Quality of Service for Ad hoc On-demand Distance Vector Routing

by

Yihai Zhang
B.Eng, Beijing University of Posts and Telecommunications, 1996

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of

MASTER OF APPLIED SCIENCE

in the Department of Electrical and Computer Engineering

We accept this thesis as conforming
to the required standard

Supervisor: Dr. T.A. Gulliver

ABSTRACT

A mobile ad hoc network (MANET) is a collection of mobile nodes that form a wireless network without the use of a fixed infrastructure or centralized administration, and every node acts as a host as well as a router. The topology of an ad hoc network changes frequently and unpredictably. The mobile nature and dynamic topology of MANETs make it very difficult to provide Quality-of-Service (QoS) assurance in such networks. Considering the limited bandwidth and battery power, finding routes that satisfy the bandwidth constraint of applications is a significant challenge.

Ad hoc on-demand distance vector routing (AODV) is an on-demand routing protocol that only provides best-effort routes. QS-AODV is proposed in this thesis. It is based on AODV and creates routes according to the QoS requirements of the applications. It is shown that QS-AODV provides performance comparable to AODV under light traffic. In heavy traffic, QS-AODV provides higher packet delivery ratios and lower routing overheads, at a cost of slightly longer end-to-end delays as the routes in QS-AODV are not always the shortest. The effects of network size and mobility on the performance of QS-AODV are shown.

Examiners:

Table of Contents

List of Tables

List of Figures

List of Abbreviations

AODV	Ad hoc On-demand Distance Vector Routing
ARP	Address Resolution Protocol
BE	Best Effort
CBR	Constant-Bit-Rate
CEDAR	Core-Extraction Distributed Ad hoc Routing
CFP	Contention Free Period
CP	Contention Period
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
CW	Contention Window
DCF	Distributed Coordination Function
DiffServ	Differentiated Services Framework
DRSVP	Dynamic RSVP Protocol
DSCP	Differentiated Service Code Point
DSDV	Destination-Sequenced Distance Vector Algorithm
DSR	Dynamic Source Routing
EDCF	Enhanced DCF
ETSI	European Telecommunications Standards Institute
FQMM	Flexible QoS Model for MANET
HCF	Hybrid CF
IBSS	Independent Basic Service Set
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force

IntServ	Integrated Services Architecture
ISP	Internet Service Provider
ITU	International Telecommunications Union
MAC	Medium Access Control
MANET	Mobile Ad hoc Network
NP	Network Performance
ns-2	Network Simulator-2
OLSR	Optimized Link State Routing
PDA	Personal Digital Assistants
PHB	Per-Hop Behaviour
PRNet	DARPA Packet Radio Network
QoS	Quality-of-Service
QS-AODV	Quality-of-Service for AODV
RERR	Route Error
RREP	Route Reply
RREQ	Route Request
RSVP	Resource Reservation Protocol
SLA	Service Level Agreement
TBRPF	Topology Dissemination based on Reverse-Path Forwarding Routing
TDMA	Time Division Multiple Access
TTL	Time To Live
UDP	User Datagram Protocol
ZRP	Zone Routing Protocol

Acknowledgement

I am taking this opportunity to thank all those who have assisted me in one way or another with my Master study. First of all, I would like to express my gratitude toward my supervisor Dr. T. Aaron Gulliver for his invaluable guidance and encouragement throughout my master studies. His kindness, and attention to detail for his students made it a pleasure to work in his research group.

I would like to offer my gratitude to Dr. Nikitas J. Dimopoulos, Dr. Eric G. Manning and Dr. Afzal Suleman for their participation on my committee.

I also would like to thank my colleagues in Wireless Communication Research Group, namely Carlos Quiroz Perez, Caner Budakoglu, Hanfeng Chen, William Chow, Mohammad Omar Farooq, Katayoun Farrahi, Majid Khabbazian, Yang Le, Wei Li, Ubolthip Sethakaset, Yongsheng Shi and Hao Zhang for their support. Their friendship has made my life here a wonderful memory.

Most importantly, researching and writing this thesis would not have been possible without the love, understanding and untiring patience of my wife and my parents.

Chapter 1

Introduction

With the development of wireless communication technologies, mobile hosts, such as laptops and personal digital assistants (PDAs), are now widely used in daily life. Since most of these devices can operate for hours with just battery power, users are free to move around without being constrained by wires. The nature of mobile devices makes wireless networks the easiest solution for their interconnection. As a consequence, wireless networks have experienced unprecedented development in the past decade. Currently, most wireless networks are connected via fixed infrastructure-based networks, such as cell phones connected through a cellular network, or laptops connected to the Internet via an access point. An infrastructure-based network is a great way to get network services, however, it takes time and potentially a high cost to setup the required infrastructure. Furthermore, there are hostile environments where a fixed communication infrastructure is unreliable or unavailable, such as in a battlefield or in a natural disaster area struck by an earthquake or flood. Thus, an alternative way to deliver network service is desired.

A Mobile Ad hoc Network (MANET) (also called mobile packet radio network or mobile multihop wireless network) is an innovative approach to provide services under these situations. Ad hoc generally means constructed from whatever is immediately available but, in this research area, it means no infrastructure. Physically, a mobile ad hoc network consists of a number of geographically distributed mobile hosts (in this thesis referred to as "mobile nodes"), sharing a common radio channel, and a network is created "on the fly" as these nodes transmit information to each other [1] [2]. The network does not depend

on a particular centralized administrator and dynamically adjusts itself as some nodes join or leave the network. Thus, such a network is both flexible and robust. A mobile ad hoc network can be quickly deployed and provide limited but much needed communications. As wireless network technology continues to envolve, ad hoc networks will play a more important role in future research and development efforts.

A majority of ad hoc applications involve voice communications while some may require video transmission (command and control in a battlefield or disaster area). These applications demand uninterrupted and clear connections for their entire duration. Thus Quality-of-Service (QoS) is desired to provide the required service differentiation to the demanding connections. Different applications have different QoS requirements, such as bandwidth, delay or delay jitter. However providing QoS assurance in MANETs is a very complex problem due to their characteristics, such as the mobile nature of the nodes resulting in an unpredictable topology, scarce wireless bandwidth which varies with the changing environmental conditions, limited mobile device power and the requirement of node cooperation to relay packets through the network. These characteristics not only make ad hoc networks differ from conventional wireless networks, but also make providing QoS assurance a extremely challenging problem in MANETs [1].

In the remainder of Chapter 1, we give an overview of MANETs and their characteristics. This is followed by an introduction of the major applications of ad hoc networks. Next, we discuss the research challenges in the mobile ad hoc network field. After the discussion, the research goals and organization of the remainder of the thesis are given. At last, we conclude this chapter.

1.1 Mobile Ad hoc Networks

A mobile ad hoc network is a collection of mobile nodes that cooperatively and spontaneously form a wireless network without the use of any fixed infrastructure (e.g., base stations or access points), or centralized administration. The system may operate in isolation,

or may have gateways connected with a fixed network. In the latter mode, it is typically envisioned as a subnetwork connected to a fixed network. The mobile devices used in ad hoc networks could include an evolution of current cell phones, PDAs, or laptops equipped with wireless interfaces.

In a MANET, each mobile node is equipped with a wireless transmitter and receiver using antennas. Nodes can communicate directly with other nodes within their wireless transmission range. However, wireless links have significantly lower capacity and transmission range than their hardwired counterparts due to effects such as signal fading, noise and limited battery power. Consequently, multiple hops may be needed for one node to exchange data with another across the network. Thus, each node must be capable of acting as a host and as a router. Packet forwarding, routing and other network operations are distributed and carried out by individual nodes. In general, mobile nodes in ad hoc networks are free to move randomly and organize themselves arbitrarily. The network topology may change with time as the nodes move or adjust their transmission power, so it can change rapidly and unpredictably.

1.2 Applications for Ad hoc Networks

The concept of mobile ad hoc networks is not new. It dates back to the DARPA Packet Radio Network (PRNet) program in the 1970's [2]. With current technology and the increasing popularity of PDAs and laptops, interest in ad hoc networks has greatly increased. New technologies such IEEE (Institute of Electrical and Electronics Engineers) 802.11a [3], b [4], g [5], and Bluetooth [6] also provide demand for practical commercial applications of ad hoc networks. These networks can be used in situations where no fixed infrastructure is available, because it may not be either economically in practical or impossible to provide the necessary infrastructure. The major applications of MANETs are described below.

1.2.1 Military Networks

As with the development of other communication technologies, the military is a major driving force behind the development of ad hoc networks due to their unique features. Ad hoc networks do not require centralized control or an existing infrastructure, which is perfect for military applications. In a battlefield, military personnel could establish an ad hoc network to communicate at anytime from anywhere. Ad hoc network technology has been used in many military operations. Tactical Internet [2] implemented by the US Army in 1997 is by far the largest-scale implementation of mobile wireless multihop packet radio networks. Since voice and video communication may be required, it is important to provide QoS assurance in military networks.

1.2.2 Collaborative Networks

Perhaps the most typical application requiring to establish an ad hoc network is a collaborative network. These networks can be established based on IEEE 802.11a [3], b [4] and g [5] technology. Mobile users gather together and collaboratively set up an ad hoc network. People exchange data at a conference or in a classroom without using any network structure except the one they create by simply turning on their computers or PDAs. QoS assurance is also desirable in these networks because of multimedia applications.

1.2.3 Emergency Services

Ad hoc network technology does not need any fixed infrastructure or centralized administration, which is very useful in situations where the existing infrastructure is destroyed or unavailable for some reason. The goal of establishing a MANET in such situations is to enable the use of wireless devices and provide network services, which is very important to emergency services. MANETs could help during disaster relief. For example, firefighters or police can remain in touch longer and provide information more quickly if they cooperate to form an ad hoc network in places where other services are damaged or not available.

Providing uninterrupted communication is very important in emergency services, thus QoS has to be guaranteed in the network.

1.2.4 Wireless Sensor Networks

Recent research interest has also been focused on networks involving a large collection of tiny sensor devices. Wireless sensor networks [7] are different from typical ad hoc networks, as each sensor in the network is used to collect information and transfer it to a processing center which analyzes and performs further actions. Once the sensors are situated, they usually remain stationary. This technology is very useful in environments where it is impossible to provide a network infrastructure. For example, if hazardous chemicals are discharged, instead of sending a emergency team, we could distribute sensors in the area to form an ad hoc network and gather desired information. The military also has great interest in this technology, because these networks can provide valuable battlefield information.

1.2.5 Personal Area Networks

Personal area networks connect devices carried by users to nearby mobile and stationary devices [1], i.e., it is a network around a person. These mobile devices include cell phones, PDAs and laptops, and other digital electronic devices. They typically provide a communication range of up to 10 meters. Bluetooth Technology [6] can be employed for these networks. Applications could include forming an ad hoc network with workspace electronic devices, or home electronic devices. People can use the laptop or PDA to transfer files, read email or get Internet services. Depending on the applications, different QoS assurances are required.

1.3 Challenges in Ad hoc networks

In an ad hoc network, nodes move randomly, self-organize and reconfigure as they move, join or leave the network, so the network topology changes frequently and dynamically. All nodes can play the same role in the network, and functions are distributed and decided among all the nodes, so the network does not need a central controller. However, this flexibility and convenience pose serious research challenges as described below [8].

- **Multihop routing protocols:** The distance between source and destination nodes usually exceeds the transmission range of mobile devices. As a consequence, the routes in ad hoc networks are mostly multihop. Considering the limited bandwidth and power, designing an efficient and reliable routing protocol becomes a very challenging task in ad hoc networks. A good routing protocol must use the limited resources efficiently, and adapt to frequent topology changes and different network conditions: node mobility, network size and traffic conditions. Routing protocols for ad hoc networks are required to have the following characteristics: loop freedom, energy efficiency, scalability, security. Because of these requirements, routing protocols designed for fixed network are not suitable for ad hoc networks.
- **Medium access control (MAC):** Among the various aspects of mobile ad hoc networks, medium access control is another active research area. The multihop feature of ad hoc networks allows spatial reuse of the wireless spectrum. Two nodes can use the same channel to transmit information if they are sufficiently apart. There are two types of medium access protocols: random access, e.g., IEEE 802.11 [9], and controlled access protocols, e.g., TDMA (Time Division Multiple Access). Ad hoc networks do not have any infrastructure support, so most proposed MAC protocols in ad hoc networks are based on random access mechanisms, namely, IEEE 802.11. IEEE 802.11 is very simple and easy to implement, it works well under light traffic but suffers from frequent collisions when the traffic becomes heavy. Furthermore, IEEE 802.11 is designed for single-hop wireless network, so it is not optimized when

used in multihop environments.

- **Scalability:** As the number of mobile nodes in an ad hoc network increases, scalability becomes an important issue. Generally, scalability in ad hoc networks is defined as the ability to provide an acceptable level of service with a large number of nodes in the network [8]. Most routing protocols adopt a flat addressing scheme where each node in a route plays an equal role, which creates excessive routing overhead as the number of nodes in the ad hoc network grows. Clustering and hierarchical solutions have been proposed to improve network performance and scalability, such as Zone Routing Protocol (ZRP) [10]. In general, nodes will be grouped into clusters based on either geographical location or functionality. Routes will be created based on clusters instead of individual nodes, which will increase the robustness of routers and decrease the overhead and the size of routing tables. How to group nodes into different clusters and manage them when the nodes are moving is the main concern.
- **Security:** Security is a very important issue with ad hoc networks. Providing security in a fixed network is simple due to central administration and a pre-determined topology. However, there is no central support in ad hoc networks, nodes move around arbitrarily and join and leave the network readily, so the topology of ad hoc networks is dynamic and unpredictable. Therefore, the security solutions for fixed networks are not suitable for ad hoc networks.
- **Energy efficiency:** Mobile devices rely on batteries for energy. However, the battery used by each node has a limited power supply, which in turn limits services that can be supported by each node. Large improvements in battery capacity are not expected in the near future, so how to efficiently manage power without degrading the applications is one of the main concerns in ad hoc network research. For a network to maximize its capacity, it is necessary for each node to adjust its transmission power carefully, maybe just to reach its nearest neighbor. Energy consumption research has a significant impact on the lifetime and usefulness of ad hoc network.

- **Quality-of-Service:** Quality-of-Service is a desirable feature for mobile ad hoc networks due to the growth of multimedia applications. These applications often have a requirement to receive data at a certain rate, or within a certain delay. Since the available bandwidth for supporting these applications is limited, proper management of the bandwidth is necessary to accommodate the applications, and provide QoS assurance to the end users. There are a number of approaches to satisfy such requirements within the Internet [11] [12]. However, due to the characteristics of the wireless medium, dynamic topology and absence of central support, wire-based QoS models are not appropriate for ad hoc networks. To guarantee quality of service in an ad hoc network, there needs to be a coordinated effort from all network components, including QoS routing, QoS MAC, and resource-reservation signaling. We will give a detailed description of quality of service in ad hoc networks later in the thesis.

1.4 Research Goals

The motivation for this research is to address concerns about quality of service in mobile ad hoc networks. Although QoS in ad hoc networks is involved with all network components, my work focuses on QoS routing protocols. Most proposed ad hoc routing protocols only provide a best effort route for an application, i.e., Ad hoc On-demand Distance Vector Routing algorithm (AODV) [13]. AODV is an on demand routing protocol, it is simple and robust, and it has been submitted to IETF as one of the candidate routing protocol standards for ad hoc network technology.

The proposed protocol provides QoS assurance based on AODV. A QoS extension has been added to AODV routing table and control packets (Routing Request, Routing Reply and Routing Error). We attempt to find routes which have sufficient bandwidth for each application. Local repair and adaptation mechanism are also used to provide a better packet delivery ratio. The techniques implemented are generic in nature and are applicable to other on-demand routing protocols.

1.5 Organization of The Thesis

The remainder of this thesis is organized as follows. Chapter 2 presents an overview of quality of service. First an introduction to quality of service is given and several QoS metrics are presented. Then we discuss QoS in ad hoc networks, and the research challenges to providing QoS assurance in ad hoc networks. Related work on QoS in ad hoc networks is also presented in this chapter.

Chapter 3 discusses and analyzes the AODV Routing protocol and presents our proposed QoS solution for AODV. We discuss our simulation environment and how to implement our design in MANETs, and simulation results are presented. We also evaluate and compare our results with AODV. Chapter 4 concludes the thesis and suggests some topics for future work.

1.6 Summary

In this chapter, an introduction to ad hoc networks was given, and the basic characteristics of ad hoc networks were presented. After the introduction, we described several major applications of ad hoc networks, namely, military networks, collaborative networks and emergency services, etc. Then we discussed the research challenges in ad hoc networks, including routing, MAC protocol, security and QoS. Finally, the research goals and organization of this thesis were given in the end of this chapter.

Chapter 2

Quality-of-Service in Ad hoc Networks

Quality of service has become a very attractive notion in recent ad hoc network research. It is quite complex and difficult due to the nature of dynamic network topology and imprecise information. In this chapter, we give the concept of quality of service in communication networks first, and discuss the metrics that can be used to evaluate network service. In section 2.3, two basic protocols of QoS in wired networks are presented. After these introductions, we describe the difficulties and proposed solutions for QoS in ad hoc network research from four different aspects: QoS model, QoS MAC, QoS signaling and QoS routing. At last, we conclude this chapter.

2.1 Quality-of-Service

A *service* in a communication network is defined by the International Telecommunications Union (ITU) as *"a service provided by the service plane to an end user (e.g. a host [end system] or a network element) and which utilizes the IP transfer capabilities and associated control and management functions, for delivery of the user information specified by the service level agreement"* [14]. The term *quality* has several meanings in different fields. In the telecommunication area, it is used to estimate whether the service satisfies the customer's expectations [15]. However, it depends on who is assessing the service. An end user may assess the service based on his expectation, whereas an engineer may rate the service according to several technical parameters.

Therefore, there are many meanings for QoS, which can cause confusion. In [16], three notions of QoS are provided which can be used to clarify this confusion: Intrinsic QoS, Perceived QoS and Assessed QoS [16]. Intrinsic QoS concerns service features from the technical perspective, it is a technical measure considered by engineers. Furthermore, Intrinsic QoS concerns the network architecture and its development, dependability, and effectiveness. It is determined by the transport network design and provisioning of network access, termination, and connections [16]. Thus, the performance is measured and compared to expected performance, it is not affected by customer opinions.

Perceived QoS reflects the end user's view about a service. It is assessed by comparing the customer's expectations to the observed performance. As a consequence, perceived QoS is influenced by the user's experience, a service with the same intrinsic QoS features may have different perceived QoS with different customers. Assessed QoS is a factor that the customer uses to decide whether to continue using a service or not. This decision is made based on the perceived quality, service price, and responses of the provider to submitted complaints and problems [16].

There are three groups providing the QoS solutions: International Telecommunications Union (ITU) [17], European Telecommunications Standards Institute (ETSI) [18], and The Internet Engineering Task Force (IETF) [19]. None of these deal with assessed QoS. QoS in the ITU/ETSI approach mainly deals with perceived QoS rather than intrinsic QoS. In addition, a notion of network performance (NP) is introduced to provide a distinction between technical perspective and user-perceivable effects [15]. The NP parameters determine the quality observed by customers but are not necessarily meaningful to them [20]. Therefore, QoS parameters in ITU/ETSI approach are user-oriented. However, QoS is understood by IETF as *"A set of service requirements to be met by the network while transporting a flow "* [19]. It only deals with Intrinsic QoS from a technical perspective, and is closely equivalent to the notion of NP defined by ITU/ETSI. QoS discussed in this thesis is based on the IETF approach, which is Intrinsic QoS.

2.2 QoS Metrics

The most important aspect of QoS assurance in communication networks is to specify the QoS requirements and quantify them. In [21], transmitted traffic through communication networks is characterized by four parameters (metrics): loss (unreliability), delay, jitter (delay variation) and bandwidth.

The value of QoS parameters can be expressed mathematically as given below [22].

- **Additive metrics:** An additive metric has the form

$$m(p) = \sum_{i=1}^{K} m(k_i), \tag{2.1}$$

  Where *m(p)* is total of metric m of route p, k_i is the *ith* link in the route p, and K is the number of links in route p. The link metric $m(k_i)$ is determined based on the QoS parameters, such as delay, delay variation (jitter) and cost.

- **Concave metrics:** A concave metric has the form

$$m(p) = min(m(k_i)) \tag{2.2}$$

  Bandwidth is the most common example of this type of metric. The *bandwidth* here is the residual bandwidth that is available for new traffic. It can be defined as the minimum of the residual bandwidths of all links on the route.

- **Multiplicative metrics:** A mulitiplicative metric has the form

$$m(p) = \prod_{i=1}^{K} m(k_i) \tag{2.3}$$

  Loss probability L is an example of this metric. The successful transmission probability metric can be expressed as follow:

$$st(p) = \prod_{i=1}^{K} st(k_i) \tag{2.4}$$

Where

$$st(k_i) = 1 - m(k_i) \tag{2.5}$$

These metrics can be used to determine the QoS requirements of an application. Several common networks applications and their QoS requirements are listed in Table 2.1.

Applications	QoS requirements			
	Loss	Delay	Jitter	Bandwidth
Email	High	Low	Low	Low
File transfer	High	Low	Low	Low, Medium, High
Telephone	Low	High	High	Low
Video on demand	Low	Low	High	High
Video conference	Low	High	High	High

Table 2.1. *Applications and their QoS requirements*

2.3 QoS Architectures of Communication Networks

Today most Internet protocols provide best effort (BE) IP forwarding. They try to deliver all traffic as soon as possible without considering packet loss, throughput or delay. Best effort forwarding may be adequate for most applications, however, QoS support is required to satisfy the growing need for multimedia applications, e.g. video on demand or IP telephony. Existing QoS models can be classified into two types according to their fundamental operation; the Integrated Services (IntServ) architecture [11] and the Differentiated Services (DiffServ) framework [12].

- **IntServ:** The IntServ model [11] was proposed by IETF in 1994, and offers per flow end-to-end reservations. The IntServ model benefits from both datagram networks and circuit switched networks. It offers circuit-switched service in packet

switched networks. The Resource Reservation Protocol (RSVP) [23] was designed as the primary signaling protocol to create and maintain connections. It is also used to transmit data and reserve resources along the route. With corresponding resource management, routers are setup to guarantee the QoS specifications of the connection, and provide quantitative QoS for every flow.

- **DiffServ:** Differentiated Services [12] was designed to overcome the difficulty of implementing and deploying IntServ and RSVP in the Internet, and provides hop-by-hop differentiated packet delivery. Unlike IntServ which provides per-flow guarantees, DiffServ maps flows into several service levels. At the network boundary, traffic entering a network is classified and assigned to different classes by assigning a special DS (Differentiated Services) field in the IP packet header (TOS field in IPv4 or CLASS field in IPv6). Then packets are forwarded based on the per-hop behavior (PHB) associated with the Differentiated Service Code Point (DSCP). This eliminates the requirement to keep information about flow state elsewhere in the network.

2.4 QoS Research Challenges in Ad hoc Networks

Recently quality of service in MANETs has received increased interest due to the growth of multimedia applications. However, MANETs differ from traditional wired networks, which introduces difficulties in providing QoS assurance in such networks. As mentioned in the last chapter, an ad hoc network is a collection of mobile nodes which dynamically create a wireless network without any fixed infrastructure and centralized administration. This network is a self-creating, self-organizing and self-administering network.

Wireless links have much lower capacity than links in a wired network. Considering the effects of fading, noise and interference in wireless channels, throughput in a wireless network is typically less than the maximum rate. Thus, congestion happens more often in a wireless network. With the increasing demand of multimedia applications, bandwidth is a major concern of ad hoc network research.

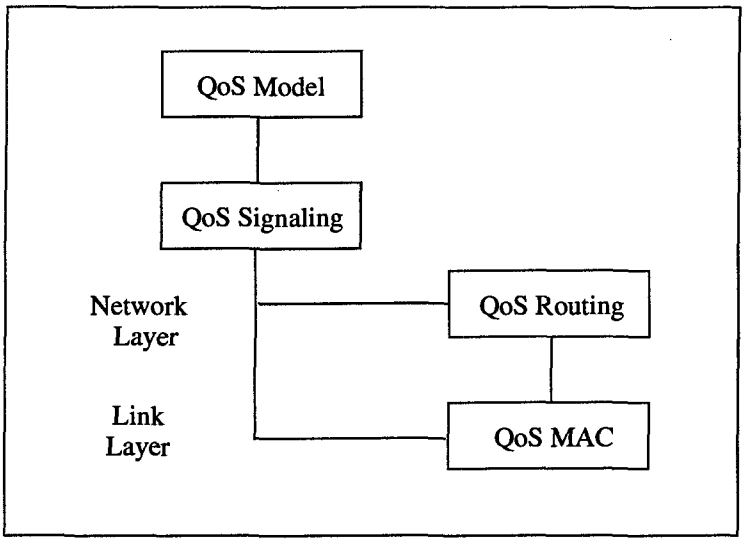

Figure 2.1. *QoS in ad hoc networks*

The ability of an ad hoc network network to provide QoS assurance depends on all the network components, from the physical layer to the MAC layer and network layer. A view of QoS protocols of ad hoc networks is shown in Figure 2.1. The research challenges and related work are discussed in the following sections.

2.4.1 QoS Model

Since ad hoc network resources (e.g., bandwidth and battery power) vary with time, current QoS models for wired networks are not suitable for a MANET, and thus a new QoS model must be defined. Specifically, IntServ [11] and DiffServ [12] do not work very well in ad hoc networks, as they both require accurate topology and link state information (e.g., delay, available bandwidth).

- **IntServ:** IntServ provides per-flow QoS assurance. In IntServ, routers have four basic functions: RSVP, admission control routing, packet scheduler and classifier [11]. These functions create high control overhead and consume power, which is limited in ad hoc networks. Furthermore, when the number of flows in the network

increases, the amount of state information also increases. Subsequently, the routers need more memory and have more routing overhead. This is the scalability problem of IntServ.

- **DiffServ:** DiffServ is using the concept of Service Level Agreement (SLA) [12]. SLA is a contract between an end-user and their Internet Service Provider (ISP) that specifies the service the customer can use. The DiffServ server must assure that it has sufficient resources to provide to the customer. In general, if a customer requires a certain quality of service and pays for this service, the customer will expect to receive that QoS. However, an ad hoc network does not have any centralized administration. Thus, it is difficult to provide required QoS to customers. Furthermore, DiffServ boundary nodes are required to monitor arriving traffic, and perform service classification and enforce the negotiated SLAs, but it is hard to define boundary nodes and core in a MANET.

In [24], the Flexible QoS Model for MANET (FQMM) was proposed to define a MANET QoS model that benefits from the concepts and features of both IntServ and Diffserv. Specifically, for applications with high priority, the per-flow QoS guarantee of IntServ is provided. For applications with lower priorities, DiffServ per-class differentiation is given. Another more realistic direction for QoS provisioning in ad hoc networks is based on an adaptive QoS model [25], which provides a set of parameters in order to adapt the application to the quality of a network. The quality of service provided is not related to any dedicated network layer, instead, it requires a coordinated effort from all layers, and applications adapt to the time varying resources offered by the network.

2.4.2 QoS MAC

The IEEE 802.11 [9] Wireless LAN standard is widely used in wireless networks. The 802.11b [4] version provides data rates up to 11 Mbps, while the 802.11a [3] version can achieve data rates up to 54 Mbps. In IEEE 802.11a and b, an ad hoc network is called an

Independent Basic Service Set (IBSS). An IBSS is based on the Distributed Coordination Function (DCF) that utilizes a random access mechanism of carrier sense multiple access with collision avoidance (CSMA-CA) [4]. However, both protocols only support best-effort service. If the sum of the transmission rates of all the flows is greater than the channel capacity, heavy channel contention will occur. This contention will result in packet loss, delay and increased jitter. Furthermore, the DCF uses a complex handshaking in order to minimize hidden-terminal and exposed-terminal problems [26], which results in extensive control packets. Therefore, IEEE 802.11 is not efficient to support QoS in ad hoc networks.

To provide MAC-level QoS assurance, currently the IEEE 802.11 Working Group is developing the IEEE 802.11e standard [27]. This standard provides QoS features to the existing 802.11b [4] and 802.11a [3] standards, and it still maintains backward compatibility with these standards. The IEEE 802.11e MAC introduce two new coordination functions: Enhanced DCF(EDCF) and controlled Hybrid CF (HCF).

The EDCF works in Contention Period (CP) only while the HCF works in both Contention Free Period (CFP) and CP. EDCF is used to enhance the DCF access method and provide a distributed access mechanism that can support differentiated service. IEEE 802.11e divides traffic into several classes based on different QoS parameters, e.g., initial window sizes, maximum window sizes, and interframe spaces. For example, a short Contention Window (CW) will be assigned to high priority classes to ensure that they are able to transmit before the lower priority classes. With this mechanism, EDCF will provide better service to high priority traffic while offering a minimum service for low priority traffic.

2.4.3 QoS Signaling

QoS signaling is used to perform admission control and scheduling, and to reserve and release resources along the route determined by QoS routing, or other routing protocols. QoS signaling is a challenging area of ad hoc network research due to the dynamic nature and imprecise link state information of ad hoc networks. There are a number of issues that need to be considered when we design a QoS signaling protocol in ad hoc networks, such as

how the control information and data are transmitted and how the flow path is established.

INSIGNIA is the first QoS signaling protocol specifically designed for resource reservation in ad hoc environments [28]. It supports in-band signaling by adding a new option field in the IP header (called INSIGNIA) to transmit the signaling control information. Like RSVP, INSIGNIA supports per-flow management, it is responsible for establishing, restoring, adapting and tearing down real-time flows. INSIGNIA includes fast flow reservation, restoration and adaptation algorithms that are specifically designed to deliver adaptive real-time service in MANETs [28]. QoS reports are sent to source nodes periodically to report network topology changes, as well as QoS statistics (loss rate, delay, and throughput).

Dynamic RSVP protocol (DRSVP) [29] is another QoS signaling protocol for MANETs based on RSVP. It provides a flexible method to adjust the reserved resources on nodes dynamically, including source node, destination node and intermediate nodes, along the reserved route according to the corresponding available resource. Each node notifies the previous hop and next hop in the reserved route if it needs to adjust the reserved resource. Therefore, DRSVP does not waste precious Internet resources to transmit unnecessary multimedia packets. In addition, the required resources in DRSVP are a resource range, not a specific value. DRSVP provides nodes with the capability to support display systems with different resolution, and supporting the characteristic bit stream of MPEG-4-based video.

2.4.4 QoS Routing

In recent years, many routing protocols have been proposed for ad hoc networks, and these can be classified into two categories: table-driven (proactive) protocols and on-demand (reactive) protocols. Proactive protocols require each node to maintain one or more tables to store routing information from each node to all other nodes in the network, regardless of whether they are actually used or not. Conversely, reactive protocols create and maintain routes only when they are desired, and differ on how they discover and maintain routes between sources and destinations. Currently, The Mobile Ad hoc Networks working group of the Internet Engineering Task Force (IETF) has been actively evaluating and standardizing

several routing protocols, e.g. Ad hoc On-demand Distance Vector (AODV) Routing [13], Dynamic Source Routing (DSR) [30], Topology Dissemination based on Reverse-Path Forwarding (TBRPF) Routing [31] and Optimized Link State Routing (OLSR) [32].

However, most routing solutions only provide best-effort routes which do not satisfy the QoS requirements of growing multimedia applications in ad hoc networks, such as delay and bandwidth constraints. A good QoS routing protocol should select routes that have sufficient resources to meet the QoS requirements of applications, and efficiently use network resources.

QoS routing for wireline networks has received extensive attention [33], however, this is not very suitable for ad hoc networks as precise network state information is required. The dynamic nature of an ad hoc network makes it extremely difficult to obtain the accurate knowledge, both instantaneous and predictive, of the network state. Furthermore, constant updates of link state information, e.g. delay, bandwidth, cost and loss rate, are required to make optimal routing decisions, which result in extensive control overhead. This can be prohibitive for bandwidth constrained ad hoc environments. Even after establishing a route that satisfies the QoS requirements, this route is hard to guarantee due to the frequent changing topology. The size of an ad hoc network is also a problem if it is large, because the computational load will be high, and it will be difficult to propagate network updates within given time bounds.

Various QoS routing algorithms have been proposed to resolve the QoS provisioning problem in ad hoc networks. A detail introduction to QoS routing in ad hoc networks was given in [34]. The Core-Extraction Distributed Ad hoc Routing algorithm (CEDAR) [35] achieve QoS provisioning by finding a route through an ad hoc network that satisfies the minimum bandwidth requirements with high probability. A set of core nodes is dynamically selected using local computation and local state information. A core node keeps the local topology information of the nodes and performs route computation on behalf of these nodes. Each core node transmits the available bandwidth information of stable high bandwidth links to core nodes which are far away from it, while information about dynamic

links or low bandwidth links is kept local. At first, route discovery establishes a core route from the core node of the source to the core node of the destination. Then, using this directional information, CEDAR tries to find a partial route from the source to the core node of the furthest possible node in the core route that satisfies the requested bandwidth using only local information. Therefore, the selected route is a shortest route with maximum bandwidth using the core path as a guideline.

S. Chen and K. Nahrstedt proposed a QoS routing protocol [36] to work with imprecise information in ad hoc networks. Multiple paths are searched in parallel to find a QoS route. The protocol limits the route discovery to a small number of paths, which reduces the routing overhead. In order to maximize the chance of finding a QoS route, the state information at the intermediate nodes are collected to make hop-by-hop route decisions. Fault tolerant techniques are also used to reduce the level of QoS disruption and route maintenance. This protocol repairs a broken route at the break, shifts the traffic to a neighbor node, and reconfigures the route around the break without rerouting the connection along a completely new path.

2.5 Summary

In this chapter, we gave a detailed definition of QoS in communication networks. Then we described several QoS metrics from a technical perspective. Two QoS protocols (IntServ and DiffServ) were presented. At the end of this chapter, we discussed the difficulties and methods of providing QoS assurance in ad hoc networks based on network components. Although many difficult problems exist for each of the network components, this thesis will only consider the issue of providing QoS routing support in ad hoc networks.

Chapter 3

Proposed Protocol

Ad-hoc On-Demand Distance Vector Routing (AODV) is a distance vector routing protocol based on the Destination-Sequenced Distance Vector Algorithm (DSDV) [37] and DSR [30], which was first proposed in 1999 [38]. It is the most popular routing protocol for ad hoc networks, and has been investigated widely by many researchers for a large number of network topologies and environments. In July 2003, the latest version of AODV [13] was recommended as a experimental routing protocol for ad hoc networks by IETF.

AODV is a pure on demand routing protocol, so that a route is only discovered when required by a source node. A node does not need to keep route or reserve bandwidth that is not needed. AODV eliminates periodic routing updates and only propagates necessary information to minimize control overhead. It is very simple and does not need much computation, so the processing overhead is low. Therefore, AODV is very suitable for bandwidth constrained routing. Based on AODV, we propose in this chapter a QoS routing protocol to provide QoS assurance in ad hoc networks. With this protocol, local state information is propagated through the network, and precise network information is not required to create a path that satisfies the QoS requirements of each session.

The rest of the chapter is organized as follows. In Section 3.1, we introduce AODV, and explain how AODV discovers and maintains routes in ad hoc networks. Then the proposed protocol is given. In Section 3.3 we evaluate the performance of this protocol and compare it with AODV. A brief summary of the chapter is given in Section 3.4.

3.1 Ad hoc On-demand Distance Vector (AODV) Routing

3.1.1 AODV Overview

AODV specifies three types of routing packets for discovering and maintaining routes: Route Request (RREQ), Route Reply (RREP), Route Error (RERR) packets. These routing packets are received using the User Datagram Protocol (UDP). When a route to a destination node is desired, the source node broadcasts a RREQ to find a route to the destination. A route can be set up when the destination node receives the RREQ packet, or an intermediate node with a 'fresh enough' route to the destination receives the RREQ packet. The term 'fresh enough' means that the route entry for the destination node is active and the destination sequence number is at least as great as that recorded in the RREQ packet. Then the destination node or intermediate node unicasts a RREP packet back to the source of the RREQ. Each node receiving the RREQ records a reverse route back to the source of the request, so that the RREP can be unicast to that source.

The Hello message is a specific type of RREP packet. Each node broadcasts a Hello message to its neighbors periodically to notify them of the node's existence. The Hello message also lists other nodes from which it has heard, so that each node has some knowledge about the network connectivity.

In AODV, each node maintains a routing table which records routing information obtained from routing packets, even for short-lived routes, such as temporary reverse routes to the source nodes. AODV uses the following fields for each route table entry [13]:

- Destination IP Address
- Destination Sequence Number
- Valid Destination Sequence Number flag
- Routing state and routing flags (e.g., valid, invalid, repairable, being repaired)
- Network Interface
- Hop Count to the destination node

- Next Hop
- List of Precursors
- Lifetime (expiration or deletion time of the route)

3.1.2 Sequence Number

Many traditional distance vector protocols suffer from a problem called "count to infinity" [39]. AODV uses a destination sequence number for each node to prevent this problem and avoid routing loops. The destination sequence number is created by the destination node and sent with routing information to the source node. Each node maintains its own sequence number. It provides a relative timeline of the routing information. A node increments its sequence number when it sends out a new route request. If a destination node receives a route request for itself, it updates its sequence number to the maximum of its current sequence number and the destination sequence number in the route request packet, and then sends a RREP packet back to the source node.

The use of sequence numbers prevents routing loops and selects the most recent route to a destination. A proof of the loop freedom of AODV is given in [38]. During route discovery, the source node or an intermediate node may receive multiple route replies for the destination. In this case, the node always selects the route to the destination with the greatest destination sequence number. This ensures that the selected route is the freshest. Given the choice between two routes with the same destination sequence number, the one with the smallest hop count is chosen.

3.1.3 Route Discovery

When a source node needs to send data packets to a destination, it first checks the routing table to see whether it already has a valid route to that destination. If not, the node performs route discovery to find a route to the destination. First, the source node creates a RREQ packet. The RREQ packet includes the IP address of the destination node, the last known

sequence number for the destination, its own IP address, its current sequence number, and the hop count which is set to zero. If the source node has no knowledge of the sequence number for the destination, it is set to zero. Each node also has a RREQ ID, which is a unique number incremented every time a node sends a route request. This RREQ ID is included in the RREQ packet to identify each route request sent by the source node.

The source node broadcasts the RREQ packet to its neighbors. When a node receives the RREQ packet, it first increases the hop count value in the RREQ and creates a reverse route entry in its routing table for both the source node and (if applicable) the neighbor node from which it received the request. The intermediate node can use this reverse route to forward a RREP packet to the source node if it later receives a RREP packet. After creating the reverse route, the node sends a RREP packet to the source if it is either the destination, or has a "fresh enough" route to the destination. Otherwise, it just rebroadcasts the RREQ packet to its neighbors. Fig 3.1 shows an example of AODV route discovery, where node S is the source node and node D is the destination node. Links in this figure represent RREQ packet broadcasting.

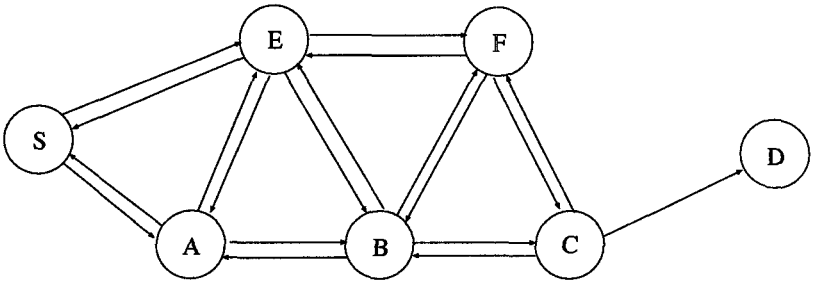

Figure 3.1. *An example of AODV route discovery*

A RREP packet contains the IP address of the destination node, the destination sequence number, the source IP address, the hop count to the destination node (if it is the destination node, it is set to zero, otherwise it is the hop count of the routing entry for the destination node), and the lifetime value of the RREP packet. A RREP packet is unicast to the source node from the destination node or intermediate node.

When a node receives the RREP packet, it first increments the hop count value in the

packet, and then creates a forward route entry for both the destination node and the neighbor node from which it received the RREP packet. The forward route entry is used to forward data packets during transmission. The node then forwards the RREP packet to the next hop towards the source node according to the reverse route entry, and so on, until the RREP packet reaches the source node. After the source node receives a RREP, it can use the route for data packet transmission. If the source node receives multiple RREPs along different paths, it will select the route with the greatest destination sequence number. Fig 3.2 shows an example of AODV route reply.

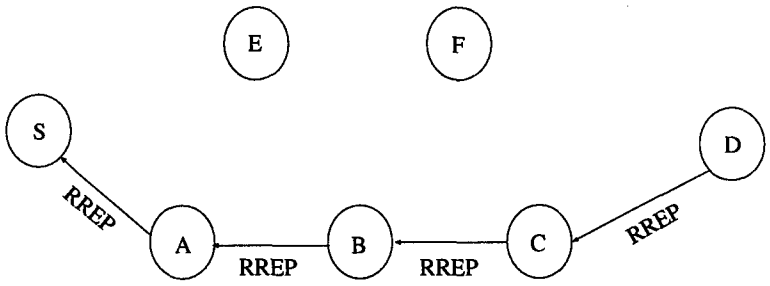

Figure 3.2. *An example of AODV route reply*

Each node records the RREQ packets that it has received. When it receives duplicate RREQs (with the same RREQ ID and source address) from neighbor nodes, they are discarded and not rebroadcast, which reduces the routing overhead caused by "flooding" broadcasts. The RREQ information recorded in each node must be kept a certain amount of time to ensure that no other node in the network is still processing request packets resulting from the same route discovery.

3.1.4 Route Maintenance

In an ad hoc network, links in active routes may break due to the nature of mobile nodes, so a method is needed to notify other nodes associated with this link in the network that the link is broken. An active route in AODV is defined as a route that has recently been utilized for data transmission. When a broken link is discovered, the upstream node of the link, which is closer to the source node, invalidates all the active routing entries in its

routing table that use the downstream node of the broken link as the next hop. Then it creates an RERR packet, in which it lists all the unreachable destinations and their known sequence number. Each routing entry includes a precursor list, which records those neighbor nodes to which a route reply was generated or forwarded. If there is only one precursor in the routing entry, then the RERR packet is unicast towards the source node along the reverse route. Otherwise the node broadcasts the RERR to all its neighbors. When a node receives an RERR packet, it first checks whether it is the next node in the route to one of the destinations listed in the packet. If it is, the node invalidates the related routes in its routing table and then retransmits the RERR packet as before. In this manner, the RERR packet is forwarded to the source nodes. After the source node receives the RERR packet, it may initiate route discovery if it still needs a route.

Each routing entry has a lifetime value. This value is assigned when a route is created, and is based on the information contained in the RREQ, RREP or Hello packet for the destination node. Each time a route is utilized in the routing table, whether it is forwarding a data packet or transmitting a routing packet, the lifetime value for that destination is updated. Receiving a Hello packet from a neighbor node results in an update of the lifetime of that neighbor's route table entry. If a route to a destination is not utilized within the lifetime, the routing entry for that destination will expire. AODV treats this as a broken route. While this conservative mechanism may remove some valid routes from the route table, it also prevents the use of routes that have become stale due to node movement [40].

For on-demand protocols, a broken route does not mean the associated application is aborted. In the first version of AODV [38], when a broken link occurred on an active route, the upstream node of this link sends a RERR packet to the source node. Before the source node receives the RERR packet, it will continue to send data packets, since it has no knowledge that the link is broken. To increase the successful data transmission ratio, local repair could be performed on the upstream node of the broken link instead of issuing a RERR packet [13]. If the destination node is not farther than MAX_REPAIR_TTL hops away, where MAX_REPAIR_TTL is determined based on the number of nodes in the

network, the upstream node of the broken link sends a RREQ packet to the destination. The sequence number of the destination node in this RREQ packet is incremented by one to prevent loops to nodes that still think they have a "fresh enough" route to the destination. While waiting for a RREP, the intermediate node buffers incoming data packets for the destination node [13]. If the local repair request is successful, a RREP will be returned either by the destination or by a node with a valid route to the destination. After the node that initiated the local repair receives this RREP, a route is created between it and the destination node, and buffered data packets can be forwarded to the destination along the route. If the node that initiated the request does not receive a RREP after a certain period of time, the local repair request is failed and a RERR packet is sent back to the source node as described before. There exists a tradeoff between reducing the packet loss ratio and reducing delay.

3.2 Proposed QS-AODV

QS-AODV is proposed here to provide QoS assurance for the AODV routing protocol. A QoS extension for AODV routing packets was proposed by Perkins in [41]. This QoS object extension includes the bandwidth or delay parameters of each application, and it also has a "session ID" which is used to identify each QoS flow that is established according to the application. The extension is added to RREQ and RREP packets to discover and create routes. The session ID and required QoS parameters are recorded in the routing tables to identify different QoS flows. QS-AODV modifies the route discovery and maintenance mechanisms of AODV to provide QoS assurance, a detailed description is given in the following sections.

Previous work has considered TDMA to support AODV and provide QoS in ad hoc networks [42] [43]. They use similar route discovery and maintenance to that of AODV. Bandwidth, which is the number of time slots in TDMA, is calculated as a RREQ packet is forwarded hop by hop. Packet extension [41] is also used in these two protocols. Local

repair is not used, even though it is considered to be useful in QoS routing as with AODV [40]. Furthermore, TDMA is a controlled access scheme, but the lack of infrastructure and the peer-to-peer nature of ad hoc networks makes it less efficient than random access schemes, i.e. IEEE 802.11 [8].

Multiple metrics may model both networks and applications more accurately, but finding a route subject to multiple metrics is inherently difficult and in many cases is considered to be an NP-complete problem [22]. Thus the only QoS metric considered in this thesis is bandwidth for a QoS flow. We assume the link capacity of each node is 2 Mbps, and all neighbor nodes must share this link capacity.

3.2.1 Route Discovery

For route discovery, when the source node requires a route to a destination node with specified bandwidth requirements, it broadcasts a RREQ packet with the QoS extension to its neighbor nodes. When a node receives a RREQ packet, it first checks if it has enough available bandwidth for the request. A node which does not satisfy the bandwidth constraint will discard the RREQ packet. If it has the required bandwidth available, a reverse route entry is created with the specified session ID and used to forward the RREP to the source node, then it rebroadcasts the RREQ packet as in the original AODV, until the RREQ packet reaches the destination node. Once the route discovery packet arrives at the destination, a route reply is generated.

In AODV, a RREP packet can be created by the destination node or an intermediate node which has a "fresh enough" route to the destination [13]. However, a RREP packet can only be created by the destination node in QS-AODV, because it has to ensure that all the nodes along the route satisfy the bandwidth constraint. When the destination node gets a RREQ packet, it first checks if it has received the RREQ packet previously. If it is a new request and the destination node has enough bandwidth, a reverse route for this session is created, the required bandwidth is reserved for this session and a RREP packet is forwarded along the reverse route to the source node. The RREP packet also includes a session ID

and the QoS extension to indicate the specified QoS flow and required bandwidth. If the destination node already received this RREQ before, it will buffer this RREQ packet until it receives a data packet from the source node.

When a node along the route receives a RREP packet, it first checks its available bandwidth, and if it still has the required bandwidth available, it creates a forward route entry to the destination node according to the session ID, reserves the required bandwidth for the application, and then forwards the RREP packet to the upstream node according to the reverse route of this session. If this node does not have enough bandwidth for the session, it drops the RREP packet, creates a RERR packet, sets the RERR flag to RREPFAIL, and sends this RERR packet to the node that the RREP packet was received from. Any node receiving a RREPFAIL RERR packet will check if it has a forward route entry for this session in its routing table, and if it does, it will invalidate the forward route entry, release the reserved bandwidth and forward the RERR packet to the next node along the forward route until the RERR packet reaches the destination node. At this time, if the destination node has another route available, it will create and transmit a new RREP packet.

In original AODV, the source node sets a lifetime value for every RREQ packet sent out, and when this lifetime expires, the source node will transmit a new RREQ packet, until the number of RREQ packets sent for the application reaches a given MAX RREQ value (set to 3 in [13]). In QS-AODV, we suppose the main reason that the source node cannot find a route to the destination is lack of available bandwidth. Therefore, when the first RREQ for the application expires, a new RREQ packet is sent to find a route to the destination, and the bandwidth parameter in the RREQ packet is degraded to a certain threshold (i.e., 50% of the required bandwidth). If a route still cannot be found, a RREQ packet is sent without any bandwidth requirement. With this adaptation, we can achieve better performance when the traffic is heavy at a cost of decreased application quality.

3.2.2 Route Maintenance

The other significant part of QS-AODV is route maintenance. Those applications using a QoS route will require a route to be rebuilt more quickly than for other applications. For this reason, a different local repair mechanism is used in QS-AODV. We first assume that when a link breaks, it means that the next node along the route is unreachable but the following node along the route will most likely be available. Therefore, unlike local repair in AODV, the upstream node of a broken link sends a local repair request to find the node following the next node along the route to the destination node. This request packet includes the session ID and required bandwidth of the QoS flow, with the TTL (Time To Live) value set to 3, which limits the broadcast area of the local repair request. To allow this mechanism, the following node of the next hop along the route is also recorded in each routing table entry. An example of this local repair mechanism is shown in Fig. 3.3.

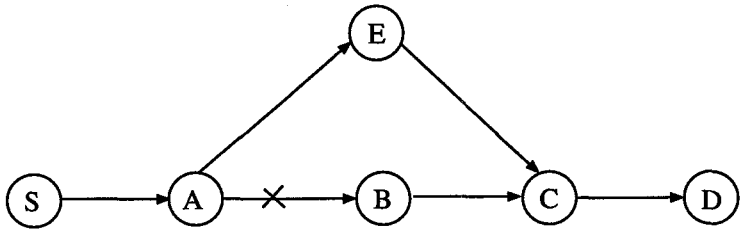

Figure 3.3. *An example of local repair in QS-AODV*

In this example, a route was created as S–A–B–C–D, so that node C follows node B. Then the link between nodes A and B was broken (perhaps because node B moved away), and we assume that node C remained available. Therefore node A sends out a local repair RREQ packet to find node C. When node E receives the RREQ packet, it first checks if it has enough bandwidth for this session. If it does, it creates a reverse route to node A and rebroadcasts the RREQ packet to its neighbor nodes. When node C receives the RREQ packet, if the route entry for this session is still valid, node C generates a local repair RREP packet and sends it back to node A. Node C does not need to do resource reservation because it already reserved the required bandwidth for the session. When Node E receives

the RREP packet, if it still has the required bandwidth available, it creates a forward route entry for the session, reserves the required bandwidth and then forwards the RREP packet back to node A. the new route is then S–A–E–C–D.

If the local repair request expires, the upstream node of the broken link checks which routes are affected by the unavailable next node. A RERR packet is delivered to the corresponding source nodes to notify them that the link is broken. In this RERR packet, the session ID and destination address of each affected session are included. If the session number is more than one, the RERR packet will broadcast to its neighbor nodes, otherwise, the packet is unicast to the upstream node of the route. This local repair mechanism quickly recovers QoS routes and eliminates numerous control packets created due to the frequency of broken links.

3.3 Simulation Environment

Our conclusions are based on the results gathered by extensive simulation of the network model which implements the protocol proposed in the thesis. We use the Network Simulator-2 (ns-2) [44] [45] which can simulate all the layers in the network. It is a popular simulator used for ad hoc networks. Ns-2 has been used with similar mobility and traffic models in many recent performance studies on ad hoc networks, for example [46] [47]. The latest version of the AODV protocol [13] is used for performance comparison. The simulation is trace-driven. A mobility trace for the nodes and session-level traffic trace are inputs to the simulator. The mobility trace provides complete trajectories of all nodes in the network. The session level traffic trace provides information about the start and end times and source-destination pairs of each session.

3.3.1 Traffic and Mobility Model

In our simulations, 20 or 50 nodes move in a rectangular area of 500m X 500m and 1500m X 300m, respectively according to a mobility model called *random waypoint*, as described

Maximum Node Speed (m/s)	1, 5, 10
Pause Time (s)	0, 100, 200, 300, 400, 500, 600, 700, 800, 900
Total Simulation Time (s)	900
Data Packet Rate (packets/s)	4, 8, 20
Packet Size (byte)	512
MAC Protocol	IEEE 802.11b
Propagation Model	Two Ray Ground
Antenna	Omni-directional Antenna

Table 3.1. *Simulation parameters*

in [48]. In this mobility model each node is randomly distributed in the simulation area initially, then it moves towards a random destination and pauses for a certain time after reaching this destination before moving again. When the node reaches the boundary of the simulation area, it reflects back with the same angle of incidence (similar to reflection of light from a mirror). The nodes move at a speed uniformly distributed between $0m/s$ and a maximum speed. The simulations were run for three different maximum speeds: 1, 5 and $10m/s$. For each speed, 10 different simulations were executed with different pause time. Higher pause times reflect lower mobility. 0s indicates a high mobility scenario, while the scenario with 900s pause time is considered as a stable network.

We use Constant-Bit-Rate (CBR) data in the traffic model. Sources generate 512 byte packets at rates of 4 packets/s, 8 packets/s and 20 packets/s, so the application bandwidth requirements are 16kb/s, 32kb/s and 80kb/s, respectively. For 50 nodes network simulation, the number of traffic sources is 10, 20, or 30 sources for each of the packet rates. For 20 nodes, the number of traffic sources is 20 for each CBR packet rate. All simulations were executed for 20 runs. The simulation parameters are shown in Table 3.1.

3.3.2 Other Considerations

IEEE 802.11b is implemented at the MAC layer, which offers a maximum data rate of 2 Mbps. The following assumptions were made:

- There exists a resource reservation protocol which allows the required resources to be reserved at each mobile node along the path.
- There exists a scheduling protocol that allows the system resources to be scheduled appropriately according to the resource reservations.

3.3.3 Parameters Monitored

We evaluated the performance of QS-AODV by measuring three parameters: data packet delivery ratio, normalized routing overhead and end-to-end delay of data packet [46] [49].

- **Data packet delivery ratio:** The data packet delivery ratio is obtained by comparing the number of packets originating at the sources to the number of packets received by the destinations. This is the efficiency of delivering data within the network. This metric is important because it reflects the maximum throughput that the network can support. It also is a measure of the completeness and correctness of the routing protocol.
- **Normalized routing overhead ratio:** This ratio is calculated by comparing the total number of routing packets transmitted during the simulation time to the number of data packets delivered. For packets sent over multiple hops, each transmission of the packet over a hop counts as one transmission. This measure indicates the efficiency of the protocol in expending control overhead to deliver data. The normalized routing overhead ratio is a very important metric for comparing routing protocols, as it measures how a protocol functions in congested or low-bandwidth environments, and the efficiency of consuming network resources (e.g., bandwidth and battery power). Protocols that send large amounts of routing overhead increase the probability of packet

collisions, and data packets may have longer delay in the network interface queues. We only measure and compare the performance of routing protocols, therefore, we do not include IEEE 802.11 MAC packets or ARP (Address Resolution Protocol) packets. Because the routing protocols could use a variety of different medium access or address resolution protocols, each of which would have a different overhead.

- **end-to-end delay:** This delay not only includes the delay in transmitting data packets through the wireless channel, but also the delay in the network interface queue due to network congestion. End-to-end delay is a measure of routing protocol effectiveness.

3.4 Performance Evaluation

We evaluated the performance of QS-AODV by comparing it with AODV. Results are shown for both 20 and 50 node networks. We consider various numbers of sessions with different packet rates and mobility models.

3.4.1 Varying the Number of Sessions and Traffic Loads

From the simulations, we observe that traffic load has a significant impact on QS-AODV and AODV performance. When the traffic is light and application bandwidth requirements are low, sufficient bandwidth can be guaranteed for applications in the network to provide a high packet delivery ratio. When traffic load increases or the required bandwidth for the applications grows, AODV performance drops quickly, and QS-AODV outperforms AODV in this case.

In Figs. 3.4 to 3.12, we measure three performance metrics with 10 sessions and different data rates. We can see that QS-AODV has an almost identical packet delivery ratio to that with AODV, but it needs more routing overhead (10-50% higher) and has a higher delay (by a factor of 1-2). The reason is that AODV has the advantage of using routing information in the intermediate nodes, if the intermediate nodes have "fresh enough" routes to the destination, RREPs can be generated. On the other hand, a RREP packet can only be

generated by the destination node in QS-AODV, which results in more routing overhead and longer time to find a route. As a consequence, AODV has slightly better performance than QS-AODV under light traffic. It can also be observed that when the application bandwidth requirements increase, the performance of QS-AODV and AODV become more similar.

Figs. 3.13 to 3.21 show that when the application bandwidth requirements increase (16kb/s to 80kb/s) with the number of sessions increasing to 20, QS-AODV has better performance than AODV. The packet delivery ratio of AODV is lower than QS-AODV by 1% (Fig. 3.13) to 7% (Fig. 3.15). Each node has an interface buffer to store incoming packets for transmission, which has limited space (50 packets), and packets in the buffer are dropped after 30s. When the required application bandwidth is high, the network becomes congested, and the buffers fill quickly, so the packets will take longer to be sent, and packets will be lost if the buffers are full. The routes created by QS-AODV can guarantee the bandwidth requirements of each session, while AODV only finds the shortest path and is not concerned with available of bandwidth, so the traffic load is more balanced with QS-AODV, and the possibility of packet loss is less with QS-AODV. Furthermore, routes become invalid more easily in AODV due to congested network, resulting in significant routing overhead and longer delays in finding new routes or repairing routes. As a consequence, the routing overhead generated by QS-AODV becomes less than with AODV as the data rate increases (up to 20% lower).

Network congestion is even worse when the number of sessions increases to 30, as shown in Figs. 3.22 to 3.30. In this case, the packet delivery ratio of QS-AODV outperforms that of AODV by 2-12%, and the normalized routing overhead is lower by about 10-30%. The cost of this good performance is longer end-to-end delay because some QoS routes are not the shortest.

3.4.2 Different Mobility Models

Different mobility models were simulated by using different pause times and node speeds. It was observed that the mobility model also has a great impact on the performance of

QS-AODV and AODV, the performance of both protocols with respect to mobility is very similar. In [46] [47] [48], similar observations for AODV were discussed.

In both cases, performance was worse with high mobility, but mobility has a greater impact on QS-AODV than AODV. For example, in Fig. 3.14, with 20 sessions, 8 packets/s packet rate and $10m/s$ maximum speed, the packet delivery ratio of QS-AODV has a lower packet delivery ratio than AODV by 3% at a lower pause time (high mobility). With a higher pause time (low mobility), QS-AODV has a 5% higher packet delivery ratio than AODV. Similar results were observed in other scenarios. With high mobility, AODV creates a route for each required destination, and it benefits from route information stored in the network. QS-AODV creates a route for each session even if they are for the same source and destination, and a RREQ to create a QoS route has to reach the destination before it can be replied. Therefore, a QoS route is harder to find than a best effort route with high mobility, so the difference in routing overhead and delay between AODV and QS-AODV is larger with higher mobility than with lower mobility. With low mobility, routes do not break frequently, so less routing overhead is needed to create and maintain routes, and less delay is required to deliver packets. Therefore, the network is less congested with low mobility, which affects the performance of QS-AODV more than that of AODV.

3.4.3 The Effects of Number of Nodes and Network Size

We now decrease the network size from 1500mx300m to 500mx500m, and the number of nodes from 50 to 20. This results in an increased packet delivery ratio, decreased routing overhead and decreased end-to-end delay for both QS-AODV and AODV, as shown in Figs. 3.31 to 3.39. This is due to the increased network density and decreased network size. In Fig. 3.31, the packet delivery ratio is always greater than 99% for both AODV and QS-AODV, as a 20 node network is small and the traffic is light, so that routes are easily found and repaired. Furthermore, most routes in this 20 node network are 2 to 4 hops long, while routes in the 50 node network are 2 to 8 hops long, so the routing overhead and delay are much less. However, when the traffic is heavy, as shown in Figs. 3.33, 3.36 and 3.39,

network congestion becomes even worse. When an area of the network is congested, a QoS route is likely to be built around it rather than through it as with AODV. As a consequence, QS-AODV has a significant advantage in a small network because it attempts to guarantee sufficient bandwidth for each application.

3.5 Summary

In this chapter, we described the Ad hoc On-demand Distance Vector routing protocol. The operations of route discovery and maintenance of AODV were introduced. A solution (QS-AODV) was proposed to provide QoS assurance, and the difference between QS-AODV and AODV was presented. Simulation environments were introduced and results under a number of scenarios were given to show the effectiveness of our approach. It is clear that QS-AODV has better performance under heavy traffic. Network size and mobility also affect the performance of both protocols.

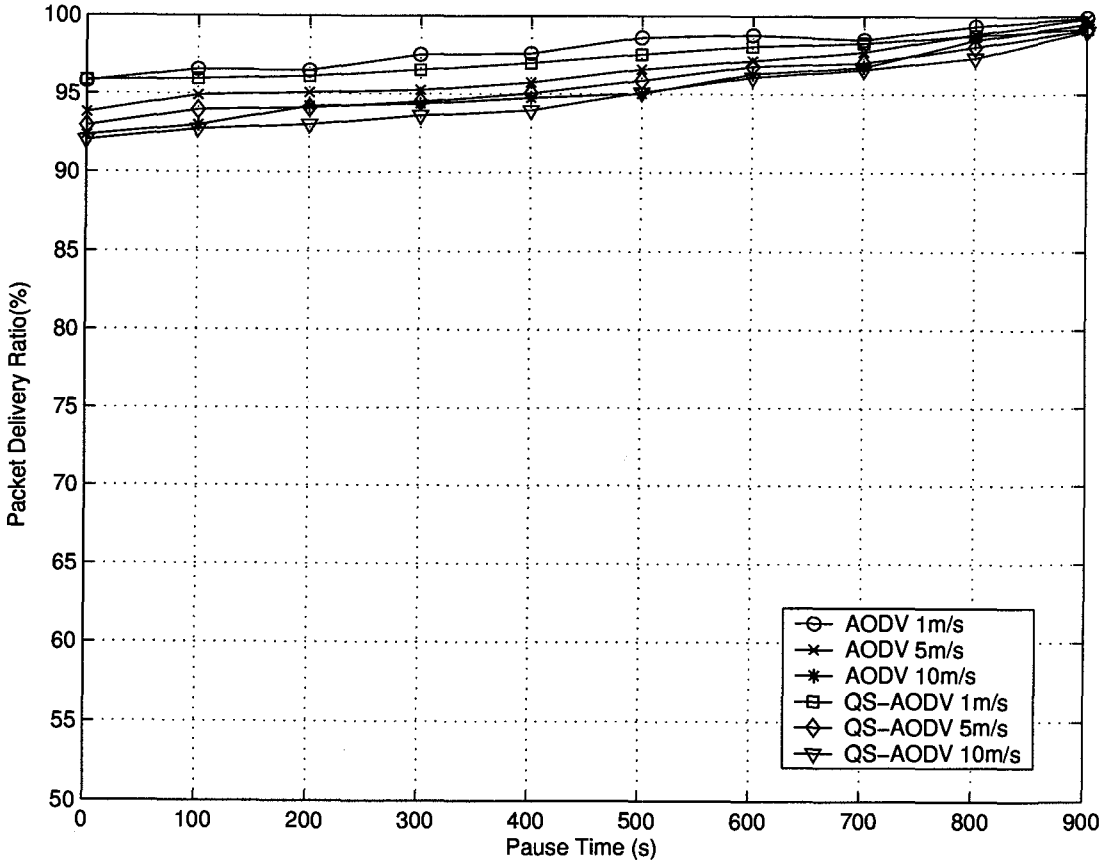

Figure 3.4. *Packet delivery ratio with 50 nodes, 10 sessions and 4 packets/s.*

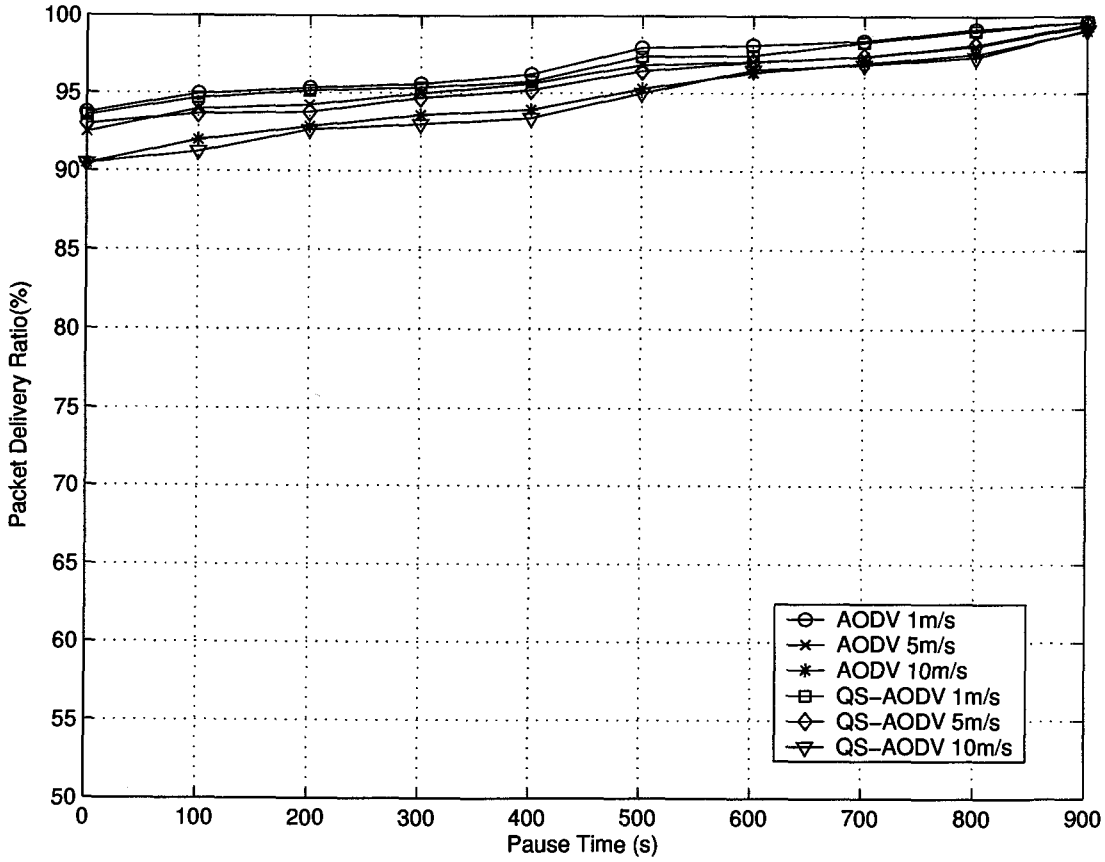

Figure 3.5. *Packet delivery ratio with 50 nodes, 10 sessions and 8 packets/s,*

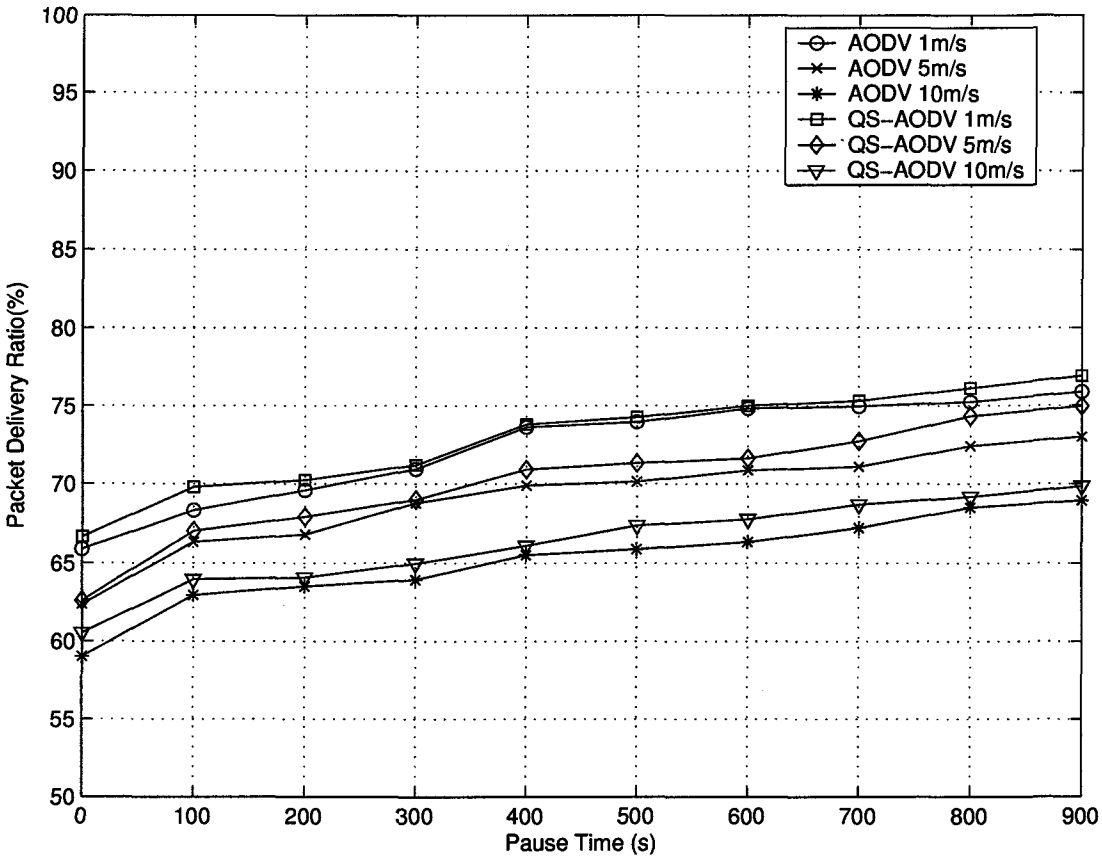

Figure 3.6. *Packet delivery ratio with 50 nodes, 10 sessions and 20 packets/s,*

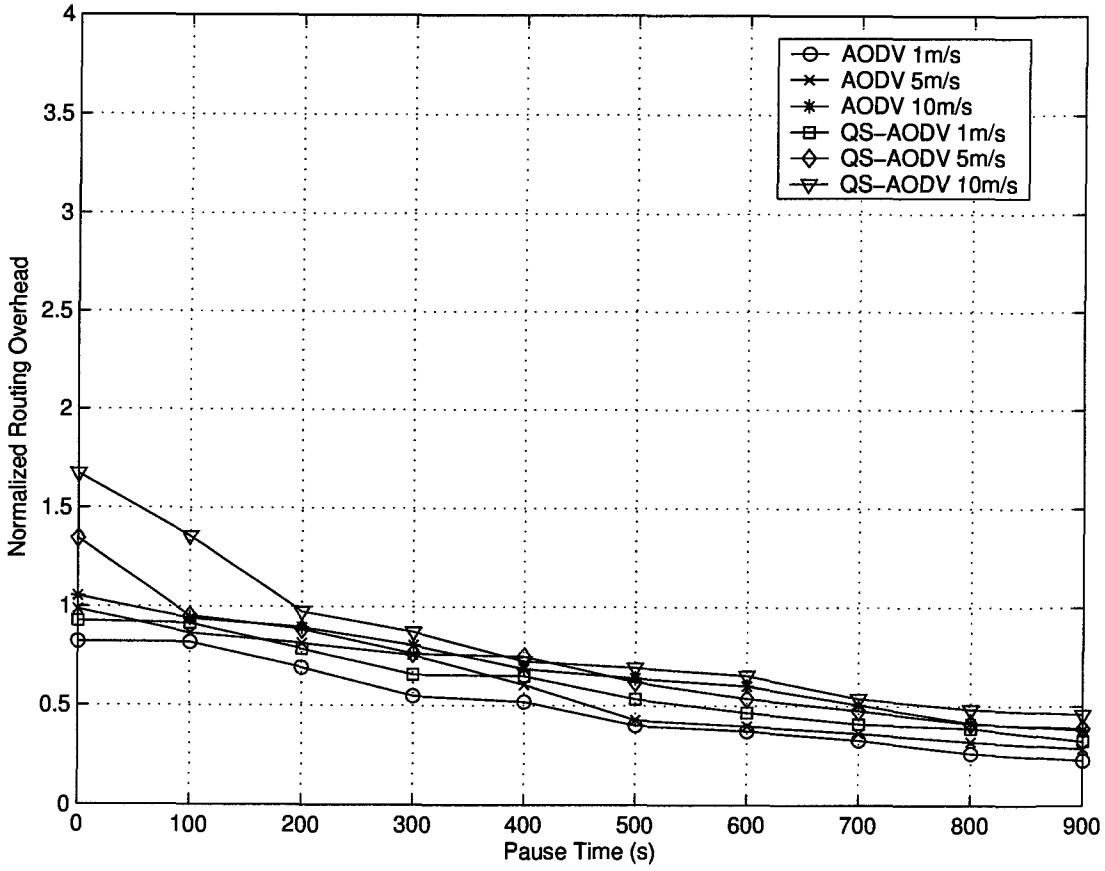

Figure 3.7. *Normalized routing overhead with 50 nodes, 10 sessions and 4 packets/s,*

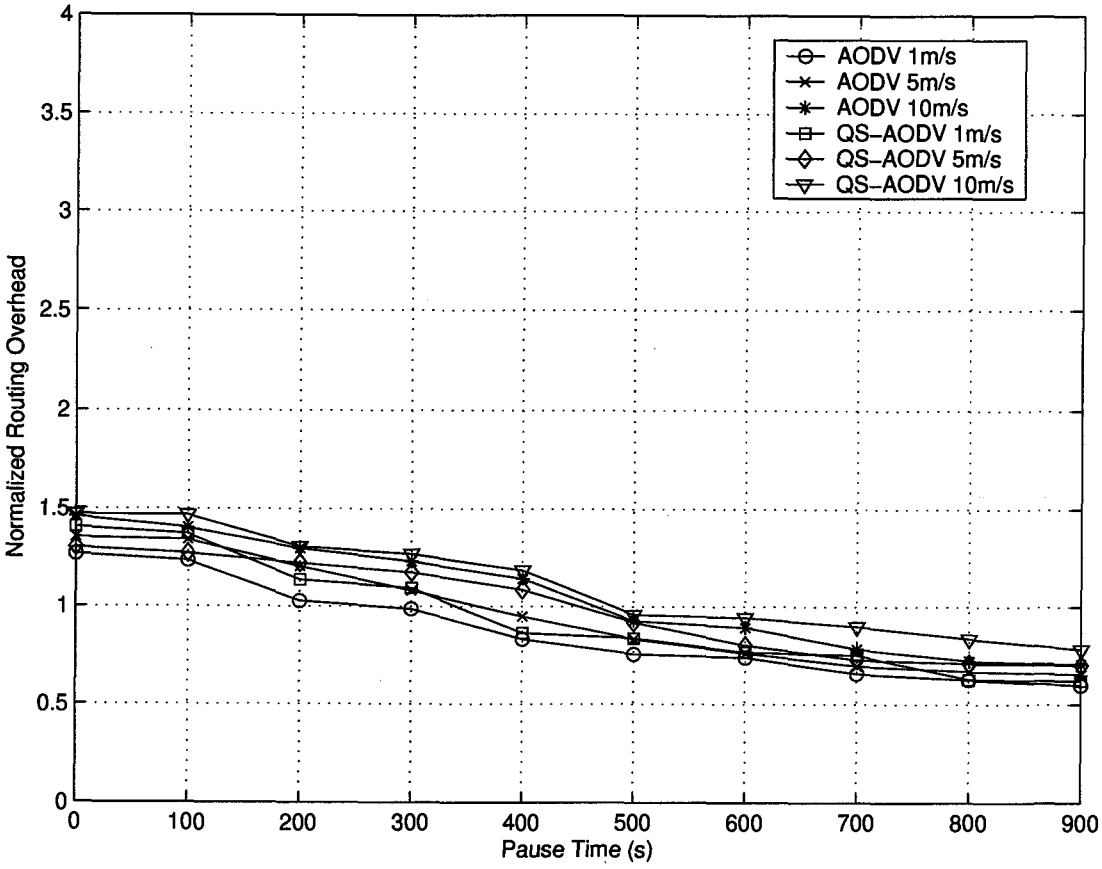

Figure 3.8. *Normalized routing overhead with 50 nodes, 10 sessions and 8 packets/s,*

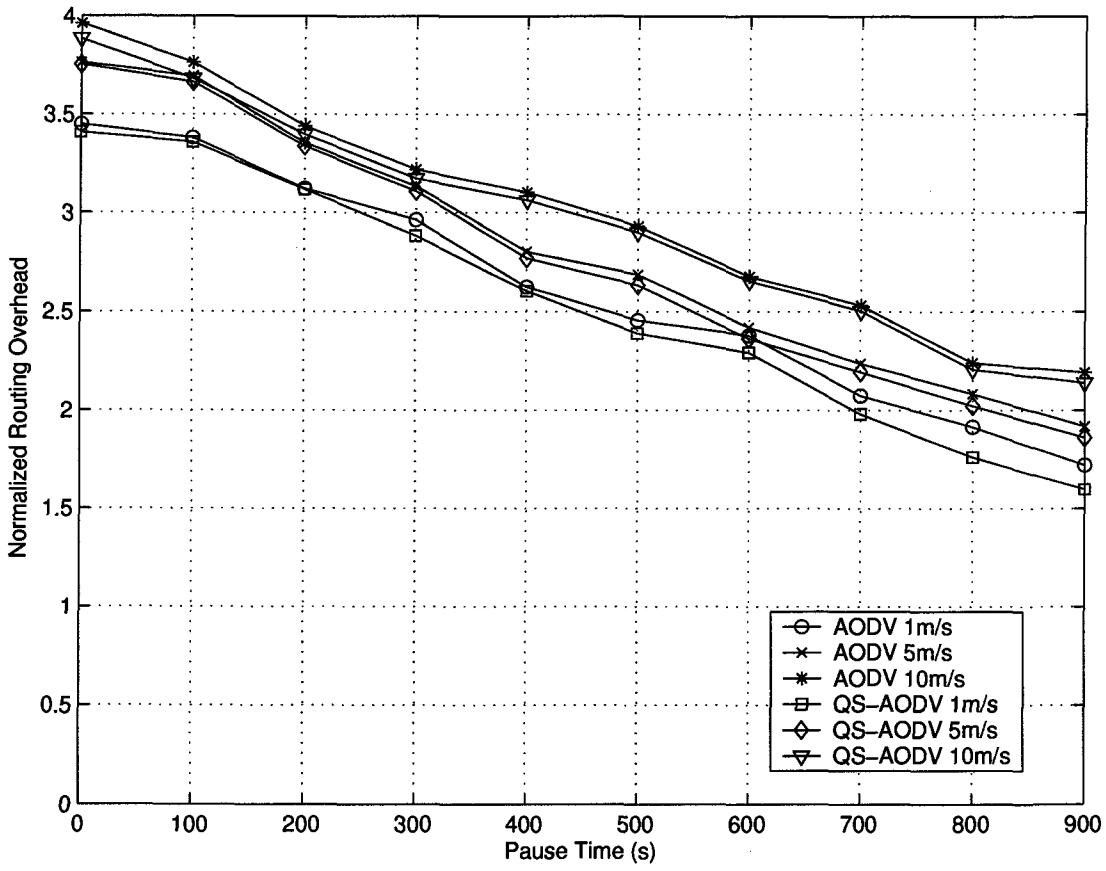

Figure 3.9. *Normalized routing overhead with 50 nodes, 10 sessions and 20 packets/s,*

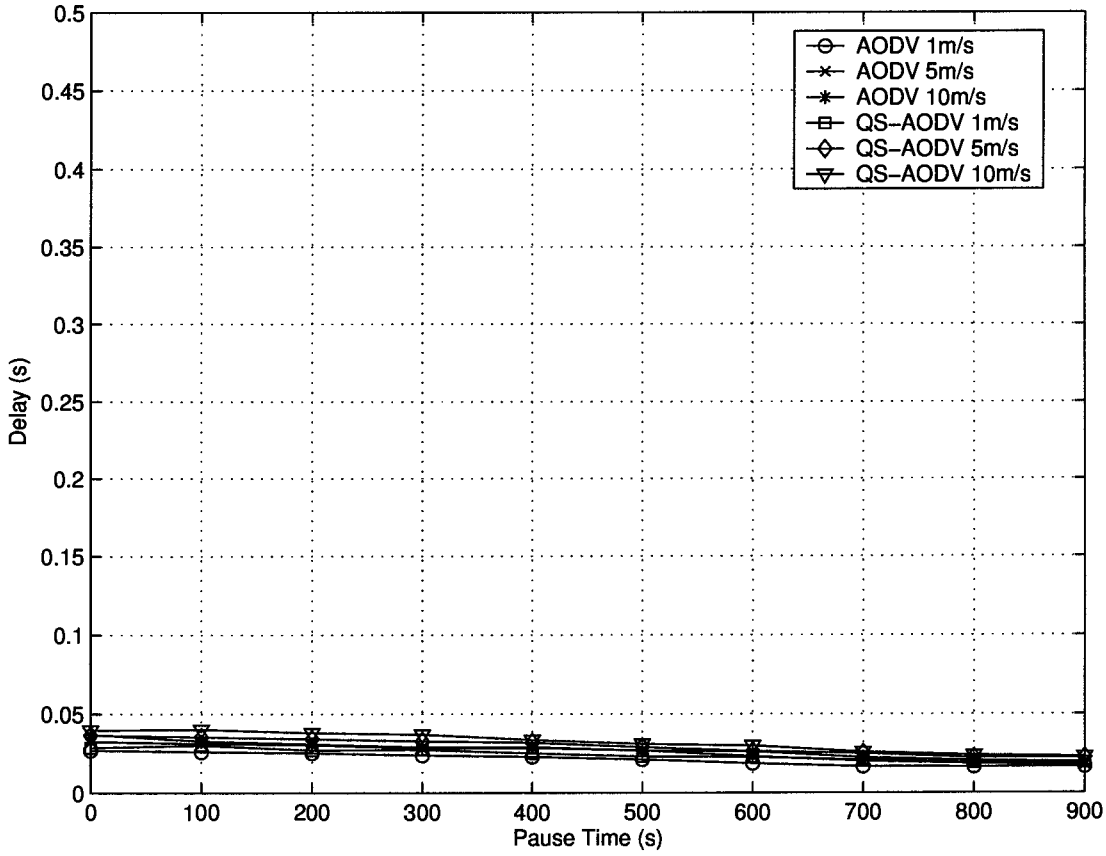

Figure 3.10. *Delay with 50 nodes, 10 sessions and 4 packets/s,*

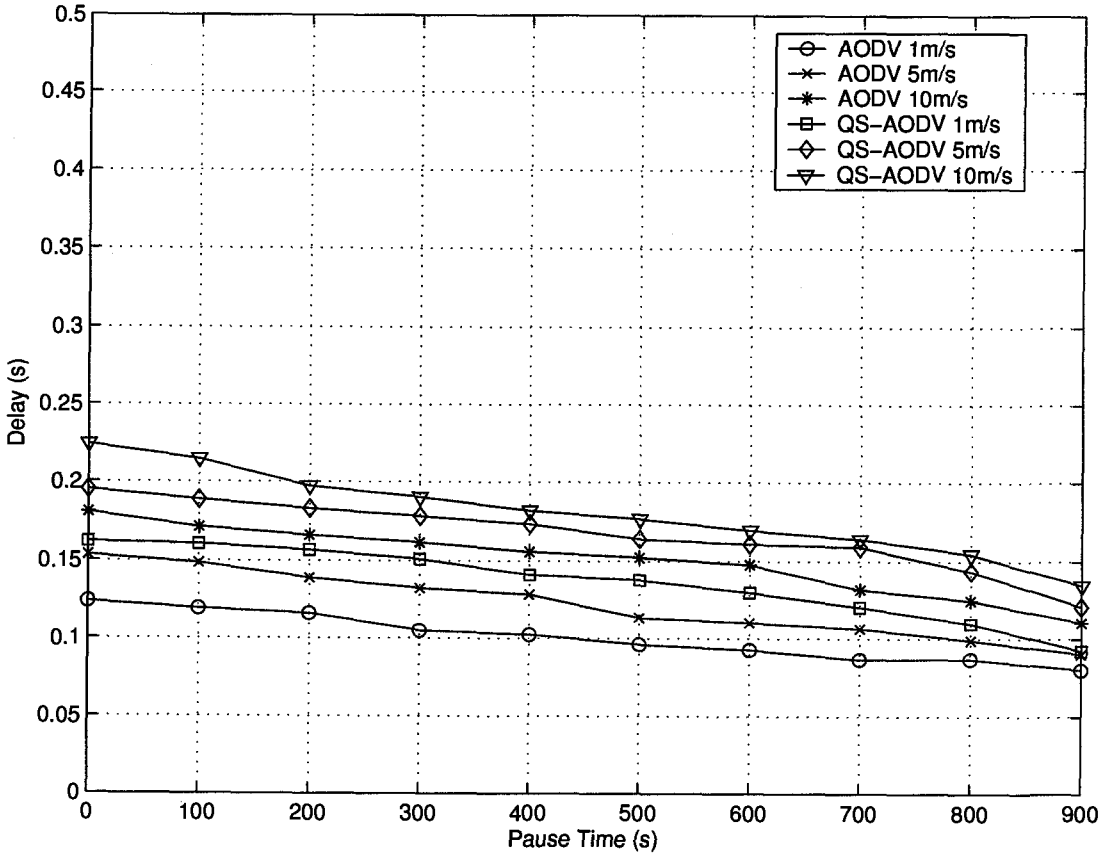

Figure 3.11. *Delay with 50 nodes, 10 sessions and 8 packets/s,*

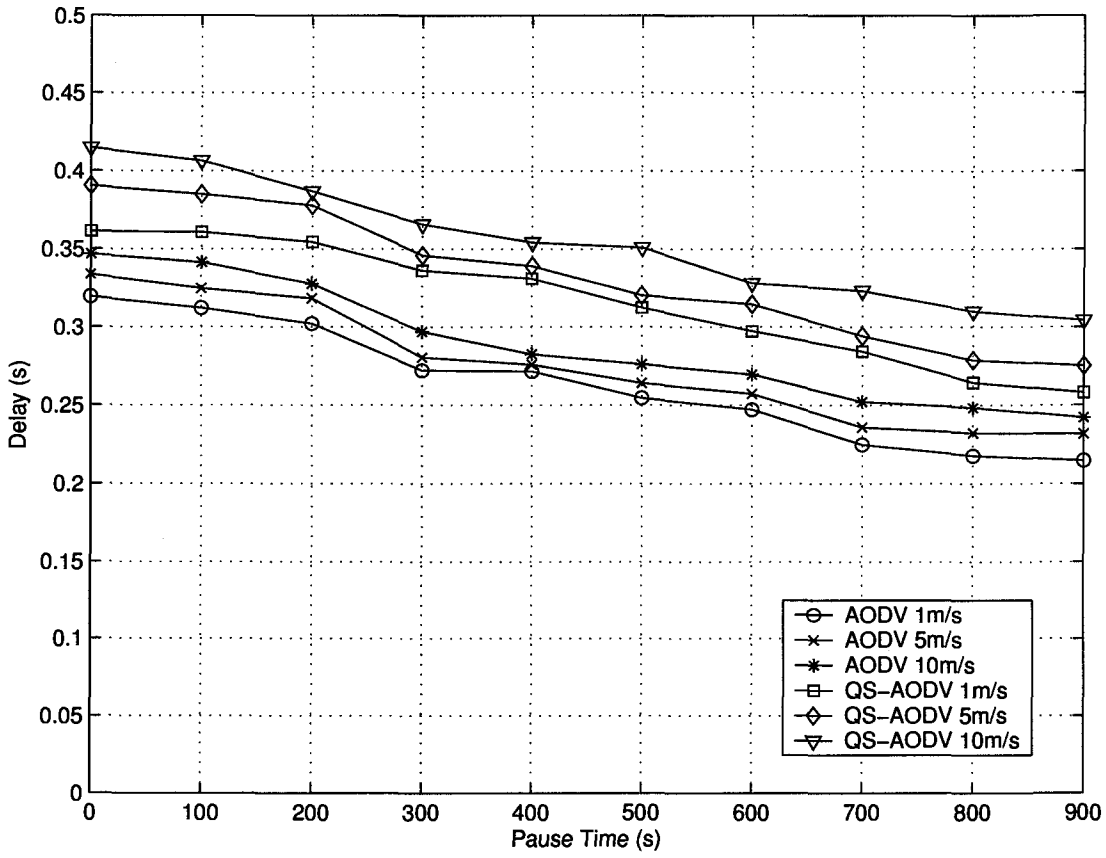

Figure 3.12. *Delay with 50 nodes, 10 sessions and 20 packets/s,*

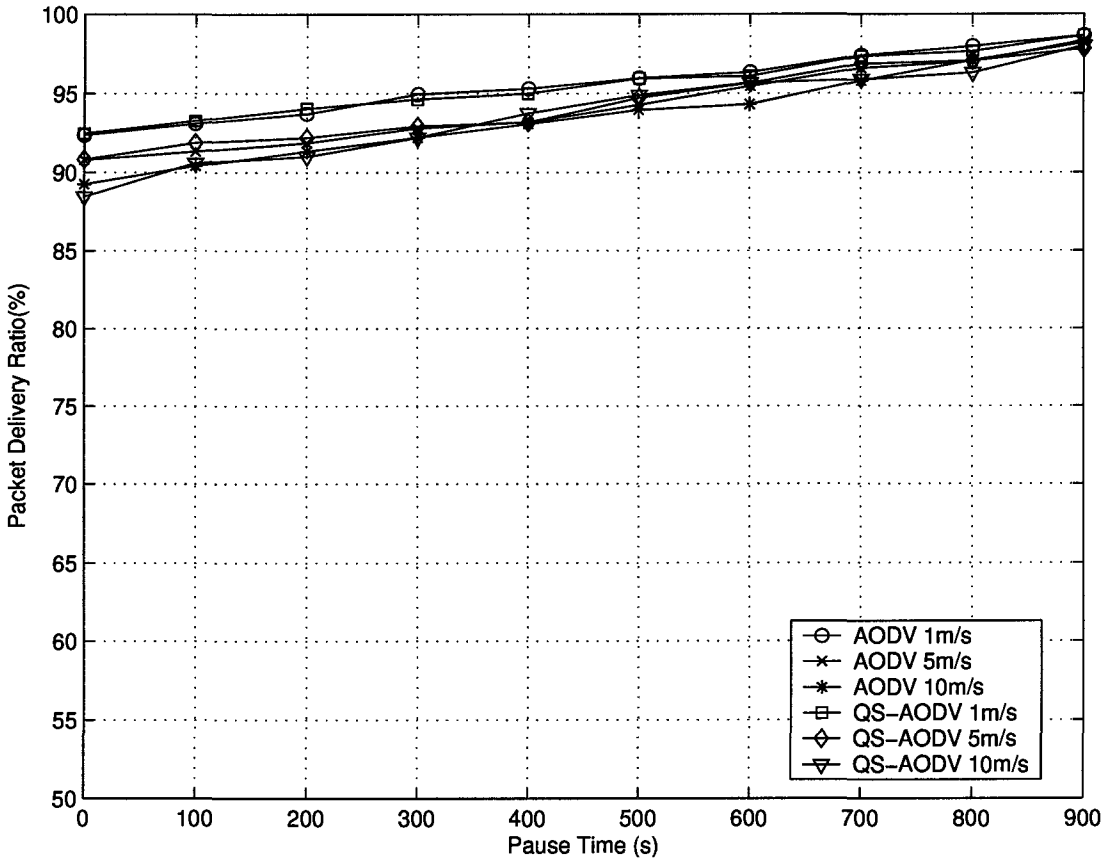

Figure 3.13. *Packet delivery ratio with 50 nodes, 20 sessions and 4 packets/s,*

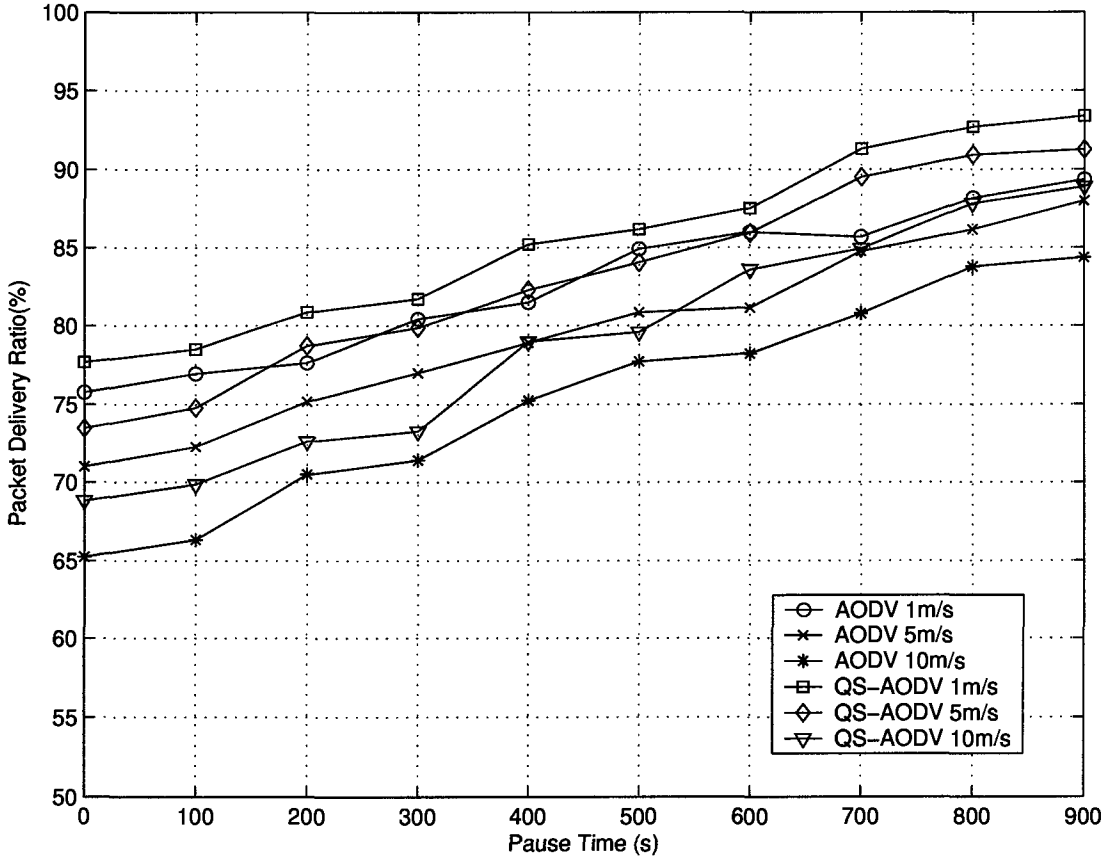

Figure 3.14. *Packet delivery ratio with 50 nodes, 20 sessions and 8 packets/s,*

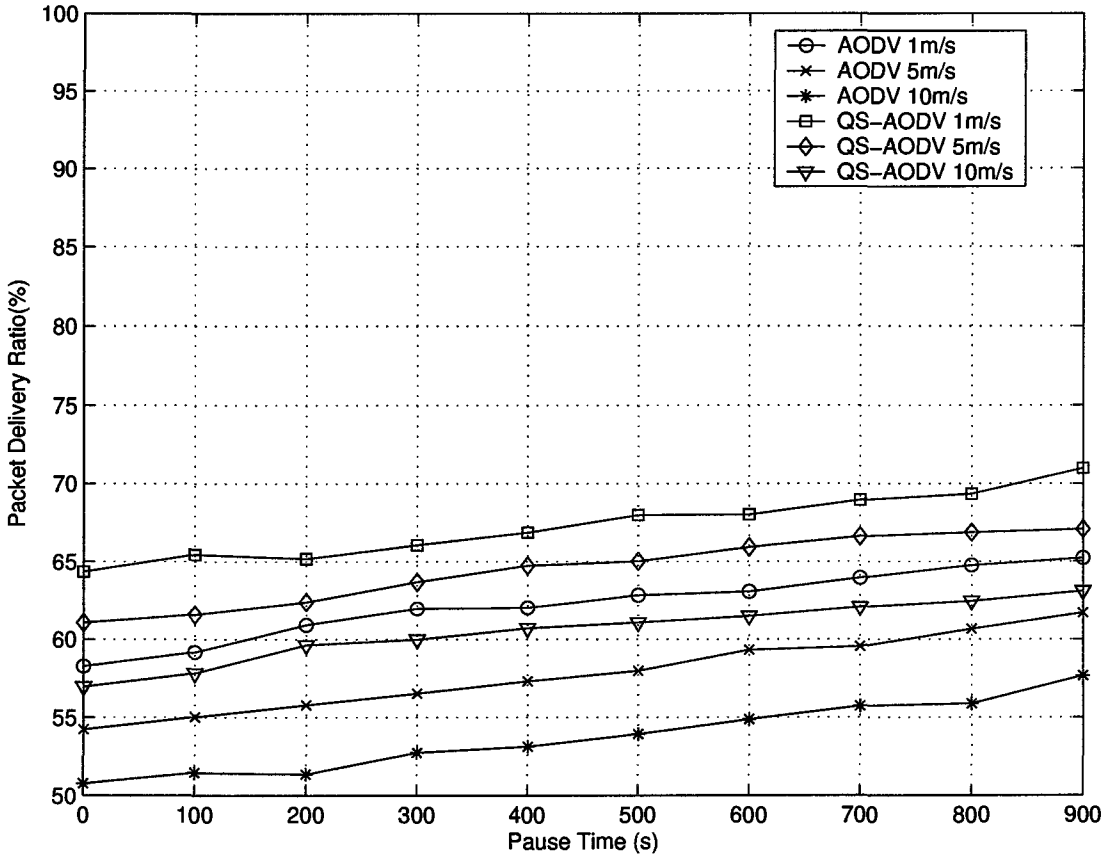

Figure 3.15. *Packet delivery ratio with 50 nodes, 20 sessions and 20 packets/s,*

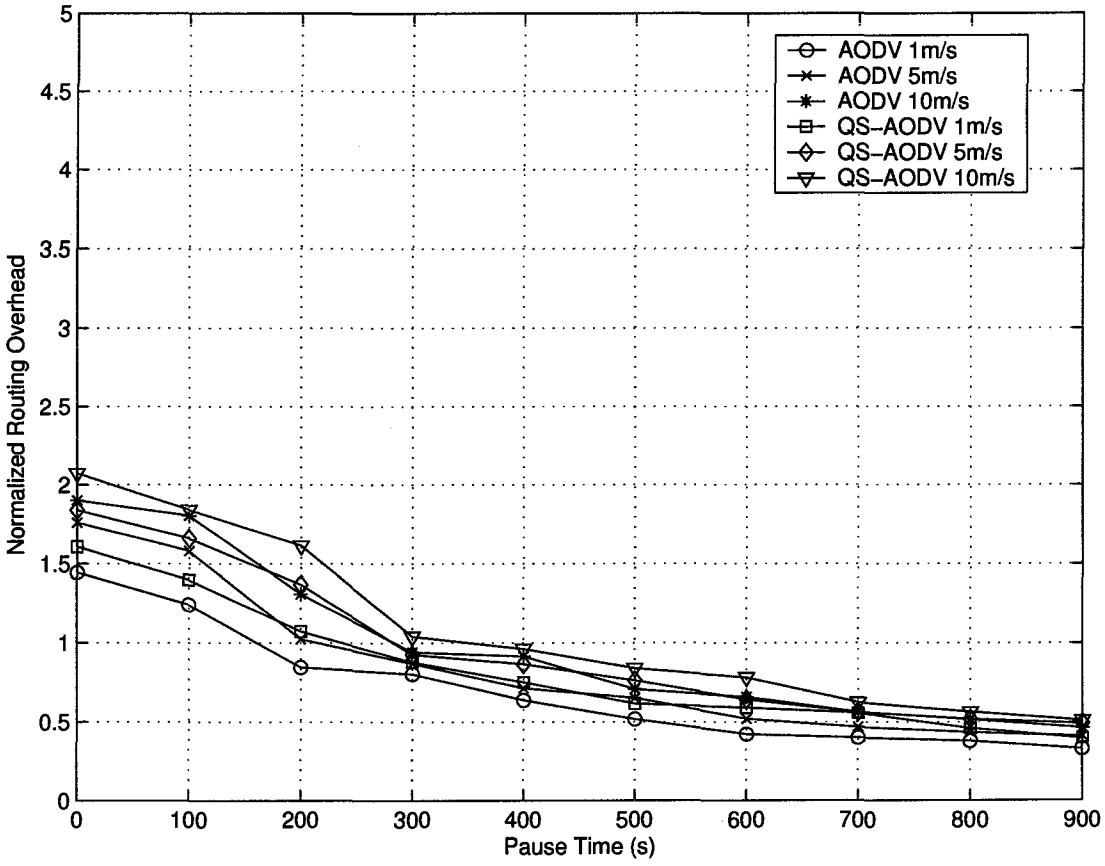

Figure 3.16. *Normalized routing overhead with 50 nodes, 20 sessions and 4 packets/s,*

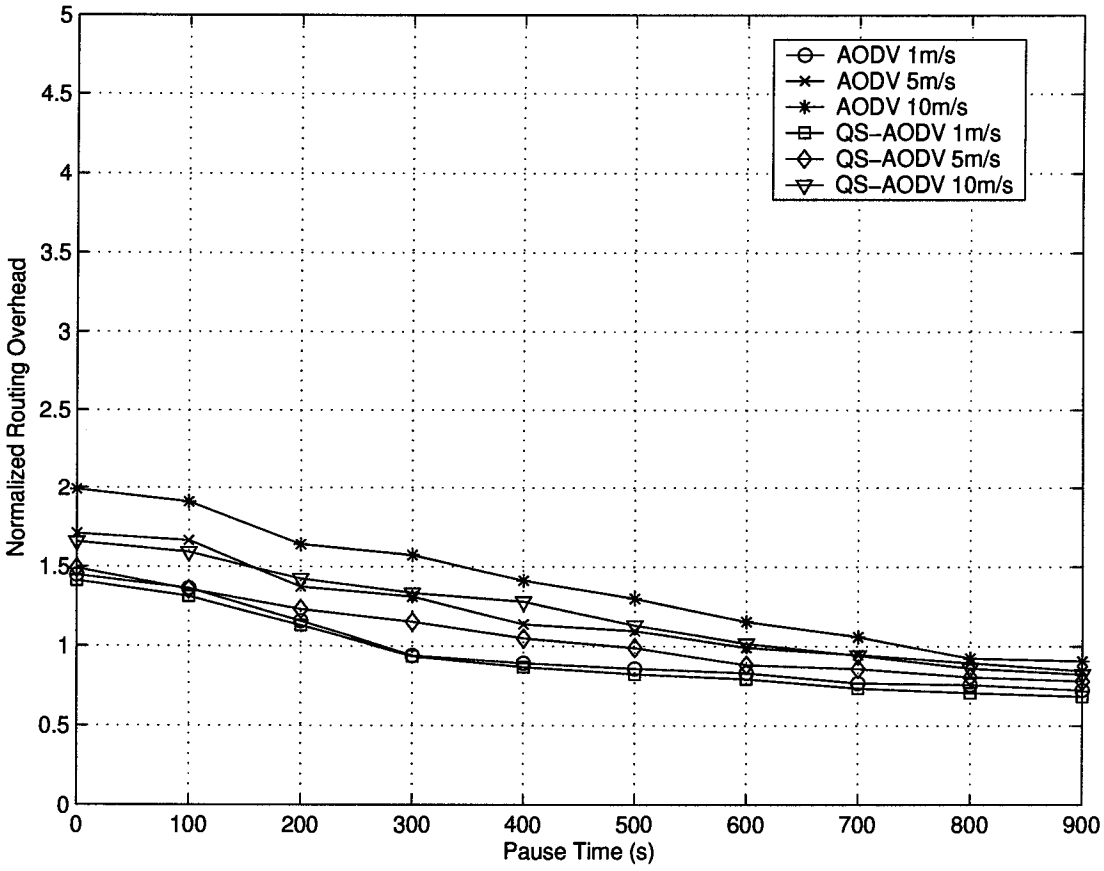

Figure 3.17. *Normalized routing overhead with 50 nodes, 20 sessions and 8 packets/s,*

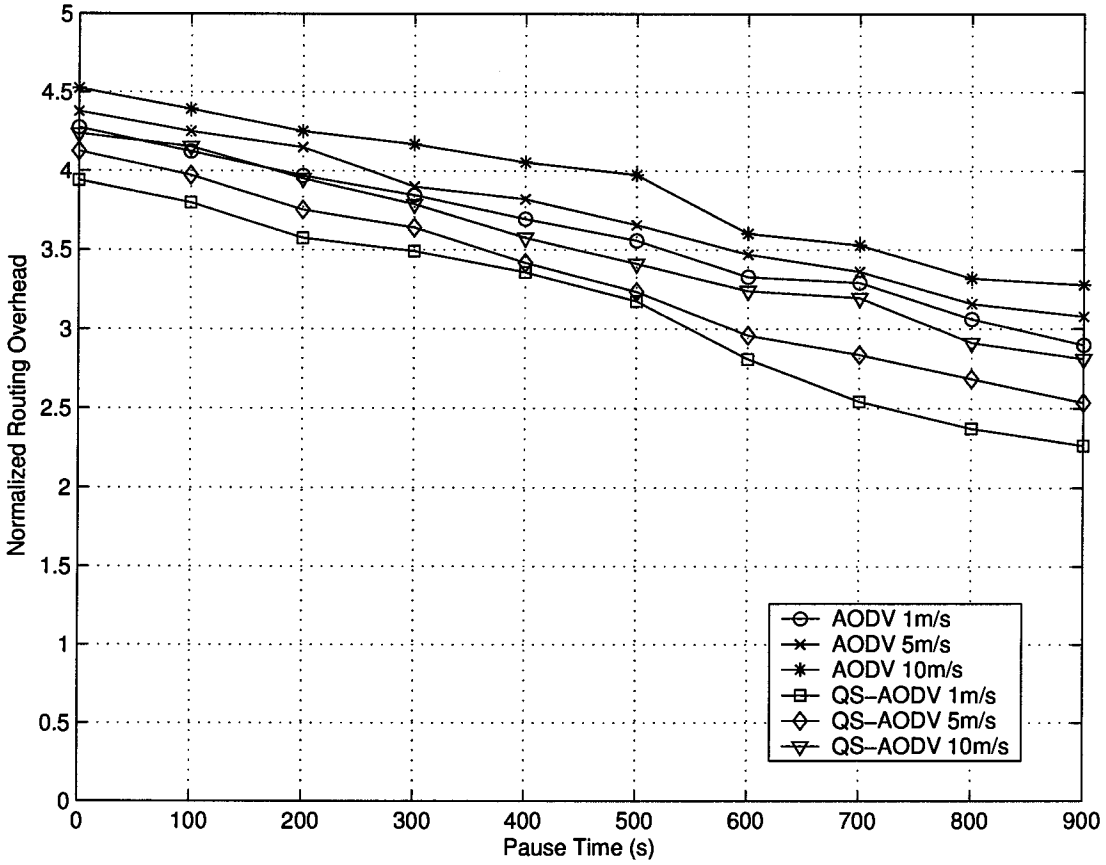

Figure 3.18. *Normalized routing overhead with 50 nodes, 20 sessions and 20 packets/s,*

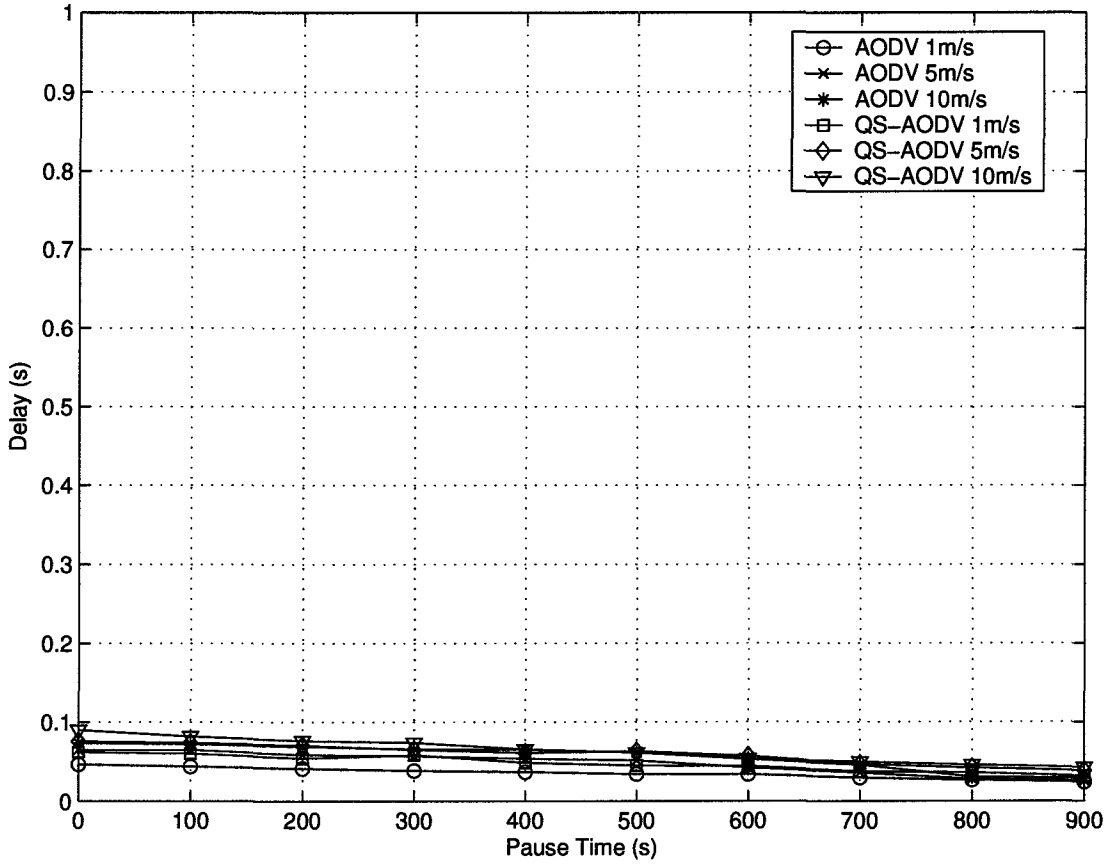

Figure 3.19. *Delay with 50 nodes, 20 sessions and 4 packets/s,*

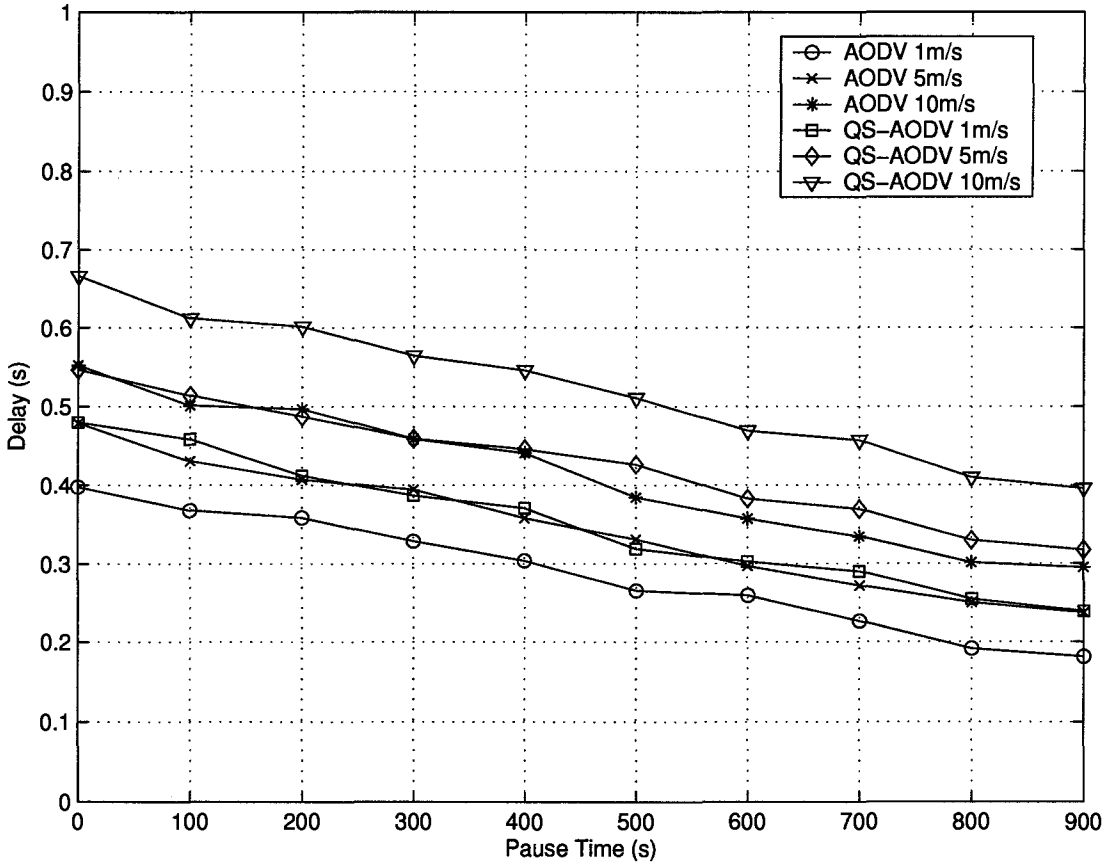

Figure 3.20. *Delay with 50 nodes, 20 sessions and 8 packets/s,*

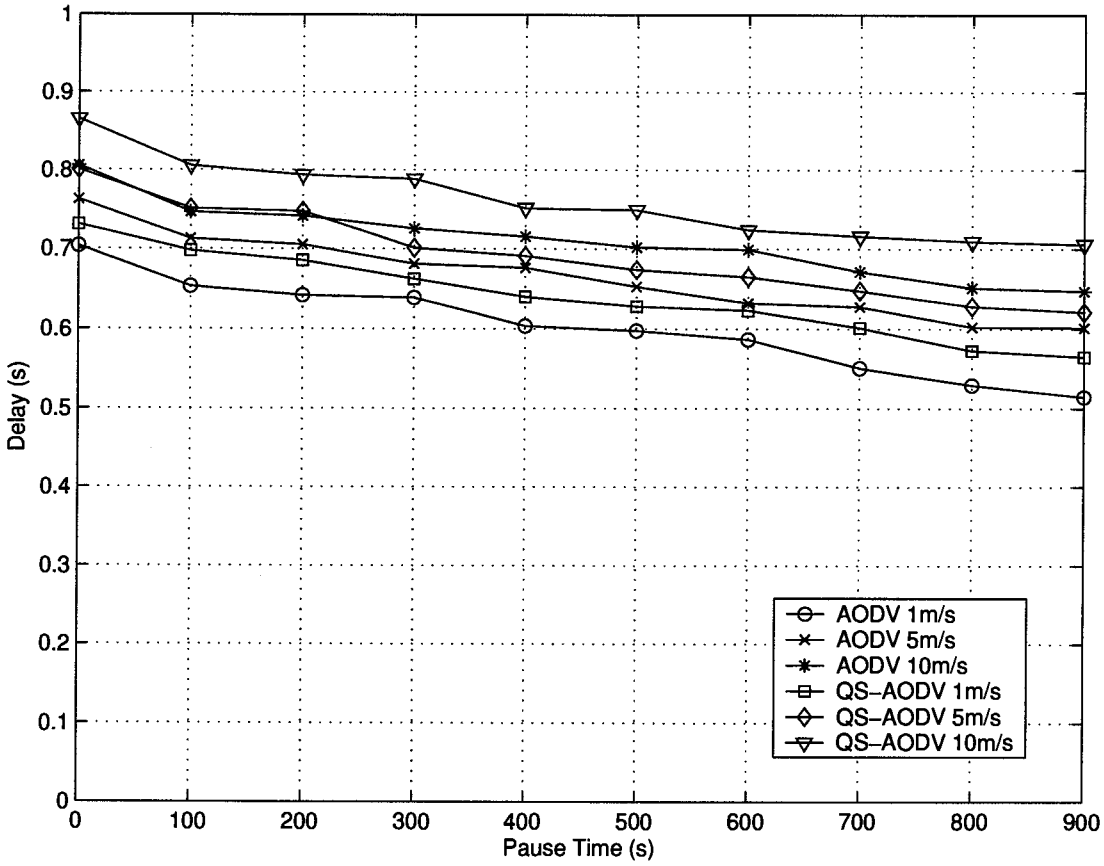

Figure 3.21. *Delay with 50 nodes, 20 sessions and 20 packets/s,*

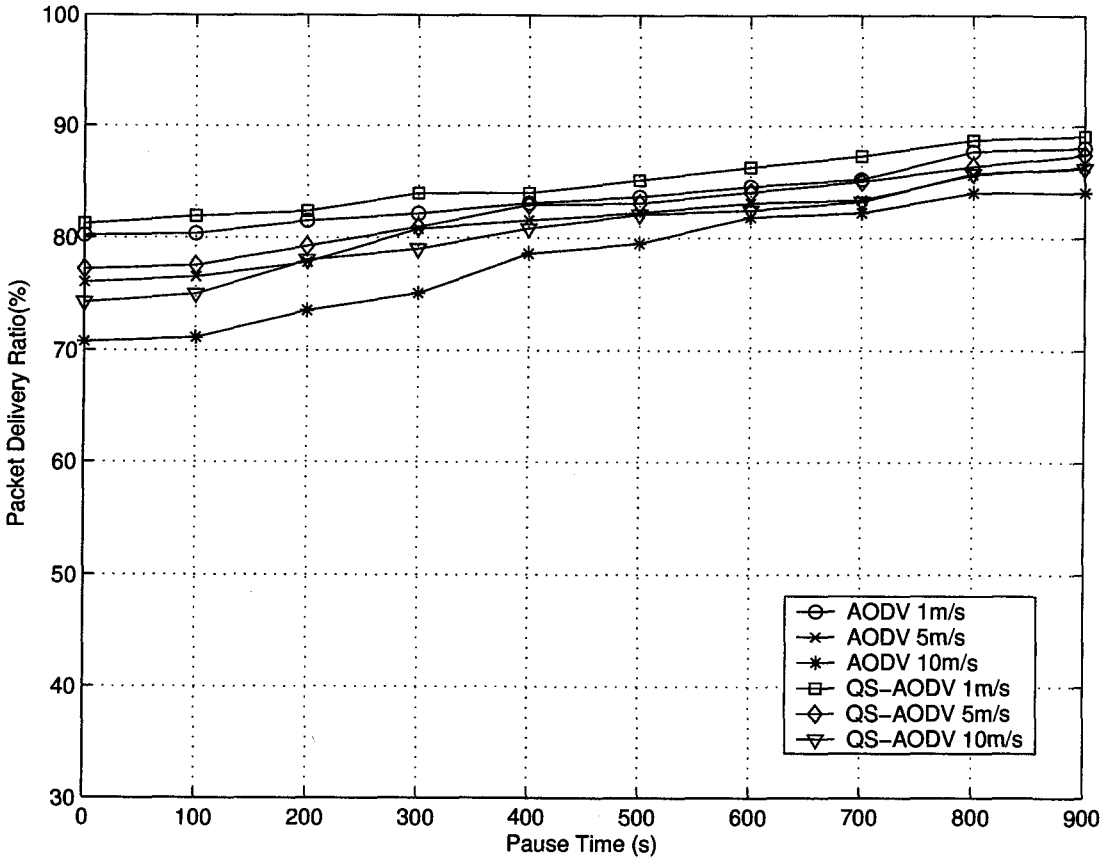

Figure 3.22. *Packet delivery ratio with 50 nodes, 30 sessions and 4 packets/s,*

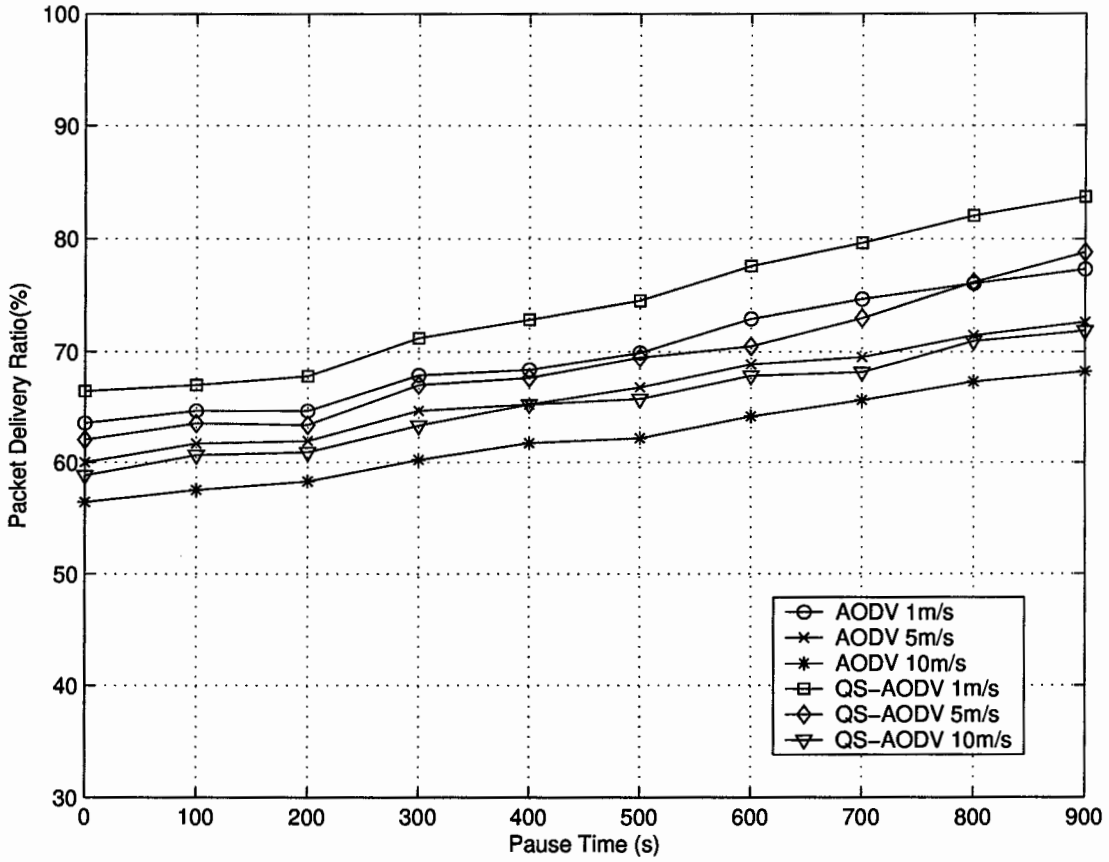

Figure 3.23. *Packet delivery ratio with 50 nodes, 30 sessions and 8 packets/s,*

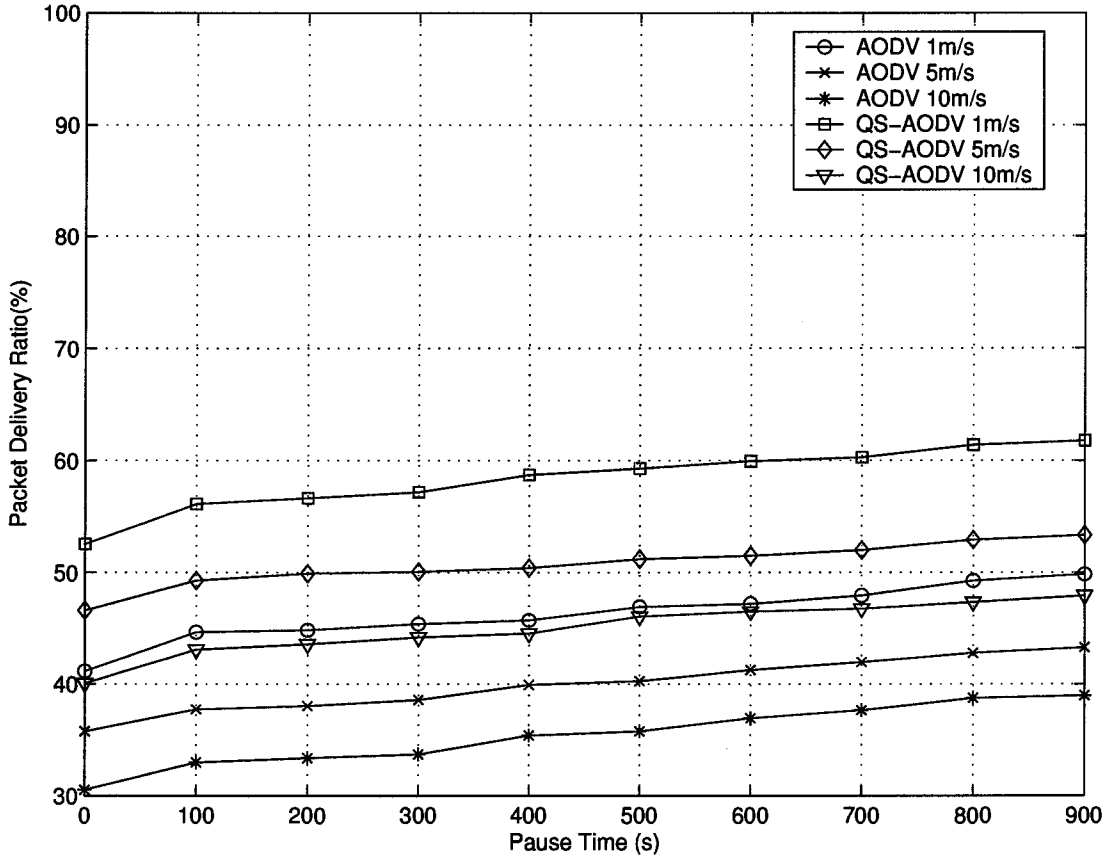

Figure 3.24. *Packet delivery ratio with 50 nodes, 30 sessions and 20 packets/s,*

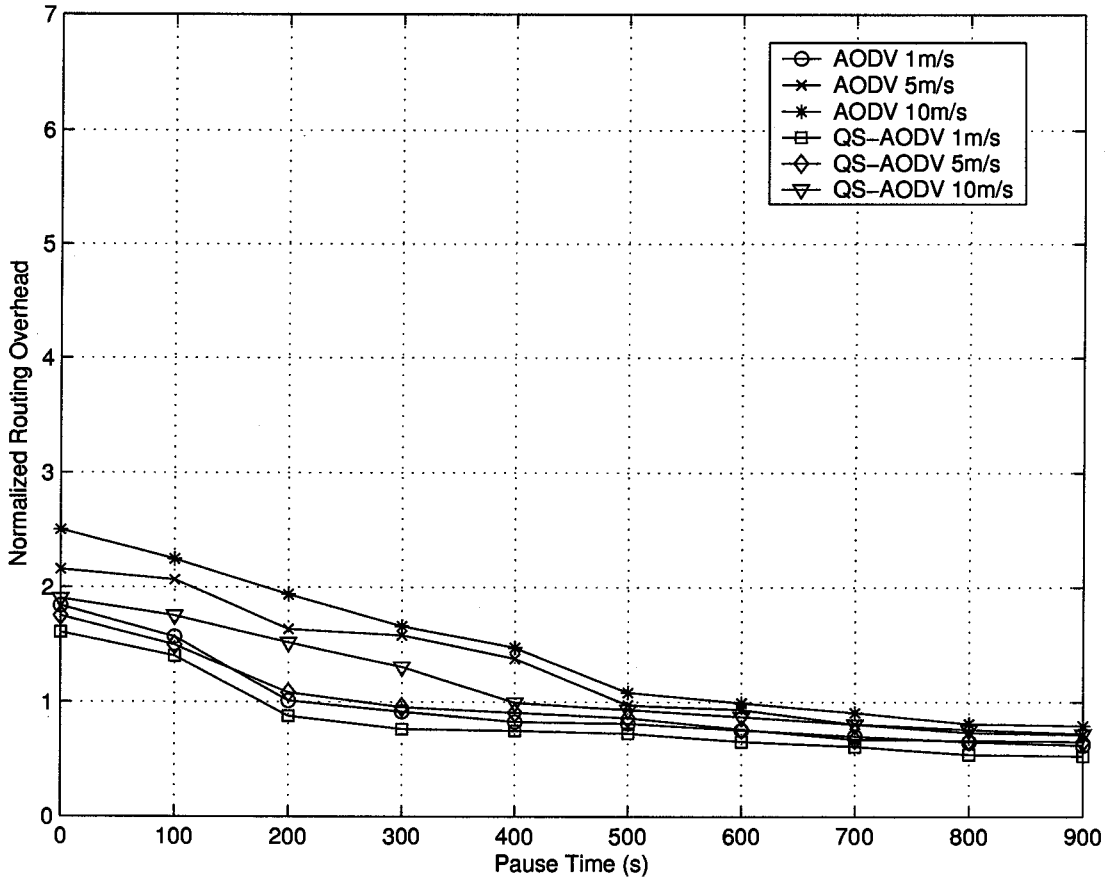

Figure 3.25. *Normalized routing overhead with 50 nodes, 30 sessions and 4 packets/s,*

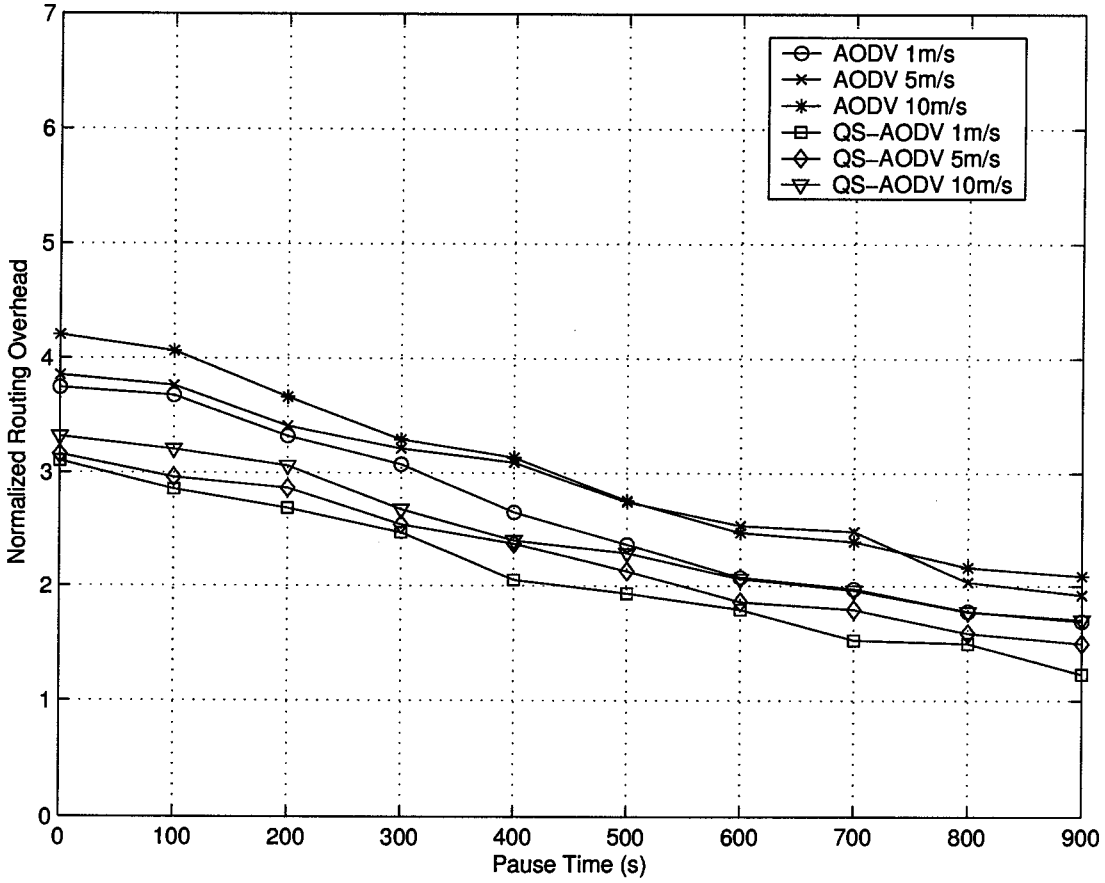

Figure 3.26. *Normalized routing overhead with 50 nodes, 30 sessions and 8 packets/s,*

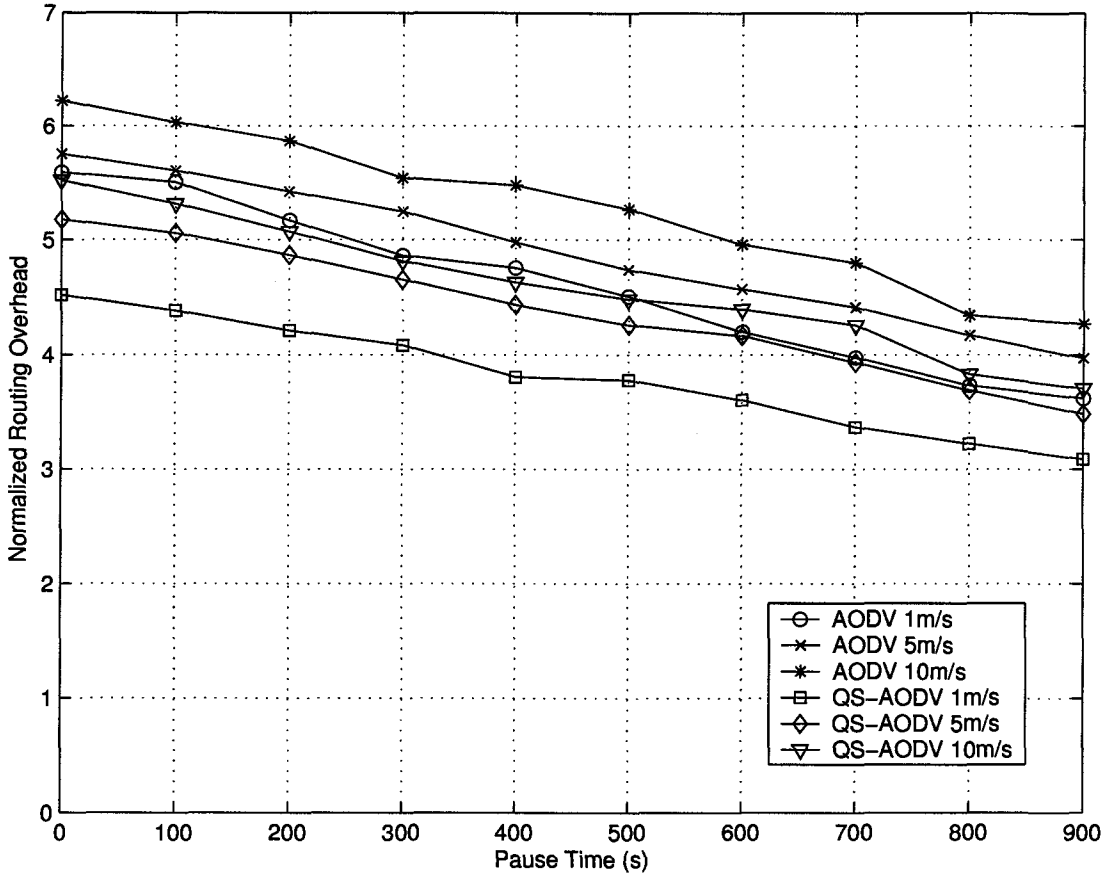

Figure 3.27. *Normalized routing overhead with 50 nodes, 30 sessions and 20 packets/s,*

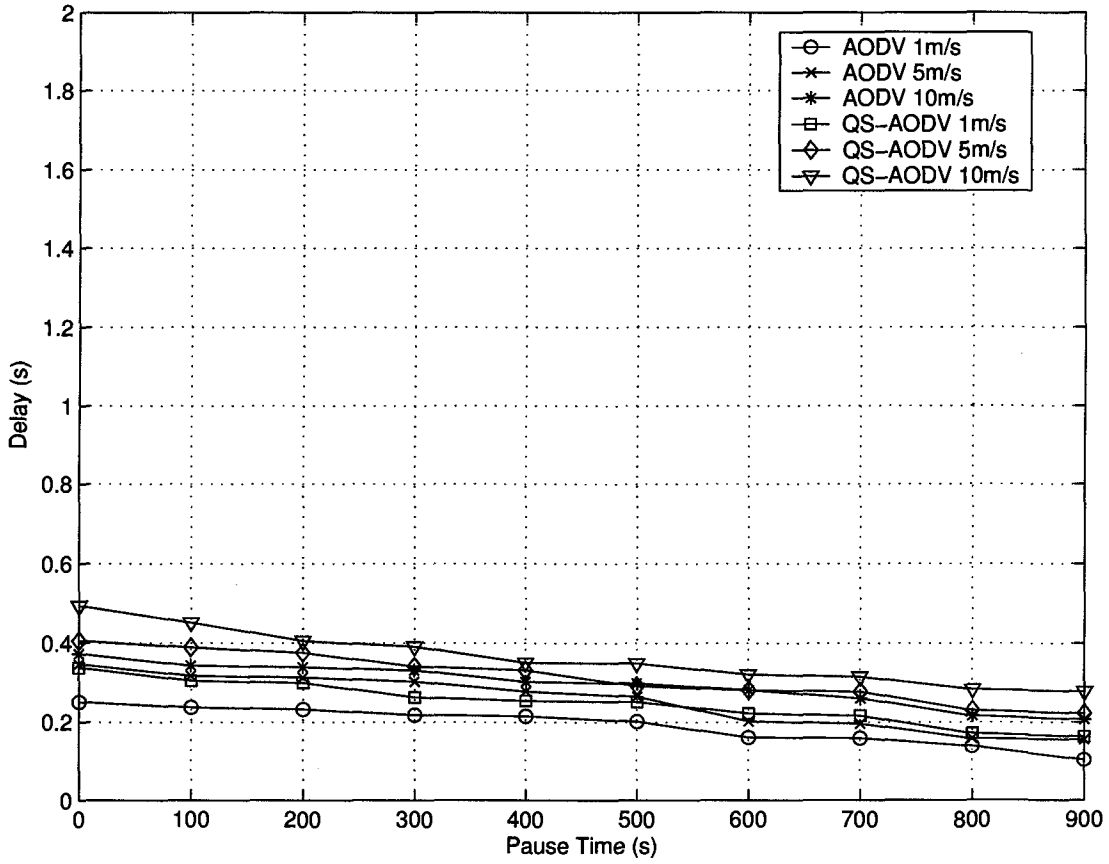

Figure 3.28. *Delay with 50 nodes, 30 sessions and 4 packets/s,*

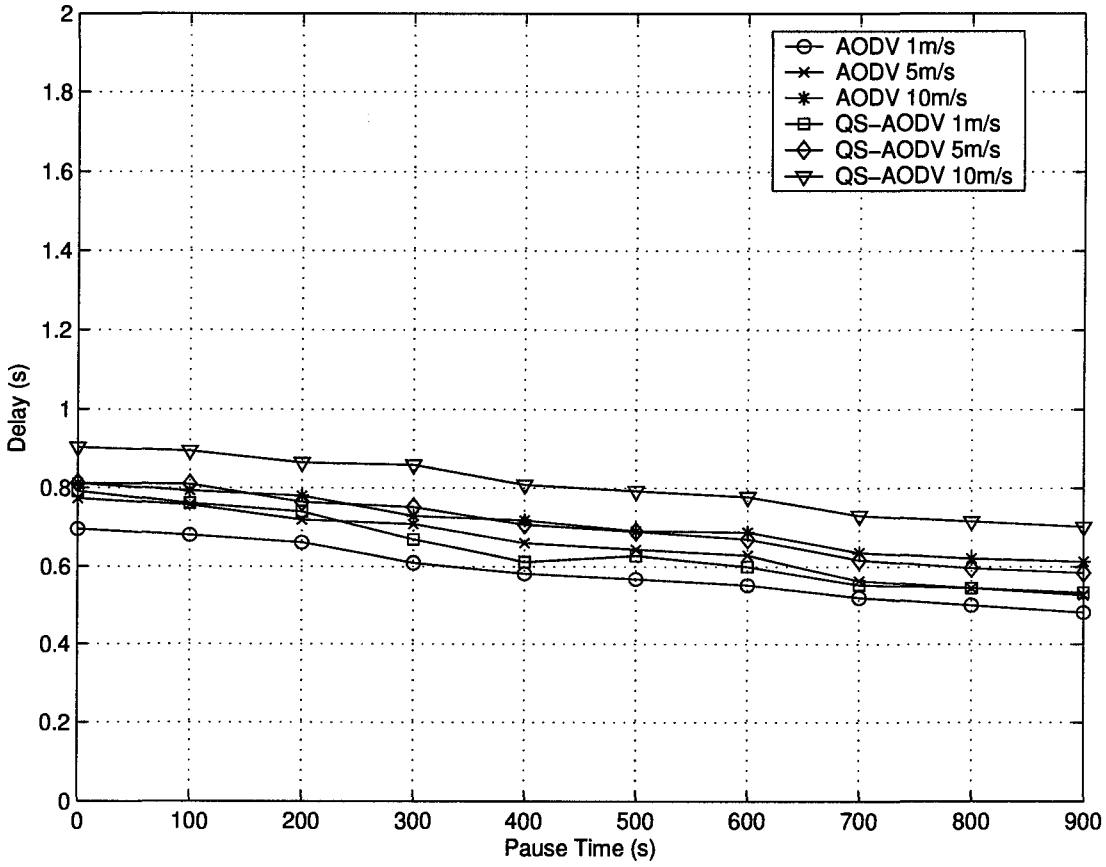

Figure 3.29. *Delay with 50 nodes, 30 sessions and 8 packets/s,*

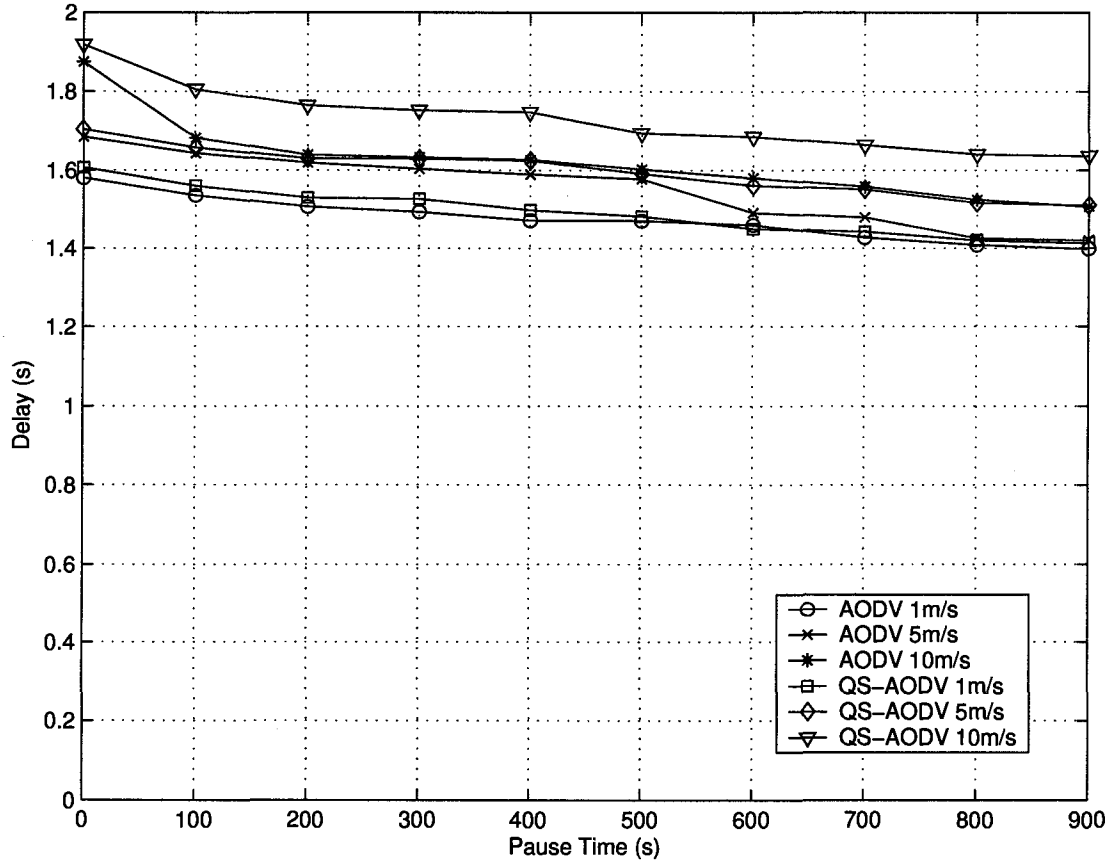

Figure 3.30. *Delay with 50 nodes, 30 sessions and 20 packets/s,*

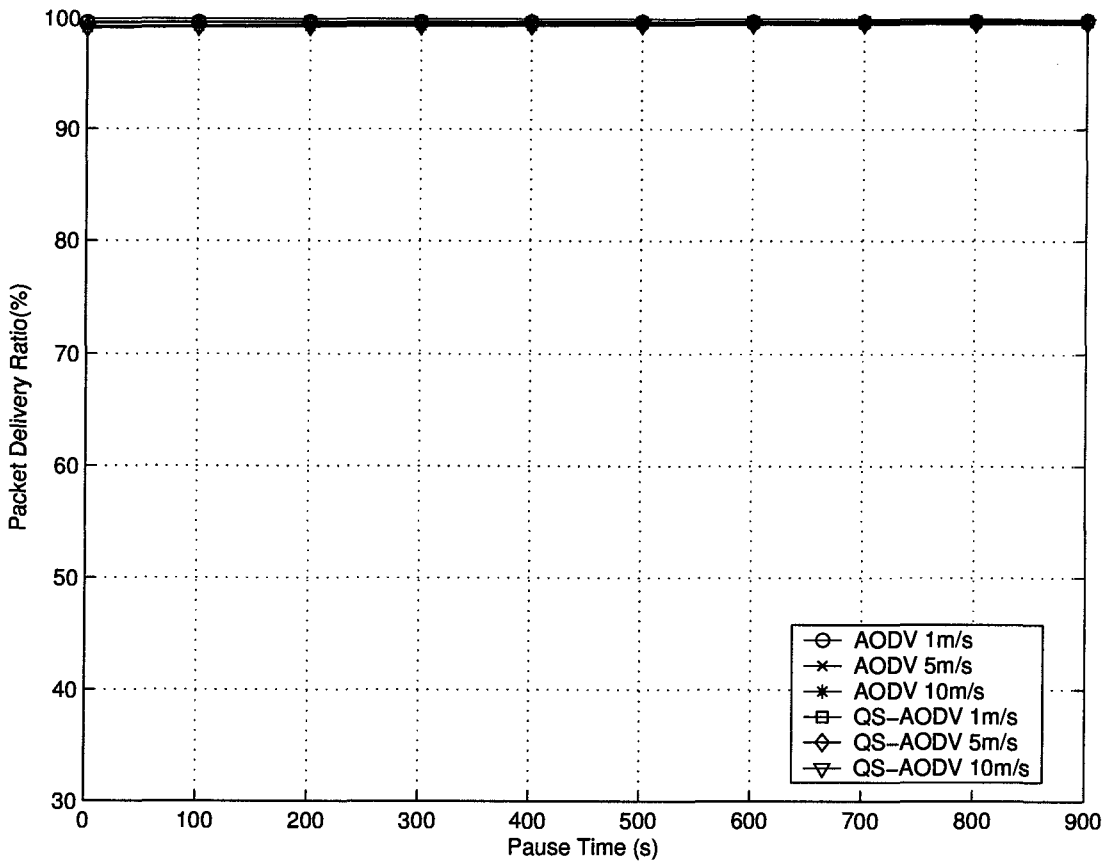

Figure 3.31. *Packet delivery ratio with 20 nodes, 20 sessions and 4 packets/s,*

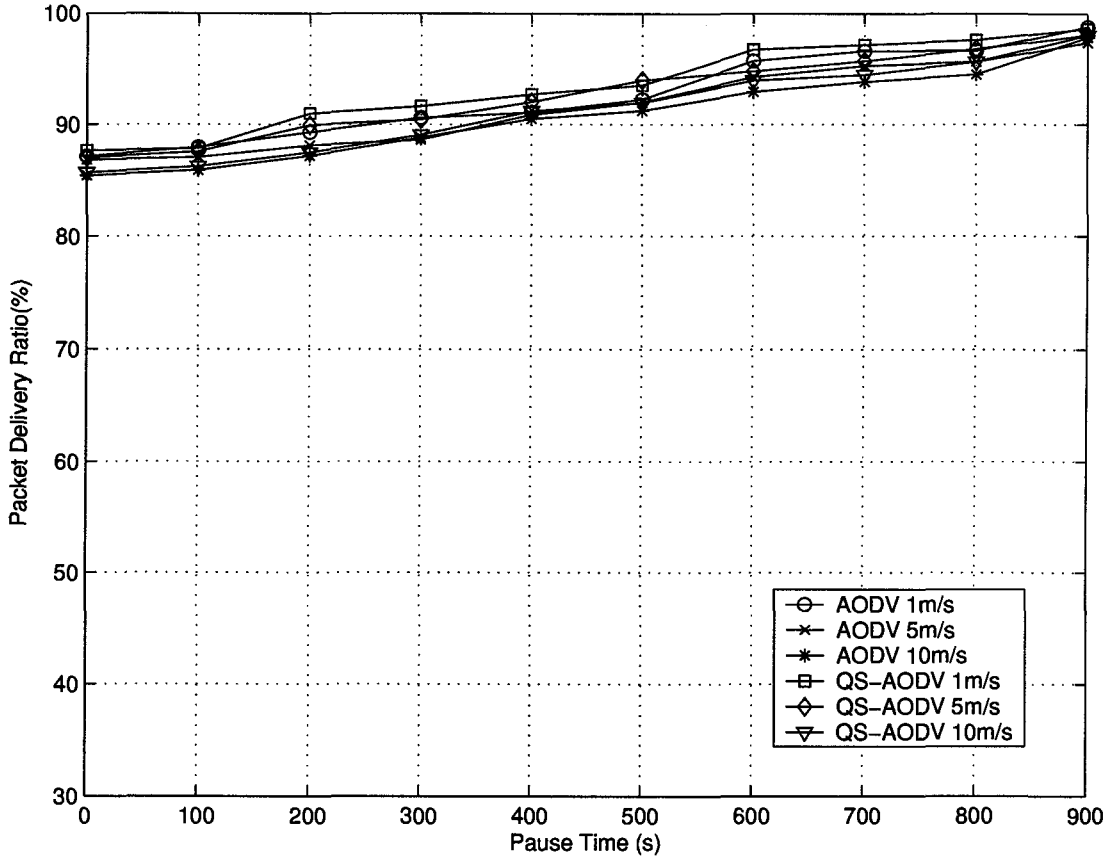

Figure 3.32. *Packet delivery ratio with 20 nodes, 20 sessions and 8 packets/s,*

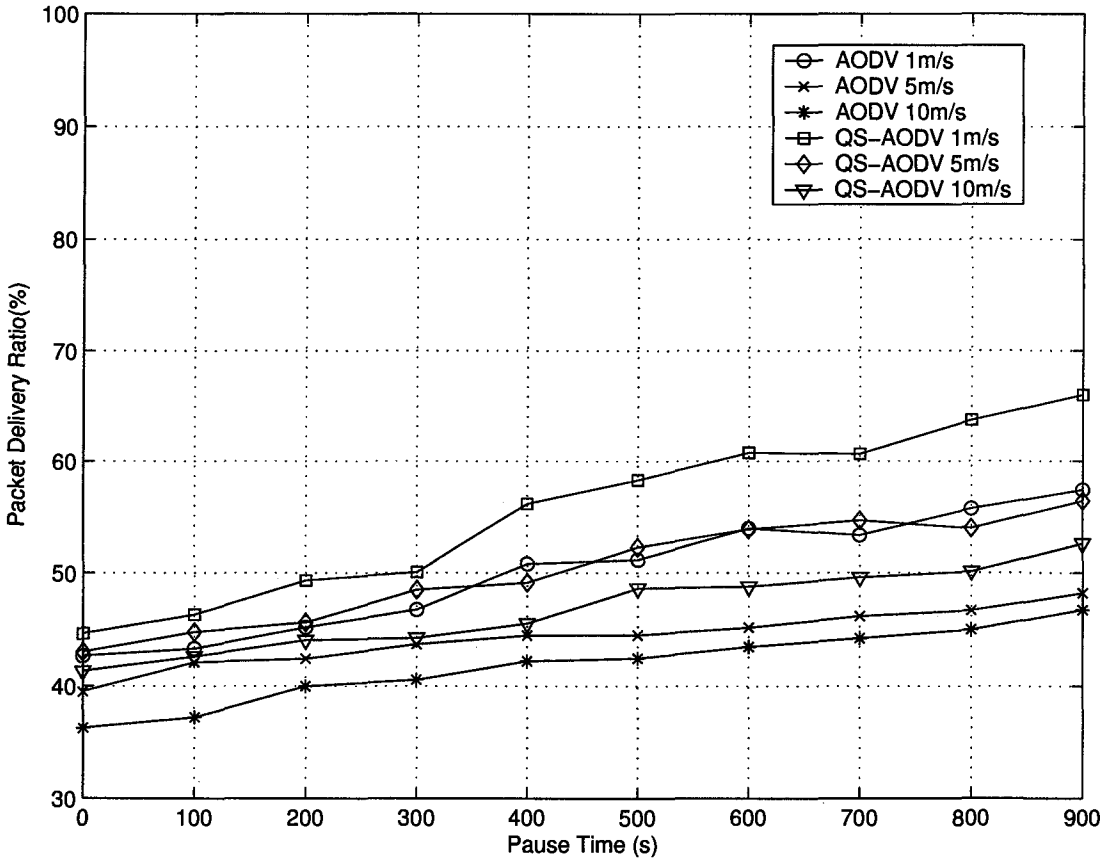

Figure 3.33. *Packet delivery ratio with 20 nodes, 20 sessions and 20 packets/s,*

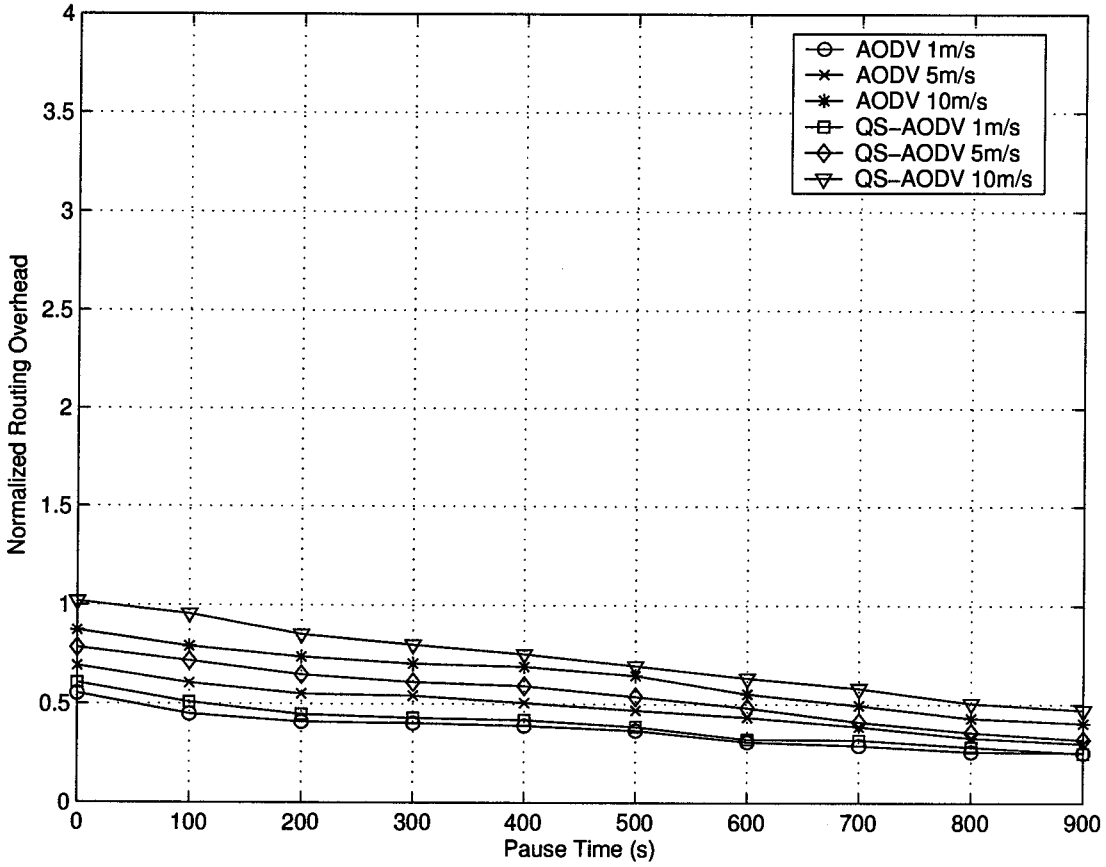

Figure 3.34. *Normalized routing overhead with 20 nodes, 20 sessions and 4 packets/s,*

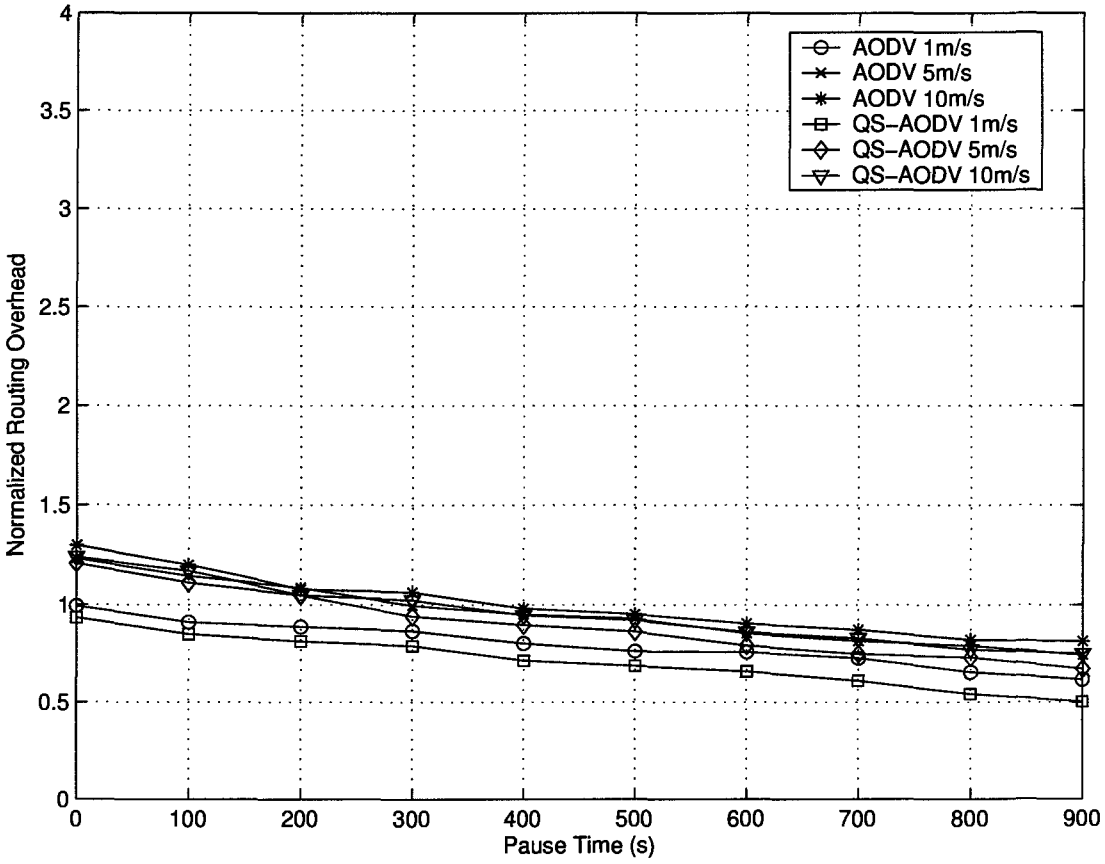

Figure 3.35. *Normalized routing overhead with 20 nodes, 20 sessions and 8 packets/s,*

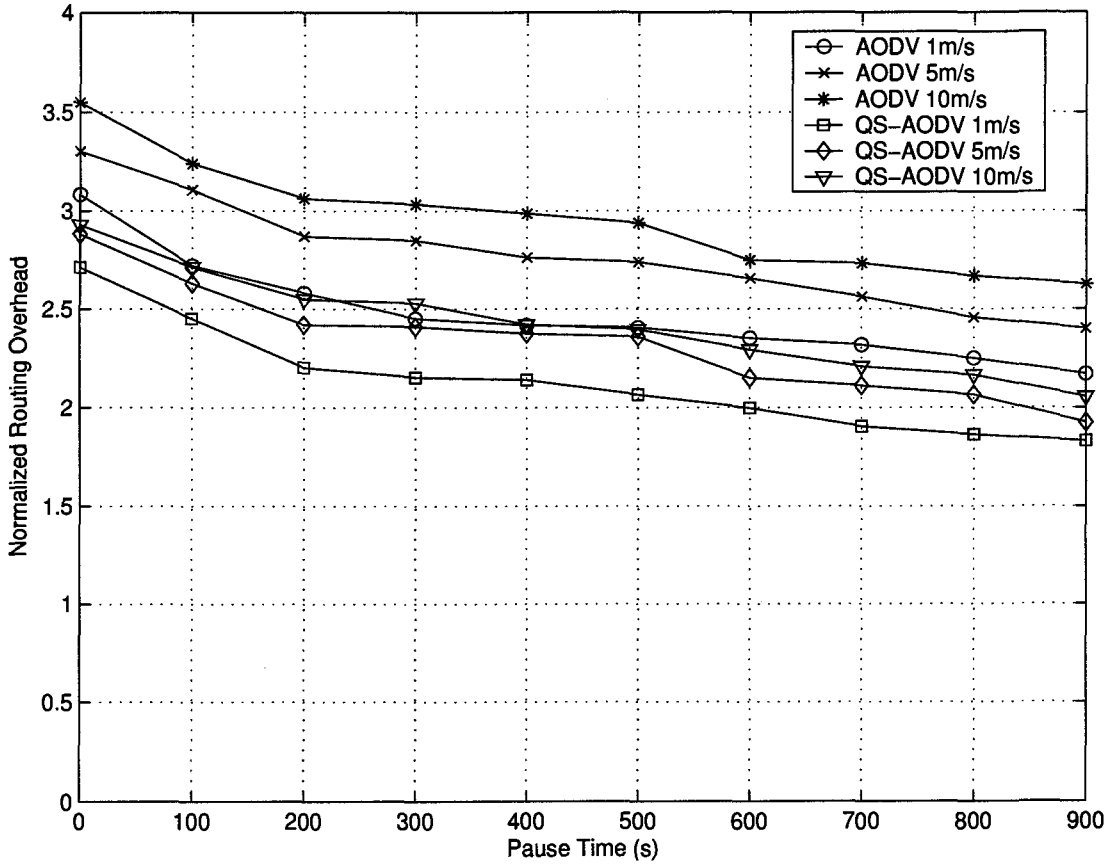

Figure 3.36. *Normalized routing overhead with 20 nodes, 20 sessions and 20 packets/s,*

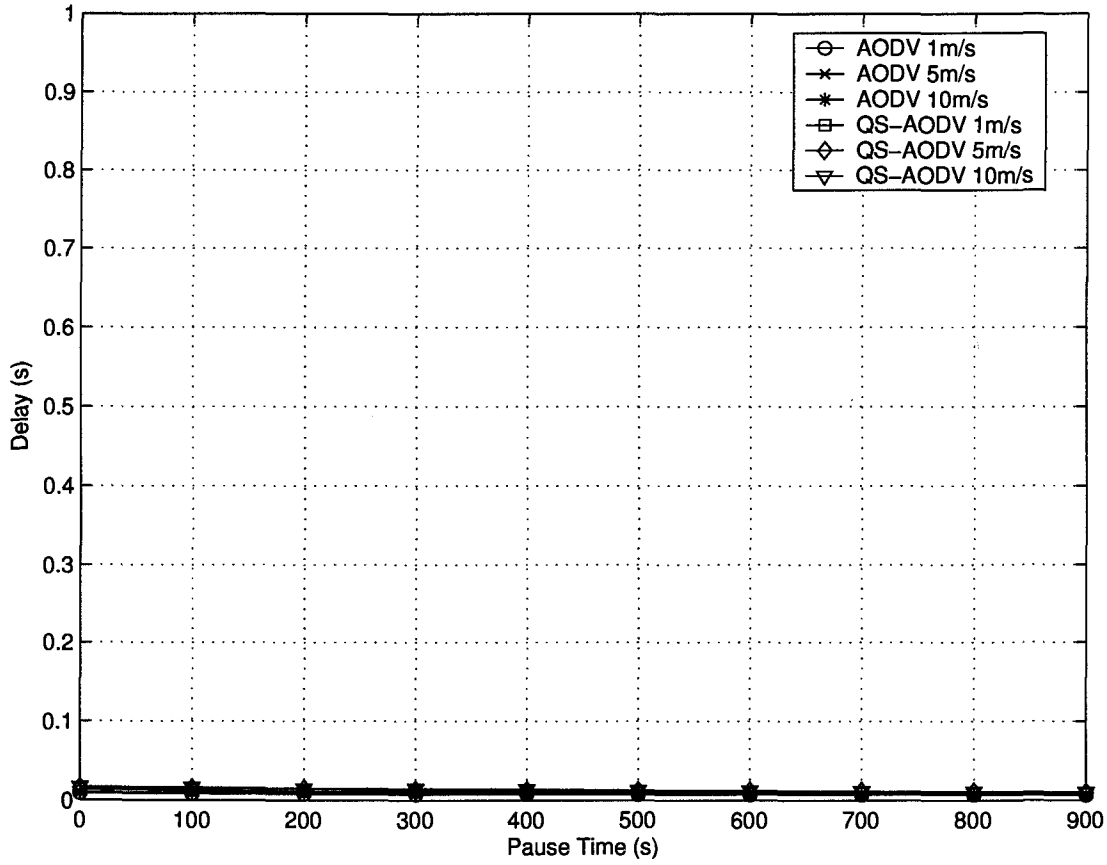

Figure 3.37. *Delay with 20 nodes, 20 sessions and 4 packets/s,*

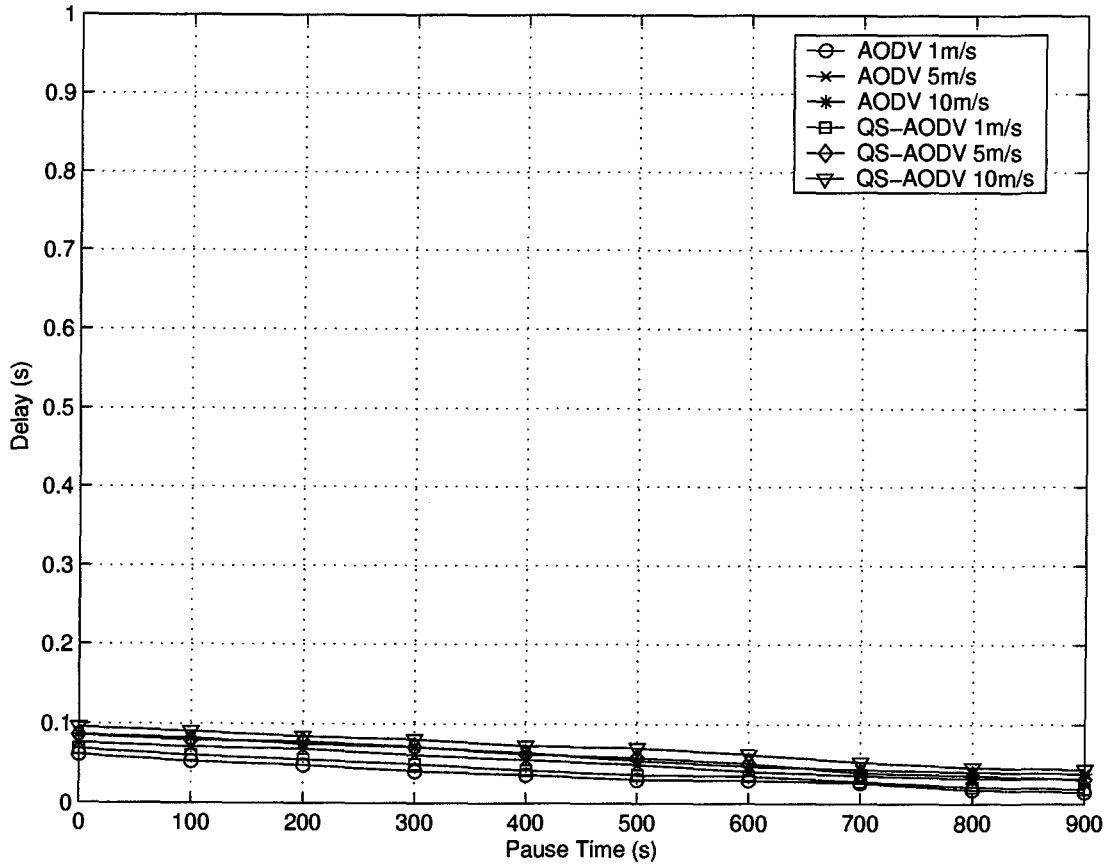

Figure 3.38. *Delay with 20 nodes, 20 sessions and 8 packets/s,*

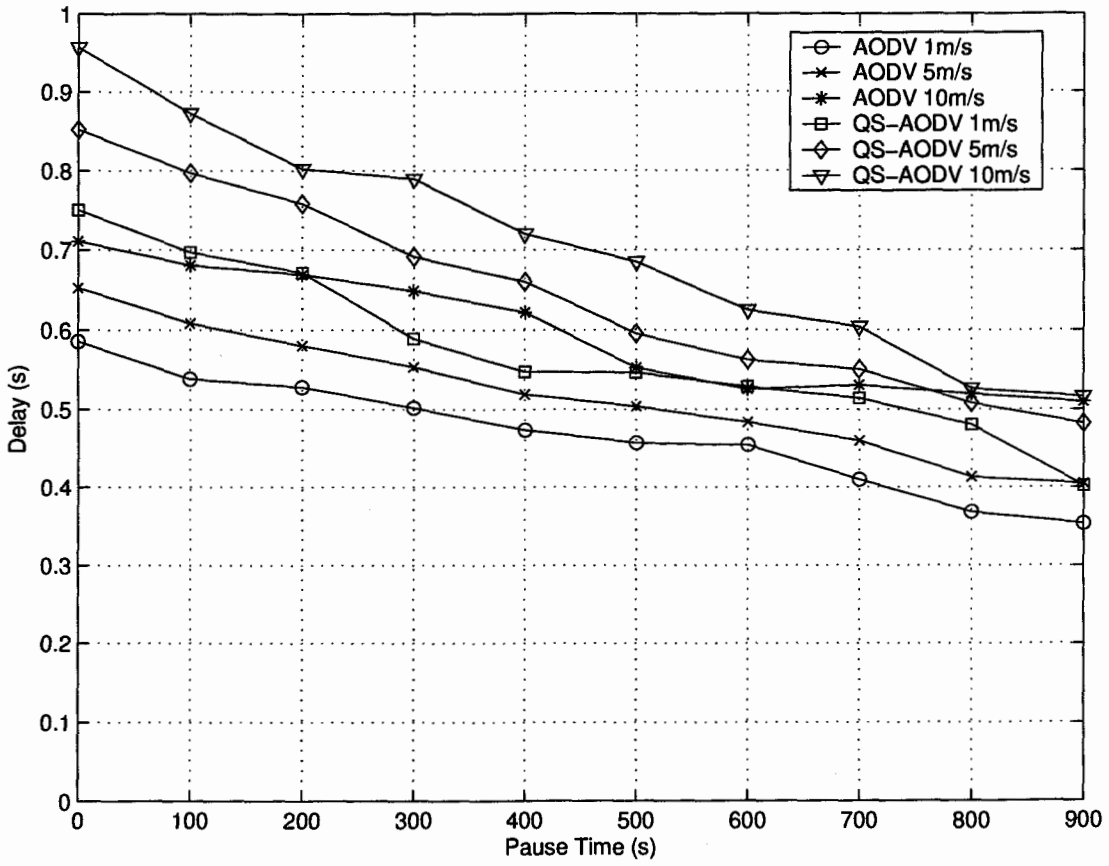

Figure 3.39. *Delay with 20 nodes, 20 sessions and 20 packets/s,*

Chapter 4

Conclusions and Future Work

This chapter concludes this thesis and presents some directions for future research.

4.1 Conclusions

An ad hoc wireless network is a distributed system in which wireless nodes are dynamically self-organized into an arbitrary network [1] [2]. Each node in the network acts as a router, forwarding data packets for other nodes. Due to mobility and a lack of infrastructure support, network topologies are constantly changing, and the communication capabilities of the network are limited by the bandwidth and the battery power of the network nodes.

Due to these features, it is difficult to provide QoS assurance in ad hoc networks. In this thesis, a QoS routing protocol was proposed based on Ad hoc On-demand Distance Vector Routing (AODV) [13] [38] to provide per flow QoS. In Chapter 1, we described the characteristics of ad hoc network technology, followed by a brief introduction of major applications of ad hoc networks. The challenges and difficulties of ad hoc network research were discussed in this chapter.

Several definitions of quality of service were presented in Chapter 2, and the differences between Intrinsic QoS, Perceived QoS and Assessed QoS were described. In this thesis, we only considered Intrinsic QoS. Next, we discussed some parameters that are used to evaluate QoS from a technical perspective. Two important QoS protocols in wired network were then presented. After the introduction of QoS in communication networks, we addressed

the research challenges of QoS support in ad hoc networks from several aspects of the QoS model, QoS MAC, QoS Signaling and QoS routing. We introduced some proposed QoS models and protocols, such as FQMM [24], INSIGNIA [28] and CERDA [35].

In this thesis, we focused on QoS routing support in ad hoc networks, with QoS assurance based on a simple and robust routing protocol - AODV. In Chapter 3, a brief description of AODV was given. We discussed the AODV routing packet structures and basic operations of route discovery and route maintenance. Then we presented our extended protocol QS-AODV, which adds a QoS extension to AODV packets based on [41], and the routing table structure is changed to contain per-flow QoS information. Routes are created according to the QoS requirement of each application. If the required bandwidth cannot be satisfied, a lower requirement is used to find a route, so the tradeoff is between application quality and packet loss ratio. To quickly rebuild routes due to broken link, a local repair mechanism is used in the proposed protocol.

QS-AODV was simulated and compared with AODV using the ns-2 network simulator. The results gained during the simulation were good. Under light traffic, QS-AODV provides a packet delivery ratio comparable to AODV, but it needs more routing overhead and longer delay due to the fact that the RREP of QS-AODV has to be generated by the destination, and the routes created are not always the shortest. However, when the traffic gets heavy or the number of sessions increases in the network, QS-AODV has better performance than AODV. Because AODV only provides the best effort route, it does not consider the bandwidth constraint of each node. When the traffic is heavy, packets are dropped and the routes may be considered broken due to network congestion, which in turn increases the number of routing packets used to find and maintain routes. Therefore, QS-AODV requires less routing overhead to find and maintain routes, and the packet delivery ratio is 2 - 12% higher than with AODV at the cost of slightly longer delay.

4.2 Future Work

In this thesis we presented our proposed protocol to provide QoS support in ad hoc networks. However, different networks have different mobility, communication capacity and energy constraints, there is no universal solution. Our protocol works well under low mobility, it provides QoS support for each required flow, which is similar to IntServ [11]. Since IntServ has limited scalability [8] [24], extensive routing overhead is created when the network size becomes large. Therefore, clustering and hierarchical solutions could be considered to improve the network performance and scalability. Nodes can be grouped into a number of overlapped clusters, and QoS routes are created between clusters instead of individual nodes, which can increase the robustness of routes and decrease the overhead. Another way to solve the scalability problem is to classify the required applications into different service classes like DiffSev [12], and create routes based on service classes.

In addition, QoS routing still needs the cooperation of QoS MAC and QoS signaling. The IEEE 802.11 MAC protocol was used in the simulations, however, it does not provide any QoS option. As the MAC protocol is invisible to the upper layer (QoS routing), the system is less efficient than a QoS aware MAC protocol. Some work has been done on TDMA protocol to support AODV and provide QoS in ad hoc networks [42]. Thus future work could consider a QoS MAC solution which is appropriate for ad hoc networks.

Support of multicast services such as video conference is an application of ad hoc networks. Some work has been done to provide multicast routing in ad hoc networks [1] [8], and it is even more complex to support QoS for multicasting. This is definitely an area for future research.

Ad hoc networking is a part of the evolution towards fourth generation wireless systems. Its flexibility, auto configuration, ease of maintenance, and cost advantages will make it a prime candidate for personal wireless communication systems. Thus it is important to consider these future research directions to realize the potential of wireless ad hoc network technology.

Bibliography

[1] M. Ilyas, *The Handbook of Ad-Hoc Networks*. CRC Press, Florida, 2003.

[2] C. Perkins, *Ad-Hoc Networking*. Addison-Wesley, USA, 2001.

[3] *Supplement to IEEE standard for information technology telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: high-speed physical layer in the 5 GHz band.* IEEE Std 802.11a, 1999.

[4] *Supplement To IEEE Standard For Information Technology- Telecommunications And Information Exchange Between Systems- Local And Metropolitan Area Networks- Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications: Higher-speed Physical Layer Extension In The 2.4 GHz Band.* IEEE Std 802.11b, 2000.

[5] *Information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band.* IEEE Std 802.11g-2003, 2003.

[6] C. Bisdikian, "An overview of the bluetooth wireless technology," *IEEE Communication Maganize*, vol. 39, no. 12, pp. 86–94, Dec. 2001.

[7] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Scalable coordination in sensor networks," in *Proceeding of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM)*, Aug. 1999, pp. 263–270.

[8] I. Chlamtac, M. Conti, and J. Liu, "Mobile ad hoc networking: imperatives and challenges," *Ad Hoc Networks*, vol. 1, no. 1, pp. 13–64, July 2003.

[9] *Information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.* IEEE Std 802.11, 1999.

[10] Z. Haas and M. Pearlman, "On the performance of a routing protocol for the reconfig-

urable wireless network," in *48th IEEE Vehicular Technology Conference*, May 1998, pp. 102–106.

[11] R. Braden, D. Clark, and S. Shenker, "Integrated services in the internet architecture," in *IETF RFC 1633*, June 1994. [Online]. Available: http://www.ietf.org/rfc/rfc1633.txt

[12] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An architecture for differentiated services," in *IETF RFC 2475*, Dec. 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2475.txt

[13] C. Perkins, E. Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," in *IETF RFC 3561*, July 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[14] ITU-T Rec. Y.1241, "Support of IP-based services using ip transfer capabilities," Mar. 2001.

[15] J. Gozdecki, A. Jajszczyk, and R. Stankiweicz, "Quality of service terminology in IP networks," *IEEE Communication Magazine*, vol. 41, no. 3, pp. 153–159, Mar. 2003.

[16] W. Hardy, *QoS: Measurement and Evaluation of Telecommunications Quality of Service*. Wiley, 2001.

[17] ITU-T Rec. E. 800, "Terms and definitions related to quality of service and network performance including dependability," Aug. 1993.

[18] ETSI, *Network Aspects (NA): General Aspects of Quality of Service (QoS) and Network Performance (NP)*, 2nd ed. Tech. rep. ETR003, Oct. 1994.

[19] E. Crawley, R. Nair, B. Rajagopalan, and H. Sandick, "A framework for QoS-based routing in the Internet," in *IETF RFC 2386*, Aug. 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2386.txt

[20] ITU-T Rec. I.350, "General aspects of quality of service and network performance in digital networks, including ISDNs," Mar. 1993.

[21] A. Tanenbaum, *Computer Networks*, 4th ed. New Jersey, Prenticfe Hall PTR, 2003.

[22] Z. Wang and J. Crowcroft, "Quality-of-service routing for supporting multimedia applications," *IEEE Journal on Selected Area in Communications*, vol. 14, no. 7, pp. 1228–1234, Sep. 1996.

[23] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, "Resource reservation protocol (RSVP) – version 1 functional specification," in *IETF RFC 2205*, Sep. 1997. [Online]. Available: http://www.ietf.org/rfc/rfc2205.txt

[24] H. Xiao, W. Seah, A. Lo, and K. Chua, "A flexible quality of service model for mobile

ad hoc networks," in *IEEE Vehicular Technology Conference Proceedings, VTC2000-Spring, Tokyo, Japan*, May 2000, pp. 445–449.

[25] N. Nikaein and C. Bonnet, "A glance at quality of service models in mobile ad hoc networks," in *Proc. of DNAC 2002: 16th Conference of New Architectures for Communications, Paris, France*, Dec. 2002.

[26] M. Joa-Ng and I.-T. Lu, "Spread spectrum medium access protocol with collision avoidance in mobile ad-hoc wireless networks," in *Proc. 18th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 99)*, vol. 2, Mar. 1999, pp. 776–783.

[27] *IEEE 802.11 WG, Draft Supplement to Part 11:Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS).* IEEE Std 802.11e/D3.3.2, Nov. 2002.

[28] S. Lee, A. Gahng-Seop, X. Zhang, and A. Campbell, "INSIGNIA: An ip-based quality of service framework for mobile ad hoc networks," *Journal of Parallel and Distributed Computing (Academic Press) , Special issue on Wireless and Mobile Computing and Communications*, vol. 60, no. 4, pp. 374–406, 2000.

[29] G.-S. Kuo and P.-C. Ko, "Dynamic RSVP protocol," *IEEE Communications Magazine*, vol. 41, no. 5, pp. 130–135, May 2003.

[30] D. Johnson, D. Maltz, and Y.-C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (DSR)," in *IETF draft*, July 2004. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt

[31] R. Ogier, F. Templin, and M. Lewis, "Topology dissemination based on reverse-path forwarding (TBRPF)," in *IETF RFC 3684*, Feb. 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3684.txt

[32] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)," in *IETF RFC 3626*, Oct. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3626.txt

[33] S. Chen and K. Nahrstedt, "An overview of quality of service routing for next-generation high-speed networks: Problems and solutions," *IEEE Network*, vol. 12, no. 6, pp. 64–79, Nov. 1998.

[34] S. Chakrabarti and A. Mishra, "QoS issues in ad hoc wireless networks," *IEEE Communication Magazine*, vol. 39, no. 2, pp. 142–148, Feb. 2001.

[35] R. Sivakumar, P. Sinha, and V. Bharghavan, "CEDAR: A core-extraction distributed ad hoc routing algorithm," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1454–1465, Aug. 1999.

[36] S. Chen and K. Nahrstedt, "Distributed quality-of-service routing in ad hoc networks,"

IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1488–1505, Aug. 1999.

[37] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," *ACM SIGCOMM Computer Communication Review*, vol. 24, no. 4, pp. 234 – 244, Oct. 1994.

[38] C. Perkins and E. Royer, "Ad hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA*, Feb. 1999, pp. 90–100.

[39] C. Hedrick, "Routing information protocol," in *IETF RFC 1058*, June 1988. [Online]. Available: http://www.ietf.org/rfc/rfc1058.txt

[40] E. Royer and C. Perkins, "Evolution and future directions of the ad hoc on-demand distance vector routing protocol," *Ad hoc Networks Journal*, vol. 1, no. 1, pp. 125–150, July 2003.

[41] C. Perkins and E. Royer, "Quality of service for ad hoc on-demand distance vector routing," in *Internet draft, draft-perkins-manet-aodvqos-02.txt*, Oct. 2003. [Online]. Available: http://people.nokia.net/ charliep/txt/aodvid/qos.txt

[42] C. Zhu and M. Corson, "QoS routing for mobile ad hoc networks," in *IEEE Proc. INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, June 2002, pp. 958–967.

[43] I. Gerasimov and R. Simon, "A bandwidth-reservation mechanism for on-demand ad hoc path finding," in *IEEE Proc. 35th Annual Simulation Symposium*, April 2002, pp. 27–34.

[44] UCB LBNL VINT Group, "Network Simulator (version 2)." [Online]. Available: http://mash.cs.berkeley.edu/ns

[45] K. Fall and K. Varadhan, *Ns notes and documentation.* The VINT Project, UC Berkeley, USC/ISI, LBL and Xerox Parc, 1999. [Online]. Available: http://www-mash.cs.berkeley.edu/ns

[46] C. Perkins, E. Royer, S. Das, and M. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks," *IEEE Personal Communications Magazine*, vol. 8, no. 1, pp. 16–28, Feb 2001.

[47] P. Johansson, T. Larsson, N. Hedman, and B. Mielczarek, "Scenario-based performance analysis of routing protocols for mobile ad-hoc networks," in *Proceedings of the 5th International Conference on Mobile Computing and Networking (ACM MOBICOM 99)*, Aug. 1999, pp. 195–206.

[48] J. Broth, D. Maltz, D. Johnson, Y.-C. Hu, and J. Jetcheva, "A performance comparison

of multi-hop wireless ad hoc network routing protocols," in *Proceedings of the 4th International Conference on Mobile Computing and Networking (ACM MOBICOM 98)*, Oct. 1998, pp. 85–97.

[49] S. Corson and J. Macker, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations," in *IETF RFC 2501*, Jan. 1999. [Online]. Available: http://www.ietf.org/rfc/rfc2501.txt