IMPROVING THE PERFORMANCE OF AD-HOC NETWORK USING ENHANCED INTERIOR GATEWAY ROUTING TECHNIQUE

[1]Nnamdi Ahuchaogu, E.N. Aneke [2]

[1]Department of Electrical Electronic Engineering, Abia State University, Uturu, Nigeria

2 Electrical and Electronic Engineering Department, Enugu State University of Science and Technology, Agbani, Enugu PMB 01660 Nigeria. ENG.Ezekiel.Aneke@ieee.org

ABSTRACT

Mobile Ad hoc Networks (MANETs) are an emerging class of network architectures that are characterized by their highly dynamic topology, limited resources (i.e bandwidth and power), and lack of fixed infrastructure. The primary motivation for such networks is increased flexibility and mobility. There are number of paths in ad hoc network for communication between the nodes and selection of the shortest path from those paths is one of the key issues. One of the particularly important networking issues in mobile ad hoc network is Routing. This research explores the use of bandwidth estimation and path selection model in determining the transmission paths with the minimum and maximum delay metric. Furthermore, the delay metrics was identified to be above the threshold of ≤ 5ms. A modified shortest path algorithm using an Enhanced Interior Gateway Routing Technique was developed to reduce the delay, routing over-head caused by flooding,and mitigate the re-routing problems in ad hoc network. A database was also developed using Microsoft structured query language software and class C Internet Protocol (IP) address to enhance easy identification and accessibility of files by the nodes and to checkmate intruders to the network using their Media Access Control (MAC) address. A performance improvement of about 5% was recorded as shown in the simulation result. The developed algorithm has a smaller end-to-end delay when compared to existing ones as it provided a reduced delay metric and enhanced the performance of ad hoc network whenimplemented. A moderate packet size should be used in ad hoc networks since a larger packet size take a higher time for transmission.

INTRODUCTION

1.1 Background of The Study

The quality of service, according to networking context, is the degree of user's satisfaction of services that a communication system provides. It aims at improving communication behaviour under a correct data transmission and an optimal use of resources (Jiang, 2014).

The Mobile Ad hoc Network (MANET) is nothing but the wireless connection of mobile nodes which provides the communication and mobility among wireless nodes without the need of any physical infrastructure or centralized devices such as a base station. The communication in MANET is done by routing protocols.

Mobile ad hoc networks, with their complex nature impose many constraints than in wired networks. Besides, the quality of service relates to the behaviour of the network, and is dealt with from different points of view. It typically addresses a set of metrics relevant to delay, throughput, bandwidth, jitter, packet loss rate, energy consumption, stability, security, and so on. It is worth noting, accordingly, that some criteria are very difficult to discern and can still be considered challenging.

One of the particularly important networking issues is Routing in mobile ad-hoc networks. From routing perspective, it is expected that data packets are routed via a stable and reliable path to avoid frequent re-routing problem, since frequent re-routing may induce broadcast storm on the network, waste the scarce radio

resources and degrade end-to-end network performance such as throughout and delay (Tseng, 2016).

Topology control focuses on network connectivity with the link information provided by Medium Access control (MAC) and physical layers (Tang, 2014).

Mobile ad-hoc network is a wireless network composed of different nodes communicating with each other without having to establish physical infrastructure. They are mainly characterized by dynamic topology (Guan, 2009).

The mobile ad hoc network consists of mobile platforms (each platform logically consisting of a router, possibly with multiple hosts and wireless communication devices).

The diverse application of mobile ad hoc networks (MANETs) in many different scenarios such as battlefield, disaster management/recovery, etc, have seen MANETs being researched by many different organizations and institutes. One interesting research area in MANET is Routing (Abolhasn, 2015).

In computer networks, the data sent from source to destination needs a specific path. There are number of paths in a computer network for communication between the nodes and the selection of a shortest path from those paths is one of the key issues. The appropriate path selection can be done by applying routing protocols.

The routing protocols enable routers to build up a routing table that associates the final destinations with next hop addresses. The router sends data on the shortest path defined in its routing table.

The order in which routers communicate with each other and exchange information is made possible by routing protocol, (Archana, 2015). Routing protocol also enables routers to select routes between any two nodes on a computer network. Routing protocol can also be said to be a language a router speaks with other routers in order to share information about the reachibility and states of the network, (Patel, 2014).

Enhanced Interior Gateway Routing Protocol (EIGRP) is interior gateway protocol suited for many different topologies and media. It offers some additional benefits over other protocols. Some of these benefits include: rapid convergence, lower bandwidth utilization, and multiple routed protocol support.

EIGRP can be easily configured and is also regarded as an enhanced IGRP as a result of its rapid convergence tendency (which it achieves using an updating algorithm known as diffuse update Algorithm) and loop free topology guaranteed at all times.

Enormous approaches were adopted and became obsolete from time to time as new technological revolutions had set the communication parameter up to date. The whole phenomenon of communication process signifies the importance of valuable and unfailing transportation of data and information from source to destination.

In this concern of intact data transportation, much development of protocols and their improvements yield very progressive results providing efficient transmission and reception of intact and undamaged data. Current information

technology trends are operating to provide easy and simple measures intended for reliable, efficient, and error free communication.

Mobile computing has been introduced (mainly as a result of major technological developments) in the past few years forming a new computing environment. Because of the fact that mobile computing is constrained by poor resources, highly dynamic variable connectivity and restricted energy sources, the design of stable and efficient mobile information systems has been greatly complicated.

Until now, two basic system models have been developed for mobile computing. The "fixed backbone" mobile system model has been used around the past decade and has evolved to a fairly stable system that can exploit a variety of information in order to enhance already existing services and yet provide new ones.

On the other hand, the "ad hoc" system model assumes that mobile hosts can form networks without the participation of any fixed infrastructure.

Mobile ad-hoc technology has attracted the attention of the communications field and host of researchers since the development of the mobile packet radio networks in research projects initiated by the US military in the 1970 and 1980s. The mobile Ad-hoc network (MANET) is an autonomous network of mobile computers that are connected via wireless links. There is no pre–existing infrastructure and thus each node in the network may act as a host or as a router (an intermediate nodes) to allow connectivity between other source and destruction hosts in the network. The term ad – hoc implies that the network is formed in a spontaneous manner to meet an immediate and specific goal.

The nodes in ad – hoc network are mobile. They can leave or enter the network anytime. (Johnson,2016).

The applications of ad hoc networks can be categorized as follows:

(a) Military Applications: ad hoc networks are particularly suited to battlefield scenarios where soldiers or unattended vehicles require mobile and instantaneous communication links operating in a hostile environment.

(b) Commercial Applications: The current application of ad hoc networking is local Area Network (LAN) or Personal Area Networking (PAN) depending on the radio range of the system. In a PAN, users' devices - such as laptops, mobile phones, and Personal Digital Assistants (PDAs) - collaborate amongst each other to set up an ad hoc network and exchange data.

(c) Emergency and Rescue Applications: ad hoc networks could be deployed in emergency and rescue situations where the fixed infrastructure may have been destroyed due to a disaster.

(d) Sensor Networks: Collection of environmental data is a typical application of such networks.

In ad hoc networks a node can directly communicate to any other node connected to it (i.e peer- to- peer connection), but when there is need to establish multipath or multi-hop communication, then, routing protocol becomes very important.

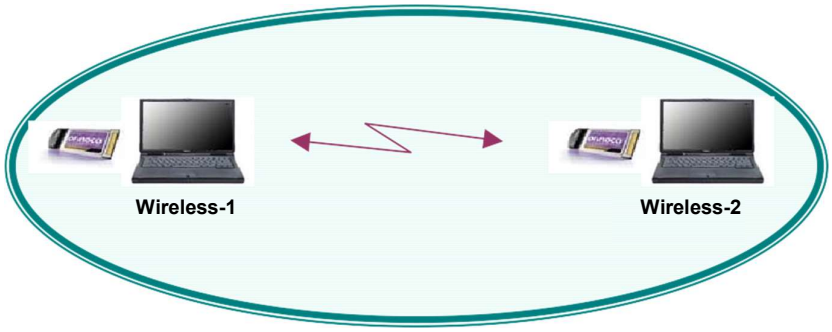

Figure 1.1: A basic peer- to- pee ad hoc network

The diagram of a peer-to- peer connected ad hoc network is shown above:

As new nodes join the network outside the range of the peer, additional features are required for multi-hop capability. Unlike in a fixed network with infrastructure, Ad hoc networks' self-healing properties appear when users join, leave, or move, making the network topology dynamic.

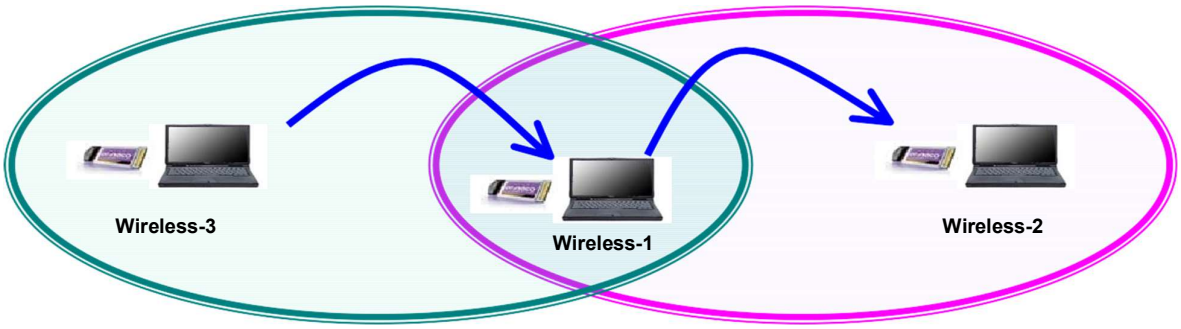

Figure 1.2: A multi hop ad hoc network

1.2 Problem Statement

With the poor quality of service provided by fixed or licensed network operators and most times the difficulties experienced in data transmission in areas with non-availability of network providers in Nigeria, especially during emergency situations, there is every need for provision of an adhoc network with an efficient routing technique to become an alternative stable means of data transmission at a reduced cost.

The occurrence of insurgency has become the order of the day in Nigerian environment today, and hence, the need for an improved ad hoc network. The delay in transmitting and receiving information in military scenario, managing and handling of emergency situations (Rescue and Relief Operations) has led to loss of lives which would have

been prevented using good mobile ad hoc network system, since the major equipment of the licensed or fixed network operators are mostly affected in such environmental condition.

Enhanced Interior Gateway Routing Protocol (EIGRP) is a technique that can be used to improve the throughput, reduce the delay and minimizing the re-routing problems, thereby improving the performance of an entire mobile ad hoc network. It is a technique that uses Diffuse Update Algorithm (DUAL) in calculating its shortest path of transmission and does not make use of loop topology during routing, and can be used to reduce delay and improve throughput in mobile ad hoc network.

Ad-hoc networks have their own requirements and constraints and require a protocol that takes into consideration these constraints and provide protected communication under such constraints. The process of Ad-hoc networks depends on the collaboration among nodes to provide connectivity and communication routes.

1.3 Aim and Objectives

The aim of this research work is to improve the performance of ad hoc Network using Enhanced Interior Gateway Routing Technique

To realize this aim, the following specific objectives were adopted:

i. To characterize the network of study in order to study/determine the need for improvement.
ii. To develop a central reference database that contain different files and work as file transfer protocol (FTP) server and Domain Name System (DNS) server-using Microsoft SQL software.
iii. To design the Enhanced Interior Gateway Routing Protocols (EIGRP) using Hyper V Software together with layer three devices (i.e. Routers & Switches) and single Autonomous system number for end to end connectivity.
iv. To develop a modified Algorithm for enhancement of EIGRP performance in a network.
v. To simulate the work and evaluate the simulation results.

1.4 Significance of The Study

With a reduction in delay in transmission of data across ad hoc network as a result of improved routing technique, the usage of ad hoc network was enhanced in handling of emergency situations and in military Scenario especially in areas with non-availability of licensed or fixed network operators or service providers.

1.5 Scope of The Study

The major challenges in ad-hoc network includes; security of connections between hosts in a network, Routing, etc. But this work focused mainly on the design of an efficient Routing technique that could reduce excessive routing overhead, mitigate re – routing problems experienced in mobile ad-hoc network and reduce the general routing problems as it affects the performance of MANET.

LITERATURE REVIEW

2.1 Theory of Mobile Ad hoc Network

Mobile Ad hoc network as the name implies, is a temporal network formed in a spontaneous manner to meet an immediate and specific goal. It is a network without any fixed infrastructure and highly affected by nodes mobility and limited resources which includes power and bandwidth. It is a network where nodes leave or enters the network at any time, no fixed or assigned bandwidth.

2.1.1 Features of Mobile Ad hoc network

The mobile Adhoc networks has the following features-

- Autonomous terminal
- Distributed operation
- Multi hop routing
- Dynamic network topology
- Fluctuating link capacity
- Light-weight terminals

2.1.2 Autonomous Terminal

In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other words, beside the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually end points and switches are indistinguishable in MANET.

2.1.3 Distributed Operation

Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed to implement functions like security and routing.

2.1.4 Multichip Routing

Basic types of Ad hoc routing algorithms can be single-hop and multichip, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multichip in terms of structure and implementation, with the lesser cost of functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.

2.1.5 Dynamic Network Topology

Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. Moreover, a user in the MANET may

not only operate within the Ad hoc network, but may require access to a public fixed network (e.g. Internet).

2.1.6 Fluctuating Link Capacity

The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subjected to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.

2.1.7 Light Weight Terminals

In most of the cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

2.1.8 Challenges of Mobile ad hoc network

Ad hoc networking has been a popular field of study during the last few years. Almost every aspect of the network has been explored in one way or other at different level of problem. Yet, no ultimate resolution to any of the problems is found or, at least, agreed upon. On the contrary, more questions have arisen. The topics that need to be resolved are as follows:

Scalability, Routing, Quality of Service, Client Server model Shift, Security, Energy Conservation, Node cooperation and Interoperability. The approach to tackle above aspects has been suggested and possible update solutions have been discussed. In present research work one of the aspects “the routing” has been reconsidered for suitable protocol performing better under dynamic condition of network.

2.1.9 Scalability:

Most of the visionaries depicting applications which are anticipated to benefit from the Ad hoc technology take scalability as granted. Imagine, for example, the vision of ubiquitous computing where networks can be of "any size". However, it is unclear how such large networks can actually grow. Ad hoc networks suffer, by nature, from the scalability problems in capacity.

To exemplify this, we may look into simple interference studies. In a non-cooperative network, where omni-directional antennas are being used, the throughput per node decreases at a of rate$1/\sqrt{N}$, where N is the number of nodes. That is in a network with 100 nodes, a single device gets, at most, approximately one tenth of the theoretical network data rate. This problem, however, cannot be fixed except by physical layer improvements, such as directional antennas. If the available capacity like bandwidth, radiation pattern of antenna sets some limits for communications.

This demands the formulation of new protocols to overcome circumvents.

Route acquisition, service location and encryption key exchanges are just few examples of tasks that will require considerable overhead as the network size grows. If the scarce resources are wasted with profuse control traffic, these networks may see never the day dawn.

Therefore, scalability is a boiling research topic and has to be taken into account in the design of solutions for Ad hoc networks.

2.1.10 Routing

Routing in wireless Ad hoc networks is nontrivial due to highly dynamic environment. An Ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any preexisting network infrastructure or centralized administration.

In a typical Ad hoc network, mobile nodes come together for a period of time to exchange information. While exchanging information, the nodes may continue to move, and so the network must be prepared to adapt continually to establish routes among themselves without any outside support.

2.1.11 Quality of Service

The heterogeneity of existing Internet applications has challenged network designers who have built the network to provide best-effort service only. Voice, live video and file transfer are just a few applications having very diverse requirements.

Qualities of Service (QoS) aware solutions are being developed to meet the emerging requirements of these applications. QoS has to be guaranteed by the network to provide certain performance for a given flow, or a collection of flows, in terms of QoS parameters such as delay, jitter, bandwidth, packet loss probability, and so on.

Despite the current research efforts in the QoS area, QoS in Ad hoc networks is still an unexplored area. Issues of QoS in robustness, QoS in routing policies, algorithms and protocols with multipath, including preemptive, priorities remain to be addressed.

2.1.12 Client-Server Model Shift:

In the Internet, a network client is typically configured to use a server as its partner for network transactions. These servers can be found automatically or by static configuration.

In ad hoc networks, however, the network structure cannot be defined by collecting IP addresses into subnets.

There may not be servers, but the demand for basic services still exists. Address allocation, name resolution, authentication and the service location itself are just examples of the very basic services which are needed but their location in the network is unknown and possibly even changing over time.

Due to the infrastructureless nature of these networks and node mobility,

a different addressing approach may be required.

In addition, it is still not clear who will be responsible for managing various network services. Therefore, while there have been vast research initiatives in this area, the issue of shift from the traditional client-sever model remains to be appropriately addressed.

2.1.13 Security

A vital issue that has to be addressed is the Security in Ad hoc networks. Applications like Military and Confidential Meetings require high degree of security against enemies and active/passive eavesdropping attacker. Ad hoc networks are particularly prone to malicious behavior. Lack of any centralized network management or certification authority makes these dynamically changing wireless structures very vulnerable to infiltration, eavesdropping, interference, and so on. Security is often considered to be the major "road block" in the commercial application.

2.1.14 Energy Conservation

Energy conservative networks are becoming extremely popular within the ad hoc networking research. Energy conservation is currently being addressed in every layer of the protocol stack. There are two primary research topics which are almost identical: maximization of lifetime of a single battery and maximization of the life time of the whole network.

The former is related to commercial applications and node cooperation

issues whereas the latter is more fundamental, for instance, in military environments where node cooperation is assumed. The goals can be achieved either by developing better batteries, or by making the network terminals operation more energy efficient. The first approach is likely to give a 40% increase in battery life in the near future (with Li-Polymer batteries).

As to the device power consumption, the primary aspect is achieving energy savings through the low power hardware development using techniques such as variable clock speed CPUs, flash memory, and disk spin down. However, from the networking point of view, our interest naturally focuses on the device's network interface, which is often the single largest consumer of power. Energy efficiency at the network interface can be improved by developing transmission/reception technologies on the physical layer.

Much research has been carried out at the physical, medium access control (MAC) and routing layers, while little has been done at the transport and application layers. Nevertheless, there is still much more investigation to be carried out.

2.1.15 Node Cooperation

Closely related to the security issues, the node cooperation stands in the way of commercial application of the technology. To receive the

corresponding services from others there is no alternative but one has to rely on other people's data. However, when differences in amount and priority of the data come into picture, the situation becomes far more complex.

A critical fire alarm box should not waste its batteries for relaying gaming data, nor should it be denied access to other nodes because of such restrictive behavior. Encouraging nodes to cooperate may lead to the introduction of billing, similar to the idea suggested for Internet congestion control.

Well-behaving network members could be rewarded, while selfish or malicious users could be charged higher rates. Implementation of any kind of billing mechanism is, however, very challenging. These issues are still wide open.

2.1.16 Interoperability

The self organization of ad hoc networks is a challenge when two independently formed networks come physically close to each other. This is an unexplored research topic that has implications on all levels on the system design.

When two autonomous Ad hoc networks move into same area the interference with each other becomes unavoidable. Ideally, the networks would recognize the situation and be merged. However, the issue of

joining two networks is not trivial; the networks may be using different synchronization, or even different MAC or routing protocols. Security also becomes a major concern. Can the networks adapt to the situation? For example; a military unit moving into an area covered by a sensor network could be such a situation; moving unit would probably be using different routing protocol with location information support, while the sensor network would have a simple static routing protocol.

Another important issue comes into picture when we talk about all wireless networks. One of the most important aims of recent research on all wireless networks is to provide seamless integration of all types of networks.

2.2 Factors to Be Considered When Deploying MANET

The following are some of the main routing issues to be considered when deploying MANETs: Unpredictability of Environment, Unreliability of Wireless Medium, Resource-Constrained Nodes, Dynamic Topology, Transmission Errors, Node Failures, Link Failures, Route Breakages, Congested Nodes or Links.

i. **Unpredictability of Environment:** Ad hoc networks may be deployed in unknown terrains, hazardous conditions, and even hostile environments where tampering or the actual destruction of a node may be imminent. Depending on the environment, node

failures may occur frequently.

ii. **Unreliability of Wireless Medium:** Communication through the wireless medium is unreliable and subject to errors. Also, due to varying environmental conditions such as high levels of electro-magnetic interference (EMI) or inclement weather, the quality of the wireless link may be unpredictable.

iii. **Resource-Constrained Nodes:** Nodes in a MANET are typically battery powered as well as limited in storage and processing capabilities. Moreover, they may be situated in areas where it is not possible to re-charge and thus have limited lifetimes.

Because of these limitations, they must have algorithms which are energy efficient as well as operating with limited processing and memory resources. The available bandwidth of the wireless medium may also be limited because nodes may not be able to sacrifice the energy consumed by operating at full link speed.

iv. **Dynamic Topology:** The topology in an ad hoc network may change constantly due to the mobility of nodes. As nodes move in and out of range of each other, some links break while new links between nodes are created.

As a result of these issues, MANETs are prone to numerous types of faults including the following-

a. **Transmission Errors:** The unreliability of the wireless medium

and the unpredictability of the environment may lead to transmitted packets being garbled and thus received packet errors.

b. **Node Failures:** Nodes may fail at any time due to different types of hazardous conditions in the environment. They may also drop out of the network either voluntarily or when their energy supply is depleted.

c. **Link Failures:** Node failures as well as changing environmental conditions may cause links between nodes to break. Link failures cause the source node to discover new routes through other links.

d. **Route Breakages:** When the network topology changes due to node/link failures and/or node/link additions to the network, routes become out-of-date and thus incorrect. Depending upon the network transport protocol, packets forwarded through stale routes may either eventually be dropped or be delayed.

e. **Congested Nodes or Links:** Due to the topology of the network and the nature of the routing protocol, certain nodes or links may become over utilized, i.e., congested. This will lead to either larger delays or packet loss.

2.2.1 Applications of Ad hoc Networks

Ad hoc networks are suited for use in situations where an infrastructure is unavailable or to deploy one is not cost effective. The following are

some of the important applications.

i. **Business Applications**: One of many possible uses of mobile Ad hoc networks is in some business environments, where the need for collaborative computing might be more important outside the office environment than inside, such as in a business meeting outside the office to brief clients on a given assignment.

   Work has been going on to introduce the fundamental concepts of game theory and its applications in telecommunications. Game theory originates from economics and has been applied in various fields. Game theory deals with multi-person decision making, in which each decision maker tries to maximize his utility.

   The cooperation of the users is necessary to the operation of ad hoc networks; therefore, game theory provides a good basis to analyze the networks.

ii. **Military Applications**: Military applications have motivated early research on ad hoc networks. The ability to quickly set up a network among military units in hostile territory without any infrastructure support can provide friendly forces with a considerable tactical advantage on the battle field.

   Recent advances in robotics have also motivated the idea of automated battle fields in which unmanned fighting vehicles are sent into battle. Supporting military applications requires self-

organizing mechanisms that provide robust and reliable communication in dynamic battle situations.

iii. **Emergency Operations**: Another promising application area for ad hoc networks is emergency services, including search and rescue and disaster recovery operations. As an example of search and rescue, consider an airline that attaches small wireless devices to the lifejackets under each seat. Suppose that the plane has mechanical problems and has to make an emergency landing in the water. Once search and rescue teams arrive at the landing site, they are provided with detailed information about the location (the coordinates and potentially the depth) of the victims through the transponders. As a result, the rescue teams can more effectively locate and reach the victims. The mobile devices could also monitor the vital signs of victims, such as heart rate or breathing rate, to prioritize the rescue of victims that are still alive.

A similar application arises when disasters, such as earthquakes, blackouts, or bombings occur. The disaster may destroy existing communication infrastructure, preventing critical contact among emergency workers.

The emergency response team scan set up Ad hoc networks quickly to replace the destroyed infrastructure, enabling the teams to better coordinate their efforts. In emergency situation the wired networks

could be destroyed. There will be a need of wireless network, which could be deployed quickly for coordination of rescue. An example is the design for future public safety communications.

A European project called Wireless Deployable Network System (WIDENS) concentrated their work on this field. WIDENS have an idea that using Ad hoc network to interoperate with existing TETRA network which is used for public safety.

iv. **Home, Office, and Educational Applications:**

Adhoc networks also have applications in home and office environments. The simple stand most direct application of Adhoc networks in both homes and offices is the networking of laptops, PDAs and other WLAN-enabled devices in the absence of a wireless base station. Another home application that falls within the Personal Area Network (PAN) class is wire replacement through wireless links, as in Bluetooth. All periphery devices can connect to a computer through wireless Bluetooth links, eliminating the need for wired connections. ad hoc networks can also enable streaming of video and audio among wireless nodes in the absence of any base station.

For instance, ultra wild band (UWB) provides a sufficiently high bandwidth (in the order of Gb/s) to support several multimedia streams. UWB-equipped nodes can autonomously set up an Ad hoc network to

stream high quality video and audio between several computers through wireless UWB connections.

Educational and recreational activities can also benefit from Ad hoc networks. For example, students attending a classroom can use their laptops to obtain the latest class material from a professor's laptop as the class progresses.

Universities and campus settings, Virtual classrooms, Ad hoc communications during meetings or lectures are some of the educational applications of Ad hoc networks. On the recreational side, the mobility and nomadic nature of Ad hoc networks enables richer multi-user games that can incorporate user mobility and proximity into the virtual game environment.

2.3 Review of Related Literature

In the quest to develop an improved routing technique that could drastically improve the performance of a mobile ad-hoc network by reducing the delay in data transmission, improve throughput and mitigating re – routing frequency considering the broadcast nature of transmission experience in mobile ad-hoc networks, many scholars have developed many routing techniques with different limitations.

Takasi and Kleinrecux proposed the first position-based routing protocol called "free method for finding a route (MFR). This is the routing protocol which is

based on the notion of progress. MFR is a well known loop free method for finding a route in a network by utilizing position information of nodes. The neighbour with the greatest progress on the straight line joining the source and destination is chosen as next-hop node for sending packets further. MFR forwards the packet to the node that is closest to the destination node in an attempt to minimize number of hops. But in case of network failure, this routing protocols uses a computational technique to find its alternative routes thereby introducing delay into the system. (Maag, 2015).

Kranakis proposed the direct information routing (DIR), popularly referred to as the compass routing. This routing protocol is based on the greedy forwarding method in which the source uses the position information of the destination node to calculate its direction. The message is forwarded to the nearest neighbour having direction closest to the line drawn between source and destination. Therefore, a message is forwarded to the neighbouring node minimizing the angle between itself, the previous node and the destination. It is also a loop free location-based routing algorithm.

Bobby R. Sawde proposed tactical on demand distance vector routing protocol. This is a routing protocol that stores routing information in a distributed fashion at every node on the route and uses a new technique called query localization technique to reduce the network traffic as well as to select the most efficient path between source and destination (Sawde,2015).

2.3.1 Interior Gate Protocols (IGP)

Dynamic Routing Protocol fall into three categories: Distance Vector (DV), link state (LS) and hybrid protocols. The knowledge information shared by different network segments is defined by the routing protocol selected, which are stored in routing tables. To maintain an up to data routing table, the router must determine the best information to be stored (kranakis,2015). Each protocol determines this, based on a certain criterion with the use of algorithms, which compile values known as metrics. Metrics are generated from as little as on characteristics of the network or more often several characteristics. The most common measurements normally include hop counts, delay, bandwidth, load reliability (i.e. errors on the look), cost, etc.

The distance vector protocol uses the distance and direction to find the best path to the destination by using an algorithm called the Bellman.

Ford algorithm Network discovery is achieved by gathering information from directly connected neighbouring routes. To share this information, distance vector protocols uses a method known as a local broadcast (Battista el al,2015).

This sends out data to any device that is connected to an interface of the router. Distance vector does not care who receive and process these broadcasts and they are periodic in their approach. These protocols will send out updates at regular intervals regardless of whether or not there is a topology change. As these packets regularly traverse the network, a large amount of unwanted network traffic, can be generated.

Examples of distance vector protocols are Routing Information, Protocol Version 1 (RIPVI), Interior Gateway Routing Protocol (IGRP), etc.

2.3.2 Routing Information Protocol Version 1 (RIP Version 1)

Version 1 is a distance vector protocol that is easy to comprehend and deploy with ad hoc system although superseded by more complex routing algorithms, RIP is still widely used in smaller ad hoc network due to its simplicity. It makes no formal destination between networks and hosts. Routers typically provide a gateway for data to leave one network and to be forwarded to another network. Routers therefore, have to make decision if there is a choice of forwarding path on offer. Routing information protocol networks use the hop count metric system (Thorenoor,2014).

Every time a router passes the routing table to other routers, a value of one (1) is added to the metric insides the routing update. The maximum number of hop count is to solve the routing loops problems.

Routing loops basically introduces confusions in a network topology that occur when the update/age out times seems or appears to be inefficient. With the hop count set to 15, the packet can be passed through a maximum of 15 routers before being discarded, without which, the packets can be passed indefinitely until either the network crashes or the routers are switched off. RIP supports up to a maximum of six (6) equal-cost path to a destination, this means that a destination is reachable over different routes that have the same amount of hops, the router will hold all routers in memory up to a maximum of six (four is the default). The

paths are all placed into the routing table and can be used to load balance when sending data.

The main features of RIP can also lead to its disadvantages, such as information flooding, ineffectiveness of metric systems, and classic routing algorithm.

2.3.3 Open Shortest Path First

Open shortest path (OSPF) is based on Open Standards and has good compatibility on a wider range of equipment, it is a prevalent routing protocol in larger enterprise networks.

It is a routing protocol which uses more complex, metric system to give efficient pathways discovery solutions to remote networks. The cost to measure the metric is worked out by taking the inverse of the bandwidth of links.

Essentially a faster link is lower in cost. The lowest cost paths to remote networks are the most preferred routers, and held in the routing table.

OSPF can load balance across a maximum of six equal-cost path links, although doing this can cause difficulties. The serial interface of the router is configured with a clock rate and a bandwidth. The clock rate is the speed that data can be sent across a link, and the bandwidth is used by the routing protocol in the metric calculations. By default, the speed of a serial interface is set to 1544kbps.

The potential hazard of the system is that whenever different clock rate are set on a different link, the bandwidth has to be accordingly configured, otherwise OSPF will regard both connections as same speed, which will cause problem with load balancing (Johansson,2014).

When routers need to run OSPF frequently, lots of resources are dedicated to the process; the potential problem can dramatically slow down the network service speed.

There are some major differences between open short path first and routing information protocol.

Firstly, Comparing to Routing Information Protocol (RIP), OSPF is a classless protocol which allows utilization of different subnet masks, which essentially gives network administrators more flexibility with IP addresses and less wastage (Mahini et al,2012).

Secondly, one appealing advantage that OSPF offers over RIP is scalability. Open short path first is able to understand the hierarchical routing structure.

Thirdly, OSPF only sends out update information when there is a change in the network, rather than sending periodic updates at regular intervals as in distance vector protocols. This quality saves the bandwidth utilization throughout the entire network communications (Mark, 2016).

Fourthly, while the Routing Information protocols uses broadcast to pass on routing information throughout networks which can cause potentials network congestion problems, OSPF uses multicast method to reduce network traffic which uses that are destined for particular machines.

Below are some of the routing techniques that could be used in ad hoc networks with some major constraints compared to the proposed techniques.

Ad-hoc on-demand distance vector (AODV) routing protocol is a routing protocol intended for use by mobile nodes in ad-Hoc network when two hosts wish to communicate with each other and a route is created to provide such connection, but it offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization and determines routes to destinations within ad hoc network. In a large and highly mobile network, considerable routing overhead is incurred by this flooding method.

Most of the reactive protocols like Ad-hoc on demand Vector (AODV) use blind flooding techniques for routing between source and destination nodes, which creates a huge amount of routing overhead (Vasudha el al,2012)

Tactical ad-hoc on demand vector (TAODV) protocol was brought to be an improvement to AODV. It uses a new technique called Query localization techniques to reduce the network traffic as well as to select the most efficient path between source and destination. Classical algorithm (like dijikstra Algorithm) had a very small search space to find distance between two points in a graph and later, the Quantum search Algorithm was developed to find distance between two points in a graph and later, the Quantum search Algorithm was developed to find the shortest path in a graph. In this algorithm, we first start with the Dijikstra algorithm and then integrate the Quantum Algorithm to it which makes the search for paths faster.

Due to dynamic nature of ad-hoc networks, the shortest path (SP) problem is very difficult to handle and this lead to the development of the Genetic Algorithm,

which uses immigrates and memory schemes to solve the shortest path problem in ad-hoc networks which is usually difficult to solve due to dynamic topology of the networks (Horneffer el al,2014).

The Ant Colony algorithm is very useful and efficient to find shortest path in an ad-hoc network but its difficult for it to find shortest path when the input as prone to some kind of noise.

The Split Multipath Routing (SMR) protocol overcomes this problem but has large routing overhead because it uses more control packets in order to build multiple routes between source and destination and that a disadvantage (Sportack,2013).

Many Routing Protocols can be made use of in mobile Adhoc Network. Also, the several failures in communication experienced or witnessed in Mobile ad hoc net are mostly due to unreliable communication link.

Majority of the delays are developed during the process of re-establishment of the failed path.

However, the unreliability of the wireless medium results in frequent communication failures. The high delays occur when the path re-establishment takes place.

So a Multi-path routing is a very promising alternative to single path routing as it provides higher resilience to path breaks and alleviates network congestion through load balancing and reduces end-to-end delay.

Thus, the multi-path routing can be highly suitable for multimedia streaming over wireless ad hoc networks.

A few research students have been done to address issues in ad hoc networks.

2.3.4 Optimized Link State Routing (OLSR)

The Optimized Link State Routing protocol communicates with the immediate neighbouring nodes of a peer in the network and adds them to a routing table it creates. These neighbours, also assumed to have OLSR, can be multipoint relays (MPRs) who perform a forwarding operation for the peer.

An MPR forwards packets to either the next MPR or to the destination node. When an MPR is no longer a neighbour, it is either further away than one hop or out of the network entirely. Although it is not necessary for a peer to have more than one MPR, it can be useful to have more than one, especially when an MPR is out of reach. An entire network broadcast of a message is more efficient when a peer has more than one MPR.

Under this protocol, nodes use two processes to maintain the routing information: neighbour sensing and topology discovery. The neighbour sensing process consists of a peer using “HELLO” messages to indicate to its neighbours that it has arrived or when the node is turned on. The neighbours use this information to determine whether to be an MPR for the sender or not.

The “HELLO” message includes and updates the state of each neighbouring link on the table. In the topology discovery process, the peer broadcasts the link state

to all its neighbours, who then forward it to all their MPRs. Therefore, the peer is capable of generating the current picture of the entire network topology.

A peer also maintains information about the neighbours that have selected it as an MPR. This set is called the Multipoint Relay Selector (MS) set of a node. A peer informs other nodes about its preference to be an MPR by stating a number in the range from 0 (never) to 7 (always) in its "HELLO" messages.

A property of a well-connected (mesh) ad hoc network is that all nodes can reach each other through a series of available MPRs, and that no network partitioning is established. An MPR flooding method is used for distributing link state information - the status of the links in the network. The route from the source to the destination is calculated such that it is a sequence of hops through the MPRs. Nodes that are not in the MS set of a particular peer do not forward traffic through the peer.

2.3.5 Peer-to-peer connection in Ad hoc network

A Peer- to –peer network may be defined as an application layer overlay (network) in which all entities are equal and all contribute some of their resources, so that each entity (peer) is both a content requestor and a content provider.

This definition makes some participating nodes both a router and a server. The word "peer" means the nodes are equal. In essence, Peer to peer means "an equal communicating with another equal". The importance of the definition lies in the

word “equal”, as it implies that no distinction theoretically exists between the entities that make up the network

Each peer is therefore analogous to both a client and a server, which we define as a node for the purposes of this work.

2.3.6 Packet Transmission in mobile Ad hoc communication.

In MANETS, Packet transmission is impaired by radio link fluctuations. An enhanced channel aware version of ad hoc on demand version (AODV) was introduced by Xiagin (Chen et al, 2011). The channel aware version of (AOD) uses the channel average non-fading duration as a routing metric to select stable links for path detection. it uses a pre-emptive hand off strategy to maintain reliable connections by exploiting channel state information.

Using similar information, paths will be unused when they become available again, rather than being not needed. This Protocol offers a dual altack for avoiding unnecessary route discoveries. The path failures leading to handoff are forecast. Then it brings paths back into play when they are again accessible, rather than simply discarding them at the first sign of a fade.

Additionally, similar information is required to forecast path failure for improving efficiency.

2.3.7 Mobility of Nodes as it affects Routing in Mobile Ad hoc Network.

In mobile ad hoc network, there are numerous applications in which mobile user's shares information, for example, collaborative rescue operations at a disaster site and trade of word-of-mouth information in a shopping mall. For such applications, enhancing data availability is a momentous issues and various studies have been conducted with this intention.

Takahiro quantified the influences of mobility patterns of data availability from different viewpoints. (Hara, 2010). It does not work of single application of protocol but the work proposes and quantifies several metrics that influence data availability.

Johnson and D. Maltz specified the operation of Dynamic sources routing protocol for routing unicast internet protocol Version four (IPV4) packets (Maltz, 2007).

The Dynamic source Routing protocol is a simple and well- organized routing protocol especially for utilization in multi-hop wireless ad hoc networks of mobile nodes. It permits the network to be entirely self-organizing and self-configuring, without the requirement for any existing network infrastructure or management. The protocol is self-possessed of the two main mechanisms such as Route detection and Route Maintenance, which work jointly to permit nodes to discover and maintain routes to random destinations in the ad hoc network. All

features of the protocol operate completely by permitting the packet overhead of Dynamic source Routing to scale routinely.

Lyudmila considered self localization problem of Mobile nodes in view of the temporal correlation in the measurement of noise (Mihaylova et al, 2011).

In this technique, node mobility is modeled as a linear system determined through a discrete-time command markov process, while the measurement models are non linear and require a reliable non-linear estimation method.

Because of the fact that the control process of the mobile node is unidentified, node mobility is modeled with manifold acceleration modes. The non-linear estimation techniques can integrate physical constraints and possibly communication among mobile nodes in the form of supplementary measurements.

Feng Li introduces the uncertainty model which reflects to the nodes confidence in terms of sufficiency of its precedent experience, and learns how the compilation of trust information affects uncertainty in nodes views (Jiewu, 2014).

After defining a method to make and complete the uncertainty in trust views, it exploits mobility. A significant characteristic of MANET is that professionally, it reduces uncertainty and speeds up trust meeting.

Sungwuon investigated Global packet services (GPS) Mobility traces of human mobile nodes and monitored super diffusive performance in all GPS traces. It is typified by a faster-than-linear growth rate of the mean square displacement of a mobile node.

Using random walk formalism, it examines a large amount of access point-based traces and builds up a theoretical framework. The degree of diffusive behaviours of mobile nodes under probably heavy-trailed pause time distribution is measure. It recommended that the diffusive performance of mobile nodes must be correctly captured and considered for the design and comparison study of network protocols.

Routing-Aware Multiple Description coding approach was introduced by Jerry D. and Yiting Liao to support data transmission over MANETS with multiple path transport.

Data transmission over error-prone mobile ad hoc networks is becoming more increasingly important as these networks become more widely deployed. A statistical model is constructed to estimate the packet loss probability of each packet transmitted over the network based on the standard ad hoc routing messages and network parameters. The frame loss probability is estimated and dynamically selects frames to alleviate error propagation caused by the packet losses.

Rezaei and others proposed a theoretical framework for incorporation of random long range routes into wireless ad hoc networking protocols.

Wireless ad hoc routing methods based on this framework and deliver the packet successfully. The proposed result is a randomized network structuring and packet routing framework while distributing the power necessity almost equal over all nodes.

Interestingly, all network formation and routing algorithms are totally decentralized. The packets arriving at a node are routed arbitrarily and separately, based only on the source and the destination positions.

The dispersed nature of the algorithm permits it to be implemented within standard wireless ad hoc communication protocols. It creates the framework for harnessing collective network resources in really large-scale wireless ad hoc networking surroundings.

Shuhui Yang and Jie Wu handled the issues of efficient broadcasting in MANETS using network coding and directional antennas.

By using network coding, the whole number of transmissions could be reduced compared to broadcasting using similar forwarding nodes without coding. They developed the usage of directional antennas to network coding-based broadcasting to further decrease energy consumption(Aboelela,2014).

Mobile Ad hoc networks have been extremely vulnerable to attacks owing to the dynamic nature of the network communications.

Among these attacks, routing attacks have acknowledged significant attention since they could cause the most devastating injury to MANET.

Ziming introduced a risk-aware response method that systematically handles the identified routing attacks. (Zhao et al, 2012). This method is based on an extended Dempster-Shafer mathematical theory of proof by introducing an idea of important metrics to identify the different types of attacks.

Communication in ad hoc network is attained by relaying data along appropriate routes that are dynamically discovered and maintained via collaboration between the nodes. Detection of such routes is a main task, both from efficiency and security point's of view.

The nature of static infrastructure causes several concerns in mobile ad hoc network, such as power utilization, node authentication and secure routing.

NathSalia designed a scheme for power efficient secure routing of data packets in MANET (Himadri, 2012). This technique reduced the computational overhead to make it more energy efficient. As there is no stationary infrastructure, every node in MANET acts as a router that forwards data packets to other nodes, consequently, the selection of effective appropriate, robust and adaptive routing

selection has reduced the amount of network activity for each node required to route a data packet.

In contrast to earlier studies that sought only the shortest route, a trusted route is needed that considers communication reliability, path length for a reliable and possible packet delivery in a MANET. (Wang et al, 2011).

Consequently, security is inherently integrated into the routing protocol where nodes evaluate the trust levels of others based on a set of attributes. The fixed probability of dropping packets adopted in other routing methods is designed based on the attributed similarity.

It gives a recommended method in calculating the degree of similarity between attributes.

Several routing protocols have been proposed in recent years for the probable deployment of MANET's in armed forces, government and commercial applications.

Abusalah estimated routing protocols with a particular focus on security features (Abusalah, 2008).

The protocols very in term of routing methodologies and the information used to create routing decisions. Four delegate routing protocols have been selected for analysis and evaluation together with ad hoc on demand distance Vector routing,

Dynamic source Routing, Optimized link state Routing and Temporally Ordered Routing Algorithm.

The Video multicast protocols were developed for multi-homed mobile terminals as a substitute stream control transmission protocol for moderately reliably multicast services (Back, 2010).

It performs with overlay peer-to-peer video multicast facility in the application layer.

In support of a multi-homed mobile terminal, an error burst might occur when a handover is in the process in the main path switch process.

The key problem concerned in this protocol is the ability to forecast packet drop. If the packet is misplaced, it retransmits the misplaced packets as soon as a mobile terminal performs switching process.

Yuanguo developed a multi-channel token ring media Central protocol for inter-vehicle communications. During adaptive ring coordination and channel scheduling, vehicles are separately organized into multiple rings operating on dissimilar services channels.

Based on the multi-channel ring arrangement, emergency messages will be disseminated with a low delay. By the token based data exchange protocol, the network throughput is further enhanced for non-safety multimedia application.

The methodical method is developed to assess the performance in terms of the average full ring delay, emergency message delay and ring throughput.

T. Bheemarjuna presented a new multi-path routing protocol that undertakes the look-alike issues of reliability (protection against failures of multiple paths) and security, while ensuring smallest amount of data redundancy. The reliability and security requirements are specified by a user and are connected to the parameters of the protocol adaptively (Paszto el al,2010).

A success likelihood function is related to every link, which could be controlled by power and rate allocation. The appearance for the networks stability region is primarily derived where the success function plays a serious role.

Giovanidis .A. considered functions with exact properties which are shown to be satisfied for different expressions of the success probability related to dissimilar modulation and coding schemes as well as outage measures (Stanczak, 2011). A network utility maximization problem with stability constraints is additionally control and scheduling the power allocation.

Beneath the convinced assumptions, the latter is relaxed to a simpler form. This allows the application of super modular game theory and the algorithmic approach is adapted to include the family of success functions of interest.

The dynamic characteristics of wireless networks and stringent quality of services requirements in applications of mobile ad hoc networks have identified

challenges for providing quality of services guarantees for real-time communication in such a wireless environment. Quality of service routing protocols can decisively contribute to the quality provision of network systems.

Jinging deployed an efficient Cluster-Based Routing protocol for real-time multimedia streaming in mobile ad hoc networks. This mechanism contributes to reduce route overhead and to increase the decodable ratio of video frame at the application layer as well.

2.3.8 Path selection in mobile ad hoc networks.

Bouk suggested a gateway selection scheme that considered multiple quality of service path parameters for instance path availability period, available capacity and latency, to choose a potential gateway node (Latha et al, 2015). It progresses the path accessibility computation accuracy and introduced a feedback system to updated path dynamics to the traffic source node. Then an efficient method to propagate quality of service parameters is suggested in the proposed scheme.

Gateway selection scheme improves throughput and packet delivery ratio with less per mode power utilization. It also develops the end-to-end delay compared to single quality of service path parameters gateway selection schemes. Additionally, by considering weighting factors to gateway selection parameters, the weighting factors develop the throughput and end-to-end delay compared to the conventional schemes.

In mobile ad hoc networks, Hierarchical architecture and distributed approaches are more realistic than flat architecture and central approaches.

Ei Hajj proposed a group of protocols that achieved a distributed planning and routing scheme for MANETs. The planned suite, which is composed of three protocols, presents scalability and extends network lifetime.

The primary protocol, specifically, the fast distributed linked dominating set, builds the Virtual backbone by designing a quick distributed Hierarchical algorithm that finds a linked dominating set in the network. The built Virtual backbone takes into account the nodes limited energy, mobility, and traffic pattern (Basant et al,2014).

MANET is a compilation of wireless mobile computers forming a temporary network without any fixed infrastructure or wired backbone.

Topological alteration in MANET frequently renders routing paths not viable. An appropriate technique for addressing this problem is to improve the diversity of paths between the source and destination. Nevertheless, multipath routing is a demanding task.

Specifically, the correlation between the failures of the paths in a path set must be as small as possible. Rambling path sets need the multiple paths to be link-disjoint or node- disjoint through selecting an optimal path set is a total difficult.

Artificial neural networks have been proposed as computational tools to resolve constrained optimization troubles. The utilization of Hopfield neural network as a path set choice algorithm is explored.

While this algorithm produces a set of backup paths with much privileged reliability, it is helpful for MANET's.

Sheikhan – M. used link expiration time between two nodes to estimates link reliability (Hemmati, 2011). In this method node disjoint and link-disjoint path sets will be found concurrently with route discovery algorithm. Consequently, if someone wants to discover both node- disjoint and link-disjoint path sets, there is no need to submit extra control messages, like overhead, to the MANET.

Cooperative communications can considerably improve transmission reliability and bandwidth effectiveness in wireless networks through many upper layer aspects of cooperative communicative value for further investigations.

Quansheing investigated its impacts on network topology and network capacity, which is determined by large aspects such as physical layer ability, interference and path extent. This is because cooperative communications improve physically layer capacity and relay selections impacts on network topology. Authors suggested a capacity optimized cooperative topology control scheme for mobile ad hoc network with cooperative communications.

MANET offers a resource constrained dynamic environment and initiates new aspects to dependability thus affecting reliability of the services provided by the mobile Agent based system organized in MANET. Mobile Agent based system on MANET can be more reliable if the agents are needed to share information and learn about the fundamental conditions.

A basic issue arising in mobile ad hoc networks is the collection of the optimal path between any two nodes. A technique that has been advocated to progress routing efficiency and to choose the most stable path so as to decrease the latency and the overhead because of route reconstruction.

Carofiglio studied both the availability and the duration likelihood of a routing path that is subject to link failures initiated by node mobility.

2.3.9 Multipath routing in wireless ad hock networks

Multipath routing is effectual in wireless ad hock networks, because connectivity along multiple paths is less likely to be broken.

Zakhor .A. suggested a multipath extension to dynamic source routing to hold multipath video communication over wireless ad hoc networks. The suggested scheme is compared with others fir interactive video applications. MANET's comprise a collection of wireless mobile nodes which dynamically trade data among themselves without the reliance on an unchanging base station ad hoc network are classically distinguished by their restricted power, processing and

memory resources with a high degree of node mobility. Therefore, routing is a critical issue to the design of a MANET.

Muceller specifically examined the issues of multipath routing in MANETs. Multipath routing allows the organization of multiple paths between a single source and single destination node. It is classically proposed in order to enlarge the reliability of data transmission or to offer load balancing in which load balancing is of special significance in MANET's because of limited bandwidth between the nodes. The application of multiple routing support application constraints, for example, reliability load balancing, power conservation and quality of service(Politis et al,2012).

Since mobile nodes have limited battery power, it is consequently very important to use energy in MANET professionally.

Because of bandwidth constraints and dynamic topology of mobile ad hoc networks, multipath supported routing is a very significant research issue.

Baolin Marshaled a network coding-based on demand multipath Routing algorithm in MANET. It is typically proposed in order to enhance the reliability of data transmission or to offer load balancing (Sun et al, 2012).

Obaidat .M. scheduled a novel multipath routing protocol for MANET's. The protocol is an alternative of the single path Ad hoc on demand Vector routing

protocol. The multipath routing protocol found node-disjoint paths that have the buck delays based on the interaction of many factors from dissimilar layers.

Further delay aware MANET's routing protocols not consider the projected involvement of the source node that is requesting a path into the whole network load.

Friend based ad hoc routing using challenges to establish an algorithm that offers secure routing in mobile ad hoc networks.

Dhurandher proposed the scheme above which has been drawn from a network of friends in real life situations. The algorithm works by sending challenges and sharing friend lists to offer a list of trusted nodes to the source node through which data broadcast lastly takes place. The nodes in the friend list are esteemed on the basis of the amount of data broadcast they accomplish and their friendship with other nodes in the network. The report of friendship of a node with other nodes in the network is obtained through the share your friends process which is a periodic event in the network.

As a consequence of this scheme of operation, the network is able to efficiently isolate the malicious nodes which are left with no role to play in the ad hoc network.

2.3.10 General Characteristics of Routing Technique

Routing in Ad hoc Networks: Routing is the process of moving packet of data from source to destination. It refers to establishing the routes that data packets take on their way to a particular destination.

Communication between non-neighbouring nodes in an ad hoc network requires the use of routing protocols or techniques so that multi-hop paths may be discovered and utilized. (Achana, 2016).

Below are some of the features of Ad hoc routing protocols:

a. Support for dynamic network topologies including the ability of path set up for nodes that move randomly and rapidly.

b. Support for bandwidth and channel constraint including path loss, interference, noise and fading.

c. Support for power constraints including optimization for power conservation for calculation of paths and processing routing information. Since the nodes are mobile, operation is typically battery dependent and hence the available power is exhaustible.

d. Support for security including secure exchange of routing information with trusted neighbours. A wireless network is prone to security threats because an intruder does not requires physical attachment to the network. Routing protocols must exchange information only with trusted nodes.

The challenges that these four features pose, coupled with the fundamental importance associated with routing protocols for communication between non-neighbouring nodes, has resulted in a situation whereby routing is the single most active area of ad hoc networking research in academia.

2.3.11 The parameters responsible for the performance of any routing protocol

Here, both the quantitative and qualitative metrics of assessing/evaluating the performance of any routing protocol were considered.

Parameters that define a networking context that should be considered during protocol design, simulation and comparison include:

a. Network Size: Measured as the number of nodes.

b. Network Connectivity: The average degree of a node (i.e. the average number of neighbours of a node

c. Topological Rate of Change: The rate with which a network's topology is changing

d. Link Capacity: Effective link speed measured in bits/ second after accounting for losses due to multiple access, coding framing, etc.

e. Fraction of Unidirectional Links: This shows the measure of how effectively a protocol performs as a result of the presence of unidirectional links.

To operate efficiently in a mobile networking context, a protocol should be designed and deployed with an expected networking context firmly in mind. Judging the merit of a routing protocols design requires metrics both qualitative and quantitative, with which to scope and measure its suitability and performance. These metrics should be independent of any given routing protocol.

The three important performance metrics of any routing protocol are throughput (in BPS), end to end delay (in seconds) and packet delivery ratio (in percentage %). The parameters here can be classified as both quantitative and qualitative

a. End-to-end data throughput and Delay: It is worth to note that statistical measure of data routing performance (e.g. means variance, distribution) are important. These are the measures of routing protocol effectiveness that is how well it does its job as measured from the external perspective of other protocols that make use of routing.

b. Efficiency: If data routing effectiveness is the external measure of a protocol's performance, efficiency then is the measure of its effectiveness.

c. Average number of data bits transmitted per data bit delivered: This can be thought of as a measure of the efficiency of delivery data within the network.

Qualitative metrics for assessing/evaluating the performance of any routing protocol include:

a. Demand-based operation: Instead of assuming uniform traffic distribution within the network (and maintaining routing between all node at all times), adopting to a varying traffic pattern on a demand or as needed basis will utilize network resources more efficiently.

b. Sleep period operation: As a result of power conservation, or some other need to be inactive, some nodes of a MANET may stop transmitting and/or receiving (even receiving requires power) for arbitrary time periods. A routing protocol should be able to accommodate such sleep periods without overly adverse consequences.

Mobile ad hoc networks have established their efficiency in the deployment for number of fields, but they are highly affected by poor routing techniques.

Unreliability of the wireless medium and the dynamic topology due to nodes mobility or failure result in frequent communication failures, and high delays for path re-establishments. The shared wireless channels have a significant impact on the performance of multi-path routing.

2.4 Summary of the Review

Many of the routing techniques used by different scholars introduce flooding into the system in an attempt to determine the shortest transmission path. Some of them also send updates to the network at regular interval regardless of whether there is a change on the network or not.

Also, for nodes to run a routing technique like Open Short Path First (OSPF), lots of resources must be dedicated to the process which makes it cost intensive. Many of the routing techniques discussed makes use of different algorithms in calculating or determining the shortest transmission paths, some of these algorithms include: Ant Colony algorithm, Genetic algorithm, Classical algorithm, Quantum search algorithm etc., and these algorithms does not make use of some metrics that could be generated from the network characteristics.

The several failures in communication experienced or witnessed in mobile ad hoc network are mostly due to unreliable communication link as majority of the delays are developed during the process of re-establishment of the failed path.

2.5 Research Gap

Many scholars or researchers have carried out research on how to improve the performance of mobile ad hoc networks using different routing techniques, though some made tremendous progress, but could not come up or develop a clear model or algorithm that could respond fast to network changes with minimum or lesser computation time and also take into account the metrics (e.g hop counts, delay, bandwidth etc) that could be generated from the network characteristics, which could be useful in determining the shortest path of transmission, considering the fact that ad hoc network does not operate on a fixed or assigned bandwidth.

MATERIALS AND METHOD

3.1 Materials

The materials used in this work includes: Laptop Computers, Personal digital Assistant (PDA),4-port wireless Routers, Microsoft SQL Software, Cisco packet tracer software, Hyper V. software, Matlab software.

3.2 Methodology

Performance improvement of a mobile ad hoc network is a method of analyzing performance problems of mobile ad hoc networks and setting up systems to ensure good performance.

Quantitative methodological approach was adopted in this research work using Bandwidth estimation and path selection model.

Enhanced interior Gateway routing protocol is a routing technique that work with diffuse update algorithm in calculating the shortest transmission path without much delay.

This technique is very fast in carrying out its routing operation, such that, if there is network change, it does not take time for the nodes involved to update themselves because it has a backup route (feasible successor) and primary path (main path) for its data transmission.

Routing is an Umbrella term for the set of protocols that determine the shortest path for sending the data over the network.

Router has a property called metric (distance), metric is also called hop count. In case of selecting the shortest path, the router selects the path with lowest metric (hop count)

Routing can be done in two ways namely:

* Static Routing: This is the manual selection of path in a router

* Dynamic Routing: This is the automatic selection of path on the basis of a routing protocol (E.g RIP, OSPF and EIGRP, etc). Dynamic routing is efficient than static Routing because it automatically adopts the topological changes that happens in the network. It is done through protocols called routing protocols.

Types of dynamic routing (IGRP) protocol

i. Interior Gateway Routing protocol (IGRP): These are the dynamic routing protocols that run within an autonomous system. E.g. RIP, OSPF, and EIGRP

ii. Exterior Gateway Routing protocol (EGRP): This is used for communication between two or more autonomous systems. E.g Boarder Gateway protocol BGP.

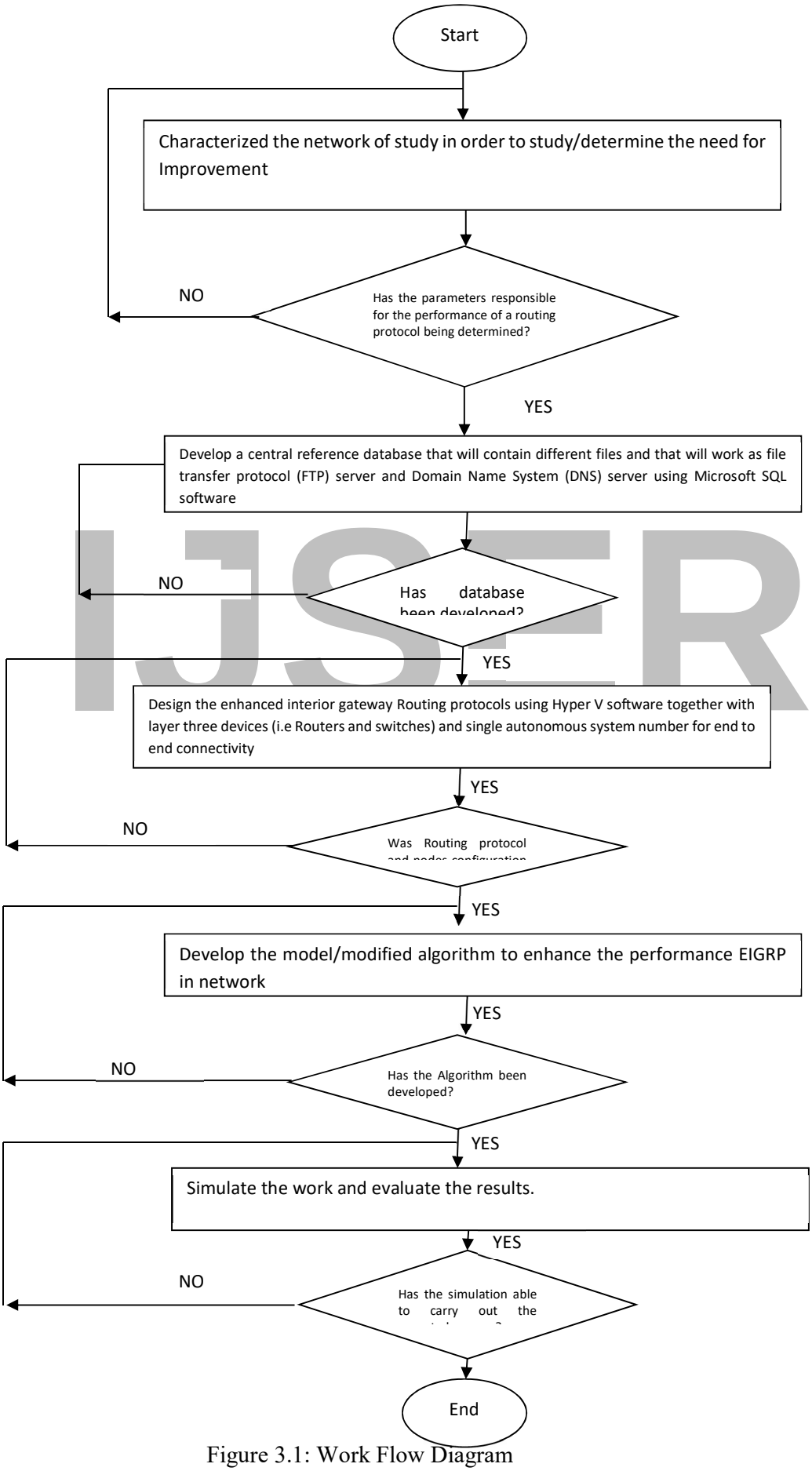

Figure 3.1: Work Flow Diagram

3.3 Enhanced Interior Gateway Routing Protocol

It is a routing protocol that uses metrics in the same way as Internal Gateway Routing protocol (IGRP). It uses a composite metric much like IGRP; except that it is modified by a multipler of 256. This routing technique is very fast in carrying out its routing operation, such that if there is network change, it does not take time for the nodes involved to update themselves because it has a back up route (feasible successor) and primary path (main path) for its data transmission.

This technique is also regarded as an enhanced (IGRP) due to its rapid convenience tendency and loop-free guaranteed at all times.

This research work will adopt Bandwidth estimation and path selection model.

Technical Overview of EIGRP

EIGRP offers many advantages over other routing protocols, these include:

* Support Variable- length subnet masking (VLSM). EIGRP is a classless routing protocol and carries the subnet mask of the route in its update.

* Fast or rapid convergence. Through the use of feasible successors, defined by diffuse update algorithm (DUAL), EIRGP is capable of preselecting the next best path to a destination. This allows for very fast convergence upon a link failure.

* Low Central Processing Unit (CPU) utilization. In the event of normal operation, only “hellos and partial updates are sent across a link. Routing updates are not flooded and processes only periodically.

* Incremental updates: EIGRP does not send a full routing update, it sends only information about the changed routes.

* Easy configuration: EIGRP supports hierarchical network design, but it does not require the strict configuration guidelines.

* Automatic route summarization: EIGRP always performs automatic summarization on major bit boundaries

3.4 Characterization of an Ad Hoc Network

The performance of an ad hoc network was characterized in order to determine the need for improvement. Bandwidth estimation and path selection model were adopted. In the characterization, Bandwidth estimation and path selection model were used to evaluate the performance of an existing network of Worldwide Net Communication Limited in the areas of total delay and minimum link bandwidth. In this evaluation, bandwidths of different values were assumed and assigned to different transmission paths with the configured delay in order to determine the EIGRP metrics (i.e the paths with minimum and maximum delay metrics with their corresponding), and the least delay was discovered to be above the threshold

giving by Nigerian Communication Commission of ≤ 5ms. The results of the characterization are shown in table 4.2 and 4.5 respectively.

Factors that affect the performance of ad hoc network includes

* Latency (Delay)

* Routing Protocol

* Throughput

* Mobility of the nodes

* Packet loss

* Transmission Range

* Size of Network

* Traffic Intensity

* Noise

*Bandwidth

It will also help in carrying out a comparative and in-depth analysis of the performance metrics using the available data and the algorithm (diffuse update Algorithm) that calculates the shortest transmission path for Enhanced Gateway Routing technique, in order to determine the need for improvement.

Ad Hoc network has so many factors that affect its performance but due to time and financial constraints, only few factors, which include: Delay, Routing protocol, size of Network, Throughput and Bandwidth.

End-to-End Delay: This is the sum of the node delay at each node + link delay at each link on the path.

$$\frac{\sum CBRsenttime - CBRreceivetime}{\sum CBRreceived} \quad (3.1)$$

* Throughput: is a measure of how fast one can actually send data through a network. It is the quantity of data sent across the network. Throughput and PDR are generally directly proportional to each other.

Throughput is the total size of packets received at destination nodes at a time which is measured in Kbps (Kilo bits per second).

* Packet Delivery Ratio (PDR): This is the ratio of data packets delivered to the destination generated by CBR, i.e.

$$PDR(\%) = \frac{\sum_i^n CBRreceived}{\sum_i^n CBRsent} \times 100 \quad (3.2)$$

i.e. PDR can be described as the ratio of data packet that are actually received at the receiver end to those which were originally sent by the sender. It is simply the ratio of number of packets received at the destination to the number of packets sent from the source.

* Loss Pack Ratio (LPR): This is the ratio of the number of packets that never reached the destination to the number of packets originated by the source.

CBR (Constant Bit Rate): This means consistent bit rate in traffic that are supplied to the network. In CBR data packets are sent with fixed size and fixed interval between each data packets.

* Routing: This is the ratio of routing protocol to the total number of packets generated by the source.

$$i.e \frac{\sum_i^n RoutingPackets}{\sum_i^n CBRreceived} \quad (3.3)$$

Evaluating the factors that affect the performance of ad hoc network of interest using EIGRP metrics algorithm.

The major factors used as EIGRP metrics in evaluating the performance of ad hoc networks are throughput, delay and Bandwidth, but throughput is majorly dependent on bandwidth in transmission of data in ad hoc network, so the evaluation be focused on bandwidth and delay.

EIGRP uses the minimum bandwidth on the path to a destination network and the total delay to compute routing metric. The bandwidth and delay metrics are determined from values configured on the interfaces of routers in the path to the destination network.

EIGRP calculates the total metric by scaling the bandwidth and delay metrics. The formula below can be by EIGRP to scale the bandwidth.

Bandwidth = (10000000/bandwidth) [i] x 256 (3.4)

Where bandwidth [i] is the least bandwidth of all outgoing interfaces on the routers to the destination. If BW [i]m is considered to be the minimum scaled bandwidth for outgoing interface i, then;

BW [i]m = minimum (BW[i] (3.5)

EIGRP also uses the following formula to scale the delay:

Delay = delay [i] x 256 (3.6)

Where delay [i] is the sum of the delays configured on the interfaces, on the router to the destination network, in tens of microseconds.

EIGRP uses the following scaled values and a multiplier of 256 to determine the total metric for the network.

$$\text{Metric} = \left[\frac{[K1 \times \text{bandwidth}] + [k2 \times \text{bandwidth}]}{[256 - \text{load}] + [K3 \times \text{delay}]} + \frac{k5}{[\text{Reliability} +}\right] \times 256 \quad (3.7)$$

Which is also known as EIGRP total delay metric [EIGRP TDM] Note, the values of k is determined by the user to produce different routing behaviours, and a mismatched k values prevents neighbours relationship between nodes from being built and can cause non convergence of the network if network changes occur. K is user-defined constant

The default values for the various values of k are;

$K_1=1$, $k_2=k_3=k_4=k_5= 0$

So by default, $EIGRP_{TDM}$ can be simplified further as;

$ETGRP_{TDM}$ = [bandwidth + delay] X 256 [3.8]

$$Bandwidith = \frac{10^7}{Scaledbandwidthusedforpathselection} \quad (3.9)$$

If we consider the effective bandwidth for path selection in the existing protocol as Bandwidth existing Aig, then from equation 3.9 and 3.4,

$$BandwidthexistingAig = \frac{10^7}{BWm} \quad (3.10)$$

But since the values are configured on the router interfaces, the expected delay on an interface and the needed bandwidth on a link were configured to suit the network needs.

In other to obtain the total delay along each path, the delays at each hop are summed. The summed delay is the link delay and is usually used by the protocol for metric calculation.

However, this delay comprised of the processing delay, propagation delay, transmission delay and queuing delay.

Hence, the total delay, [DT] can be expressed as:

$D_T = PG_d + PC_d + T_d + Q_d$ [3.11]

Where PG_d = Propagation delay

[PC_d = Processing delay

T_d = Transmission delay

Q_d = Queuing delay

$$Therefore\ DT = \sum_{i=1}^{N}[PG_d + PC_d + T_d + Q_d \qquad (3.12)$$

Transmission Delay Td: This is the time between the transmission of first bit and last bit of the packet.

It is given by (T_d) =$\frac{L}{R}$ (3.13)

Where

L = size of packet and R = Transmission Rate

Note: If the packet size is fixed, then the time is constant.

Queuing Delay (Q_d) = This is the length of time a packet awaits the interface queue before being sent to the transmit ring.

It depends on numbers and size of packets in the queue, and the queuing methods used.

Q_d = [n-1] L/R [3.14]

Where n = Number of packet

Propagation delay (PG_d) This is the time it takes the packet to move from one end of the link to the other. It depends on the type of media, such as fiber or wireless links.

$PG_d = M/S,$ [3.15]

Where:

M = link distance and S = link speed

Processing Delay (PC_d) This is the time it takes a packet to move from the input interface of the router or layer 3 switches, to the output interface. It depends on switching node, speed of central processing unit, routers architecture, and interface configuration.

$$PC_d = \frac{B_s \times 8}{R} \quad (3.16)$$

Where

B_s = Size of File

$$Delay = \frac{L}{R} + \frac{M}{S} + N\left(\frac{M}{S}\right) + 8\,\frac{(Bs)}{R}$$

Where M = Link distance

N = Number of nodes

Bs = Size of file

S = Link speed L = Packet size

L = Packet size

R = Transmission Rate/Link

: From equation,9,10,11,12,13, 14, 15, and 16 respectively, we have that;

$$EIGRP_{TDM}\ old = 256\left[\frac{10^7}{BW_m} + \frac{L}{R} + \frac{M}{S} + N\frac{M}{S}\ 8\ \frac{[Bs]}{R}\right] \qquad [3.17]$$

In a network with many routers, EIGRP chooses the path with least metric.

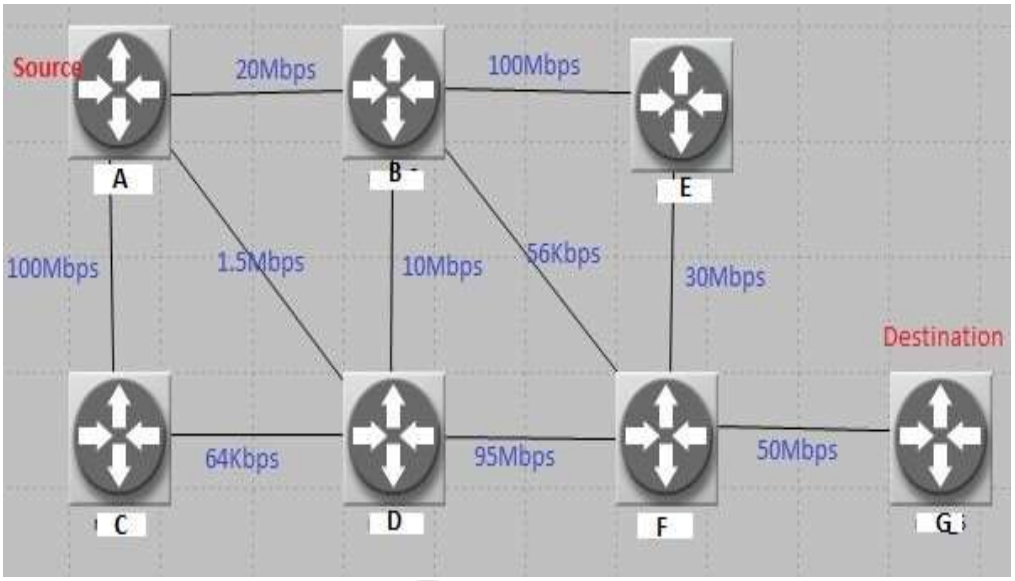

Figure 3.2: Simple Network Configuration for EIGRP performance

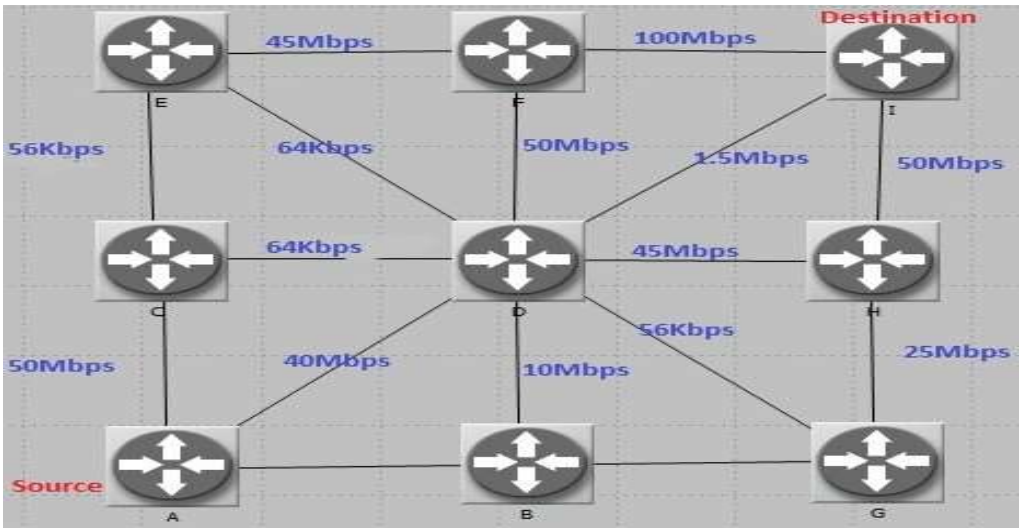

Figure 3.3: Sample of a more Complex Network Configuration for EIGRP performance.

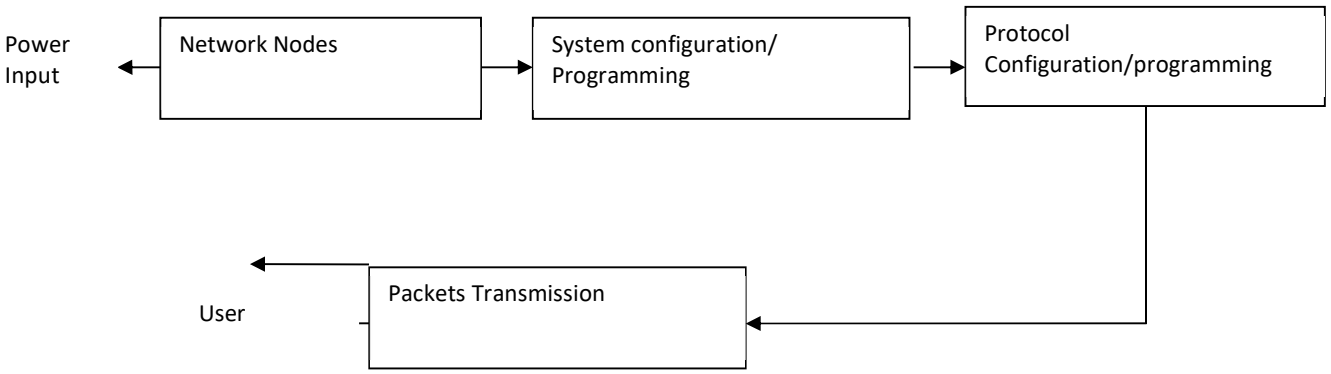

Fig: 3.4: Block diagram of a typical ad-hoc Network

3.5 Developing a central reference database that contain different files and work as file transfer protocol (FTP) sever and Domain Name System (DNS) Sever using Microsoft SQL software.

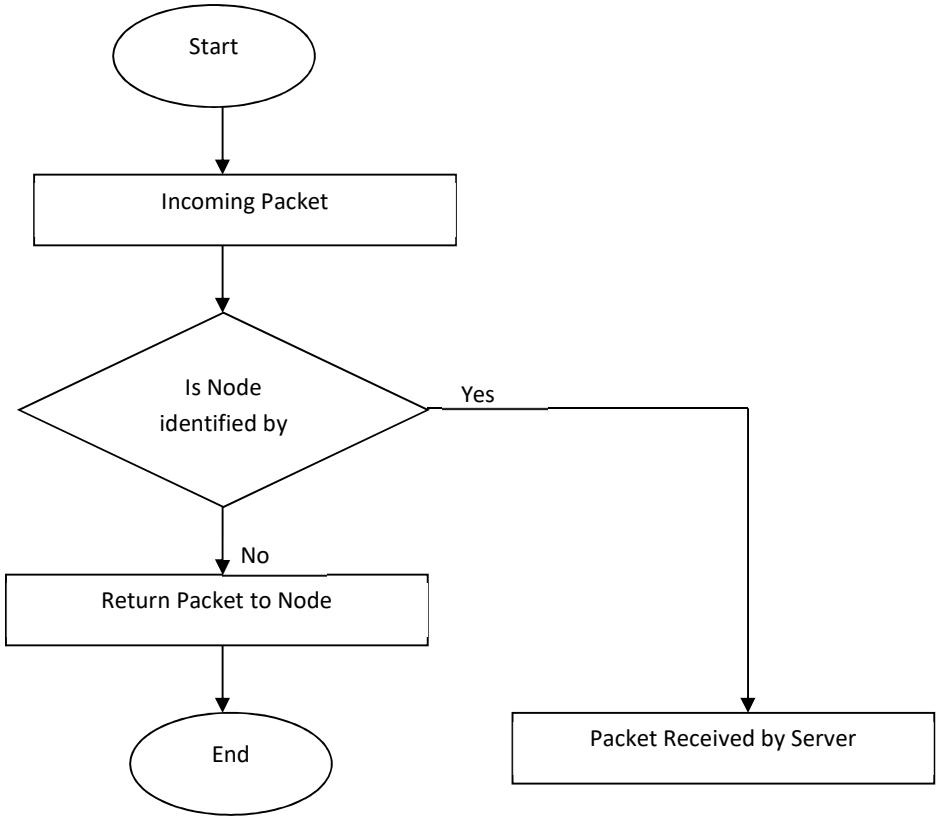

Figure 3.5: Database flow chart

The database is a system that contains the information concerning the functionality of the other nodes on the network. The database was developed using Microsoft SQL server software. In configuring the nodes that constituted the database, the default gateway and subnet mask remain the same for all the nodes, where only the host numbers in the IP address were varied. The Router was also configured to operate in a Dynamic Host Configuration Protocol (DHCP) mode so as to assign IP addresses to the nodes automatically.

IP address 192.168.10.2

Subnet mask 255.255.255.0

Default Gateway 192.168.10.1

The sequel or structured Query language is a domain specific language used in programming and designed for managing data held in a relative database management system or for stream processing in a relational data stream management system.

This was done to enhance easy identification and accessibility of files by the nodes. It also gave room for database updates and the possibility for administrative information exchange with other clients if need be. It will also help to checkmate intruders using their Media Access Control (MAC) address

3.6 To design the Enhanced Interior Gateway Routing Protocols (EIGRP) using Hyper V Software with layer three devices (i.e. Routers and Switches) and single autonomous system number for end to end connectivity.

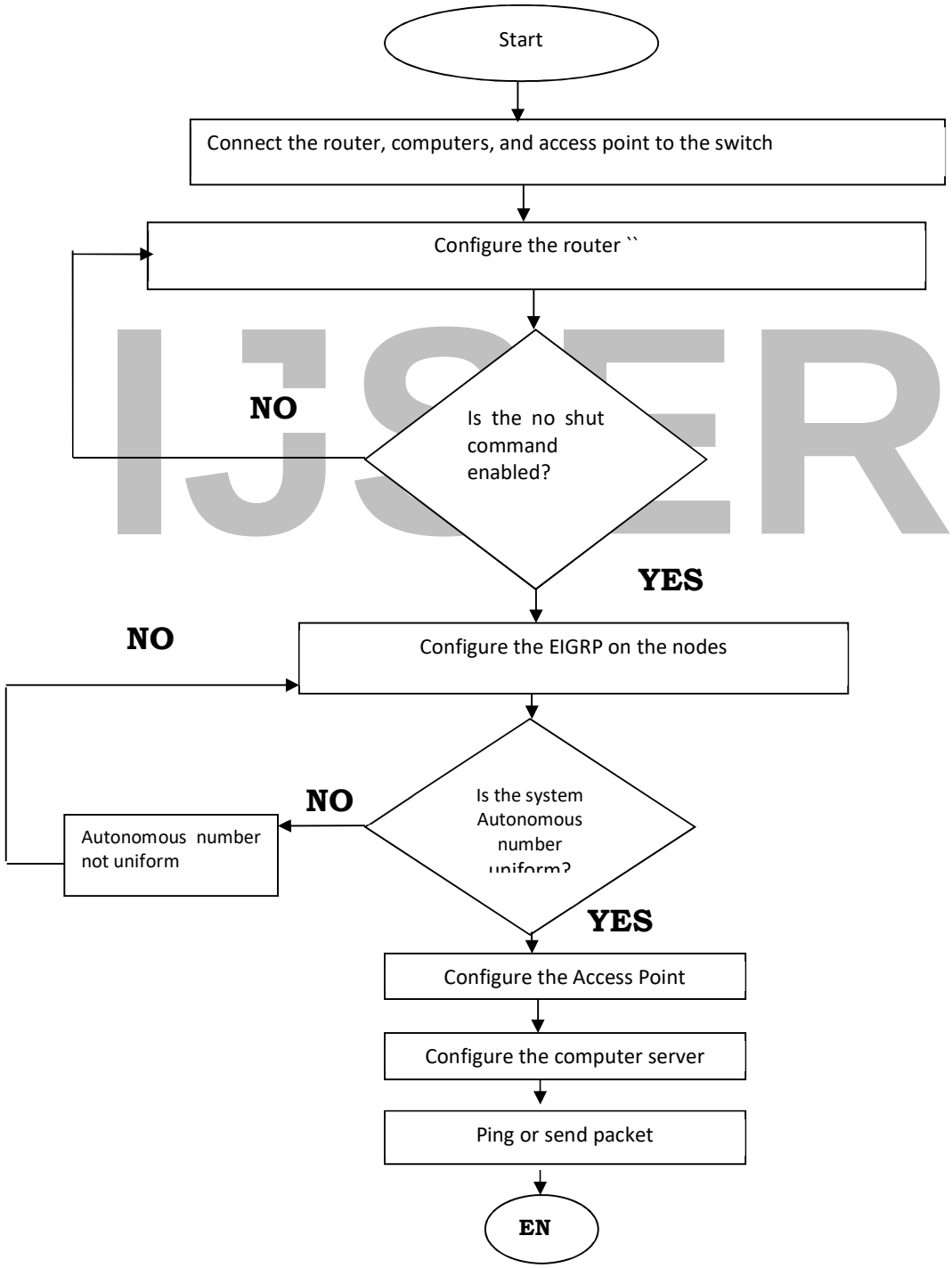

Figure 3. 6 Flow Chart showing the design of Enhanced Interior Gateway Routing Protocols (EIGRP) with layer three devices

ELGRP adds together weighted values of different network link characteristics in order to calculate a metric for evaluating path selection. The characteristics include:

- Delay (measured in Tens of microseconds)
- Throughput (measured in bits per second)
- Reliability (in numbers ranging from 1 to 255; 255 being the most reliable)
- Load (in numbers ranging from 1 to 255; 255 being saturated)

EIGRP has faster convergence and fewer networks overhead, since it uses incremented updates. Another important feature of EIGRP is routing loop free topology, and route summarization.

Terms Related with Enhanced Interior Gateway Routing Protocol (EIGRP)

DUAL: This stands for diffused update Algorithm used by EIGRP to calculate its shortest path.

NEIGHBOUR TABLE: This is the table that contains a list of the EIGRP neighbours.

TOPOLOGY TABLE: This contains a list of all destination and paths the EIGRP router learned. There is a separate topology table for each routed protocol. This stores the alternative routes for packet transmission.

SUCCESSOR: This is the best path to reach destination within the topology table.

FEASIBLE SUCCESSOR: This is the best backup path to reach a destination.

ETHERNET: This is a technology introduced to ensure that packets sent on a network gets to its destination.

Ethernet Evolution includes:

i. **Standard or traditional Ethernet:** This transmits packet at 10MBPS. It uses half duplex mode of transmission. It makes use of a hub and does not segment a LAN system rather it sees the entire network as a single segment unlike the switch.

ii. **Fast Ethernet:** This transmits data at 100 MBPS. It uses both half and full duplex mode of transmission. Half duplex when it is implemented using a Hub and full duplex when it is implemented using a switch or bridge.

iii. **Gigabyte Ethernet:** Transmits data at 1GBPS. Uses duplex mode of transmission. It can be implemented using switch and router.

iv. **10 Gigabyte Ethernet:** Transmits data at 10GBPS. It uses duplex mode of transmission.

The bandwidth used on Ad hoc network is dependent on the switches and routers used on the network. An Ethernet managed switch introduced by IEEE has the ability to share the bandwidth to a computer or computers on the network according to the bandwidth the network cards supposed to be transmitting on the network. Most of the routers and switches comes in different Ethernet category. And for this work, Gigabyte and 10Gigabyte Ethernet were applied and class C internet protocol (IP address) maintained, i.e. the IP address that uses the first three Octets to signify the networks and the remaining Octet for the host).

255. 255. 255. 0 = subnet mask by default.

Note: The highest value of an IP address in decimal form cannot exceed 255 [i.e. eight bits of ones converted to decimal].

Devices/Nodes Configuration Using Enhance Interior Gateway Routing Protocol (EIGRP)

Router Configuration:

The router configuration was done using hyper V software which usually comes with windows xp operating system, but was embedded in the Cisco packet tracer software used in the design of this work.

The router used in this work was Gigabyte and 10 Gigabyte routers (which shows the rate at which data could be transmitted from one node to another). The router usually has two interfaces by default and was able to see the network in different interface using EIGRP. Each interface of the router represents a particular network. The two interfaces of each of the routers were configured and IP address assigned.

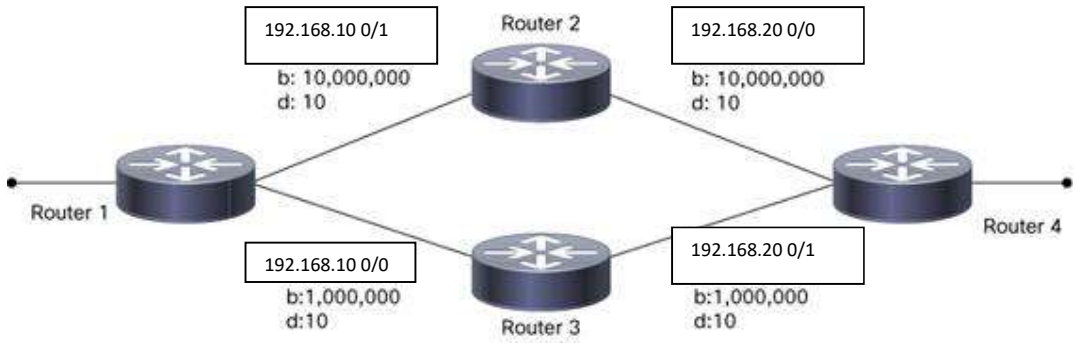

Figure 3.7: Router Configuration

From figure 3.7, EIGRP was used to establish communication between interface 0/1 of R1, 0/1 of R2, 0/0 of R2, 0/1 of R3, 0/0 of R3, 0/1 of R4 and then 0/0 of R4 respectively.

IP addresses (class C) was assigned to the different interfaces of the router followed by subnet mask which must correspond with the IP address used.

Example, at the interface 0/0 of R1, 192.168.10.0 255.255.255.0, was assigned followed by a no shut command. This was because all interfaces of router were shut down by default.

The above configuration was done at the global configuration mode (interface configuration mode) on the hyper V software.

EIGRP configuration:

Before EIGRP could be configured in the routers the following must be done:

- The autonomous system number must be defined [which represents the entity or domain of the EIGRP network).
- Definition/specification of the networks and the router interfaces to be advertised by the router to its neighbours.

NOTE**:** The autonomous system number must be the same in all nodes that has the EIGRP in it, signifying the same domain system.

Router (config) router eigrp 100

Router > # network 192. 168. 10.0

network 192.168.20.0 no shut

The above shows the IP addresses (Class C) of two different networks used in configuring EIGRP, where as the numbers 10 and 20 as used in the configuration denotes the network numbers.

3.7 Modified Shortest Path Algorithm for Enhancement of EIGRP Performance in Ad Hoc Network

Recall that EIGRP uses the minimum bandwidth on the path to a destination network to compute it's routing metric i.e. the EIGRP uses minimum link bandwidth to determine the shortest path and hence to select the routing path. However, using only, the minimum bandwidth deprives the path of its optimal metric values.

Therefore, to obtain optimal metric values, the average bandwidth across a path was considered. This led to the development of the modified shortest path Algorithm.

By assuming (BW_i) to be the average of all the scaled bandwidth for outgoing interfaces i, n as the number of outgoing interfaces, and BW (i) as the scaled bandwidth for outgoing interface i as given in equation (4) then equation (3) can be re-written as:

$$(BW(i)avg = \frac{\sum_{i-1}^{i-n}(BW)(i)}{n} \qquad (3.18)$$

The proposed algorithm (modified shortest path algorithm) uses (BW_i) avg (i.e. the average of all the scaled bandwidth for outgoing interface) for its path selection

From equation (10) and (4), we have;

$$\text{Bandwidth}_{\text{newAig}} = \frac{10^7}{BW[i]avg} \qquad (3.19)$$

Let $\text{EIGRP}_{\text{TDM}}$ for the modified diffuse algorithm for EIGRP be defined as:

$$\text{EIGRP}_{\text{TDMnew}} = [\text{Bandwidth}_{\text{newAig}} + \text{Delay}] \text{ X } 256 \qquad [3.20]$$

Substituting into eqn (17), we have

$$\text{EIGRP}_{\text{TDMNew}} = \left[\frac{10^7}{BW[i]}\right] avg + \text{Delay} \text{] X } 256 =$$

$$256\left(\frac{10^7}{BWavg} + \frac{L}{R} + \frac{M}{S} + N\left(\frac{M}{S}\right) + 8\,\frac{[Bs]}{R}\right) \qquad (3.21)$$

Finally, the enhanced Interior gateway routing protocol [EIGRP] could use two metrics for calculating its shortest path for transmission. The first was EIGRP Total delay metric which was computed based on the value of the minimum scaled bandwidth (BWm) for all the outgoing interface of the router, and the second one was the EIGRP Total delay metric, which was computed based on the value of average of all the scaled bandwidth (BW_{avg}) for all the outgoing interface in the router, and this signifies the modified algorithm for calculating the shortest path of transmission in EIGRP.

3.8: **TO SIMULATE THE WORK AND EVALUATE THE SIMULATION RESULTS**.

By considering the number of hops with the highest frequency (i.e. 4 & 5 hops) in the computations gotten from both the simple and complex network configurations in figures. 3.2 and 3.3 using equation (3.12), (3.17) and (3.21) respectively, and putting the values into MATLAB, the following simulations were carried out.

Simulation One:

Transmission Rate R = 50000000, 43750000, 15389000, 6126600

No. of hops = 4

Link delay = 0.004721, 0.005221, 0.012592, 0.004077

Simulation Two:

Transmission Rate R = 150000, 56000, 64000

No of hops = 4

Link Delay = 0.117887, 3.126221, 2.735596

Simulation Three:

Transmission Rate1 R = 50000000,43750000,15389000,6126600

Transmission Rate2 R = 383000, 3202400

No of hops = 4 and 5

Link delay1(microseconds) = 0.004721, 0.005221, 0.012592, 0.004077

Link delay2(microseconds) = 0.006051, 0.006998

Simulation Four:

Transmission Rate1 R = 150000, 56000, 64000

Transmission Rate2R = 56000, 100000, 560000

No of hops = 4 and 5

Link delay1 = 0.117887, 3.126221, 2.735596

Link delay2 = 3.304792, 0.019721, 3.304792.

Simulation Five:

Link delay = 0.004721, 0.005221, 0.012592,0.004077

No of hops = 4

Packet size(bytes) = 10000, 15000, 20000, 25000

4. RESULT AND DISCUSSION

4.1. The result of the analysis of both the existing EIGRP metrics and the modified algorithm are presented in this section.

This section present parameters and their values for the computation of the results. Table 4.1 details the different paths through which data can be transmitted from source to destination. It also shows minimum bandwidth along each path and the computed average link bandwidths, the different bandwidths are used to calculate EIGRP metrics for selecting the best path. It was assumed that data of 10kb is to be transmitted from source to destination as shown in the Table 4.2: EIGRP metrics are the values from the computation gotten using either the minimum or average bandwidth with configured delay as indicated in equation 3.17 and 3.21.

Table 4.1: The different path through which data can be transmitted from source to destination. It also shows the minimum bandwidth along each path as in Figure 3.2.

Path	No. of Hops	Minimum Bandwidth	Average Bandwidth (total bandwidth from source to destination divided by total number of hops)
A-B-E-F-G	4	20Mbps	50Mbps
A-B-F-G	3	56Kbps	23.35Mbps
A-B-D-F-G	4	10Mbps	43.75Mbps
A-D-F-G	3	1.5Mbps	48.83Mbps
A-D-B-E-F-G	5	1.5Mbps	38.3Mbps
A-D-B-F-G	4	56Kbps	15.38Mbps
A-C-D-F-G	4	64Kbps	61.2Mbps
A-C-D-B-E-F-G	6	64Kbps	48.3Mbps

Table 4.2: The Computed delay and metrics of different paths calculated using minimum link bandwidth. It also shows the computed EIGRP metrics based on the minimum scaled bandwidth as indicated in figure 3.2.

Paths	No. of hops	No. of packets	EIGRP Bandwidth	Delay total (Dt)	EIGRP Metrics
A-B-E-F-G	4	1.5625	7.8125	0.009971	2002.553
A-B-F-G	3	1.5625	2790.179	2.947649	715040.3
A-B-D-F-G	4	1.5625	15.625	0.018721	4004.793
A-D-F-G	3	1.5625	104.1667	0.111221	26695.14
A-D-B-E-F-G	5	1.5625	104.1667	0.124554	26698.55
A-D-B-F-G	4	1.5625	2790.179	3.126221	715086
A-C-D-F-G	4	1.5625	2441.406	2.735596	625700.3
A-C-D-B-E-F-G	6	1.5625	2441.406	3.048096	625780.3

Table 4.3: The computed EIGRP metrics for the modified algorithm (with average link bandwidth) as indicated in Figure 3.2.

Paths	Transmission Rate (R)	No. of Hops	EIGRP Bandwidth	Delay Total (Dt)	EIGRP Metrics
A-B-E-F-G	50000000	4	3.125	0.004721	801.2085
A-B-F-G	23352000	3	6.691076	0.008286	1715.037
A-B-D-F-G	43750000	4	3.571429	0.005221	915.6222
A-D-F-G	4883333.3	3	31.99659	0.035009	8200.089
A-D-B-E-F-G	38300000	5	4.079634	0.006051	1045.935
A-D-B-F-G	15389000	4	10.15336	0.012592	2602.483
A-C-D-F-G	61266000	4	2.550354	0.004077	653.9344
A-C-D-B-E-F-G	48344000	6	3.232045	0.005254	828.7487
A-C-D-B-F-G	32024000	5	4.879153	0.006998	1250.855

Table 4.4: Different paths and their corresponding links in the network as indicated in figure 3.3

Path	No. of Hops	Minimum Bandwidth	Average Bandwidth (total bandwidth from source to destination divided by total number of hops)
A-B-G-H-I	4	1.5Mbps	26.625Mbps
A-B-D-G-H-I	5	56Kbps	17.311Mbps
A-B-D-H-I	4	1.5Mbps	26.625Mbps
A-B-D-I	3	1.5Mbps	4.333Mbps
A-B-D-F-I	4	1.5Mbps	40.375Mbps
A-D-B-G-H-I	5	10Mbps	31Mbps
A-D-G-H-I	4	56Kbps	28.764Mbps
A-D-H-I	3	40Mbps	45Mbps
A-D-I	2	1.5Mbps	20.75Mbps
A-D-F-I	3	40M	63.333Mbps
A-C-D-B-G-H-I	6	64Kbps	27.510Mbps
A-C-D-G-H-I	5	56Kbps	25.024Mbps
A-C-D-H-I	4	64Kbps	36.266Mbps
A-C-D-I	3	64Kbps	17.221Mbps
A-C-D-F-I	4	64Kbps	36.266Mbps
A-C-E-D-B-G-H-I	7	56Kbps	23.588Mbps
A-C-E-D-G-H-I	6	56Kbps	20.862Mbps
A-C-E-D-H-I	5	56Kbps	29.024Mbps
A-C-E-D-I	4	56Kbps	15.405Mbps
A-C-E-D-F-I	5	56Kbps	40.024Mbps
A-C-E-F-I	4	56Kbps	48.764Mbps

Table 4.5: The computed delay and metrics of the different paths calculated using minimum bandwidth. It also shows the computed EIGRP metrics for existing algorithm based on the minimum scaled bandwidth as indicated in figure 3.3.

Paths	Transmission Rate(R)	No. of Hops	EIGRP Bandwidth	Delay (Dt)	EIGRP Metrics
A-B-G-H-I	1500000	4	104.1667	0.117887	26696.8458
A-B-D-G-H-I	56000	5	2790.179	3.304792	715131.741
A-B-D-H-I	1500000	4	104.1667	0.117887	26696.8458
A-B-D-I	1500000	3	104.1667	0.111221	26695.1392
A-B-D-F-I	1500000	4	104.1667	0.117887	26696.8458
A-D-B-G-H-I	10000000	5	15.625	0.019721	4005.0485
A-D-G-H-I	56000	4	2790.179	3.126221	715086.027
A-D-H-I	40000000	3	3.90625	0.005346	1001.3685
A-D-I	1500000	2	104.1667	0.104554	26693.4325
A-D-F-I	40000000	3	3.90625	0.005346	1001.3685
A-C-D-B-G-H-I	64000	6	2441.406	3.048096	625780.313
A-C-D-G-H-I	56000	5	2790.179	3.304792	715131.741
A-C-D-H-I	64000	4	2441.406	2.735596	625700.313
A-C-D-I	64000	3	2441.406	2.579346	625660.313
A-C-D-F-I	64000	4	2441.406	2.735596	625700.313

Table 4.6: The computed EIGRP metrics for the modified EIGRP paths (with average link bandwidth) as shown in figure 3.3.

Paths	Transmission rate(R)	No. of hops	EIGRP Bandwidth	Delay total (Dt)	EIGRP Metrics
A-B-G-H-I	26625000	4	5.868545	0.007793	1504.343
A-B-D-G-H-I	17311200	5	9.025949	0.011907	2313.691
A-B-D-H-I	26625000	4	5.868545	0.007793	1504.343
A-B-D-I	4333333	3	36.0577	0.039298	9240.83
A-B-D-F-I	40375000	4	3.869969	0.005555	992.1342
A-D-B-G-H-I	31000000	5	5.040323	0.007188	1292.163
A-D-G-H-I	28764000	4	5.432137	0.007305	1392.497
A-D-H-I	45000000	3	3.472222	0.004887	890.1401
A-D-I	20750000	2	7.53012	0.008691	1929.936
A-D-F-I	63333333	3	2.467105	0.003826	632.5584
A-C-D-B-G-H-I	27510666.7	6	5.679615	0.008309	1456.109
A-C-D-G-H-I	25024000	5	6.244006	0.008614	1600.671
A-C-D-H-I	36266000	4	4.308443	0.006046	1104.509
A-C-D-I	17221333	3	9.073049	0.010802	2325.466
A-C-D-F-I	36266000	4	4.308443	0.006046	1104.509
A-C-E-D-B-G-H-I	23588571.4	7	6.62397	0.009911	1698.274
A-C-E-D-G-H-I	20862666.7	6	7.489455	0.010568	1920.006
A-C-E-D-H-I	29024000	5	5.383476	0.007595	1380.114
A-C-E-D-I	15405000	4	10.14281	0.012581	2599.78
A-C-E-D-F-I	40024000	5	3.903908	0.005843	1000.896

4.2 FIGURES SHOWING SIMULATION RESULTS

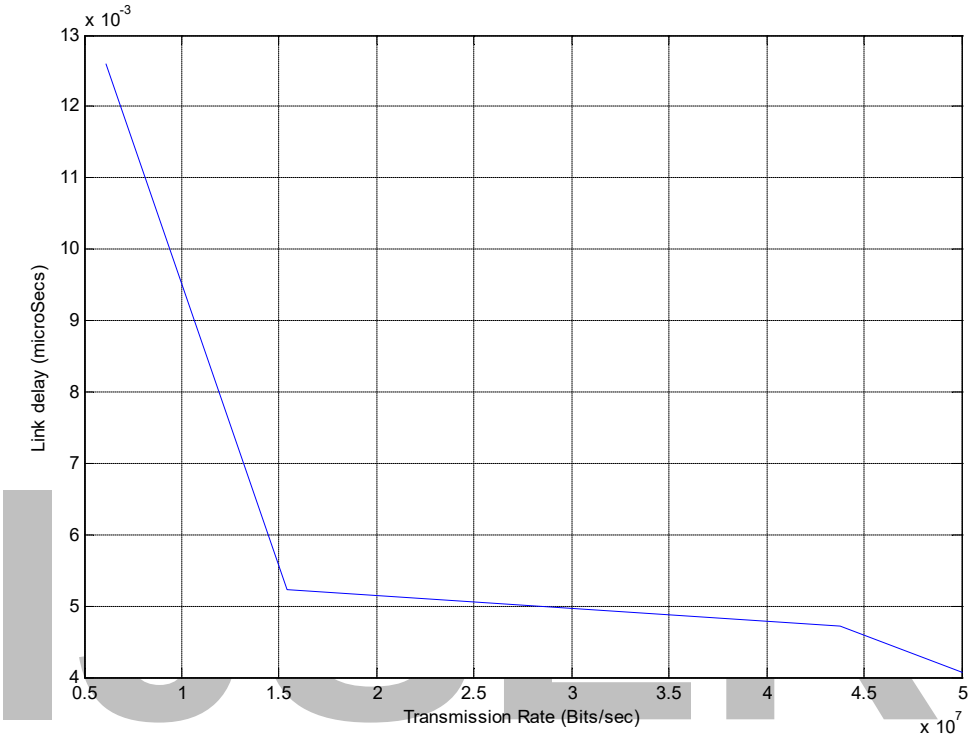

Fig 4.1: Effect of Transmission Rate on link transmission delay for four hops(with average link bandwidth in simple network configuration).

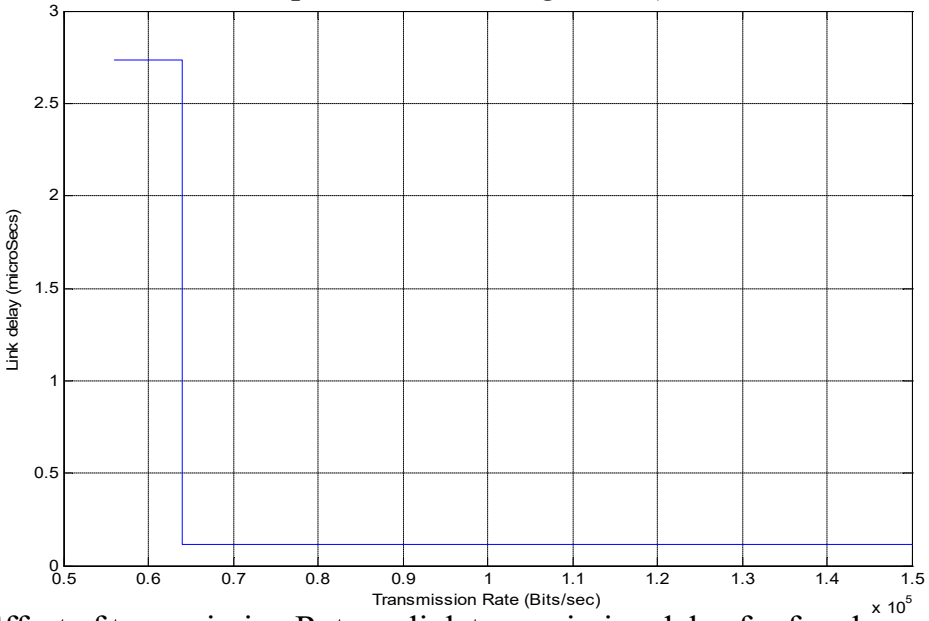

Fig 4.2: Effect of transmission Rate on link transmission delay for four hops (with minimum link bandwidth in complex network configuration).

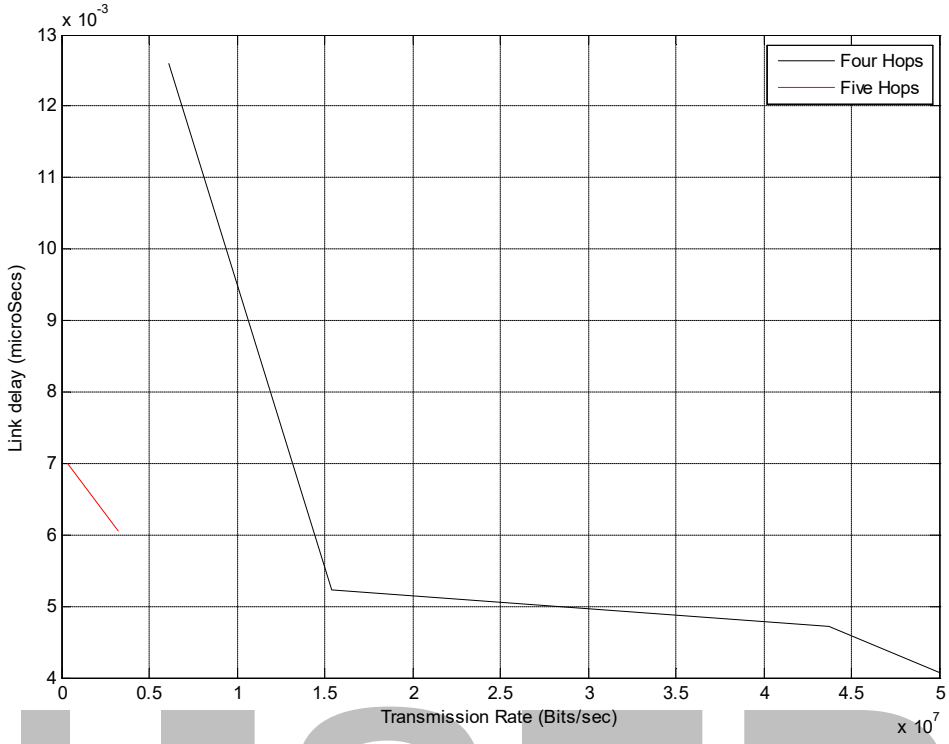

Fig 4.3: Effect of transmission Rate on link transmission delay for four and five hops(with average link bandwidth in simple network configuration).

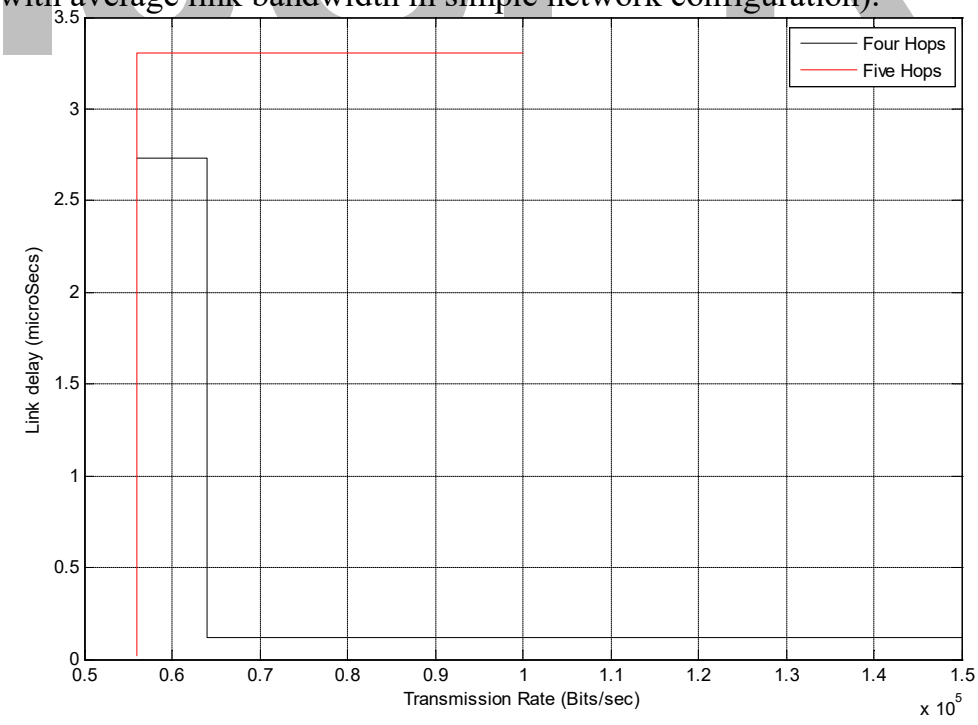

Fig 4.4: Effect of transmission Rate on link transmission delay for four and five hops(with minimum link bandwidth in complex network configuration).

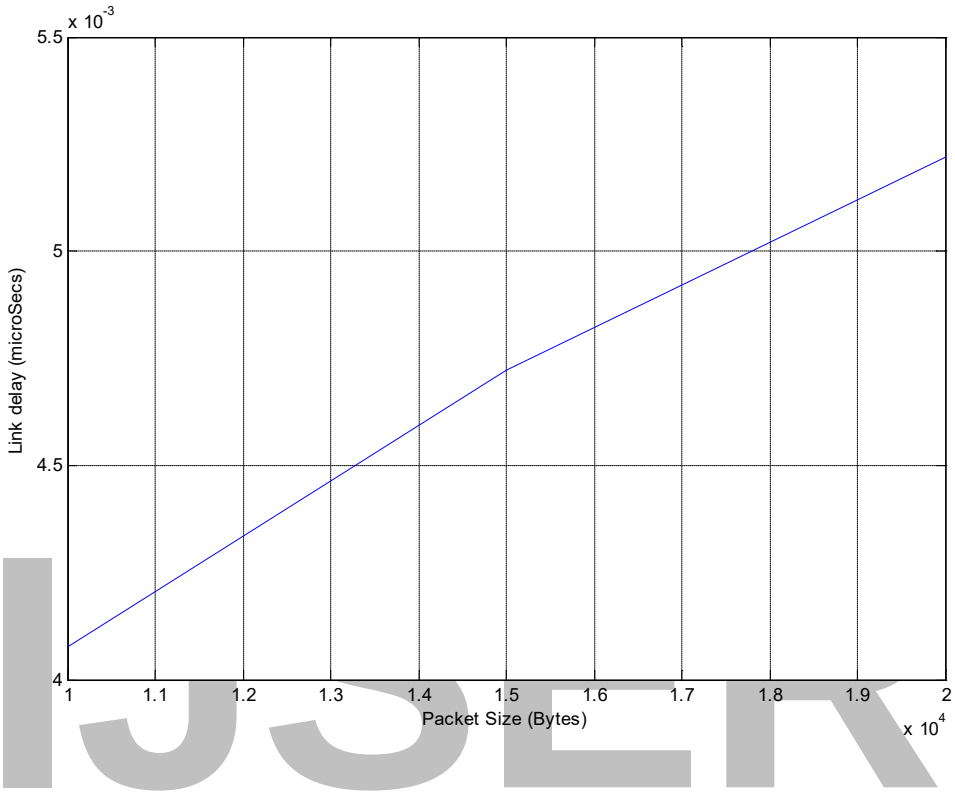

Fig 4.5: Effect of packet size on transmission delay (with average bandwidth in simple network configuration).

4.3: Discussion and Findings based Computed Metrics and Simulation Result

In Table 4.1, the different paths through which data can be transmitted from source to destination were identified. It also shows the minimum bandwidth along each path as indicated in Figure 3.2 and the computed average link bandwidths. The different bandwidths were used to calculate the EIGRP Metrics for selecting the best path. Data of size of 10Kb was transmitted, from source to destination. A higher packet size takes higher time for transmission.

The computed delay and metrics of the different paths were calculated using minimum link bandwidth as shown in Table 4.2. From the table it was deduced that the path with the minimum Metric was path A-BE-F-G with minimum metric value of 2002.553 which is truncated to 2002. This implies that protocol selected the path through A-B-EF-G for routing packets.

Table 4.3 shows the computed delay and Metrics of the different paths calculated using the newly developed algorithm in equation 3.21 (average link bandwidth). From the table it was observed that the path with the minimum Metric is path A-C-D--F-G with minimum metric value of 653.9344 which is truncated to 653. This implies that the protocol selected the path through A-C-D-F-G for routing packets.

It can be deduced from the two scenarios that different paths were chosen by EIGRP for routing packets across the network.

Furthermore, it was observed that the Metric values for both the existing and new formula are not the same; while the minimum metric for the existing formula is 2002, that of the new formula is 653 which is far smaller compared to the existing metric. Also discovered was the delay difference in both the existing and newly developed algorithm. It takes longer time to route packets from source to destination using the existing algorithm than the new one; meaning that the newly developed algorithm also improved the delay.

Table 4.4 identifies the different paths and their corresponding minimum link bandwidth as indicated in Figure 3.3 and average path bandwidths. It also

identifies the diverse paths in the network through which packets can be transmitted from source to destination and their corresponding minimum link bandwidth and computed average path bandwidths. It highlights the number of hops along each path from source to destination. The different bandwidths were used to calculate EIGRP metrics for selecting the best path. It was assumed that data of size 10Kb was transmitted from source to destination as shown in Table 4.4

Table 4.5 shows the computed delay and Metrics of different paths calculated using minimum link bandwidth. From the table, it was observed that two paths have the same delay and minimum bandwidth metric value.

The routes through A-D-H-I and A-D-F-I have equal delay value of 0.005346 and equal metric value of 1001.3685. This implies that the protocol chooses the path through any of these two links with equal metric or may divide the packets through both paths.

Table 4.6 shows the computed delay and Metrics of the different paths calculated using the new algorithm (average path bandwidth). From the table, it was observed that only one path has a minimum metric of 632.5584 as opposed to that of the existing algorithm which saw two paths with same delay and minimum bandwidth metric value. The routes through A-D-H-I was the path with minimum bandwidth. This implies that EIGRP protocol selected the path through A-D-H-I to transmit packets from source to destination. One can say that the newly developed algorithm was more precise than the existing algorithm as observed in

tables 4.3 and 4.6. It was also observed that the values for both delays and metrics for the new algorithm was smaller compared to that of the existing algorithm. Using the two formulas, the metric for the different data sizes larger than 10Kb were computed and the degree of improvement of the newly developed algorithm over the existing one were observed. In Figures 4.1 and 4.2 the effect of packets transmission rate on the total transmission delay for 4 hops was investigated. It was observed that the increase in the rate of transmission resulted in reduced total transmission delay.

This can be explained from the fact that, as the rate of transmission increased, more packets was transmitted and the delay in transmission was reduced and this was more significantly shown or observed in the modified algorithm. In figures 4.3 and 4.4, the effect of packets transmission rate on the total transmission delay for 4 hops and 5 five hops was investigated.

It was observed that the increase in the rate of transmission results in reduced total transmission delay. This can be explained from the fact that, as the rate of transmission increased, more packets was transmitted and the delay in transmission was reduced. Also noted was the fact that with the 5 hops, the delay was higher than that of 4 paths. This concludes that as the number of hops increases, so is the total transmission delay.

Figure 4.5 depicts the effect of packet size on delay for the modified algorithm. As the packet size increases, the transmission delay increases. It can be concluded that, a larger packet size takes a higher time for transmission.

5.0 CONCLUSION, CONTRIBUTION AND RECOMMENDATION

5.1 CONCLUSION

When it comes to determining the quality of service, network performance is crucial. A better routing technique, such as an enhanced interior gateway routing protocol with an improved shortest path algorithm, can dramatically increase the performance of an ad hoc network. The existing EIGRP path algorithm was analyzed, flaws were recognized, and the shortest path algorithm was devised to address the highlighted problems in this research.

The end-to-end delay in the existing shortest path algorithm utilized by several routing protocols is the problem addressed in this research.

To quantitatively represent the performance of the existing algorithm and the performance of the developed algorithm for EIGRP, mathematical expressions were developed.

When compared to the existing shortest path algorithm utilized by other routing protocols, the proposed technique has a shorter end-to-end delay.

5.2 CONTRIBUTION TO KNOWLEDGE

This research and study provides the following contributions.

- Introduces the use of configured delay and bandwidth as metrics for computing the shortest path for data transmission.
- It provides more efficient bandwidth utilization in ad hoc Network.
- It improved the Adhoc Network's security by introducing the usage of the nodes' Media Access Control (MAC) addresses in detecting intruders.

It promotes the use of average link bandwidth on the path to a destination network as a metric in determining the shortest path and selecting the routing path to a destination, guaranteeing that the paths' optimal metric values are used.

5.3 RECOMMENDATION

With the findings, it can be concluded that ad hoc network with improved routing technique could be a good alternative for data communication in the absence of fixed or licensed network operators if some modifications on the system parameters are made. It is on this basis that the following recommendations are made in order to ameliorate the observed defects.

a. Because ad hoc networks do not have a fixed bandwidth allocation, Ethernet switches and routers with a moderate capacity should be used while setting up ad hoc networks.

b. When setting up an ad hoc network employing Enhanced Interior Gateway Routing Techniques, all nodes with EIGRP must have the same autonomous System number, indicating the same domain system.

c. In order to maximize the available bandwidth and reduce delay, the number of nodes connected in ad hoc networks and the size of files transmitted within the network should also be minimized.

REFERENCES

Aboelela, S.N.(2014),"Computer Networks: Network Simulation Experiment Manual.2nd ed. San Francisco"Morgan Kaufmann.21 – 43

Abolhasn, F. N.(2015),"performance Enhancement of mobile networks usingquery localization technique.

Basant S. et al,(2014) "Performance metrics in Ad hoc Network". *International Journal of Latest Trends in Engineering and Technology*.Vol.1 issue 1.

Battista, G. D. and Cittadini, L. (2015),"Doing donts:Modifying BGP attributes within and Autonomous system," in Network Operations and Management Symposium(NOMS), IEEE.

Cittadini, L. and Visicchio, S.(2016) "iBGP deceptions: More sessions, fewer routes in INFOCOM Proceedings IEEE,

Dovrolis C. and Reena S. (2015) "Performance Analysis of Routing Protocols for Real Time Application".*International Journal of Advanced Research in Computer and Communication Engineering* 3 (1): 23-25.

Fernandez, P. A. and Sendra S. (2014) "Study and Performance of Interior Gateway IP Routing Protocols, "Network Protocols & Algorithms. Vol. 2.

Guan, Q. and Ding, Q (2009). "A Minimum energy path topology control Algorithm for wireless multihop networks.

Hara, P.A.(2010),"Throughput, Delay and Mobility in Wireless Ad Hoc Networks,"IEEE Communications Society,Technical Program 2010.

Horneffer, M. and Martini, P. (2014) "Root causes for iBGP routing anomalies," in local computer Networks (LCN) IEEE 35th Conference

Jiang, Y. and Yin, Q. (2014). "Provisioning of Adaptability to Variable topologies for routing schemes in MANETs, "IEEEJ. On selected Areas in Com.Vol. 22.

Johansson,G. N. (2014),"Bandwidth efficient AMR Operation for VOIP"IEEE proceedings of the workshop on speech coding,3,150 – 152.

Johnson,D. A.(2016),"performance and Analysis of a delay-Threshold Based Bandwidth.

Karanakis, S.D. (2015),"IP Routing Fundamentals,"2nd ed,California ciscopress,pp23.

Kalyan, G. S. and Prasad, V. V (2014) "Optimal selection of Dynamic Routing Protocol withreal time case studies, "in Recent Advances in Computing and Software Systems (RACSS), International Conference on.

Lachhman, S. and Asad, Y. (2013). "Performance analysis of WLAN standards for video conferencing applications", *International Journal of Wireless & Mobile Networks (IJWMN)* vol. 3 No 6.

Latha, O. and Wilford, H.(2015)."Mobile Ad hoc Network" *International Journal Of science and Research, volume 2 issue 4.*

Mark, N. (2016),"Voice Over IP Technologies",Building the converged Network"2nd ed.New York: John Wiley and sons,Inc pp.234 – 237

Mahini, A. and Berangi, R. (2012) "MLET: A power efficient approach for TCAM based IP Lookup Engines in Internet, "*International Journal of Computer Networks & Communications,* Vol. 2

Maag, S and Sarakbi,B. (2015)."Partial Complete ibgp," in Communications (ICC) IEEEInternational Conference.

Maltz ,(2007),"Quantitative lesson from a full-scale multi- hop wireless ad hoc network testbed,"IEEE 2007.

Molnar G. et al,(2014),"Algorithm for Routing protocol."American *Journal of Intelligent Systems* 6(2) 31 – 41,DOI: 10.5923/j.aji

Owezarski, G. J. (2014) Rethinking IBGP routing" in ACM SIGCOMM ComputerCommunication Review.

Patel, B. and Srivastava, S. (2014) "Performance Analysis of Zone routing protocols in Mobile AD Hoc Networks, "Communications (NCC) National Conference.

Politis C.et al,(2012)" Secure Routing for Supporting Ad hoc Extreme Emergency Infrastructures,"proc. Of IEEE future and Network Mobile summit.

Pasztor, S. and Fengi,W.(2010),"The Packet Size Dependence of packet pair like method,"IEEE/IFIP Int'l,WkspQos.

Sawde, K. and Dayanand,A.(2015),"End-to-End Available Bandwidth:Measurement Methodology,Dynamics and Relation with TCP Throughput,"ACM SIGCOMM,34,295-299.

Sportack, G. N.(2013),"IP Routing Fundamentals,"2nd ed. California:cisco press pp.23

Thorenoor, F. K.(2014) "Dynamic Routing protocol implementation decisionBetween OSPF and RIP based on Technical Background using OPNETmodeler second international conference on computer and Network Technology (ICCNT 2014),191 – 195.

Tang, J.(2014). "Cross-layer modeling for quality of services guaranteesover wireless links, "IEEE Trans. Wireless. Common. Vol. 6

.

Tseng,(2016). "A Study of MANET Routing Protocols Joint Node Density Packetlength and Mobility 978-1-4244-7755.

Vasudha et al, (2012)."Performance Evaluation of Routing Protocols for MANETs under Different Traffic Conditions" 2nd International Conference on
Computer Engineering and Technology (Volume 6) 978-1-4244-6349.

APPENDIX

SIMULATION CODES

```
%Effects of transmission Rate on link transmission delay for four hops
%(with average link bandwidth in simple network configuration)
x = [6126600 15389000 43750000 50000000];
y = [0.012592 0.005221 0.004721 0.004077];
plot(x, y)
gridon
xlabel('Transmission Rate (Bits/sec)')
ylabel('Link delay (microSecs)')
```

```
%Effects of transmission Rate on link transmission delay for four hops
%(with minimum scale bandwidth in complex network configuration)
x = [56000 64000 64000 150000 150000];
y = [2.735596 2.735596 0.117884 0.117887 0.117887];
plot(x, y)
gridon
xlabel('Transmission Rate (Bits/sec)')
ylabel('Link delay (microSecs)')
```



```
%Effects of transmission Rate on link transmission delay for four hops and
%five hops with average link bandwidth in simple network configuration)
x1 = [6126600 15389000 43750000 50000000];
x2 = [3202400 383000];
y1 = [0.012592 0.005221 0.004721 0.004077];
y2 = [0.006051 0.006998];
plot(x1, y1, 'k', x2, y2, 'r')
gridon
xlabel('Transmission Rate (Bits/sec)')
ylabel('Link delay (microSecs)')
legend('Four Hops', 'Five Hops')
```

```
%Effects of transmission Rate on link transmission delay for four hops and
%five hops with minimum link bandwidth in complex network configuration)
x1 = [6126600 15389000 43750000 50000000];
x2 = [3202400 383000];
y1 = [0.012592 0.005221 0.004721 0.004077];
y2 = [0.006051 0.006998];
plot(x1, y1, 'k', x2, y2, 'r')
gridon
xlabel('Transmission Rate (Bits/sec)')
ylabel('Link delay (microSecs)')
legend('Four Hops', 'Five Hops')
```

```
%Effects of Packet Size on link transmission delay for four hops
%(with minimum scale bandwidth in complex network configuration)
x = [10000 15000 20000];
y = [0.004077 0.004721 0.005221];
plot(x, y)
gridon
xlabel('Packet Size (Bytes)')
ylabel('Link delay (microSecs)')
```