ESTIMATION OF OPTIMAL NODE DEGREE FOR AD-HOC SENSOR NETWORKS

A Thesis by

Michael Stanis Deepak

Bachelor of Engineering, Bharathiar University, India, 2004

Submitted to the Department of Electrical and Computer Engineering
and the faculty of the graduate school of
Wichita State University
in partial fulfillment
of the requirements for the degree of
Master of Science

May 2009

ESTIMATION OF OPTIMAL NODE DEGREE FORAD-HOC SENSOR NETWORKS

The following faculty members have examined the final copy of this thesis for form and content, and recommend that it be accepted in partial fulfillment of the requirement for the degree of Master of Science with a major in Electrical Engineering.

Ravi Pendse, Committee Chair

Kameswara Rao Namuduri, Committee Member

Krishna Krishnan, Committee Member

Edwin Sawan, Committee Member

DEDICATION

This thesis is dedicated to my parents and my sisters

ACKNOWLEDGEMENTS

I would like to thank my advisor, Dr. Ravi Pendse, for his guidance, support, and encouragement throughout my graduate study at Wichita State University. I would also like to thank Dr. Kameswara Rao Namuduri and Dr. Krishna Krishnan for their time spent in reviewing this thesis work.

My special thanks to Nagaraja Thanthry for providing me with ideas, suggestions, and helping me complete my thesis work.

I appreciate all my friends for their continued support, especially, thanks to Murali Krishna Kadiyala for listening patiently to my ideas, providing me with valuable suggestions, and reviewing my thesis report. I am grateful to my roommates Natarajan Venugopalan, Vishwanath for supporting me morally through the years I have known them.

Finally, I am very grateful to my family members for their love and support.

ABSTRACT

Recent developments in sensor networks have led to a number of routing schemes that use the limited resources available at sensor nodes more efficiently. Control traffic analysis plays a major role in ad hoc sensor networks in optimizing the energy used in the network.

In this research, we present an effective method to estimate the number of nodes to be deployed in a given area. We analyze the optimal node degree under different levels of mobility. We consider two parameters, packet delivery ratio and control traffic for the estimation of optimal node degree. The quantitative and simulation results provide a detailed analysis of the working of protocols and they can be used to design efficient routing protocols for ad hoc networks.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure page

LIST OF ABBREVIATIONS

AODV	Ad-Hoc On-Demand Distance Vector Routing
CBR	Constant Bit Rate
CTS	Clear To Send
DCF	Distributed Coordination Function
DSDV	Destination-Sequenced Distance-Vector Routing
DSR	Dynamic Source Routing
FTP	File Transfer Protocol
Glomosim	Global Mobile Information Systems Simulation Library
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
MAC	Medium Access Control
MANET	Mobile Ad-Hoc Network
OLSR	Optimized Link State Routing
QOS	Quality Of Service
RERR	Route Error
RREP	Route Reply
RREQ	Route Request
RSVP	Resource Reservation Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
RTS	Request To Send
RTS	Request To Send
SARP	Self-Learning Ad-Hoc Routing Protocol

LIST OF ABBREVIATIONS (CONT.)

SNR	Signal to Noise Ratio
SSR	Signal Stability Routing
STAR	Source Tree Adaptive Routing
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	Time to Live
UDP	User Datagram Protocol
VC	Virtual Circuit
WLAN	Wireless Local Area Network
WRP	Wireless Routing Protocol

LIST OF SYMBOLS

λ	Lambda
$\sum$	Summation
μ	Micro
ρ	Rho

CHAPTER 1

INTRODUCTION

The emergence of miniature sized wireless communication sensors has initiated a new embedded system. These systems are deployed in an environment where there is no specific control path. These wireless sensor nodes are attached to circuits and applications to monitor and sense their usage. Together they form a multi hopping network which is decentralized in nature. An ad hoc network can be described as a network which is formed for a particular occasion. The ad-hoc networks consist of nodes which have wireless capability and may be mobile without the need of centralized infrastructure. The ad hoc networks can quickly self configure to form a network topology. The challenging issues in ad hoc networks are the limitation in resource availability like bandwidth and battery power. So these devices cannot handle complex routing protocols which are deployed in the modern wireless devices which require a good quality of service (QOS).

One important characteristic of an ad hoc network is that the devices themselves are the network. This allows seamless communication, in a self-organized fashion and with easy deployment. This self organizing capability makes ad hoc networks completely different from other network solutions. Ad hoc networks are dependent on the inter-node communication and this communication depends on the availability of intermediate nodes.

The dynamic and self-organizing nature of networks makes them useful in specific situations where on demand network deployments are required. From the network perspective, the main properties of ad hoc networks include:

- Ad-hoc networks establish connection on the fly. Hence, installing network and network management must be dynamic.

- They are usually very large networks comprising of thousands or even hundreds of thousands of dynamically connected nodes.
- The communication channel must have the following characteristics: (a) handle communication errors which arise due to wireless channel impairments, (b) ability to operate in a limited bandwidth as the wireless nodes communicate in a limited bandwidth channel and (c) maintain connectivity and preserve link qualities among the neighboring nodes which change automatically according to the received signal strength.
- Data has to travel through multiple nodes before reaching the final destination.

Frequent topological changes are assumed due to mobility of nodes. To manage the routing issues for reliable and efficient data communication, there are different routing protocols that have been suggested for ad hoc networks like destination-sequenced distance vector routing (DSDV) [1], dynamic source routing (DSR) [2], ad-hoc on demand distance vector routing (AODV) [3]. Most of these ad-hoc routing protocols choose routes to based on the destination on some criteria like minimum number of hops or by choosing a route that will reach the destination first with the goal that the route being selected will be the shortest in terms of delay or distance from the source. Recent studies with ad-hoc routing protocols have revealed that choosing a route based on the first received route request (RREQ) packet without taking into account the stability of the route leads to frequent route failures [4] and studies have revealed that choosing routes based on signal strength often yields more stable routes [5]. Most of the routing overhead in a network is due to the number of control packets generated while maintaining and installing new routes. Whenever there is a link break along the path in a route, a route maintenance function is called. This function involves the generation of a route error packets by the intermediate node which detects the link breakage. When the source is

made aware of the route failure through the route error packet (RERR), it invokes the route discovery function. Frequent generation of these Control packets leads to increase in the routing overhead, thereby decreasing the available bandwidth to other data packets. The route discovery process which initiates the route request packets (RREQ) throughout the network, results in an increase in control overhead. This results in a delay arising due to the route re-establishment, in addition to a considerable decrease in the packet delivery ratio.

The most widely used and powerful wireless access technology, most commonly known as IEEE 802.11 or the wirelesses LAN, has given a massive impulse for the dissemination of wireless ad-hoc networks. In this type of networks, the stations, namely the nodes which are in proximity to each other help each other in acquiring and maintaining the route. The nodes compete for the shared transmission medium. The medium access control layer of IEEE 802.11 makes use of distributed coordination function (DCF). However, several studies have shown that, the DCF tends to equally share the transmission medium among the contending stations [6]. Although this property of DCF appears to be a very fine property, this fineness will lead to many undesirable situations. For example, if one of the nodes begins to function as a bridge toward each of the nodes, group of nodes, or to the worldwide internet which questions the stability of the network. Recently, work has been done to improve the QoS - for the IEEE 802.11 standard, which is so called the EDCA 802.11("e") version [7]. In other words, the 802.11e extension provides mechanisms to prioritize certain traffic patterns (or nodes) over others.

The main objective of this thesis is to propose a mathematical analysis of the optimal node degree in ad hoc networks. The analytical and simulation results presented in this research work provide an insight to the working of the ad hoc routing protocol.

Chapter 2 gives a literature survey introducing ad hoc networks and brief description of the existing ad hoc routing protocols. In Chapter 3, the proposed mathematical analysis of the optimal node degree is analyzed In Chapter 4, an overview of the simulation environment and analysis of the results is given. In Chapter 5 gives the conclusions made and possible future work.

CHAPTER 2

LITERATURE SURVEY

In this chapter, we provide a summary of the existing literature. This chapter is divided into two sections. In the first section, we discuss the ad-hoc networks. In the rest of the sections we deal with the review of current ad hoc routing protocols. The last section gives a brief overview of the related work done.

2 .1 Ad-Hoc Networks

Mobile wireless networks are put into two broad categories as infrastructure and infrastructure less networks. Examples of infrastructure networks are cellular networks, which consist of centralized infrastructure with stationary base stations and mobile nodes. In order to provide an uninterrupted service, a handoff mechanism is used, when the node moves from one base station to another. Other example of infrastructure based networks include wireless local area networks (WLAN), which has a centralized base station namely router. The second category of network includes the ad-hoc networks, which do not require a centralized infrastructure. Each individual node not only acts as a host but also as a router forwarding packets to the neighboring nodes. Communication in these types of networks are called multi-hop, where all the intermediate nodes between the source and destination should forward the data as well as the control packets. We assumed that all the intermediate nodes will participate in the forwarding of route packets. Figure 2.1 shows multi-hop communication between the source and destination in a wireless ad-hoc network. The packet has to traverse through multiple nodes before it reaches the destination. The packet traverses through multiple nodes from source A

before it reaches the destination O namely B, I, M, O. Data may travel through multiple hops to reach destination as in the case of node M. The one good thing about multi-hop network is that it increases the overall bandwidth since the spatial domain can be re-allocated for individual sessions which are physically separated.

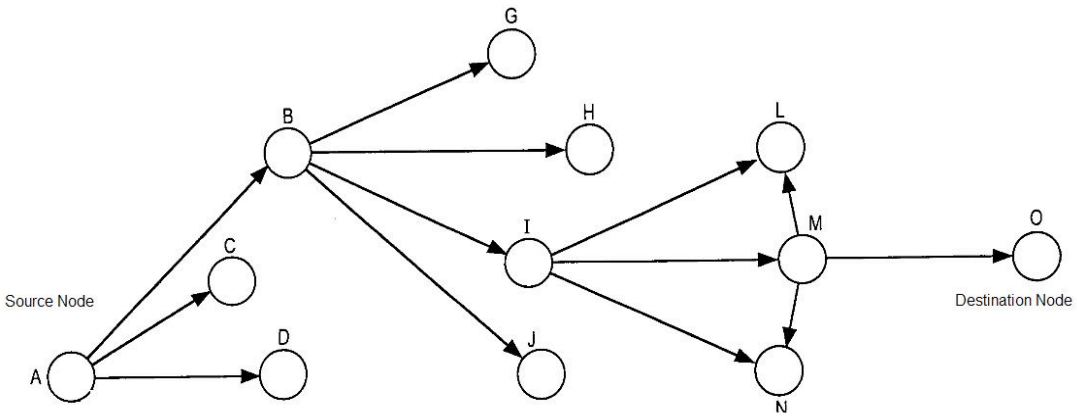


Figure 2.1 : Multi-hop Ad-Hoc Networks

Several routing protocols have been proposed for the mobile ad hoc networks [1], [2], [3], [4]. The routing protocols can be categorized as the proactive protocols, the reactive protocols or the hybrid of the reactive and proactive protocols. The proactive protocols are table driven while the reactive protocols are source initiated or demand driven. Routing protocols are designed to cooperate with rapid changes in the network topology. In fixed networks, when a router or a link becomes invalid, the routing mechanism finds an alternative route from source to destination [5]. In ad-hoc networks, movement of nodes continuously changes the topology of the network. Some nodes become unreachable while new nodes may become available, old links are removed while new ones are established. Theoretically, a routing protocol should trace network changes and allow nodes to find each other. However, the routing protocols developed for fixed networks (like RIP or OSPF [6]) cannot handle rapid changes in the network and create a relatively large routing overhead. Therefore, for ad-hoc networks special routing

protocols are needed. These protocols, if they are fast and efficient, should solve the mobility problem. Routing in ad-hoc networks is basically a compromise between the method of dealing with routing overhead and fast topology changes.

In proactive routing protocols, routing information to reach all the other nodes in a network is always maintained in the form of the routing table on all the nodes. When the network topology changes which is accompanied by a movement of nodes, creation of new links or the removal of existing nodes, such changes in topology are communicated to all nodes in the network. Thus, links to all possible destinations are discovered before the packet transmissions. However rapid changes in the network flood the network with control messages and these overwhelming packets will affect throughput of actual data transmissions. The examples of proactive protocols are distance vector (DV) protocol [7], WRP (wireless routing protocol) [8], destination sequenced distance (DSDV) protocol [9], and FSR (fisheye state routing) protocol [10]. These four routing protocols are also called as table-driven protocols, since their routing table will be updated for each change in link states of the network. Reactive protocols discover routes only when there is an actual transmission. When a node wants to send a message to another node in a network, a source node initiates a route-discovery process. Once a route is discovered, it is maintained in the route cache at a source node till it is expired or unless some event like a link failure happens that requires another route discovery to start over again. Reactive protocols require comparatively less routing information at every node, compared to the proactive protocols, as there is no necessity to obtain and maintain the routing information at all the nodes in a network. Another advantage of reactive protocols is that the intermediate nodes do not make the routing decisions. The disadvantage of reactive protocols is delay due to route discovery, called the route acquisition delay. However if the routing information changes frequently, route discoveries are needed for those

changed routes, reactive protocols may result in a huge routing overhead, since route recoveries require global broadcasts. The popular reactive protocols are dynamic source routing (DSR) protocol [2], ad hoc on demand distance vector (AODV) protocol [3], and ABR (associatively based routing) protocol [11]. Since the initial delay due to route discovery and high control overhead in reactive protocols, a pure reactive protocol may not be the best solution for routing in MANETs, while a pure proactive protocol when used for a big network may not be feasible because of the large routing overhead. Hybrid protocols are protocols that use the best features of both reactive and proactive protocol which may be a better solution for MANETs. An example for such an approach is the ZRP (zone routing protocol) [11], although it is not the solution for all the limitations of other protocols.

Error! Reference source not found.

Figure 2.2 : Types of ad-hoc routing protocols

2.2 Ad-Hoc on Demand Distance Vector Routing Protocol (AODV)

Ad-hoc on demand distance vector (AODV) protocol [3] is a reactive routing protocol that has a characteristic of providing a compromise between reactive source routing protocols and proactive protocols. The trade-off AODV addresses is the one between high messaging overhead due to periodic link updates states in proactive protocols and the large packet header to contain the entire route information to reach a destination in source routing protocols. Unlike other distance vector protocols, routes are discovered and maintained on demand in AODV. Unlike DSR, AODV maintains a distributed approach, meaning that source nodes do not maintain a complete sequence of intermediate nodes to reach a destination. Different from distance vector and WRP, each

path is established as a pair of two streams of pointers chained between a source and a destination node which eliminates the need of broadcasting an error packet on a route link failure. Similar to DSR, AODV uses the route discovery and route reply mechanism to initiate and maintain a route.

2.2.1 Route Discovery Mechanism

When a source node needs to send a data packet to a destination node, it first verifies in its own routing table that no route exists between the source and the destination node. In the absence of a valid route, the source node initiates the route discovery mechanism by broadcasting a route request (RREQ) packet across the network. The RREQ in turns sets up a timer for the reception of the reply. The RREQ packet contains the source ip address, source sequence number, destination ip address, last obtained destination sequence number, broadcast identifier, and number of hops. The globally broadcasted RREQ packets are uniquely identified by the combination of the source address and the broadcast address. Any node that receives the route request packet which either has a valid route to the destination with a sequence number at least as great as that contained in RREQ packet or is the destination node itself will respond to route request message. If either of this condition is satisfied the node will respond with a route reply (RREP) packet. Otherwise, the packet is rebroadcasted to the other nodes as shown in figure 2.3a. Also, each node which receives the route request packet will maintain a reverse route to the source in the routing table.

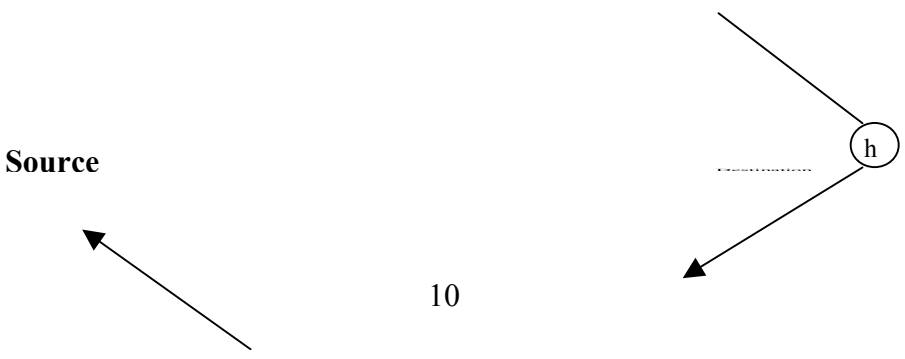
The route discovery mechanism can be visualized as a pair of pointers namely a forward pointer and the backward pointer. When the route request message is broadcasted a series of forward pointers are set up between the source and the destination. Identically, a series of back pointer are set up, while the route reply packet travels from either the destination to source or from the node, which has a valid route to the destination. Thus,

all the intermediate nodes in a route contain a pair of the forward pointer and the back pointer for every control packet that pass through them. If the route encounters a duplicate set of intermediate node in the routing table, then the route request message will be discarded. Thus a loop free routing is guaranteed.

The working principal of the AODV protocol can be better understood by the following figure 2.3. When the source node ‘a’ wishes to transmit data to destination node h’, the aodv protocol will check its routing table for the route. In the absence of a route the destination, it will initiate a route discovery process by sending the RREQ packet to all its neighbors. The propagation of RREQ packet is shown in Figure 2.3 (a). When the intermediate node receives the RREQ packet and if it finds that it is not the destination, it will first check its routing table for a path to the destination. If found, it will forward the RREP packet back to the source else it will broadcast the RREQ packet in the network. When the RREQ packet finds its way to the destination, the destination node will initiate a RREP packet back to the source. Figure 2.3 (b) shows the propagation of RREP packet to the source node ‘a’. In this case it is assumed that the RREQ takes the path via g-f since it reaches the destination before the other paths, the obvious reason being the shortest path and the least number of hop counts. The RREP packet travels to the source on a hop by hop basis along the reverse path that has been discovered during the process of RREQ propagation. When the source node ‘a’ receives the RREP packet, it will start transmitting the data, and update its routing table with the new route.

Error! Reference source not found.

(a)



(b)

a) Propagation of RREQ.
b) Data path of RREP.
Figure 2.3 : Route Discovery Mechanism

2.2.1.1 Route Request Packet Format

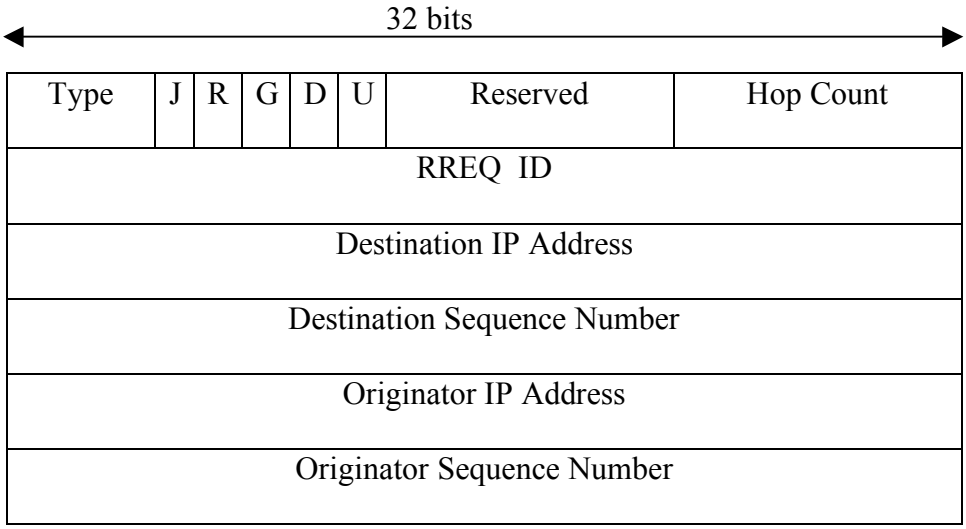


Figure 2.4: RREQ packet format in AODV

- Type: This field represents the type of the packet in AODV. It is 1 for RREQ
- J,R,G,D,U: These flags indicate the join flag, repair flag, gratuitous reply flag, destination only flag and unknown sequence flag
- Reserved: This field is unused and set to 0
- Hop Count: Number of hops from the source node to the node which handles the request
- RREQ ID: A sequence number which uniquely identifies the RREQ packet while taking into account the originating node's IP address
- Destination ip Address: This is the ip address of the destination node for which the data is intended.
- Destination Sequence Number: The latest sequence number received
  By the originator for any route to the destination
- Originator IP Address: The ip address of the source that initiated the route request
- Originator Sequence Number: The sequence number pointing towards the originator of the route request.

2.2.1.2 Route Reply Packet Format

The RREP packet generated by the destination is a unicast packet to the source as the destination. Each intermediate node in the network along will forward the packet back to the source using the path discovered during the propagation of RREQ packet. Figure 2.5 shows the packet structure of the RREP packet in AODV. Once the source node receives the RREP the data transfer is initiated from the source to the destination. Unlike the route discovery process in DSR the RREP does not have the full route or path information in the packet, but it has information of the next hop at each intermediate node, in the routing table.

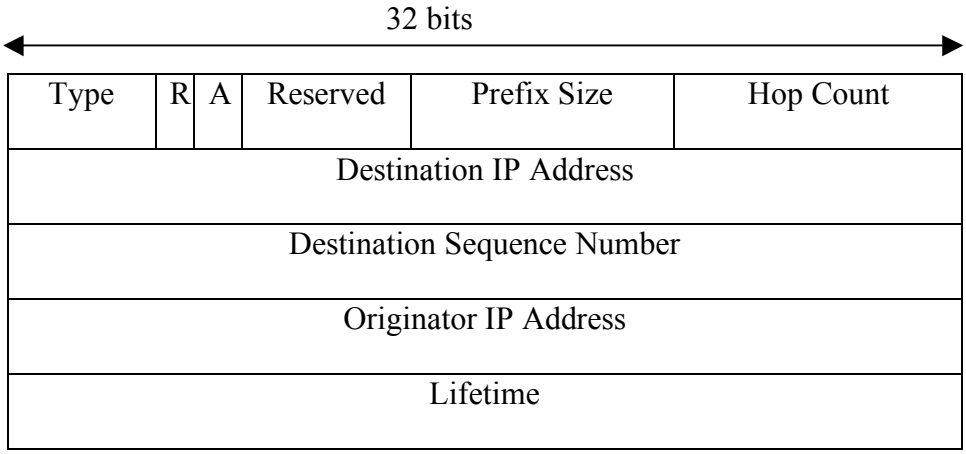


Figure 2.5: Format of a RREP in AODV.

- Type: This field indicates the type of the packet in AODV. It is 2 for a route reply
- R: The repair flag is used for multicasting
- A: This flag is required for acknowledgement
- Reserved: This field is unused and is set to 0
- Prefix Size: If this bit is non zero then it indicates that the next hop may be used for any nodes with the same routing prefix as that of the requested destination
- Hop Count: The number of hops traversed from the source IP address to the Destination IP address
- Destination IP address: The IP address of the destination node for which the data is intended.
- Destination Sequence Number: The destination sequence number associated with the destination node
- Originator IP address: The IP address of the node of originator of RREQ packet
- Lifetime: The time to live field for the route reply packet for which the route is valid. It's measured in milliseconds.

2.2.2 Route Maintenance Mechanism

Route maintenance is initiated when there is a breakage in the link along the path to the destination node. This is achieved by using the Route Error (RERR) packets. Figure 2.6 shows the format of the RERR packet. The link breakage can be detected by two mechanisms. The first one is by the retransmissions of wireless MAC layer and acknowledgments. The other method is by generating a periodic HELLO messages to the surrounding nodes. In the first method, when there is a linkage break, it will generate a RREP packet with an infinite hop count and larger sequence number to all the nodes in the reverse direction. Hence each route that has the broken link will be invalidated. In the HELLO messages method, each node will periodically send HELLO messages with all its next hop nodes. If the HELLO message is not received in a particular route for an extended period of time, the node will assume that the route no longer exists and a route maintenance mechanism is initiated.

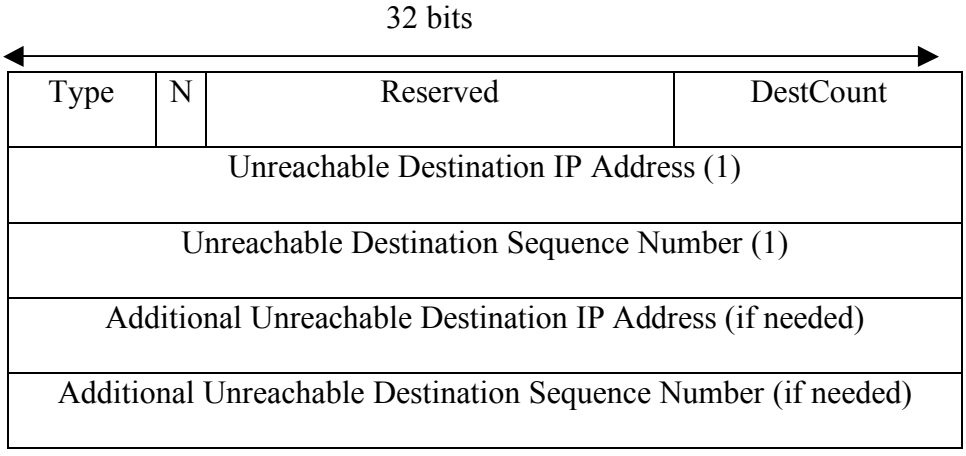


Figure 2.6 : Packet format of RERR in AODV

CHAPTER 3

PROPOSED MODEL

Wireless ad-hoc networks are characterized by highly varying wireless channels frequent node movements. The nodes may have direct links with their neighbors and each node acts as a relay node for routing traffic to destination. At any instant of time, regardless of the mobility model and the topology involved the ad hoc network can be represented as a graph with a set of nodes representing the network and set of edges representing the links between the nodes. We assume that the link between the nodes is bi-directional. Two nodes are connected, if a signal transmitted at one end is received at the other end above minimum power thresholds.

3.1 Modeling Ad hoc Networks

Wireless ad hoc network consist of radio nodes spread over a geographical area. The ad hoc network can be modeled as a graphical representation using the graph theory. At any instant an ad-hoc network can be represented as a graph with a set of vertices indicating nodes and a set of edges consisting of the links in the network. A graph, G = (V, E) is defined as a set of vertices V and a set of edges E. The vertices and edges are always assumed to be finite. An edge is a connection between two vertices. An edge (i, j) denotes the link between vertices i and j. The vertices i and j are the end points of this edge. If an edge exists between two vertices, then they are said to be adjacent or neighboring vertices of G. Two edges are called adjacent if they have exactly one common end point

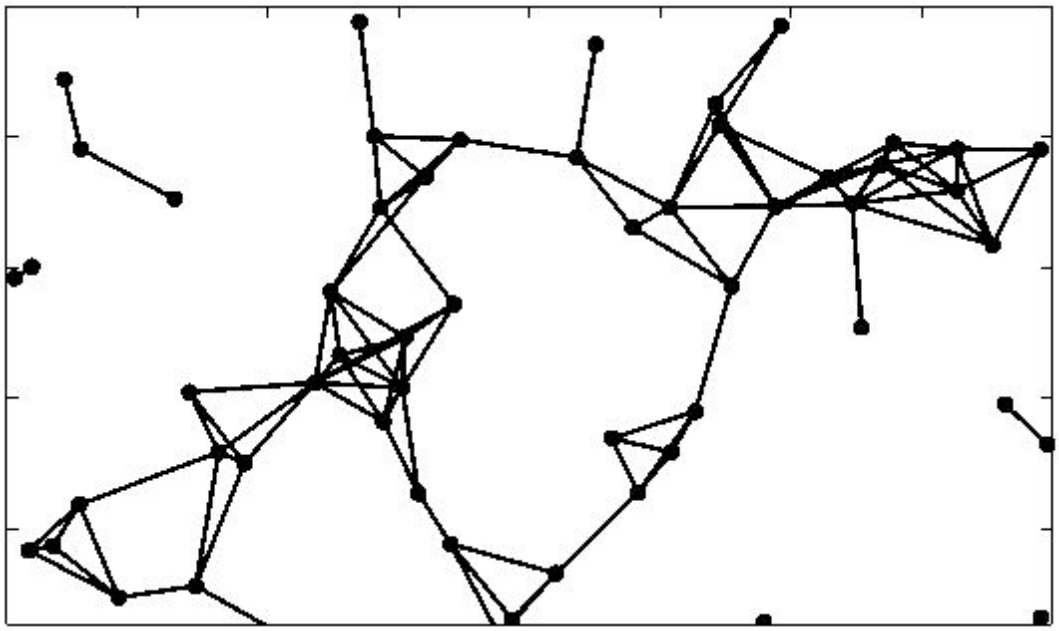


Figure 3.1: Graphical Representation of ad hoc model

3.1.1 Random Graph Model

A random graph with N vertices and K edges can be constructed by starting with N vertices and zero edges. Then K edges are chosen randomly and independently from the N (N − 1)/2 possible vertices. In total, there are $\binom{N(N-1)/2}{L}$ equally probable random graphs with N vertices and K edges. The expected value of edges in the random graph is thus given by equation

$$E[K] = \frac{pN(N-1)}{2} \qquad (1)$$

where p is the probability that the vertices pairs are connected.

3.1.2 Calculation of the Average Hop Count

A random graph is denoted as $G_p(N)$, with an assumption that the presence or absence of one link does not affect the presence and absence of another link. The degree of a node ‘a’ can be defined by using the binomial distribution [19]

$$p_r(d_a = k) = \binom{N-1}{k} p^k (1-p)^{1-n-k} \approx \frac{w^k e^{-w}}{k!} \quad . \tag{2}$$

Equation (2) approximates to the Poisson distribution.

In this equation, w denotes the average degree of the node, i.e.,

$$w = E[d_a = k] = (N-1)p. \tag{3}$$

The variance of w is given by (N-1)p(1-p).

All nodes in the random graph are interconnected by w other nodes. It can be approximated that all nodes will be reached in w^h. The average hop count is calculated by Newman and Strogatz [20].

$$E[h] = \frac{\log(N / E[d])}{\log(E[d(d-1)] / E[d])}. \tag{4}$$

The above equation (4) can be further approximated as equation (5)

$$E[h] = \frac{\log(N)}{\log(E[d])} \tag{5}$$

Where'd' is the random variable which denotes the degree of node and E(d) is the average degree of the node.

3.1.3 Link Density of Ad Hoc networks

We model the ad hoc networks based on the geometric random graph model. In this graph model, the connections between two nodes are based on the geometric distance between the nodes. An undirected geometric random graph with N nodes can be represented as $G_{p(r_{ab})}(N)$, where $p(r_{ab})$ is the probability that there is a link between a and b. The 'N' nodes are considered to be distributed in the entire service area.

In this graph model the expected number of links (L) is give by the following equation

$$L = \sum_{a=1}^{N} \sum_{b=a+1}^{N} P(r_{ab}) \quad . \tag{6}$$

In order to estimate the link density, we use a dissection technique. The N nodes are considered to be distributed in an areaΩ. This area is assumed to be covered with m > N squares and each $\Delta\Omega$ square can hold only one node. The total number of combination that can be formed by N nodes in the area is $\binom{m}{n}$.

The average number of bi directional links is given by [23] as follows:

$$E[L] = \frac{n(n-1)}{m(m-1)} \sum_{a=1}^{m} \sum_{b=a+1}^{m} p(r_{ab}) \tag{7}$$

Link density (ρ) is the ratio of average number of links to the maximum number of bi- directional links.

$$\rho = E[L] / E_{max} \tag{8}$$

where E_{max} is the maximum number of bi-directional links n(n-1)/2

The average degree of node is defined as the product of number of available nodes (n-1) and link density (ρ)

$$E[d] = (n-1)\,\rho = 2E[L]/n. \tag{9}$$

3.2 Mobility Model Ad-Hoc Networks

In our thesis we assume that the nodes are uniformly distributed. Let us assume that the nodes a and b are travelling with a velocity V_a and V_b. The relative velocity can be calculated as difference of the two velocities.

$$V_d = V_a - V_b. \tag{10}$$

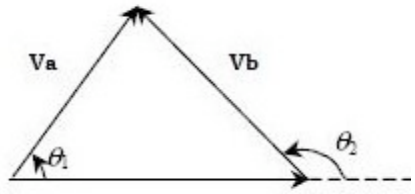


Figure 3.2 Relative velocity between nodes a and b

Let (x,y), (x_1,y_1) and (x_2,y_2) are the Cartesian coordinates of the vectors V_a, V_b and V_d.

Hence the Cartesian and Polar coordinates can be calculated as follows

$$f_{dv,xy}(v_d,\theta) = f_{dv,xy}(v_x v_y)\begin{vmatrix} \frac{\partial v_{dr}}{\partial v_x} & \frac{\partial \theta}{\partial v_x} \\ \frac{\partial v_d}{\partial v_y} & \frac{\partial \theta}{\partial v_x} \end{vmatrix} and$$

$$= f_{dv,xy}(v_d \cos\theta v_d \sin\theta) v_d \ . \tag{11}$$

3.2.1 Link Availability Time

The link available time is defined as the probability that the link is available after a time‘t’ seconds. Let two mobile nodes Mn1 and Mn2 are separated by a distance d.

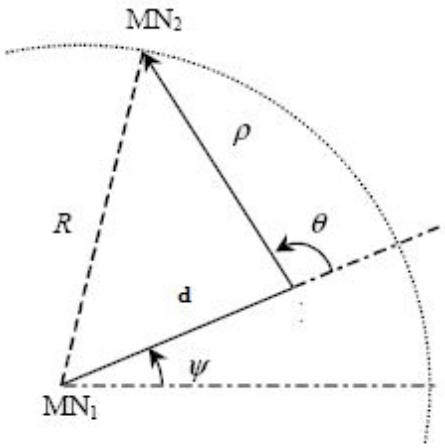


Figure 3.3 Time of Link Availability

The link availability time [21]. can be expressed by the following equation

$$p(\mathrm{d}, \Psi, t) = 1 - F_a(\mathrm{d}, \Psi, t). \quad (12)$$

3.2.2 Path Availability Model

We use random ad hoc mobility model in which nodes are considered to move in sections of random length intervals. These random length intervals are called 'mobile epochs'. The speed and direction of a node 'a' are given by V_a^i and θ_a^i, which is random and different for each epochs.

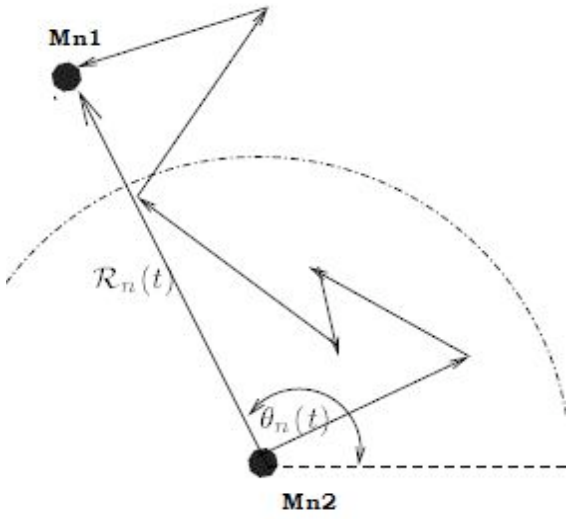


Figure 3.4 Random Ad hoc Mobility Model

The parameters involved in the random mobility model are λ_a, σ_a^2 and μ_a. The following assumptions are considered for calculating the path availability

- The epoch length T_a^i are independent and exponentially distributed with mean λ_a
- The speed V_a^i are distributed randomly with mean μ_a and variance σ_a^2.and constant for the entire duration of the epoch
- The direction of the node θ_a^i is informally distributed over an angle $(0,2\pi)$ and is constant for a particular epoch length.

The link availability model is used to determine the probabilistic status of a wireless link. The status of a link may depend on many conditions like atmospheric change and the range of transmitter and receiver. The transmission range of node 'a' may be approximated to a circle with radius $R_{eq.}$ If the node 'b' is within the transmission range it will be able to intercept the transmission from node 'a'. The Link availability between the nodes 'a' and 'b' is defined as the probability that there is a link at time $(t+t_0)$ provided that there is a link at t_0. The probabilistic equation can be estimated based on [22].

$$L_{ab}(t) \approx 1 - \phi\left(\frac{1}{2}, 2, \frac{-4R_{eq}^2}{\alpha_{ab}}\right) \quad \text{and} \quad (13)$$

$$\alpha_{ab} \approx 2t\left(\frac{\sigma_a^2 + \mu_a^2}{\lambda_a} + \frac{\sigma_b^2 + \mu_b^2}{\lambda_b}\right). \quad (14)$$

where $\Phi(a, b, z)$ is the Kummer-Confluent Hypergeometric function.

R_{eq} is the radius of the transmission range

t – time after which the link status is to be estimated.

By assumption the nodes maintain a mean speed (μ), variance (σ) and the length of the epoch (λ). Hence equation (13) and (14) can be rewritten as equation (15) and (16)

$$L(t) \approx 1 - \phi\left(\frac{1}{2}, 2, \frac{-4R_{eq}^2}{\alpha}\right) \quad (15)$$

$$\alpha \approx 2t\left(\frac{\sigma^2 + \mu^2}{\lambda}\right). \quad (16)$$

3.3 Calculation of Control Traffic

In this section, we estimate the total number of control traffic generated during a route discovery process. The route discovery process involves the generation of RREQ, RREP and RERR as discussed in the literature review. We use AODV routing protocol to support our research work. At the beginning all the nodes in the network have zero caches. As the route discovery process is initiated, the network learns the routes and populates the caches.

3.3.1 Number of RREQ generated

As the network learns the routes, the number of hops taken by the nodes decreases, based on the knowledge gained by the intermediate nodes. The number of RREQ is calculated based on [24]. It is a function of degree of node based on equation (9) and average hop counts given by equation (18).

$$N_{rreq} = E[d] + E[d]^2 + E[d]^3 + \ldots E[d]^{E(h)}. \quad (17)$$

$$E[h]_{after\ route\ cache} = \sum_{h=1}^{h\max} hp_k(h). \quad (18)$$

Where $p_k(h)$ is the probability of an intermediate node at a distance 'h'hops away from the source.

3.3.2 Number of RREP generated

A RREP packet is sent when the packet reaches the destination or the intermediate node which know the path to the destination. AODV uses sequence numbers to prevent duplicates. There is only one RREP packet generated for each route and other RREPs are discarded based on sequence number. The sequence number reduces the number of RREP's generated. Therefore, for each route discovery process the number of route

replies N_{rrep} generated will be equal to the number of hops between the node generating the RREP and the source

$$N_{rrep} = c(\Delta t)\, E[h]_{\text{after- route cache}}. \quad (19)$$

Where $c(\Delta t)$ is the number of session in a time interval (Δt).

3.3.3 Number of RERR generated

A RERR is generated when the packet does not reach the destination. It is based on the number of link failures. Whenever there is a link failure between the neighbors, AODV protocol transmits a RERR to the source node which is using that link. Based on link availability defined equation (13), we determine the probability of link failure ($p_{lf}(t)$) as follows:

$$p_{lf}(t) = 1 - A(t). \quad (20)$$

The number of link failures ($R_{lf}(t)$) is defined as the product of the probability of link failure and the expected number of total number of links in a network with n nodes.

$$R_{lf}(t) = p_{lf}(t)\, nE_{max}. \quad (21)$$

where E_{max} is the total number of bi directional links given by equation (9).

The total number of Route Errors is given by equation (22) based on [24] as follows:

$$N_{rerr}(t) = E[h]\, R_{lf}(t) \quad . \quad (22)$$

3.4 Packet Delivery Ratio

The packet delivery ratio is defined as the ratio of successfully delivered packets to the total number of packets delivered. The Number of packets delivered will change based on the traffic in the network.

$$\text{Packet delivery ratio } (\gamma) = \frac{\text{Total number of packets delivered}}{\text{Total number of packets generated}}.$$

CHAPTER 4

Simulation Environment and Results

In this Chapter, we give an overview of the simulation environment and the results of different scenarios simulated in the estimation of optimal node degree with respect to AODV protocol. We start with an introduction of the simulator used and its functions. The chapter also gives the details of the implementation and the values of the parameters involved.

4.1 Glomosim Simulator

The network simulator we have used for simulation is Glomosim. Glomosim is an acronym of global mobile information system simulator [22] which is a scalable network simulation environment for wireless networks, which was developed in the University of California (UCLA) at the parallel computing laboratory. Glomosim is built using the parallel discrete even Simulation Library (PARSEC) [23]. The parallel execution of Glomosim helps in scalability and to reduce the simulation time. GloMoSim can be used to simulate thousands of mobile nodes without abstracting the details of the lower layer protocols.

Glomosim can be used in the simulation of variety of wireless network protocols including ad-hoc networks, traditional routing protocols and asymmetric satellite communication protocols. Glomosim is built using a layered approach that is based on the seven layer network architecture of OSI. It uses a similar API for communicating between the layers. Table 1 gives a detail view of the layered architecture of Glomosim. This layered architecture of Glomosim facilitates the easy up gradation of different network layer protocols written by different people.

Layers	Protocols
Mobility	Random waypoint, Trace model
Radio Propagation	2 ray, Free space
Radio Model	Noise
Packet Reception Models	SNR based , BER based with BPSK/QPSK modulation
Data Link	(MAC) CSMA, 802.11 and MACA
Network (Routing)	AODV, Bellman-Ford, DSR, Fisheye, LAR ODMRP, WRP
Transport	TCP, UDP
Application	FTP, CBR, HTTP and Telnet

Table 1: Layers of Glomosim

4.2 Glomosim Architecture

The layered architecture of Glomosim facilitates the implementation and improvement at various layers. The detailed layered architecture of Glomosim at each API layer is given in figure 4.1. The layered API provides a solid platform for different people to modify and implement new protocols in the existing layers without affecting the other layers.

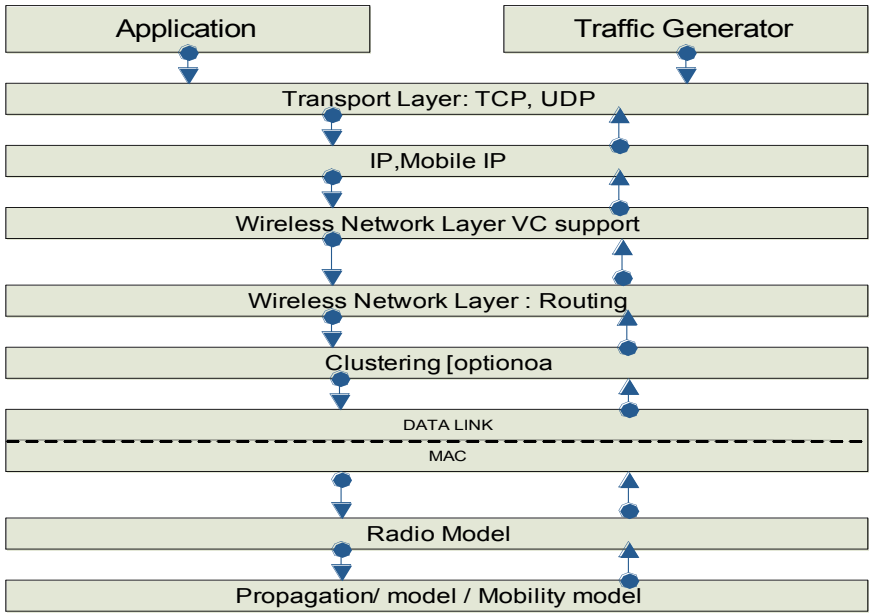


Figure 4.1: Layered architecture of Glomosim

GloMosim is coded using C compiler and it makes use of the PARSEC. The academic version is shipped with the sequential version of PARSEC which can run discrete event in parallel simulations and makes use of parallel programming language. The parallel executions are handled by the PARSEC and the end user does not have to worry about the logic behind the parallel executions. Since PARSEC is almost transparent to the programmer, the end user need not worry about learning the PARSEC compiler. Glomosim is called a discrete-event simulator since the entire simulation is modeled as different events occurring throughout the course of the simulation. We define the event as an incident, which causes the system to change from one form to another. A definite event or a group of events may trigger other events and this process is regenerative and this is how the simulation continues. The event can range from a simple packet reception to the mobility of the node. Discrete events are allowed to occur during a definite period of time and are restrained between time units.

4.3 Glomosim Configuration

The following are the parameters which is included in the configuration file, which is built inside the glomosim.

- PROPAGATION-LIMIT: The strength of the radio signal becomes week as the stations moves away from the origin. In free space the attenuation can be computed as twice the distance travelled. This parameter informs the simulator, when the signal should be ignored by the simulation as the signal becomes too weak. The propagation-limit is measured in dBm.
- PROPAGATION-PATHLOSS: The mitigation of the radio signal may arise due to number of factors in the surrounding atmosphere. Factors like frequency, obstacles, indoor or outdoor environment, long and short-term fading etc affects the attenuation of a radio signal. In order to capture properties of the network model in specific environment we have to make use of different propagation path models. For instance the free space model is describing the attenuation in an open environment with no obstacles.
- NOISE-FIGURE: The noise figure refers to the noise arising due to the background noise, which is most commonly found in the simulation environment. The origin of noise may be from electronic devices like wireless routers, microwave oven and wireless transmitters. Other sources of interferences include cosmic background radiation and thermal noise.
- TEMPARATURE: This parameter is directly proportional to the thermal noise, which is caused by the agitation of electrons. Most of electronic devices and transmission units have thermal noise and is difficult to eliminate.
- RADIO-TYPE: This parameter takes into account interferences from other sources when considering the radio type RADIO-ACCNOISE. The strength of the signal must

be sufficiently higher than the noise level to be received apparently without any error. The radio type considers interference from other transmitters in the simulation when deriving the received SNR (Signal to Noise Ratio). The RADIO-NONOISE is an abstract model, which does not take care of interference.

- MAC-PROTOCOL: The Medium Access Protocol is the protocol which we use in MAC access layer.
- RADIO-FREQUENCY: This is the frequency in which we transmit and receive packets. The parameter is measured in hertz. (Hz)
- RADIO-BANDWIDTH: The parameter gives the maximum bandwidth supported by the channel. The value of the radio bandwidth is in bits per second
- RADIO-RX-TYPE: The radio receiver type is the reception model of a packet. It is expressed in terms Signal to Noise Ratio (SNR). SNR is a ratio between the received signal strength to the interference in dB. A higher value of SNR signifies a strong signal and less interference due to noise. A higher SNR value signifies a higher probability for packet reception. When the radio receiver type is set to use BER-BASED, the probability is derived using an SNR based BER (bit error rate) table for calculating the packet reception. In the table SNR values are mapped to BER values. For a specific SNR value there is a certain bit error rate.
- RADIO-RX-THRESHOLD: This parameter is the minimum power for a received packet. The power of the received packet must be more than this threshold for the receiver to sense the packet. Radio receiver threshold is measured in dBm.
- RADIO-ANTENNA-GAIN: It is a ratio of the intensity of radiation in a specific direction to the intensity of radiation averaged for Omni direction. It is a measure of the directivity of an antenna in dB.

- RADIO-RX-SENSITIVITY: It is minimum sensitivity of the receiver to sense the weak signals. The lesser the value of sensitivity, the lesser is the signal sensed by the receiver. The value of the sensitivity in dBm.
- RADIO-TX-POWER: This gives the maximum power the transmitter can send a signal. The radio transmission power is measured in dBm. The power is usually expressed as milliwatt (mW) but in this Glomosim simulator dBm is used. The dBm is a ratio between the expressed powers in milliwat to one milliwatt.

4.3.1 Calculating the Radio Range

In Glomosim the transmitted power is expressed in terms of dBm. This poses a difficulty in finding the transmission, which is usually expressed in terms of meters. Glomosim makes use of two propagation models namely free space and two ray models. We make use of the free space model for our simulations. We calculate the transmission range based on this equation

$$P_r = P_t \left(\frac{\lambda}{4\pi d}\right)^n G_t G_r .$$

Where P_r - Received power in milliwatts

P_t - Transmitted Power in milliwatts

λ - Receiver wavelength in meters

d – distance between the transmitter and reciever

n – Path loss coefficient

G_t - Gain at the antenna transmitter

G_r - Gain at the antenna receiver

Glomosim is shipped with a program called radio_range which is used to calculate the transmission range. The name of the configuration file has to be given as a argument

while calculating the transmission range. The following syntax is used to calculate the transmission range.

%/radio_range config.in

4.4 Simulation Configuration

We chose the values for the configuration file in Glomosim based on the values we used in the mathematical analysis.

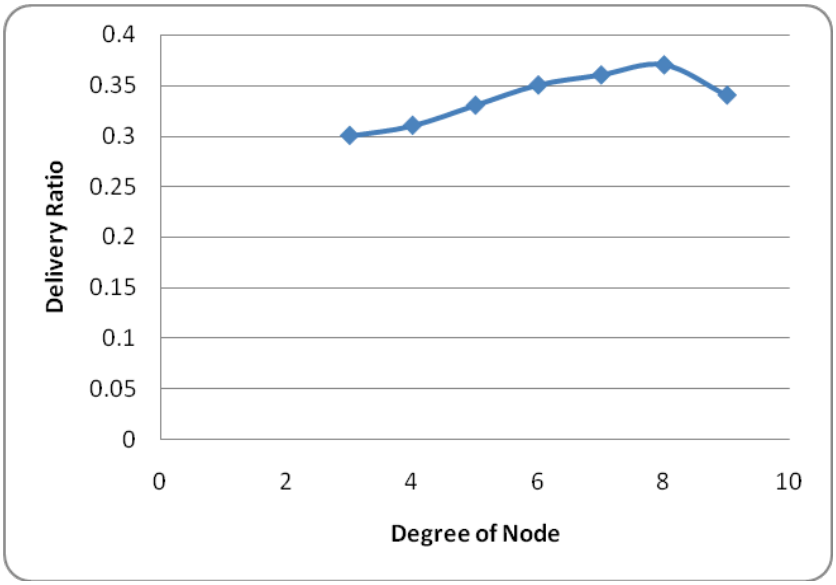
- The radio transmission range is set as 300 m using the program radio_range.
- The mobility is defined using random way point mobility model and mean speed is selected as 10 kph (2.78m/s).
- The simulation area is selected as 1000 mx1000 m.
- The node placement was done randomly over the simulation area.
- 802.11 is used as the MAC protocol.
- The propagation model is free space.
- Bandwidth of radio channel is 2 mbps.
- Radio model used is RADIO-ACCNOISE.
- We use constant bit rate (CBR) traffic to make ten different nodes to communicate with ten other nodes throughout the simulation with 512 kb of data

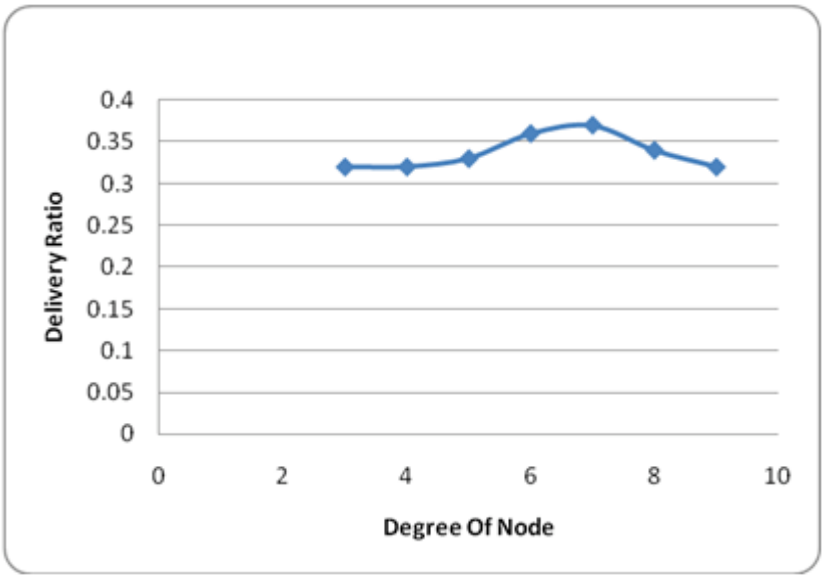
4.5 Simulation Results

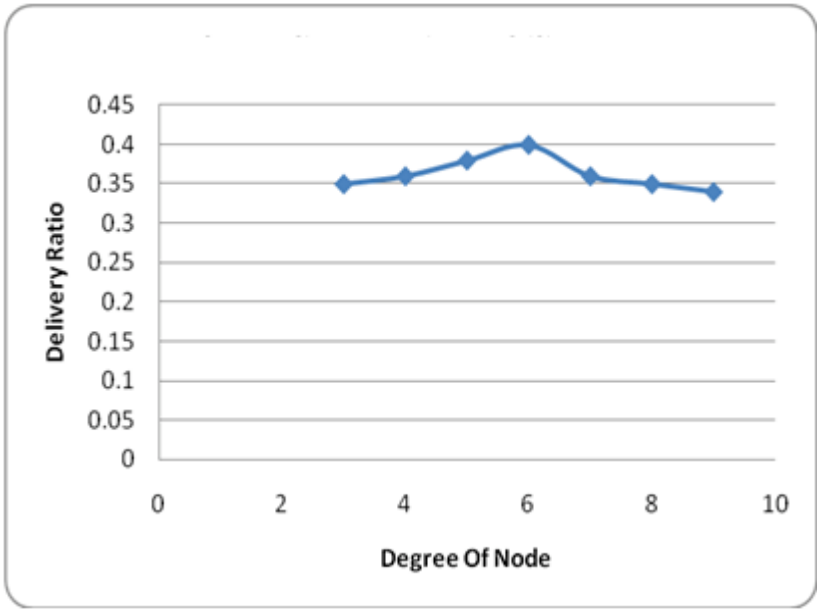
We find the optimal node degree based on two cases. For the first scenario we use the packet delivery ratio and for the second case we use the total control traffic (RREQ, RREP and RERR) under different mobility scenarios to calculate the optimal node degree.

4.5.1 Case 1

The packet delivery ratio can be as the ratio of the number of packets delivered to a destination to those originated by the sources. This is a measure of the efficiency of the routing protocols such as AODV or DSR. The packet delivery ratio of AODV protocol is shown in fig 4. We have shown three mobility models and their graphs are illustrated in the sub figures. It has been shown that for smaller degree of nodes, less data packets are delivered due to the limited availability of routes. However, when the mobility of the nodes increases, the number of packets delivered increases rapidly. This is because as the mobility of the node increases, the availability of the routes increases. However, as the density of the network increases the network becomes saturated and hence the rate of increase is nearly linear.



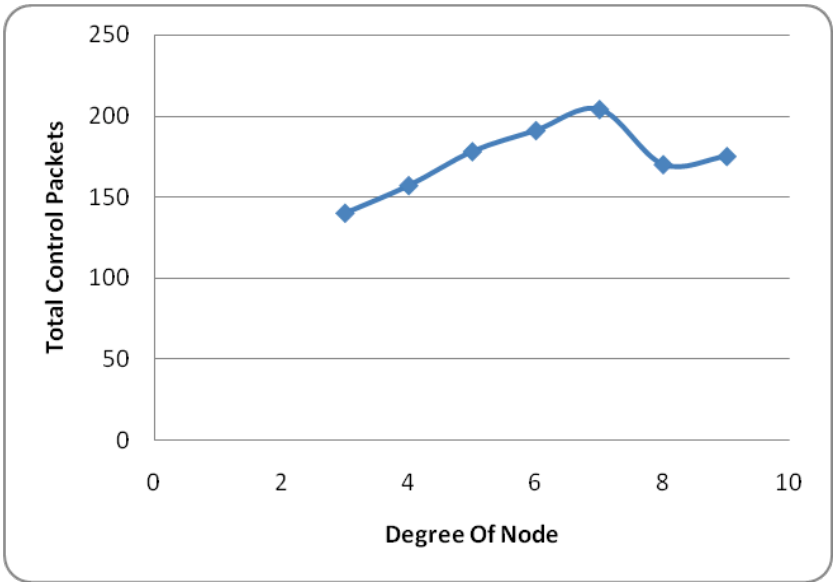


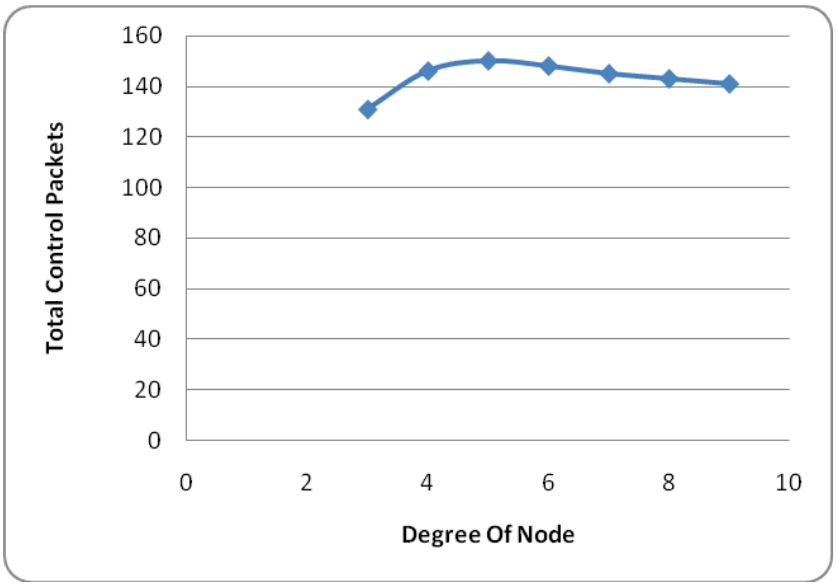


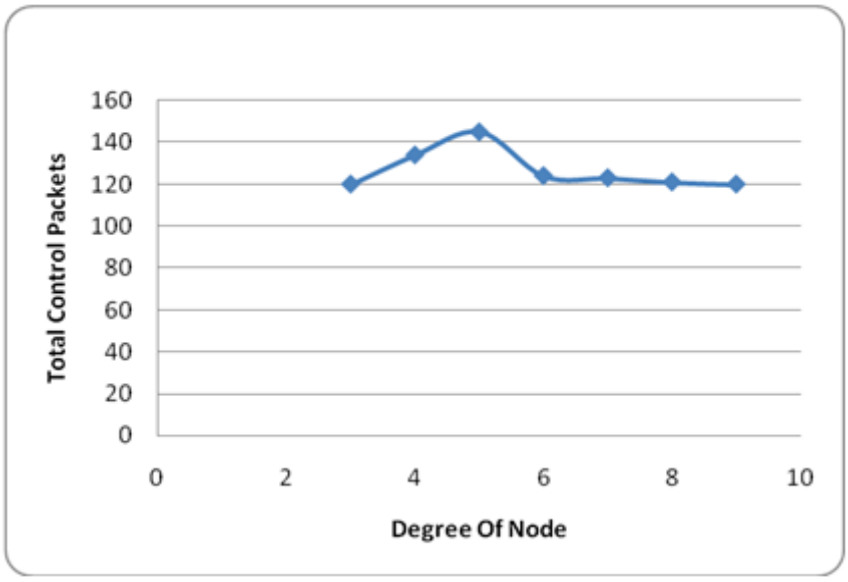
a) Mobility 8 ms.
b) Mobility 2.78 ms.
c) Mobility: none.
Figure 4.2: Packet Delivery Ratio of AODV.

4.5.2 Case 2

In this scenario we compare the total control traffic generated i.e. total of RREQ, RREP and RERR with different degrees of node. In figure 4.2 we have illustrated the variation of control traffic with different mobility patterns. It is seen that the total control packets generated is less at optimal node degree of six. However, the optimality shift towards the right as the mobility increases. The graph also shows that at higher densities the total number of control packets tend to be linear as the networks get saturated the total number of control packets generated also remains the same.







a) Mobility 8 ms.
b) Mobility 2.78 ms.
c) Mobility:none.

Figure 4.3: Total Control Packets generated by AODV Protocol

From the above two cases, we observe that for optimal performance of the ad hoc sensor network the degree of the node changes. We have observed that for stationary networks the degree of the node is 5. For higher mobility networks the degree of the node moved towards 8 and in between for less mobile networks. As packet delivery ratio and control packets are the basic criteria for measuring the performance of ad hoc sensor networks, we can prove that the degree of node plays a vital role in saving energy in sensor networks which have a limited infrastructure.

We have generalized the result based on the observation that packet delivery ratio is high at higher mobility and total control packets generated is less at higher mobility. The reason being at higher mobility the packet delivery ratio is high and due to more availability of routes the control traffic generated is less.

CHAPTER 5

Conclusions and Future Work

The Ad hoc networks are becoming popular nowadays and are slowly being used in the day to day life apart from military applications. As the demand keeps rising, it is crucial that we take into consideration optimal performance of the protocol. The parameter degree of a node is vital information in calculating the optimal performance of the network.

In this thesis we have proposed optimal node degree estimation for ad hoc networks. We used on demand distance vector protocol AODV for our analysis. We have considered two parameters total control packets and packet delivery ratio for estimating the optimal node degree for the network. We have proved that for optimal performance the degree of separation varies from 5 to 8 based on the mobility and load on the network. The degree of the node seems to shift towards the right as the mobility of the node increases. Although this can be generalized for any algorithm, the optimum level may change for reactive protocols. Also we need more simulation to be more precise regarding the optimum degree of the node. Also we have done the simulations in free space, which is not ideally the case when it comes to real world as we have to take into consideration terrain and atmospheric conditions. These factors may affect the performance and connectivity of the network.

REFERENCES

LIST OF REFERENCES

[1] Perkins, C., and Bhagwat, P., "Highly Dynamic Destination Sequenced Distance Vector Routing for Mobile Computers," Proceedings of the SIGCOMM '94 Conference on Communication Architectures, Protocols and Applications 1994, pp. 234-244.

[2] Johnson, DB., And Maltz, DA., "Dynamic Source Routing in Ad-Hoc Wireless Networking, Mobile Computing," Kluwer Academic Publishing: New York, 1996.

[3] Perkins, V., Samir, R., and Royer,E., "Ad-hoc On Demand Distance Vector (AODV) Routing," RFC 3561.

[4] Chakeres, D., and Royer,E., "The utility of hello messages for determining link connectivity," in Proceedings of the 5th International Symposium on Wireless Personal Multimedia Communications (WPMC), Honolulu, Hawaii, October 2002.

[5] Henrik, L., Erik N., and Christian T., "Coping with communication gray zones in IEEE 802.11b based ad hoc networks," in Proceedings of the 5th ACM international Workshop on Wireless Mobile Multimedia, Atlanta, GA, September 2002, pp. 49–55.

[6] Litjens, R., Roijers, R., van den Berg, J.L., Boucherie, R.J., Fleuren, M.J., "Analysis of flow transfer times," in IEEE 802.11 wireless lans. Annals of Telecommunications Vol. 59, 2004, pp 1407–1432.

[7] Ieee std 802.11e - 2005, 'part 11: 'Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications. Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. amendment to IEEE 802.11 std, 2005.

[8] Corson, MS., and Ephremides A., "A Distributed Routing Algorithm for Mobile Wireless Networks," ACM Baltzer Wireless Networks Journal, Vol. 1, No. 1,1995, pp: 61-81.

[9] Huitema,C., Routing in the Internet, second edition Prentice Hall PTR,NJ, January 2000.

[10] Thomas, SA., "IP Switching and Routing Essentials: Understanding RIP, OSPF, BGP, MPLS, CR-LDP, and RSVP-TE". Wiley Computer Publishing, December 2001.

[11] Ford, LR., and Fulkerson DR., Flows in Network, Princeton University Press: Princeton, NJ, 1962.

[12] Murthy, S., and Garcia-Luna-Aceves JJ., "Loop-free Internet Routing Using Hierarchical Routing Trees," Proceedings of the IEEE INFOCOM, 1997, pp : 101-108.

[13] Iwata A., Chiang CC., Pei G., Gerla M., and Chen TW. "Scalable Routing Strategies for Ad hoc Wireless Networks," IEEE Journal on Selected Areas in Communications, Special Issue on Wireless Ad hoc Networks, 1999, Vol. 17, No. 8, pp: 1369-1379.

[14] Murthy, S., and Gracia-Luna-Aceves JJ., "An Efficient Routing Protocol for Wireless Networks," ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communications Networks, 1996, pp: 183-197.

[15] Peralman, MR., and Haas, ZJ., "Determining the Optimal Configuration for the Zone Routing Protocol," IEEE Journal on Selected Areas in Communications, Special Issue on Wireless Adhoc Networks, 1999, Vol. 17, No. 8, pp:1395-1414.

[16] Feeney, L., "An energy consumption model for performance analysis of Routing Protocols for Mobile ad-hoc networks,", presented at IETF Manet, July 1999.

[17] Perkins, C., Bhagawat,P., " Highly Dynamic Destination-Sequenced Distance Vector (DTDV) for Mobile Computers," Proc of the SIGCOMM 1994 Conference on Communications Architectures, Protocols and Applications, Aug 1994, pp: 234-244.

[18] David, B., David, A., Maltz and Yih-Chun Hu, IETF Internet-Draft <draft-ietf-manet-dsr-09.txt>

[19] Bollobas, B., Modern Graph Theory. Springer-Verlag New York, 1998.

[20] Newman, M. E. J., Strogatz, S.H., and Watts, D.J. "Random graphs with arbitrary degree distributions and their applications," Physical Review E, vol. 64, 026118, July 2001.

[21] Dan,Yu., Hui, L., and Ingo, A.G., "Path Availability in Ad Hoc Network," ICM N PG SP RC FR Gustav-Heinemann-Ring.

[22] McDonald, A.B., and Znati, T., "A Path Availability Model for Wireless Ad-Hoc Networks," In Proceedings of IEEE WirelessCommunications and Networking Conference (WCNC) 1999.

[23] Hekmat, R., Mieghem, P.V., "Degree Distribution and Hopcount in Wireless Ad-hoc Networks," The 11th IEEE International Conferenceon Networks (ICON), 2003, pp. 603-609.

[24] Namuduri, K., and Pendse, R., "An Analytical Framework for Estimating the Control Traffic Generated by On-Demand Routing Protocols in Ad-hoc Wireless Networks", IEE VTC 2005.

[25] Global Mobile Information Systems Simulation Library. URL: http://pcl.cs.ucla.edu/projects/glomosim/ (cited May 2009).

[26] Bagrodia,R., “PARSEC: A Parallel Simulation Environment for Complex Systems,” IEEE Computer, Vol. 31, No. 10, October 1998, pp:77-85.

[27] Martin, J., “Tutorial on GloMoSim Simulation Environment for Networks”, PARSEC Workshop’99. URL: http://pcl.cs.ucla.edu/slides/workshop99/Jaytut-pw99/index.htm (cited May 2009).

APPENDIX

APPENDIX A

RESULTS

Degree	Delivery Ratio
3	0.3
4	0.31
5	0.33
6	0.35
7	0.36
8	0.37
9	0.34

Table A. 1 Packet Delivery, Ratio mobility: 8ms Case 1

Degree	Delivery Ratio
3	0.35
4	0.36
5	0.38
6	0.4
7	0.36
8	0.35
9	0.34

Table A. 2 Packet Delivery Ratio mobility: none Case 1

Degree	Delivery Ratio
3	0.32
4	0.32
5	0.33
6	0.36
7	0.37
8	0.34
9	0.32

Table A. 2 Packet Delivery Ratio mobility: 2.78ms Case 1

Degree	Total control Packets
3	140
4	157
5	178
6	191
7	204
8	170
9	175

Table A. 3 Total Control Packets, mobility: 8ms Case 2

Degree	Total control Packets
3	120
4	134
5	145
6	124
7	123
8	121
9	120

Table A. 2 Total Control Packets, mobility: none Case 2

Degree	Total control Packets
3	131
4	146
5	150
6	148
7	145
8	143
9	141

Table A. 4 Total Control Packets, mobility: 2.78ms Case 2