Chapter One

Introduction

1.1 Background

In mobile ad-hoc networks, communications are done over wireless media between stations directly in a peer-to-peer fashion without the help of wired base station or access points. There are many applications for MANET like Tactical networks, Emergency services, Commercial and civilian, Home and enterprise and education [1] for more details about these applications see section 2.4.

The ad-hoc On Demand Distance Vector (AODV) [1] routing protocol is designed for use in ad-hoc mobile networks, It is simple, efficient and effective routing protocol having wide applications. There are other famous routing protocols like Dynamic Source Routing (DSR) DSR is a reactive protocol it doesn’t use periodic advertisements. It computes the routes when necessary and then maintains them [2] .Optimized Link State Routing protocol (OLSR), is a proactive routing protocol it has an advantage of having the routes immediately available needed [2]. Zone Routing Protocol (ZRP) It effectively combines the advantages of both proactive and reactive routing protocols. The key concept used in this protocol is to use a proactive routing within a zone in the r-hop neighborhood of every node and use a reactive routing for nodes outside this zone [3] read section 2.6.7 for more details about ZRP. The AODV routing protocol has been chosen in this study due to its characteristics, which will be discussed in more detail in chapter 2.

As mentioned, there are many applications for MANET this study is focused on the virtual classroom environment application, which is a real time application. The virtual classroom application is widely used in universities [1] inside the classroom students try to access the applications in the main computer, these applications may be video, audio or text. Sometimes in the virtual classroom when more than one student try to access the main node at the same time, some of students are losing the connection with the main node, this is lead to decrease the student's productivity and waste time.

Quality of Service (QoS) in ad hoc networks become more and more required because more and more real time applications are implemented on the network. Many revisions are done to the traditional AODV protocol to meet QoS challenges focused on pause time, end-to-end delay, speed moving, and energy and mechanism overheads [4].

1.2 Problem Statement

In virtual classroom environment more than one users try to access the main node concurrently, some of these trials have failed. This is lead to adverse impact on performance of AODV routing protocol and decrease student's productivity. Thus, a mechanism to balance between the number of students and their corresponding acceptable QoS is needed.

1.3 Research Question

How can we provide set of recommendations to optimize the configuration parameters of MANET node in an adaptive manner according to the traffic load?

1.4 Aim and Objectives

The aim of this thesis work is to:

- Propose a simulation environment for virtual class-room to study the behavior of the AODV.
- Performance evaluation of AODV routing protocol.
- Optimization the performance of AODV routing protocol by adjusting the best values of the quality of service metrics like data rate, packet size and queue size.

The outcomes of the above-mentioned objectives to make decision about the optimum values of data rate, packet size and queue size in AODV. To be considered as an adaptive set of recommendations according to the network load and the expected QoS.

1.5 Methodology

This thesis work is based on the literature research method relying on the materials listed in the references. In addition, the approach used in case study is to do simulations. The simulation is done using NS2. In this study, the data of performance metrics is collected from a sample of small virtual classroom contains 25 students within an area of 50m*50m, from the collected data , several parameters have been considers such as data rate, packet size and queue size furthermore their effect on packet loss , packet delivery fraction , delay, jitter and throughput.

The aim of this study is to evaluation and optimization the performance of AODV. The focus will be on study the effect of data rate, packet size and queue size on the packet loss , packet delivery fraction , delay, jitter and throughput when more than one computer try to access the same computer . AODV is reactive routing protocol. It is simple, efficient and effective routing protocol having wide applications. The topology of the network in AODV gets change time to time so dealing with same and as well as maintaining the PDF, Packet Loss ,delay, jitter, and throughput is great challenge. Many revisions are done to the traditional AODV protocol to meet QoS challenges focused on pause time, end-to-end delay, speed moving, energy and mechanism overheads, for more details about related work read chapter three .

1.6 Scope of the Research

With the popularity of ad hoc networks, many routing protocols have been designed for route discovery and route maintenance. They are mostly designed for best effort transmission without any guarantee of quality of transmissions. Some of the most famous routing protocols are Dynamic Source Routing (DSR) Ad hoc On Demand Vector (AODV) Optimized Link State Routing protocol (OLSR), and Zone Routing Protocol (ZRP). In MAC layer, one of the most popular solutions is IEEE 802.11 [5]. In this research, the following topics have been discussed. A study of AODV routing protocol , performance evaluation of AODV protocol , evaluation of performance according to the workload of the network and propose set of recommendation to optimize the usage of virtual classroom environment .

1.7 Thesis Outlines

Chapter one gives the scope and the aim of this thesis work outline of the thesis is described.

Chapter two introduces the physical and MAC layer standards in addition to the routing protocols that are used in ad hoc networks , also it presents what QoS is and how QoS aware routing protocols can be achieved.

Chapter three explores the research methodology, the plan of the research is discussed.

In chapter four, the simulation tool called NS2 is introduced, and some scenarios based on AODV routing protocol are simulated. The performance results in AODV are compared and analyzed.

Chapter five concludes the thesis and gives some suggestions for future works.

Chapter Two

Literature Review

2.1 Overview of Mobile Ad-hoc Networks

This chapter gives an overview of mobile ad hoc networks. The history and the applications will be summarized first. After that, IEEE 802.15.4 protocol will be discussed in detail. Finally, various routing protocols developed for ad hoc networks are discussed and compared.

2.2 History of Mobile Ad- hoc Networks

“A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose"”[6].

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

Mobile Ad-Hoc Network (MANET) is a recent developed part of wireless communication. The difference to traditional wireless networks is that there is no need for established infrastructure. Since there is no such infrastructure and therefore no preinstalled routers, which can, for example, forward packets from one host to another, this task has to be take each of those nodes take equal roles, what means that all of them can operate as a host and as a router. Next to the problems of traditional wireless networks such as security, power control, transmission quality

and bandwidth optimization, new problems come up in Ad-Hoc networks.

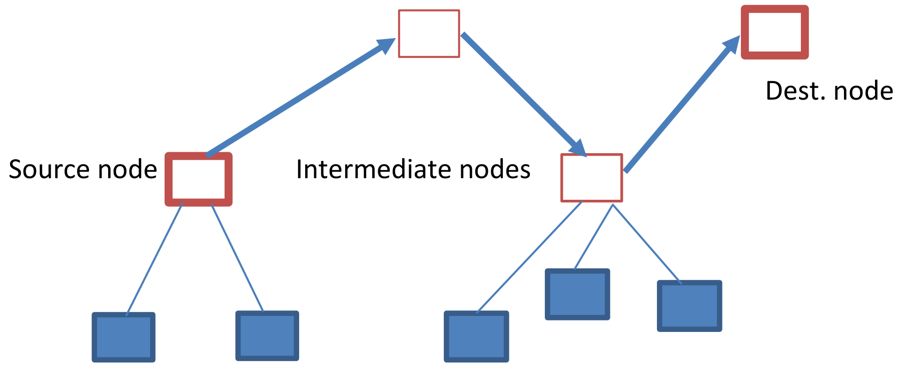


Figure 2-1: LAN Network

Figures 2-1, 2-2 and 2-3 show examples for an infrastructure, a wireless and a Ad-hoc network respectively.

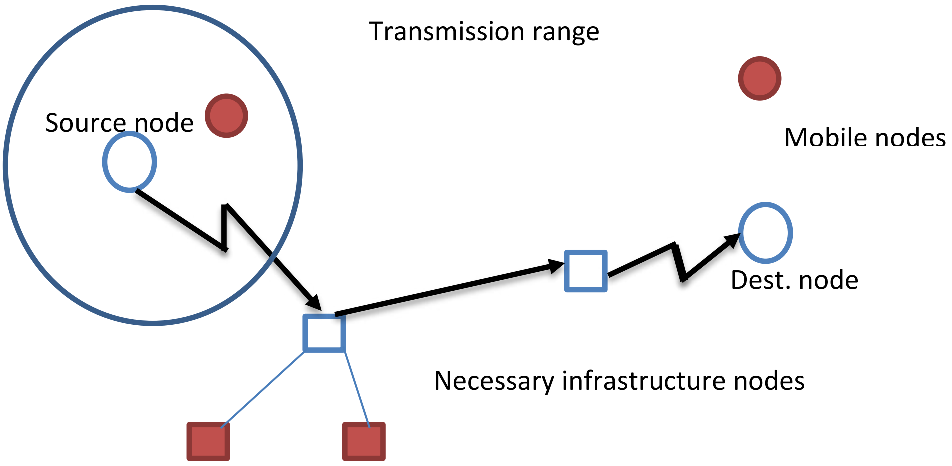


Figure 2-2: wireless network

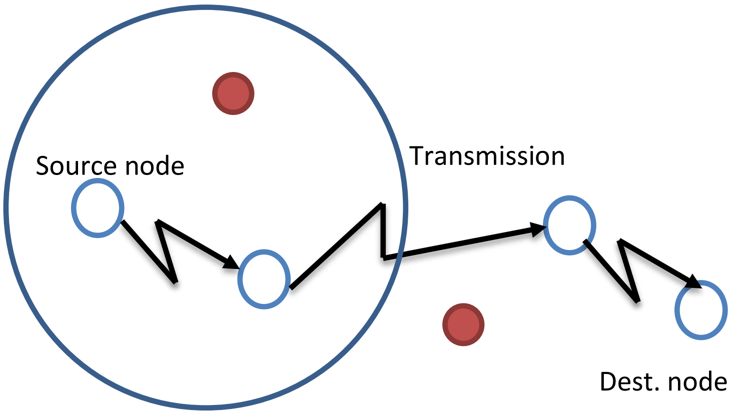


Figure 2-3: MANET network

2.3 Characteristics of Mobile Ad-hoc Network

• **Nodes** – All the nodes in a mobile Ad-Hoc network, regardless of their position, can communicate with other nodes with the same priority. Since there is no infrastructure, there is a need, in order to let distant nodes communicate with each other, of nodes in the network who take over the position of a router.

•**Loss rate and delay** – The communication medium of wireless networks, electromagnetic waves, encounter during their propagation many interference coming from objects which are in the propagation way of the waves or from other transmitting wireless devices. Therefore, we have in MANETs a higher loss rate and delay than in wired networks.

•**Topology** – Since the nodes in an Ad-Hoc network are mobile, the chance of frequent changes in the topology of the network is high. Algorithms for Ad-Hoc networks have to consider these topological changes.

• **Security** – Because the computer communicate over the air, every node, equipped with the necessary utilities, inside the transmitting area of a sending node, can receive the sent messages. For this reason wireless network are less secure than wired ones.

• **Capacity** – At the moment is the amount of data which a link of a wireless network is able to transmit per unit of time smaller than the one of a wired network.

2.4 Mobile Ad-hoc Network Applications

There are many applications for MANET like tactical networks, which is applied in military communication and operations and in automated battlefields. Emergency services which is applied in search and rescue operations , disaster recovery , replacement of fixed infrastructure in case of environmental disasters, policing and firefighting, supporting doctors and nurses in hospitals.

Commercial and civilian application, which is applied in e-commerce electronic payments anytime and anywhere Environments. Business: dynamic database access, mobile offices. Vehicular services: road or accident guidance, transmission of road and weather conditions, taxi cab network, inter-vehicle networks. Sports stadiums, trade fairs, shopping malls. Networks of visitors at airports.

Home and enterprise application which is used in Home/office wireless networking ,conferences, meeting rooms, personal area networks (PAN), Personal networks (PN) , networks at construction sites. Education application which is used in universities and campus settings , virtual classrooms Ad- hoc communications during meetings or lectures [1].

2.5 IEEE 802.11 Standard

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication. With the popularity of IEEE 802.11 standard family used in laptops, and Personal Digital Assistants (PDAs), this standard is considered one of the solutions used in ad hoc networks.

Especially in the simulations, IEEE 802.11 standard is used in ad hoc networks by most of the people [5].

2.5.1 IEEE 802 Families

IEEE 802 refers to a family of IEEE standards dealing with local area networks and metropolitan area networks .IEEE 802 specifications are focus on the data link layer and physical layer of the Open System Interconnection (OSI) reference model. Some of the main family members of IEEE 802 are listed in Table 2-1[7].

Table 2-1: IEEE 802 families

IEEE Standard	Network Definition	Known As
802.3	wired Local Area Network	Ethernet
802.11	Wireless Local Area Network (WLAN)	Wi FI
802.15.1	Wireless personal Area Network (WPAN)	Bluetooth
802.15.4	Low Rate-Wireless Personal Area Network (LR-WPAN)	ZigBee
802.16	Wireless metropolitan area network (WMAN)	Wi Max
802.20	Mobile Broadband wireless Access (MBWA)	

2.5.2 Components of the IEEE 802.15.4

A system conforming to IEEE 802.15.4 consists of several components. The most basic is the device. A device can be an RFD or an FFD. Two or more devices within a POS communicating on the same physical channel constitute a WPAN. However, a network shall include at least one FFD, operating as the PAN coordinator**.**

An IEEE 802.15.4 network is part of the WPAN family of standards although the coverage of an LR-WPAN may extend beyond the POS, which typically defines the WPAN.

A well-defined coverage area does not exist for wireless media because propagation characteristics are dynamic and uncertain. Small changes in position or direction may result in drastic differences in the signal strength or quality of the communication link. These effects occur whether a device is stationary or mobile as moving objects may impact station-to-station propagation [5].

2.5.3 IEEE 802.15.4 Architecture

The LR-WPAN architecture is defined in terms of a number of blocks in order to simplify the standard. These blocks are called layers. Each layer is responsible for one part of the standard and offers services to the higher layers. The layout of the blocks is based on the open systems interconnection (OSI) seven-layer mode. The interfaces between the layers serve to define the logical links that are described in this standard. An LR-WPAN device comprises a PHY, which contains the radio frequency (RF) transceiver along with its low-level control mechanism, and a MAC sub layer that provides access to the physical channel for all types of transfer. Figure 2.4 shows these blocks in a graphical representation. The upper layers, shown in Figure, consist of a network layer, which provides network configuration, manipulation, and message routing, and an application layer, which provides the intended function of the device. The definition of these upper layers is outside the scope of this standard. An IEEE 802.2™ Type1 logical link control (LLC) can access the MAC sublayer through the service specific convergence sublayer (SSCS), defined in Annex A. The LR-WPAN architecture can be implemented either as embedded devices or as devices requiring the support of an external device such as a PC [5].

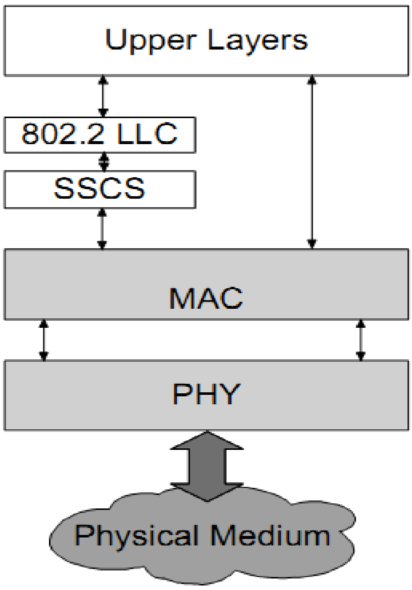


Figure 2-4: IEEE 802.15.4

2.6 Routing protocols in Ad hoc Wireless Networks

Routing Protocol is needed whenever a packet needs to be transmitted to a destination via number of nodes. The routing protocols for wired networks cannot be used for mobile ad hoc networks because of the mobility of networks. The ad hoc routing protocols can be divided into two classes table-driven (proactive), On-demand (reactive) and hybrid routing protocol as shown in Figure 2-5.

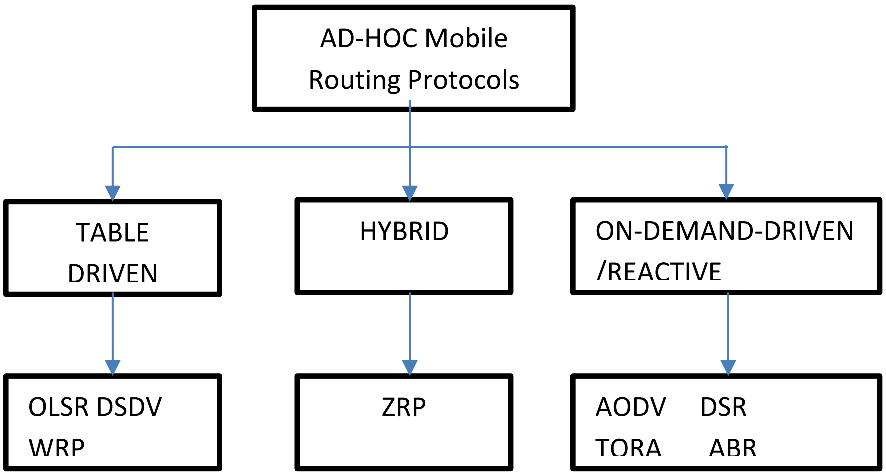


Figure 2-5: Routing protocol in ad hoc network

In addition, protocols can also be classified according to the utilization of specific resources, such as power aware routing protocol and load aware routing protocols and so on [22].

2.6.1 Proactive Routing Protocols

In Proactive or Table-Driven Routing Protocols, each node continuously maintains up-to-date routes to every other node in the network. Routing information is periodically transmitted throughout the network in order to maintain routing table consistency. Once, there is a need of transmission, source node could check from the routing table, the route will be get immediately. Some of the used proactive routing protocols used in ad hoc networks are Optimized Link State Routing protocol (OLSR), Destination Sequenced Distance-Vector routing protocol (DSDV), and Wireless Routing Protocol (WRP) [23].

2.6.2 Open Shortest Path First routing protocol in Internet

The OSPF routing protocol is the most important link state routing protocol on the Internet. Open Shortest Path First (OSPF) protocol is a link state protocol that handles routing for IP traffic. It is based on Dijkstraís Shortest-Path-First (SPF) algorithm. Routers in the interior network send Link State Advertisements (LSAs) to all the other routers within the same hierarchical area. LSAs received from other routers are saved in a link state database. That is, the link state database of the router includes all the link information received from others. Routing table is calculated by using the information in the link state database as shown in Figure 2-6 [24].

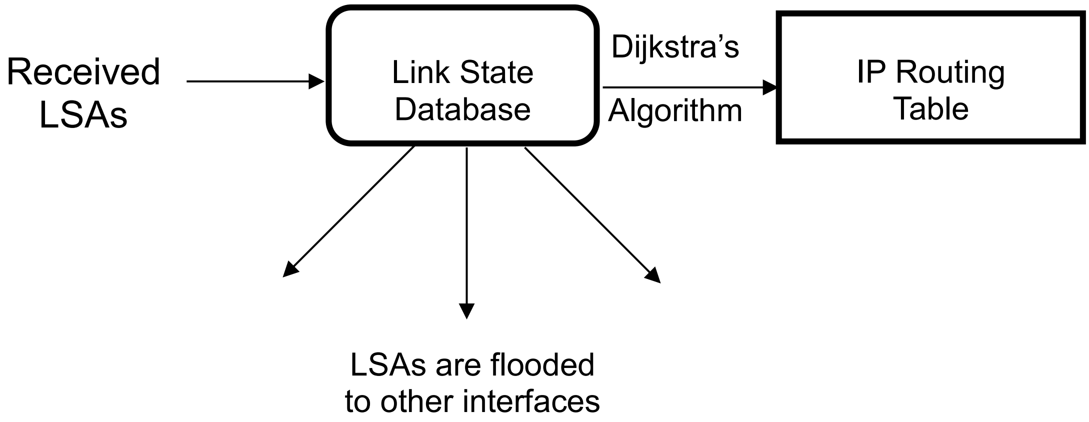


Figure 2-6: Operation of a Link State Routing protocol

OSPF has three sub-protocols named Hello protocol, Exchange protocol and Flooding protocol. The Hello protocol ensures links working by exchange Hello messages with its neighbors during the last Hello interval. The designated router (used in broadcasting) and backup designated router are also selected by Hello protocol. The exchange protocol initially synchronizes link database with the designated protocols also give some basic idea of how QoS aware routing protocol could be achieved based on the existing routing protocol. Flooding protocol continuously maintains the link database integrity of the area[24].

Extended protocol for OSPF is QOSPF (Quality of Service Open Shortest Path First) In order to increase the QoS to satisfy the need of real-time traffic, e.g. video conference, streaming video/audio, QoS aware routing protocols are considered for Internet. The first considered metric is available data rate.

Generally speaking, the routing algorithm is to find a path, which could use the minimum hop-count with satisfaction of the data rate and delay requirements. In other words, the aim is to find the feasible path with the cost of minimal amount of recourse. The difficulty of OSPF is that all nodes need to have a consistent view of the network [24].

2.6.3 Reactive Routing Protocols

In Reactive Protocols, a node initiates a route discovery throughout the network, only when it wants to send packets to its destination. For this purpose, a node initiates a route discovery process through the network. It costs too much data rate to transmit the topology Information. The main advantage of the using on demand routing protocols is to reduce the routing overhead in order to save bandwidth in ad hoc networks. Some Reactive Protocols are Cluster Based Routing Protocol (CBRP), AODV, DSR, TORA, Associativity-Based Routing (ABR), Signal Stability Routing (SSR) and Location Aided Routing (LAR)[23].

2.6.4 Ad Hoc On-Demand Distance Vector Routing Protocol

AODV routing protocol is another on demand routing protocol. Routes are established when they are required. Not like in DSR (Dynamic Source Routing) that stations have all the route information in the routing table, in the routing table of AODV, the station only has the information of the next hop and destination pair. Route discovery and maintenance processes in AODV routing protocol will be discussed as follows.

AODV defines 3 message types:

– Route Requests (RREQs).

– Route Replies (RREPs).

– Route Errors (RERRs).

• RREQ messages are used to initiate the route finding process.

• RREP messages are used to finalize the routes.

• RERR messages are used to notify the network of a link breakage in an active route.

2.6.5 Route Discovery Generate RREQs

When a node wishes to send a packet to some destination It checks its routing table to determine if it has a current route to the destination If Yes, forwards the packet to next hop node If No, it initiates a route discovery process. Route discovery process begins with the creation of a Route Request (RREQ) packet source node creates it. The packet contains source node's IP address, source node's current sequence number, destination IP address, and destination sequence number. Packet also contains broadcast ID number. Broadcast ID gets incremented each time a source node uses RREQ. Broadcast ID and source IP address form a unique identifier for the RREQ. Broadcasting is done via Flooding.

Once an intermediate node receives a RREQ, the node sets up a reverse route entry for the source node in its route table. Reverse route entry consists of Source IP address, Source seq. number, number of hops to source node, IP address of node from which RREQ was received. Using the reverse route a node can send a RREP (Route Reply packet) to the source. Reverse route entry also contains lifetime field. RREQ reaches destination In order to respond to RREQ a node should have in its route table unexpired entry for the destination and seq. number of destination at least as great as in RREQ (for loop prevention)[8].

- **RREQ reaches destination:**

If both conditions are met & the IP address of the destination matches with that in RREQ the node responds to RREQ by sending a RREP back using unicasting and not flooding to the source using reverse path. If conditions are not satisfied, then node increments the hop count in RREQ and broadcasts to its neighbors. Ultimately, the RREQ will make to the destination[8].

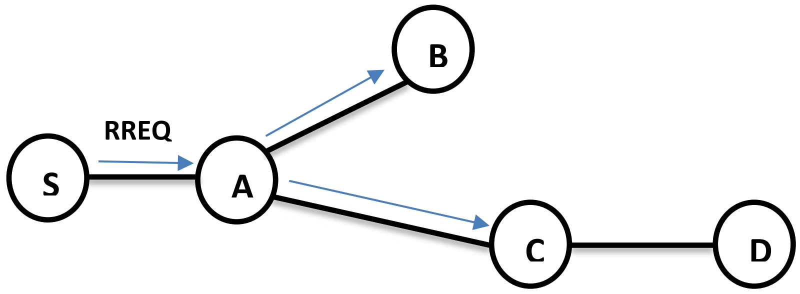


Figure 2-7: Route Discovery - RREQ

In Figure 2-7 node S needs a route to D and creates a Route Request (RREQ) enters D's IP addr, seq#, S's IP addr, seq#, hopcount (=0). Node S broadcasts RREQ to neighbors. Node A receives RREQ and makes a reverse route entery for S dest=S, nexthop=S, hopcount=1. It has no routes to D, so it rebroadcasts RREQ. Node C receives RREQ makes a reverse route entry for S dest=S, nexthop=A, hopcount=2 It has a route to D, and the seq# for route to D is D's seq# in RREQ. C creates a Route Reply (RREP) Enters D's IP addr, seq#, S's IP addr, hopcount to D (=1) and unicasts RREP to A [8].

- **Receives RREP**

Node A receives RREP Figure 2-8 makes a forward route entry to D dest=D, nexthop=C, hopcount=2 and unicasts RREP to S.

When a node determines that it has a current route to respond to RREQ i.e. has a path to destination it creates RREP (Route Reply). RREP contains <IP address of source and destination>.If RREP is being sent by destination it will also contain the <current sqn # of destination, hop-count=0, life-time>. If RREP is sent by an intermediate node it will contain its record of the <destination sequence number, hop-count=its distance to destination, its value of the life-time>.

When an intermediate node receives the RREP, it sets up a forward path entry to the destination in its route table. Forward path entry contains<IP Address of destination, IP address of node from which the entry arrived, hop-count to destination, life-time>. To obtain its distance to destination i.e. hop-count, a node increments its distance by 1 if route is not used within the life time, its deleted. After processing the RREP, the node forwards it towards the source[8].

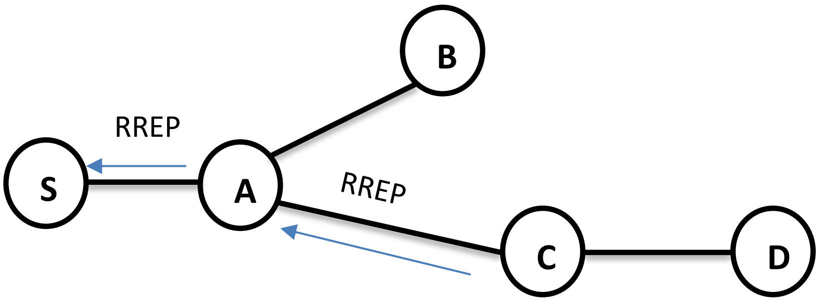


Figure 2-8: Route Discovery - RREP

Node S receives RREP Makes a forward route entry to D dest=D, nexthop =A, hopcount = 3. A node may receive multiple RREP for a given destination from more than one neighbor. The node only forwards the first RREP it receives may forward another RREP if that has greater destination sequence number or a smaller hop count. Rest are discarded reduces the number of RREP propagating towards the source. Source can begin data transmission upon receiving the first RREP.

- **Data Delivery:**

Node S receives RREP Makes a forward route entry to D dest=D, nexthop =A, hopcount = 3 sends data packet on route to D

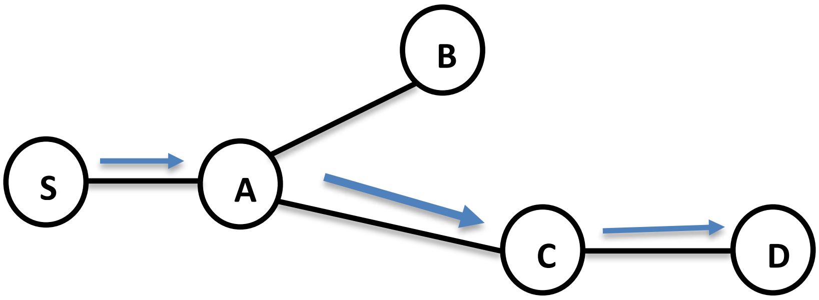


Figure 2-9: Data delivery

- **Timeouts**

A routing table entry maintaining a reverse path is purged after a timeout interval, timeout should be long enough to allow RREP to come back. A routing table entry maintaining a forward path is purged if not used for a active_route_timeout interval. If no is data being sent using a particular routing table entry, that entry will be deleted from the routing table (even if the route may actually still be valid)

- **Link Failure Reporting**

A neighbor of node X is considered active for a routing table entry if the neighbor sent a packet within active_route_timeout interval and was forwarded using that entry. If a source node moves, a new route discovery process is initiated. If intermediate nodes or the destination move The next hop links break resulting in link failures. Routing tables are updated for the link failures. All active neighbors are informed by RERR message.

- **Route Maintenance - RERR**

RERR is initiated by the node upstream (closer to the source) of the break. Its propagated to all the affected destinations. RERR lists all the nodes affected by the link failure Nodes that were using the link to route messages (precursor nodes). When a node receives an RERR, it marks its route to the destination as invalid setting distance to the destination as infinity in the route table. When a source node receives an RRER, it can reinitiate the route discovery.

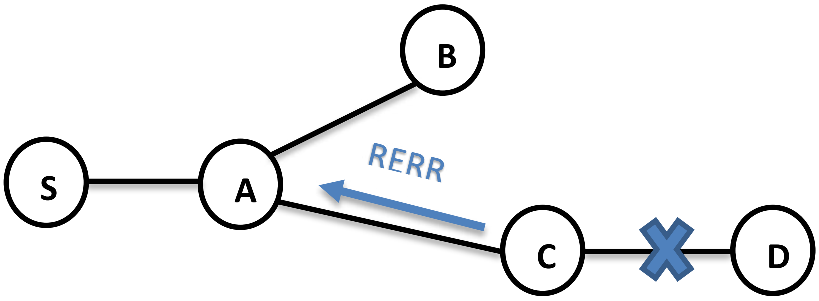


Figure 2-10: Route maintenance

Link between C and D breaks Figure 2-10 . Node C invalidates route to D in route table and C creates Route Error message lists all destinations that are now unreachable sends to upstream neighbors. Also node A receives RERR checks whether C is its next hop on route to D and deletes route to D (makes distance infinity) then forwards RERR to S. finally node S receives RERR checks whether A is its next hop on route to D, deletes route to D and rediscovers route if still needed.

- **Route Error :**

When node X is unable to forward packet P (from node S to node D) on link (X,Y), it generates a RERR message. Node X increments the destination sequence number for D cached at node X. The incremented sequence number N is included in the RERR. When node S receives the RERR, it initiates a new route discovery for D using destination sequence number at least as large as N.

- **Optimizations**

Route Requests are initially sent with small Time-to-Live (TTL) field, to limit their propagation. DSR also includes a similar optimization. If no Route Reply is received, then larger TTL tried

AODV Optimizations

- ➢ Expanding Ring Search,

- Prevents flooding of network during route discovery.
- Control Time to Live (TTL) of RREQ to search incrementally larger areas of network.
- Advantages: Less overhead when successful.
- Disadvantages: Longer delay if route not found immediately.

- ➢ Local Repairs

- Repair breaks in active routes locally instead of notifying source.
- Use small TTL because destination probably hasn’t moved far
- If first repair attempt is unsuccessful, send RERR to source.
- Advantage: repair links with less overhead delay and packet loss.
- Disadvantages: longer delay and greater packet loss when unsuccessful.

2.6.6 Comparison between DSR and AODV routing protocols

There are a few differences between DSR and AODV routing protocols. Firstly, compared with DSR, the source node of AODV only knows the route to the destination, but in DSR, source node knows the route to intermediate node also. On the other hand, because in DSR, each data packet has to take the whole route information in the header, it costs large overhead, which will waste data rate. Another difference between DSR and AODV is the usage of timer. In the DSR protocol, there is no timer used for the validation of routes. Stale routes could be used for routing. In AODV, timer is used for the freshness of a route. In DSR, with stale route, it is possible that the route is not validated. It will cause the loss the packets before source node is notified that the route is invalid. On the other hand, if the route is still valid, route overhead is saved for route discovery process.

In AODV, route which has not been used for a period of expire time will be deleted. The set of expire time is important since short expire time may lead to the deletion of still valid route and long expire time will give more non-fresh routes.

Thirdly, it is about RREP. The destination of DSR could send RREQ more than once for the same RREQ without considering whether the same RREQ had been replied just a second ago for other routes. In addition, multiple route entry could be store in the route table for the same destination in the same source node. That is, a source node has multiple route entries for one destination. While, in AODV, only one route reply can be sent by the destination and only one route entry per destination is stored in the route table.

The advantage of having more than one route entry per destination is that it can provide backup routes when there is a break on the current route. It means that there is no need to send a RREQ again to search for the route. On the other side, if the network has high mobility, the freshness of the backup route could be a problem and reinitiate a new RREQ should be a better choice. With the above analysis, it is found that AODV protocol should perform better in high mobility ad hoc network [8].

2.6.7 Hybrid routing protocol-Zone Routing Protocol

Zone Routing Protocol (ZRP) is a hybrid routing protocol. It effectively combines the advantages of both proactive and reactive routing protocols. The key concept used in this protocol is to use a proactive routing within a zone in the r-hop neighborhood of every node and use a reactive routing for nodes outside this zone. The table driven scope is limited within a zone and when a destination is out of the table driven scope, on demand routing search is initiated. In this situation, control overhead is reduced, compared to both the route request flooding mechanism employed in on demand protocols and periodic flooding of outing information packet in table driven protocol[3].

2.7 QoS-Aware Ruting Protocols In Ad- hoc Networks

In this chapter, general concepts of QoS are introduced first. It includes the QoS definition, QoS parameters, the aim of QoS in different layers and systems, and the existing model for QoS. Since, in this thesis, the QoS is mainly discussed aiming at real time traffics, the difference between real time traffic and non-real time traffic are compared to show the need of QoS for real time services. After that, challenges of achieving QoS in ad hoc networks are presented. The generally used parameters in the routing layer of ad hoc network are shown. The most important part in this chapter is the summarization of the calculation of metrics, including delay and data rate. The detailed steps of computing the available data rate of nodes with different methods are given. Finally, two QoS aware routing protocols for ad hoc network are introduced.

2.7.1 Definition of QoS

Quality of Service is the performance level of a service offered by the network to the user. In the originally used network model, traffic is transmitted only with best effort. It means that there is no quality guarantee for each transmission. When with the real-time traffic is transmitted in the network, QoS becomes demanding. In addition, because of the limitation of network resources especially in wireless networks, real time traffic need to be given higher priority to ensure that the real time traffic arrives the destination on time [1].

2.7.2 QoS Parameters

QoS parameters differ from application to application. For example, for multimedia applications, the data rate and delay are the key factors, whereas, in military use, security and reliability become more important. If considering QoS required by emergency cases such as rescue, the key factor should be the availability. In sensor networks, battery life and energy conservation would be the prime QoS parameters. The QoS parameter considered here is aimed to real time applications. In real time applications, QoS requests can be expressed in term of many metrics in routing protocols. The most popular metrics are data rate and delay. To satisfy QoS requirements, the corresponding available data rate and delay that could be provided by the network of each route should be calculated in order to see which route could be used with satisfying QoS. As a result, we will see how available data rate and delay are calculated.

2.7.3 Real Time Traffic vs. non Real Time Traffic

Why does real-time traffic require QoS? It is because there are some essential differences between the non-real time data and real-time data. For the transmission of non-real time data, timing is not a critical issue, the data is elastic. As a result, the non-real time network could work well without guarantee of timely delivery of data. But it always has high requirement for packet loss. Retransmissions are used if there are some lost packets. The applications of non-real time data transmissions are Telnet, FTP, E-mail and web browsing. For real time transmission like telephone, video conference, streaming video and audio, the basic requirement is to transmit packets to the destination on time. People cannot tolerate large delay for example on the phone. As a result, some QoS mechanisms are badly needed to ensure the required quality of the connection.

2.7.4 QoS in Different Layers

QoS of a network can be considered at different layers. QoS considered in physical layer means the quality in terms of transmission performance. For example, through transmission power control both the stations that are near the sender or far away from the sender could hear the signal clearly with different transmission power. Power control is used both to ensure the quality of reception and to optimize the capacity.

QoS implemented in MAC layer is also important. It could provide high probability of access with low delay when stations with higher user priority want to access the wireless medium. QoS implemented in the routing layer aims to find a route which provides the required quality. The metric which helps to choose the route is not only the number of needed hops along the route but also some other metrics like maximum delay and minimum data rate.

2.7.5 Challenge of QoS Routing in Ad- hoc Networks

Mobile ad hoc networks differ from the traditional wired networks. They have certain unique characteristics, which cause difficulties for providing QoS in such networks. The unique characteristics are dynamically varying network topology, lack of precise state information, shared radio channel, limited resource availability, hidden terminal problem and insecure medium. These characteristics and their effects on ad hoc networks will be discussed in this part one by one.

Dynamically varying network topology in mobile ad hoc networks, nodes are mobile and network topology is changing dynamically. Consequently, the route which is already set up with required QoS could not satisfy QoS anymore if one of the nodes on this established route moves. For example, a node could move to an area with more interference to it. The node whose data rate has been overused should take some actions. The information about loss of QoS should be sent by this node to all sources whose transmission is going through the overloaded node. Sources who receive this message have to find another possible route by using QoS aware routing protocol again. This procedure will cause delay, which may not be acceptable.

- Lack of precise state information

Due to the dynamic characteristic, information of nodes transmitted to other nodes may change right after this information is transmitted to its neighbors. The information here can be the data rate available at the neighboring node, since available data rate of nodes is affected by the data rate of its neighbors. As a result, this information which is already transmitted may have been out of date and it may lead to a wrong routing decision.

- Shared radio channel

Data transmitted on the radio channel can be received by stations, which are in the carrier sensing range of the transmitter. This broadcast characteristic will cause interference to other stations when traffic is transmitted over the air interface. Thus, stations have to share channel with neighbors in their carrier sensing range. This is very different from the wired channel, which will not cause that much interference between each other because of proper construction of lines that attenuates crosstalk interference significantly.

- Limited resource availability

The resources such as data rate, battery life, and storage space are all very limited in ad hoc networks. The battery life in a sensor network is a very good example. In a sensor network, each sensor has very limited battery life, so routing based on power consumption is widely considered.   The data rate is very limited for wireless links if we compared it with the data rate available in wired network. In addition, the basic characteristics of the wireless channel e.g. fading, noise, and shared data rate between neighbor nodes (neighbor nodes have to keep silent when it senses some node is transmitting) will also degrade the wireless data rate The actual radio data rate becomes much smaller. As a result, it is hard for a wireless network to provide too high data rate, which could be provided, by the wired network. It also brings problem of cooperation between wireless network and wired network.

2.7.6 Classification of Generally Used Metrics

The QoS metrics can be classified into three categories. They are additive metrics, concave metrics, and multiplicative metrics. Additive metrics is defined as sum of the value of the metric on all links along the path. Delay and jitter are additive metrics. Delay along the path is the sum of the delay at every link along the path. A concave metric means the minimum metric value over a path. Metric value on every link along the path is taken into account. The minimum metric value stands for the metric value of the whole path. Data rate is a concave metric. The minimum data rate of all the links along the path should be the data rate of this route. A multiplicative metric represents the product of the metric values on all links over a path. The criteria of reliability or availability of one link, e.g. link outage probability is a multiplicative metric. The generally used metrics for real time applications are data rate, delay, delay variance (jitter), and packet loss. Two of the most important ones are data rate and delay. They will be discussed in detail in the following sections.

2.7.7 Traffic on Wireless

Multimedia applications over wireless networks become more and more demanding with respect to Quality of Service (QoS). Type of traffic is a very important factor affecting the overall system performance. the most appropriate type of traffic for multimedia applications is continues bitrate. (CBR) is a term used in telecommunications ranging from 8kbps (Kilobits per second) to 320kbps [9] .

2.7 Related Works

The aim of this study is to evaluation and optimization the performance of AODV. The focus will be on study the effect of data rate, packet size and queue size on the packet loss, packet delivery fraction , delay, jitter and throughput when more than one computer try to access the same computer at the same time .One of the most important research in this area has done by Dr.Vijendra Rai he evaluate the AODV on parameter such as throughput , packet loss number and delay[10]. The results for throughput, packet loss number and delay shown in table 2-2, table 2-3 and 2-4 respectively.

The previous study [10] evaluates the performance of AODV by determining values of the throughput packet loss and delay when one computer sends to one computer or when two computers send to two computers or when four computers send to four computers. This thesis evaluates and optimizes the performance of AODV by calculating the value of packet loss, packet delivery fraction, delay, throughput and jitter when more than one computer send to one computer concurrently.

Table 2-2: throughput

Throughput (kbps)	Time T1 (30 sec)		Time T2 (50 sec)		Time T3 (70 sec)	
Protocol	AODV		AODV		AODV	
Number of nodes	20	30	20	30	20	30
1 Agent , 1 Sink	257.600	506.0	248.400	496.800	248.400	506.0
2 Agent , 2 Sink	110.400	230.0	128.800	82.799	128.800	55.200
3 Agent , 3 Sink		257.600	64.400	46.0	128.800	73.599
4 Agent , 4 Sink	0	82.799	73.599	110.400	55.200	147.199

Table 2-3: Packet loss (No.of packet)

Packet loss (No.of packets)	Time T1 (30 sec)		Time T2 (50 sec)		Time T3 (70 sec)	
Protocol	AODV		AODV		AODV	
Number of nodes	20	30	20	30	20	30
1 Agent , 1 Sink	35	0	15	0	35	0
2 Agent , 2 Sink	110	90	85	50	75	85
3 Agent , 3 Sink	180	35	100	5	140	120
4 Agent , 4 Sink	5135	135	140	110	70	145

Table 2-4: Delay (sec)

Delay (sec)	Time T1 (30 sec)		Time T2 (50 sec)		Time T3 (70 sec)	
Protocol	AODV		AODV		AODV	
Number of nodes	20	30	20	30	20	30
1 Agent , 1 Sink	0.0	0.00369	0.0	0.00370	0.00755	0.00364
2 Agent , 2 Sink	0.01319	0.01155	0.00951	0.03724	0.00805	0.00637
3 Agent , 3 Sink	0.01953	0.01351	0.0	0.02318	0.01204	0.00735
4 Agent , 4 Sink	0.08927	0.1809	0.02019	0.06490	0.01645	0.00839

This previous study evaluate the performance of AODV by determine values of the delay and jitter when one computer send to one computer or when two computer send to two computer or when four computers send to four computers. This thesis evaluate and optimize the performance of AODV by calculate the value of delay and jitter when more than one computer send to one computer concurrently.

Various researches have been carried out on above factors. Lalet.al.[11] Implemented new NDMP-AODV that is able to provide low end-to-end delay and high packet delivery ratio, while keeping low routing overhead. Raj Kumar G.et.al [12] evaluated the AODV and DSR on parameter such as Throughput, Delay, Network Load and Packets Drop against pause time .

They observed that AODV performs well in the presence of noise gives better throughput level with less delay, consumes less energy and less packets get drop. Maurya1et.al. [13] Compared on-demand routing protocols that is reactive and proactive routing. They observed that reactive protocol offers quick adaptation to mobile networks with low processing and low bandwidth utilization. In [14] Das et.al. two on-demand routing protocols, DSR and AODV had been compared. In future, they have studied more routing protocols such as DSDV, TORA based on parameters such as fraction of packet delivery, end-to-end delay and routing overhead.Yanget.al.

Compared the AODV, R-AODV and SR-AODV .From simulation they have concluded that SR-AODV improves the performance of AODV in most metrics, as the packet delivery ratio, end-to-end delay, and Power consumption. Yanget.al.[15]analyzed the performances of AODV and M-AODV they observed that in M-AODV route discovery succeeds in fewer tries than AODV. When the simulation is carried out, they conclude that M-AODV improves the performance of AODV in most metrics, as the packet delivery ratio, end-to-end delay, and energy consumption. Li et.al. [16] evaluated the TRP with S–AODV and it is observed that TRP improves network performance in terms of energy efficiency and average routing delay.

In [17] Thanthryet.al.th they verified the EMAODV with the AODV. The results obtained from the simulations show that EMAODV performs better than AODV in terms of throughput, number of route discoveries, control overhead and packet drops but, the average end-to-end delay of EM-AODV was found to be higher than AODV. Khelifaet.al.[18] investigated the performances of M-AODV and AODV they observed route discovery succeeds in that M-AODV improves the performance of AODV in terms of metrics, packet delivery ratio, end to end delay, and energy consumption. Furthermore they studied the implementation of Energy AODV mechanism to conserve more energy. Sharma et al. evaluated the effect of different scheduling algorithms for AODV and modified AODV. They reduce the average delay between the nodes communication. Chaurasia et.al. [19] examined on OLSR, DSDV, DSR, AODV, and TORA protocols They observed that due to the Infrastructure less structure of protocol security and power awareness is difficult to achieve in mobile ad hoc networks .In future they work on core issues of security and power consumption in these routing protocol. M.Ushaet.al. [20] implemented new advanced AODV name RE-AODV (Route-Enhanced AODV). They observed routing overhead is reduced by 25% and end to end delay of packets 11% as compared to normal AODV protocol. It has been observed in AODV routing protocol that power consumption is more which make AODV a costly one .The end-to-end delay is more, there increase the chances for loss of information while transaction between the source node and destination node. So the effort are required to be taken regarding the reduction of power consumption and end-to-end delay in order to reduce the costing in implementation of AODV routing protocol.

The related work in the field of AODV routing protocol really creates the motivating impact on the mind for further research .The implementation of the AODV routing protocol with all features such as less end-to-end delay, maintenance of network Load, Packet loss and cost is really a challenging one. The proposed work mainly concentrates on implementation of all above parameters. This implementation will really prove advantageous for the networking technology.

Chapter Three

Methodology

3.1 Introduction

This thesis work is based on the literature research method relying on the materials listed in the references. In addition, the approach used in case study is to do simulations. The simulation experiment is carried out in LINUX (Ubuntu 10). The simulation is based on network simulator-2 version 2.34. The NS2 can be used to create the statistical data like trace file in addition to define the topology, and structure of the network and so on.

The Trace file is the output of the simulation network, example of trace file in the appendix A. In this study, the data of performance metrics has been collected from two sources the first source is a sample of small virtual classroom contains 25 students within an area of 50m*50m. These performance metrics are data rate, packet size and queue size in addition to the delay, jitter and throughput. The second source of performance metrics data is the previous studies in this field [1].

3.2 Performance Metrics

Five performance metrics such as packet-delivery-fraction (PDF), Data packet loss, delay, jitter and throughput have been considered in this study.

1) Packet-delivery-fraction (PDF)

The Ratio of the number of data packets delivered to the destinations to those generated by the CBR Sources.

$$PDF = \frac{\text{Received packet}}{\text{sent packet}} \times 100 \qquad 3.1$$

The higher the value gives the better performance. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness. [21]. Method for determining the PDF will be discussed in section 3.6.

2) Data Packet Loss (PER)

Mobility-related packet loss may occur at both the network layer and the MAC layer. Here packet loss concentrates for network layer. When a packet arrives at the network layer, the routing protocol forwards the packet if a valid route to the destination is known. Otherwise, the packet is buffered until a route is available. A packet is dropped in two cases: the buffer is full when the packet needs to be buffered and the time that the packet has been buffered exceeds the limit. [21]

PER = Total Packet Sent – Total Packet received 3.2

Method for determining the PER will be discussed in section 3.6.

3) Delay

defined as the time taken by a packet to travel from the source to the destination.

4) Jitter

Jitter is the variation of delay. That it is the variation in the delay of received packets. At the sending side, packets are sent in a continuous stream with the packets spaced evenly apart. Due to network congestion, improper queuing, or configuration errors, this steady stream can become cumbersome, or the delay between each packet can vary instead of remaining constant. Low jitter value gives better result [21] .

5) Throughput

Also called packet delivery ratio, this is the ratio of the number of packets received by the CBR sink to the number of packets sent by the CBR source, both at the application layer. Packets that are sent but not received are lost in the network due to malicious drops, route failures, congestion, and wireless channel losses. A higher throughput will directly impact the user's perception of the quality of service (QoS).[4] Method for determining the delay, jitter and throughput will be discussed in section 3.7.

3.3 Simulation Environment

Here we give the emphasis for the evaluation and optimization of performance of Ad Hoc routing protocol AODV with varying the number of packet size, queue length, and data rate. The simulations have been performed using network simulator NS-2. The network simulator ns-2 is discrete event simulation software for network simulations, which means it simulates events such as sending, receiving, forwarding and dropping packets.

The latest version, ns-allinone-2.34, supports simulation for routing protocols for ad hoc wireless networks such as AODV, TORA, DSDV, and DSR. Ns-2 is written in C ++ programming language and Object Tool Common Language (OTCL).

Although ns-2.34 can be built on various platforms, we chose a Linux platform [Ubuntu] for this thesis, as Linux offers a number of programming development tools that can be used along with the simulation process.

To run a simulation with ns-2.34, the user must write the simulation script in OTCL, get the simulation results in an output trace file.

The performance metrics are graphically visualized in ns-wireless and excel application. Ns-2 also offers a visual representation of the simulated network by tracing nodes movements and events and writing them in a network animator (NAM) file, as can be seen from Figure 3-1.

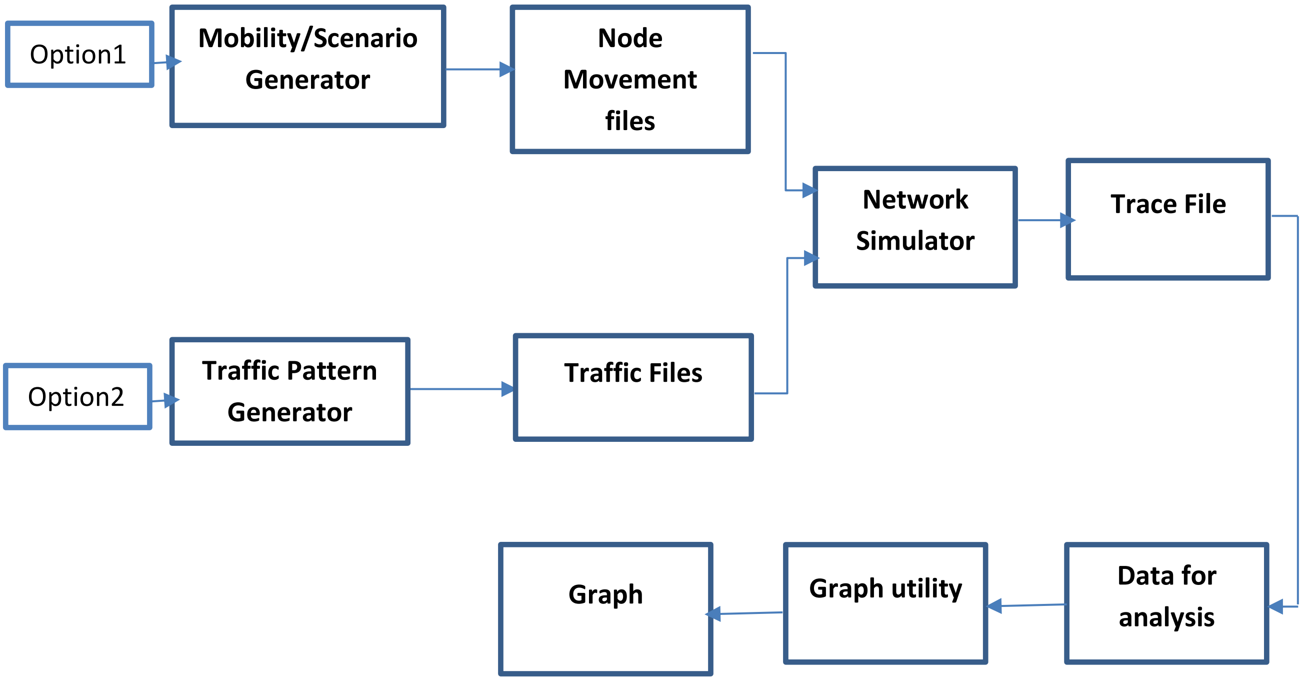


Figure 3-1: Simulation model

3.4 Traffic Model

Appropriate type of traffic for multimedia applications is continues bitrate. (CBR) is a term used in telecommunications ranging from 8kbps (Kilobits per second) to 320kbps.

3.5 Find Optimal Values of Performance Data:

To find an optimal value of performance data a group of different values of data rate, packet size and queue size are tested using network simulation.

3.5.1 Data Rate Test

Data rate values ranging from 10 to 500 kbps are tested as shown in Figure 3-2 until we got the optimal value of data rate. For further information pleases reference to TCl script in appendix A for data simulation.

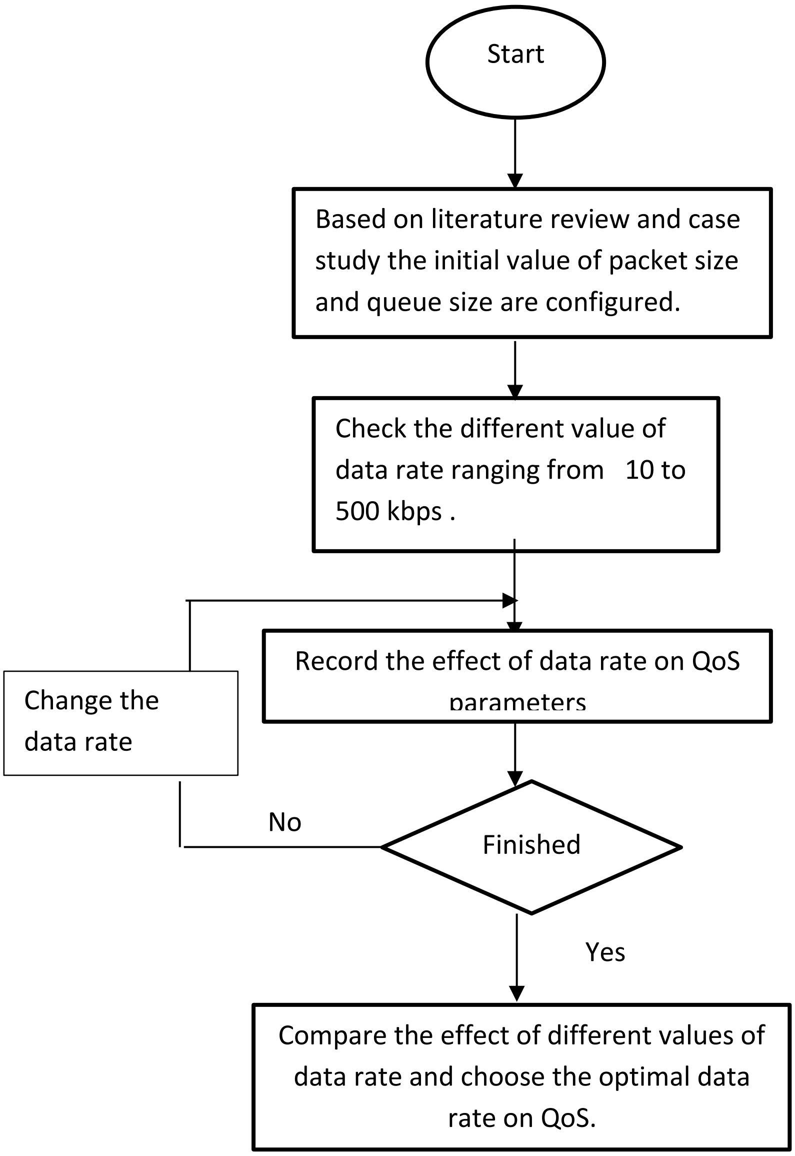

Start
Based on literature review and case study the initial value of packet size and queue size are configured.
Check the different value of data rate ranging from 10 to 500 kbps .
Record the effect of data rate on QoS parameters
Change the data rate
No
Finished
Yes
Compare the effect of different values of data rate and choose the optimal data rate on QoS.

Figure 3-2: Test different values of data rate

3.5.2 Packet Size Test

Packet size values ranging from 50 to 120 byte are tested as shown in Figure 3-3 until we got the optimal value of packet size. For further information pleases reference to TCl script in appendix A for packet size simulation.

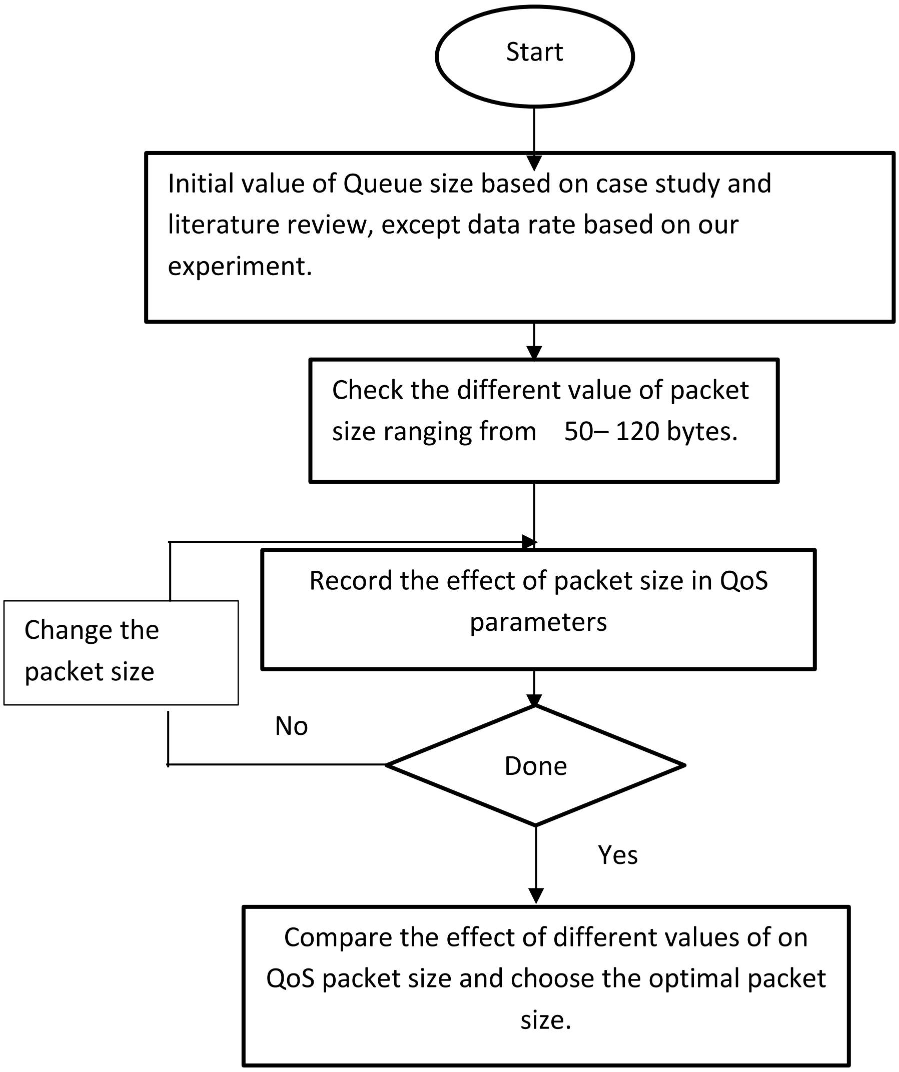

Start
Initial value of Queue size based on case study and literature review, except data rate based on our experiment.
Check the different value of packet size ranging from 50– 120 bytes.
Record the effect of packet size in QoS parameters
Change the packet size
No
Done
Yes
Compare the effect of different values of on QoS packet size and choose the optimal packet size.

Figure 3-3: test different values of packet size

3.5.3 Queue Size Test

Queue size values ranging from 50 to 1000 packet are tested as shown in Figure 3-4 until we got the optimal value of queue size. For further information pleases reference to TCl script in appendix A for Queue size simulation.

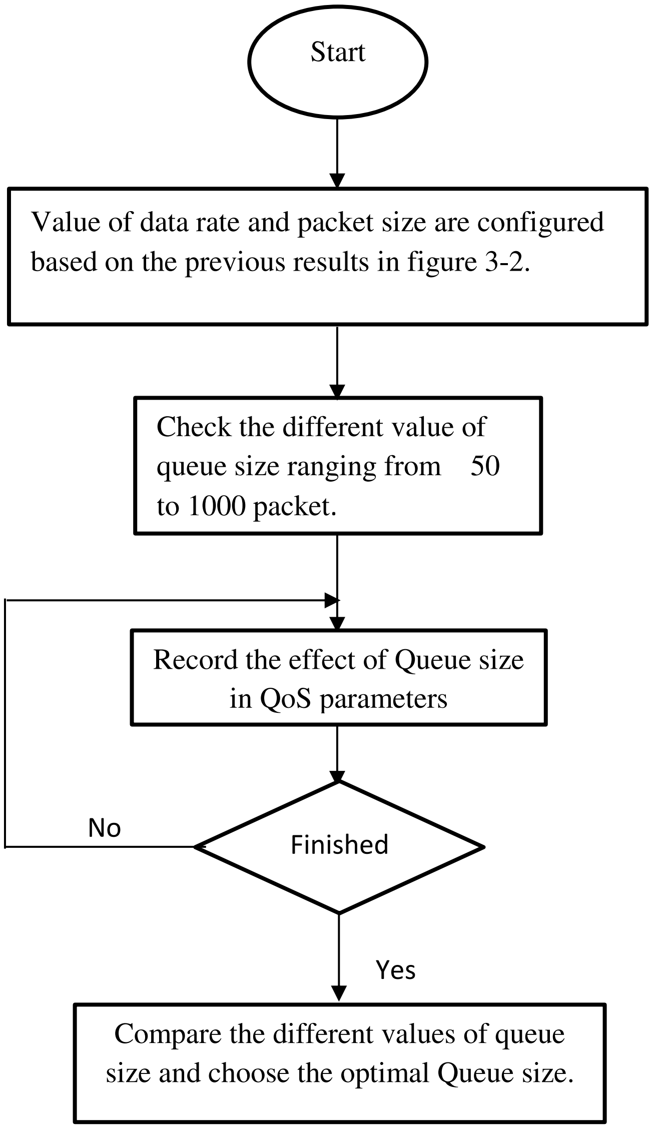
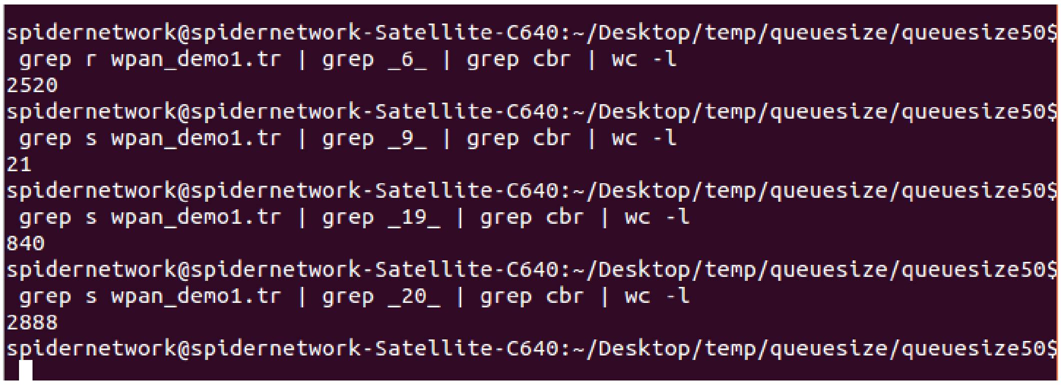

Start
Value of data rate and packet size are configured based on the previous results in figure 3-2.
Check the different value of queue size ranging from 50 to 1000 packet.
Record the effect of Queue size in QoS parameters
No
Finished
Yes
Compare the different values of queue size and choose the optimal Queue size.

Figure 3-4: Test different values of queue size

3.6 Calculate values of PDF and Packet loss:

Values of PDF and packet loss number are calculated from the trace file to test the effect of different values of data rate on them. PDF and packet loss value are calculated by using grep command, as shown in Figure 3-5.



```
spidernetwork@spidernetwork-Satellite-C640:~/Desktop/temp/queuesize/queuesize50$
 grep r wpan_demo1.tr | grep _6_ | grep cbr | wc -l
2520
spidernetwork@spidernetwork-Satellite-C640:~/Desktop/temp/queuesize/queuesize50$
 grep s wpan_demo1.tr | grep _9_ | grep cbr | wc -l
21
spidernetwork@spidernetwork-Satellite-C640:~/Desktop/temp/queuesize/queuesize50$
 grep s wpan_demo1.tr | grep _19_ | grep cbr | wc -l
840
spidernetwork@spidernetwork-Satellite-C640:~/Desktop/temp/queuesize/queuesize50$
 grep s wpan_demo1.tr | grep _20_ | grep cbr | wc -l
2888
spidernetwork@spidernetwork-Satellite-C640:~/Desktop/temp/queuesize/queuesize50$
```

Figure 3-5: PDF and packet loss value are

Figure 3-5 display Sample of the results to show how to calculate packet loss and packet delivery fraction.

Sample of relationship between two QoS metric such as PDF and data rate is represented in graphical manner using Microsoft Excel as shown in Figure 3-6.

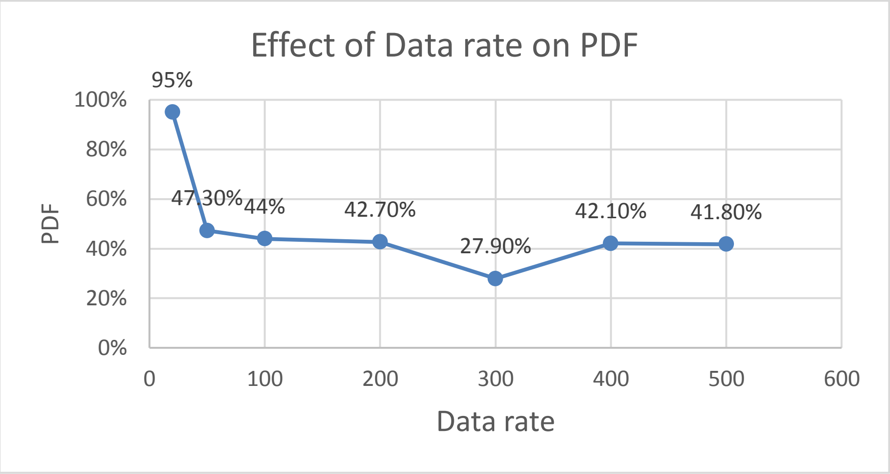
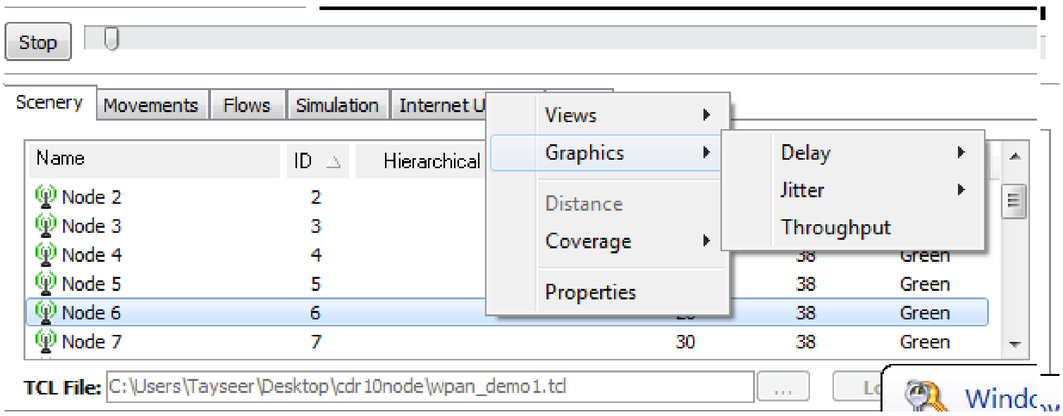


Figure 3-6: Effect of Data rate on PDF

3.7 Calculate values of delay, jitter and throughput

The values of delay, jitter and throughput are calculated by ns-wireless program. Ns- Wireless application use trace file as an input to generate values of delay, jitter and throughput. Interface of ns- wireless is shown in Figure 3-7.



Name	ID	Hierarchical			
Node 2	2				
Node 3	3				
Node 4	4			38	Green
Node 5	5			38	Green
Node 6	6			38	Green
Node 7	7		30	38	Green

TCL File: C:\Users\Tayseer\Desktop\cdr10node\wpan_demo1.tcl

Figure 3-7: ns-wireless application interface

Trace file is imported from ns-2 to ns-wireless application. For further information pleases reference to trace file in appendix A.

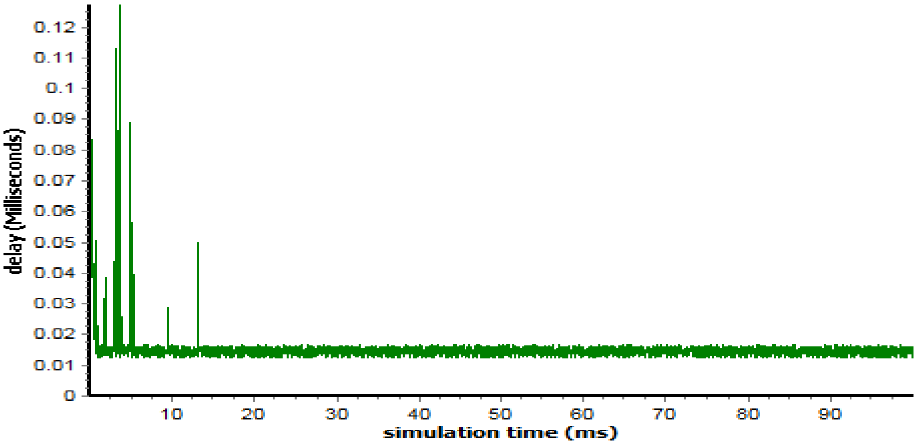


Figure 3-8: sample of the results show the delay over time at the main node

The output of ns-wireless is shown in Figure 3-8.