A ROBUST MULTICAST ROUTING PROTOCOL FOR AD HOC NETWORKS

PADMINI VELLORE [redacted]

A Robust Multicast Routing Protocol for Ad Hoc Networks

by

© *Padmini Vellore*

A thesis submitted to the
School of Graduate Studies
in partial fulfilment of the
requirements for the degree of
Doctor of Philosophy

Faculty of Engineering and Applied Science
Memorial University of Newfoundland

December 2010

St. John's Newfoundland

Abstract

Ad hoc networks are tetherless networks where nodes not only act as source or destination but also as routers on demand. The key features of ad hoc networks (AHNs) include quick deployment and circulation of messages. These features make them well-suited for applications where reliability and robustness are crucial. In such environments, multicasting improves the efficiency of communication by sending information to more than one node in a single transmission. Multicasting in BitTorrent Enabled Ad hoc Network (MBEAN) routing protocol is presented in this research for multicasting in ad hoc networks. MBEAN is based on the concept of BitTorrent protocol, used in peer-to-peer file sharing in the Internet. MBEAN uses a mesh-based approach to establish multiple connections among multicast members in a network. The mathematical framework for member-to-member connectivity, which indicates member reliability, of MBEAN is developed in this research. Analytical explanations for packet delivery ratio and bounds for routing and control overhead are also presented. Simulations conducted show that MBEAN achieves higher member reliability and improved packet delivery ratio with reduced overall overhead compared to other multicast routing protocols such as, Multicasting in Ad Hoc On Demand Distance Vector (MAODV) and Protocol for Unified Multicasting through Announcements (PUMA). The robustness of MBEAN is also demonstrated for realistic application-based scenarios for various kinds of message sources.

Unicasting in BitTorrent Enabled Ad Hoc Network (BEAN) routing protocol is also presented in this research and is primarily developed to deliver unicast communications in a multicast domain. BEAN protocol applies on-demand methodology and establishes multiple disjoint routes among pairs of nodes. The probability of multiple disjoint paths that are necessary for BEAN is investigated through analytical expressions and validated using simulations. The performance of BEAN in terms of improved delivery of information is illustrated through medium access control mechanism. Simulations are conducted to demonstrate the performance of BEAN under practical network conditions and the results are compared with those of AODV, a traditional routing protocol.

Acknowledgements

I express my sincere thanks to my supervisors, Dr. P. Gillard and Dr. R. Venkatesan, for their intellectual assistance, financial support, and continuous encouragement during the prolonged course of my research. I also thank them for patiently agreeing to participate in every Internet meeting, even at short notice. Their enthusiasm towards my research was contagious and motivational during difficult times of my graduate program. I thank Dr. Peter Chen for the wonderful teaching offered by him when I was doing my course work, which in turn significantly helped in my research.

I thank Dr. Noreen Golfman, Dean of Graduate Studies, for the financial support endowed on me during my stay at Memorial. I also thank the Associate Dean of Graduate Studies, and I would like to acknowledge Ms. M. Crocker, Office of the Associate Dean, for doing a yeoman's service in guiding all my concerns from commencement to completion of my work at Memorial University.

I thank Prof. H. Mouftah for taking the time to read my work and offer invaluable comments and suggestions. I thank Mr. N. White, System Administrator, Department of Computer Science, for providing all the computing facilities required while I worked remotely. I would like to specially thank Dr. C. Li for being a mentor and immensely encouraging me during critical times.

Lastly, I thank my family (my parents and my sisters), for their boundless love, encouragement and confidence in all my pursuits. I would also like to thank my patient husband, Hari, whose incessant support has assisted me in completing my Ph.D. I thank all my friends for constantly reminding me of my aspiration.

Contents

List of Tables

List of Figures

Nomenclature

A_0	Ad hoc network area
CW_{max}	Maximum backoff counter value
d	Distance between two nodes
f_a	Link distance pdf for the alternate path
f_l	Link distance pdf
h_f	hop count through forwarding nodes
$h_f^{'}$	hop count through non-forwarding nodes
m	Number of multicast members in the network
m_1	Number of members within the transmission range of any member, m_i
m_i	A multicast member
m_j	A multicast member
m_t	Number of members located at t-hop distance
n	Number of nodes in the network

n_i	Number of hops in path (i)
P_C	Collision probability as seen by a node excluding the effects of packet capture and channel errors
p_{i_1}	Collision probability of n_i links along path (i)
q	Probability that a node has packets available in its queue
q_i	Success probability of path (i)
R	Transmission range of each node
S_k	Number of packets sent by path (k)
t_j	Average number of hops for the alternate path
W	Backoff counter value of the contention window of a node
$w(r)$	Probability of being able to establish a communication
x_i	x-coordinate of node i or multicast member m_i
x_j	x-coordinate of node j or multicast member m_j
y_i	y-coordinate of node i or multicast member m_i
y_j	y-coordinate of node j or multicast member m_j
ACK	Acknowledgment
AHN	Ad Hoc Network
AODV	Ad Hoc On Demand Distance Vector Routing Protocol

BEAN	BitTorrent Enabled Ad Hoc Network
BT	BitTorrent
BW	Bandwidth
CBR	Constant Bit Rate
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
DCF	Distributed Coordination Function
DSSS	Direct Sequence Spread Spectrum
FTP	File Transfer Protocol
GloMoSim	Global Mobile Information System Simulator
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Standards Organization
JiST	Java in Simulation Time

LLC Logical Link Control

MAC Medium Access Control

MANET Mobile Ad Hoc Network

MAODV Multicasting in Ad Hoc On Demand Distance Vector

MBEAN Multicasting in BiTtorrent Enabled Ad Hoc Network

ns-2 network simulator

OFDM Orthogonal Frequency Division Multiplexing

OPNET Optimized Network Engineering Tools

OSI Open System Interconnection

oTcl Object Oriented Extension of Tool Command Language

PDA Personal Digital Assistant

PDR Packet Delivery Ratio

PRNET Packet Radio NETwork

PUMA Protocol for Unified Multicasting Through Announcements

QoS Quality of Service

RERR Route Error Message

RREP Route Reply Message

RREQ Route Request Message

RTS Request To Send

RTT Round Trip Time

SimPy Simulation in Python

SMTP Simple Mail Transfer Protocol

TCP Transmission Control Protocol

TELNET Virtual Terminal

TTL Time To Live

VINT Virtual InterNetwork Testbed

Wi-Fi Wireless Fidelity

WiMAX Worldwide Interoperability for Microwave Access

WLAN Wireless Local Area Network

WPAN Wireless Personal Area Network

Chapter 1

Introduction

1.1 Ad Hoc Networks

An ad hoc network (AHN) is a decentralized system with each node in the network acting not just as the source or destination but also as a router. The router (or intermediate node) moves in a random manner and its location may be difficult to predict. The network formed by such routers experiences frequent topology changes due to the mobile nature of the wireless nodes. The network can be a stand-alone network, or, it can be connected to several similar networks, or to the base station of a centralized wireless network or, to the fiber optic cable of wired networks. Figure 1.1 shows a typical AHN environment. AHNs belong to the class of multi-hop wireless networks with the additional property of independence from other nodes in the network. AHNs are more suitable for recent applications where reliability and robustness are critical. Examples of such applications include military battlefields, search and rescue operations, scenes of natural disaster [1], etc.

Figure 1.1: An Ad Hoc Network

Contemporary applications of AHNs include home or small office networking, and collaborative computing with laptop computers in a small area such as conference hall, single building, convention center, etc. [1]. The applications of interest in this thesis include downloading files among users waiting in an airport, among spectators in a ballpark, among attendees of a presentation in a conference area, and, a modern classroom where students need not necessarily be present in the classroom. Such applications demand quick dissemination of files among the nodes involved. Additionally, more power is required and less bandwidth is available for communication through a wireless link when compared with a wired link.

Multicasting improves the efficiency of communication in such networks by sending information to more than one node in a single transmission by exploiting the inherent broadcast nature of wireless transmissions. Even though multicasting is of great importance to ad hoc networks, providing multicast transmission poses a key challenge in the realm of ad hoc networks. Numerous unicast and multicast routing protocols have been proposed for AHNs. Certain protocols have been improved upon to suite specific applications. The protocol furnished in this thesis is one such application-specific protocol suitable for the more recent applications listed above.

1.2 Ad Hoc Network Challenges

Most of the issues or problems faced by AHNs are due to the structural differences between the wired and other wireless networks [1].

1.2.1 Dynamic Topology

The rate at which topological changes occur in AHNs is so high that frequently, by the time the change can be updated in a node's routing table, a packet might have been routed through a path that is not optimal or a path that no longer exists. When the path does not exist anymore, the packet would be dropped which leads to loss of packets. Certain links connecting the ad hoc nodes may be unidirectional. In such circumstances, the availability of a forward shortest path from source to destination may not be useful to the source as the link was unidirectional and the reverse route did not exist.

1.2.2 Technological Limitations

The problems that AHNs face occur due to the limitations in the particular technology that is being used. For example, protocols that use the proactive update of routing tables cause wastage of bandwidth because they send updates even when there is no more data to be sent. Protocols can find the location of each node with respect to others by means of Global Positioning System (GPS) or other such systems that provide location information. Such protocols may not perform satisfactorily when the location information is not available in time for routing decisions to be made. Many protocols find the best route based on the shortest path. The selection of a best route from source to destination must be based on other criteria like battery life of the nodes in the path from source to destination, fairness in terms of distributing the load of routing among all the nodes, and therefore routes, rather than just a single node, etc.

1.2.3 Wireless Channel

Another problem faced by AHNs is the changing environment. The nodes of AHNs rely excessively on the transmission medium - air, that a small change in the environmental condition may cause a reduction in bandwidth thereby increasing the delay through certain links. Breakage of links causes more problems than just the need for re-calculating the route. They cause the throughput to vary anywhere between 0% and 100% within a small period of time. This jeopardizes the Quality of Service (QoS) guarantees like delay, bandwidth and security issues which are the major requirement for the more recent complex multimedia applications of AHNs.

1.2.4 Resource Availability

The devices that are used by AHNs include laptops, PDAs, Smartphones, etc. These devices usually have limited battery power and memory capacities. They are also usually powered up only for a short duration. The bulk of the power is expended on signal transmission and reception. There are also constraints on the amount of computation they can handle since the processors, memory and other I/O components connected to these devices have limited power and capacity.

Considering the challenges discussed above, the desirable properties of a routing protocol for AHNs include loop avoidance, fast convergence upon link changes, localized reaction to changes in topology, availability of multiple routes information, unidirectional link support, QoS support, and, independency of alternate routes.

1.3 Applications of Ad Hoc Networks

1.3.1 Emergency Search and Rescue Operations

In the case of an earthquake where existing cellular network is destroyed, an ad hoc network is the ideal choice. The network created in an ad hoc fashion in an earthquake disaster scene could involve the rescue crew present at the scene scanning for survivors, the paramedics on the way to the scene, the helicopter scanning for the extent and distance of the disaster, and the hospital preparing for the arrival of affected persons.

1.3.2 Military Battlefield Operations

The quick formation and dissemination of an ad hoc network created by the military personnel for the purpose of exchanging short messages to plan for an attack or to defend an attack is a very useful application of ad hoc network. Apart from this, the battlefield consists of airborne vehicles that wish to communicate intelligent information about the location of the enemy to ground vehicles or to military personnel present in the area.

1.3.3 Other Commercial Applications

The commercial applications of AHNs include monitoring the mechanical parts in a car, conference participants wishing to share files or enter in to a discussion on a topic, or, students in cafeteria interacting with other students present anywhere in the campus to share files, etc.

1.4 Routing in Ad Hoc Networks

AHNs need routing protocols for delivering packets from a source node to a designated destination node. Unicast routing protocols generally route data packets between a pair of source and destination nodes. Multicast routing protocols involve more than one destination. A set of nodes usually form a group and any node within the group or outside the group will send packets to the group.

Any routing protocol proposed for AHNs should be able to address some of the basic issues of AHNs such as changing topology, constrained bandwidth, error-prone channel, hidden and exposed terminal problem and resource constraints [2]. An ideal routing protocol must be able to adapt to frequent topology changes, be distributed, involve minimum nodes to compute route, be localized, be loop-free, be optimal, store only local information and provide QoS [2].

Unicast routing protocols can be classified as table-driven or proactive, on-demand or reactive, or, hybrid based on how the routing information is updated in the network

[2].

An ideal multicast routing protocol proposed for AHN applications should be robust, efficient, incur less control overhead, provide QoS, be independent of the unicast routing protocol and manage resource effectively [2]. In reality, achieving all these properties is challenging due to the inherent problems with AHNs. Each protocol that has been proposed tries to achieve one property at the expense of another.

Multicast routing protocols may be tree-based or mesh-based depending on the type of multicast topology they create. They may also be classified as source-initiated or receiver-initiated based on the type of initialization procedure. Some multicast protocols are also application-specific. Such protocols are usually designed for a specific application and handle the needs of that particular application effectively.

In addition to the above classifications, routing protocols proposed for AHNs may or may not be QoS aware. A separate class of routing protocols called multipath routing protocols also exist. Such protocols form more than one path between the source and destination nodes. Tables of classification of several unicast and multicast routing protocols are presented in [2].

1.5 Motivations and Objectives

The problems discussed in Section 1.2 are applicable to unicasting and multicasting. Multicasting is particularly challenging in AHNs mostly due to the properties of AHNs discussed previously. As an example, in AHNs, if the nodes move when multicast data packets are being transmitted, the packets may be dropped on the way to the destination nodes. Thus not all messages would reach all the intended destination nodes. To overcome this problem, if the rate of routing updates is increased, then the network may be congested with the additional control overhead over the existing scarce bandwidth of the wireless link. This means, the amount of control information that is being exchanged among the nodes must be limited. Also, the number of intermediate forwarding nodes that are not members of the multicast group must be small enough not to waste their power consumption by just forwarding others' messages. This is what makes multicasting more challenging in AHNs.

As discussed in Section 1.4, many routing protocols have been proposed that address these issues. Nevertheless, there is no single algorithm that has overcome all these problems [2]. Each routing algorithm tries to address one problem usually at the expense of some of the others. As a result, there is clearly a need for a new routing algorithm for both unicast and multicast cases in AHNs.

The objectives of this thesis are:

1. To develop a multicast routing protocol, called Multicasting in BitTorrent Enabled Ad hoc Network (MBEAN) routing protocol, suitable for a specific set of applications and that supports improved reliability and robustness to failures in ad hoc environments.

2. To analyze the performance of MBEAN protocol by conducting simulations for simple scenarios and comparing the results with other existing protocols like MAODV and PUMA.

3. To apply the MBEAN protocol for more realistic scenarios under crucial network conditions and mobile environments

4. To develop a unicast multipath routing protocol, called BitTorrent Enabled Ad hoc Network (BEAN) routing protocol, to support simple unicasting needs in multicast environments.

5. To analyze the performance of BEAN protocol by conducting simulations for simple scenarios and comparing the results with AODV, a traditional unicast routing protocol.

1.6 Thesis Contributions

The following are the thesis contributions listed briefly.

- Designed a multicast routing protocol, called Multicasting in BitTorrent Enabled Ad hoc Network (MBEAN) routing for AHNs, based on BitTorrent protocol for peer-to-peer communications in Internet. The protocol improves the connectivity among members in the multicast group so that when the source is disconnected or a path fails, the members can still receive the message in full.

- Derived analytical proof of member-to-member connectivity, provided analytical explanation for packet delivery ratio (PDR) and routing and control overhead.

- Compared the performance of MBEAN with MAODV (tree-based) and PUMA (mesh-based) multicast protocols in terms of member reliability, PDR and routing and control overhead for simple scenarios.

- Applied MBEAN to realistic scenarios like ballpark, airport waiting area and conference area and discussed the strengths and drawbacks of MBEAN, PUMA and MAODV for such applications.

- Proposed a unicast multipath routing protocol called BitTorrent Enabled Ad hoc Network routing protocol (BEAN) for AHNs which uses the BitTorrent concept to exchange routing information.

- Derived the probability distribution of multiple disjoint paths in BEAN and validated the analytical formulation through simulations.

- Presented expressions for throughput and compared the performance of BEAN with a traditional unicast protocol, AODV routing protocol.

1.7 Thesis Overview

The rest of the thesis is organized as follows. Chapter 2 provides a detailed review of the unicast and multicast protocols proposed for AHNs. Some of the multipath routing protocols proposed are also discussed.

Chapter 3 discusses the protocol specifications of the multicast protocol, MBEAN. The chapter also provides analytical proof of member-to-member connectivity and therefore, reliability, and, provides analytical explanations for PDR and routing and control overhead. Chapter 4 presents the simulation results for MBEAN comparing it with other multicast routing protocols namely, MAODV and PUMA for simple scenarios.

Chapter 5 presents the applicability of MBEAN under various realistic situations and mobile conditions. Various traffic arrival patterns like data, voice and video sources are simulated and the improved performance showed by MBEAN compared to MAODV and PUMA are presented. The merits and demerits of MBEAN in comparison with MAODV and PUMA for such applications are also discussed.

Chapter 6 presents the protocol specifications and working of the unicast protocol BEAN, along with the distribution of multiple disjoint paths a multipath routing protocol. Chapter 7 presents analytical expressions for PDR, throughput and control and routing overhead for BEAN. The chapter also shows the simulations results comparing BEAN with AODV.

Chapter 8 concludes the thesis and presents a path for future work.

Chapter 2

Protocols for Ad Hoc Networks

2.1 Introduction

The theory behind ad hoc networking emanates from multi-hop relaying [2]. The concept of multi-hop relaying dates back to 500 B.C. when repeater towers were used to rebroadcast the messages through men standing on top of the towers. The recent interest in the field led to ALOHAnet which started as a single-hop wireless packet switching and later became packet radio network (PRNET). Several applications including military applications led the Internet Engineering Task Force (IETF) to form a special group called the mobile ad hoc network (MANET) working group to standardize the protocols and specifications for ad hoc networks. Existing routing protocols pertaining to AHNs proposed by several researchers during the last decade are discussed in this chapter.

Firstly, the standardization of the various protocols for various layers of communication between hosts in a telecommunication network, in particular in an ad hoc network, is outlined in this chapter. An overview of unicast and multicast routing protocols proposed for ad hoc networks over the last decade and earlier is presented in this chapter along with their advantages and disadvantages. A brief description of the BitTorrent Protocol, which is the basis for the thesis and multipath routing are given. Several network simulators available for simulating an ad hoc network are listed and the network simulator used in this thesis is defined. The simulation parameters assumed in our simulations are also revealed. The chapter concludes differentiating the routing protocols introduced and justifying the need for a new routing protocol.

2.2 OSI Layer Implementation

The Open System Interconnection (OSI) reference model was developed by International Standards Organization (ISO) to describe a modular framework for implementing a network [3]. The OSI model consists of seven layers and a protocol is defined for each layer to implement the functions described by the OSI model. Figure 2.1 shows the various layers present in the model. Most applications did not require the session and presentation layers as they were found to be performing redundant operations [2]. Furthermore, the OSI reference model does not take in to account the presence of a lossy channel in ad hoc networks. The layers of the OSI system as applicable to AHNs are discussed in Figure 2.1.

2.2.1 Physical Layer

The physical layer for AHNs has to address the issues of error-prone wireless channel. The most commonly used radio propagation models are free-space propagation model,

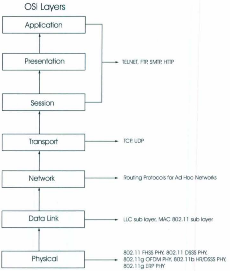

OSI Layers
Application
Presentation
Session
Transport
Network
Data Link
Physical
TELNET, FTP, SMTP, HTTP
TCP, UDP
Routing Protocols for Ad Hoc Networks
LLC sub layer, MAC 802.11 sub layer
802.11 FHSS PHY, 802.11 DSSS PHY,
802.11g OFDM PHY, 802.11b HR/DSSS PHY,
802.11g ERP PHY

Figure 2.1: OSI Reference Model

two-ray ground propagation model and shadowing model [4].

In the free-space model, the channel is assumed to be ideal with only one propagation path between the transmitter and receiver. The two-ray ground model assumes a direct path and a ground reflected path. This model shows good results for larger distances only. Therefore a threshold is defined and any receiver that is at a distance less than the threshold is assumed to follow the free-space path and any receiver that is at a distance greater than the threshold is assumed to follow the two-ray ground reflected path. The shadowing model introduces fading effects.

Generally the IEEE 802.11 technology is used for physical and data link layers in ad hoc networks. In the physical layer, IEEE 802.11b and IEEE 802.11g both use the 2.4 GHz ISM band. 802.11b uses the direct sequence spread spectrum (DSSS) modulation scheme to control interference. Similarly, 802.11g uses orthogonal frequency division multiplexing (OFDM) method to control interference. The main difference between 802.11b and g is the data rate that they can support. 802.11g can support a higher data rate of up to 54 $Mbps$ compared to 802.11b which supports up to 11 $Mbps$.

2.2.2 Data Link Layer

The data link layer consists of two sub layers, namely, logical link control (LLC) layer and medium access control (MAC) layer. The LLC layer controls error and flow. The MAC layer controls access to the shared medium. Several IEEE standards for MAC layer of wireless networks have been proposed in the literature such as IEEE 802.11a/b/g/n for WLAN and Wi-Fi, IEEE 802.15 for WPAN and IEEE 802.16 for

WiMAX [2].

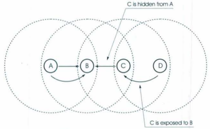


Figure 2.2: Hidden and Exposed Terminal Problem in AHNs

One of the problems of the MAC layer is the hidden and exposed terminal problem which is illustrated in Figure 2.2. In Figure 2.2, if node C is not aware of the transmission from node A to node B, then if node C has a packet to transmit to node B, it might transmit at the same time node A is transmitting to node B. Thus, there is collision at node B and both the transmissions are dropped. This is called as the hidden node problem. If, however, node C wishes to send a packet to node D at the same time when node B wishes to send to node A, both nodes B and C might backoff although the two transmissions can be simultaneous. This is the exposed terminal problem. IEEE 802.11 standard has a MAC implementation with a distributed coordination function (DCF) component that uses carrier sense multiple access with collision avoidance (CSMA/CA) scheme. According to this scheme, a node that wishes to transmit through the common channel first requests the use of the channel. This is illustrated in Figure 2.3.

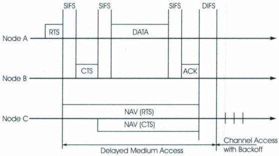


Figure 2.3: RTS/CTS Access Mechanism taken from [5]

In Figure 2.3, when node A wishes to transmit to node B, it first broadcasts a Request to Send (RTS) message which contains node B's address and the length of the data packet it wishes to send. On receiving the RTS message, node B responds with a Clear to Send (CTS) message, which is also broadcast. Any node, such as node C, listening to the CTS message from node B, will know that node B is about to receive a data packet with a specified length from node A and will therefore, not transmit during that interval, thereby avoiding a collision. Once the transmission is complete, an acknowledge (ACK) message is sent by node B back to node A. This avoids the hidden node problem. Since the RTS and CTS messages carry the destination address and the length of data packet following them, the exposed terminal problem can also be eliminated.

In [5], Bianchi studied the performance of IEEE 802.11 DCF protocol for a saturated network by evaluating the throughput. The Markov chain in [5] shows the transition probabilities for a network where each node always has packets to send or the node's queue is always logged. The unsaturated case includes multiple hops where the nodes are not always backlogged with packets. In other words, the intermediate nodes, which are also the nodes under consideration, do not have packets always in the queue. This led to the modification of Bianchi's Markov chain by Duffy in [6], to indicate the absence of packets in queue, by introducing an idle state for each backoff attempt. Having one idle state for each backoff attempt was modified by Daneshgaran in [7] to having only one idle state to indicate the absence of a packet. In [8], the effect of of hidden nodes and packet capture on throughput of IEEE 802.11 protocol were studied. All of the above papers discuss the performance of IEEE 802.11 protocol.

2.2.3 Network Layer

AHNs frequently succumb to topological changes and the network layer takes charge of finding and maintaining routes for data transfer. The network layer implements the routing protocol for finding a shortest path between a source node and an intended destination node. In the case of multicast, the routing protocol forms a multicast group and any source node can send data packets to all the members of the multicast group using the inherent broadcast nature of AHNs. Several routing protocols have been detailed in Section 2.3.

2.2.4 Transport Layer

The objective of the transport layer is to deliver the packets that it receives from the application layer to a destination node in the network following the route specified by the routing layer. The transport protocols usually perform flow control at the source node with the help of acknowledgments received from the destination node. The two main transport protocols are User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) [2]. TCP provides assurance in transmission: every packet is acknowledged by the receiver, lost packets are retransmitted and a congestion control mechanism is used to adjust the rate of data flow in the network to avoid packet loss due to overloading. UDP does not guarantee service as TCP does.

Although receiving acknowledgments and having a congestion control mechanism are attractive for a network, the ad hoc network environment is very unreliable. The loss of packets cannot be entirely attributed to congestion in the network, instead, they are generally due to lossy wireless medium. The overhead incurred on the network by TCP is high for shared wireless channel and the battery powered wireless devices used in ad hoc wireless networks. Therefore, many ad hoc wireless network studies include UDP packets in addition to TCP packets.

Several variations of TCP exist based on the congestion window decisions they make. Few of them include TCP Tahoe [9], TCP Reno [10], TCP SACK [11], [11], TCP Vegas [12] and TCP New Reno [13]. The working of TCP Tahoe is explained briefly below.

TCP Tahoe maintains a congestion window which limits the number of unacknowledged packets that can remain in transit between the source and destination nodes. When a connection is initiated, TCP protocol enters the slow-start phase as shown in Figure 2.4. According to this phase, the congestion window (W) starts at one and is doubled for each round trip time (RTT). After reaching a threshold, called as $ssthresh$, the protocol enters a new phase called congestion avoidance. In this phase, congestion window increases linearly for each RTT. The number of packets sent in

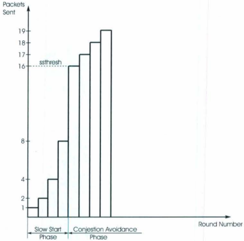


Figure 2.4: Congestion Avoidance in TCP

each round during the slow start and congestion avoidance phases are shown in Figure 2.4. In TCP Tahoe, when duplicate acknowledgments are received or when there is a timeout, then the protocol, as a means to avoid congestion, sets the congestion window back to one.

2.2.5 Application Layer

This layer provides access to user applications. It consists of the applications that are used as a means of communicating between the source node and destination node for tasks such as database access, electronic mail communication and even connect to remote machines. File Transfer Protocol (FTP) is one of the most commonly used protocols for file transfer between machines. Other application layer protocols include virtual terminal (TELNET), simple mail transfer protocol (SMTP) and hypertext transfer protocol (HTTP) [2].

2.3 Brief Description of Unicast and Multicast Routing Protocols for AHNs

Routing protocols for AHNs have been proposed for both unicast and multicast applications. In general, routing protocols for AHNs are classified based on the implementation of the routing algorithm by the routing protocol. The manner in which the routing algorithms discover routes and maintain them between various source-destination pairs may be classified as table-driven or proactive protocols [14, 15, 16, 17, 18, 19, 20, 21, 22, 23] source-initiated or on-demand or reactive protocols

[24, 25, 26, 27, 28, 29, 30, 31, 32] and, hybrid protocols [33, 34, 35, 36]. Another class of routing protocols that uses hierarchy as a new aspect combined with both proactive and reactive routing approaches is the hierarchical routing protocols [16, 19].

A separate class of routing protocols called multipath routing protocols [37, 38, 39, 40]also exist. Such protocols form more than one path between the source and destination nodes. The advantage of multipath routing protocols is that they are resilient to route failures.

Furthermore, multicast routing protocols are classified as tree-based and mesh-based, depending on the multicast topology [41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57]. In addition to the classification based on topology, multicast routing protocols proposed for AHNs may be Quality of Service (QoS) aware [58, 59, 60]. Multicast protocols are also designed to be application-specific [61, 62, 63]. These protocols improve on one particular property based on the demand by the application for which they are developed.

The multicast routing protocol proposed in this thesis is a mesh-based application-specific routing protocol that uses the reactive approach for route formation. The following sections briefly discuss about each of the above classifications of unicast and multicast routing protocols.

2.3.1 Unicast Protocols

2.3.1.1 Proactive Protocols

Proactive protocols [14, 15, 16, 17, 18, 19, 20] aim at maintaining the routes by exchanging routing information continuously as the nodes move. Thus when a route is required for forwarding packets from a source node to any destination node, the route is already available. The control overhead is a serious limitation in this case due to the frequent exchange of routing table updates even when data is not actually being sent. The working of the routing protocols that fall under this category is similar to that of IP routing protocols.

2.3.1.2 Reactive Protocols

Reactive or on-demand protocols [24, 25, 26, 27, 28, 29] send a control message to exchange routing information only when necessary, for example, when they need to discover a route from a source node to any destination node. This method reduces the control overhead drastically. However, since a route is not available when the source requests a route, the time required for the initial establishment of the route is higher than that of the proactive protocols.

AODV

Ad Hoc On-Demand Distance Vector (AODV) routing protocol [25] is a unicast reactive routing protocol based on queries and responses. A route to the destination node is established on a need basis or on demand by the source node. AODV is one of the earliest routing protocols proposed for AHNs. QoS aware AODV is also available. The general working of AODV routing protocol is detailed below in several phases.

Local Connectivity: AODV achieves local connectivity between mobile nodes by the use of frequent *hello* messages. Each node that broadcasts the *hello* message informs its presence to its immediate neighbors or nodes within its transmission range. The nodes that receive the *hello* message update their routing tables with the information of their neighbor. Each node sends the *hello* message once every *hello_interval*.

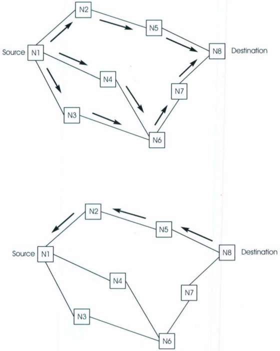


Figure 2.5: AODV RREQ and RREP Flow taken from [64]

If a node does not hear from its neighbor for more than *allowed_hello_loss* times, then it assumes that the link has failed and that the neighbor is inactive.

Route Discovery: As long as there is no need to send messages along the network, AODV plays no role. When a route to a new destination node is needed, the source node broadcasts route request (RREQ) to its neighbors as shown in Figure 2.5. On receiving the RREQ, the destination node, or, the node which has a route to the destination, sends a unicast RREP message through one of the several routes, usually through the best route, to the source node as shown in Figure 2.5. The best route is the route which has the least number of hops to the destination node. In QoS-aware AODV, the best route is also the route that satisfies the minimum bandwidth requirement and maximum tolerable delay. Each node has a precursor list that has the IP address for its neighbors that are likely to use it as a next hop towards each destination. When a node's battery gets depleted or it wanders far out of range or it suffers software or hardware failure, a route error message (RERR) is sent to these nodes. The source then starts sending a new RREQ message to reach the destination.

AODV initiates routing on demand or in reaction to traffic arrival in the network at a node. AODV uses sequence numbers to keep the routes fresh and to avoid routing loops. The sequence number is carried by each routing packet.

Route Maintenance: The routing table in AODV is maintained on a per destination basis. There is one table entry for each destination. A routing table entry expires if it has not been used recently. Each routing table entry contains a set of predecessor nodes that indicate the neighboring nodes in order to route RERR packets if a link is broken. All the sources that had been using the failed link will be disabled by this method.

Extensions to AODV: An improved version of AODV controls the flooding of RREQ by introducing the *expanding ring search* method [65]. In this method, the Time To Live (TTL) of the RREQ packet is increased on a need basis.

Apart from the basic AODV routing protocol, further extensions to the basic protocol have been proposed. For example, QoS-aware AODV provides QoS by adding extensions to the existing messages in the route discovery process [66]. The maximum delay and the minimum bandwidth values can be specified for the route between a source and destination node. Additional fields should be added to the routing tables in each node to store the tolerable delay and bandwidth values and the list of sources that demand QoS guarantees.

Ad Hoc On-Demand Multipath Distance Vector Routing Protocol (AOMDV) is an extension of AODV that uses the concept of multipath routing [67]. The protocol is loop-free and achieves path disjointness. All the paths to the destination carry the same sequence number. Each path differs from the other in terms of additional fields in the route entry such as *hop count* and *last hop*. These two fields also address the problem of loop freedom and path disjointness.

AODV supports only symmetrical links. That is, the forward and reverse routes are the same for any particular source-destination route.

2.3.1.3 Hybrid Protocols

Usually a combination of both proactive and reactive approaches is used in order to improve the efficiency of the routing protocol. This gives rise to the third class of routing protocols called hybrid protocols [33, 34, 35]. Routing protocols that follow the hybrid approach use a proactive approach of updating the routing tables up to a small area or zone and then use a reactive approach beyond this area. This is a localized proactive approach.

2.3.1.4 QoS-based Protocols

Apart from the protocols discussed above, there are other protocols that have been proposed to specifically handle applications requiring QoS. These protocols hunt for routes that have sufficient resources like bandwidth, or satisfy certain minimum hops. Generally bandwidth of a route is calculated as minimum bandwidth (concave metric) of all the links in the route or path between the source and destination nodes. The delay of a route is the sum of all the delay through each of the links in the route. A protocol that supports QoS requires that the route information is updated frequently to maintain freshness of route and accuracy of the available metrics.

2.3.1.5 Multipath Protocols

A subclass of the reactive protocols are the multipath routing protocols. The reactive protocols rely on flooding the network with query packets to find the best route between two nodes. The multipath routing protocols exploit the flooding technique by finding more than one path between the source and destination nodes. Essentially the paths found are disjoint and so are useful to route packets between the source and destination when the best path fails. Such protocols also reduce the need for frequent flooding in the network when a route fails. The unicast protocol proposed in this thesis is a multipath routing protocol. Multipath routing protocols are discussed more in Section 2.5.

2.3.2 Multicast Protocols

Based on the multicast topology, multicast routing protocols are classified as tree-based or mesh-based. Based on how the multicast groups are formed, the multicast routing protocols may be source-initiated and receiver-initiated routing protocols. The three methods of exchanging the routing information for multicast routing algorithms are flooding, proactive approach and reactive or on-demand approach.

2.3.2.1 Tree-based Protocols

The tree-based multicast protocols are classified as source-tree-based and shared-tree-based routing protocols. The source-tree-based multicast routing protocols [41, 42, 44, 45, 46, 47, 48, 49, 68, 69], have one tree from each source to the multicast destinations. Thus there are multiple source-based trees present in the network. The shared-tree-based routing protocols [43, 50, 51, 70] have only one tree with the root at the core of the tree. Thus a single tree is shared by all the multicast nodes. The problem with this kind of routing protocols is that if the core node fails, then the entire tree has to be reconstructed.

MAODV

Among the two basic kinds of multicast routing protocols namely tree-based and mesh-based protocols, MAODV is a tree-based multicast routing protocol [50]. Like its unicast protocol, MAODV is an on-demand (reactive) routing protocol.

Multicast Tree Formation: When a node wishes to join the multicast group, it broadcasts an RREQ message with the join (J) flag set (for multicast) with the group address as the destination address as shown in Figure 2.6. Any member of the

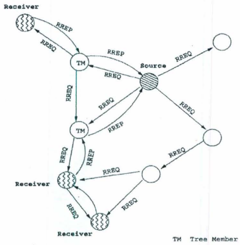


Figure 2.6: Route Discovery in MAODV Protocol taken from [71]

multicast group (tree) can reply to the request with an RREP packet. If a node is not a member of the multicast group, it rebroadcasts the request. The request propagates until it reaches a multicast tree member (TM). When the multicast member replies to the request, each node along the path that was followed by the request will record the next hop information. The node also updates its routing table with the new sequence number.

The source may receive more than one reply. The source node waits for a specified period of time to receive all the RREPs. It selects the one with the most recent sequence number or the path of least hop count. The source node will then unicast a *multicast activation* (MACT) message to the group through the selected next hop. On receiving the MACT message, the next hop will activate the entry for this source node. If the source of the request does not receive a reply within a certain period, it rebroadcasts the request until a certain number of retries (RREQ_RETRIES). After that the source assumes that no such multicast group exists and forms a new multicast group with itself as the group leader. The group leader frequently broadcasts *group hello* (GRPH) message to maintain the connectivity in the group. Apart from this, nodes broadcast frequent *hello* messages.

Multicast Tree Maintenance: When a node that is part of the multicast tree moves or expires, the tree breaks. When the tree breaks, it has to be reconnected immediately in order to avoid serious loss of packets to part of the members of the group. When a link breaks, the downstream node takes responsibility to repair the link. The downstream node sends a new RREQ message with the J flag set and with the multicast group leader address as the destination address.

If after several retries the node is not able to establish a connection with the multicast group, it assumes that the tree is partitioned. Then the node, if it is a multicast member, will become the group leader and broadcasts a GRPH message. If the node is not a multicast member, it prunes itself from the group and sends a MACT message with the *prune* flag set. In future if these two groups come in range of each other, then the group leader with the lower IP address will initiate a RREQ message with *repair* flag (R) set. When the group leader with the higher IP address receives this request, it sends a GRPH message with the *update* flag (U) set. Thus the two groups merge.

The maintenance of the multicast tree in MAODV may seem complicated and time consuming compared to the mesh based protocols discussed below. However the total number of control messages exchanged to maintain the tree are not too high. When a link breaks, the time taken for the multicast tree to recover is long. When the group leader fails, the entire group has to be reestablished. When the group size of the multicast group is large, the packet delivery ratio is low. MAODV is dependent on the underlying unicast (AODV) protocol and therefore, the protocol is not flexible.

2.3.2.2 Mesh-based Protocols

Mesh-based multicast protocols [72, 73, 52, 53, 54, 55, 56, 74] contain more than one route between the source and the multicast destinations. Therefore, when any link between the source and one of the mutlicast members breaks, an alternate route is available. The availability of multiple routes makes this kind of protocols more *robust*.

ODMRP

On-Demand Multicast Routing Protocol (ODMRP) [72] is a multicast routing protocol based on mesh topology. This protocol uses forwarding groups to create a multicast mesh. A *forwarding group* is a set of nodes that take the responsibility of forwarding multicast data packets among members through shortest paths. The basic working of the ODMRP protocol is discussed below.

Mesh Formation: The source that wishes to form or join a multicast group broadcasts a *join request* message with a data packet piggybacked. This is shown by solid lines in Figure 2.7. Each node that receives the *join request* message forwards it to the upstream node. When any node receives the request, it stores the source address and the packet identifier in its routing table and rebroadcasts the request.

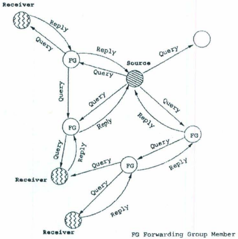


Figure 2.7: ODMRP Group Setup and Maintenance taken from [71]

The receivers reply to the source with a *join reply* message. This message is broadcast by the receiver. When any intermediate node receives the *join reply* message, it updates its own routing table making itself the forwarding node of the multicast group. The intermediate node also sets the *forwarding group* (F) in the reply message and forwards the reply to its upstream node. Thus the *join reply* propagates back to the source through forwarding group members. The path of the *join reply* is shown in Figure 2.7.

A mesh of nodes is constructed connecting the sources and receivers. This mesh is

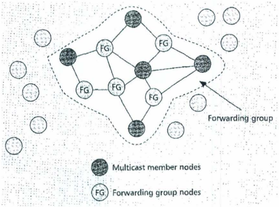


Figure 2.8: ODMRP Forwarding Group Concept taken from [72]

called the forwarding group as shown in Figure 2.8. If one of the intermediate nodes moves, then the message can still reach the multicast receiver through an alternate route. This is the advantage of the mesh-based protocol.

Mesh Maintenance: The source floods the *join request* message frequently to maintain the established mesh. This packet refreshes the existing mesh membership information and updates the routes. The *join request* and *join reply* also refreshes the forwarding group information. Thus the protocol uses a soft-state approach to maintain the mesh thereby providing robustness. This however, results in high control overhead. The disadvantage of this protocol is that there is more than one path to each receiver. This means several copies of the packet are sent through various routes of the mesh. This reduces the efficiency of the multicast protocol.

ODMRP can operate with any unicast routing protocol. It can also act as a unicast routing protocol efficiently. Therefore, while multicasting using the ODMRP protocol, there is no need for a separate unicast protocol. Based on level of mobility of the network, ODMRP's *refresh interval* is selected. The *refresh interval* is the amount of time after which the *join request* has to be sent in order to maintain the group and route information. Highly dynamic network environments demand a smaller *refresh interval*. However, this causes frequent *join request* messages congesting the network. An appropriate prediction for the *refresh interval* has been proposed in [72].

PUMA

Protocol for Unified Multicasting (PUMA) is another mesh-based multicast protocol for ad hoc networks that has been proven to attain higher packet delivery ratios compared to ODMRP and MAODV while incurring less control overhead [73]. The routing decisions made in PUMA are described in this section. PUMA uses multicast announcements for exchanging all kinds of control information such as electing a core dynamically, finding routes for sources outside the multicast group, joining and leaving the mesh and maintaining the mesh.

Mesh Formation: Multicast group establishment starts with a node that wishes to join the multicast group. If it does not already have a route to the mesh, then it assumes itself to be the core and broadcasts a *multicast announcement*. Each node that receives the announcement changes its core information if the core ID is higher than what it already has, if the distance to the core from itself is shorter and, if the new announcement is recent enough. This way, every node has only one core. All the information about electing a core (if there was partitioning) or establishing a

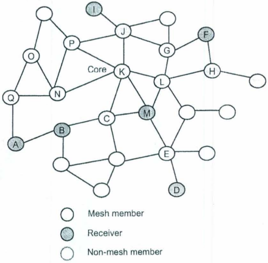


Figure 2.9: Mesh Creation in PUMA taken from [73]

multicast group is carried out by the *multicast announcement* message.

Initially only receivers are mesh members. A non-receiver can become a mesh member if it is directly connected to the mesh member. The mesh creation in PUMA is shown in Figure 2.9. In this figure, Node K is elected as the core. Every node in the network has information about its distance to the core node. In the figure, the receivers (I, F, A, B, D and M) set themselves to be mesh members by default. The neighboring nodes (G, H, J, K, L, C, E) of these receivers which are on the path to the core also become mesh members.

The only control and routing message sent in PUMA is the *multicast announcement*. Each node maintains a *connectivity list* which resembles the multicast routing table in MAODV. Every time a *multicast announcement* is received, the connectivity list is updated. The connectivity list consists of all the routes to the core. The *multicast announcements* are sent frequently to keep the multicast group active. This results in frequent flooding of the multicast group with control messages.

Mesh Maintenance: Each node generates a *multicast announcement* when there is a change in the core or when it receives a fresh *multicast announcement* from one of its neighbors or when there is a change in its mesh member status. If a node does not announce a change in its mesh member status immediately to its neighbors, then it results in packet loss due to outdated mesh member information. The data packets are forwarded until a mesh member is reached. Once a mesh member is reached, the packet is flooded among the mesh members.

2.3.2.3 Comparisons for Multicast Protocols

In [75], Lee et al., compared the performance of five multicast routing protocols. They compared two tree-based multicast protocols namely, AMRoute and AMRIS. The remaining protocols are mesh-based multicast protocols namely, ODMRP, CAMP and Flooding. The metrics used by them to compare these protocols include packet delivery ratio (PDR), ratio of number of data packets transmitted to data packets delivered, ratio of number of control packets transmitted to data packets delivered and number of control and data packets transmitted to data packets delivered. The variables against which these metrics were compared include mobility, number of sources, group size and network traffic load. As expected they concluded that generally mesh-based protocols that contain alternate routes performed better than tree-based protocols. They concluded that ODMRP was very effective and efficient compared to the other four multicast routing protocols. However, the problem with ODMRP as observed by Lee et al. is that with increasing number of sources in the network the overhead increased rapidly.

In [76], Yuo et al. have conducted a research on multicast routing protocols for AHNs. They have arrived at a taxonomy of the multicast protocols based on several protocols proposed in literature. This taxonomy is based on what kind of information of AHNs is exploited by each routing protocol and the roles taken by each node for multicasting. This is insufficient especially when each protocol proposed is applied to various recent applications. It is necessary to have a classification based on more criteria.

In [77], a taxonomy of routing protocols for ad hoc networks is presented. In this chapter, the new class of routing protocols called the multipath routing protocols is detailed with few examples. In [78], a taxonomy of multicast routing protocols for ad hoc networks is provided. The authors have illustrated every multicast routing protocol with simple figures and described the advantages and disadvantages of each protocol.

This thesis compares the performance of the proposed MBEAN routing protocol with that of PUMA and MAODV routing protocols since they were readily available in the network simulator used for simulation.

2.3.3 Application-specific Protocols

Many of the protocols mentioned so far try to find a feasible route from source to destination. Recently more application-dependent protocols have been proposed. The protocol that we propose in this work tries to find a routing scheme that will be useful for selected applications. Our protocol considers applications where large files need to be transferred which is expected to be one of the prospective applications of ad hoc wireless networks.

Compared to the Internet era, wireless networks have emerged more rapidly. The protocols for routing in ad hoc networks have been proposed during the last decade or more. The routing protocol manifested in this thesis is recommended for commercial applications and is based on BitTorrent Protocol, which is introduced briefly below.

2.4 BitTorrent Protocol

The BitTorrent (BT) protocol works at the application layer with the Internet Protocol in the background. Thus, any routing protocol that works in the network layer for Internet applications finding a route from source to destination is sufficient for the BT file distribution system to function. The BT protocol has been in use for over ten years. The main entities of the BT protocol are [79]

- An ordinary web server
- A static *metainfo* file
- A BitTorrent downloader

- The end user web browsers

- The end user downloaders.

To deploy the concept of BitTorrent protocol, a static file with *.torrent* extension, called the *metainfo* file is placed on the web server. This file contains information about the actual file available for download (that is, the actual file's length, name, hashing information and the URL of the tracker). *Tracker* is a server on the Internet that coordinates the actions of the BitTorrent clients. The *tracker* helps peers (end user downloaders) that wish to download the same file identify and connect to each other. *Tracker* returns a random list of peers interested in downloading the same file. *Trackers* also store upload and download rate for the purpose of statistics. During the transfer, the *tracker* provides up-to-date information to the peers about the status of the download and upload, that is, the amount of uploaded and downloaded information and the time left to finish.

Each of the end user downloaders download a part of the file, typically one forth of a megabyte, called a *piece* from the original downloader, also called the seed. Now each end user downloader advertises the *pieces* it has, to the rest of the peers it is connected to, so that, any peer interested in this *piece* can download it from this end user downloader rather than from the original downloader (This causes an overhead of less than one tenth of a percent of the total bandwidth). Thus the download burden is shared among all the peers interested in the file and the download time is also reduced. Cohen [79] details the working of BitTorrent protocol.

The main advantage of using BT protocol is to make every peer who wishes to download a file, share the burden by not just downloading but also uploading *pieces*

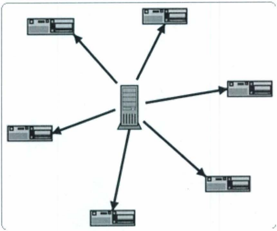


Figure 2.10: Traditional File Sharing Approach taken from [79]

to other peers. Thus the uploading link capacity is not wasted. The multicasting technique or the commonly used file sharing servers work as shown in Figure 2.10. In this figure, the *seed* or source of the file experiences the entire burden of file transfer. Besides, the upload capacities of all the six peers are left unused. The BT protocol conquers this problem by making the peers or end user downloaders share the burden of uploading the file. The model of BT protocol is shown in Figure 2.11. The research carried out in this thesis aspires to apply this concept to AHNs, to assist every node in the network make use of the assigned upload link bandwidth.

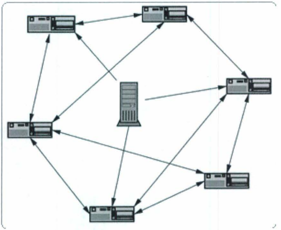


Figure 2.11: BitTorrent File Distribution Approach taken from [79]

2.5 Multipath Routing

All the on-demand routing protocols need the flooding of RREQ, or a similar message through the network every time a route is required to a destination. The source node needs to flood the RREQ message when it first has packets to a particular destination node. However, the flooding does not stop here. Every time the established route fails because of a link breakage or because a node has moved out of its neighbor's range or when a node is dead due to loss of power, the source node needs to flood the RREQ. Such flooding occupies the network bandwidth excessively. Therefore, multipath routing have been proposed that exploit the flooding by finding more than one path between the source and destination.

A few of the multipath routing protocols allow the source to send packets through all the established routes [80]. In certain protocols, the source uses only one path, the best path, to send the packets and when this path fails, the source uses one of the alternate paths that was previously established along with the best path [81, 67, 82]. Other multipath routing protocols find an alternate path from each intermediate node to the destination [83]. That way, any intermediate node fails, its neighbor can use the alternate path from itself to the destination to send packets. Most protocols establish disjoint paths [84]. Two paths are said to be disjoint if they do not have any node that is common to both the paths except for the source and destination nodes. Path disjointness for networks has been discussed by [85].

The routing protocol addressed in this thesis is a multipath protocol that employs only the best path to send packets. When the best path fails, the protocol designates the next best path to send packets to the destination node. The alternate paths, although disjoint, are within the range of each other and therefore, using only one path is effective. Sending through more than one path at a time would only slow down the rate of packet transfer due to severe contention for the channel.

2.6 Network Simulator

Several network simulation tools have been proposed for simulation of network environment. Most of them are event-driven simulators. The most notable among these are ns-2 (network simulator) [4], ns-3 [86], OMNet++ [87], where individual modules are implemented in C++ and the modules are combined together through Network

Description Language (NED) developed for this purpose, SimPy [88], implemented in Python, Java in Simulation Time (JiST) [89] implemented in Java, OPNet [90] also implemented using C and C++ codes and GloMoSim [91] which uses C code with Parsec functions. OPNet is not available for free. [92] is a recent paper that compares these network simulators.

ns-2 was developed by VINT research group at University of California, Berkeley and further extended by Monarch research group at Carnegie Mellon University for wireless networks. ns-2 has a shortcoming in that it was not designed for large networks with hundreds or thousands of nodes that are required for the recent applications like wireless sensor networks. Therefore, a more scalable improvement of ns-2 was introduced in 2008, called ns-3.

Since the simulation phase of the research started earlier than 2008, the most common simulator then available namely, network simulator (ns-2) is used in this thesis for testing and comparing the working of the proposed protocols with the existing protocols already available in ns-2. ns-2 consists of C++ codes with oTcl scripts for controlling the simulations.

IEEE 802.11 DSSS physical layer model is implemented in ns-2. The radio propagation models that have been implemented in ns-2 include free space propagation model, two-ray ground propagation model, and shadowing model. Two-ray ground propagation model is assumed for our simulations. The antennae gains and system losses are assumed to be one in ns simulator.

ns-2.31 has IEEE 802.11 DCF standard MAC protocol implemented in it. IEEE 802.11 protocol implemented in ns-2 follows $RTS/CTS/DATA/ACK$ pattern for all unicast protocols and only $DATA$ packets for all broadcast packets. Thus for all the multicast applications, there is no collision avoidance.

The applications present in ns-2 are virtual. Generally actual packets are not being sent. Instead, the size of the packet and the corresponding time taken to send the packets are used in simulations. The applications that can be assumed to be transmitted by the ns-2 through the transport protocol include, data files through CBR or TCP packets, voice traffic through on-off source and video files through exponential traffic. CBR packets are also used in multicast simulations.

2.7 Application Specific Needs

The applications for which the multicast protocol is presented in this research have specific needs related to the environment in which they will exist. In a ballpark scenario, a group of people could wish to share the statistics of the game. Presentations are held in various buildings in a conference area and a person could wish to attend a talk without being physically present in the presentation hall. In an airport area, people in the gate area and business lounges could wish to share files while waiting for the flight.

All these applications have the following characteristics or needs:

- Nodes willfully join the group for quick dissemination of files
- A few mobile nodes
- Small to moderate size network
- Length of data exchange is not large

- Types of traffic include data, voice and video

Existing multicast routing protocols are designed for general multicasting in AHNs usually for military battlefields, emergency search and rescue operations, classrooms, conference hall and other such applications. Each protocol tries to achieve improved efficiency, robustness, reliability, quality of service, etc. Certain multicast routing protocols have also been designed specific to a particular application. The multicast protocol, called MBEAN, presented in this thesis has been developed to satisfy the above listed needs by using the BitTorrent concept in order to deliver the message among the hosts in an AHN.

2.8 Concluding Remarks

Various OSI layers of the communication model in ad hoc networks and the protocols implementing the functions of these layers are portrayed. This chapter has introduced the need for an application-specific routing protocol for ad hoc networks. The simulators available for characterizing an ad hoc network environment and realizing the routing protocol are listed.

This chapter has presented a basis for the multicast routing protocol, Multicasting in BitTorrent Enabled Ad Hoc Network (MBEAN) and the unicast routing protocol, BitTorrent Enabled Ad Hoc Network (BEAN). The multicast and unicast protocols, namely PUMA, MAODV and AODV, discussed in this chapter will be compared with the corresponding multicast (MBEAN) and unicast (BEAN) protocols illustrated in this thesis. The next chapter will explicate the working of the multicast routing protocol, MBEAN.

Chapter 3

Multicasting in BitTorrent Enabled Ad Hoc Network Routing Protocol

3.1 Introduction

Communication through a wireless link requires more power and the bandwidth available is less when compared with a wired network. Therefore multicasting improves the efficiency of communication in wireless links by sending information to more than one node in a single transmission.

The concept of BitTorrent protocol is used in the BitTorrent file distribution system for sharing information among hosts in the Internet. The BitTorrent protocol aims at sharing the upload and download functionalities among the peers of the network rather than imposing all the upload capability on the source. The source, rather than uploading the file to each peer entirely, will upload pieces of the file to various peers. Each peer in turn takes up the responsibility of acquiring the pieces of the file it needs from other peers. This concept is directly applicable to multicast scenarios, where the multicast hosts can be given the responsibility of sharing the multicast message among each other.

Some of the main applications of ad hoc networks require multicasting. For example, in a conference hall, where several users are connected in an ad hoc fashion, typically a user (say, the speaker) would send a document or data to a set of users. This chapter presents the Multicast BitTorrent Enabled Ad hoc Network (MBEAN) routing protocol which is based on the BitTorrent protocol concept.

This chapter illustrates the basic functionality of the MBEAN routing protocol including the establishment of the group, the various message formats involved and maintenance of the group. The routing properties of MBEAN are discussed in terms of member reliability, packet delivery ratio and control and routing overhead. The analytical proof of member-to-member connectivity is derived. Analytical explanations of packet delivery ratio, and, routing and control overhead are also presented. Simulation results comparing MBEAN with MAODV and PUMA are also discussed.

3.2 Protocol Overview

MBEAN is based on the BitTorrent Protocol where peers communicate between each other for file transfer. The source need not be present until all the peers receive the file in the BitTorrent protocol. As long as one of the peers receives the complete file, the source can withdraw itself from the transfer. Since MBEAN involves transfer of large files to more than one user or node, it follows the BitTorrent Protocol closely. In MBEAN, the source need not be present in the group until all the members of the group have received the complete message. As long as one member of the group (usually the closest to the source) receives the complete message the rest of the members can receive the message in full with high probability.

MBEAN is a mesh-based multicast routing protocol unlike the most commonly known multicast protocol, MAODV [50], which is a tree-based routing protocol. The reason for using a mesh-based approach is the fact that the members of the multicast group can communicate among themselves without the intervention of the multicast group leader (as in the case of MAODV) or core (as in other core-based routing protocols) [73], which causes additional overhead. In MBEAN when each member joins the group it connects itself with several of the existing members. Thus the reception of a packet will be unaffected by the failure of a single path between the member and the source thereby increasing the probability of receiving of the entire information by all the members.

The objectives of the protocol are:

- Group Establishment: Find several paths between multicast members reactively, as discussed in Section 3.3.

- Group Maintenance: Circulate frequent neighbor updating information to keep the mesh alive, as discussed in Section 3.6.

- Message Dissemination: Distribute the multicast message among members as quickly as possible with increased reception probability by all the members, as discussed in Sections 3.9.1 and 3.9.2.

3.3 Group Establishment

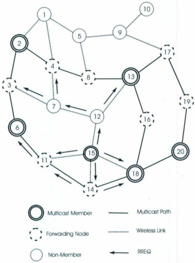


Figure 3.1: Multicast Group Establishment - Path of RREQ

Multicast group establishment in MBEAN begins with a node that wishes to join a multicast group transmitting a Join Route Request (RREQ) message. The node waits for a certain amount of time for a Route Reply (RREP) and if it does not receive any reply, the node concludes that no such multicast group exists. The node keeps sending RREQ until it finds the multicast group. If two nodes are interested in forming a multicast group, they first set their status to be group members and then send RREQ with Join flag set.

A forwarding node is defined as an intermediate node in the multicast group which is involved in routing the packets among the members of the multicast group, but is not actually a member itself. A multicast table consists of a set of entries that provides information about a node's group status and also assists in determining the next hop for a packet. A node that receives the Join Route Request message checks its multicast table to observe if it is a member of the multicast group or if it is a forwarding node for the group. If the node is a member, then it sends an RREP for the request. The multicast group ID is unique for each multicast group established. These two nodes are now members of the multicast group and they share a common multicast group IP address. This way, all the nodes that wish to join the multicast group will send an RREQ message. Thus a multicast group will be established.

Figure 3.1 shows an example of node 15 that wishes to join the existing multicast group indicated by dark circles. Node 15 will broadcast an RREQ message with the join request flag (J) set.

3.4 Message Formats

3.4.1 RREQ Message Format

Figure 3.2 shows the format of an RREQ message. Type (1 byte long) is 1, indicating that this is an RREQ message. If the source or the node requesting the route has a minimum bandwidth (BW) requirement, or a maximum tolerable delay, it includes these values in the RREQ. If any intermediate node does not see the minimum re-

<table>
<tr><td colspan="6">0</td><td>31</td></tr>
<tr><td colspan="2">Type</td><td>J</td><td>R</td><td>RREQHpCnt</td><td>RREQFwdHpCnt</td><td>minBW..</td></tr>
<tr><td>...</td><td colspan="3">MaxDelay</td><td>CurMinBW</td><td>CurMxDly</td><td></td></tr>
<tr><td colspan="7">RREQ ID</td></tr>
<tr><td colspan="7">Destination IP address/Multicast group IP address</td></tr>
<tr><td colspan="7">Source IP address</td></tr>
<tr><td colspan="7">Source neighbor IP address</td></tr>
<tr><td colspan="7">Timestamp</td></tr>
</table>

Figure 3.2: Route Request Message Format (RREQ)

quired link capacity, it discards the RREQ message (since the BW constraint was not satisfied). Similarly, if the delay experienced so far by the RREQ is greater than the maximum delay, then the node discards the RREQ message (since the delay constraint was not satisfied).

The destination address is the multicast group address. There is no multicast group leader unlike MAODV. The source IP address (4 bytes long) is the address of the node initiating the route request. This is the node wishing to join the multicast group (also called as route requesting node). Timestamp (4 bytes long) carries the time at which the source sends the request. This allows to determine the time taken by the RREQ message to reach a particular node.

If a multicast group exists, which is the case here, each non-member increments the Hop count (1 byte long) by one and forwards the RREQ message. If the node is a multicast forwarding node, then it also increments the RREQ Forwarding Hop Count. Each node that receives the join request updates the route information in its multicast routing table.

Multicast Route Table Entries:

- MulticastGrpIPAddress
- SourceAddress
- HopCntToNearestMembers
- NearestMembers
- NextHopAddresses
- TTL
- minBW
- maxDelay

Time to live (TTL) is the time in terms of number of hops for which the RREQ will be valid. In Figure 3.1, TTL is set to 3. After transmitting the join request (which is the RREQ with the Join flag set), the node (node 15 in the figure) waits for RREP up to RREP_WAIT_TIME. If it does not receive any reply then it assumes that a multicast group does not exist and sends the RREQ message again with increased TTL value. TTL is incremented by 2 for each attempt of the same request.

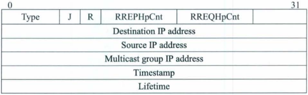
There may be many sources for a single multicast group. There is no need to maintain the address of all these sources. As long as the message is from one of the group members, the node will accept the data packet. The next hop addresses of both to and from routes are recorded in the next hop addresses linked list shown below.

NextHopAddresses - Linked List Entries:

- NextHop
- ConnectMember
- HopCountToMember
- LinkDirection
- LinkExpiry

If a particular node is a multicast group member, then it updates the routing table and replies with a Route Reply (RREP) message to the node that initiated the request.

3.4.2 RREP Message Format



0					31
Type	J	R	RREPHpCnt	RREQHpCnt	
Destination IP address					
Source IP address					
Multicast group IP address					
Timestamp					
Lifetime					

Figure 3.3: Route Reply Message Format (RREP)

Figure 3.3 shows the format of the RREP message. Type (1 byte long) is 2 indicating that this is a route reply message. A is the acknowledgment flag which means that the RREP needs an acknowledgment from the neighboring node. Nodes set this on an individual basis depending on whether they need a RREP_ACK or not from the node to which they sent the RREP message. The RREP hop count (1 byte long) is incremented and if this node is a member of the multicast group, then the RREP member hop count (1 byte long) is also incremented. The hop count of the RREQ is also attached so that the source node (that initiated the join request) can decide on the best route based on the hops traveled by the RREQ. The RREP ID will be the same as the RREQ ID, so that each intermediate node and also the source would know to which RREQ the RREP corresponds. Lifetime (4 bytes long) indicates the time for which the RREP is valid. If the source does not receive the reply within this time, the RREP is discarded.

The requesting node gets several RREPs as shown in Figure 3.4. Now the source of RREQ (node 15) has a multicast neighbor route table, shown below, containing details about the multicast tree that it has formed from routes (not the complete route, but the destination address, and next hop address) to each member of the group. It uses all these routes for sending or forwarding multicast packets.

Multicast Neighbor Routing Table Entries:

- MulticastGrpIP
- MulticastMemberIPAddresses

Once a multicast group has been established, any node (multicast source) that wishes to send information to the group will simply send the packets of the information

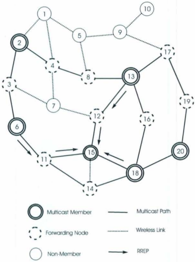


Figure 3.4: Multicast Group Establishment - Path of RREP

to each of the member nodes to which it is attached through its neighbors. Each of these member nodes will in turn send the packets that they receive to the member nodes to which they are attached. This way, the burden of sending the information is not constrained to just a set of nodes but is shared by all the nodes in the multicast group. This is similar to the functioning of the BitTorrent Protocol.

3.4.3 MCAST_P Message Format

<table>
<tr><td>Type</td><td>Flags</td><td>Reserved</td><td>MCAST_P Hop Count</td></tr>
<tr><td colspan="4">Group Destination IP Address</td></tr>
<tr><td colspan="4">MCAST Source IP Address</td></tr>
</table>

Figure 3.5: Multicast Prune Message Format (MCAST_P)

If a multicast member wishes to sever itself from the multicast group, it sends a multicast prune message. The message format of the prune message is shown in Figure 3.5. The prune message is sent to all the members that this node is attached to. The multicast members on receiving the prune message will remove this node from their multicast neighbor routing table.

3.5 Routing Through Forwarding Nodes

Figure 3.6 shows a section of a multicast group where node 18 is a multicast member and receives several requests to join the group. For multicast route establishment, each member node receiving the requests should keep track of the number of multicast

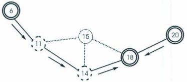


Figure 3.6: Routing Through Forwarding Nodes

forwarding nodes along the path from itself to the requesting node to which it will be attached. Thus when the node has to choose a route, it chooses the one which travels through most of the existing forwarding nodes, node 14 in this figure, rather than the one with shortest route. The route thus chosen should not be too long. Therefore, a limit on the route is employed such that

$$2(h_f^{'}) \geq h_f, \tag{3.1}$$

where $h_f^{'}$ is the hop count through non-forwarding nodes and h_f is the hop count through forwarding nodes.

When this condition is not satisfied, use of non-forwarding nodes might be faster for other multicast group members to receive the packets. The multiplication factor of two can be established through simulation. The member node updates its multicast route table with the address of the requesting node. The requesting node also adds one entry for each member of the multicast group in their multicast route table. Now the source of RREQ has a multicast neighbor route table containing details about the multicast tree that it has formed from routes (not the complete route, but the destination address) to each member of the group, as does the replying multicast member.

3.6 Group Maintenance

In order to maintain connectivity with other group members or forwarding nodes leading to group members, each node sends a proactive message called the *hello* message. The *hello* messages are broadcast frequently by each node that has an entry in its multicast routing table. This message is received by its neighbors and they keep their multicast routing table entries containing this node, active.

There is no need for a core (as in the case of PUMA) or a group leader (as in the case of MAODV) to maintain the multicast group established. If a node does not receive any *hello* message from its neighbor node which is present in its routing table, for *allowed_hello_loss* times, then that neighbor node is assumed to be absent. In other words, any multicast connection entry through that neighbor is removed from the multicast routing table.

3.7 Advantages of Group Establishment in MBEAN

In MBEAN, the new node will establish routes with all the nearest member nodes. That is, each node forms a tree with itself as the root and routes to other nearest members (not all) of the multicast group as the leaves. Overall, the structure would be a mesh. Since each member node is attached to more than one member node, it can receive messages from any of them. Thus when a route fails due to link or node failure, there is no need for reestablishing that route unless a multicast member is separated from the group completely, in which case, the member sends an RREQ message and initiates connection to the group.

In order to have a fresh enough route and fresh values for delay and bandwidth through any route, only the destination or multicast group member can send the RREP, since the traffic at this instant is responsible for the observed delay, and, a previously stored route will have an outdated delay value.

3.8 Comparison with MAODV, PUMA and ODMRP

In comparison with MAODV, in our protocol, only the multicast group member or destination can respond to a RREQ. Although this might cause an increase in the time involved in connection establishment, it will give a fresh delay and BW measure during connection set up. In addition, there is no need for a group leader in MBEAN, which directly relates to the simplicity of the algorithm.

MBEAN has been implemented as a reactive routing protocol. In other words, the route is formed only when there is a message available to be multicast. Although MAODV is a reactive routing protocol, improved MAODV implemented for ns-2 is based on a proactive approach. The routing tables are updated frequently even if there is no route required.

Apart from being proactive, the implementation predicts when the link might break and just before the link breaks, new routes will be constructed. Thus the MAODV protocol is able to establish an alternate route before a link fails thereby helping it to recover from a link failure much faster or eliminating the time spent on recovering from failure. Since the basic and improved implementations of MAODV are based on forming a multicast tree, this kind of route reconstruction is necessary.

In the case of MBEAN, there is no need to construct a new route when a link fails since MBEAN is a mesh-based protocol and several alternate routes will be available. A node checks the available next hops and sends the packet to those nodes. If a node detects that the link to reach a multicast member is broken, it simply removes that particular entry from its routing table. If there are no upstream nodes for a multicast member, then it sends an RREQ message to join the group. Although this could be time consuming, the chances of such a situation occurring are low due to the availability of several alternate routes. If several links fail, some time would have to be spent on reestablishing parts of the mesh. However this is not a major concern as multiple failures do not occur frequently in a dense network containing only a few mobile nodes.

Among the several multicast routing protocols proposed, this thesis compares the performance of MBEAN with that of MAODV and PUMA. MAODV is a tree-based routing protocol while PUMA is a mesh-based routing protocol. Both MAODV and PUMA are based on establishing a core, in the case of MAODV, the core is the group leader of the tree whereas in PUMA, the core is established dynamically and serves as a contact between the multicast members. ODMRP is another mesh-based routing protocol that has been proven to be better than many mesh-based routing protocols [52]. In spite of having a core, the control overhead in PUMA is claimed to be orders of magnitude smaller than in MAODV and ODMRP while achieving the same packet delivery ratios.

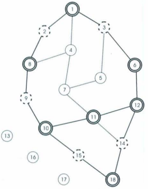


Figure 3.7: Example Scenario

3.9 Routing Properties of MBEAN

The routing properties of the protocol are explained with the help of an example scenario shown in Figure 3.7. Consider a scenario of 18 nodes with a multicast group size of 7 members. Nodes 1, 6, 8, 10, 11, 12 and 18 are chosen as multicast group members with Node 1 acting as the source. In this particular case, for the sake of simplicity in analysis, the source is also a member of the multicast group. In general, the source need not be a group member. When the source node has packets to send, it establishes communication with the multicast group, when it automatically becomes a multicast group member.

In Figure 3.7 nodes 2, 3, 9, 14 and 15 act as forwarding nodes in the multicast mesh. When there are only 7 members in the group, each member is connected to more than one member. Although, this results in multiple copies of each packet being received by each member, it supports higher packet delivery ratio.

MBEAN is not an exact ad hoc network replica of the BitTorrent protocol. However, it has made use of the peer-to-peer independency of the BitTorrent protocol. For instance, in the above example, node 6 might not receive the packet from the source node since the source node has disconnected itself from the network. As long as the source node, node 1, is able to send the entire message to at least one of its neighbors, namely node 2, the message will reach all the group members with high probability. For example, in Figure 3.7, member 6 is connected to two other members. If node 6 does not receive the packet from the source node, it is still capable of receiving the packet from member 12. This independency of the members on the source node is due to the increased member-to-member connectivity and therefore, reliability.

The routing properties that are discussed in the following subsections include member reliability, packet delivery ratio and, control and routing overhead. Analytical models are used to design protocols since they provide a concise preview of the protocols behavior before the actual deployment. Thus when the network is deployed, it can be characterized faster.

3.9.1 Member Reliability

The advantage of measuring the member-to-member connectivity is lucid in the following definition of member reliability. *Member reliability* of a packet is 1, if it has been received by all the members, and, is 0, if it has not been received by at least one member. Member reliability for the simulation is defined as the ratio of the total number of packets with member reliability of 1 to the total number of packets sent. Therefore, the more members each member is connected to, the more the member-to-member connectivity, which increases the member reliability of the mesh.

The analytical expression for member-to-member connectivity in MBEAN is derived as follows.

Assume a network where n nodes and m multicast members are uniformly distributed in an area $A_0 = a \times a$ with a transmission range of each node, R. Average number of members, m_1, within the transmission range of any member, m_i, can be expressed as

$$m_1 = \frac{\pi R^2}{A_0} m. \tag{3.2}$$

Consider two members m_i and m_j in this network, shown in Figure 3.8. The

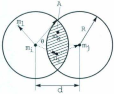


Figure 3.8: Member Connectivity in 2-hop Range

Euclidean distance between these two nodes can be given as

$$d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}, \tag{3.3}$$

where (x_i, y_i) is the location of node m_i, and (x_j, y_j) is the location of node m_j. The member m_i may establish direct contact with m_1 members if the distance, d, between them is less than R. Therefore, probability that m_i can have a direct link to m_1 members can be expressed as,

$$P_1(d) = \begin{cases} 1, & d < R \\ 0, & d \geq R. \end{cases} \tag{3.4}$$

Let the number of members whose distances lie between R and $2R$ be represented as m_2. Consider the case in which member m_i needs to establish connectivity with m_2. In such a case, the probability that m_i can connect to m_2 members can be expressed as,

$$P_2(d) = 1 - \left(1 - \frac{A}{A_0}\right)^{n-m}, \tag{3.5}$$

where, A is the intersection area given by,

$$A = 2R^2(\theta - \sin\theta\cos\theta) \tag{3.6}$$

and $\theta = \cos^{-1}(d/2R)$. Equation (3.5) establishes the probability that at least one of $(n-m)$ nodes is present in the intersection area A. This is illustrated in Figure 3.8 where, m_i and m_j, whose distance d is within R and $2R$, establish member connectivity through node n_i.

Consider the case in which the member m_i has no direct link with m_t members that are located at t-hops and cannot communicate with fewer than t-hops. In this case, let m_t be the number of members located at t-hop distance from m_i, as shown in Figure 3.9. Let $w(r)$ be the probability of being able to establish communication within an intersection area A. If this area is increased by dA by increasing r to $r+dr$ as shown in Figure 3.9, then the probability of being able to establish a communication within the new area, dA, can be written as,

$$[P_{t-1}(r) - P_{t-2}(r)]2r\phi/A_0, \tag{3.7}$$

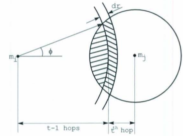


Figure 3.9: Connectivity between Two Nodes at t-hop Distance

where,

$$\phi = \cos^{-1}\left(\frac{d^2 + r^2 - R^2}{2dr}\right). \tag{3.8}$$

The term $P_{t-1}(r) - P_{t-2}(r)$ in (3.7) denotes the probability of reaching a member node that is at a distance r in exactly $t-1$ hops.

This approach is similar to that of Chandler [93] and is based on the assumption that connecting members are exactly $t-1$ hops away from member m_i and one hop away from the member m_j. Equation (3.7) is based on the assumption that a connection has been established up to a distance of $t-1$ hops and thus has to be solved iteratively. The probability of not establishing a communication using any node in the transmission area within limits $d-R$ and $d+R$ is given by $[1-w(r)]^{n-t}$, where,

$$w(r) = \int_{d-R}^{d+R} \frac{[P_{t-1}(r) - P_{t-2}(r)]A'}{A_0} dr \tag{3.9}$$

and $A' = 2r\phi$. The probability of not being able to establish a connection with t hops or less is given by

$$1 - P_t(d) = [1 - P_{t-1}(d)][1 - w(r)]^{n-t}. \tag{3.10}$$

Therefore, the probability that the member, m_i, can connect to m_t members can be expressed as,

$$P_t(d) = 1 - [1 - P_{t-1}(d)] \cdot [1 - w(r)]^{(n-m-t)} \tag{3.11}$$

where, $w(r)$ is defined in (3.9) and, $A' = 2r\phi$ and $\phi = \cos^{-1}(\frac{d^2+r^2-R^2}{2dr})$. The recursive method of determining the probability of member-to-member connectivity given in (3.11) assumes that the connecting members are exactly $t-1$ hops away from member i and one hop away from member j [94].

Since the members are uniformly distributed, distance d between any two members m_i and m_j can be computed up to t hops. Connection probability between these two members can be evaluated using (3.2), (3.4) or (3.11).

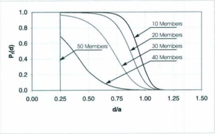


Figure 3.10: Probability Distribution of Member-to-member Connectivity

Figure 3.10 shows the variation of probability of member-to-member connectivity versus distance (d)between any two members normalized with respect to their transmission range (a) up to 5 hops for an area of 1000 m × 1000 m with a transmission range of 250 m. The curves represent results for 10, 20, 30, 40 and 50 member cases for a network of 50 nodes.

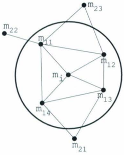


Figure 3.11: Connectivity for the Limiting Case

For the 10 member case out of 50 nodes, each member can be connected with as high as 95% probability with most of the other nine members in the group. For the case of more than 10 members in the group, the probability for a member to connect to all the other members in the group decreases. However, each member will still be connected to close to 10 members with 95% probability.

When $n \rightarrow m$, $p_2(d) \rightarrow 0$, which reflects the limiting case that m_i can only be connected to m_1 members as shown in Figure 3.11. With reference to Figure 3.10, this refers to the 50 member case, in which a member is only connected to the members that are in its transmission range. This is directly associated with the progress of route request packets that stop at members. In other words, the route request packets from a member stop at the member's neighbors (who are also members) since all nodes are members.

The above derivation shows that each member is connected to more than one member via several paths which results in higher member reliability.

3.9.2 Packet Delivery Ratio

Packet delivery ratio (PDR) is defined as the ratio of total packets delivered successfully (to each member averaged over all the members) to the total packets sent by the source. Several paths are established connecting the multicast members. The success probability of each of these paths is affected by the collision probability of the individual links. Due to uneven traffic in the network the collision probability of every link is dissimilar. Thus, the success probability of each path, i, with n_i hops, may be expressed as,

$$q_i = (1 - p_{i_1})(1 - p_{i_2}) \cdots (1 - p_{i_{n_i}}), \tag{3.12}$$

where, $p_{i_1}, p_{i_2}, \ldots, p_{i_{n_i}}$ is the collision probability of links n_i, along the path (i). Since all the paths are being used to receive packets from the source node, each multicast member may receive more than one copy of each packet, thereby achieving higher PDR. The PDR for a multicast member can be calculated as

$$PDR = S_1 \cdot q_1 + S_2 \cdot q_2 + \cdots + S_k \cdot q_k, \tag{3.13}$$

where S_1 to S_k are the number of packets sent by path (1) to path (k). In this case, if only the best path was present, the PDR would converge to the success probability of that path. The presence of alternate paths allows for more packets, which were otherwise collided and dropped in the best path, to be delivered, thereby increasing the overall PDR at any particular member.

3.9.3 Routing and Control Overhead

The overhead is defined as the additional information sent in order to successfully transmit a data packet. Routing overhead is defined based on the packets sent to exchange routing information, including establishing the multicast group. Control overhead is defined based on the additional control packets sent in order to identify active neighbors.

Each node that wishes to join the multicast group sends a RREQ packet. Thus, the total number of RREQ packets generated is bound by the number of members in the network. Similarly, each node that receives a RREQ packet forwards it only once. Thus, the total number of times a single RREQ packet will be forwarded is bounded by the size of the network. Thus for a network with n nodes and m members, the total number of RREQ packets that will be sent across the network is upper bounded by,

$$O_{RREQ} \leq n \cdot m. \tag{3.14}$$

Consider x nodes out of m that are already a part of the multicast mesh (as forwarding nodes), then they need not send new RREQs to join the group. The new bound would then be,

$$O_{RREQ} \leq n \cdot (m - x). \tag{3.15}$$

The number of RREP packets is generally equal to the number of alternate paths discovered by each member to connect it to other members multiplied by the number of hops for each resultant path. For the best path between each multicast member and the source, the number of RREPs can be given by,

$$N_{RREP} = \sum_{i=1}^{m} f_{l_i} \cdot h_i, \tag{3.16}$$

where, m is the number of members in the group, f_l is the link distance pdf, and, h is the average number of hops corresponding to the distance. If each member m has exactly one alternate path, then the number of RREPs can be given by,

$$N_{RREP} = \sum_{i=1}^{m} f_{l_i} \cdot h_i + \sum_{j=1}^{m} f_{a_j} \cdot t_j, \tag{3.17}$$

where, f_a is the link distance pdf for the alternate path, and, t_j is the average number of hops for the alternate path.

3.10 Conclusions

This chapter presents the protocol specifications and working of MBEAN, a multicast routing protocol which is based on the notion of BitTorrent Protocol used in Internet for fast file transfer. The establishment of the multicast group, maintenance of the group and dissemination of the multicast message among the members of the group are illustrated in detail with a model scenario. The simplicity of the algorithm in comparison with other multicast routing protocols like MAODV, ODMRP and PUMA is explained. In addition, MBEAN shows unique characteristics of increased member-to-member connectivity which not only results in improved packet delivery ratio, but also higher reliability.

The routing properties of MBEAN are illustrated with an example scenario. An analytical expression for member-to-member connectivity, which affects the reliability is presented. For a typical scenario of a 50-node network, it was shown that each member can be connected to at least 10 members with very high probability. Analytical explanations for packet delivery ratio are also given. A bound on the total number of routing and control packets that will be sent in the network is discussed.

The next chapter compares the performance of MBEAN with MAODV and PUMA through simulations. From the simulation results it will be concluded that MBEAN shows higher and consistent PDR, better member reliability, and, smaller control and overall overhead than both MAODV and PUMA.

Chapter 4

Performance Analysis of MBEAN Protocol

4.1 Introduction

The key features of AHNs, such as quick deployment and circulation of messages, make them well-suited for applications, where reliability and robustness are crucial such as ballpark, conference area and airport. The merits of the MBEAN protocol, presented in Chapter 3, is verified in this chapter through extensive simulations.

The chapter compares the performance of MBEAN with that of MAODV, a representative of tree-based protocols and PUMA, representing mesh-based protocols by subjecting them to diverse simulation conditions. The protocols are quantitatively compared to project the difference in their behaviors and to elucidate that MBEAN is preferred for a short-lived network.

Simulation methodology used in the comparison of the protocols are presented.

Analytical expressions derived in Chapter 3 have shown that high member-to-member connectivity can be achieved in MBEAN. In this chapter, simulations are conducted to manifest the effect of high member-to-member connectivity on member reliability and PDR. The analytical bounds of overhead discussed in the previous chapter are also substantiated in simulations. All these properties are investigated against metrics such as traffic load, group sizes and number of senders.

4.2 Simulation Model and Methodology

The simulation is implemented using the network simulator (ns-2) [4] as discussed in Chapter 2. 50 nodes are uniformly distributed in a simulation area of 1000 m × 1000 m. The transmission or the radio propagation range of each node is 250 m and the carrier sense range is 550 m. Although the signal can be sensed at a much lower SNR level, a conservative estimate of -65 dBm receive power to decode a packet and -90 dBm receive power for carrier sensing has been assumed by ns-2. With these values a carrier sense range of 550 m can be obtained. The channel capacity or the data rate is set at 2 *Mbps*. The simulation time is set to 500 s. Each scenario is tested for 10 runs of varying random seeds and the results are averaged. The packet size is fixed at 256 *bytes*.

4.2.1 Channel and Radio Model

Two-ray ground reflection model is used in the simulations. According to this model, two nodes have a direct path and a ground reflection path. The model behaves as a free space propagation model with shorter distances between two nodes. The transmission power is set at 0.2818 W, which correspondes to 250 m transmission range. The simulator defaults are assumed for other parameters.

4.2.2 Medium Access Control

IEEE 802.11 MAC protocol with Distributed Coordination Function (DCF) is assumed in the basic access mode. DCF is used for ad hoc mode. The access pattern is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Fragmentation of the packets did not seem relevant at this point where the data packets sizes are assumed to be fixed and small (256 *bytes*). However, it is possible to introduce fragmentation when the need for combining packets for the implementation of network coding arises.

4.2.3 Traffic Pattern

Constant bit rate (CBR) traffic sources arrive from the traffic generator. The arrival rates are varied for each scenario based on the traffic load required. TCP packets could not be used in the multicast simulations since multicast is inherently broadcast. With TCP packets acknowledgments are required. Thus the simulations were tested with CBR traffic over UDP.

4.2.4 Metrics

The metrics used to evaluate the performance of the MBEAN and compare it with MAODV and PUMA are packet delivery ratio (PDR), member reliability, and, routing and control overhead. The variables against which these metrics are compared include, group size, traffic load and number of senders. These metrics have been defined in the previous chapter.

4.3 Simulation Results

4.3.1 Packet Delivery Ratio

4.3.1.1 Effect of Traffic Load

For a single source and 50 nodes in the network, the packet delivery ratio is now measured for increasing traffic load. Figure 4.1 shows the PDR results for various group sizes of 10, 30 and 50 members.

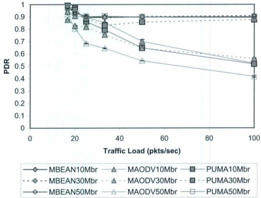


Figure 4.1: Load vs. PDR for Various Group Sizes

The inter-arrival time (IAT) of packets is varied and consequently the traffic load varies. As seen in Figure 4.1 above, as the load increases, the packet delivery ratio of MAODV drops for obvious reasons of increasing contention for the channel. However, MBEAN achieves almost a constant PDR. At light loads, MBEAN is able to deliver above 90% of the packets. As the load increases, for 30 and 50 members, MBEAN is able to maintain the delivery ratio around 90%. With low number of members in the network, the PDR is maintained above 90%. In the case of PUMA, the 10 member case shows the least PDR for heavy traffic load. This is because, in PUMA, with smaller group sizes, there are insufficient alternate paths between the members of the group. This results in PUMA and MAODV having similar PDRs for smaller group sizes. For higher group sizes PUMA's performance is similar to that of MBEAN. With lower load, the PDR of MAODV is high. As the load increases, more packets are sent per second and more redundant control messages to maintain the group (Group Hello message) are sent and consequently, the PDR drops. In MAODV, as the traffic load increases, the PDR drops as much as 40%.

The PDR curves shown in Figure 4.1 also show the upper and lower confidence limits assuming t-distribution. The derivation is shown in Appendix A. Since the upper and lower prediction limit values are negligible, they are not shown in the rest of the simulation results.

4.3.1.2 Effect of Group Size

The scenario is now tested for packet delivery ratio for increasing number of group members in the network. Number of members varies from 5 members in a network of 50 nodes to all 50 nodes acting as members. The packet delivery ratio is tested for

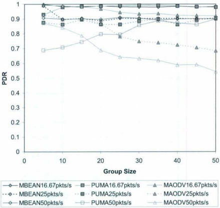


Figure 4.2: Group Size vs. PDR for Various Loads

different load conditions varying from 16.67 *packets/s* to 50 *packets/s*. The results are plotted in Figure 4.2.

It can be seen that as the group size increases, the PDR remains almost a constant for MBEAN. MAODV shows a gradual fall in the PDR for increasing group size. PUMA shows improved PDR for increasing group sizes. The difference in PDR for the smallest group size to the highest group size is generally less than 5% for MBEAN. This is also true for PUMA for lighter loads. For MAODV, as the group size increases, the PDR drops as high as 30% in some cases. It should also be noted that the PDR is above 90% for smaller group size for MBEAN and above 85% for MAODV. However, the PDR of PUMA is as low as 70% with heavy loads and smaller group sizes.

The effectiveness of the MBEAN multicast routing protocol as a function of the multicast group size can be seen from this figure. The little or no change in the performance of MBEAN for increasing group size is because of the new multicast members present within the existing multicast mesh. There is very little need to create new paths to connect to all the members as the group size increases. The presence of alternate paths among the multicast members assists in achieving a steady PDR in this case. MAODV needs to expand the tree structure to include the new multicast members as the group size increases. The tree structure of MAODV is such that there is only one path between a source and each multicast member. Therefore, a break in any link causes a major drop in PDR. As discussed previously, PUMA fails to show good connectivity between members for smaller group sizes.

4.3.2 Member Reliability

4.3.2.1 Effect of Load

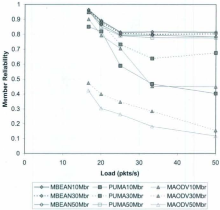


Figure 4.3: Traffic Load vs. Member Reliability for Various Group Sizes

The member reliability as defined in the previous chapter is tested with various loads. The load is varied from 16.67 *packets/s* to 50 *packets/s*. The performance is tested for various multicast group sizes ranging from 10 to 50 members in the group. The network size is 50 nodes.

From the Figure 4.3 it can be seen that as the load increases, the reliability reduces for all the three protocols, namely, MBEAN, PUMA and MAODV. As expected, MAODV shows much lower reliability for increased load compared to MBEAN. MAODV also shows lowest reliability for 30 and 50 member cases. PUMA shows lower member reliability for 10 member case compared to 30 and 50 member cases.

The reduction in reliability is due to the increased packet transmissions within the network with increasing load. As the load increases, more transmissions are present in the network challenging the reception of each packet by all the members of the group. With increasing load, even if at least one member does not receive a packet, then the member reliability is seriously affected. Although PUMA showed higher PDR for increasing loads compared to MAODV, it fails in terms of member reliability for smaller group sizes.

4.3.2.2 Effect of Group Size

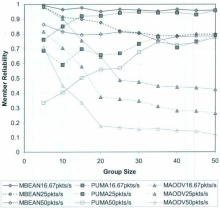


Figure 4.4: Group Size vs. Member Reliability for Various Traffic Loads

The scenario is now tested for member reliability. For various group sizes, the member reliability is measured as the ratio of the number of packets received by all the members of the group to the number of packets sent. The results are plotted in Figure 4.4 for various cases of traffic load from 16 packets per second to 50 packets per second.

With increasing group size, the protocols are expected to show a drop in reliability, because as the group size increases, the probability that all the nodes will receive each packet will reduce. That is, with high probability at least one member might not receive a packet, which results in lower member reliability. However, MBEAN loses only 10-15% of member reliability for increasing group size. MAODV loses at least 50% of reliability with increasing group size. For lower loads, the member reliability is high for MBEAN and MAODV. As the load increases, MBEAN is able to maintain reliability within 15% of the reliability under low load conditions. MAODV shows twice the drop of MBEAN. PUMA is unique in the results it produces. As with the PDR, the member reliability is lower for smaller group sizes and increases with increasing group size.

The results show that MBEAN is highly reliable compared to MAODV and PUMA. Some of the reasons that make MBEAN so reliable are the presence of multiple alternate paths among the multicast members (for small and large group sizes). Even if the source detaches itself from the group after sending the packets, as long as at least one of the members receives a packet, with very high probability all the members receive the packet. Although the presence of multiple alternate path introduces redundancy in the network, the high reliability achieved, compensates for the redundancy. As will be seen later in the chapter, the overhead involved in achieving

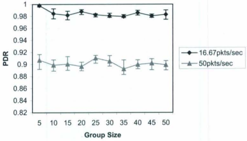


Figure 4.5: Group Size vs. PDR for MBEAN with Confidence Interval

such a high reliability is not too high and is lower in many cases.

The PDR and member reliability curves obtained for MBEAN have been calculated as an average over 10 scenarios, various group members and traffic loads. Assuming t-distribution, the 95% upper and lower prediction limits (UPL and LPL respectively) to the average PDR values are plotted in Figure 4.5. The UPL and LPL PDR values do not vary by more than 2% in the figure. The availability of UPL and LPL PDR values facilitate forseeing the results of experimental set up. Moreover, knowing the UPL and LPL PDR values shows the sensitivity of the PDR values to varying scenarios.

4.3.3 Control and Routing Overhead

The following discussion examines the performance of the protocol in terms of overhead. In this thesis, overhead is defined as the additional packets, containing information about the routes and about each other's neighbors, sent in order to support successful data transmission. This thesis classifies overhead as routing and control overhead. Routing overhead is defined as the the ratio of the number of routing packets (or bytes) sent to the total data packets (or bytes) successfully delivered.

The routing overhead of all three protocols are compared based on the number of routing packets each protocol sends to establish the multicast tree or mesh. The routing packets include RREQ and RREP. The RREP packets are followed by ACK (acknowledgement) packets sent by the MAC layer. Since the performance of the routing protocol is of concern, the ACK packets are not included as part of the routing overhead. Generally, in the simulations, 90% of the routing overhead is consumed during the initial multicast tree or mesh establishment. The remaining 10% is consumed during the simulation, when any route fails either due to link failure or due to mobility.

Control overhead is measured as the ratio of the number of control packets (or bytes) sent during the simulation (or during the data transfer) to the total data packets delivered throughout the simulation. The control packets include frequent HELLO packets sent to maintain the neighbor node details. Control packets in MAODV include both HELLO and GROUP HELLO (GRPH) messages. The GRPH messages are sent by the group leader frequently to maintain the tree structure and to advertise the address of the group leader to the multicast members and other nodes that are part of the multicast tree. In PUMA, it is difficult to clearly distinguish between routing and control packets. Therefore, the control packets sent before the actual transfer of data packets are taken as routing packets and the control packets sent during data transfer are taken as control packets. There are no specific RREQ or RREP packets in PUMA. Therefore, it is not possible to compare the number of

RREQ and RREP packets in PUMA with the other two protocols.

4.3.3.1 Effect of Load on Routing Overhead

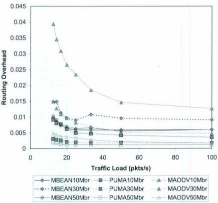


Figure 4.6: Traffic Load vs. Routing Overhead for Various Group Sizes

Figure 4.6 shows the amount of routing overhead for various traffic loads. The figure shows the routing overhead as a function of load in *packets/s*.

As the load increases, the routing overhead reduces contrary to initial expectation. This is because, as the load increases, the routing protocol is able to send more data packets for the same routing packets. Thus, the ratio of the routing packets to data packets successfully delivered reduces. As can be seen in this figure, the routing overhead is higher for MAODV for the 10 member case than MBEAN. This is due to the need for electing a group leader in MAODV. MBEAN shows higher routing overhead compared to MAODV and PUMA in all other cases. In MAODV, as the group size increases, the overhead in group leader election is less compared to the number of data bytes that are being sent. PUMA shows the least routing overhead since it does not differentiate between RREQ and RREP packets. All the routing information is present in the control packets exchanged at the start of the group establishment.

4.3.3.2 Effect of Load on Control Overhead

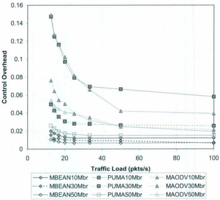


Figure 4.7: Traffic Load vs. Control Overhead for Various Group Sizes

Figure 4.7 shows the control overhead for various traffic loads. Control overhead consists of HELLO packets in the case of MBEAN used to exchange neighbor node information. In the case of MAODV, the control overhead consists of both the HELLO messages and GRPH message sent by the group leader of the multicast group to inform the group about the address of the group leader. The results are plotted for three cases of multicast group sizes (10, 30 and 50 members).

With increasing load, MBEAN shows consistently low control overhead. Control overheads of MAODV and PUMA reduce with increasing load. This is because, as load increases, the number of data packets successfully sent by the two protocols increases. However, the number of control packets remains the same for both MAODV and PUMA. As the load increases, the control overhead reduces from 0.15 to 0.06 for the 10 member case for MAODV. In MBEAN, even as the load increases greatly, it does not involve sending more control messages. In fact, the ratio of control packets to the data packets remains the same for increasing loads for MBEAN.

The reason for the steady control overhead in MBEAN is due to the fact that the control message that is being sent is the HELLO message sent every second by the nodes that are part of the multicast group, either acting as forwarding nodes of the group or multicast members. The increase in these messages is consistent with the increase in the data packets sent that there is very little change in the resulting control overhead. The overall control overhead for MBEAN is much less than that of MAODV since it does not involve frequent GRPH messages. Similarly, PUMA needs to send more control messages to maintain the multicast group information compared to MBEAN. The frequent HELLO messages are sufficient for MBEAN to maintain the group information.

4.3.3.3 Effect of Load on Overall Overhead

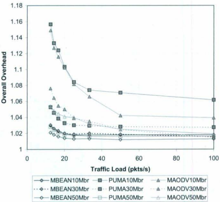


Figure 4.8: Traffic Load vs. Overall Overhead for Various Group Sizes

Figure 4.8 shows the number of additional packets that need to be sent for each data packet. For example, the scale along the y-axis shows that for each data packet to be successfully received, the amount of overhead ranges from 0.01 to 0.16. As before, various loads are applied to the scenario. The scenario is also tested for various multicast group sizes. This figure contains the resultant of both the routing and control overhead.

Based on the figure, it can be noticed that MBEAN involves lower overall overhead than MAODV and PUMA. MBEAN is also less sensitive to increasing traffic loads and increasing group sizes. PUMA on the other hand, shows the highest overall overhead for smaller group sizes and the an overhead as low as MBEAN for larger group sizes. Thus, PUMA is clearly suitable for larger group sizes and almost unsuitable for smaller group sizes.

4.3.3.4 Effect of Group Size on Routing Overhead

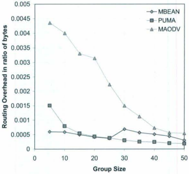


Figure 4.9: Group Size vs. Routing Overhead

Figure 4.9 shows the deviation of routing overhead for various group sizes. The routing overhead is now plotted in terms of ratio of bytes of routing packets to bytes of data packets. The group size is increased from 5 members in a network of 50 nodes to all 50 nodes behaving as members. The case is tested for a load of 12 to 13 *packets/s* and for two sources. The reason for testing this with 2 sources is to see the discrepancy in the working of MBEAN and MAODV varying number of sources in the group.

As can be seen in this figure, the routing overhead of MAODV is much higher than MBEAN and PUMA with smaller group sizes than with larger group sizes. As discussed earlier, the routing overhead of MBEAN is higher for larger group sizes.

In this case, the routing overhead of MAODV is much higher due to the presence of two sources. As the number of sources increase, the routing overhead of MAODV is higher as more time has to be spent in finalizing the group leader. Since MBEAN has no group leader, having more than one source does not greatly affect its routing overhead. However, as will be seen in the next figure, the control overhead of MBEAN increases with increasing number of sources. The routing overhead of PUMA is unaffected by the increasing number of sources.

4.3.3.5 Effect of Group Size on Control Overhead

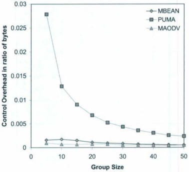


Figure 4.10: Group Size vs. Control Overhead

Figure 4.10 shows the control overhead plotted in terms of bytes of control packets to bytes of data packets delivered. Again the load is set at 12 to 13 *packets/s* and the multicast group has two sources.

The control overhead of MBEAN is higher than that of MAODV. It should also be noted that the control overheads of both the protocols appear to approach each other as the group size increases. The control overhead of PUMA is the highest for two sources. For two sources, the control overhead of PUMA is much higher than MAODV and MBEAN.

Since both the multicast sources belong to the same multicast group, there will be only one group leader for MAODV. Thus, only one set of GRPH messages will be sent for both the sources, thereby reducing the overall control overhead. The frequency of HELLO messages (every sec) in MBEAN cannot be compromised as, that is what keeps the mesh fresh enough. As will be seen in the next figure, this will not greatly affect the overall overhead for each data packet delivered. PUMA needs more control packets to maintain the groups with two sources.

4.3.3.6 Effect of Group Size on Overall Overhead

In Figure 4.11, the total overhead, that is the sum of routing and control overhead in terms of bytes to the total data bytes delivered is shown. The number of sources is set at 2 and packets arrive at the rate of 12 to 13 *packets/s*.

Although the control overhead of MBEAN is higher than that of MAODV, the overall overhead incurred on the data packet is less for MBEAN. PUMA involves the highest overall overhead in ratio of bytes. This figure shows the routing and control bytes sent per data byte delivered.

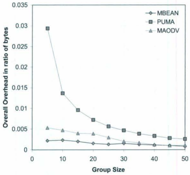


Figure 4.11: Group Size vs. Overall Overhead

The overhead of MBEAN is low compared to MAODV for smaller group sizes. Thus for the two source case, MAODV needs more routing packets to achieve a tree structure. MBEAN does not show much increase in the routing overhead for the two-source case. However, as the group size increases, the two protocols show very similar total overhead. Although PUMA has low routing overhead, the control overhead is so high for the two sources case that the overall overhead of PUMA is highest of the three protocols.

4.4 Discussion of Results

The previous section discussed in detail all the simulation cases and the results obtained from each case as a comparison among the three protocols namely MBEAN, PUMA and MAODV.

4.4.1 Packet Delivery Ratio

MBEAN is able to keep its delivery ratio fairly constant for increasing group sizes and traffic loads. PUMA, on the other hand behaves consistent with the way mesh-based protocols operate by showing improved delivery ratios for larger group sizes and for lower traffic loads. Furthermore, as with any tree-based multicast protocol, MAODV displays poor delivery ratios for increased traffic loads and group sizes.

4.4.2 Member Reliability

Member reliability of MBEAN reduces for increasing group sizes and traffic loads, but the rate of reduction is much lower compared to both PUMA and MAODV. In fact, PUMA once again shows poorer member reliability for smaller group sizes than larger group sizes unlike both MAODV and MBEAN. The member reliability of MBEAN follows its PDR more closely than that of MAODV and PUMA. As a matter of fact, the difference is higher for MAODV than for PUMA, since MAODV has a single path connecting all the members while PUMA has fewer paths for smaller group sizes than for larger group sizes. Member reliability following PDR closely emanates from the fact that, as long as one member receives the multicast message, the member is able to disperse the message to all the remaining members in the group successfully.

4.4.3 Overhead

All the three protocols follow the receiver-initiated approach in joining the muticast group. However, PUMA involves the election of one of the members as a core in the multicast group. MAODV, on the other hand, involves the election of a group leader.

Conversely, MBEAN is a distributed protocol that does not involve a group leader or core as in the case of MAODV or PUMA respectively. In MBEAN each member cares only about its connection with the nearest multicast members in the group. No member is aware of the complete set of nodes present in the nodes.

The routing overhead of MBEAN is higher than both PUMA and MAODV for a single source, since it establishes connection with multiple members in the group. With increasing number of sources, MAODV shows higher routing overhead than MBEAN and PUMA, inspite of its shared-tree approach. However, the control overhead of MBEAN is much lower than both MAODV and PUMA. In fact, PUMA shows highest control overhead for both single and two source case for smaller group sizes. Comparing the results of overall overhead for all the three protocols, MBEAN shows lowest overall overhead irrespective of the number of sources.

4.5 Conclusion

The objective of this chapter is to conduct a performance evaluation of three multicast protocols, MBEAN, MAODV and PUMA. The network simulator has enabled a fair and accurate comparison of the protocols under varying simulation environments for a range of parameters including multicast group size, traffic load, and number of senders.

A general conclusion from the simulation analysis is that, under different traffic loads and varying group sizes, MBEAN exhibits robust performance in terms of PDR and member reliability while incurring low overall overhead. The mesh-based approach in MBEAN involves several redundant messages, however, it delivers the highest PDR and member reliability. PUMA, which also uses the mesh-based approach lacks sufficient alternate paths connecting the members for smaller group sizes and therefore delivers fewer packets which in turn degrades the member reliability. MAODV portrays a typical tree-based multicasting approach by showing low performance for increased loads.

The scenarios tested consist of uniformly distributed nodes in a square network. Generally AHNs consist of a non-uniform deployment of nodes, various types of incoming traffic such as voice, video and data, and, occasional mobile nodes. Formulating and maintaining a multicast group in the presence of such demanding nodes is challenging. The next chapter discusses the applicability of MBEAN to various realistic network scenarios that represent the applications of interest more closely.

Chapter 5

Performance Analysis of MBEAN in Selected Applications

5.1 Introduction

Interactive media services are contemplated to be a major application area in AHN communications. Examples of such services include data, voice and video. Typical application domain that handle such services include ballpark area, conference area, an airport waiting area, etc. In this chapter, MBEAN is evaluated in these concrete ad hoc environments. The applicability of MBEAN in such realistic situations is investigated and a comparative analysis with other protocols like, PUMA and MAODV, is carried out. This chapter discusses the most common applications for which the MBEAN protocol was designed.

In a ballpark scenario, a group of people could wish to share their comments about the game. Presentations are held in various buildings in a conference area and a person could wish to attend a talk without being physically present in the presentation hall. In an airport area, people in the gate area and business lounges could wish to share files while waiting for the flight.

An overview of these applications for which MBEAN is considered suitable is presented in this chapter. The simulation environment for each application and the results of the simulation for three protocols namely, MBEAN, PUMA and MAODV are illustrated. The strengths and drawbacks of MBEAN and other protocols are discussed for various realistic situations.

5.2 Practical Applications

In a typical ad hoc network domain, nodes communicate with each other by establishing groups. The applications listed in the previous section are portrayed in this section based on the kind of traffic and size of the network they demand. The traffic types include data, voice and video sources. The type of devices that might use such traffic include Blackberry, IPhone, etc. The traffic arrival rates are chosen to be close to real rates. Normally a Blackberry's upload rate starts from 6 *kbps* to 25 or 33 *kbps*. The file sizes have been chosen at a moderate size of 4.5 MB video file, 1.5 MB data file. We assume that video files are compressed before being shared. Voice sources are generally not characterized using a file size, but are characterized by arrival rates and duration of messages.

The applications considered include nodes that willfully join the group for quick dissemination of files. Thus they include few mobile nodes with a small to moderate size network. The nodes are assumed to be randomly distributed within the network.

That is, the nodes have equal probability of being present in any location in the network. A good approximation of such a reference distribution is the uniform distribution. The applications that are elaborated in the following subsections include ballpark scenario, conference area and airport area.

5.2.1 Ballpark Scenario

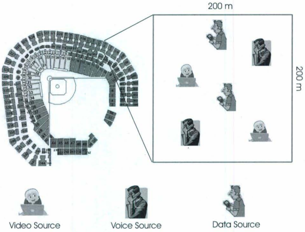


Figure 5.1: Ballpark Scenario

The ballpark AHN application includes nodes seated among the audience who wish to exchange their comments about the game or bet about the outcome of the game. Such nodes, if mobile, are expected to move at walking speed. The length of the data exchange is not long enough for the walking speed to significantly affect the performance of the protocol. The type of traffic generally present in a ballpark would be data source. Such data sources rely on high member reliability. Devices that are generally used in such an application include ITouch, IPod Touch, IPhone, Blackberry, IPad, or sometimes netbooks.

An example of the ballpark scenario is shown in Figure 5.1 with uniform distribution of nodes in a square area. Although a ballpark may be pictured as rectangular area, the intention is not to provide coverage for the entire ballpark. Presence of several access points within the ballpark will suffice to provide overall coverage. The aim is to quickly spread the message within a small to moderate sized group.

This figure shows a ballpark with a small area that is interested in sharing information zoomed in. This area shows the typical seating arrangements and the possible position of nodes interested in exchanging information.

5.2.2 Conference Area Scenario

The second application discussed in the thesis includes a conference area where presentations and panel sessions are expected to take place simultaneously at various rooms or halls. Persons interested in attending a presentation from locations other than the presentation hall could do so by connecting to the presentation. A person may also be following two different presentations concurrently taking place at two different halls in the conference area. People generally wait in lounges where seats are provided. Within the conference area there may be rooms that are unoccupied. In such a case, the distribution is unlikely to be uniform.

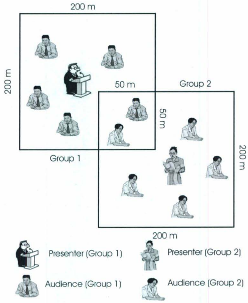


Figure 5.2: Conference Area

We have chosen a network as shown in Figure 5.2 where, two square networks overlap diagonally for a small square area. Thus, there are both empty spaces in the network and densely populated areas. This shows a typical node distribution in a conference area. The types of sources primarily present in a conference application include voice and video. Both of them can tolerate low member reliability. Wireless devices generally used in such an application are laptops and netbooks.

5.2.3 Airport Waiting Area Scenario

The third AHN application is an airport waiting area. People (nodes) may be waiting in the gate areas or business lounges and would want to continue the business meeting or share opinions post meeting during the wait. The type of devices that are generally used in such an application are laptops, Blackberry, IPhone, IPod, Cellular phone etc. Here the nodes may be mobile or stationary.

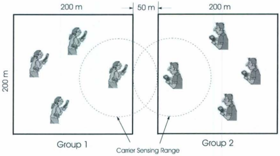


Figure 5.3: Airport Waiting Area

Variables	Values
Channel bandwidth	2 $Mbps$
Transmission range	50 m
Carrier sense range	110 m
Packet size	256 bytes
Number of nodes	50
Capture threshold	10
Group sizes	10, 20, 30, 40, 50

Table 5.1: Simulation Parameters

Generally there may be more than one group exchanging information simultaneously in a small area. Such a scenario is shown in Figure 5.3. In this figure, two groups are separated by a distance equal to the transmission range so that they are within the carrier sense range of each other. This case will show how each group's member reliability is affected by the presence of another group within the carrier sense range of some of the nodes and members involved in the group.

5.3 Simulation Models

In this section, the parameters set in the simulations run to evaluate and compare MBEAN protocol with PUMA and MAODV under realistic scenarios are summarized. Table 5.1 lists some of the parameters. Omni-directional antenna is assumed for each node and two ray ground propagation model is used. The capture threshold indicates the signal to interference ratio. If this ratio is greater than 10, then the signal is received successfully. The following are some of the cases for which the performance of MBEAN protocol is tested against that of PUMA and MAODV. Below, each case is described in terms of the traffic arrival rate, size of the network, duration of the traffic source, and the possible source-destination combinations.

5.3.1 Various Types of Sources

In this case, a network of size 200 $m \times 200$ m is considered with 50 nodes in the network. Various traffic sources are tested such as data, voice and video. This scenario is well suited for ballpark application where a quick group can be established among the spectators in the surrounding area. For the data source, constant bit rate packets arrive at the source for the duration of the simulation at rates 50 *kbps* and 80 *kbps*. Due to the inherent broadcast nature of multicast, TCP packets which require acknowledgments are not tested.

For the voice source, ON-OFF traffic generator is used with arrival rates of 64 and 69 *kbps* and a pause time of 90 s. We use Pareto traffic source for voice with on and off burst of 50 ms. Realistically, both speakers will not talk at the same time and when one talks the other listens. Therefore on-off traffic source is ideal for voice. For the video source, exponential traffic arrival is used with arrival rates of 73 and 100 *kbps*. Simulations are run between 100 and 200 s based on the length of the message and the applied load.

5.3.2 Simultaneous Groups

Two different groups which are separated by a distance of 50 m are establishing communication among themselves as shown in Figure 5.3. This type of scenario is suitable for both airport and conference area applications. The network is of size 450 m × 200 m, with two 200 m × 200 m square networks separated by a distance of 50 m along the x-axis. The two groups transmit and the PDR and member reliability of the groups when they transmit simultaneously and separately are compared. The network has 100 nodes in all, with each 200 m × 200 m square consisting of 50 nodes.

Each group has a data source with an arrival rate of 25 $kbps$. The members and nodes that are within the carrier sense range of the other group are affected by the other group's transmissions. Thus the overall member reliability is expected to be affected. The amounts by which the reliability is affected for various protocols are discussed in this case. Only data sources are tested for overlapping groups, since the performance of a protocol is more affected by the arrival rate of packets than the actual type of traffic source (inferred from the results of testing various traffic sources in Section 5.4.1).

5.3.3 Overlapping Groups

The scenario consists of two groups overlapping each other as shown in Figure 5.2. The size of the network is 350 m × 350 m with a 200 m × 200 m square network along the top left corner and bottom right corner. There is an area of intersection where both the groups overlap. This is a 50 m × 50 m square. One member is chosen to be common to both the groups. This is an example of a typical conference area. The waiting area is in the center. Presentations are taking place at two corners of the network. A person interested in both the presentations is sitting in a waiting area attending both the talks. A similar scenario with 3 common nodes is tested. The new network size is 300 m × 300 m with a 100 m × 100 m intersecting area. In this case, the PDR and member reliability are plotted against traffic load rather than group size. The group size is not chosen as a variable since then, it would not possible to put a limit on the number of members or nodes that overlap.

5.3.4 Mobility

The case with mobile nodes shows that MBEAN is better than MAODV and PUMA in spite of the presence of mobile nodes. The speed of the mobile nodes is set at a constant 1 m/s walking speed. Out of 50 nodes, only 10 nodes are assumed to be mobile. The mobile nodes have a pause time of 90 s. To avoid the disadvantages of the random mobility model (where in the ns-2 implementation of the model the speed of a mobile node would eventually slow down to zero over a period of time), the minimum speed is set to a value greater than zero. In fact, since the mobile nodes are assumed to be walking, the minimum and maximum speeds are both set to 1 m/s. The packet arrival rates for data, voice and video are 25 $kbps$, 32 $kbps$ and 30 $kbps$ respectively.

5.4 Simulation Results

This section reviews the simulation results for the cases listed in the previous section. The simulations are run using ns-simulator. In addition to MBEAN, two protocols, PUMA, an example of a mesh-based multicast protocol, and, MAODV, an example of tree-based multicast protocol are also implemented in the simulator. The results of the three protocols are compared to understand the difference in performance and the uniqueness of MBEAN. The metrics used for comparison of the three routing protocols, MBEAN, PUMA and MAODV are packet delivery ratio (PDR) and member reliability.

5.4.1 Various Types of Sources

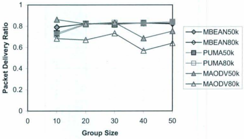


Figure 5.4: Group Size vs. PDR for Data Source

Figure 5.4 shows the variations in packet delivery ratio for various group sizes for the three protocols. The simulations are conducted for two different traffic arrival rates. From the figure, MBEAN shows very consistent PDRs for both the traffic rates and for various group sizes. PUMA is always affected by smaller group sizes due to the presence of insufficient alternate paths among the multicast members.

With increasing group size, PUMA is able to have member-to-member connection with fewer hops while at the same time have fewer number of overall transmissions. With increasing group size, MBEAN faces increasing number of transmissions. This however does not affect MBEAN's PDR although it is less than that of PUMA by an insignificant percentage. On the other hand, PDR of MAODV is affected by increasing traffic load.

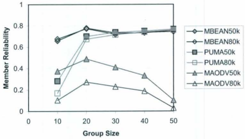


Figure 5.5: Group Size vs. Member Reliability for Data Source

Figure 5.5 shows the plot of group size versus member reliability for the same protocols. Here, the difference in member reliability for increasing traffic load is explicit for MAODV. The difference is explicit for PUMA for smaller group sizes. The member reliability of PUMA is very poor for smaller group sizes making it unsuitable for data applications such as the ballpark AHN scenario.

The PDR results of voice source and video source are shown in Figures 5.6 and 5.7. The member reliability results of voice and video sources are also shown in Figures 5.8

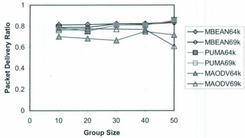


Figure 5.6: Group Size vs. PDR for Voice Source

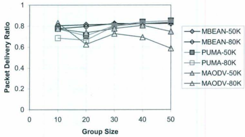


Figure 5.7: Group Size vs. PDR for Video Source

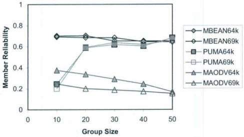


Figure 5.8: Group Size vs. Member Reliability for Voice Source

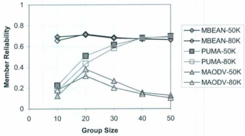


Figure 5.9: Group Size vs. Member Reliability for Video Source

and 5.9. The results are consistent with those for data traffic.

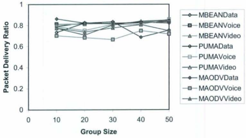


Figure 5.10: Group Size vs. PDR for Various Traffic Sources

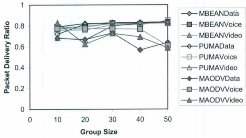


Figure 5.11: Group Size vs. PDR for Various Traffic Sources

Figure 5.10 shows the plot of PDR for various traffic sources for all three protocols for light load of 50 *kbps* for data, 64 *kbps* for voice and 73 *kbps* for video source. Here, irrespective of various types of sources, MBEAN has consistent PDR results. PUMA shows lower PDR for smaller group sizes for various traffic sources. But the difference in PDR for various sources is more for the 10 and 20 member cases. MAODV, on the other hand, shows higher PDR for data source and for smaller group sizes and lower PDR for voice source for all cases. These results show that each protocol gives importance to various sources, yet their performance is more dependent on the actual arrival rate of packets.

Referring to Figure 5.11, which shows PDR for heavy load of 80 *kbps* for data, 68 *kbps* for voice and 100 *kbps* for video, both MBEAN and PUMA show similar results for varying traffic loads. However, MAODV is inconsistent. It should however be agreed that overall MAODV shows poor results compared to PUMA and MBEAN. Looking at the subtle difference in the performance of the three protocols, it can be noted that their performance depends on the arrival rates of the packets more than on the type of traffic source.

5.4.2 Simultaneous Groups

In this case, the three protocols are compared based on whether the two groups present within carrier sense range of each other are affected by each other or not. Figure 5.12 shows the packet delivery ratio for the three protocols without the presence of simultaneous groups and with their presence. It can be noted that the difference is very minor.

Figure 5.13 shows the corresponding member reliability values for the same case. It can be inferred from this figure that all three protocols are affected by the presence of another group in the carrier sense vicinity. However, the difference is the lowest in the case of MBEAN compared to PUMA and MAODV. The two protocols PUMA and MAODV show a big drop in member reliability when all nodes are group members. This makes them unsuitable for larger group sizes within the airport or conference area.

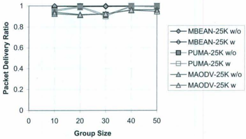


Figure 5.12: Group Size vs. PDR for Simultaneous Groups

5.4.3 Overlapping Groups

In this case, only two protocols, namely, MBEAN and PUMA are compared. Since MAODV has shown poor performance for all the cases discussed previously no performance improvement is expected in this case and hence excluded from comparison. Figure 5.14 shows the packet delivery ratios of MBEAN and PUMA with simultaneous and independent transmissions of both the groups that include a common member. When the two overlapping groups are not transmitting simultaneously, MBEAN and

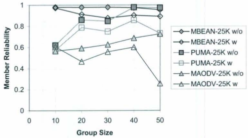


Figure 5.13: Group Size vs. Member Reliability for Simultaneous Groups

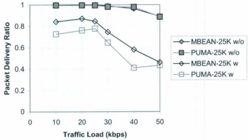


Figure 5.14: Traffic Load vs. PDR for Overlapping Groups (one overlapping member)

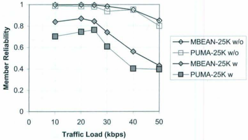


Figure 5.15: Traffic Load vs. Member Reliability for Overlapping Groups (one overlapping member)

PUMA show similar results for a traffic arrival rate of 25 *kbps* data source.

When the two groups transmit simultaneously, *one member* which is common to both the groups, is expected to receive from two different sources and therefore show *poor PDR* for this member which would result in poor overall member reliability. However, in this case, the overall PDR is also affected for both MBEAN and PUMA. The rate of reduction in PDR in MBEAN is less than that of PUMA. Figure 5.15 shows that member reliability follows PDR very closely for both the protocols. Figure 5.16 shows the PDR when 3 members overlap out of 50 nodes. The results are similar to the one overlapping node case. However, here the member reliability, shown in Figure 5.17, does not follow PDR closely. This is because with increasing number of overlapping nodes, there are more chances that at least one member will not receive a packet.

In both the above cases, there is a drastic reduction in PDR and member reliability

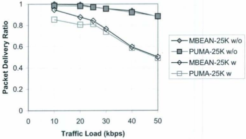


Figure 5.16: Traffic Load vs. PDR for Overlapping Groups (3 overlapping members)

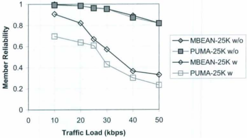


Figure 5.17: Traffic Load vs. Member Reliability for Overlapping Groups (3 overlapping members)

from the figures. This is because, in the overlapping case, the *load* is varied. That is, the load is increased and the corresponding PDR and member reliability are measured. With increasing load and the presence of overlapping node(s), the two protocols show a drastic reduction in the PDR. The overlapping nodes get overloaded and therefore there are more collisions in the intersecting area which may contain routes to other members and which is densely populated. This is a typical example of the non-uniform distribution of nodes present in the conference area.

5.4.4 Mobility

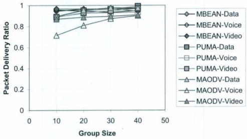


Figure 5.18: Group Size vs. PDR for Mobile Case

From Figure 5.18, due to the breakage of links owing to mobility, MAODV shows lower PDR for smaller group sizes. The presence of a single path to form a multicast tree is a disadvantage in this case. However, MBEAN shows very consistent PDR for various group sizes. PUMA also shows good PDR but the member reliability

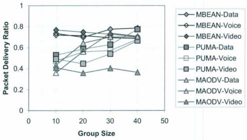


Figure 5.19: Group Size vs. Member Reliability for Mobile Case

of PUMA for smaller group sizes is very low under mobile conditions, as shown in Figure 5.19. The group size is varied from 10 to 40. Instead of keeping all nodes to be members we avoid having a mobile destination. Generally it is assumed that source and destination are stationary in both unicast and multicast applications.

5.5 Discussion of Results

From the results discussed in the previous section, MBEAN shows robust performance for diverse applications and for various loads and group sizes.

In the above simulations, the transmission range is chosen such that it will suffice to establish a multicast group within a moderate number of hops. For a network of this size, if the transmission range is higher, then most of the multicast members can be reached within one or two hops. In such cases, the effectiveness of the presence of alternate paths in MBEAN protocol is not explicit. When the number of hops between members extends beyond one or two hops, the availability of alternate paths will become an advantage. Thus, when members are located in the corners of the network, MBEAN is able to establish several alternate paths between the multicast members.

In MAODV, the converse is true. When members are located within one or two hops of the source, MAODV shows the best performance in terms of PDR and member reliability. When the members are located towards the corner of the network, the tree established by MAODV consists of more than one or two hops and that results in loss of packets on the way through lossy links. This effect is more pronounced with small group sizes and heavy loads. Therefore, to be fair, members are selected randomly for each simulation.

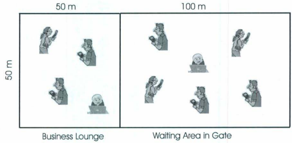


Figure 5.20: Airport's Business Lounge and Gate Area

To illustrate the above discussion, the airport scenario has also been tested for a rectangular area which usually occurs when a group needs to be established between

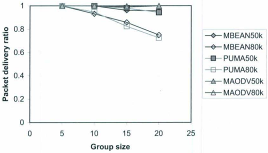


Figure 5.21: Group Size vs. PDR for Data Source and Rectangular Area

a gate area and a business lounge as shown in Figure 5.20. In such cases, it is inferred that a tree structure (as in the case of MAODV) is well suited. The limited number of nodes present along the y-axis in a rectangular area becomes a challenge in establishing alternate paths between members. Since MBEAN greatly relies on the presence of alternate paths between members, the additional transmissions involved become a hindrance rather than support the overall packet delivery ratio. Thus MBEAN is unsuitable for very small networks with insufficient nodes to form alternate paths.

This has been concluded from simulations carried out for a small network of 150 m × 50 m with a transmission range of 25 m. In this case, the formation of the rectangle with y-axis being twice that of the transmission range, it is not possible for MBEAN to establish alternate paths. Therefore, the performance of MBEAN is inferior compared to MAODV, which uses a tree structure to form the multicast group. The rectangular area is well suited for the tree structure and so, MAODV shows superior results. The PDR of such an example case is shown in Figure 5.21. This figure shows the PDR for two different traffic arrival rates of 50 *kbps* and 80 *kbps*. From this figure, it can be observed that MBEAN and PUMA both show similar but poorer results than MAODV.

5.6 Conclusions

This chapter discusses various applications with concrete scenarios to which MBEAN routing protocol can be applied. From the results presented in Section 5.4 MBEAN shows consistent results irrespective of the size of the group. PUMA shows poor performance for smaller groups and superior performance for larger groups. For large groups, MBEAN behaves on par with PUMA.

With large groups, the number of retransmissions for a single packet increases in MBEAN thereby causing more collisions. Each member is capable of receiving more than one copy of a packet in MBEAN. This can be used for convenience, especially in the case of larger group sizes by the introduction of network coding. The source can combine more than one packet in each transmission through each path to multicast members. The members could eventually abstract the individual packets from a combination of transmissions.

The conclusion is that MBEAN is a better choice for the AHN applications disclosed in this chapter. MBEAN works better than MAODV and PUMA in nearly all situations. However, MBEAN is not suitable for small rectangular networks due to insufficient alternate paths among multicast members. It is insurmountable to realize a routing protocol that is optimal for all or most scenarios and operating conditions.

Nevertheless, there is always a need for application-specific routing protocols. The next chapter discusses the working of the BEAN routing protocol for unicast communications with example scenario.

Chapter 6

BitTorrent Enabled Ad Hoc Network Routing Protocol for Unicast Traffic

6.1 Introduction

This chapter describes the Bittorrent Enabled Ad Hoc Network (BEAN) routing protocol developed for unicast communications in a multicast domain. BEAN routing protocol applies the concept of BitTorrent Protocol used in BitTorrent File Distribution System, discussed in Chapter 2, by sharing the routing information among several nodes in the network. The BitTorrent Protocol used in traditional Internet aims at sharing the upload and download functionalities among the peers of the network rather than imposing all the upload capability on the source. The source, rather than uploading the file to each peer entirely, will upload pieces of the file to various peers. Each peer in turn takes up the responsibility of acquiring the pieces of the file it needs from other peers. The concept of BitTorrent Protocol has been found to be suitable for multicast routing in AHNs. The BEAN routing protocol is presented in this chapter to support unicast routing for multicast applications.

Paths are said to be *disjoint* when a communication is established between a source node and a destination node via multiple paths, given the paths do not meet anywhere except at the source and destination. BEAN is a multipath routing protocol that establishes multiple disjoint paths between source and destination nodes in an ad hoc network. Two paths are said to be disjoint when they do not have any common intermediate node. By maintaining multiple paths instead of a single path as in the case of AODV, the protocol is able to continue the communication between the source and destination nodes in spite of a failure of a node or a link or mobility of an intermediate node along the path. This reduces the control overhead involved in establishing a new path when there is a failure.

The probability distribution of disjoint multiple paths for a set of nodes distributed in an ad hoc network is also derived in this chapter. The distribution is obtained analytically by the convolution of the probability distribution of the link distance between any two nodes (source and destination nodes) and the probability distribution of the number of hops required to establish a connection between the two nodes in a random network. Such a connection probability obtained using Binomial distribution, for reasons discussed in Section 6.4.2, is for the best path in any multipath routing protocol. The probability of having at least one alternate path between the two nodes with two or more hops is also obtained. The analytical formulations are validated with simulations conducted using network simulator [4].

6.2 BitTorrent Enabled Ad Hoc Network Routing

6.2.1 Protocol Overview

Assume an ad hoc network that consists of nodes distributed randomly over a certain area. The nodes in the network communicate with each other either directly (if they are in the same transmission range) or via other nodes in the network (multihop). Routing protocols may also be single path or multipath. Multipath routing protocols establish more than one path between the source and destination nodes, so that when one path fails, the source node can send packets through one of the alternate paths thereby increasing the overall packet delivery ratio [95].

BEAN routing protocol is a multipath routing protocol wherein the packets are transmitted through the best path, and the alternate paths are available as a substitute. When the best path fails, one of the alternate paths is selected for transmission of the remaining message to the destination node. BEAN routing protocol forms multiple *disjoint* paths. The primary objectives of the protocol are:

- Route discovery: Find a path only when it is necessary or on-demand
- Route maintenance: Circulate frequent neighbor updating information to keep the routes alive
- Route recovery: Rapidly switch to existing active alternate path during path failure

6.2.2 Route Establishment or Discovery

By sending hello messages, each node can identify its neighbors. When the source node needs to communicate with a destination node, it makes a route request (RREQ) (the same RREQ packet in MBEAN with the Join flag cleared) to all its neighbors as shown in Figure 6.1 which is the same as in traditional ad hoc networks. In Figure 6.1 node 1 (S) is the source node. In the RREQ message, the source also indicates the minimum bandwidth (BW) required for the route from source to destination and also the maximum delay that it can tolerate for the route from source to destination. Each neighbor receives the request, and, if it is not the destination node, forwards the request to its neighbors. Before forwarding the request, each node increments the hop count, and also updates the BW and delay values. This way, the request reaches the destination, node 8 (D) in this figure.

6.2.2.1 Reverse Route Formation

Each node also updates its routing table with the reverse route information. The reverse route information consists of the address of the source node and the next hop, which is the previous hop from which the request was received, to reach the source node. Such an update is called reverse route formation and is shown in Figure 6.1 in dotted lines. Each node also sets a Time To Live (TTL) until which the reverse route information will be valid. The routing table entry of each node consists of the following information:

- Destination IP address
- Next Hop IP address

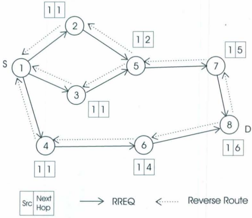


Figure 6.1: Path of RREQ and Reverse Route Formation

- Number of hops to reach destination
- Source neighbor for this route
- minimum bandwidth
- maximum delay
- Time to Live

Now, the destination would have received several requests through its neighbors along with details like BW, delay and hop count. The destination node replies (RREP) through all the neighbors as shown in Figure 6.2, as solid lines, instead of just one RREP as in the case of traditional ad hoc networks. In Figure 6.2, node

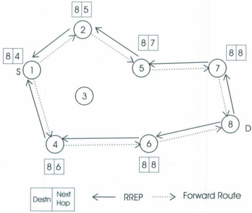


Figure 6.2: Path of RREP and Forward Route Formation

8 (D) is the destination node. The destination node appends the BW, delay and hop count details along with the RREP message to the source. If a node does not receive an RREP until Time To Live (TTL), then it invalidates the reverse route entry.

6.2.2.2 Forward Route Formation

Each intermediate node that receives the RREP, updates its routing table by activating the reverse path. Each node also adds a new entry to its routing table. This new entry will contain the forward route information, that is, the address of the destination node and the next hop address to reach the destination node. This is called the forward route set up. The forward route formation is shown in Figure 6.2 as dotted lines. Once the forward path is set, any packet received by the intermediate nodes will eventually be forwarded to the destination.

The source gets several RREPs through its neighbors. Each RREP contains details such as the minimum bandwidth along the route from source to destination, maximum delay along the route and also the hop count for the communication from source to destination through a particular route. The source now enters these values in its routing table (similar to the metainfo file in BitTorrent protocol). Once the routing table is updated, the source node implements a simple algorithm (sorting algorithm) to decide on a particular route (the best route) from the information on several routes received. The source then sends packets to the destination through this selected route. The remaining routes will be stored in the routing table in the source node. In fact, the source node only stores the next hop address and the destination address as part of storing the alternate routes.

6.2.3 Route Failure and Recovery

If a link on the route between the source and destination fails or a node leaves the currently active route, then the node that detects the failure will send a route error message (RERR) back to the source using the reverse path formed. The source decides on the next available (and best) route from the previously saved routes for communication between the source and the destination nodes. Ad hoc networks are prone to frequent changes in the network topology and therefore, maintaining more than one alternate route has become a requirement.

6.2.4 Message Formats

6.2.4.1 RREQ Message Format

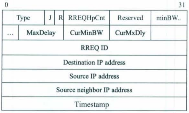
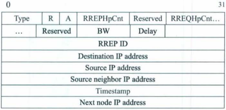


Figure 6.3: Route Request Message Format

In BEAN, the way the source differentiates one route reply corresponding to a route from that corresponding to an alternate route is by appending the source's first neighbor along with the route request message. That is, the source sends each route request with a RREQ_ID as shown in Figure 6.3. When the RREQ message reaches the next node, that is, when the source's immediate neighbor receives the RREQ, it will append the RREQ message with its own address so as to differentiate this RREQ from the RREQ received by another neighbor of the source. In Figure 6.3, Type (1 byte long) is 1, indicating that this is an RREQ message. R is the Repair flag and is set to repair a broken link or a failed node locally. It will find a new route to the next hop specified in the Destination IP address. A local Route Reply will be sent for this request and the packets will bypass the broken route through this new route established locally. If there is no broken link, R flag is not set.

If the source has a minimum bandwidth (BW) requirement, or a maximum tolerable delay, it includes these values in the RREQ. If any intermediate node does not meet the minimum required link capacity, it discards the RREQ message (since the BW constraint was not satisfied). Similarly, if the delay experienced by the RREQ so far is greater than the maximum delay, then the node discards the RREQ message (since the delay constraint was not satisfied). The destination IP address (4 bytes long) is the address of the node that the source wishes to communicate. The source IP address (4 bytes long) is the address of the node initiating the route request or the node that wishes to communicate with destination. Timestamp (4 bytes long) indicates the time at which the request was dispatched by the source node. Timestamp assists in calculating the time taken for an RREQ to reach the destination node through a certain path.

6.2.4.2 RREP Message Format

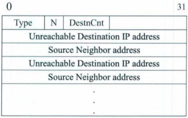


0					31
Type	R	A	RREPHpCnt	Reserved	RREQHpCnt...
...	Reserved		BW	Delay	
RREP ID					
Destination IP address					
Source IP address					
Source neighbor IP address					
Timestamp					
Next node IP address					

Figure 6.4: Route Reply Message Format

If the destination is within 5 hops, then the destination replies to the RREQ with an RREP message the format of which is shown in Figure 6.4. In Figure 6.4, Type (1 byte long) is 2 indicating that this is a route reply message. R is the repair flag indicating that this is an RREP for a repairing RREQ. A is the acknowledgment flag which means that the RREP needs an acknowledgment from the neighboring node. This is set by each node depending on whether it needs an RREP_ACK or not from the node to which it sent the RREP message. This flag is usually set if the node sending the RREP message is not sure of the link availability to the neighboring node. The RREP hop count (1 byte long) is incremented. The hop count of the RREQ is also included along so that the source will decide on the best route based on the hops traveled by the RREQ. The RREP_ID will be the same as the RREQ_ID so that each intermediate node and also the source would know to which RREQ the RREP corresponds.

6.2.4.3 RERR Message Format


0 31

Type | N | DestnCnt

Unreachable Destination IP address

Source Neighbor address

Unreachable Destination IP address

Source Neighbor address

.
.
.

Figure 6.5: Route Error Message Format

The source node receives several RREPs as shown in Figure 6.2 and selects one route for transmission as explained previously. If a node sees a broken link to its neighbor, it will send an error message called route error message (RERR) to the source. The source may then use one of the alternate routes available. The RERR message format is shown in Figure 6.5. In Figure 6.5, Type is 3, indicating that it is an RERR message. N is a no delete flag which, if set, informs the source that a local repair has been done and that there is no need to use one of the alternate routes. Destination count gives the number of unreachable destination addresses.

6.2.5 Local Connectivity

Each node should maintain its local connectivity with respect to other nodes in its vicinity. This is done proactively in BEAN as long as there is a route information present in a node's routing table. Periodic *hello* messages are broadcast by each node to its immediate neighbors. On receiving a *hello* message, each node updates the TTL value in its routing table that corresponds to this neighbor. The node also maintains a next hop linked list which contains all the next hop nodes' addresses. If there is no *hello* message from a neighbor for *allowed_hello_loss* times, then that neighbor is assumed to be absent. Then the node removes any routing table entry it contains with this neighbor as the next hop. When there is no active route entry present in a node's routing table, it ceases to send the *hello* message, thereby reducing redundant control messages.

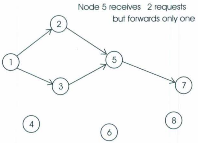


Figure 6.6: Loop Avoidance

6.3 Routing Properties of BEAN

6.3.1 Loop Avoidance

In BEAN, formation of loops are avoided the same manner in which they are avoided in AODV routing protocol. That is, when more than one RREQ reaches any particular node, the node will respond to only one RREQ. This concept is illustrated in Figure 6.6, where node 5 receives two RREQs: one through node 2 and other through node 3. However, the RREQ through node 2 is received first and therefore, the other RREQ is ignored. Node 5 will rebroadcast the RREQ from node 1 only once. The way the node decides which RREQ to respond is based on which RREQ arrives first. The node that arrives first will be the node that traveled through a link that has the highest capacity and the node that has followed the route of least delay and therefore, will also be the RREQ that followed the best route. Moreover, since BEAN supports storing multiple routes, the fact that only one RREQ can be forwarded by each node enforces the property that the multiple routes obtained are all independent of each other.

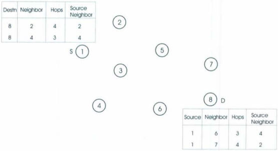
6.3.2 Fast Convergence with Changes in Link

When the link between a node and its neighbor fails, the node will send an RREQ message to find a new route through a different link to reach its neighbor if the node is forwarding an RREP message to the next hop. If the link fails during data transmission, the source is informed through RERR message. The source then uses one of the alternate routes available. If the link capacity reduces, this will affect an existing route that provides quality-of-service. In this case, the node sends a QoS_LOST message to the source informing it about exactly what has failed. For example, if the BW constraint has failed due to a link change, then the BW flag is set and the value of the current minimum BW is also appended along with the QoS_LOST message so that the source can make a decision between choosing an alternate route and using the existing route with reduced minimum bandwidth.

6.3.3 Localized Reactions to Changes in Topology

Rate of topological change in ad hoc networks is very high. When topological changes are extremely rapid, little can be done to ensure that routing algorithms converge fast enough to track topological changes. The reasons for which a node cannot reach its neighboring node include:

- The node may wander too far out of range
- Its battery may be depleted



Destn	Neighbor	Hops	Source Neighbor
8	2	4	2
8	4	3	4

Source	Neighbor	Hops	Source Neighbor
1	6	3	4
1	7	4	2

Figure 6.7: Multiple Routes Information Stored in Source and Destination

- It may suffer a software or hardware failure

When a node cannot reach the next hop during transmission, then the node sends an RERR message back to the source to indicate the source that the route has failed. The source may decide to choose one of its alternate routes. The node also sends a local RREQ message in order to fix the failure. This local RREQ message will have the next hop node address as the destination address. The destination (next hop node in the route) will then reply with an RREP message. Once this local route to next hop has been established, the complete route would have been reconstructed including the change in topology. This way, the source can again make use of the original route. This technique has been adapted from Associativity Based Routing (ABR) [26].

6.3.4 Multiple Routes Information

Multiple replies are obtained when the source broadcasts RREQ. The number of neighboring nodes the destination is attached to will limit the number of RREQ messages that reach the destination. The destination then replies to each of these RREQs through RREP message. Each of the RREP messages will reach the source. This means the number of neighbors the destination is attached to will also limit the number of RREPs that the source will receive. This means the same number also limits the number of alternate routes the source will have. The source just has to decide on the best route among these alternate routes. The source and each of the nodes in the route from source to destination will store these alternate routes in their routing table. The source will also have an additional field in its routing table that indicates the priority of each of these routes with '1' indicating the highest priority. Thus the source has multiple routes to the destination as shown in Figure 6.7 and the complexity involved in choosing the best route will not be too high due to the limitation on the number of alternate routes available. This technique is adapted from Dynamic Source Routing (DSR) [24]. However, in DSR, the entire route is placed in the RREP message and in the data packets. BEAN does not require the entire route to be stored in the RREP message. Thus the RREP messages in BEAN have lesser control overhead compared to DSR in spite of having multiple routes to the destination.

6.3.5 Unidirectional Link Support

When compared with AODV (which supports only bidirectional links) with simple changes to existing BEAN implementation, it can support unidirectional links. The RREQs reaching the destination will account for the forward route from source to destination. However, the RREP from the destination has to reach the source in order for the source to make a decision on the best route. If, however, when the RREP message travels back to the source, a particular node is not able to reach the next hop given in its routing table owing to the fact that the link is unidirectional, the node sends a local RREQ message with the next hop address as the destination address. The next hop node, once it receives the local RREQ message replies with an RREP message. The node that saw the unidirectional link will now send the RREP message to the next hop address through this new local route. This way, even if the link is unidirectional, the route is still available for communication.

6.3.6 Quality of Service Support

As explained before in the RREQ and RREP message formats, just like AODV, BEAN also provides quality of service by selecting the routes based on minimum BW requirement and the maximum tolerable delay. Unlike AODV where any node that has a route to the destination can respond to RREQ, the uniqueness of BEAN lies in the fact that only the destination can respond to RREQ, since, only then we will have a fresh enough value for the delay experienced and the BW available through any route. This is because the traffic at this instant is responsible for the delay caused and the BW available and, a previously stored route will have outdated delay and

BW values.

6.3.7 Independency of Alternate Routes

Alternate routes in BEAN are independent of each other due to the convergence nature of the routing protocol. That is, when the RREQs are forwarded, each node forwards only one RREQ. This means that each RREQ that reaches the destination would have followed a different route. Similarly, when the RREPs are sent back to the source there is no collision of the RREPs if all the links are bidirectional. If some links are unidirectional, then only those RREPs will be forwarded through different routes. The route from source to destination will still remain independent of other alternate routes. Thus BEAN ensures that a failure in one link does not affect the alternate routes.

6.4 Probability Distribution of Multiple Disjoint Paths in BEAN

Figure 6.8 shows the established route of a multipath routing protocol in ad hoc networks. In the figure, nodes are distributed randomly over a certain area. Node 1 is the source node and node 18 is the destination node. The best path between the source node and destination node includes the path via nodes 4, 7, 10 and 15, indicated by the dashed lines in this figure, contributing to a total of 5 hops. The alternate routes each have a 6-hop route to the destination node from the source node. According to the BEAN routing protocol, the packets sent by the source node follow

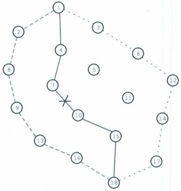


Figure 6.8: Multipath Routing

the best path until a link in that path fails, as shown by the broken link between nodes 7 and 10 in the figure. When the best path fails, one of the remaining two routes is used to send packets to the destination node (node 18). All the three paths are disjoint, that is, there is no intermediate node that is common to two or more paths. Thus the alternate paths are unaffected by a failure in the best path.

Previously, Bettstetter, in [96], found the probability distribution of the minimum number of hops between two nodes. He also found the connection probability for two hops and defined analytical bounds for connections greater than two hops. Similarly, Miller also found the *two-hop* connection probability assuming Gaussian distribution of nodes in [97]. Chandler, in [93], calculated the expected number of hops required to connect two nodes given the distance between them. Chandler used the Poisson distribution in calculating the hop probability. The probability distribution of disjoint multiple paths for a set of nodes distributed uniformly in an ad hoc network is derived next.

6.4.1 Link Distance Distribution

Let n nodes in an ad hoc network be distributed uniformly in a square area of side a with area,

$$A_0 = a \times a. \tag{6.1}$$

An independent and identical uniform distribution of nodes is assumed here as it is consistent with the classroom or conference hall scenario for which our routing protocol was proposed [98]. Consider two nodes i and j in this network, shown in Figure 6.9 as S and D respectively. The Euclidean distance between these two nodes can be given as

$$d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \tag{6.2}$$

where (x_i, y_i) is the location of node i (S in the figure), and (x_j, y_j) is the location of node j (D in the figure). The probability density function (pdf) for a uniform distribution of nodes as derived by Miller in [99] $f_d(\xi)$, for the distance, d, is given by

$$f_d(\xi) = \begin{cases} 0, & \xi < 0 \\ 2\xi(\xi^2 - 4\xi + \pi), & 0 \leq \xi < 1 \\ 8\xi\sqrt{\xi^2 - 1} & \\ -2\xi(\xi^2 + 2) & \\ +4\xi(\sin^{-1}(1/\xi) & \\ -\cos^{-1}(1/\xi)), & 1 \leq \xi < \sqrt{2} \\ 0, & \text{otherwise} \end{cases} \tag{6.3}$$

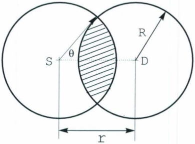


Figure 6.9: Intersection Area between Two Nodes

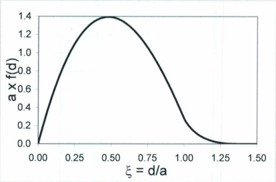


Figure 6.10: Link Distance pdf for a Rectangular Area [99]

where, $\xi = d/a$. This link distance pdf is depicted in Figure 6.10.

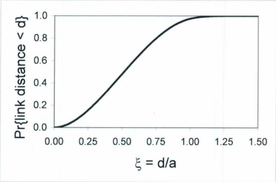


Figure 6.11: Link Distance cdf for a Rectangular Area [99]

Then cumulative distribution function (cdf), $F_d(\xi)$, for the distance is given by

$$F_d(\xi) = \begin{cases} 0, & \xi < 0 \\ \xi^2(\frac{1}{2}\xi^2 - \frac{8}{3}\xi + \pi), & 0 \leq \xi < 1 \\ \frac{4}{3}\sqrt{\xi^2 - 1}(2\xi^2 + 1) & \\ \quad -(\frac{1}{2}\xi^4 - 2\xi^2 - \frac{1}{3}) & \\ \quad +2\xi^2[\sin^{-1}(1/\xi) & \\ \quad - \cos^{-1}(1/\xi)], & 1 \leq \xi < \sqrt{2} \\ 1, & \sqrt{2} \leq \xi. \end{cases} \tag{6.4}$$

The link distance cdf is shown in Figure 6.11.

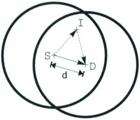


Figure 6.12: Two Nodes in the Same Transmission Range

6.4.2 Distribution of Multiple Disjoint Two-hop Paths

Two nodes, S and D, may establish a direct link (one hop), as shown in Figure 6.12, if the distance between them (d) is less than R, where R is the transmission radius of a node. Therefore, the probability of establishing a connection between any two nodes within *one* hop, P_1, in a network with $n \geq 2$ is [93],

$$P_1(d) = \begin{cases} 1, & d < R \\ 0, & d \geq R. \end{cases} \tag{6.5}$$

Consider the case in which the two nodes have no direct link but can communicate over at least one path in two hops, as shown in Figure 6.13. In this case, two conditions must be satisfied:

1. the distance, d, should be in the range between R and $2 \times R$;
2. at least one other node must exist within the intersection area A established by the two nodes.

Figure 6.13 shows one best path, indicated by I_1 and two alternate paths, indicated

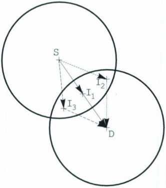


Figure 6.13: Two Todes at Two-hop Distance

by I_2 and I_3. From Figure 6.9, area A, of the shaded region is given by (6.6).

$$A = 2R^2(\theta - \sin\theta\cos\theta) \tag{6.6}$$

where $\theta = \cos^{-1}(d/2R)$. Since the nodes are uniformly distributed, the probability that a node can exist in the area A is A/A_0. The area A is assumed to be present within the total area A_0.

The probability that at least one node is located in the area A is given by (6.7) for a network with $n \geq 3$.

$$P_2(d) = 1 - \left(1 - \frac{A}{A_0}\right)^{n-2}. \tag{6.7}$$

Equation (6.7) is based on the Binomial distribution. Although Chandler's approach is based on the Poisson distribution, this paper uses the Binomial distribution for the following reasons:

1. the closeness to real world examples,

2. simpler to evaluate since it gives two mutually exclusive results (i.e. either a connection can be established or not), and,

3. precision in terms of the decision it makes.

6.4.2.1 Best Path

The connection probability of paths, ranging between R and $2R$, that may communicate in two hops is given by

$$\eta_2(d) = \begin{cases} \int_R^{2R} f_d(r) P_2(r) dr, & R < r \leq 2R \\ 0, & r > 2R. \end{cases} \tag{6.8}$$

Equation (6.8) gives the probability that a connection can be established between a source and destination node (shown in Figure 6.13), when the distance between the two nodes is between R and $2R$. In other words, this is the connection probability for path I_1 in Figure 6.13.

6.4.2.2 Alternate Path

Figure 6.13 also shows two alternate paths, named I_2 and I_3. In order to be able to have an alternate path for I_1, there has to be another node present in the intersection area, A. The probability that at least *two* nodes are located in the area A for a network with $n \geq 4$ is given by

$$Q_2(d) = 1 - \left(1 - \frac{A}{A_0}\right)^{n-2} + 1 - \left[(n-2)\left(1 - \frac{A}{A_0}\right)^{n-3}\left(\frac{A}{A_0}\right)\right]. \tag{6.9}$$

Equation (6.9) is the probability of having one alternate path. The probability of having more than one alternate path can be generalized as,

$$Q_2(d) = 1 - \left[\sum_{i=0}^{k}(n-2)C_i\left(1-\frac{A}{A_0}\right)^{n-2-i}\left(\frac{A}{A_0}\right)^{i}\right] \tag{6.10}$$

where, k is the number of the alternate path for which the probability is being calculated. Equation (6.9) can be compared to (6.7) in that they represent the probability that a node (or two nodes) is (are) present in the intersection area. Replacing $Q_2(d)$ for $P_2(d)$ in (6.8) we can obtain the connection probability of having at least one alternate path between two nodes separated by a distance ranging between R and $2R$, and, that may communicate in two hops.

$$\tau_2(d) = \begin{cases} \int_R^{2R} f_d^{'}(r)Q_2(r)dr, & 0 < r \leq 2R \\ 0, & r > 2R. \end{cases} \tag{6.11}$$

In (6.11), $f_d^{'}(r)$ is the pdf of links that can have alternate paths. This is not the same as $f_d(r)$ since the number of connections that can have alternate paths may be fewer than the total number of best paths that can be established. This is limited by the density of the network. Alternately, the distribution for $f_d^{'}(r)$ can be presented using a scalar variable as,

$$\int_R^{2R} f_d^{'}(r)dr = \frac{\int_R^{2R} f_d(r)dr}{\gamma} \tag{6.12}$$

where γ is the scalar variable that represents the ratio between the number of best paths that can be established to the number of alternate paths that can be established. This variable approaches unity as the density increases. In other words, if a path exists for all $R < r < 2R$, all the connections will have alternate paths and thus, $\int_R^{2R} f_d^{'}(r)dr$ will converge to $\int_R^{2R} f_d(r)dr$.

6.4.3 Distribution of Multiple Disjoint Paths with More Than Two Hops

The discussion in Section 6.4.2 is limited to two hops for both the best and alternate paths. Consider the case in which two nodes have no direct link and cannot communicate over at least one path with at most t hops. In this case, two conditions must be satisfied:

1. there is no direct connection between the source and destination node; i.e. the link distance is greater than R;

2. any node or a set of nodes cannot establish a connection between the two nodes in less than or equal to $t - 1$ hops.

6.4.3.1 Best Path

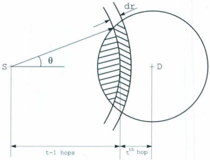


Figure 6.14: Intersection Area between Two Nodes Separated by t Hops

Figure 6.14 shows the case where two nodes are separated by a distance of t hops. Let $w(r)$ be the probability of being able to establish communication within an intersection area A. If this area is increased by dA by increasing r to $r + dr$ as shown in Figure 6.14, then the probability of being able to establish a communication within the new area, dA, can be written as,

$$[P_{t-1}(r) - P_{t-2}(r)]2r\phi/A_0 \tag{6.13}$$

where,

$$\phi = \cos^{-1}\left(\frac{d^2 + r^2 - R^2}{2dr}\right). \tag{6.14}$$

The term $P_{t-1}(r) - P_{t-2}(r)$ in (6.13) denotes the probability of reaching a destination node that is at a distance r in exactly $t - 1$ hops. This approach is similar to that of Chandler [93] and is based on the assumption that connecting nodes are exactly $t - 1$ hops away from the source node and one hop away from the destination node. Equation (6.13) is based on the assumption that a connection has been established up to a distance of $t - 1$ hops and thus has to be solved iteratively. The probability of not establishing a communication using any node in the transmission area within limits $d - R$ and $d + R$ is given by

$$[1 - w(r)]^{n-t} \tag{6.15}$$

where,

$$w(r) = \int_{d-R}^{d+R} \frac{[P_{t-1}(r) - P_{t-2}(r)]A'}{A_0} dr \tag{6.16}$$

and $A' = 2r\phi$. The probability of not being able to establish a connection with t hops or less is given by

$$1 - P_t(d) = [1 - P_{t-1}(d)][1 - w(r)]^{n-t}. \tag{6.17}$$

Therefore, the probability of having a path with t hops is given by

$$P_t(d) = 1 - [1 - P_{t-1}(d)][1 - w(r)]^{n-t}. \tag{6.18}$$

6.4.3.2 Alternate Path

Following the procedure in two-hop case, the probability of having an *alternate* path with t hops is given by

$$\begin{aligned} Q_t(d) &= 1 - [1 - P_{t-1}(d)] \times \\ &\quad \left\{[1 - w(r)]^{n-t} + n[1 - w(r)]^{n-t-1}w(r)\right\}. \end{aligned} \tag{6.19}$$

Therefore, the probability of establishing a connection to a destination node that is at a distance of t hops is given by

$$\eta_t(d) = \begin{cases} \int_{2R}^{tR} f_d(r)P_t(r)dr, & 2R < r \leq t \times R \\ 0, & r > t \times R. \end{cases} \tag{6.20}$$

Likewise, the probability of establishing a connection through at least one alternate path with a destination node that is at a distance of t hops is given by

$$\tau_t(d) = \begin{cases} \int_{2R}^{tR} f_d^{'}(r)Q_t(r)dr, & 2R < r \leq t \times R \\ 0, & r > t \times R. \end{cases} \tag{6.21}$$

In (6.21) $f_d^{'}(r)$ is defined by (6.12) for limits between $2R$ and tR. Equation (6.19) gives the probability of having *one* alternate path in t hops. The probability of having more than one alternate path, say k paths, can be developed from (6.19) as

$$\begin{aligned} Q_t(d) &= 1 - [1 - P_{t-1}(d)] \times \\ &\quad \left\{\sum_{i=0}^{k}(n-t)C_i[1 - w(r)]^{n-t-i}[w(r)]^i\right\}. \end{aligned} \tag{6.22}$$

6.4.4 Comparison with Simulation Results

Simulations are carried out to verify the analytical expressions derived in the previous section. The simulations are implemented using network simulator (ns-2) [4]. In a network of 50 nodes uniformly distributed in an area of 1000 m × 1000 m, all possible connections are established for a transmission range of 250 m and the probability density function (pdf) and cumulative distribution function (cdf) of best path (that is, the path with the least number of hops between two nodes) are plotted. Figure 6.15 shows the probability density function (pdf) of the distance between two nodes in terms of number of hops. This figure shows the analytical results obtained from (6.20). The analytical results are compared against results obtained from simulations conducted for several scenarios generated using the network simulator. Higher pdf for 2-3 hops is due to larger pdf links between 250-500 m, which agrees with analytical results obtained by Miller [97].

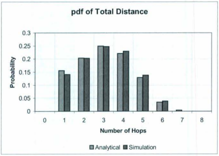


Figure 6.15: pdf of Total Distance

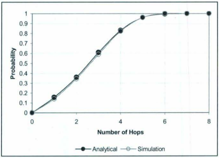


Figure 6.16: cdf of Total Distance

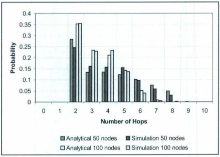


Figure 6.17: pdf of Alternate Path

The pdf and cdf of alternate paths for a multihop, multipath ad hoc network is plotted in Figures 6.17 and 6.18. For the 50 node case, the cdf for both analytical

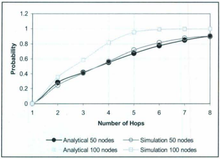


Figure 6.18: cdf of Alternate Path

and simulation does not converge to 1.0 when compared with the case of best path in Figure 6.18. This is due to the non-availability of alternate paths for a scenario with 50 nodes. In other words, the node density is not sufficient to establish alternate paths for all possible link distances. This is evident when compared with the case of 100 nodes, where the cdf converges to 1.0.

Figures 6.19 and 6.20 show the pdf and cdf of the connection probabilities of both the best and alternate paths for 50 and 100 nodes. Comparison of the pdf and cdf for alternate paths for 50 and 100 nodes indicate that at least one alternate path can be established when the number of nodes is increased from 50 to 100, i.e, under higher node density.

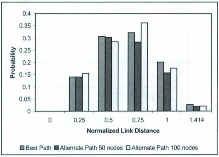


Figure 6.19: pdf of Best and Alternate Paths

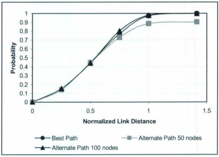


Figure 6.20: cdf of Best and Alternate Paths

6.5 Conclusion

This chapter illustrates the route deployment, maintenance and response to failure in BEAN routing protocol. Owing to the establishment of multiple paths, the probability distribution of the connection probabilities for both the best and at least one alternate path are arrived at. The derivation of connection probability of the first alternate path is extended to multiple alternate paths. The results are compared with simulations carried out and are found to match well.

The availability of alternate path is critical for the multipath routing protocols. Simulations were carried out for networks of 50 and 100 nodes. Increasing the number of nodes causes an increase in density and eventually all the connections established have at least one alternate path. Alternately, when the transmission range is increased, it is possible for all connections to have at least one alternate path.

The next chapter illustrates the performance of the BEAN routing protocol by deriving an analytical expression for throughput, additional data delivery and by comparing simulation results with AODV routing protocol.

Chapter 7

Performance Analysis of Unicast BEAN Routing

7.1 Introduction

The performance analysis of routing in BEAN, the unicast multipath routing protocol presented in Chapter 6, is reported in this chapter. In BEAN, several alternate routes are established during initial route discovery. Once the routes are established, the source sends data packets through the best route. All the routes are kept active until a need for one of the alternate routes arises when a route fails either due to link or node failure, or, due to mobility. When the route fails, the error message propagates to the source node which then chooses one of the alternate routes and sends packets through the next best route immediately. Rather than expending time on re-establishing the route, BEAN switches to an alternate route thereby supporting data packet transfer during that time, which increases the total number of packets sent. Depending on the frequency of route failure, the BEAN routing protocol can be advantageous in terms of throughput. The performance analysis of BEAN, in terms of packet delivery ratio (PDR), throughput, and latency, is carried out.

The cost of maintaining multiple routes is high in multipath routing due to lack of abundant resources in ad hoc scenarios. However, applications for which the BEAN protocol was proposed [100] include minor unicast communications lasting for short durations in the presence of numerous or prolonged multicast communications. Such applications include an airport scenario where the individuals waiting for their respective flights interact with each other, a ballpark where the audience wish to discuss the game while the game is in progress, a modern classroom where the students are not bound to the classroom space but can still be connected to the classroom network, etc. In such cases, the demand for swift response to route failure for the short duration of the communication surmounts the high maintenance cost.

The throughput performances of BEAN and AODV obtained analytically in Section 7.3 and are verified against those from simulations in Section 7.4 for a simple ad hoc network. The additional data packet transfer supported by BEAN upon route failure is analytically shown in Section 7.5. The performance analysis of realistic network for various parameters such as traffic pattern, transmission effects, number of connections are conducted in simulations using ns-2 simulator in Section 7.6. The protocol against which BEAN is compared, AODV, is a popular single path routing protocol which was readily available in the network simulator (ns-2) used for simulations.

7.2 Definitions of Performance Characteristics

Some of the characteristics of BEAN that are used to compare it against AODV in the simulations conducted in this chapter are discussed below:

7.2.1 Packet Delivery Ratio

Packet delivery ratio (PDR) is defined as the ratio between the total number of data packets successfully received by the destination node to the total number of data packets sent by the source node. A PDR of one indicates no loss of packets on the route from the source to destination node. There are several reasons for a packet to be lost along the path. A packet may be dropped in the queue, due to queue overflow, while waiting for access to the wireless channel. A packet may also be lost or collided with another packet during transmission through the wireless channel by the source or one of the intermediate nodes on the path to the destination node. Thus, PDR is likely to be lower with heavy traffic loads and higher for lighter loads.

7.2.2 Throughput

Throughput for a given connection between a source and destination is defined as the number of bits of data packet sent per second over the wireless channel. The throughput measured from any given link can be defined as the ratio of number of bits of packets that it sends to the total time. The unit for throughput is *bps*. When the throughput is high, the wireless channel is efficiently utilized and vice versa.

7.2.3 Latency

Latency of a data packet is defined as the end-to-end delay in sending the packet from a source node to destination node and is measured in seconds or milliseconds. Latency includes the delay in waiting for the wireless channel to be available, the transmission time of each packet from each node and the propagation time for the packet to traverse the route. Latency is expressed in seconds or milliseconds. The latency plotted in the results discussed in Section 7.6 is the average of the latency of all the data packets.

7.3 Analytical Throughput Model

In this section, throughput performance is verified analytically against that of simulation for a simple ad hoc network. Assume a random unsaturated network with uniformly distributed nodes, which resembles a ballpark, classroom or conference hall AHN scenario etc. Assume a single connection between a source node and destination node. The packet arrivals at the source are based on CBR traffic in which packets arrive at a constant rate. The medium access control (MAC) scheme used is IEEE 802.11 DCF, in the basic access mode.

As the packets from the source are being sent along the route, they encounter collisions due to transmission by neighbor nodes or hidden nodes. In this section, the packet capture effect is ignored to simplify the analysis of throughput [7]. That is, all packets in a collision are dropped irrespective of the power with which they are received. From [7] and ignoring the effects of packet capture and channel errors, the transmission probability (τ) of a node in an unsaturated network is given by,

$$\tau = \frac{2(1-2P_C)q}{d_1+d_2} \tag{7.1}$$

where, P_C is the collision probability as seen by a node excluding the effects of packet capture and channel errors and q is the probability that a node has packets available in its queue (for the saturated case, $q = 1$). The parameters d_1 and d_2 in the denominator are given by,

$$d_1 = q[(W+1)(1-2P_C) + WP_C(1-(2P_C)^m)] \tag{7.2}$$

$$d_2 = 2(1-q)(1-P_C)(1-2P_C) \tag{7.3}$$

Here, W is the backoff counter value of the contention window of a node, and m is the backoff stage. The maximum contention window is given by $CW_{max} = 2^m W$.

For a random network with a single connection, the collision probability of a node is defined as the probability that at least one of the remaining $N_{unit}-1$ nodes belonging to the connection (given N_{unit} nodes within a transmission range that participate in a connection) transmits at the same time as this node. Thus, collision probability can be written as [5],

$$P_C = 1 - (1-\tau)^{N_{unit}-1}. \tag{7.4}$$

Now, we have (7.1) and (7.4), with two variables, P_C and τ. Solving these two equations, we can obtain the expression for collision probability. Based on the collision probability derived in (7.4), the throughput (S_A) is calculated as,

$$S_A = (1-P_C)\ .\ t_{DATA}\ .\ d_{rate}\ .\ N_{data}/t_{total}. \tag{7.5}$$

In the above equation, N_{data} is the total number of data packets sent, t_{total} is the total time under consideration, d_{rate} is the data rate, and, t_{DATA} is the time taken to send a single packet of size 512 bytes.

7.4 Comparison of Throughput from Simulation

In this section, the analytical expression obtained in (7.5) is used to compare the performance of BEAN and AODV with the throughput obtained from simulation. Consider a scenario of 100 nodes distributed uniformly in a network of size 1000 m × 1000 m. Consider a route formed between a source and a destination node in this network. According to the BEAN routing algorithm, two routes are successfully established. Initially the shortest route is used to send packets between the source and destination. Upon route failure, the alternate route is chosen almost immediately. According to the AODV routing algorithm, only one optimal route is established initially. Upon route failure, a new optimal route is re-established. The time and cost of initial route establishment for both AODV and BEAN are not compared since it is a one time expense. The parameters used in calculating throughput are tabulated in Table 7.1.

The expected throughput (S_A) at steady state *before* failure is calculated theoretically based on (7.5) and the results for both AODV and BEAN protocols are tabulated in Table 7.2. The minor difference in throughput of BEAN and AODV is attributed to the number of data packets sent during the time frame under consideration.

The simulation is carried out for the same network and connection and the throughput values of the route *before* failure at steady state are measured for both BEAN and AODV. The throughput (S_S) is calculated as the rate of packets (in terms of bits) successfully sent during the time frame under consideration. The network is

Table 7.1: Analytical Model Parameters

Variables	Values	Variables	Values
$DIFS$	$128\mu s$	t_{prop}	$2ns$
$t_{PHY} + t_{MAC}$	$576\mu s$	d_{rate}	$1Mbps$
t_{DATA}	$4096\mu s$	W	32
$SIFS$	$28\mu s$	m	3
t_{ACK}	$38\mu s$		

Table 7.2: Analytical Results for BEAN and AODV Before Failure

	Ana Thrpt in Mbps, S_A	Sim Thrpt in Mbps, S_S
BEAN	0.2393	0.2415
AODV	0.2380	0.2392

said to have reached steady state when there are no more control packets (route request, route reply, route error, etc.) The throughput obtained through simulation, for an arbitrary intermediate link, for both AODV and BEAN routing protocols are tabulated in Table 7.2.

From the table, it can be noted that the analytical and simulation values of throughput (for both AODV and BEAN) differ by no greater than 1% thereby verifying the analytical model.

7.5 Packet Delivery for BEAN Upon Route Failure

In this section, the delivery of additional packets by BEAN during AODV's recovery from route failure is demonstrated. Unlike BEAN, in the case of AODV, when the route fails, a new route has to be re-established. The mechanism of re-establishing a new route in AODV is illustrated in Figure 7.1. When the route fails, AODV exchanges additional control information to find a new optimal path. However, BEAN routing protocol relies on quick recovery from failure by using a less optimal alternate path as shown in this figure.

The time line involved in re-establishing the new route for AODV is illustrated in Figure 7.2. The time taken to find a new route for AODV is evaluated theoretically as shown below. The parameters used to calculate the time taken to establish a new route are tabulated in Table 7.3. The transmission time of a packet is calculated as,

$$txt = p/d_{rate} \tag{7.6}$$

where p is the size of the packet in bits.

Time taken to wait for average backoff (W_{avg}) counts is calculated as,

$$t_{W_{avg}} = W_{avg} \cdot t_{slot} \tag{7.7}$$

where t_{slot} is the duration of an empty slot time. Time taken for RREQ to travel one hop is given by,

$$txt_{RREQ1} = txt_{RREQ} + DIFS + t_{W_{avg}} + t_{prop}. \tag{7.8}$$

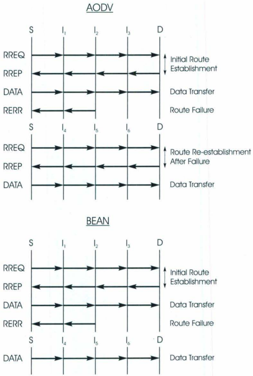


Figure 7.1: Route Failure and Recovery in AODV and BEAN

Similarly, time taken for RREP to travel one hop is given by,

$$txt_{RREP1} = txt_{RREP} + DIFS + t_{W_{avg}} + t_{prop}. \tag{7.9}$$

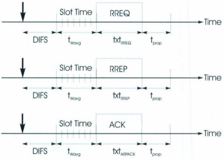


Figure 7.2: Route Establishment Mechanism for AODV

Table 7.3: Parameters to Calculate Route Establishment Time for AODV

Variables	Values	Variables	Values
p_{RREQ}	$800\ bits$	d_{RTRMAC}	$25\mu s$
p_{RREP}	$768\ bits$	$DIFS$	$128\ \mu s$
p_{ARPRQ}	$800\ bits$	W_{avg}	16
p_{ARQRP}	$800\ bits$	t_{prop}	$2\ ns$
p_{ARPACK}	$304\ bits$	$SIFS$	$28\ \mu s$
d_{rate}	$1\ Mbps$	t_{slot}	$50\ \mu s$

Time taken for ARP ACK to travel one hop is given by,

$$txt_{ARPACK1} = txt_{ARPACK} + DIFS + t_{W_{avg}} + t_{prop}. \tag{7.10}$$

In (7.8), (7.9) and (7.10), txt_{RREQ}, txt_{RREP} and txt_{ARPACK} are obtained using (7.6) by substituting p for their respective packet sizes.

Time taken for ARP Request, txt_{ARPRQ1}, and Reply, txt_{ARPRP1} to travel one hop is the same as that for RREQ. Thus,

$$txt_{ARPRQ1} = txt_{ARPRP1} = txt_{RREQ1}. \tag{7.11}$$

Therefore, total time taken to find a new route of n hops by AODV is given by,

$$\begin{aligned} t_{AODV} &= n\left[txt_{RREQ1} + txt_{RREP1}\right] \\ &\quad + n\left[2\left(txt_{ARPRP1} + txt_{ARPACK1}\right)\right] \\ &\quad + n\left[2\left(d_{RTRMAC}\right)\right] \end{aligned} \tag{7.12}$$

where d_{RTRMAC} is the router to MAC delay. The results for all the terms in (7.12) are tabulated in Table 7.4. For a connection with 4 hops, using (7.12), t_{AODV} was calculated as 0.3465 seconds. t_{AODV} was also measured in simulation as 0.3427 seconds thereby verifying the expression for t_{AODV} derived in (7.12).

In the case of BEAN, the time taken to switch to the alternate route is measured. In comparison with the above calculation, the time taken to switch to one of the alternate routes in simulation in BEAN is measured as 0.009036 seconds, which is negligible.

Using (7.5) for S_A, additional bits of packets that BEAN can send during the time t_{AODV} is

$$n_{A'} = S_A \cdot t_{AODV}. \tag{7.13}$$

Substituting values for t_{AODV} and S_A from (7.12) and (7.5), $n_{A'}$ is arrived as 10.36 kB , assuming the throughput obtained before failure is maintained upon failure. The additional number of data packets that BEAN can send during AODV's route

Table 7.4: Theoretical Results in the Calculation of Route Acquisition Time and Data Packet Transmission Time

Variables	Values in μs	Variables	Values in μs
txt_{RREQ}	800	txt_{RREQ1}	1728.002
txt_{RREP}	768	txt_{RREP1}	1696.002
txt_{ARPRQ}	800	$txt_{ARPACK1}$	1232.002
txt_{ARPRP}	800	txt_{ARPRQ1}	1728.002
txt_{ARPACK}	304	txt_{ARPRP1}	1728.002
txt_{DATA}	4096	t_{AODV}	34653.048
txt_{ACK}	304	t_{DATA1}	5384.004
$t_{W_{avg}}$	800		

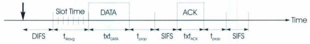


Figure 7.3: Data Transfer Mechanism for BEAN

recovery is estimated next. The time line for BEAN to send a data packet and receive its corresponding acknowledgment is illustrated in Figure 7.3.

Time taken for BEAN to send a data packet to a node's neighbor and receive an acknowledgment is calculated as

$$t_{DATA1} = DIFS + t_{W_{avg}} + txt_{DATA} + txt_{ACK} + 2(t_{prop}) + 2(SIFS). \qquad (7.14)$$

In the above equation, txt_{DATA} is the time taken for the data packet to travel over one hop, txt_{ACK} is the time taken for an acknowledgment packet to travel over one hop and t_{prop} is the average propagation delay. The result for this expression is also tabulated in Table 7.4. Comparing t_{AODV} (for AODV) and t_{DATA1} (for BEAN), during the additional time the AODV routing protocol spends in finding a new route, BEAN routing protocol is able to send at least 7 packets at a data rate of 1 Mbps. Depending on the number of hops present in the connection and the number of times the route for a connection might fail (which depends on the overall traffic in the network), BEAN can send additional packets during the time AODV spends in finding a new route, thereby supporting higher throughput than AODV.

7.6 Simulation Results

The analytical derivation of throughput discussed in the Section 7.3 was tested only for a simple case. More realistic cases, such as introducing different traffic patterns, packet capture effects and having more connections in the network, make the task of analytically evaluating the protocol performance cumbersome. Therefore, the realistic cases are tested in the simulator. The simulation parameters are tabulated in Table 7.5.

Simulations are carried out using the network simulator (ns-2). For the same $1000\ m \times 1000\ m$ network, the simulation is now run for $500\ s$ with 50 nodes. Data rate of 11 $Mbps$ is chosen based on the IEEE 802.11b standard. The choice of the particular variation of IEEE 802.11 is purely arbitrary and the simulator is not affected by various data rates.

Table 7.5: Simulation Parameters for Stationary case

Variables	Values
Number of nodes	50, 100
Simulation Time	500 s
Packet size	512 bytes
Data rate	11 Mbps
Capture threshold	10
Number of connections	10, 20, 30, 40, 50
Number of scenarios	3
Packet interarrival time	0.1, 0.01, 0.001, 0.0001 s
Traffic type	CBR, TCP

7.6.1 Stationary Nodes

The applications for which BEAN is proposed consists mostly of stationary nodes. Various PDR, latency and throughput values are plotted for both BEAN and AODV for the case when all nodes are stationary.

7.6.1.1 Packet Delivery Ratio for CBR Traffic

The results for constant bit rate (CBR) traffic with arrival rates of 0.1 s, 0.01 s, 0.001 s and 0.0001 s are shown in Figure 7.4.

Figure 7.4 corresponds to a network of 50 nodes and 10 to 50 sources for various interarrival times (IATs). For IAT of 0.1 s with 10 sources or connections in the

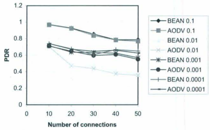


Figure 7.4: PDR for CBR Traffic for various IATs

network, the PDR of BEAN is the same or higher than that of AODV. As the number of connections is increased up to 50, the corresponding PDR drops for both BEAN and AODV, which is due to the amount of traffic present at an individual node.

For an inter-arrival time of 0.01 s similar results are obtained. However, the overall PDR has dropped considerably for both BEAN and AODV than for the case of 0.1 s IAT due to the random selection of source and destination pairs. The effect of reduced PDR is also attributed to some connections being longer than others. Additionally, certain nodes act as the source and destination of more than one connection, which results in overload on those nodes and causes a reduction in the overall PDR. Since the PDR values of both AODV and BEAN are consistent, the drop in PDR is acceptable.

For an IAT of 0.001 s and 0.0001 s, the PDR of AODV is marginally higher than that of BEAN for larger number of connections. This increase is due to the longer alternate route that is formed by BEAN compared to AODV's new route and the failure of the best route during the early stages of the simulation. The rest of the simulation continued with BEAN using its long alternate route and AODV using its new shortest route.

Upon failure, BEAN utilizes the alternate route readily available while AODV re-establishes a new route. The availability of alternate routes in BEAN makes it fault tolerant for multiple failures.

7.6.1.2 Packet Delivery Ratio for TCP Traffic

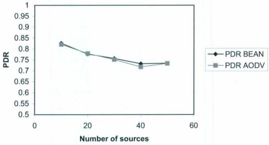


Figure 7.5: PDR for TCP Traffic

The simulation is then carried out for TCP sources to simulate real networks. The PDR plot is shown in Figure 7.5 for a network with 50 nodes. For TCP traffic BEAN routing protocol shows similar or better performance compared to AODV routing protocol. The overall PDR for BEAN and AODV is higher compared to CBR traffic even for the case with 50 connections in the network which is due to the adjustable congestion window size of TCP.

7.6.1.3 Latency for TCP Traffic

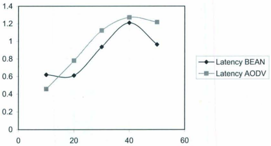


Figure 7.6: Latency for TCP Traffic

As per the TCP Tahoe protocol, the source adjusts the congestion window size based on slow-start procedure and exponential increase. This results in low latency as the traffic arrival adjusts itself to the load that the network can handle. As can be seen in Figure 7.6, the latency of BEAN is less than that of AODV for larger number of connections in spite of having to use less optimal routes during route failure.

7.6.1.4 Throughput for TCP Traffic

For TCP traffic source, the throughput is plotted against varying numbers of connections ranging between 10 and 50 as shown Figure 7.7. As discussed in Section 7.5, the throughput of BEAN is consistently higher than that of AODV, thereby showing that BEAN is able to handle more traffic through the network. The difference in throughput between AODV and BEAN is as high as 10% for the case of 40 connections.

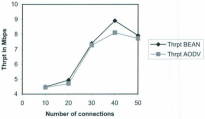


Figure 7.7: Throughput for TCP Traffic

The performance would further improve as the number of route failures increases and as more alternate paths become available for BEAN. The lower throughput for 50 connections as compared to that of 40 connections is as follows: each node is acting as the source, destination and also an intermediate node, and this results in more collisions and loss of packets.

7.6.2 Mobile Nodes

Here, we simulate a scenario of an airport waiting area, where only a part of the nodes are mobile at any point of time. In other words, partial mobility of the nodes is considered. While two-thirds of the nodes remain stationary throughout the simulation, the remaining one-third of the nodes move following the random waypoint mobility model with a minimum, average and maximum speed of 1 m/s. In this section, the simulation is run for networks with both 50 and 100 nodes for TCP sources to simulate real networks. The results are shown in Figures 7.8 and 7.9.

As can be seen in Figures 7.8 and 7.9, the PDR steadily decreases as the number

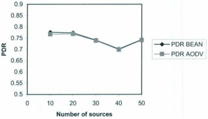


Figure 7.8: PDR with Partial Mobility for 50 nodes

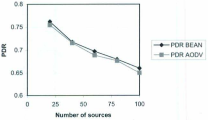


Figure 7.9: PDR with Partial Mobility for 100 nodes

of connections or sources in the network increases. It can also be seen that with 100 nodes in the network, both AODV and BEAN are more consistent than with 50 nodes. With the 50-node case, BEAN is not always able to establish alternate routes. However with 100 nodes, BEAN is able to find more than one route for almost all connections and hence the higher consistency in PDR compared to AODV.

7.7 Conclusions

The good performance of BEAN routing protocol is based on achieving multiple alternate routes between source and destination nodes in an ad hoc network. During a route failure, BEAN selects an existing alternate path for data packet transfer. On the other hand, AODV routing protocol re-establishes a new path during route failure.

In this chapter, for a simple network, the throughput performance of the two protocols, BEAN and AODV, is analytically defined and verified with simulation. The additional number of data packets that BEAN can send following a route failure during the time AODV can re-establish a new optimal route has also been analytically evaluated.

Simulations were conducted to evaluate the performance of the two protocols for realistic situations, such as different traffic patterns, presence of packet capture effects and a large number of connections in the network. Simulation results show that BEAN's performance is as good as AODV's in terms of PDR for CBR traffic. For TCP traffic, BEAN shows similar or improved performance in terms of throughput, latency and mobility. The throughput and PDR of BEAN would improve further in comparison with AODV when the number of route failures increases and with larger node densities.

Chapter 8

Conclusions and Future Work

8.1 Conclusions

The choice of routing protocols for various ad hoc network applications plays an important role in infrastructureless communications. The multicast requirements of the class of applications for ad hoc networks, such as communications within a ballpark, conference area or airport waiting area, drive the need for the deployment of newer routing protocols. BitTorrent protocol used with the Internet provides quick dissemination of files by sharing the upload and download capabilities among the peers. This concept has encouraged multicast routing in ad hoc networks. In this thesis, we have reported a multicast routing protocol (MBEAN) where hosts agree to share the responsibility of uploading and downloading the multicast message among themselves similar to the BitTorrent concept. Multicast communications in ad hoc networks also consist of minor unicast communications. This thesis has reported a unicast routing protocol (BEAN) for such purposes.

MBEAN is based on the concept that the source need not participate until all the multicast members receive the message. As long as the immediate neighbors of the source that are in the multicast group receive the message in full, it is possible to disseminate the entire multicast message among the members with very high probability.

In the MBEAN protocol design, the work presented in this thesis consists of the message formats for the multicast group formation and maintenance, and the working of the protocol in terms of making decisions on the choice of the route. The work has identified various properties of the protocol and presented the behavior of MBEAN in comparison with existing on-demand multicast protocols namely, MAODV and PUMA. Such a comparison has unraveled the simplicity of MBEAN. This behavior characterization should enable experimental implementers to anticipate the performance of the routing protocol.

In the analytical demonstration of MBEAN, effort has been taken to introduce a metric for assuring reliability to *all* the members in the multicast group. The metric has been termed as member reliability and is based on the mutual connectivity among members of the multicast group. Analytical proof of such an interconnectivity is derived along with expressions for packet delivery ratio and routing overhead. All the analytical results have been shown to be consistent with simulations for simple scenarios.

The above inferences have been illustrated by incorporating the MBEAN protocol in network simulator to assist researchers and designers to utilize the code for their comparisons. Scripts have been developed for measuring member reliability, PDR and overhead. MBEAN has shown exceptional qualities of enhanced member-to-member connectivity which not only results in improved packet delivery ratio, but also higher member reliability compared to MAODV, ODMRP and PUMA for varying group sizes and traffic loads. The overall overhead incurred by MBEAN has also been shown to be lower. The comprehensive verdict from all the simulation analyses is that, MBEAN displays robust performance, a distinguishable quality that is particularly appealing to the multicast applications discussed above.

Another contribution is the scenario development for emulating ad hoc networks environments like non-uniform distribution of nodes and various kinds of traffic sources, which enables the users of ad hoc networks to experiment the behavior of the protocols without the cost of actually deploying a comprehensive network. It was found that MBEAN is not suitable for small rectangular networks due to minimal connectivity among members. This can be overcome by the use of directional antennae as will be discussed in the next section.

Multicasting in ad hoc networks include unicast communications. Rather than deploying a new routing protocol for unicasting, the research has reported a unicast routing protocol (BEAN) that relies on forming alternate paths between a source and destination. The alternate paths serve as a substitute during a path failure. The working of the protocol is defined in detail projecting the advantages of having alternate paths. The probability distribution of establishing best and alternate paths have been derived and verified through simulations. It has been shown through analytical proofs and verification by simulation that the availability of alternate paths relies on sufficient node density.

Finally, the throughput of BEAN is derived and the explicit savings in packet delivery on route failure is compared to traditional AODV protocol. The behavior of BEAN is compared with that of AODV for various cases by incorporating the algorithm in network simulator. BEAN has shown comparable performance with AODV thereby proving that it can act with MBEAN under ad hoc environments without the need for implementing a separate unicast routing protocol.

8.2 Suggested Future Work

In order to improve the existing design and implementation through simulator, the following advancements are suggested.

The two protocols are designed and tested through simulations. Experiments are a more dependable way of verifying the performance of the protocols. A suggested next step would be to build an experimental set up for implementing the routing protocols.

The unicast protocol relies on the availability of alternate paths. Rather than using the alternate paths as a substitute, it is possible to send packets through all the paths simultaneously by the use of directional antennae. This will allow the exploitation of disjoint paths created by the protocol. The overall speed of packet delivery will be greatly improved.

The use of directional antennae are also useful for multicast environments where the scenario does not allow the achievement of connections among members. One such scenario is a rectangular scenario of a small sized network such as a gate area in an airport. The directional antenna will assist the establishment of multiple connections among the members in such cases.

With the existing implementation of the protocol when the density increases, more re-transmissions of the messages will lead to more collisions and overload of the network. Network coding is efficient in such cases since with network coding, it is possible to combine packets and send through each member and let the members share and decode the original message. Thus network coding will assist in achieving the multicast capacity of the protocol.

Allocation has been made for quality of service constraints in the current implementation of the protocol in the message formats for route request and reply. The simulation results do not however reflect these QoS constraints. Additional simulations and experiments need to be conducted to test the QoS provisioning of the routing protocols presented in this thesis.

Bibliography

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

[2] C. S. R. Murthy and B. S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols.* Prentice Hall Communications Engineering and Emerging Technologies Series, 2004.

[3] ISO/TC97/SC16/N890, "Information processing systems-open systems interconnection-basic reference model," in *International Standards Organization (ISO 7498)*, Feb. 1982.

[4] S. McCanne and S. Floyd. ns network simulator. [Online]. Available: http://www.isi.edu/nsnam/ns/

[5] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE Journal on Selected Areas in Communications*, vol. 18, pp. 535–547, 2000.

[6] K. Duffy, D. Malone, and D. J. Leith, "Modeling the 802.11 distributed coordination function in non-saturated conditions," *IEEE Communications Letters*, vol. 9, pp. 715–717, 2005.

[7] F. Daneshgaran, M. Laddomada, F. Mesiti, and M. Mondin, "Unsaturated throughput analysis of IEEE 802.11 in presence of non ideal transmission channel and capture effects," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1276–1286, 2008.

[8] P. C. Ng and S. C. Liew, "Throughput analysis of IEEE 802.11 multihop ad hoc networks," *IEEE/ACM Transactions on Networks*, vol. 15, pp. 309–322, 2007.

[9] V. Jacobson, "Congestion avoidance and control," in *Proceedings of ACM SIGCOMM*, August 1988, pp. 314–329.

[10] ——, "Modified tcp congestion avoidance algorithm," in *Email to the end2end-interest mailing list*, April 1990.

[11] M. Mathis, J. Mahdavi, S. Floyd, and A. Ramanow, "TCP selective acknowledgement options," in *RFC 2018*, Apr. 1996.

[12] A. Kumar, "Comparative analysis of versions of TCP in a local network with a lossy link," *IEEE/ACM Transactions on Networking*, vol. 6, no. 4, pp. 485–498, 1997.

[13] N. Parvez, A. Mahanti, and C. Williamson, "TCP NewReno: Slow-but-steady or impatient," in *In Proceedings of IEEE International Conference on Communications (ICC)*, 2006.

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

[15] S. Murthy and J. J. Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks," *ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks*, vol. 1, no. 2, pp. 183–197, 1996.

[16] C. C. Chiang, H. K. Wu, W. Lie, and M. Gerla, "Routing in clustered multihop mobile wireless networks with fading channel," in *Proceedings of IEEE SICON*, Apr. 1997, pp. 197–211.

[17] J. J. Garcia-Luna-Aceves and M. Spohn, "Source-tree routing in wireless networks," in *Proceedings of IEEE ICNP 1999*, Oct. 1999, pp. 273–282.

[18] T. H. Clausen, G. Hansen, L. Christensen, and G. Behrmann, "The optimized link state routing protocol, evaluation through experiments and simulation," in *Proceedings of IEEE Symposium on Wireless Personal Mobile Communications 2001*, Sept. 2001.

[19] A. Iwata, C. C. Chiang, G. Pei, M. Gerla, and T. W. Chen, "Scalable routing strategies for ad hoc wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1369–1379, 1999.

[20] T. W. Chen and M. Gerla, "Global state routing: A new routing scheme for ad hoc wireless networks," in *Proceedings of IEEE ICC 1998*, June 1998, pp. 171–175.

[21] Y.-Z. Lee, M. Gerla, J. Chen, J. Chen, B. Zhou, and A. Caruso, "Direction forward routing for highly mobile ad hoc networks," *Ad Hoc and Sensor Wireless Networks*, vol. 2, no. 2, 2006.

[22] T. Parker and K. Langendoen, "Guesswork: Robust routing in an uncertain world," in *2nd IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2005)*, Nov. 2005.

[23] A. Belghith and M. A. Abid, "Dynamically self adjustable proactive routing protocols for mobile ad hoc networks," in *34th IEEE Conference on Local Computer Networks*, 2009, pp. 506–513.

[24] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing.* Kluwer Academic Publishers, 1996, pp. 153–181.

[25] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing." Los Alamitos, CA, USA: IEEE Computer Society, 1999, pp. 90–100.

[26] C. K. Toh, "Associativity-based routing for ad hoc mobile networks," *Wireless Personal Communications*, vol. 4, no. 2, pp. 1–36, 1997.

[27] R. Dube, C. D. Rais, K. Y. Wang, and S. K. Tripathi, "Signal stability-based adaptive routing for ad hoc mobile networks," in *IEEE Personal Communications Magazine*, Feb. 1997, pp. 36–45.

[28] W. Su and M. Gerla, "IPv6 flow handoff in ad hoc wireless networks using mobility prediction," in *Proceedings of IEEE GLOBECOM 1999*, Dec. 1999, pp. 271–275.

[29] R. S. Sisodia, B. S. Manoj, and C. S. R. Murthy, "A preferred link-based routing protocol for ad hoc wireless networks," *Journal of Communications and Networks*, vol. 4, no. 1, pp. 14–21, 2002.

[30] P. Appavoo and K. Khedo, "SENCAST: A scalable protocol for unicasting and multicasting in a large ad hoc emergency network," *International Journal of Computer Science and Network Security*, vol. 8, no. 2, Feb. 2008.

[31] S. Khurana, N. Gupta, and N. Aneja, "Reliable ad-hoc on-demand distance vector routing protocol," in *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL 2006)*, 2006.

[32] S. K. D. an M. S. Obaidat and M. Gupta, "A reactive optimized link state routing protocol for mobile ad hoc networks," in *17th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, 2010, pp. 376–370.

[33] P. Sinha, R. Sivakumar, and V. Bharghavan, "CEDAR: A core extraction distributed ad hoc routing algorithms," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1454–1466, 1999.

[34] Z. J. Haas, "The routing algorithm for the reconfigurable wireless networks," in *Proceedings of ICUPC 1997*, vol. 2, Oct. 1997, pp. 562–566.

[35] M. Joa-Ng and I. T. Lu, "A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1415–1425, August 1999.

[36] A. Pandey, M. N. Ahmed, N. Kumar, and P. Gupta, "A hybrid routing scheme for mobile ad hoc networks with mobile backbones," in *IEEE International Conference on High Performance Computing, HIPC 2006*, Dec. 2006, pp. 411–423.

[37] R. Wei, M. Wu, and T. Yu, "LSMR:a label switching multipath routing protocol for ad hoc networks," in *Eigth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, vol. 2, 2007, pp. 546–551.

[38] Y. Ping, B. Yu, and W. Hao, "A multipath energy-efficient routing protocol for ad hoc networks," in *International Conference on Communications, Circuits and Systems Proceedings*, vol. 3, 2006, pp. 1462–1466.

[39] J. Liu, J. Chen, and Y. Kuo, "Multipath routing protocol for networks lifetime maximization in ad hoc networks," in *5th International Conference on Wireless Communications, Networking and Mobile Computing*, 2009, pp. 1–4.

[40] S. Bitam, M. Batouche, and A. Mellouk, "QoSBeeMagnet: A new qos multipath routing protocol for mobile ad-hoc networks," in *IEEE Globocom Workshops*, 2010, pp. 1648–1652.

[41] X. Zhang and L. Jacob, "MZRP: An extension of the zone routing protocol for multicasting in manets," *Journal of Information Science and Engineering*, vol. 20, no. 3, pp. 535–551, 2004.

[42] P. Sinha, R. Sivakumar, and V. Bharghavan, "MCEDAR: Multicast core extraction distributed ad hoc routing," in *Proceedings of IEEE WCNC 1999*, Sept. 1999, pp. 1313–1317.

[43] E. Bommaiah, M. Liu, A. McAuley, and R. Talpade, "AMRoute: Ad hoc multicast routing protocol," in *Internet Draft (work in progress)*, Aug. 1998.

[44] T. Ozaki, J. B. Kim, and T. Suda, "Bandwidth efficient multicast routing protocol for ad hoc networks," in *Proceedings of IEEE ICCCN 1999*, Oct. 1999, pp. 10–17.

[45] V. Devarapalli, A. A. Selcuk, and D. Sidhu, "MZR: A multicast protocol for mobile ad hoc networks," in *Internet Draft (work in progress)*, July 2001.

[46] C. K. Toh, G. Guichala, and S. Bunchua, "ABAM: On-demand associativity-based multicast routing for ad hoc mobile networks," in *Proceedings of IEEE VTC 2000*, Sept. 2000, pp. 987–993.

[47] L. Ji and M. S. Corson, "Differential destination multicast - a MANET multicast routing protocol for small groups," in *In Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2001)*, vol. 2, 2001, pp. 1192–1201.

[48] S. K. Das, B. S. Manoj, and C. S. R. Murthy, "Weight-based multicast routing protocol for ad hoc wireless networks," in *Proceedings of IEEE GLOBECOM 2002*, vol. 1, Nov. 2002, pp. 17–21.

[49] R. S. Sisodia, I. Karthigeyan, B. S. Manoj, and C. S. R. Murthy, "A preferred link-based multicast protocol for wireless mobile ad hoc networks," in *Proceedings of IEEE ICC 2003*, May 2003, pp. 2213–2217.

[50] E. M. Royer and C. E. Perkins, "Multicast operation of the ad hoc on-demand distance vector (MAODV) routing," in *Proceedings of ACM MOBICOM 1999*, Aug. 1999, pp. 207–218.

[51] C. W. Wu, Y. C. Tay, and C. K. Toh, "Ad hoc multicast routing protocol utilizing increasing id-numbers (AMRIS) functional specification," in *Internet Draft (work in progress)*, Nov. 1998.

[52] S. J. Lee, M. Gerla, and C. C. Chiang, "On-demand multicast routing protocol," in *Proceedings of IEEE WCNC 1999*, Sept. 1999, pp. 1298–1302.

[53] S. K. Das, B. S. Manoj, and C. S. R. Murthy, "A dynamic core-based multicast routing protocol for ad hoc wireless networks," in *Proceedings of ACM MOBIHOC 2002*, June 2002, pp. 24–35.

[54] C. C. Chiang, M. Gerla, and L. Zhang, "Forwarding group multicasting protocol for multi-hop, mobile wireless networks," *ACM/Baltzer Journal of Cluster Computing: Special Issue on Mobile Computing*, vol. 1, no. 2, pp. 187–196, 1998.

[55] S. Lee and C. Kim, "Neighbor supporting ad hoc multicast routing protocol," in *Proceedings of ACM MOBIHOC 2000*, Aug. 2000, pp. 37–50.

[56] J. J. Garcia-Luna-Aceves and E. L. Madruga, "The core-assisted mesh protocol," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1380–1394, 1999.

[57] L. Junhai, Y. Danxia, X. Liu, and F. Mingyu, "A survey of multicast routing protocols for mobile ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 1, pp. 78–91, 2009.

[58] G. D. Kondylis, S. V. Krishnamurthy, S. K. Dao, and G. J. Pottie, "Multicasting sustained CBR and VBR traffic in wireless ad hoc networks," in *Proceedings of IEEE ICC 2000*, June 2000, pp. 543–549.

[59] I. Karthigeyan, B. S. Manoj, and C. S. R. Murthy, "Multicast priority scheduling protocol for ad hoc wireless networks," in *Technical Report*, Jan. 2004.

[60] K. Bur and C. Ersoy, "Ad hoc quality of service multicast routing," *Elsevier Science Computer Communications*, vol. 29, no. 1, pp. 136–148, 2005.

[61] L. Briesemeister and G. Hommel, "Role-based multicast in highly mobile but sparsely connected ad hoc networks," in *Proceedings of ACM MOBIHOC 2000*, Aug. 2000, pp. 45–50.

[62] H. Zhou and S. Singh, "Content-based multicast (CBM) in ad hoc networks," in *Proceedings of ACM MOBIHOC 2000*, Aug 2000, pp. 51–60.

[63] Y. B. Ko and N. H. Vaidya, "Geocasting in mobile ad hoc networks: Location-based multicast algorithms," in *Proceedings of IEEE WMCSA 1999*, Feb. 1999, pp. 101–110.

[64] E. M. Royer and C.-K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE Personal Communications*, vol. 6, no. 2, pp. 46–55, 2002.

[65] M. Hollick, J. B. Schmitt, C. Seipl, and R. Steinmetz, "The ad hoc on-demand distance vector protocol: An analytical model of the route acquisition process," in *In Proceedings of Second International Conference on Wired/Wireless Internet Communications*, 2004, pp. 201–212.

[66] C. E. Perkins, E. M. Royer, and S. R. Das, "Quality of service in ad hoc on-demand distance vector routing," in *IETF Internet Draft*, July 2000.

[67] M. K. Marina and S. R. Das, "Ad hoc on-demand multipath distance vector routing: Research articles," *Wireless Communication and Mobile Computing*, vol. 6, no. 7, pp. 969–988, 2006.

[68] Sajama and Z. J. Haas, "Independent-tree ad hoc multicast routing (ITAMAR)," *Mobile Networks and Applications*, vol. 8, no. 5, pp. 551–566, 2003.

[69] D. Pompili and M. Vittucci, "PPMA, a probabilistic predictive multicast algorithm for ad hoc networks," *Ad Hoc Networks*, vol. 4, no. 6, pp. 724–748, 2006.

[70] C.-C. Shen and C. Jaikaeo, "Ad hoc multicast routing algorithm with swarm intelligence," *Mobile Networks and Applications*, vol. 10, no. 1, pp. 47–59, 2005.

[71] K. Viswanath, K. Obraczka, and G. Tsudik, "Exploring mesh and tree-based multicast routing protocols for MANETs," *IEEE Transactions on Mobile Computing*, vol. 5, no. 1, pp. 28–48, 2006.

[72] S. H. Bae, S.-J. Lee, W. Su, and M. Gerla, "The design, implementation, and performance evaluation of the on-demand multicast routing protocol in multihop wireless networks," *IEEE Network*, vol. 14, pp. 70–77, 2000.

[73] R. Vaishampayan and J. J. Garcia-Luna-Aceves, "Efficient and robust multicast routing in mobile ad hoc networks," in *Proceedings of IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, Oct. 2004, pp. 304–313.

[74] S. Park and D. Park, "Adaptive core multicast routing protocol," *Wireless Networks*, vol. 10, no. 1, pp. 53–60, 2004.

[75] S.-J. Lee, W. Su, J. Hsu, M. Gerla, and R. Bagrodia, "A performance comparison study of ad hoc wireless multicast protocols," *In Proceedings of IEEE INFOCOM*, vol. 2, pp. 565–574, 2000.

[76] J. Luo, X. Liu, and D. Ye, "Research on multicast routing protocols for mobile ad-hoc networks," *Computer Networks*, vol. 52, no. 5, pp. 988–997, 2008.

[77] A. Boukerche, M. Z. Ahmad, Damla, Turgut, and B. Turgut, "A taxonomy of routing protocols for mobile ad hoc networks," in *Chapter 5 of Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks*, 2009, pp. 129–163.

[78] O. S. Badarneh and M. Kadoch, "Multicast routing protocols in mobile ad hoc networks: A comparative survey and taxonomy," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, 2009.

[79] B. Cohen, "Incentives build robustness in BitTorrent," 2003, available at `http://bitconjurer.org/BitTorrent/bittorrentecon.pdf`.

[80] S. J. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in *IEEE International Conference on Communicaitons*, 2001.

[81] M. K. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks," in *Proceedings of the IEEE ICNP 2001*, 2001, pp. 14–23.

[82] A. Valera, W. K. G. Seah, and S. V. Rao, "Cooperative packet caching and shortest multipath routing in mobile ad hoc networks," in *In Proceedings of the IEEE INFOCOM*, vol. 1, 2003, pp. 260–269.

[83] A. Nasipuri and R. Castañeda, "Performance of multipath for on-demand protocols in mobile ad hoc networks," *Mobile Networks and Applications*, vol. 6, pp. 339–349, 2001.

[84] A. M. Abbas and T. A. Abbasi, "An analytical framework for disjoint multipath routing in mobile ad hoc networks," *IFIP International Conference on Wireless and Optical Communications Networks*, 2006.

[85] D. Sidhu, R. Nair, and S. Abdallah, "Finding disjoint paths in networks," *SIGCOMM Comput. Commun. Rev.*, vol. 21, no. 4, pp. 43–51, 1991.

[86] T. R. Henderson, S. Roy, S. Floyd, and G. F. Riley, "ns-3 project goals," in *In WNS2 06: Proceeding from the 2006 workshop on ns-2: the IP network simulator.* ACM, 2008.

[87] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *In Proceedings of the First International Conference on Simulation Tools and Techniques for Communications, Networks and Systems*, Mar. 2008.

[88] K. Meuller. SimPy documentation. [Online]. Available: http://simpy.sourceforge.net/discuss.htm

[89] R. Barr, Z. J. Haas, , and R. van Renesse, "JiST: An efficient approach to simulation using virtual machines," *Software - Practice and Experience*, vol. 35, no. 6, pp. 539–576, 2005.

[90] OPNET technologies inc. OPNET modeler website. [Online]. Available: http://www.opnet.com/solutions/network_rd/modeler.html

[91] X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: A library for parallel simulation of large-scale wireless networks," in *in Workshop on Parallel and Distributed Simulation*, 1998, pp. 154–161.

[92] E. Weingrtner, H. vom Lehn, and W. Klaus, "A performance comparison of recent network simulators," in *Proceedings of the IEEE International Conference on Communications*, 2009.

[93] S. A. G. Chandler, "Calculation of number of relay hops required in randomly located radio network," *Electronics Letters*, vol. 25, no. 24, pp. 1669–1671, November 1989.

[94] P. Vellore, P. Gillard, and R. Venkatesan, "Probability distribution of multi-hop multipath connection in a random network," in *IEEE GLOBECOM '09: Proceedings of the 2009 IEEE Global Communications Conference*, December 2009.

[95] G. Parissidis, V. Lenders, M. May, and B. Plattner, "Multi-path routing protocols in wireless mobile ad hoc networks: A quantitative comparison," *6th International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking*, pp. 313–326, May-June 2006.

[96] C. Bettstetter and J. Eberspacher, "Hop distances in homogeneous ad hoc networks," in *57th IEEE Semiannual Vehicular Technology Conference*, vol. 4, April 2003, pp. 2286–2290.

[97] L. E. Miller, "Probability of a two-hop connection in a random mobile network," in *35th Conference on Information Sciences and Systems*, March 2001, pp. 66–70.

[98] P. Gillard, P. Vellore, and R. Venkatesan, "BitTorrent enabled ad hoc networks," in *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, vol. 3, August 2005, pp. 186–191.

[99] L. E. Miller, "Distribution of link distances in a wireless network," *Journal of Research of the National Institute of Standards and Technology*, vol. 106, no. 2, pp. 401–412, March-April 2001.

[100] P. Vellore, P. Gillard, and R. Venkatesan, "Delivery analysis of multicasting in BitTorrent enabled ad hoc network (MBEAN) routing," in *IWCMC '06: Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing*, 2006, pp. 1135–1140.

Appendix A

Confidence Interval Calculation

The standard error can be calculated as follows:

$$SE = s/sqrt(n), \tag{A.1}$$

where SE is the standard error, s is the standard deviation and n is the sample size. Assuming 95% confidence interval, let

$$\alpha = 1 - (confidenceinterval/100). \tag{A.2}$$

Critical probability can be given as,

$$p = 1 - \alpha/2. \tag{A.3}$$

The degrees of freedom can be represented as,

$$df = n - 1. \tag{A.4}$$

Using the t-distribution, the critical value (CV) can be obtained using df, as the degree of freedom an p, as the probability. The margin of error (ME) can be calculated as

$$ME = CV * SE. \tag{A.5}$$

The range of confidence interval is defined as the average value of PDR or member reliability ± margin of error.