Nodes 37
3.10.2 Load Introduced 37
3.11 SUMMARY 37
4 DESCRIPTION OF IMPLEMENTED MODELS 38
4.1 INTRODUCTION 38
4.2 802.11B MEDIUM ACCESS CONTROL LAYER OPERATION 38
4.2.1 Basic Operation 38
4.2.2 Implementation Details 42
4.3 IMPLEMENTATION OF AODV 43
4.3.1 Routing Parameters 43
4.3.2 Operation of the Protocol Model 44
4.4 IMPLEMENTATION OF RTRP 46
5 SIMULATION RESULTS 48
5.1 OVERVIEW 48
5.2 PACKET DELIVERY FRACTION 50
5.2.1 5 Sources 50
5.2.2 10 Sources 51
5.2.3 15 Sources 53
5.3 MISSED DEADLINE FRACTION 54

5.3.1 5 Sources *54*

5.3.2 10 Sources *54*

5.3.3 15 Sources *56*

5.4 ROUTING OVERHEAD 57

5.4.1 5 Sources *57*

5.4.2 10 Sources *58*

5.4.3 15 Sources *59*

5.5 AVERAGE ETE DELAY 60

5.6 SUMMARY 63

6 SUMMARY AND RECOMMANDATIONS 64

6.1 SUMMARY 64

6.2 FUTURE RECOMMENDATIONS 66

APPENDIX A. MODEL VALIDATION 67

A.1. VALIDATION OF THE 802.11 MAC MODEL 67

A.2. VALIDATION OF THE AODV MODEL 69

A.3. SUMMARY 69

APPENDIX B. SIMULATION RESULTS 71

B.1. SIMULATION RESULTS 71

B.2. ANOVA TABLES 75

B.3. PAIRED OBSERVATION COMPARISONS 77

BIBLIOGRAPHY 79

VITA 82

List of Figures

FIGURE 1. AN AD HOC NETWORK 7

FIGURE 2 OPERATION OFCGSR 12

FIGURE 3 AODV ROUTE DISCOVERY PROCESS 16

FIGURE 4 TORA HEIGHT METRIC 18

FIGURE 4. OSI REFERENCE MODEL 27

FIGURE 5. BASIC MEDIUM ACCESS SCHEME 39

FIGURE 6. THE MANAGEMENT OF THE NAV VALUE 41

FIGURE 7. PACKET DELIVERY FRACTION FOR 5 SOURCES 51

FIGURE 8. PACKET DELIVERY FRACTION FOR 10 SOURCES 52

FIGURE 9. PACKET DELIVERY FRACTION FOR 15 SOURCES 53

FIGURE 10. MISSED DEADLINE FRACTIONS FOR 5 SOURCES 55

FIGURE 11. MISSED DEADLINE FRACTION FOR 10 SOURCE NODES 55

FIGURE 12. MISSED DEADLINE FRACTION FOR 15 SOURCES 57

FIGURE 13. ROUTING OVERHEADS FOR 5 SOURCE NODES 58

FIGURE 14. ROUTING OVERHEAD FOR 10 SOURCE NODES 59

FIGURE 15. ROUTING OVERHEAD FOR 15 SOURCES 60

FIGURE 16. AVERAGE ETE DELAY FOR 5 SOURCE NODES 61

FIGURE 17. AVERAGE ETE DELAY FOR 10 SOURCES 62

FIGURE 18. AVERAGE ETE DELAY FOR 15 SOURCES 62

FIGURE 19. SATURATION THROUGHPUTS OF 802.11 MODEL AND [BFO96] 68

FIGURE 20. LOAD VS. THROUGHPUT 68

FIGURE 21. PACKET DELIVERY FRACTION FOR AODV VALIDATION 70

FIGURE 22. ROUTING OVERHEADS FOR AODV VALIDATION 70

List of Tables

TABLE 1. SYSTEM FACTORS 32

TABLE 2. WORKLOAD CHARACTERISTICS 37

TABLE 3. SIMULATION RESULTS FOR PACKET DELIVERY FRACTION 71

TABLE 4. 90% CONFIDENCE INTERVALS FOR PACKET DELIVERY FRACTION RESULTS 72

TABLE 5. SIMULATION RESULTS FOR MISSED DEADLINE FRACTION 72

TABLE 6. 90% CONFIDENCE INTERVALS FOR MISSED DEADLINE FRACTION RESULTS 73

TABLE 7. SIMULATION RESULTS FOR ROUTING OVERHEAD 73

TABLE 8. 90% CONFIDENCE INTERVALS FOR ROUTING OVERHEAD RESULTS 74

TABLE 9. SIMULATION RESULTS FOR ETE DELAY 74

TABLE 10. 90% CONFIDENCE INTERVALS FOR MEAN ETE DELAY RESULTS 75

TABLE 11. ENUMERATION OF FACTORS 75

TABLE 12. ANOVA TABLE FOR PACKET DELIVERY FRACTION 75

TABLE 13. ANOVA TABLE FOR MISSED DEADLINE FRACTION 76

TABLE 14. ANOVA TABLE FOR ROUTING OVERHEAD 76

TABLE 15. ANOVA TABLE FOR AVERAGE ETE DELAY 76

TABLE 16. COMPARISON OF PROTOCOLS FOR PACKET DELIVERY FRACTION 77

TABLE 17. COMPARISON OF PROTOCOLS FOR MISSED DEADLINE FRACTION 77

TABLE 18. COMPARISON OF ROUTING PROTOCOLS FOR ROUTING OVERHEAD 77

TABLE 19. COMPARISON OF ROUTING PROTOCOLS FOR AVERAGE ETE DELAY 78

AFIT/GCE/ENG/01M-02

Abstract

Mobile networks take the communication concept one step further than wireless networks. In these networks, all nodes in the network are assumed to be mobile. These networks are also called mobile ad hoc networks, due to their mobility and random configurations. Ad hoc networking is a relatively new concept; consequently, many researches are in progress focusing on each level of the network stack of ad hoc networks.

This research focuses on the routing of time-sensitive data in ad hoc networks. A routing protocol named Ad hoc On-demand Distance Vectoring (AODV), which has been developed by Internet Engineering Task Force (IETF) for ad hoc networks, has been studied. Taking this protocol as a point of departure, a new routing protocol named as Real Time Routing Protocol (RTRP) was developed while considering the characteristics of time-sensitive data. These two routing protocols have been modeled using OPNET, a discrete-event network simulation tool, and simulations were run to compare the performances of these protocols.

It has been discovered that, for lightly loaded networks the protocols performed very similarly. However, when the network load was increased, RTRP began to outperform AODV significantly. For some cases, RTRP delivered more than twice the number of packets that AODV delivered. Taking these results into account, some properties that a real-time routing protocol should have are proposed.

ROUTING OF TIME-SENSITIVE DATA IN MOBILE AD-HOC NETWORKS

1 INTRODUCTION

> *"Everything that can be invented has been invented."*
>
> Letter to President W. McKinley from U.S. Patent Office, 1899

1.1 Introduction

It was not long ago, only a hundred years, when a letter containing above words was sent to the President of the United States. From most people's point of view, these words reflected the reality at that time; however, time has shown that these people mispredicted what was coming in the following hundred years.

The advances in technology have far exceeded even the most imaginative person's predictions in twentieth century. Before this century, there had already been enormous technological advances that helped the human race to advance to the industrial age from the agricultural societies of the middle Ages. However, these advances are not as significant as the inventions that have been made in the twentieth century. Through the introduction of the transistor, electronics has entered almost every field of daily life in this century. Consequently, with the help of electronics and miniaturization, we have crossed the threshold of information age.

Today, in almost every device that people use, there is some kind of electronic circuitry. From electronic engine controls in vehicles to digital circuits in the televisions, electronics have become part of daily life. Perhaps the most impressive use of electronics in the twentieth century is in computers. Since the introduction of computers, the manufacturing industry has become widely dependent on these devices. Manufacturing lines are now utilizing the computers in almost every control system. Furthermore, with the development of cheaper and more capable processors, personal computers are available to the average user. Today, it is estimated that 61% of households in the US owns at least one personal computer.

As the number of computers increases, the need to connect these computers rises. As a result of this need, local area networks (LANs) have been widely installed throughout the world. Today, with Ethernet cards priced less than $40, local area networks have been available even to ordinary households. Furthermore, the evolution of the Internet from a military and academic to a worldwide network has made communication and dissemination of information much easier than ever before.

Another impressive area that integrated electronics has found its way into is communications. Again, with the introduction of integrated electronics, means of communicating have evolved impressively. Today's communication tools are far more advanced than could be imagined two decades ago. Besides the wired networks such as telephone and cable television, the wireless communication era was born with the development of highly reliable, miniature, solid-state radio frequency hardware in the 1970s [Rap96]. The number of cellular phone users grew from 25,000 in 1984 to about 16 million in 1994, and since then, wireless services have been experiencing customer growth rates well in excess of 50% per year [Rap96].

As wireless technologies become more affordable, researchers have been integrating computer and wireless technologies into wireless networks. Wireless computer networks have become an area that considerable research effort has been directed. These networks have many benefits for all types of users. With the development of the Wireless LAN MAC protocol by IEEE in 1997, IEEE 802.11 [IEEE99], new products that utilize wireless technology have begun to appear on the market.

1.2 Research Objectives

With the emerging interest in wireless computer networks, researchers working in this field of study have been developing many routing protocols to make these networks perform more efficiently. Each of these routing protocols approaches the problem of routing with a different philosophy. However, since it is a relatively new research area, there are not many simulation studies that analyze the performance of these networks, even with the non-time sensitive loads. This is especially true for ad hoc networks.

The objectives of this research are two-fold. The first objective of this research is to accomplish a performance analysis of routing protocols for mobile ad hoc networks that are used to carry time-sensitive voice data. The metrics that are used to measure the performance of the wireless networks are slightly different than the performance metrics that are used in wired networks. In accordance with this, this study performs an analysis of the packet delivery ratio of ad hoc networks within the time constraints of real time data while trying to maximize the load that is introduced to the network. This analysis is conducted using simulation.

To accomplish this task, routing protocols needed to be implemented in the simulation environment. The first routing protocol that has been implemented is the Ad

Hoc on Demand Routing Protocol (AODV) which has been developed by the Internet Engineering Task Force (IETF). Taking the unique characteristics of time sensitive data into account, a new routing protocol named Real Time routing Protocol (RTRP) was developed using AODV as the point of departure. The simulations were designed in OPNET, a discrete event simulation tool.

The second objective of this research was to improve the understanding of mobile ad hoc networks.

1.3 Organization of the Document

The first chapter makes a brief introduction into the computer and communication networks. The research goals and the organization of this document were also given in this chapter.

The second chapter presents an overview of different approaches taken in routing in mobile ad hoc networks. Short overviews of the routing protocols that demonstrate these different approaches have also been given in this chapter. These routing protocols have been organized in two categories: table-driven and on-demand driven. Also, brief descriptions of the constraints that are associated with the mobile wireless networks are given in this chapter.

The third chapter is devoted to methodology. This chapter outlines the system under test (SUT), component under study (CUS), factors, and parameters of the system. The design of experiments, as well as the workload that is introduced to the system is also presented in this chapter.

Chapter four contains a brief description of the 802.11 Wireless LAN protocol that was developed by the IEEE. This chapter also gives brief information about the implementations of this protocol, as well as AODV and RTRP in OPNET.

The fifth chapter presents the results of simulation runs that were accomplished for the purposes of this research. A performance comparison of the two protocols is performed and the results are presented in this chapter.

Chapter six contains the conclusions drawn from the results of the research. Furthermore, this chapter presents the recommendations for future work that should be accomplished for further analysis of mobile ad hoc networks.

2 LITERATURE SURVEY

2.1 Introduction

Since the first demonstration of radio's ability to provide continuous contact with the ships sailing in the English Channel in 1897 [Rap96], wireless communication methods have evolved. Especially with the emergence of the integrated circuits in 1970s, the wireless communication industry has grown by orders of magnitude.

Wireless networks are communication networks in which some of the nodes are mobile. These nodes connect to the network by utilizing radio frequency (RF), infrared (IR), or laser technologies. There are two types of wireless networks. The first type is infrastructure wireless networks. These networks have routers and gateways as stationary components to which mobile nodes within the network connect. Mobile nodes connect to the nearest base station whose communication radius covers the area that the nodes are in. When a mobile node moves out of the coverage area of a base station, it is handed of to a new base station that covers the area that the node is now in. Cellular phone technology is a typical example of an infrastructure network.

The second type of wireless network is the ad hoc network. In this type of network, all nodes in the network are mobile as before; however, there are no wired or stationary parts of the network. Figure 1 shows an example to ad hoc networks with three nodes. Additionally, in ad hoc networks there are no dedicated routers or gateways. Instead, all of the nodes that participate in the network have the responsibility of acting as a router and forwarding packets to their destination addresses as needed. Due to their mobility, ad hoc networks have continuously changing topologies. Consequently, routing becomes a major player in the performance of these networks.

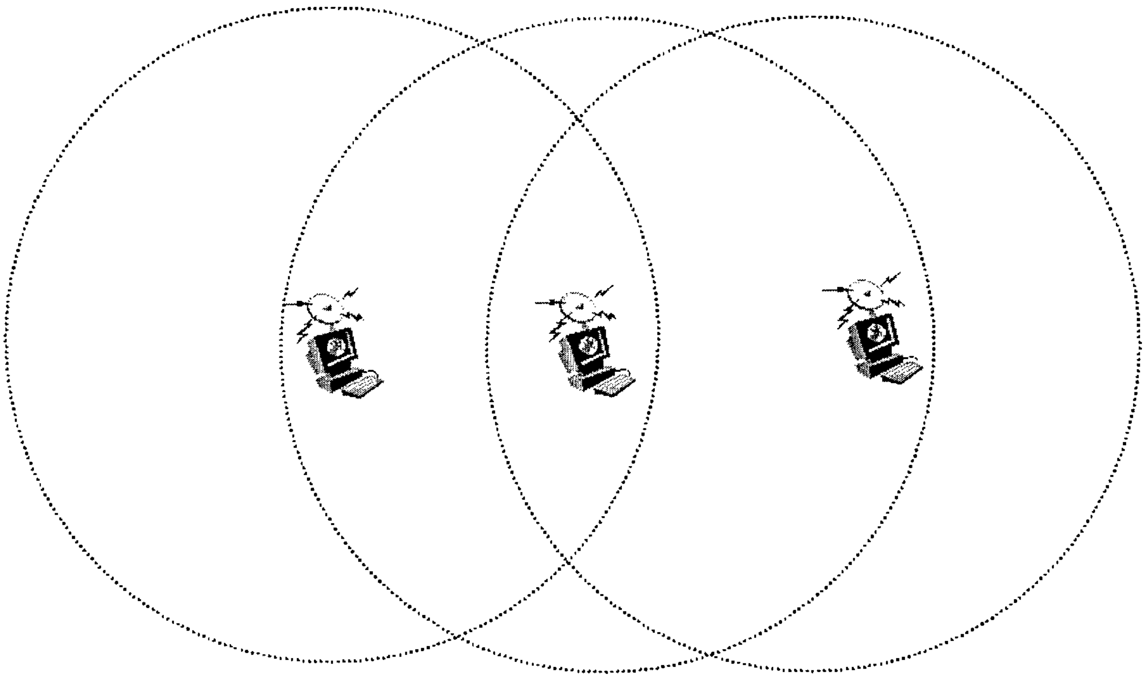


Figure 1. An Ad Hoc Network

Ad hoc networks are a relatively new concept. Therefore, routing packets within the network is still an open research area [TLG00]. There have been, however, some studies on the development of the protocols for ad hoc networks. In this chapter, an overview of the protocols that are developed for ad hoc networks and a short comparison of these protocols are presented.

2.2 Ad Hoc Protocols

Since ad hoc networks have unique characteristics, the routing algorithms developed for wired networks cannot be readily adapted to run efficiently in them. The characteristics of ad hoc networks include relatively low bandwidth, high bit error rate, and the need for low power consumption. In order to overcome these problems, new protocols have been developed for ad hoc networks. Each of these protocols deals with the above limitations using different approaches.

The routing protocols that are developed to date can be categorized as, (a) table-driven protocols, or (b) source-initiated-on-demand-driven protocols. These two types of protocols have different philosophies in the way they handle the establishment and the maintenance of the routes in a network. The particular routing protocols that fall in these two categories are:

1. Table Driven Protocols
    - Destination Sequenced Distance Vectoring Routing Protocol
    - Wireless Routing Protocol
    - Cluster-head Gateway Switch Routing Protocol
2. Source-Initiated-On-Demand Driven Routing Protocols
    - Dynamic Source Routing Protocol
    - Ad Hoc On-demand Distance Vectoring Protocol
    - Temporarily Ordered Routing Algorithm Protocol
    - Zone Routing Protocol
    - Associativity Based Routing Protocol
    - Signal Strength Routing Protocol

Each category of the routing protocols will be examined in the following sections.

2.2.1 Table Driven Routing Protocols

The table driven routing protocols are similar to the connectionless approach of forwarding packets used in wired networks. These protocols try to maintain the consistent and up-to-date routing information about each node in the network. Typically, these protocols require all nodes to keep tables to maintain state information about existing routes in the network. The area where these routing protocols differ is the number and the structure of the routing tables and the different methodologies they use during the changes in the network structure [RT99].

2.2.1.1 Destination-Sequenced Distance Vectoring Protocol

Destination-Sequenced Distance Vectoring (DSDV) Protocol is based on the classical Bellman-Ford algorithm [PB94]. It requires every node in the network to maintain a routing table with all possible destinations and the number of hops to that destination recorded. Updates to the routing tables are periodically transmitted throughout the network in order to maintain consistency. Each route in the network is tagged with a sequence number. Additionally, a next hop field is used to determine the next hop for each route in the table.

Since DSDV does not assume mobile nodes have synchronized clocks, it uses sequence numbers to determine the freshness of the routes. Each node in the network advertises a monotonically increasing sequence number periodically. Nodes that receive this transmission update their route entries for this node. DSDV also requires each node to broadcast updates to the routing tables. As a result, when a neighboring node hears an advertising node's update transmission, it updates routing table entries accordingly.

When a neighboring node determines that its link to a node has been broken, it broadcasts a sequence number greater than the broken link's sequence number with an infinite metric. Nodes that are routing packets through this node will update their table entries with the infinite distance metric and not use that link anymore.

The DSDV routing protocol guarantees the loop-freedom property because of the changes made to the Bellman-Ford algorithm [PB94]. If the sequence numbers are the same for different routes, DSDV uses the shortest path approach when choosing a route. The shortest path is defined based on the number of hops in the route.

2.2.1.2 Wireless Routing Protocol

The Wireless Routing Protocol (WRP) [MGA96] is also a table based distance-vector routing protocol. Each node in the network maintains four tables to perform the routing. These tables are as follows:

1. Distance table
2. Routing table
3. Link-cost table and
4. Message retransmission list (MRL).

In its distance table, a node S keeps track of the distances to every destination node via the neighboring node, N, the downstream neighbor of node N. The routing table of S contains the distance to each destination node from node S, the predecessor and the successor of node S on this path, and a tag to identify if the entry is a simple path, a loop, or invalid. The upstream and downstream nodes are kept to check the link consistency and loop freedom property of the routes. The link-cost table is used to keep the costs of the links to the neighboring nodes with the number of time-outs since the last communication with the nodes.

Nodes in a wireless network inform each other about links they have via update messages. These messages are transmitted periodically or in the event of a change of the state of a link. Update messages are broadcast among only neighboring nodes. Neighbors that receive these update messages update their table entries accordingly.

Nodes in the network become aware of their neighbors by these update messages. If a node does not have any change in its links' states, it broadcasts a hello message after a time-out period to ensure connectivity.

MRL is used to keep track of the acknowledgements for the update messages received from the neighboring nodes. Each entry in the MRL has a sequence number of the update message, a retransmission counter, and an ack-required flag for each of the neighbors of the node. MRL keeps track of the update messages and the neighbors that need to acknowledge these updates.

2.2.1.3 Cluster-head Gateway Switch Routing Protocol

The Cluster-head Gateway Switch Routing Protocol (CGSR) [CWLG97] is based on the DSDV routing protocol. In this protocol, the nodes are grouped into clusters, and a node within a cluster is chosen as the cluster-head. Gateways are nodes that can receive from two or more cluster-heads at the same time. Figure 2 illustrates an ad hoc network that is grouped into three clusters, and operation of the CGSR is demonstrated as well.

When a node has a packet to transmit, the packet is first passed to the cluster-head of the node. Next, the cluster-head sends the packet either to the cluster-head of the destination or to a cluster-head on the way via a gateway to the other cluster-head. When the packet arrives at the destination node's cluster-head, it passes the packet to the destination node.

Cluster-heads are chosen when a node goes offline or out of the transmission range of any other node. Each node in the network keeps a routing table similar to the DSDV. Additionally, each node also has a table in which the cluster-heads of the possible destination nodes are kept. Table updates are transmitted similar to the DSDV.

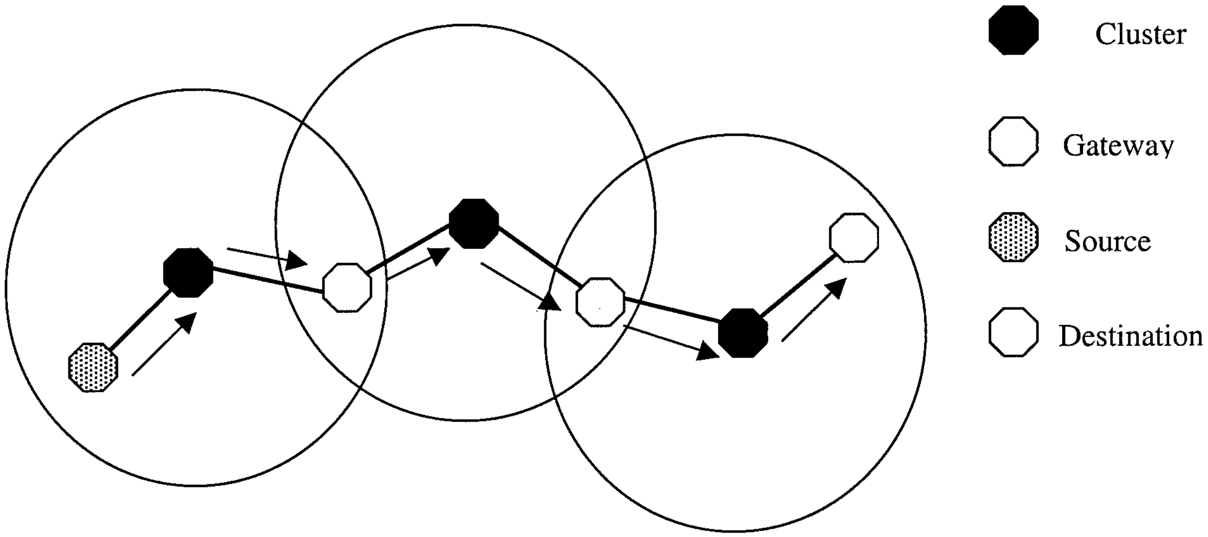


Figure 2 Operation of CGSR in an Ad Hoc Network

2.2.2 Source-Initiated On-Demand Driven Routing Protocols

The table driven approach tries to keep track of all the possible routes in the network, whether they are needed or not. Source-initiated on demand driven routing, on the other hand, is a conceptually different approach. This type of routing creates routes when they are needed. When a node decides to send a packet to a destination, it will initially check its existing routes to determine if an existing route already exists. If there is not a route to the destination, then a route discovery process is initiated. This discovery process is terminated when a route is found or when it is determined that the destination is unreachable. When a route is discovered, the route will be maintained by some means of route maintenance policy depending on the protocol. These routes are kept until the routes are no longer needed or the link is broken.

2.2.2.1 Dynamic Source Routing

Dynamic Source Routing (DSR) [JM96] [BJM99] is a protocol developed by the Monarch Project at Carnegie Mellon University. DSR is an on-demand routing protocol that uses the concept of source routing. In the source routing approach, a packet that is sent to a destination carries the information about the nodes it will pass through within the packet itself. That is, the source node explicitly determines the route.

The DSR protocol uses two mechanisms to perform routing. The first mechanism is the route discovery process that is initiated when a route to a destination is needed. Second mechanism is the route maintenance process that is initiated after a route is established.

There are four data structures that DSR implements. These data structures are:

1. Route Cache,
2. Route Request Table,
3. Send Buffer, and
4. Retransmission Buffer.

All routing information is saved in the route cache. The route cache is updated upon receiving a route request (RREQ) or a route reply (RREP) message. The route cache is logically indexed by the destination addresses. For any destination, DSR allows more than one route entry in the route cache.

The route request table is used to keep track of forwarded or originated RREQ packets. This table is indexed by the destination address and contains the following information: time of attempt, remaining time before next attempt, and the time to live (TTL) field from the IP header.

A send buffer is used to hold packets that are waiting for route discovery. A retransmission buffer holds packets that have been transmitted and waiting for acknowledgement.

When a node needs to send a packet, it initially checks its route cache to see if there is an unexpired route to the destination. If there is, the node puts the route information in the packet and sends it via this route. If there is not any current route in the route cache, the source node initiates a route discovery process by broadcasting a RREQ packet. The RREQ packet contains the address of the source node, address of the destination node and a unique sequence number. Upon receiving the packet, the neighboring nodes check to see if they have a route to the destination in their own route caches. If they do not have any route to the destination, they add their address in the packet's route record and broadcast it. In order to limit of propagation of a RREQ packet, the nodes also put the RREQ packet's information in the RREQ tables. As a result, if the nodes receive other copies of the packet, they will ignore it.

If any of the intermediate nodes have a route to the destination, then a RREP packet is created. If the RREP packet is sent by an intermediate node, the node combines the route information from its route cache with the route record field of the RREQ packet.

Depending on the implementation of DSR, there are different ways a RREP message is sent to the source node. If the implementation supports bi-directional links, then the route that the packet took to this point is reversed. If the links are asymmetrical, a new route discovery process is initiated if the source node of the RREP message does not have a current link to the source of the RREQ message.

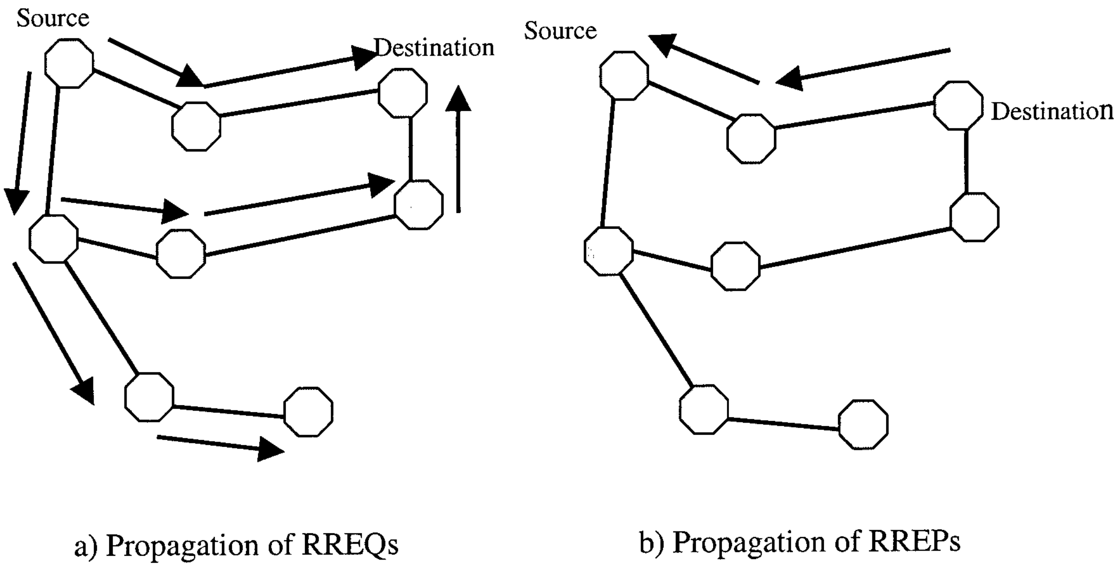
Route maintenance is accomplished using route error (RERR) and acknowledgement packets. When a node determines that its link to a node has been broken, it broadcasts a RERR message. Nodes receiving this message will check their route caches and update their links. Also, acknowledgement packets are used to make sure that the route links are operating correctly. In addition to acknowledge packets, DSR uses passive acknowledgement, as well. A node assumes that the reception of a packet is acknowledged if it hears the receiving node transmitting it to the next node on the route.

2.2.2.2 Ad Hoc On Demand Distance Vectoring Routing Protocol

The ad hoc on demand distance vectoring (AODV) [PR99] [PRD00] is a routing protocol that is built on DSDV and DSR. AODV borrows the route maintenance and route discovery approach from DSR and hop-by-hop routing and sequence numbers from DSDV.

AODV has three types of messages that are used in the route discovery and route maintenance processes. These messages are route requests (RREQ), route replies (RREP), and route errors (RERR). These message types are similar to the DSR message types. AODV also has a multicast capable version that has some additional message types used for multicasting.

In AODV, in addition to the routing table, a retransmission buffer may be implemented to hold the packets waiting for an acknowledgement. This table becomes necessary when the implementation is using a MAC protocol that does not have a link layer acknowledge notification. If the implementation is using IEEE 802.11 as the MAC layer protocol, then an acknowledge process is not required by the routing protocol since IEEE 802.11 has link layer acknowledgement.



a) Propagation of RREQs b) Propagation of RREPs

Figure 3 AODV Route Discovery Process

AODV borrows sequence number usage from DSDV. A sequence number field is created for each route entry in the routing table. The source node broadcasts these sequence numbers in a monotonically increasing manner, as in DSDV.

Figure 3 gives an illustration of route discovery process in AODV. When a node has a packet to transmit, it initially checks its routing table. If there is not a route entry in the table or the route has expired, it broadcasts a RREQ message. The RREQ message contains a broadcast ID, which is incremented individually within each node and becomes a unique ID of the RREQ message combined with the source node address, the sequence number of the source and, if known, the sequence number of the last route to the destination. If no destination sequence number is available, then zero is used instead. The receiving nodes forward the packet until it arrives either to the destination or to a node that has a fresh route to the destination. During the forwarding process, each intermediate node in the route records the source address, broadcast id and the reception time of the packet into a broadcast record list. If further copies of the same RREQ packet are received, they are discarded. When the packet arrives to a node with a fresh route to the destination, it creates a RREP message and sends it to the neighboring node that the packet has arrived from. As the RREP message is routed back, every node on the reverse path updates their routing tables to set a forward route to the destination via the node that the RREP message has arrived from. Because the RREP message is transmitted back on the same path, AODV supports the use of only symmetric links.

During a link failure, a RERR message is sent back to the source node. If route is failed because of the source node's movement, the source node reinitiates the route discovery process if the route is still needed.

As an additional feature, AODV makes use of the hello messages to assure the connectivity. Also, like DSR, AODV passively listens the neighboring nodes for routing table updates.

2.2.2.3 Temporally Ordered Routing Algorithm

Temporally ordered routing algorithm (TORA) [PC97] [PC99] is a distributed routing algorithm that makes use of link reversal. Its distinctive properties are the quick discovery of routes, multiple routes to a destination and localization of messages. To achieve the localization of messages that are caused by topological changes in the network, all nodes keep information about the neighboring nodes.

There are three mechanisms that are used in TORA to create and maintain routes. These are route creation, route maintenance, and route erasure.

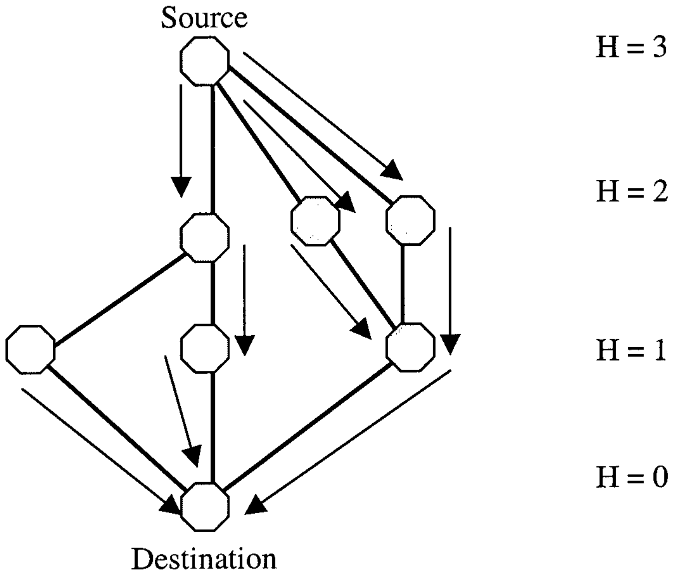


Figure 4 TORA Height Metric

During the creation of a route, a height metric is used by the nodes to create a directed acyclic graph. The destination node becomes the root of the tree and the links are created upwards or downwards depending on the height of the neighboring nodes. Figure 4 illustrates the use of the height metric. It is simply the distance from the destination node.

A copy of TORA is run on each of the nodes in the network. When a node needs a route to send packets, it broadcasts a query (QRY) message containing the address of the destination node. Initially, the source node sets its height to null. The packet propagates through the network until it arrives either to the destination or to a node that has a route to the destination. The final recipient of the QRY message replies back with an update (UPD) message including its height relative to the destination node. As the packet is routed back to the source node, each intermediate node sets its height greater than the previous node. This approach ends up creating a directed link from the source to the destination node.

When a link is broken, the node at the end of this link transmits an UPD packet with a height which is greater than its neighboring nodes. Consequently, the link is reversed to adapt the new height of the node. When a node discovers a network partition, it transmits a clear message and invalid routes are removed from the network.

An important aspect of TORA is the requirement for synchronization between nodes. This synchronization may be accomplished through an external clock, such as GPS. Also, the synchronization requirement has the potential for oscillations if the coordinating sets of nodes concurrently delete routes, build new routes or discover partitions in the network.

2.2.2.4 Zone Routing Protocol

The zone routing protocol (ZRP) [Haa97] is a hybrid protocol that uses both a reactive and a proactive approach in building routes. A zone is defined to be the collection of nodes that are at most R nodes away from a node. ZRP uses a proactive approach for communication within this zone and a reactive approach for communication with nodes that are out of the zone.

For intra-zone communication, each node keeps the routing information to each destination node. This is implemented by DSDV protocol. When an intra-zone packet is sent, the packet is flagged to stay within the zone. Changes in the topology of the network or the link state trigger the broadcasting of update packets.

Inter-zone communication, on the other hand, is implemented by a modified DSR protocol. When a node needs a route to a destination node out of its own zone, it broadcasts a RREQ message to the nodes that are on the border of its own zone. If the nodes on the border have a route to the desired destination, they reply with a RREP message, otherwise, they broadcast the request to the nodes that are on other zones' border.

2.2.2.5 Associativity Based Routing

The associativity based routing protocol (ABR) [Toh96] uses a totally different approach for routing. In ABR protocol, the stability of the mobile nodes is chosen as the main metric and routes are chosen accordingly. ABR provides loop-free operation and packet duplication is prevented.

The main goal of ABR is providing long-lived routes. In order to establish this goal, each node in the network broadcasts a beacon periodically. Neighboring nodes that receive this beacon update the associativity of the node, increasing the dependability of the node. When a node moves out of the reception area of the other node, since its beacons are not received, its associativity is eventually reset.

ABR has three mechanisms to provide routing. These mechanisms are route discovery, route reconstruction, and route deletion. When a node needs a route to a destination it sends a broadcast query (BQ) message. Intermediate nodes receiving the packet add their address and associativity to the packet and delete the upstream neighbor's associativity. When a packet arrives at the destination, the destination node is able to check the packets coming along different routes and choose the route with the highest associativity. Consequently, a reply message is sent along the route with highest associativity.

2.2.2.6 Signal Stability Routing

Signal stability routing (SSR)[DRWT97] uses yet a different metric than the other routing protocols. In this protocol, routes are selected depending on the strength of their connection. SSR consists of two different cooperating protocols. These are the dynamic routing protocol (DRP) and the static routing protocol (SRP).

DRP is responsible for maintaining the signal stability table (SST) and the routing table. Nodes participating in the network broadcast periodic beacons. These beacons are used to measure the signal strength of the transmitting node and are kept in the SST. DRP is also responsible for reception of all packets. After processing these packets, DRP passes the packets to SRP.

SRP checks the packet to see if the destination is the receiving node. If the receiving node is the destination, SRP passes the packet to higher layers in the network stack, otherwise, it checks its routing table to see if it has a route to the destination. If there is a route in the table, the packet is forwarded along this route; otherwise, SRP initiates a route discovery process. A route request packet is broadcast through the network and is forwarded only if it was received on a strong channel. If there is no route that can be established over strong channels to the destination, the source node initiates another route request process after a certain time-out period; this time accepting routes containing weak channels.

2.3 Comparison of the Routing Protocols

2.3.1 Table-driven Routing Protocols

The first protocol examined was the DSDV protocol. The DSDV protocol is based on the classical Bellman-Ford algorithm and guarantees a single, loop-free route to the destination by always selecting the shortest path. However, since the routing protocol requires all the nodes to have state information of the network at all times, periodic updates must be done to the routing tables. These updates increase the overhead that is introduced to the network. In order to decrease the amount of the overhead, two types of mechanisms are developed for updates. The first type is called a “full-dump” where a node broadcasts its routing table completely. The second type is “incremental” updates where only changes are broadcast. Even though the use of incremental updates decrease the amount of the overhead associated, it still consumes bandwidth in DSDV. This feature of the DSDV makes it inefficient for larger networks since the overhead grows as $O(n^2)$ [RT99].

WRP has a different approach than DSDV. The first difference is the number of tables that must be maintained. WRP requires each node maintain 4 tables that may lead to a memory problem when the network becomes large enough. In addition to this disadvantage, WRP utilizes “hello” messages to ensure the freshness of the links when no traffic is received for a certain period of time. These messages both consume bandwidth and power, which may become a problem if the nodes are running on battery power.

CGSR has DSDV as the underlying scheme. As a result, it inherits the benefits and disadvantages of this protocol. Additionally, the cluster-head election process increases the overhead that is introduced into the network. Furthermore, since cluster-heads and gateways are used extensively in routing, these nodes may become the bottlenecks of the system. Finally, utilizing a cluster-head table increases memory consumption.

To summarize all table-driven routing protocols, it can be said that each protocol has the same communication complexity since all nodes in the network are affected by route changes. Finally, messages that are needed to maintain the state information of the network consume a certain amount of bandwidth in table-driven protocol based networks.

2.3.2 Source-Initiated on Demand Routing Protocols

The DSR and the AODV routing protocols share some common features. AODV borrows route discovery and route maintenance methods from DSR. However, the overhead that is associated with DSR is higher than the overhead in AODV since DSR uses source routing where AODV uses hop-by-hop routing. Packets in DSR carry all the routing information, whereas they only carry next node information in AODV. When the network becomes large enough, this feature may decrease the throughput of the network significantly.

An important feature of DSR is that more than one route may be maintained to a destination. This feature allows the source node to use remaining routes, if any, during a link failure. As a result, the time and bandwidth consumption for a new route discovery process can be avoided. However, if the broken link is the only route available, a route discovery process must be initiated which consumes the same amount of bandwidth as AODV.

As in DSR, TORA also allows multiple routes between the source and the destination. The major feature that distinguishes TORA from the rest of the routing protocols is the construction of a directed acyclic graph. TORA also utilizes a multicast capability. The major disadvantage of this routing protocol is the dependency of the nodes to an external clock, such as GPS, for synchronization. If an external clock is not available, TORA cannot be implemented.

SSR and ABR take different approaches than the rest of the routing protocols. ABR is a protocol that is based on the associativity of the nodes where SSR is based on the signal strength. In order to determine associativity of the nodes, each node in the network broadcasts periodic beacons. These beacons consume bandwidth as well as power. One of the disadvantages of SSR is the fact that only the destination can respond with a route reply packet.

2.4 Summary

The major difference between the two classes of mobile network routing protocols is their approach to maintaining routes. Table-driven routing protocols require all nodes keep state information of the network and maintain routes whether they are needed or not. This approach has the advantage of using a route without any delay whenever it is needed. However, this availability comes at the cost of bandwidth for periodic updates.

On, the other side, on-demand routing protocols do not require periodic updates to maintain the state information of the network. A route is discovered as it is needed. This feature reduces bandwidth consumption for maintenance of state information. However, if there is no route in the cache to a destination, packets have to wait until a route is discovered. This causes an initial delay depending on the network size.

Another difference among the routing protocols is the method used for addressing. CGSR uses a hierarchical addressing scheme where the others use flat addressing. Hierarchical addressing is an advantage in large scale networks. However, as in CGSR, hierarchical addressing can increase the load on some nodes such as cluster-heads or gateways. Flat addressing is easier and simple to use. However, when the network size increases, it may cause some problems such as memory requirements for the storage of the routes and the number of broadcast messages in case of a link failure [BCSR].

3 OBJECTIVES AND METHODOLOGY

3.1 Overview

In this chapter, the methodology that is used in this research is presented. The effect of the research methodology on the outcome of the research cannot be underestimated. As a result, in order to perform a complete analysis and to avoid common mistakes; the following methodology is used [Jai91]:

1. State the goals of the study and define system boundaries,
2. List the system services and possible outcomes,
3. Select performance metrics,
4. List system and workload parameters,
5. Select factors and their values,
6. Select evaluation techniques,
7. Select the workload, and
8. Design the experiments.

3.2 Objectives and System Boundaries

The objective of this research is to improve the performance of an ad hoc packet data network that is transporting time sensitive data. The aspects of performance that are studied in this research are the packet delivery ratio and the throughput of the network.

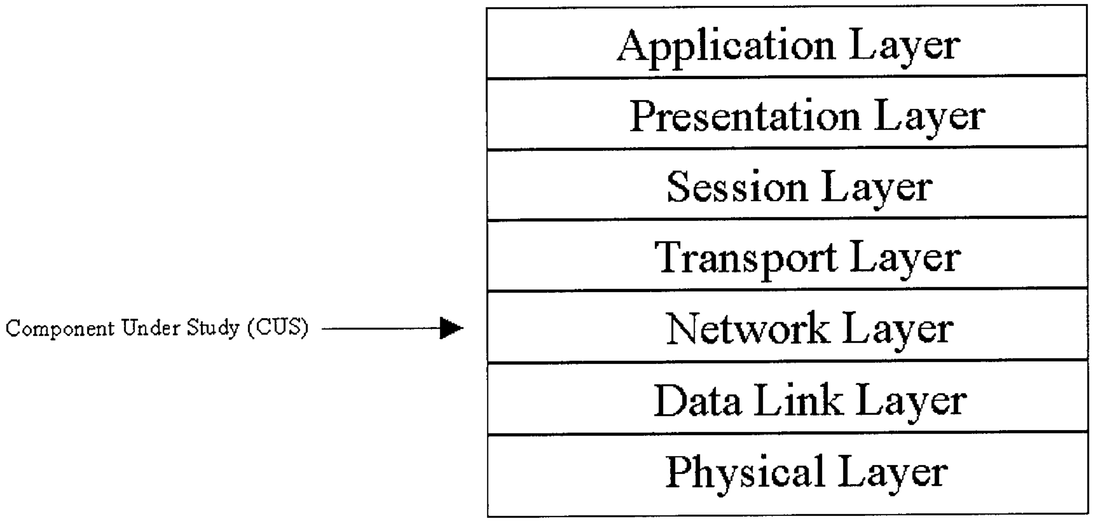


Figure 5. OSI Reference Model

To achieve this objective, a routing protocol is introduced specifically designed for this purpose.

The system under test (SUT) is the ad hoc network. This system consists of two or more mobile nodes. Using the OSI network model as a reference, the component under study is the network layer since routing protocol lies in this layer, as shown in figure 4.

Routing protocols that have been designed for ad hoc networks were briefly discussed in Chapter 2. All of these routing protocols assume that the ad hoc network is being used to transport non real-time data or data is not time sensitive. As a result, the performance of these protocols with respect to real-time data is degraded since these protocols do not consider the unique requirements of real-time. Using AODV as the point of departure, a routing protocol named as Real Time Routing Protocol (RTRP) was developed specifically for time sensitive data and simulations were run for both AODV and RTRP. The results of these simulation runs were statistically analyzed to reach a final conclusion.

The two protocols' performance was tested using the same network. Additionally, since the routing protocol was implemented in the network layer of the OSI model, the same data link and physical layers were used throughout the simulations. For the data link layer, the IEEE 802.11 MAC protocol [IEEE99] was used. However, since the data link layers and the network layers are closely related with each other [BCSR], some additions are made to the data link layer for both RTRP and ADOV. The IEEE 802.11 MAC protocol and the changes that are made to this protocol are discussed in Chapter 4.

3.3 System Services

The service that is provided by the system is the on-time delivery of the real-time data that is introduced to the network. There are three possible outcomes of this service: on-time delivery, late-delivery and no-delivery. Delivery is considered on-time delivery if the packet arrives before the deadline, and it is assumed to be a no-delivery if the packet is dropped due to a missed deadline. Although the system is designed to drop the aged packets at every hop, it is still possible that a packet can miss the deadline due to transmission and propagation delays. This leads to a late-delivery.

3.4 Performance Metrics

3.4.1 Missed Deadline Fraction

Missed Deadline Fraction is among the important metrics in networks where the load is time-sensitive. For this research, missed deadline is measured by dividing the number of dropped or discarded packets by the total number of packets sent. For AODV, the number of dropped or discarded packets represents the packets that reach their destination after their deadlines. For RTRP, this number includes both the packets that are dropped en-route to their destination and the packets that are discarded at their destination due to a missed deadline.

3.4.2 Mean End-to-End Delay

Mean end-to-end (ETE) delay is another metric that is used to measure the performance of a network. However, for real-time systems this metric becomes of secondary importance because of the time sensitivity of data. The packets in a real time system are not delivered to their destinations once they miss their deadlines. As a result, mean ETE delay is not an adequate measure of performance. For this research ETE delay is reported only to have the ability of comparing the system with other systems.

3.4.3 Packet Delivery Fraction

Packet delivery fraction is the most important performance metric for a mobile ad hoc network that transports time sensitive data. In such a network, there are many reasons that a packet cannot be delivered to its destination. First, the mobility of the nodes can make the establishment of a route to a destination impossible. Second, the packets can miss their deadlines due to the route establishment and/or medium access delays. Consequently, the packet delivery fraction, calculated as the number of packets delivered to their destination within their time-constraints divided by number of packets introduced to the system becomes the major performance metric in this research.

3.4.4 Routing Overhead

Although it is not a measure of the performance of the networks, routing overhead is a measure of protocol efficiency. The routing overhead is calculated by dividing all the routing packets that are generated by network layer by data packets that reach their destinations. It is measured in packets.

3.5 System and Workload Parameters

The system and the workload characteristics that affect the performance of the network are called parameters [Jai91]. In accordance with this definition, the system parameters that affect the performance of the network are data rate, channel bit error rate, workload, network topology, and movement models, MAC layer parameters, routing protocols and parameters, number of total and source nodes and node speeds.

3.5.1 Data Rate

The IEEE 802.11b protocol specifies 4 different data rates: 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps [IEEE99]. The data rate chosen for this study is 2 Mbps for all of the simulation runs. The data rate of the channel has a direct effect on the performance of the network. However, for routing studies, choosing the data rate as a parameter rather than a factor is more appropriate.

3.5.2 Channel Bit Error Rate

The channel chosen for the simulation study is the ideal channel where the bit error rate is zero. Increasing the bit error rate will introduce additional packet losses to the system, however, this research focuses on the performance of the routing algorithm rather than lower layer functions.

3.5.3 Workload

The workload that is chosen for this research is voice data. Each source node introduces packetized voice data to the network in accordance with the parameters described in the following subsections.

3.5.4 Network Topology and Movement Models

The nodes are designed to move randomly within a 300 m x 900 m area. The trajectories that the nodes move along within an area are generated randomly before the simulation runs starting from random locations. The distance between the nodes and the movement models described above allows dynamic changes in the routes since the receiving node positions change dynamically. No pause times are added to the movement models at each hop to make the scenarios challenging for the protocols.

3.5.5 MAC Layer Parameters

The MAC layer parameters have a significant role on the performance of the routing algorithm that is implemented in the network. For this research, the IEEE 802.11 MAC layer specification for DSSS is used as the MAC layer parameters. The most important parameters that affect the performance are given below.

Slot time: 20 μs

SIFS time: 10 μs

DIFS time: 50 μs (calculated as described in 802.11 specification)

MAC processing delay: 0 μs

Cwmin: 31 (minimum value for contention window)

Cwmax: 1023 (maximum value for contention window)

Retry Limit: 9

3.5.6 Routing Protocols and Parameters

The two routing protocols that are used in this research are AODV and RTRP. The authors of AODV specification [PRD00] have suggested some default values for the protocol. The default values are used to the maximum extend possible. The parameters and their values are given in Chapter 4 for both of the routing protocols with a brief description of each parameter.

3.5.7 Number of Total and Source Nodes

The total number of nodes that participate in the networks are 30. The number of source nodes varies between 5 and 15.

3.6 System Factors

The factors that were chosen to be varied are number of source nodes, speeds of the nodes and the routing protocols.

Number of Source Nodes	5, 10 and 15
Node Speeds	7.2 km/h, 36 km/h, 72 km/h
Routing Protocols	AODV, RTRP

Table 1. System Factors

3.6.1 Number of Source Nodes

Not all of the nodes that are participating in the network are considered as source nodes. The three different numbers of source nodes are 5, 10, and 15. These numbers are chosen to determine the characteristics of the model developed under lightly loaded, medium loaded and heavily loaded situations.

3.6.2 Node Speeds

The nodes are classified into three categories based on their speeds: slow nodes, medium speed nodes, and fast nodes. Slow nodes are designed to move at a speed of 7.2 km/h to represent the slow moving vehicles that are in heavy traffic. Medium speed nodes are designed to move at a speed of 36 km/h representing vehicles moving within a city. Finally, fast nodes are selected to move at a speed of 72 km/h to represent fast moving vehicles. All nodes in the network are designed to move on random trajectories.

3.6.3 Routing Protocols

The routing protocols are also considered as a factor since two different routing protocols were used for the simulations designed for the purposed of this research. The details of the implementations of the protocols are given in Chapter 4.

3.7 Evaluation Technique

The evaluation technique chosen for this research is simulation. There are three evaluation techniques described in [Jai91]: analytical, simulation, and direct measurement. Since there is no system that has the properties described above at present, direct measurement technique is unavailable for this research. Also, constructing such a network for the research done becomes unacceptably expensive. Second, since a comparison is done between two different routing protocols, the analytical evaluation technique becomes computationally infeasible. As a result, simulation technique becomes the most suitable evaluation technique for this study.

For simulation modeling, OPNET was chosen. The model developed is a discrete time model. The simulation results were analyzed statistically to determine the confidence intervals and ANOVA tables.

3.8 Workload

The workload selected for this study is a synthetic workload that simulates real-time voice data. There are many coding techniques that are widely implemented to improve the performance in cellular and speech-based communication systems [Rap96]. Most of these coding techniques require 32 Kbps or lower data rates for two-way communications. For this research, a 32 Kbps data rate is used as the load introduced by each source node. It should be noted that 32 Kbps data is the load introduced by a source node to the network. Since most of the routes that the packets are forwarded over have at least two hops, the load introduced to the wireless channel as data is greater than this amount.

There are many methods used in modeling sources for two-way conversations. The most common technique is defining the voice source as a two-state finite machine with ON and OFF states. For this research voice sources are modeled as bursty data sources with ON and OFF states; typical values that are used for the duration of the states are exponentially distributed with means of 1.0 second for ON state and 1.35 seconds for OFF state. Each source simulates a voice source that has a 32 Kbps data rate sampled at every 20 msec by generating data packets according to a constant distribution with a mean of 20 msec. Each packet is 80 bytes long and is assumed to contain 20 msec voice data.

The destinations for the data packets are chosen randomly at the start of each burst. That is, when a source switches to ON state, it randomly chooses a destination, and the packets are sent to that destination until the node switches back to OFF state.

3.9 Design of Experiments

Among the various design techniques for experiments described in [Jai91], the full factorial design technique with replication is selected as the experimental design. This design technique requires the largest number of simulations, however, it is the most comprehensive one and gives the fullest description of the system under the situations described. Since the levels for each factor are at maximum three, the number of simulations that this technique introduces becomes reasonable. For this research, 54 different simulation runs were accomplished.

3.10 Summary of the Developed Model

This section summarizes each of the steps described above in tables.

Objective:	To improve the real-time performance of ad hoc networks
Performance Metrics:	1. Missed Deadline Fraction 2. Mean End-to-End Delay 3. Packet Delivery Fraction 4. Routing Overhead
Evaluation Technique:	Discrete-Event Simulation using OPNET
System under test:	Ad hoc mobile network consisting of 30 nodes with 5, 10, and 20 source nodes.
Component under study:	Routing Protocol in Network Layer.

Channel Data Rate	2 Mbps
Channel Bit Error Rate	Errorless
Transmission Range	250 meters
Network Topology	Three types of speeds for nodes: • Slow-7.2 km/h • Medium-36 km/h • Fast-72 km/h Two types of motion for nodes: • Circular (randomly moving in an area) • Linear (passing through an area)
MAC Layer Parameters	Slot time 20 μs SIFS time 10 μs DIFS time 50 μs MAC processing delay 0 μs Cwmin 31 Cwmax 1023
Routing Protocol Parameters	Given in Chapter 4

Table 1. System Parameters

3.10.1 Number of Source Nodes	5,10 and 15 nodes
3.10.2 Load Introduced	32 Kbps for the online period of a typical source node generated by a constant distribution with 20 msec. mean. Exponentially distributed ON and OFF periods with means of 1.0 and 1.35 seconds respectively.
Routing Protocols	1. AODV 2. RTRP

Table 2. Workload Characteristics

3.11 Summary

This chapter presents the methodology used in this research. Section 3.2 gives the system boundaries and the objectives. System services and performance metrics are given in sections 3.3 and 3.4 respectively. In section 3.5, system and workload parameters are given, followed by system factors in section 3.6. The evaluation technique is given in 3.7. The workload characteristics are defined in section 3.8. Finally the design of experiments is given in 3.9.

4 DESCRIPTION OF IMPLEMENTED MODELS

4.1 Introduction

This chapter presents an overview of the IEEE 802.11b Wireless LAN protocol and the changes that were made to it. More detailed information on this MAC protocol can be found in [IEEE99]. Following this short description, the AODV implementation and RTRP implementation have been given. The model validations are given in Appendix A. Additionally, the routing parameters that are used in the simulation runs are presented.

4.2 802.11b Medium Access Control Layer Operation

4.2.1 Basic Operation

The basic channel access technique that is specified in 802.11b is the Distributed Coordination Function (DCF), a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) technique. This coordination function is the only coordination function that needs to be implemented in Independent Basic Service Sets (IBSS), in other words, ad hoc networks. Before looking at how the access mechanism works, a brief description of the timing intervals is given.

The 802.11 DCF implements three different time intervals for frame exchanges. The first one is called Short Inter-Frame Spacing (SIFS), the shortest time period used in this DCF. SIFS is used between the transmissions of frames when two nodes are in a frame exchange sequence. The second one is named as Distributed Inter Frame Spacing (DIFS). DIFS period is longer than SIFS and is used when a node is trying to start a frame exchange sequence or after unsuccessful transmissions. The last and the longest time interval is the Extended Inter Frame Space (EIFS). EIFS is used instead of DIFS when the station senses a collision on the channel.

Another feature of the 802.11b is the introduction of a virtual carrier sensing mechanism, named the Network Allocation Vector (NAV). The NAV is used as an additional way of sensing the channel in addition to the physical carrier sensing. When a node needs to access the channel, both mechanisms must indicate the channel is empty before the transmission can start.

To avoid a problem known as the hidden terminal problem, 802.11 DCF introduces RTS/CTS packet exchange sequence before transmission of any data packet. The RTS/CTS packets carry the information about the duration needed to transmit the upcoming data packets. The nodes that receive either RTS or CTS packets use this duration information to track channel allocation by updating their NAVs. The protocol does not mandate the use of this packet exchange. That is, it can be used for each packet or not, or a threshold may be set to use RTS/CTS exchange for larger packets.

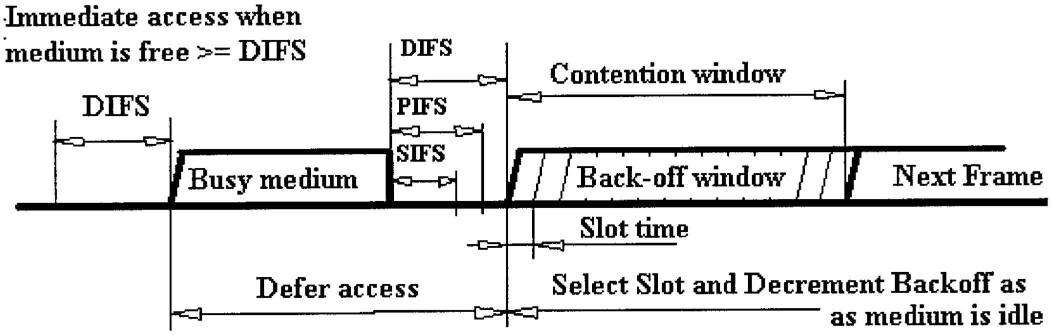


Figure 6. Basic Medium Access Scheme

The operation of the DCF access procedure is given in figure 6. When a node has a packet to transmit, it first senses the channel both physically and virtually. The channel is physically idle if there is no station transmitting at that time. The channel is virtually idle if NAV does not indicate that the channel is reserved for any other node. If the channel is determined to be idle using both mechanisms, the node waits for DIFS period before accessing the channel. If the channel stays idle for this period, then the source node sends an RTS packet to the destination, if this feature is enabled.

If the channel becomes busy within this DIFS time, or if it was already busy, the node must defer until the medium becomes idle. To defer, it calls the back-off procedure and waits for a time period determined by the back-off procedure. A random number of slots are specified by this procedure depending on the number of the transmission attempts for the current packet. A back-off timer is set to this value and the timer is decremented by one for each slot that the channel stays idle. However, if there is any activity in the channel within a time slot, then the back-off timer is suspended and is not decremented for that slot. When the back-off timer expires, the node is allowed to transmit.

If the transmission is unsuccessful at the end of the back-off, the node waits for DIFS period and another random back-off time is selected within the exponentially increased range of contention window value.

When the RTS packet is transmitted successfully, the receiving node is expected to send a CTS packet after a SIFS period of time. CTS frame is sent only if the receiving node's NAV value indicates that the channel is idle. Otherwise, the recipient should not send CTS frame. If the source node does not receive CTS frame before its timer expires, then it assumes that the transmission is unsuccessful and call its back-off procedure for a retransmission attempt if the retransmission limit is not reached. If the source node receives the CTS packet, it sends the data packet after a SIFS period. The destination node will send an ACK packet to indicate the reception of the data packet.

Neighboring nodes that hear the RTS or CTS frames update their NAV values after the successful reception of these frames. In Figure 7, the operation of the NAV is presented. The nodes that are represented by "other" in the figure are neighboring nodes that hear either the RTS or the CTS frames. The NAV value above the "other" line belongs to nodes that hear the RTS packet, and the NAV value below the "other" line represents the NAV values of the nodes that receive CTS packet. NAV values are only updated if the new NAV value is greater than the existing one and the frame's recipient address is not the node itself. The following figure gives the operation of the NAV value.

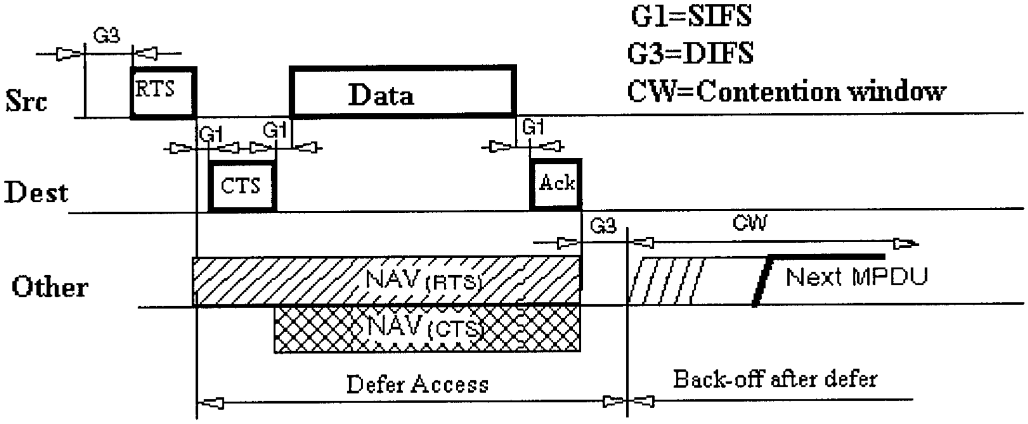


Figure 7. The Management of the NAV Value

4.2.2 Implementation Details

The 802.11b model provided within the standard OPNET models is used. This model provides the basic access technique that is described in the protocol. Additionally, this model also supports the fragmentation and defragmentation of data packets. Since this research is not focused on the performance of the MAC layer, the fragmentation feature of the model is disabled.

A link failure notification feature is added to the MAC layer to provide feedback to the routing protocol. That is, when the MAC layer reaches the retransmission limit for a packet, it notifies the network layer before dropping the packet.

Furthermore, packets that are sent from the network layer are prioritized in the queue before transmission attempts. Routing packets are given higher priority than data packets to minimize the delays that are associated with the route discovery process.

The MAC model that is used in the RTRP node model has the added feature of dropping aged packets before the transmission is started. When a node gains access to the channel, the deadlines of data packets are checked to see whether they have been exceeded or not. If the deadlines have been exceeded, the MAC layer discards the packet. Otherwise, the transmission is started.

The standard model that is supplied with OPNET only sends a packet to the upper layer if its destination is that station. This has been changed for this research. The MAC layer sends all data packets (routing packets are also considered as data packets by the MAC layer) to the upper layer regardless of their destination. The routing protocols use this feature to update or create the routes as described in the following section.

4.3 Implementation of AODV

4.3.1 Routing Parameters

AODV has been implemented in accordance with the specifications of the protocol given in [PRD00]. This reference is a draft in progress. As a result, future specifications of this routing protocol may be different than the version used in this research.

There are many parameters that may affect the performance of the routing protocol. The major parameters that are used in this research for AODV are:

- **Active Route Time Out:** This parameter is used to determine the time that a route expires. When a new route is created or a route is used for forwarding data, the end of life for that route is set to current time plus active route time out. It is set to 3 seconds.
- **Broadcast Record Time:** When a broadcast packet is received for the first time, it is recorded to broadcast record list and the record is kept until current time plus broadcast record time. If any other copies of this packet are received, then the time is updated in the same manner. Its value for this research is 2 seconds.
- **Net Diameter:** This number determines the maximum number of hops that a route can have. It is set to 10 for this research.
- **Node Traversal Time:** This is a conservative estimate of the traversal time of single hop. It includes the queuing delay, medium access delay at MAC, transmission and propagation delays, and processing delay. It is set to 2 msec.
- **RREQ Retries:** This is the maximum number of retries for broadcasting RREQS to establish a route. Its value is set to 6.

- **TTL Start, TTL Increment, TTL Threshold:** The AODV model used in this research uses an expanding ring search technique to avoid flooding the network by RREQ packets. The TTL field of the RREQ packet is set to current time + TTL Start * 2 * Node Traversal Time when it is transmitted for the first time. For retransmission attempts, this field is set to current time + (TTL Start + number of retires + TTL Increment) * 2 * node traversal time. If the TTL threshold is reached, then the node uses current time + TTL Threshold * 2 * Node Traversal time. The values for TTL start, TTL increment and TTL Threshold are 3, 2, and 7 respectively.

4.3.2 Operation of the Protocol Model

When a data packet is received from the upper layer, the model first checks its route table to see if there is a route to this destination. If there is a route that is active, the packet is forwarded using this route. On the other hand, if there is no route to the destination, or the route is no longer active, the protocol broadcasts a RREQ message and sets the destination address as broadcast address (defined as –9999 in the model).

When a node receives a packet, the first thing it does is check the type of the packet and extracts the appropriate fields from the packet. Next, the routing protocol creates or updates reverse routes to the source node of the packet, as well as to the transmitting station if it is different than the source node. This procedure is applied to all packets that are forwarded by the lower layer regardless of the destination address. If the node has sent any RREQ packets for routes to the source and the transmitting stations, the protocol model avoids further retransmissions. Furthermore, if there are any data packets waiting for a route discovery, they are also checked and data packets that are waiting for this source and transmitting nodes are sent to MAC layer for transmission.

After creating or updating the routes to the source and transmitting nodes, the packet is processed only if it is a broadcast packet or is sent to this node. For the RREQ packets, the time-to-live (TTL) field of the packet is checked to see if the packet has exceeded its TTL. If the packet has not exceeded this limit and is received for the first time, the node checks if it has a route to the destination or the destination is itself. In either case, the protocol model creates a RREP and unicasts it (sets the recipient address) to the node the packet was received from. Also, the RREQ packet's source address and broadcast ID is recorded in a list to avoid processing multiple copies of the packet.

If there is no route to the destination, the RREQ packet is broadcasted if the TTL is not exceeded. The node sets the transmitting address to its node address and increases the hop count field by one before transmission.

If the received packet is a RERR packet, the node updates the routes to each of the unreachable destinations listed in the RERR packet. If any of these routes has a precursor node that forwards packets using this route, this node also creates a RERR packet and broadcasts this packet after placing the unreachable destinations that have precursors.

When a node receives a RREP packet, the node consults its route table and forwards the packet using the route to the source address. If the node itself is the source, it simply destroys the packet since the route to the destination is already created when the packet is received.

If a node receives a data packet whose destination is not itself, it forwards the packet using the route to the destination. If there is no route to the destination, the node creates a RERR and broadcasts it after putting the destination address of the data packet in the RERR packet as unreachable. If it is the destination, then the packet is forwarded to higher layers.

When the protocol receives a notification from the MAC layer, it updates the route to the destination node as invalid. If there are any nodes that are using this route for forwarding packets, the node creates a RERR and broadcasts this packet after setting the destination address as unreachable.

The AODV specification given in [PRD00] proposes some additional mechanisms such as local repair and mechanisms for maintaining local connectivity. These two mechanisms are not implemented for the purposes of this research.

4.4 Implementation Of RTRP

RTRP has been built taking AODV as a point of departure. The basic mechanisms and packets formats between AODV and RTRP are similar. However, the following changes have been made to compensate for the time-sensitive data in RTRP.

The RREQ packet format that is used in RTRP is similar to that of AODV. The AODV RREQ packet format includes only source and the transmitting address of the packet. When an intermediate node receives a RREQ packet, it creates reverse routes to the source and the transmitting nodes only. This has been changed in RTRP. In RTRP, RREQ packets include the addresses and the sequence numbers of all the nodes that a RREQ packet travels through. As a result, a node receiving a RREQ packet can create routes to all the nodes between itself and the source node. This will increase the benefit that is gained from the RREQ packets. When a node creates a RREQ packet, it puts its address, sequence number, and hop count in the packet. The next node receiving this packet extracts this information, and creates a reverse route. If this node needs to rebroadcast this packet, it increases the hop count of source node by one, adds its address, sequence number and hop count to the packet. This continues until the packet reaches the destination.

The RREP packets also have the feature described above. When a destination (or a node with a fresh route to the destination) creates a RREP packet, the node addresses and the sequence numbers are placed in the RREP along with the hop counts by each node on the way back to the source.

The most prominent change that is made to the RTRP is the deadline check of the data packets in three places. In any of these checks, if the data packet is found to exceed the deadline, it is dropped and the missed deadline statistics is updated. When a node receives a data packet from the upper layers, the packet is forwarded to lower layers if a route to the destination exists. If there is no route to the destination, then the packet is queued and a route discovery sequence is initiated. When a route is discovered, the data packets that are waiting for this route are extracted and their deadlines are checked against the current time. This is the first place that stale packets are dropped. The second check is done when the packet is in MAC layer and the packet is removed from the queue for transmission. Finally, the receiving nodes check packet deadlines before processing them. The deadlines are set to be 200 milliseconds for all the simulation runs.

5 SIMULATION RESULTS

5.1 Overview

This chapter presents results obtained from the simulation runs. The simulation results are organized based on the performance metrics. The confidence intervals that are given for the results are for a 90% confidence level throughout this chapter. Section 5.2 gives the simulation results for packet delivery fraction. Section 5.3 gives results for missed deadline fraction. Section 5.4 gives the results for routing overhead. The results for mean ETE delay are given in Section 5.5. Finally, results are summarized in section 5.6.

For packet delivery ratio, the number of source nodes is the primary factor that explains the major amount of the variation by 84%. This can be observed from the graphics that presents the packet delivery fraction results for 5, 10 and 15 nodes. This is not an unexpected situation since by increasing the number of source nodes, the load that is introduced to the network is also increased. Additionally, an increase in the number of sources means an increase in the number of channel attempts, which results in more collisions and delays in the wireless medium.

For the missed deadline fraction, number of sources is still the primary factor that affects the outputs with a percentage of 38%. The second important factor is the routing protocols with an explained percentage of 28%. The effect of the number of sources is obvious because of the reasons listed above. The effect of the routing protocols, however, is due to the fact that RTRP drops the aged packets en-route where AODV transports these packets regardless of their deadlines. This feature of RTRP accounts for a less busy wireless medium, thus resulting in lower missed deadline ratio than AODV.

For routing overhead, the most important factor that affects the results obtained is the number of source nodes with a percentage of about 77%. Routing protocols, on the other hand, account for only the 6% of the variation. Combined with the number of source nodes, routing protocols account for another 10% of the variation.

For mean ETE delay, the percentages of the variation explained are not different much than the other factors. Number of source nodes accounts for approximately 70% of the variation. Routing protocols explains the 14% where node speeds accounts for a percentage of less than 1%. Combined with the number of sources, routing protocols account for another 8 percent of the variation.

It is clear that the number of source nodes is the most prominent factor that affects the performance of the networks. This is not very surprising since the number of source nodes also represents the load that is increased to the network. Each source node introduces the network an average 32 Kbps load. With 5, 10, and 15 sources, the load that is introduced to the network is about 160 Kbps, 320 Kbps, and 480 Kbps respectively for the time periods that all nodes are in ON state. It should be noted that this is only the user data that is introduced to the network. Considering that most of the routes in the network have more than two hops, the actual load that is introduced to the wireless medium as user data is higher than this amount. In addition to the data packets introduced to the network, a total of three packets, an RTS, CTS, and an ACK are transmitted for each one of the data packets for every hop due to the properties of the 802.11 protocol. Furthermore, for scenarios where the node mobility is relatively higher, the routing packets consume a significant amount of bandwidth, making the medium even more congested. These details make it clear why the number of source nodes accounts for most of the variation in the results.

The following sections summarize the results for each factor individually.

5.2 Packet Delivery Fraction

5.2.1 5 Sources

Packet delivery fractions for 5 source nodes are summarized in Figure 8. For lightly loaded networks, packet delivery fractions of both of the protocols are close to each other. When the node speeds are increased, these fractions tend to decrease slightly. The major decrease in the packet delivery fraction is when the node speeds are increased to 32 km/h from 7.2 km/h for both protocols. RTRP tends to deliver packets with a slightly higher ratio at all three speeds. However, there is not a significant difference to reach to a conclusion.

When the nodes are set to slower speeds, AODV provides a packet delivery fraction between 0.9809 and 0.9873 with a mean of 0.9841 with 90% confidence interval. RTRP, on the other hand, provides a packet delivery fraction between 0.988 and 0.995 with a mean of 0.9914 with the same confidence interval.

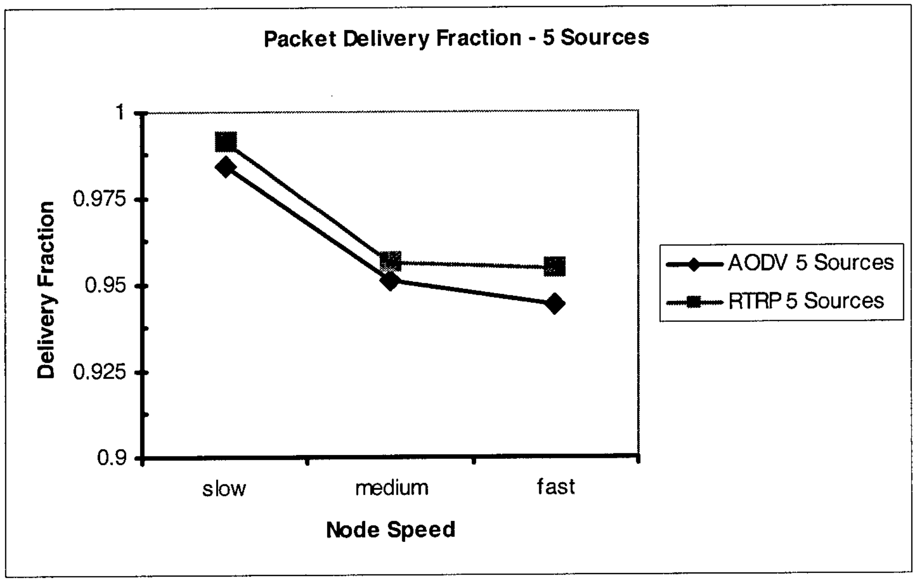


Figure 8. Packet Delivery Fraction for 5 Sources

5.2.2 10 Sources

Figure 9 gives the packet delivery fraction for 10 source nodes for both protocols. When compared to the 5 sources, packet delivery fraction decreases significantly for 10 source nodes for both protocols. Both protocols deliver approximately the same amount of packets when the node speeds are set to slow. However, RTRP's packet delivery ratio increases significantly when the node speeds are increased to 36 km/h.

When the node speeds are increased to 72 km/h, packet delivery fractions continue to decrease slightly. AODV tends to have a higher packet delivery fraction than RTRP when the node speeds are 72 km/h. However, the difference is not significant to reach a conclusion.

For 10 source nodes at slow speed, AODV provides a packet delivery fraction between 0.7983 and 0.9221 with a mean of 0.8602 where RTRP provides a mean ratio between 0.8575 and 0.9560 with a mean of 0.9067. For medium speed, these intervals become 0.5654 and 0.7498 with a mean of 0.6576 for AODV and 0.9882 and 0.9925 with a mean of 0.9903 for RTRP. Finally, AODV provides a delivery ratio between 0.5243 and 0.7292 with a mean of 0.6267 where RTRP gives a confidence interval of 0.5248 and 0.6136 with a mean of 0.5692.

For 10 source nodes, the protocols give close results for packet delivery fraction except 10 sources. The increase in RTRP's packet delivery fraction for 10 source nodes, on the other hand, is due to the trajectory patterns that are used in these experiments. For a larger number of samples with different trajectory sets, the packet delivery fraction results are expected to have less difference for protocols.

The similarity among the results of the protocols for 10 source nodes is not unexpected. RTRP has the same basic mechanisms that AODV has for establishing and maintaining the routes. The differences between the protocols, however, are most obvious for the experiments where the number of source nodes is set to 15. These results are presented in the next Section.

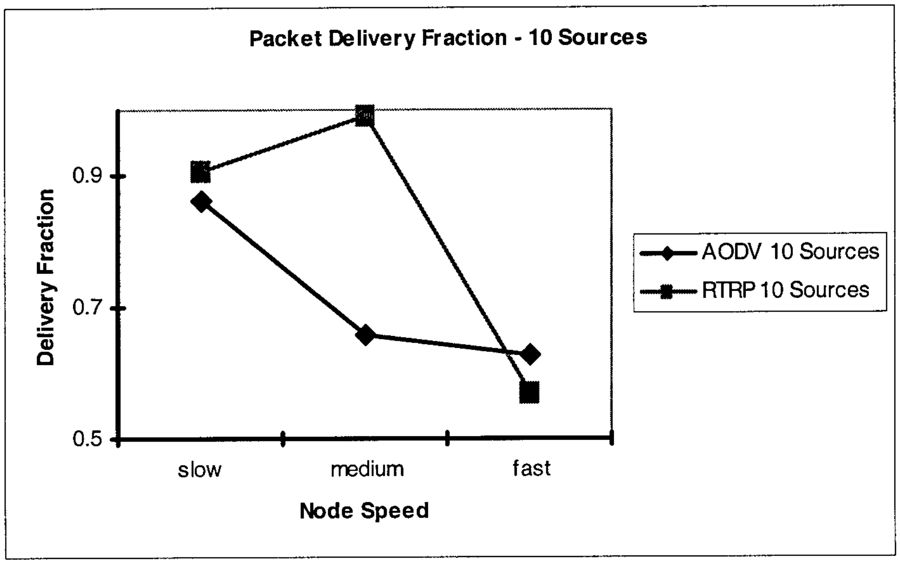


Figure 9. Packet Delivery Fraction for 10 Sources

5.2.3 15 Sources

Figure 10 summarizes the packet delivery fraction for 15 source nodes. When the number of sources is increased to 15 sources, RTRP begins to significantly outperform AODV in packet delivery fraction significantly. The node speeds are not as significant as they are in 5 and 10 source nodes for 15 sources. RTRP has a delivery ratio of more than 200% compared to AODV at all speeds.

For slow node speeds, AODV has a 90% confidence interval of 0.1088 to 0.1658 with a mean of 0.1373 and RTRP has a 90%confidence interval of 0.3338 to 0.4509 with a mean of 0.3924. For medium speeds, these intervals become 0.0740 to 0.16 27 for AODV and 0.3488 to 0.5033 for RTRP. Finally, for 15 sources 0.081 to 0.1097 confidence interval for AODV and 0.3697 to 0.3990 for RTRP are observed.

As it is clear from the results, when the network begins to get congested, the optimizations done to RTRP begin to create a difference in the packet delivery ratio.

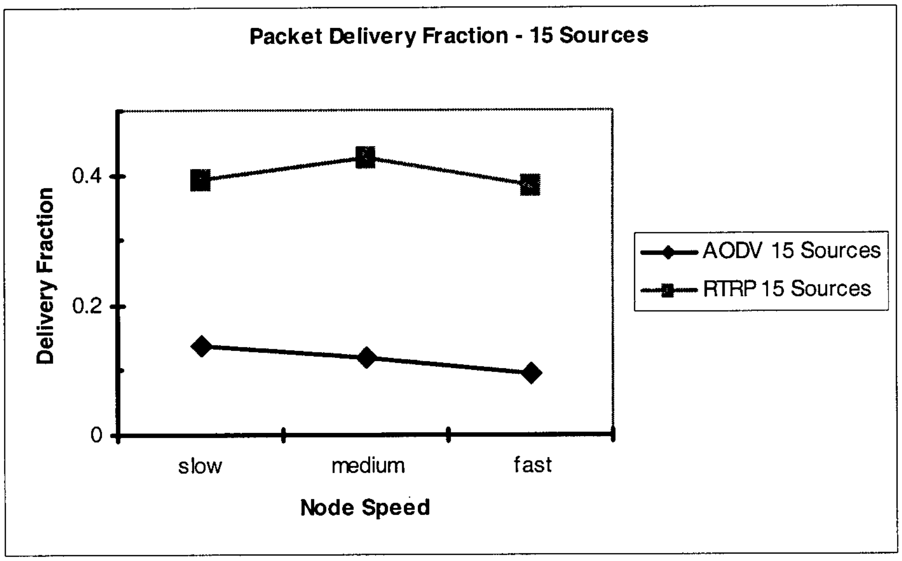


Figure 10. Packet Delivery Fraction for 15 Sources

5.3 Missed Deadline Fraction

Missed deadline fraction and the packet delivery fractions seem to be two factors that sum up to 1. This would be the case if the network layer was the only layer that the packets are dropped. In this research, however, this is not the case. In addition to the packet losses in the network layer, the MAC layer and the physical layer are the other two layers that the packets are dropped. As a result, for the purposes of this research, the missed deadline fraction represents the ratio of the packets that are dropped or discarded by network layer due to the missed deadlines.

5.3.1 5 Sources

Missed deadline fractions are summarized in Figure 11 for 5 sources. Since almost all of the packets are delivered to their destinations with 5 sources, missed deadline fraction tends to be very small for 5 sources, less than 1% at all cases. When the node speed is set to 72 km/h, AODV tends to deliver packets after the deadline slightly. However, there is not a significant difference between the protocols for 5 source nodes as it can be observed from Figure 10.

5.3.2 10 Sources

Figure 12 gives the missed deadline fraction for the routing protocols for 10 source nodes. When the node speeds are 7.2 km/h, missed deadline ratio is almost the same between the protocols. However, when the node speeds are increased to 32 km/h and later to 72 km/h, RTRP tends to have a lower missed deadline ratio than AODV. This observation points out to the fact that RTRP is losing more packets than AODV in lower layers due to collisions or retransmission limits with 10 sources and when the mobility is higher.

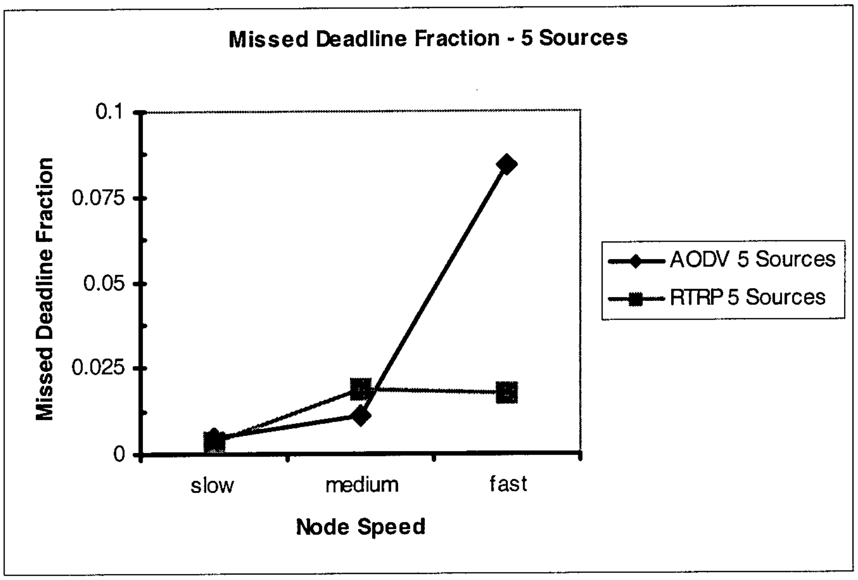


Figure 11. Missed Deadline Fractions for 5 Sources

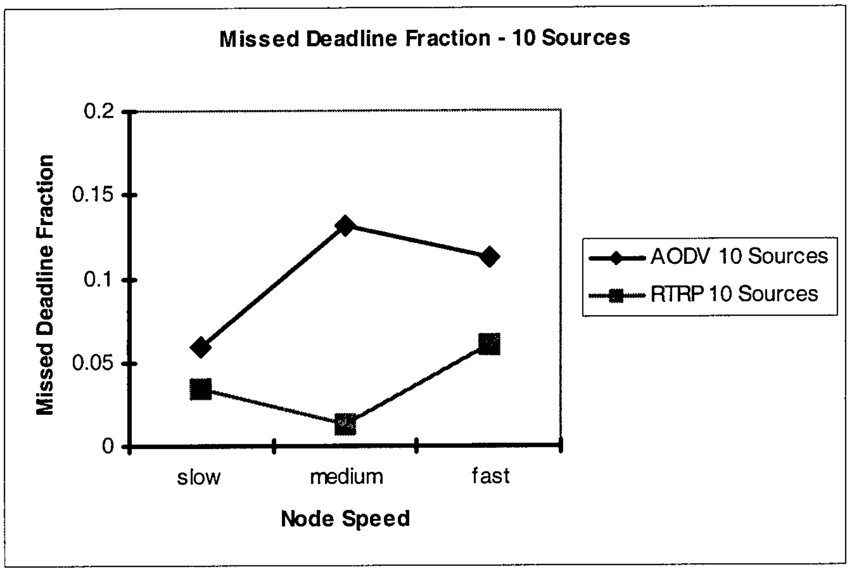


Figure 12. Missed Deadline Fraction for 10 Source Nodes

When the node speeds are set to 7.2 km/h, AODV has a missed deadline fraction with a mean of 0.05913 where RTRP has a mean missed deadline fraction of 0.0343. The difference between the routing protocols increases when the node speeds are increased to 32 km/h. At this speed, AODV has a mean of 0.1317 and RTRP has a mean of 0.0132. Finally, the difference decreases when the node speed is set to 72 km/h where AODV has a mean missed deadline fraction of 0.1129 and RTRP has a mean fraction of 0.0606.

5.3.3 15 Sources

Missed deadline fraction is summarized in Figure 13 for 15 sources scenario. AODV has a significantly higher missed deadline fraction than RTRP when the source nodes are increased to a total of 15. This is due to the fact that RTRP drops the aged packets en-route to their destination, decreasing the load significantly where AODV delivers the packets to the destinations regardless of the deadlines. As a result, RTRP has a lower fraction than AODV. It should be noted that when the packet delivery fraction and the missed deadline fraction are examined together, AODV is losing more packets in lower layers than RTRP due to the collisions occurring in the busier wireless medium

For slow speeds the difference between the protocols is at maximum for 15 source nodes. AODV has a mean missed deadline fraction of 0.3041 where RTRP has a mean of 0.0514. Form medium speed, AODV has a mean of 0.2274 where RTRP has a mean of 0.0628. Finally, for node speeds around 72 km/h, AODV has a missed deadline of 01989 and RTRP has a mean of 0.0527.

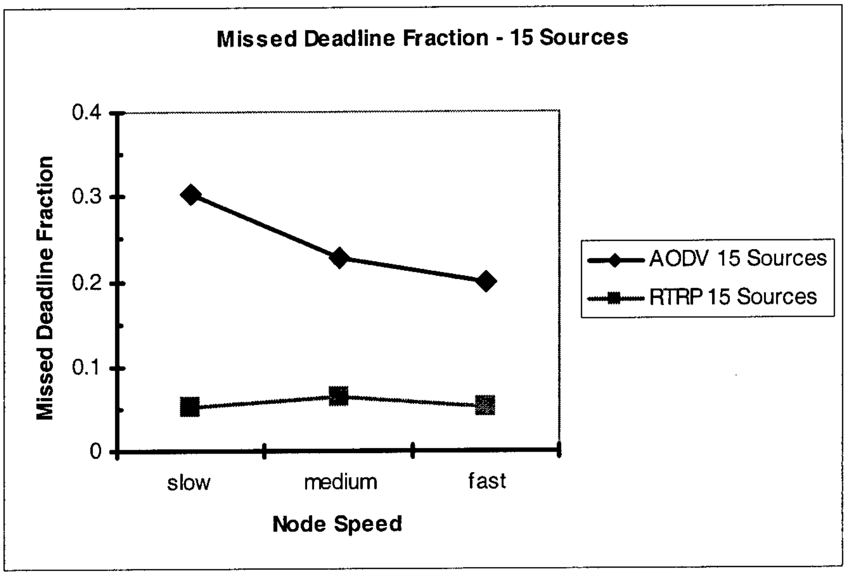


Figure 13. Missed Deadline Fraction for 15 Sources

5.4 Routing Overhead

5.4.1 5 Sources

Routing overhead is given for 5 sources in Figure 14. Since the nodes are almost stationary for slow speeds, the routing overhead is relatively less than higher speeds. For 7.2 km/h, AODV has a mean overhead of 0.4021 where RTRP has a mean overhead of 0.3421. When the node speeds are increased to 36 km/h, the increment in the overhead is has a steeper angle than the increment from 36 km/h to 72 km/h. This is expected because the increment in the speed of the nodes is 5 times from slow to medium and 2 times from medium to fast. RTRP has a slightly lower routing overhead than AODV due to the fact that RTRP RREQ and RREP packets carry the addresses of all the nodes that they travel through where these packets in AODV carry only the addresses of the source and the transmitting stations' addresses.

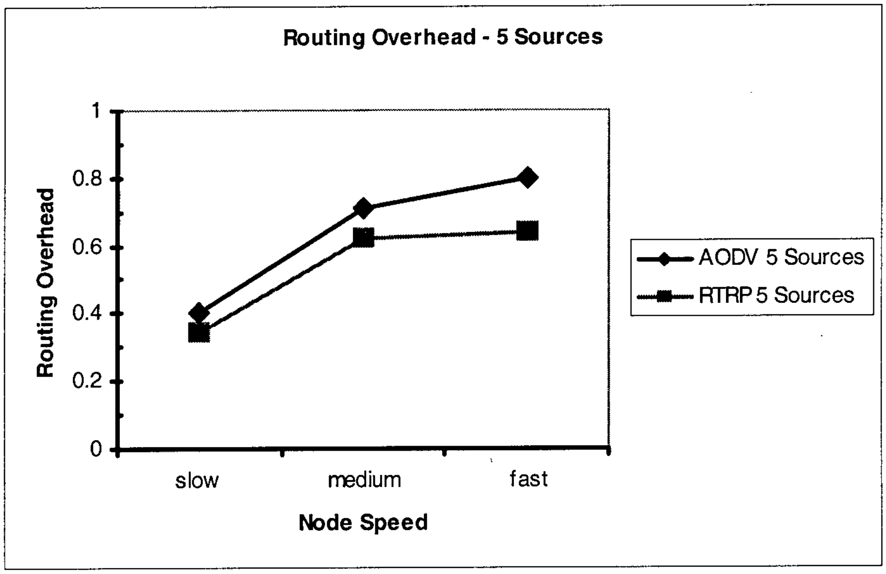


Figure 14. Routing Overheads for 5 Source Nodes

5.4.2 10 Sources

Routing Overhead is given in Figure 15 for 10 source nodes. When the nodes are set to a slow speed, both protocols tend to have a routing overhead around 0.8 , with AODV having slightly higher routing overhead than RTRP. When the node speeds are increased, routing overhead for RTRP reaches to a value of 2.8, and the routing overhead for AODV reaches to a value of 2 for 72 km/h.

AODV has a lower routing overhead than RTRP for the node speeds around 72 km/h. This result is an unexpected result since RTRP outperforms AODV much or less in every other experiment. However, for mobile nodes, the trajectories of the nodes also play a major role on the reception of the nodes. As a result, it is estimated that these results are because of the trajectories of the nodes, and increasing the sample size should result in similar ratios between overhead fractions to results of other experiments.

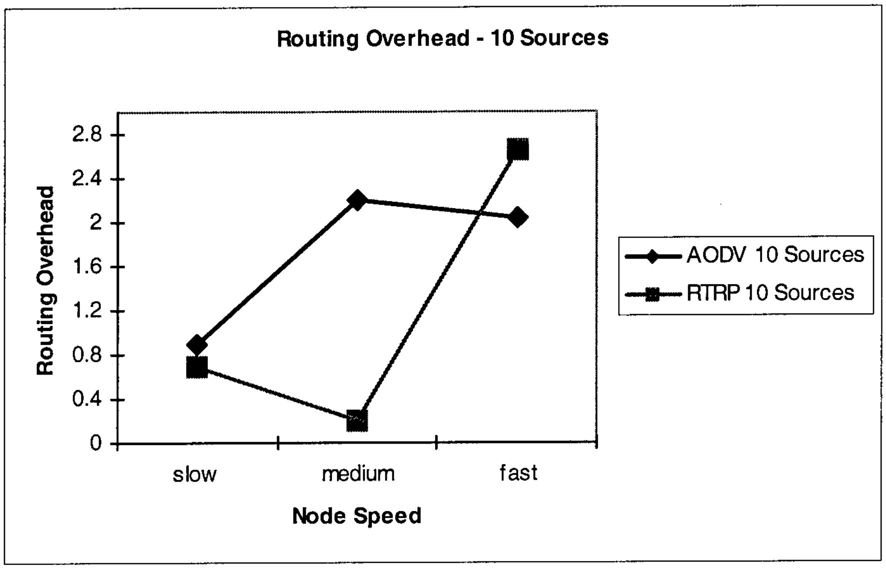


Figure 15. Routing Overhead for 10 Source Nodes

5.4.3 15 Sources

Figure 16 summarizes the routing overhead for the protocols with 15 sources. As shown in the Figure 15, AODV has a significantly higher routing overhead than RTRP between 2 to 3 three times for all three speeds. This is an expected result. Since RTRP drops aged packets en-route to their destinations, the wireless medium is not congested with aged packets as it is in AODV. As a result, the routing packets are propagated through the network more easily than they are propagated in AODV.

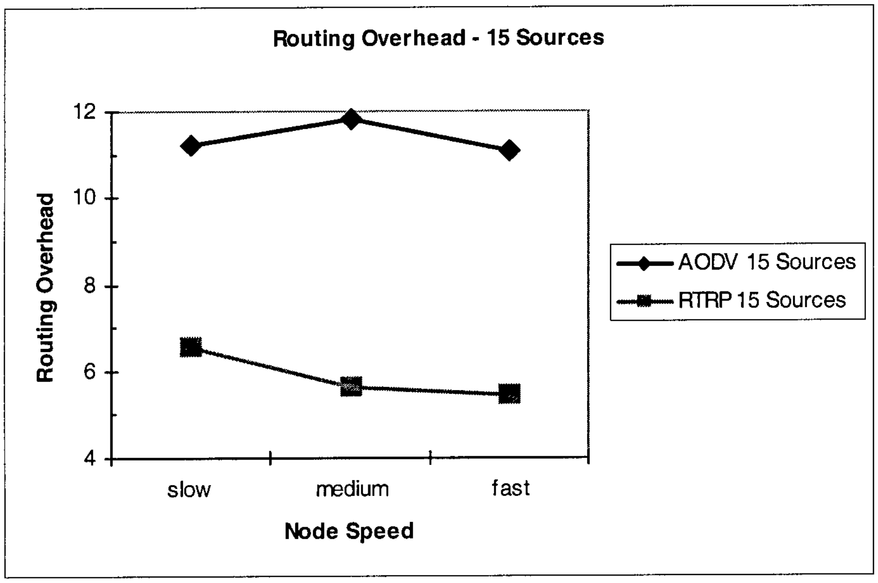


Figure 16. Routing Overhead for 15 Sources

5.5 Average ETE Delay

The mean ETE delay does not imply a lot about the performances the routing protocols as stated earlier. However, the results are given in order to have the ability to compare the results with other protocols.

Average ETE delay is given in Figure 17 for the protocols for 5 sources. This metric does not represent much about the performances of the protocols since the deadline cannot be exceeded as the average ETE delay. For 5 sources, both of the protocols have very low ETE delay which are not significantly different than each other. The mean ETE delays average around 5 msec. for both protocols.

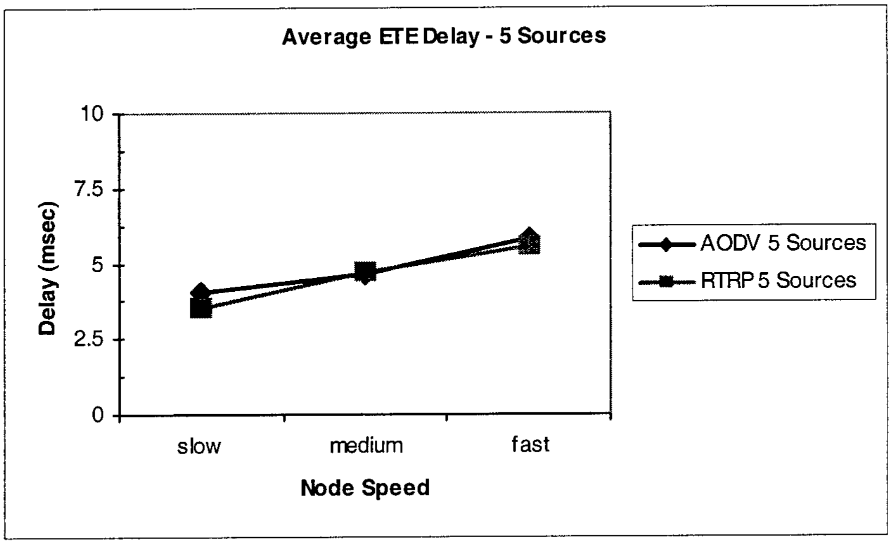


Figure 17. Average ETE Delay for 5 source Nodes

The ETE delay for 10 source nodes are given in Figure 18. The mean ETE delays increases for both protocols when the source number is increased from 5 to 10. AODV has a slightly higher ETE delay than RTRP for all experiments with 10 source nodes. However, the difference is not significant enough to claim that one protocol outperforms the other. For 10 source nodes, the speeds of the nodes do not affect the ETE delay significantly.

The average ETE delay is given in Figure 19 for 15 sources. RTRP has a lower delay than AODV as in other experiments with different speeds. For 15 sources, again, the node speeds does not play a significant role and explains less than 1% of the variation in ANOVA tables.

The reason for having such low ETE delays is the network diameter. With all the nodes scattered in a 900 m x 1500 m area, the routes are relatively short. Also, having a relatively small network limits the number of hops that a route can have to a maximum of 5. As a result ,the queuing (medium access) and transmission delays are relatively small.

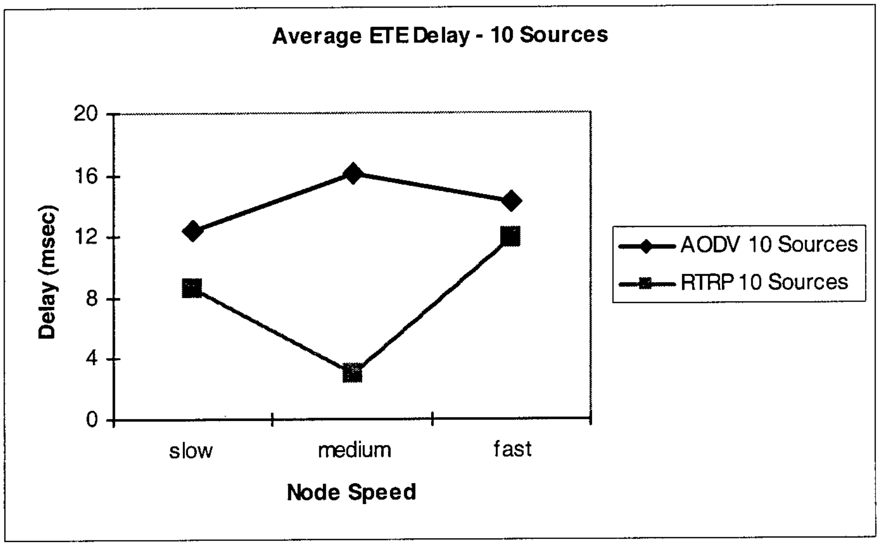


Figure 18. Average ETE Delay for 10 Sources

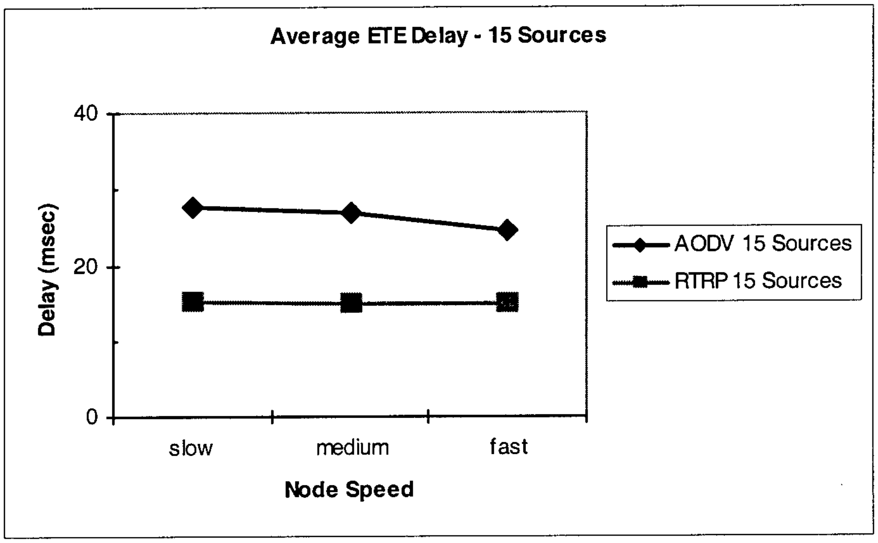


Figure 19. Average ETE Delay for 15 Sources

5.6 Summary

Due to the fact that RTRP has basic mechanisms in common with AODV, AODV and RTRP do not have significant differences when the number of nodes in the network is low. However, when the number of source nodes increases, RTRP's packet delivery fraction tends to be higher than AODV due to the fact that RTRP drops the aged packets en-route, easing the load on the wireless medium.

When the number of source nodes is low and the node speeds are also slow, RTRP and AODV have approximately the same routing overheads. However, the routing overhead remains lower for RTRP for higher source number scenarios. When the network starts to get congested, AODV's routing overhead increases significantly. This is because of the fact that AODV tries to route the aged packets to their destinations where RTRP drops these packets on the intermediate nodes. Since the RREQ packets have their TTL fields set, these packets also get aged, and are not propagated in the network, similar to RREQ packets in RTRP. This leads to more retries for route discoveries as well as more routing packets broadcast for AODV. Another reason for the difference in the routing overheads is the fact that RTRP RREQ and RREP packets carry more information than the RREQ and RREP packets in AODV, affecting the number of routing packets needed.

As a summary, it can be stated that RTRP has better performance for higher load situations than AODV.

6 SUMMARY AND RECOMMANDATIONS

This research has focused on the routing process in ad hoc networks. The selected workload was time-sensitive data. Taking into account the deadline characteristic of time-sensitive data, a routing protocol has been developed, named RTRP taking AODV as the point of departure.

Simulation results showed that, for lower network loads, the routing protocols performed similarly, although RTRP had slightly better performance than AODV in most experiments. However, when the network load was increased, AODV began to perform significantly worse than RTRP. This is due to the fact that RTRP was designed to drop the aged packets en-route to the destination, whereas AODV tries to forward these packets regardless of their deadlines, congesting the medium with useless packets. Additionally, combined with the above, the design of RREQ and RREP packets in RTRP decreased the overhead associated with route discovery process, thus keeping the medium less busy and decreasing delays that are associated with route discovery.

6.1 Summary

Chapter 1 provided an explanation of the problem that was studied, and presented a brief overview of the objectives of this research and the document organization. In Chapter 2, different approaches that were taken in routing in ad hoc networks have been presented. Also in this Chapter, the benefits and disadvantages of the protocols having different philosophies have been given. Following, a comparison of these routing protocols presented.

In Chapter 3, the methodology that has been followed throughout the research has been provided. The details of the objectives, system boundaries, performance metrics, system factors, evaluation technique, workload characteristics and design of experiments were given in the subsections of this chapter.

Chapter 4 presented a brief overview of the 802.11 wireless LAN specification's DCF, the basic channel access mechanism. Following this description, the details of implementations of 802.11, AODV and RTRP were presented. The differences between AODV and RTRP and the services that were provided by 802.11 implementation were also discussed in this chapter. The link failure notification and RTS/CTS packet exchange sequence were presented among the services provided by 802.11. The aged packet discarding mechanism and differences in RREQ and RREP packets were given as the major differences between the routing protocols.

Chapter 5 presented results of the simulation runs. The results were organized under performance metrics and were briefly discussed in this chapter. Additionally, the reasons that lye behind the results were explored.

Chapter 6 gives a summary of the research done and the paper organization. Also in Section 6.2, future recommendations for the studies that will be done in the same research area have been given.

Finally, the appendices provide the results obtained from the simulation runs. In appendix A, validation of the models that were used in the simulations is presented. In appendix B, the results are presented in tabular form, among with the confidence intervals and ANOVA tables for the performance metrics.

6.2 Future Recommendations

This research has been accomplished using a relatively small network size. Also, the scenarios that the experimental design contained were limited due to many reasons. Taking these facts into account, the following are recommended as future research.

1. Increase the network size to observe the performance of the protocol in routing scenarios with relatively longer routes.
2. Study the performance of RTRP in the networks where telemetry data is used as the workload.
3. Study the performance of RTRP using different network topologies other than random trajectories.
4. Study the performance of RTRP without using RTS/CTS frame exchange feature of 802.11.

APPENDIX A. MODEL VALIDATION

This chapter presents the validation of the models. Section A1 gives the validation of 802.11 model. Section A2 presents the validation of AODV.

A.1. Validation of the 802.11 MAC Model

The model has been validated against the results given in [BFO96]. Figure 20 shows the saturation throughputs for the model developed and the results from [BFO96]. The model has been validated for 5, 10, 15 and 20 source nodes and for different contention window values. The differences between results are less than 3% for all the source nodes.

Figure 21 gives the throughputs of both the model and [BFO96] under different loads. The throughputs are measured for 5 and 10 source nodes only. The results are close to each other for 5 and 10 sources and the difference is less than 3% for both number of sources under different loading conditions.

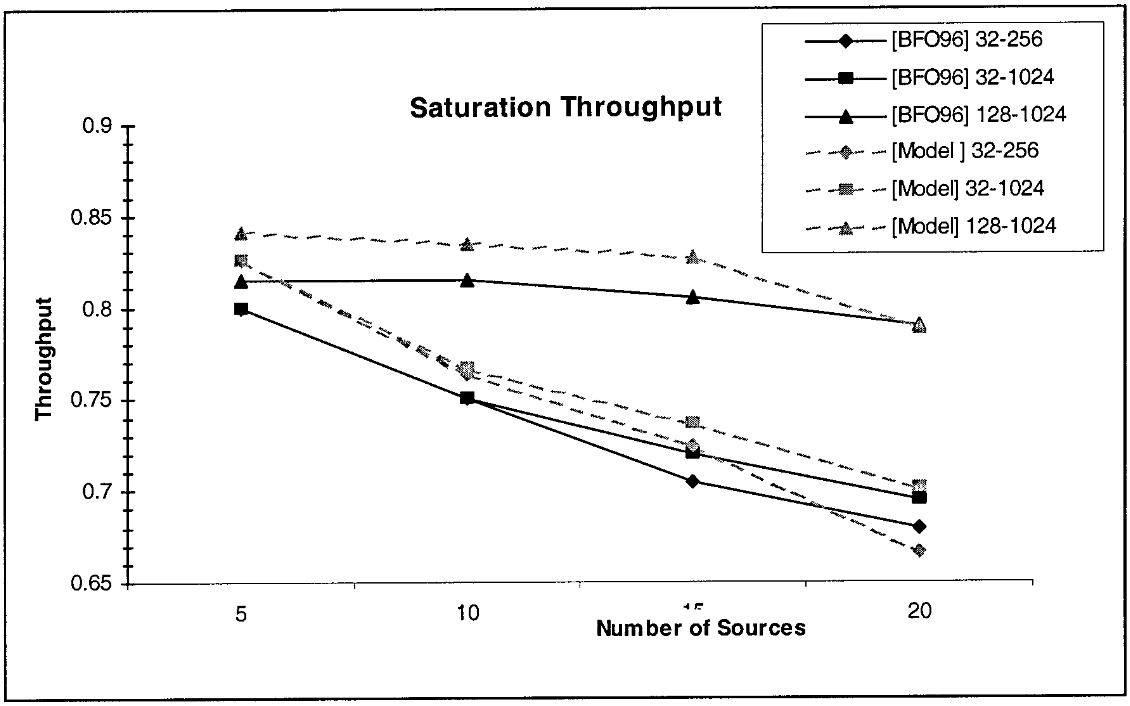


Figure 20. Saturation Throughputs of 802.11 Model and [BFO96]

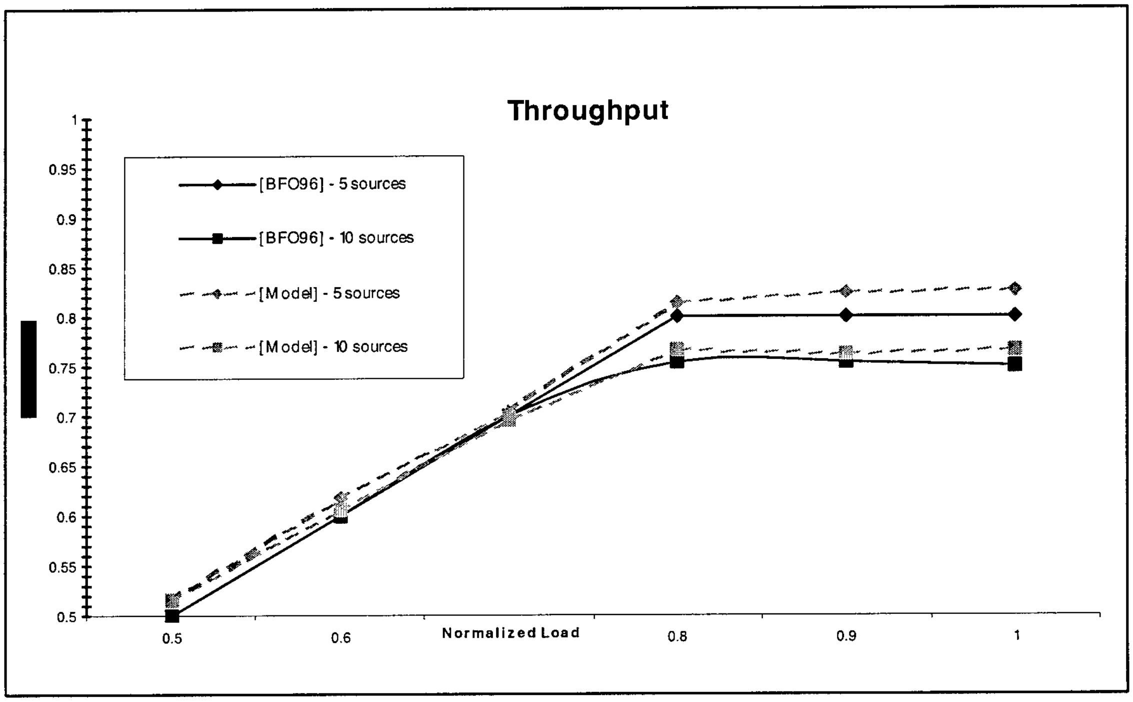


Figure 21. Load vs. Throughput

A.2. Validation of the AODV Model

The AODV model that is used in this research is validated using the results from [DPR00]. The validation has been accomplished for 10 and 20 sources. The node speeds are 0 km/h for stationary results and a random speed between 0 and 20 m/h for no pause results. The nodes do not pause once they reach a waypoint on their trajectories.

Figure 22 presents the packet delivery ratio for both the model developed and [DPR00]. When the number of sources is 10 and the nodes are stationary, both models deliver 100% of the packets without any loss. For 10 sources no pause scenario, the delivery ratios drop about 2% for the model and 3% for [DPR00]. However the difference between the models is not significant.

For 20 sources, the differences are still insignificant for both scenarios. The differences for packet delivery ratio do not exceed 2% for any scenarios validated.

Figure 23 gives the results for routing overheads for both the model and [DPR00]. For stationary scenarios, the routing overhead is close to zero. This is expected since once the routes are established, AODV does not play any role in forwarding process of the packets. Consequently, the routing overhead remains close to zero for both models.

A.3. Summary

This appendix presents the results of the validation of the models. Section A.1 gives the validation results for 802.11 model used in this research. Section A.2 presents the results of validation of AODV against the results presented in [DPR00].

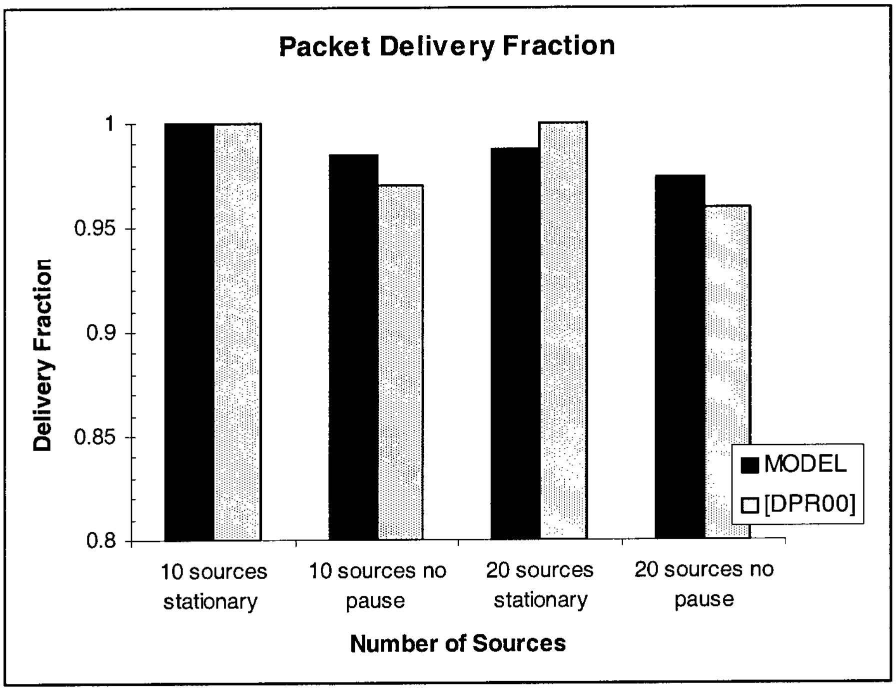


Figure 22. Packet Delivery Fraction for AODV Validation

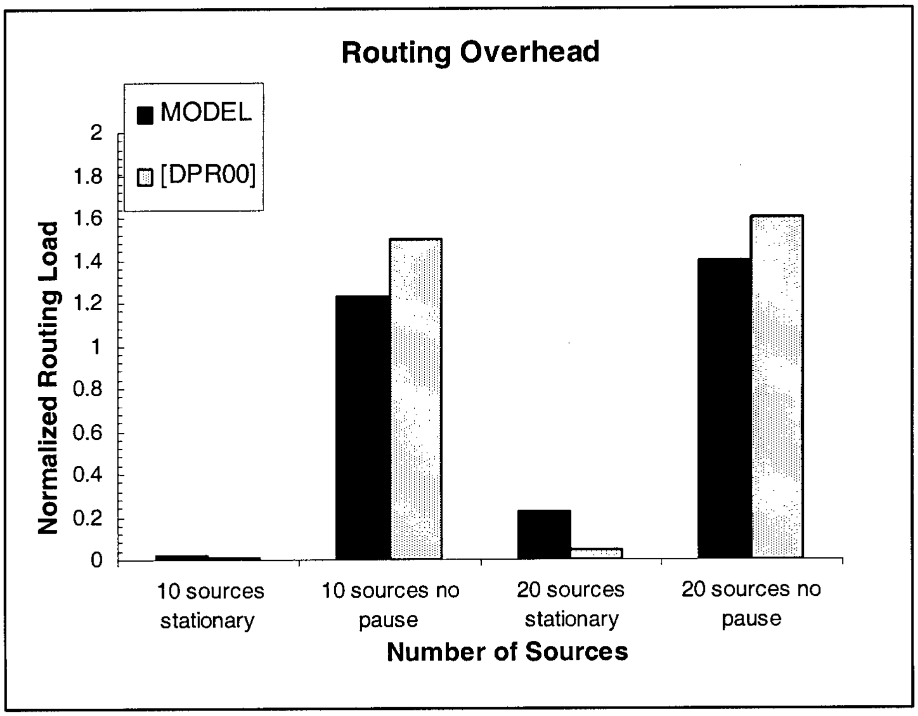


Figure 23. Routing Overheads for AODV Validation

APPENDIX B. SIMULATION RESULTS

This section presents the results obtained from simulation runs. Additionally, the ANOVA tables for the performance metrics are presented in this section.

B.1. Simulation Results

This section presents the results obtained from simulation runs. Each experiment is has three replications. The confidence intervals for the results of the experiments are also given following the table.

Packet Delivery Ratio							
	AODV			RTRP			
	slow	medium	fast	slow	medium	fast	yi...
5 Sources	0.9876	0.9588	0.9449	0.9879	0.9611	0.9556	17.3462
	0.9809	0.9479	0.9498	0.9912	0.9548	0.9519	
	0.9839	0.9463	0.9387	0.9951	0.9536	0.9562	
10 Sources	0.8473	0.547	0.7299	0.9406	0.9914	0.6176	13.8324
	0.8025	0.7286	0.6356	0.847	0.9877	0.5243	
	0.9309	0.6972	0.5147	0.9326	0.9919	0.5656	
15 Sources	0.1462	0.0781	0.1127	0.3507	0.5109	0.4018	4.6606
	0.1038	0.1696	0.0879	0.4632	0.4185	0.3788	
	0.1619	0.1074	0.0847	0.3632	0.3488	0.3724	
BC totals y.jk.	5.945	5.1809	4.9989	6.8715	7.1187	5.7242	35.8392
y.j..	16.1248			19.7144			

Table 3. Simulation Results for Packet Delivery Fraction

Level	STD DEV	90% CI	mean	upper bnd	lower bnd
1	0.925390645	0.878803076	8.05305	8.931853076	7.174246924
2	0.006802206	0.006459757	0.951	0.957459757	0.944540243
3	0.005562673	0.005282628	0.944466667	0.949749294	0.939184039
4	0.003604164	0.003422717	0.9914	0.994822717	0.987977283
5	0.004028647	0.00382583	0.9565	0.96032583	0.95267417
6	0.002328805	0.002211565	0.954566667	0.956778231	0.952355102
7	0.065169727	0.061888843	0.860233333	0.922122177	0.79834449
8	0.0970606	0.092174212	0.6576	0.749774212	0.565425788
9	0.107873645	0.102442889	0.626733333	0.729176223	0.524290444
10	0.051885001	0.049272919	0.906733333	0.956006253	0.857460414
11	0.002294196	0.002178697	0.990333333	0.992512031	0.988154636
12	0.046752148	0.044398473	0.569166667	0.61356514	0.524768194
13	0.030055116	0.028542031	0.1373	0.165842031	0.108757969
14	0.046725404	0.044373075	0.118366667	0.162739742	0.073993592
15	0.015325795	0.014554238	0.0951	0.109654238	0.080545762
16	0.061661036	0.058556792	0.392366667	0.450923459	0.333809874
17	0.081314472	0.077220802	0.426066667	0.503287469	0.348845864
18	0.01546135	0.014682968	0.384333333	0.399016302	0.369650365

Table 4. 90% Confidence Intervals for Packet Delivery Fraction Results

Missed Deadline Fraction							
	AODV			RTRP			
	slow	medium	fast	slow	medium	fast	yi...
5 Sources	0.0032	0.0061	0.1037	0.0063	0.0164	0.0168	0.4204
	0.0053	0.0149	0.0078	0.0037	0.0183	0.0202	
	0.0049	0.0126	0.1417	0.0008	0.0219	0.0158	
10 Sources	0.0694	0.1695	0.0925	0.0487	0.013	0.0567	1.2354
	0.0807	0.1093	0.1385	0.0508	0.0171	0.0644	
	0.0273	0.1164	0.1076	0.0033	0.0096	0.0606	
15 Sources	0.3107	0.2026	0.2068	0.0497	0.0776	0.0577	2.69236
	0.2925	0.2353	0.1862	0.051	0.0568	0.0502	
	0.3092	0.2444	0.2038	0.0536	0.0541	0.05016	
BC totals y.jk.	1.1032	1.1111	1.1886	0.2679	0.2848	0.39256	4.34816
y.j..	3.4029			0.94526			

Table 5. Simulation Results for Missed Deadline Fraction

Level	STD DEV	90% CI	mean	upper bnd	lower bnd
1	0.001115	0.001059	0.004467	0.005526	0.003408
2	0.004564	0.004334	0.0112	0.015534	0.006866
3	0.069005	0.065531	0.0844	0.149931	0.018869
4	0.002751	0.002613	0.0036	0.006213	0.000987
5	0.002793	0.002653	0.018867	0.021519	0.016214
6	0.002307	0.00219	0.0176	0.01979	0.01541
7	0.028141	0.026725	0.059133	0.085858	0.032409
8	0.032899	0.031243	0.131733	0.162976	0.100491
9	0.023448	0.022267	0.112867	0.135134	0.090599
10	0.026838	0.025487	0.034267	0.059754	0.008779
11	0.003755	0.003566	0.013233	0.0168	0.009667
12	0.00385	0.003656	0.060567	0.064223	0.05691
13	0.010103	0.009594	0.304133	0.313727	0.294539
14	0.021982	0.020876	0.227433	0.248309	0.206558
15	0.011129	0.010569	0.198933	0.209502	0.188365
16	0.001986	0.001886	0.051433	0.053319	0.049548
17	0.012859	0.012212	0.062833	0.075045	0.050621
18	0.004342	0.004123	0.052687	0.05681	0.048564

Table 6. 90% Confidence Intervals for Missed Deadline Fraction Results

Routing Overhead							
	AODV			RTRP			
	slow	medium	fast	slow	medium	fast	yi...
5 Sources	0.3928	0.6953	0.8196	0.3737	0.6267	0.6699	10.5512
	0.4145	0.6897	0.7748	0.3422	0.6683	0.6177	
	0.399	0.7501	0.809	0.3104	0.5605	0.637	
10 Sources	0.9322	3.018	1.7791	0.4834	0.2045	2.6843	26.0469
	1.1503	1.7021	2.3453	1.0286	0.2015	2.6196	
	0.6081	1.871	1.9921	0.5691	0.2013	2.6564	
15 Sources	10.3319	15.0775	9.112	6.5564	3.4044	4.5231	154.9059
	14.1075	8.3919	11.4815	5.5498	6.8584	6.5756	
	9.1597	12.0267	12.5754	7.4777	6.5626	5.1338	
BC totals y.jk.	37.496	44.2223	41.6888	22.6913	19.2882	26.1174	191.504
y.j..	123.4071			68.0969			

Table 7. Simulation Results for Routing Overhead

Level	STD DEV	90% CI	mean	upper bnd	lower bnd
1	0.011177209	0.010614507	0.4021	0.412714507	0.391485493
2	0.033373043	0.031692921	0.7117	0.743392921	0.680007079
3	0.023413102	0.0222344	0.801133333	0.823367733	0.778898933
4	0.031650118	0.030056735	0.3421	0.372156735	0.312043265
5	0.054365798	0.051628824	0.6185	0.670128824	0.566871176
6	0.026393623	0.025064871	0.641533333	0.666598204	0.616468462
7	0.27282145	0.259086615	0.896866667	1.155953281	0.637780052
8	0.71597591	0.67993105	2.197033333	2.876964383	1.517102284
9	0.285978344	0.271581143	2.038833333	2.310414476	1.767252191
10	0.293180201	0.278420431	0.6937	0.972120431	0.415279569
11	0.001792577	0.001702332	0.202433333	0.204135666	0.200731001
12	0.032451862	0.030818116	2.653433333	2.684251449	2.622615218
13	2.585534537	2.45536922	11.1997	13.65506922	8.74433078
14	3.347048427	3.178545701	11.83203333	15.01057903	8.653487632
15	1.77041836	1.681288989	11.0563	12.73758899	9.375011011
16	0.964264457	0.915719838	6.527966667	7.443686505	5.612246828
17	1.914499102	1.818116177	5.608466667	7.426582844	3.790350489
18	1.05392109	1.000862826	5.410833333	6.41169616	4.409970507

Table 8. 90% Confidence Intervals for Routing Overhead Results

Average ETE Delay							
	AODV			RTRP			
	slow	medium	fast	slow	medium	fast	yi...
5 Sources	3.56	4.8	6.32	4.19	4.19	5.15	84.92
	4.12	4.37	5.95	3.27	4.62	6.06	
	4.49	4.73	5.26	3.07	5.34	5.43	
10 Sources	13.9	21.9	11.9	7.7	3.17	12.5	199.08
	13.5	12	15.6	10.1	3.11	12	
	10	14.5	15.1	8.2	2.7	11.2	
15 Sources	29.3	25.7	23.2	16	15.9	14.9	371.7
	27	26.8	23.4	13.9	13.8	14.8	
	26.7	28.2	27	15.5	14.7	14.9	
BC totals y.jk.	132.57	143	133.73	81.93	67.53	96.94	655.7
y.j..	409.3			246.4			

Table 9. Simulation Results for ETE Delay

Level	STD DEV	90% CI	mean	upper bnd	lower bnd
1	0.468223593	0.444651496	4.056666667	4.501318162	3.612015171
2	0.2307235	0.21910803	4.633333333	4.852441364	4.414225303
3	0.537990087	0.510905687	5.843333333	6.354239021	5.332427646
4	0.597327381	0.567255724	3.51	4.077255724	2.942744276
5	0.581062246	0.551809435	4.716666667	5.268476102	4.164857231
6	0.466082968	0.442618638	5.546666667	5.989285304	5.104048029
7	2.145538006	2.037523732	12.46666667	14.5041904	10.42914293
8	5.148138822	4.888962582	16.13333333	21.02229592	11.24437075
9	2.00748599	1.906421763	14.2	16.10642176	12.29357824
10	1.266227994	1.202481421	8.666666667	9.869148087	7.464185246
11	0.255799401	0.242921518	2.993333333	3.236254851	2.750411815
12	0.655743852	0.622731295	11.9	12.5227313	11.2772687
13	1.42243922	1.350828398	27.66666667	29.01749507	26.31583827
14	1.252996409	1.189915962	26.9	28.08991596	25.71008404
15	2.138535324	2.030873592	24.53333333	26.56420693	22.50245974
16	1.096965511	1.041740234	15.13333333	16.17507357	14.0915931
17	1.053565375	1.00052502	14.8	15.80052502	13.79947498
18	0.057735027	0.054828433	14.86666667	14.9214951	14.81183823

Table 10. 90% Confidence Intervals for Mean ETE Delay Results

B.2. ANOVA Tables

index	factor	level
A	Number of Sources	3
B	Routing Protocols	2
C	Node Speed	3
n	Number of Replications	3

Table 11. Enumeration of Factors

Source of Variation	SS	DF	MS	Fo	Ftable	Sign.?	%
A	4.76654	2	2.38327	968.6906	2.46	Yes	83.9796
B	0.238615	1	0.238615	96.98625	2.85	Yes	4.20406
C	0.132127	2	0.066064	26.85181	2.46	Yes	2.327889
AB	0.176333	2	0.088166	35.83563	2.46	Yes	3.106732
AC	0.148942	4	0.037236	15.13458	2.11	Yes	2.624153
BC	0.046914	2	0.023457	9.534236	2.46	Yes	0.82656
ABC	0.077788	4	0.019447	7.904323	2.11	Yes	1.370514
Error	0.088571	36	0.00246				1.560491
TOTAL	5.675831	53					
SSR	5.587259813		**R^2**		**0.984395091**		

Table 12. ANOVA Table for Packet Delivery Fraction

Source of Variation	SS	DF	MS	Fo	Ftable	Sign.?	%
A	0.147199253	2	0.073599627	149.2716	2.46	Yes	38.05631
B	0.111851748	1	0.111851748	226.8529	2.85	Yes	28.91771
C	0.001464102	2	0.000732051	1.484714	2.46	Yes	0.378523
AB	0.067883397	2	0.033941699	68.83908	2.46	Yes	17.5503
AC	0.018995521	4	0.00474888	9.631473	2.11	Yes	4.911027
BC	4.70003E-05	2	2.35001E-05	0.047662	2.46	Yes	0.012151
ABC	0.021602151	4	0.005400538	10.95314	2.11	Yes	5.584934
Error	0.017750108	36	0.000493059				4.589042
TOTAL	0.386793281	53					
SSR	0.369043173		R^2		0.954109576		

Table 13. ANOVA Table for Missed Deadline Fraction

Source of Variation	SS	DF	MS	Fo	Ftable	Sign.?	%
A	697.834	2	348.917	228.463	2.46	Yes	76.88713
B	56.65219	1	56.65219	37.09458	2.85	Yes	6.24192
C	1.621191	2	0.810596	0.53076	2.46	Yes	0.178622
AB	81.44842	2	40.72421	26.6653	2.46	Yes	8.973961
AC	7.876082	4	1.96902	1.28927	2.11	Yes	0.867784
BC	3.53431	2	1.767155	1.157093	2.46	Yes	0.389409
ABC	3.661628	4	0.915407	0.599388	2.11	Yes	0.403437
Error	54.98051	36	1.527236				6.057735
TOTAL	907.6084	53					
SSR	852.6278588		R^2		0.939422652		

Table 14. ANOVA Table For Routing Overhead

Source of Variation	SS	DF	MS	Fo	Ftable	Sign.?	%
A	2316.166	2	1158.083	423.7548	2.46	Yes	68.97857
B	491.415	1	491.415	179.814	2.85	Yes	14.63501
C	12.64536	2	6.32268	2.313536	2.46	Yes	0.376596
AB	282.2076	2	141.1038	51.63139	2.46	Yes	8.404528
AC	46.02545	4	11.50636	4.210301	2.11	Yes	1.370701
BC	42.67581	2	21.33791	7.807767	2.46	Yes	1.270944
ABC	68.28502	4	17.07126	6.246555	2.11	Yes	2.033621
Error	98.38467	36	2.732907				2.93003
TOTAL	3357.804	53					
SSR	3259.41977		R^2		0.970699703		

Table 15. ANOVA Table for Average ETE Delay

B.3. Paired Observation Comparisons

PAIRED OBSERVATIONS				
-0.0003	-0.0023	-0.0107	Mean:	-0.132948
-0.0103	-0.0069	-0.0021	Var:	0.026281
-0.0112	-0.0073	-0.0175	90% CI	0.040995
-0.0933	-0.4444	0.1123	LB	-0.173943
-0.0445	-0.2591	0.1113	UB	-0.091953
-0.0017	-0.2947	-0.0509	Diff?	YES
-0.2045	-0.4328	-0.2891		
-0.3594	-0.2489	-0.2909		
-0.2013	-0.2414	-0.2877		

Table 16. Comparison of Protocols for Packet Delivery Fraction

PAIRED OBSERVATIONS				
-0.0031	-0.0103	0.0869	Mean:	0.091024
0.0016	-0.0034	-0.0124	Var:	0.007507
0.0041	-0.0093	0.1259	90% CI	0.02191
0.0207	0.1565	0.0358	LB	0.069114
0.0299	0.0922	0.0741	UB	0.112933
0.024	0.1068	0.047	Diff?	YES
0.261	0.125	0.1491		
0.2415	0.1785	0.136		
0.2556	0.1903	0.15364		

Table 17. Comparison of Protocols for Missed Deadline Fraction

PAIRED OBSERVATIONS				
0.0191	0.0686	0.1497	Mean:	2.048526
0.0723	0.0214	0.1571	Var:	10.02409
0.0886	0.1896	0.172	90% CI	0.800638
0.4488	2.8135	-0.9052	LB	1.247888
0.1217	1.5006	-0.2743	UB	2.849163
0.039	1.6697	-0.6643	Diff?	YES
3.7755	11.6731	4.5889		
8.5577	1.5335	4.9059		
1.682	5.4641	7.4416		

Table 18. Comparison of Routing Protocols for Routing Overhead

PAIRED OBSERVATIONS				
-0.63	0.61	1.17	Mean:	6.033333
0.85	-0.25	-0.11	Var:	33.9949
1.42	-0.61	-0.17	90% CI	1.474417
6.2	18.73	-0.6	LB	4.558916
3.4	8.89	3.6	UB	7.50775
1.8	11.8	3.9	Diff?	YES
13.3	9.8	8.3		
13.1	13	8.6		
11.2	13.5	12.1		

Table 19. Comparison of Routing Protocols for Average ETE Delay

Bibliography

[BCSR] D. Baker, M. S. Corson, P. Sass, and S. Ramanatham. "Flat vs. Hierarchical Network Control Architecture." *ARO/DARPA Workshop on Mobile Ad-Hoc Networking* *http://www.isr.umd.edu/Courses/Workshops/MANET/program.html*

[BFO96] Bianchi G., Fratta L., Oliveri M.. "Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LANs." *The Seventh IEEE International Symposium on Personal, Indoor and Mobile Radio Communications PIMRC '96, October 1996.*

[BJM99] Brosch, J., Johnson, D. B., Maltz, D. A. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks." *IETF MANET Workgroup Internet Draft, 22 October 1999 (in progress).*

[CWLG97] Chiang, C. C., Wu, H. K., Liu, W., Gerla, M. "Routing in Clustered Multi-hop, Mobile Wireless Networks with Fading Channel." *Proceedings of IEEE SICON 97, 1997.*

[DPR00] Das, Samir R., Perkins, Charles E., Royer, Elizabeth M. "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks." *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, Tel Aviv, Israel, March 2000, p. 3-12.

[DRWT97] Dube, R., Rais, C. D., Wang, K. Y., Tripathi, S. K. "Signal Stability Based Adaptive Routing for Ad Hoc Mobile Networks." *IEEE Personal Communications, February 1997.*

[Haa97] Haas, Zygmunt J., D. A. "A New Routing Protocol for the Reconfigurable Wireless Networks" *ICUPC'97*, San Diego, CA, October 12-16, 1997.

[Jai91] Jain, Raj. "The Art of Computer Systems Performance Analysis." *John Wiley and Sons Inc, 1991.*

[JM96] Johnson, D. B., Maltz, D. A. "Dynamic Source Routing in Ad Hoc Wireless Networks." *Mobile Computing, T. Imielinskiand H. Korth Kluwer Academic Publishers, 1996.*

[IEEE99] "IEEE 802.11 Wireless LAN Specification." *ISO/IEC 8802-11:1999(E), ANSI/IEEE.*

[MGA96] Murthy, Shree, Garcia, J. J., Aceves, Luna. "A Routing Protocol for Packet Radio Networks." *ACM Mobile Networks and Communications Journal, Special Issue on Routing in Mobile Communication Networks, 1996.*

[PB94] Perkins, C. E., Bhagwat, P. "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers." *Computer Communications Review, 1994.*

[PC97] Park, Vincent D., Corson, M. Scott. "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks." *Proceedings of INFOCOM 97, April 1997.*

[PC99] Park, V., Corson, S. "Temporarily Ordered Routing Algorithm (TORA) Ver. 1 Functional Specification." *IETF MANET Workgroup Internet Draft, 22 October 1999 (in progress).*

[PR99] Perkins, C.E., Royer Elizabeth M. "Ad-Hoc On Demand Distance Vector Routing." *Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 1999.*

[PRD00] Perkins, C. E., Royer, Elizabeth M., Das, Samir R. "Ad-Hoc On-Demand Distance Vector (AODV) Routing." *IETF MANET Workgroup Internet Draft, 14 July 2000 (in progress).*

[Rap96] Rappaport, Theodore S. "Wireless Communications, Principles & Practice." *Prentice Hall Publications, 1996. ISBN 0-13-375536-3.*

[RP99] Royer, Elizabeth M., Perkins, Charles E. "Multicast Operation of the Ad-Hoc On-Demand Distance Vector Routing Protocol." *Proceedings of Mobicom 99, August 1999.*

[RT99] Royer, Elizabeth M., Toh, C. K. "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks." *IEEE Personal Communications, Vol. 6, 1999.*

[TLG00] Tschudin, Christian, Lundgren, Henrik, Gulbrandsen, Henrik. "Active Routing for Ad Hoc Networks." *IEEE Communications Magazine, April 2000.*

[Toh96] Toh, Chai-Keong. "A Novel Distributed Routing Protocol to Support Ad Hoc Mobile Computing." *Proceedings of 1996 IEEE 15th Annual Intl. Phoenix Conference on Computers and Communications, March 1996.*

Vita

Lt. Necdet KILIC was born Osmaniye, Turkey. After graduating form Maltepe Military High School in 1992, he entered Turkish Air Force Academy. Upon graduating from the Academy with a Bachelor of Science Degree in Computer Engineering in 1996, he attended Euro-NATO Joint Jet Pilot Training (ENJJPT) program in Sheppard AFB, TX in 1997. Following his undergraduate pilot training, Lt. KILIC attended IFF training in Konya, Turkey in 1998. Next, he was assigned to 143rd Oncel Training Squadron. He completed his F-16 basic training before entering Air Force Institute of Technology (AFIT) in WPAFB, Ohio in 1999.