Sudan University of Science and Technology

College of Engineering

School of Electronics Engineering

Evaluation of multi-hop ad-hoc Routing protocol

A Research Submitted In Partial Fulfillment for the Requirements of the Degree of B.Sc. (Honors) in Electronic Engineering

Prepared By:

1. Ibrahim Abd-Elwahab Hamdna Allah
2. Mohammed Ashraf Abd-Elhadi
3. Mohammed Ibrahim El-Amin
4. Samer Osman Elmobark

Supervised By:

Dr. Sami Hassan Omer Salih

September 2015

Dedication

To Our beloved parents who they support us all the time to complete this project.

To all teachers and Doctors who learn us.

To all friends who they stand with us through this project .

To Dr. Sami Hassan Omer Salih who guided us through the long process.

Acknowledgements

This document is our journey through Sudan University of Science and Technology, it could not have been possible alone. We want to take a moment to thank the most important to us.

First to Allah, whose grace, blessings and guidance helped us finding our way.

To Dr. Sami Hassan Omer Salih, who very patiently guided us through the long process and provided us with the required information's to be able to complete this work

We would also like to thank our parents and their patient ears through our frustration and aggravation insuring that we achieve success.

To my friends and colleagues, whose mentoring and humor helped us and know how lucky we were to be surrounded by such great people.

Abstract

This thesis investigates the performance of the Ad-hoc On-Demand Distance Vector (AODV) Routing protocol on Voice over Internet Protocol (VoIP) applications in Wireless Ad hoc Networks . Using VoIP over it takes advantage of the mobility and versatility of a WMAN environment and the flexibility and interoperability a digital voice format affords. Research shows that VoIP-like traffic can be routed through an ad hoc network using the Ad hoc On-demand Distance Vector routing protocol.

Representative VoIP traffic is submitted to a WMAN and end-to-end delay and packet loss are observed. Node density. On two scenarios.

Results show that node density, number of data streams, and mobility affect Delay and packet loss. Even with the increase in both packet loss and delay, AODV is still a suitable routing protocol for VoIP traffic

المستخلص

في هذا البحث تم التحقق من اداء بروتوكول شبكة المؤقتة اللاسلكية عند الحوجة في تقنيه نقل الصوت عبر بروتوكول الانترنت في شبكات المؤقتة اللاسلكية . استخدام تقنيه الصوت عبر بروتوكول الانترنت في الشبكه يتيح الاستفادة من امكانية التنقل بجانب ميزة تعدد الاستخدام الموجودة في بيئة الشبكة اضافة الي كل ذلك المرونة وقابلية التبادل الموفرة في انظمة الصوت الرقمية.

البحث يوضح ان استخدام ال الصوت عبر بروتوكول الانترنت كحزمة بيانات بامكانه التنقل عبر شبكة المؤقتة اللاسلكية باستخدام بروتوكول شبكة المؤقتة اللاسلكية عند الحوجة .

ومن خلال نتائج الدراسة تم التوصل الى ان البروتوكول شبكة المؤقتة اللاسلكية عند الحوجة مناسب للاستخدام كبروتوكول توجيه ونقل حزم الصوت.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

List of Abbreviations

AODV	Ad hoc On-demand Distance Vector
CBR	Constant Bit Rate
CEDAR	Core Extraction Distributed Ad Hoc Routing Protocol
CPU	Central Processor Unit
DSR	Dynamic Source Routing
ITU	International Telecommunications Union
Manet	Mobile Ad-hoc network
MWN	Multi-hop Wireless Network
NIC	Network Interface Card
OLSR	Optimized Link State Routing
OS	Operating System
RREQ	Route Request
RREP	Route Reply
RERR	Route Error Message
RAM	Random Access Memory
SUT	System under Test
UDP	User Diagram Portocol
VoIP	Voice over Internet Protocol
WMAN	Wireless Multi-hop Ad-hoc network
ZRP	Zone Routing Protocol

Chapter One

Introduction

Chapter One

Introduction

1.1 introduction

Ad Hoc Wireless Network is a collection of wireless device hosts forming a temporary network. Every device has the role of router and actively participates in data forwarding and communication between two nodes can be performed directly if the destination is within the sender's transmission range, or through intermediate nodes acting as routers if the destination is outside sender's transmission range.

A Wireless Ad hoc Network poses a challenging environment for Voice over Internet Protocol (VoIP) due to multi-hop routing and dynamic route calculation. Routing in a WMAN uses routing protocols such as Ad hoc On-demand Distance Vector (AODV) and Optimized Link State Routing (OLSR). The major difference between these two protocols is AODV is a reactive protocol that searches for new routes as required while OLSR is a proactive protocol that calculates all valid routes whether they are needed or not.

Evaluating performance in a WMAN for VoIP traffic requires end-to-end delay and packet loss be minimized since VoIP applications are sensitive to any type of latency and packet loss. These metrics are compared to the recommended values for each to determine whether AODV can support VoIP traffic in a WMAN.

VoIP is a category of hardware and software that enables people t o use the Internet as the transmission medium for telephone calls by send ing voice data in packets using IP rather than .

1.2 Problem statement

The dynamic architecture of Ad-hoc network affect the stability of coherent traffic such as real-time conversations. Especially when a multi-hop is required to deliver the information.

In VoIP context a certain level of voice quality has to assure in order to satisfy the customer needs. This an evaluation of VoIP over multi-hop ad-hoc network. The research goals are met by sending representative VoIP traffic across WMAN .Objective measurement of delay, jitter and packet loss determines whether AODV provides acceptable performance on the WMAN.

1.3 Propose Solution

A test-bed is to be implemented with different scenarios to evaluate VOIP over multi-hop ad-hoc network.

1.4 Methodology

Establish using two nodes as test-bed to check connection of ad-hoc network and pinging each other, after insurance of ad-hoc connection is working, another hop were added. After that separate nodes from each other till it were unreachable. By applying AODV module nodes were able to see each other again and packets were captured and analyzed.

1.5 Thesis Outlines

Chapter two describe AD-HOC MULTI-HOP network, AODV as routing protocol and previous researches that are related to this topic. Chapter three represent the implementation of Multi-hop Ad-hoc network and AODV, metrics of VOIP. In chapter four represent the result of implementation and usage of VOIP over MULTI-HOP AD-HOC networks.

Chapter five include the Conclusion and Recommendations for further researches and evolutionary of VOIP over MULTI-HOP AD-HOC network.

Chapter Two

An Over view of multi-hop ad-hoc networks

Chapter Two

An Over view of multi-hop ad-hoc networks

2.1 Background

An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other. In Latin, ad hoc literally means "for this," meaning "for this special purpose" and also, by extension, improvised or impromptu.

Similar to Manet network WMAN is no infrastructure exists and every node is mobile, in a mesh network there is a set of nodes, the mesh routers, which are stationary and form a wireless multi-hop ad hoc backbone. Maybe some of the routers are attached to the Internet, and provide connectivity to the whole mesh network for example:

2.1.1 Multi-hop Wireless Network (MWN)

-A wireless network adopting multi-hop wireless technology without deployment of wired backhaul links.

Like they said it's Similar to Mobile Ad hoc Networks (MANET), but:

-Nodes in MWN is relative ‘fixed’.

-MWN may introduce ‘hierarchy’ network architecture.

2.1.2 Multi-hop Wireless Networks had two categories

-Relay:

Tree based topology, one end of the path is the base station

Dedicated carrier owned infrastructure

-Mesh:

Mesh topology, multiple connections among users routing by carrier owned infrastructure or subscriber equipment

2.1.3 Cons of multi-hop technology

-Rapid deployment with lower-cost backhaul.

-Easy to provide coverage in hard-to-wire areas.

-Under the right circumstances, it may:

*Extend coverage due to multi-hop forwarding.

*Enhance throughput due to shorter hops.

*Extend battery life due to lower power transmission.

2.1.4 Bros of multi-hop networks

-Routing complexity.

-Path management.

-Extra delay due to multi-hop relaying.

2.1.5 Ad Hoc Routing Protocols

Routing in an ad hoc network is different than routing in an infrastructure-based network, because ad hoc networks have characteristics not found in infrastructure-based networks such as multi-hop routing. A routing protocol can be evaluated using the following metrics [1]:

• End-to-end Data Throughput and Delay: Throughput and delay are measured from the perspective of applications that use the routing. Throughput and delay measure a routing policy’s effectiveness and are important when dealing with Constant Bit Rate (CBR) applications such as real-time audio or video.

• Route Acquisition Time: This is the time required to establish route(s) when requested and is affected by the type of routing protocol.

• Efficiency: This is the internal measure of the routing protocol's effectiveness and can be measured as either overhead or throughput versus input traffic.

The routing protocols for MWN can be classified into three main types - proactive, reactive, and hybrid [1]. Table 2.1 compares the three types of MWN routing protocols classified as flat routing.

Table 2.1: Classification of Ad Hoc Routing Protocols: [2]

	Proactive	Reactive	Hybrid
Routing Structure	Can be flat or hierarchical	Mostly flat	Mostly Hierarchical
Route Availability	Always available	On-demand	Depends on location of destination
Volume of Control Traffic	High	Lower than Proactive	Lowest
Periodic Update	Yes	Not required	Yes, within zone or cluster or between gateways
Delay	Low	High	Depends on location of destination

2.1.5.1 Proactive Routing Protocols

Nodes exchange routing information periodically to maintain accurate routing information. The path can be computed rapidly based on the updated information available in the routing table.

2.1.5.2 Reactive Routing Protocol

A route discovery mechanism is initiated only when a node does not know a path to a destination it wants to communicate with. Perform better with significantly lower overheads than proactive routing protocols has two main operations are Route discovery and Route maintenance ,example for reactive protocols have been proposed.

-Ad Hoc On-demand Distance Vector (AODV).

-Dynamic Source Routing (DSR).

2.1.5.3 Hybrid Routing Protocols

Some routing protocols are hybrid of proactive and reactive mechanisms. Examples of hybrid routing protocols:

-Zone Routing Protocol (ZRP).

-Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR).

2.1.6 AODV Routing protocol

AODV is a method of routing messages between mobile computers. It allows these mobile computers, or nodes, to pass messages through their neighbors to nodes with which they cannot directly communicate. AODV does this by discovering the routes along which messages can be passed.

AODV makes sure these routes do not contain loops and tries to find the shortest route possible. AODV is also able to handle changes in routes and can create new routes if there is an error. The diagram shows a set-up of four nodes on a wireless network. The circles illustrate the range of communication for each node. Because of the limited range, each node can only communicate with the nodes next to it.[10]

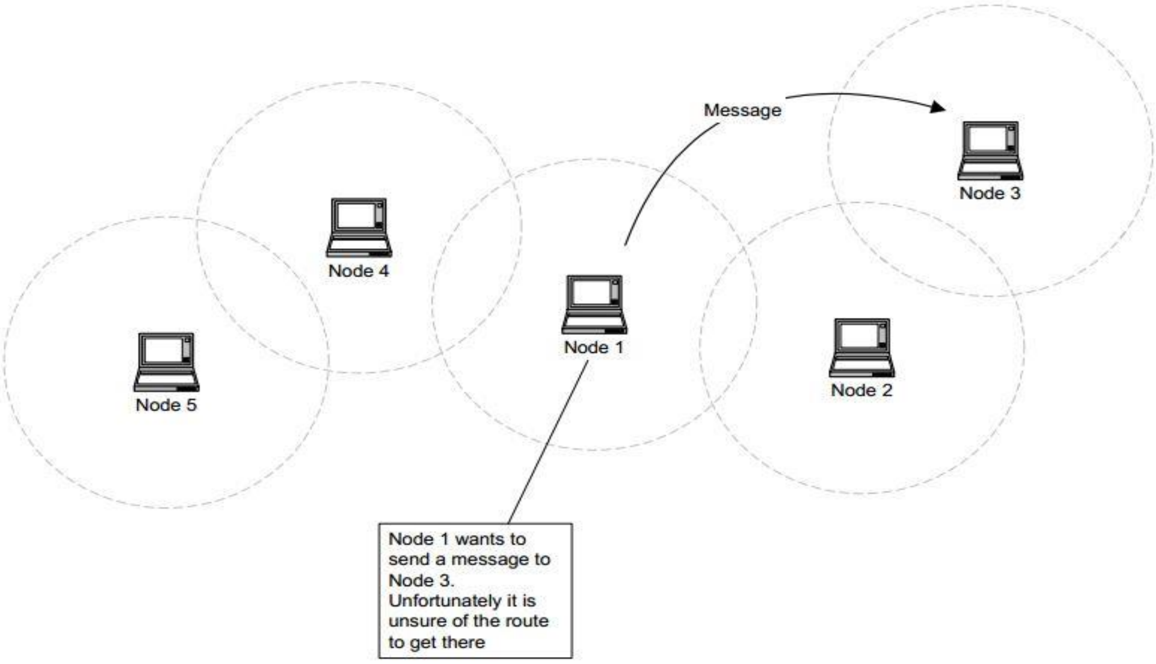

Figure 2.1 AODV setup of 5 nodes

Nodes you can communicate with directly are considered to be Neighbors. A node keeps track of its Neighbors by listening for a HELLO message that each node broadcast at set intervals.

When one node needs to send a message to another node that is not its Neighbor it broadcasts a Route Request (RREQ) message. The RREQ message contains several key bits of information: the source, the destination, the lifespan of the message and a Sequence Number which serves as a unique ID. [10]

In the example, Node 1 wishes to send a message to Node 3. Node 1's Neighbors are Nodes 2 + 4. Since Node 1 can not directly communicate with Node 3, Node 1 sends out aRREQ.

The RREQ is heard by Node 4 and Node . [10]

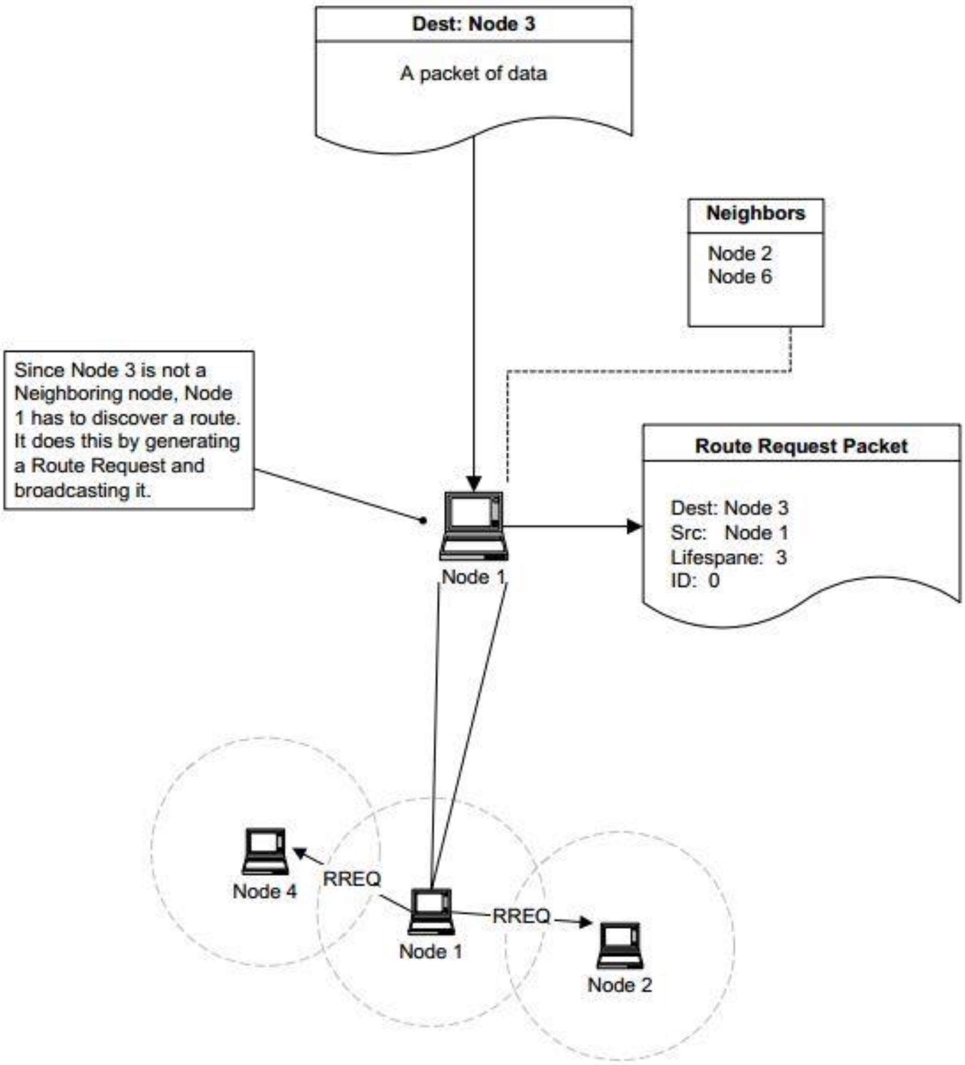

Figure 2.2 AODV routing message

When Node 1's Neighbors receive the RREQ message they have two choices; if they know a route to the destination or if they are the destination they can send a Route Reply (RREP) message back to Node 1, otherwise they will rebroadcast the RREQ to their set of Neighbors. [10]

The message keeps getting rebroadcast until its lifespan is up. If Node 1 does not receive a reply in a set amount of time, it will rebroadcast the request except this time the RREQ message will have a longer lifespan and a new ID number. [10]

All of the Nodes use the Sequence Number in the RREQ to insure that they do not rebroadcast a RREQ In the example, Node 2 has a route to Node 3 and replies to the RREQ by sending out a RREP. Node 4 on the other hand does not have a route to Node 3 so it rebroadcasts the RREQ.

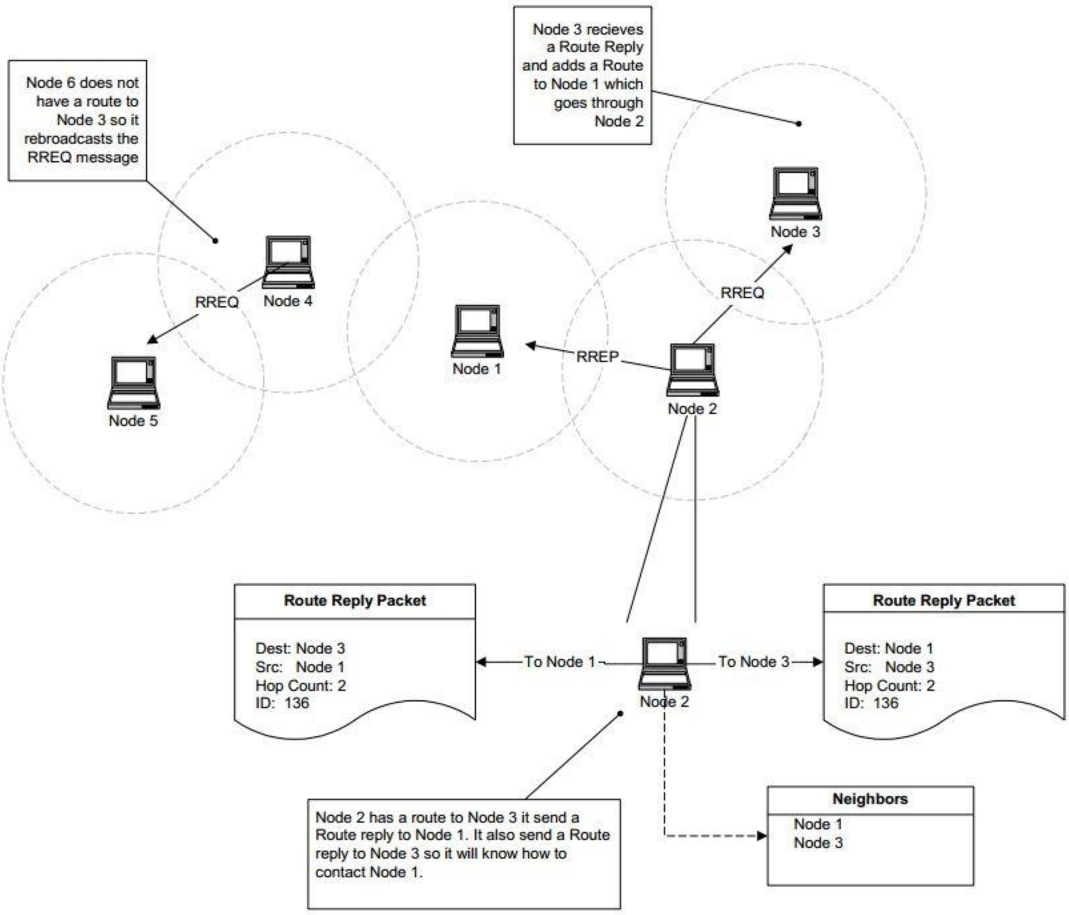

Figure 2.3 AODV replay message

2.1.6.1 Sequence Numbers

Sequence numbers serve as time stamps. They allow nodes to compare how “fresh” their information on other nodes is.

Every time a node sends out any type of message it increase its own Sequence number. Each node records the Sequence number of all the other nodes it talks to. A higher Sequence numbers signifies a fresher route. This it is possible for other nodes to figure out which one has more accurate information.

In the example, Node 1 is forwarding a RREP to Node 4. It notices that the route in the RREP has a better Sequence number than the route in it’s Routing List. Node 1 then replaces the route it currently has with the route in the Route Reply. [10]

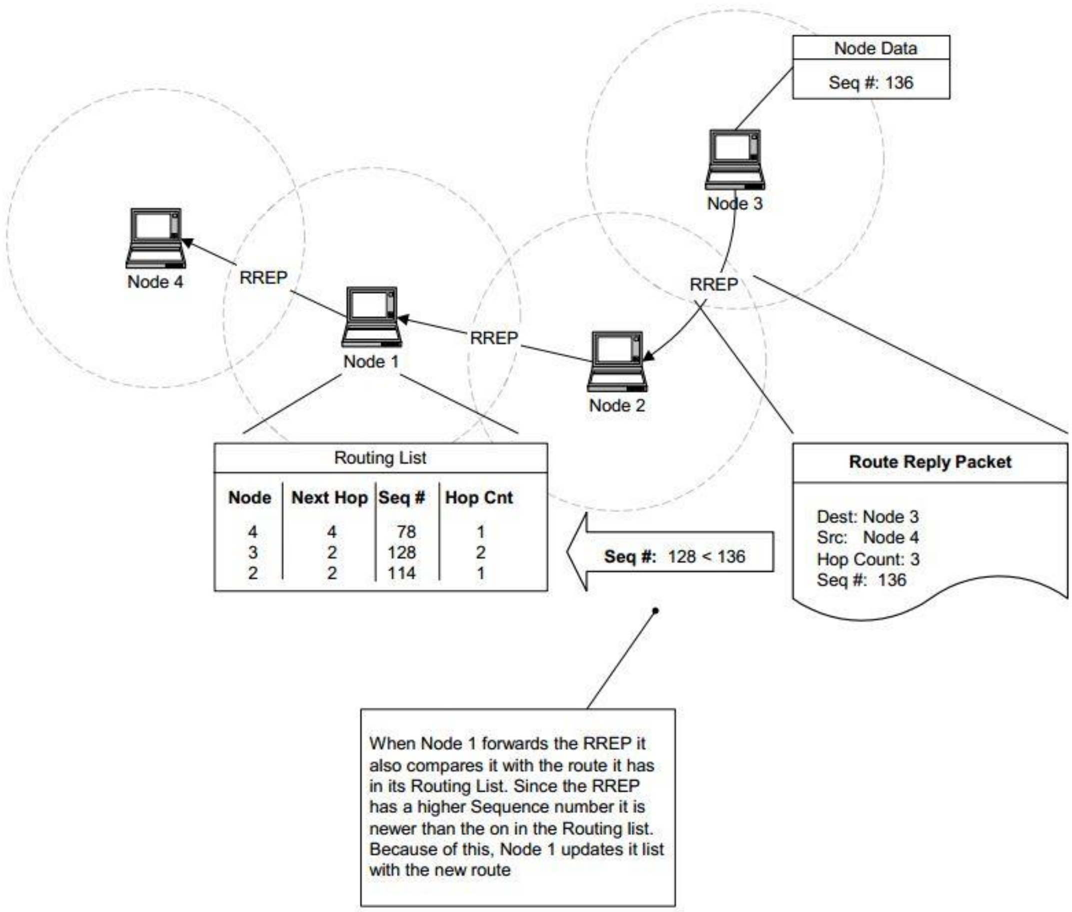

figure 2.4 AODV sequence number

2.1.6.2 Error Messages

The Route Error Message (RERR) allows AODV to adjust routes when Nodes move around. Whenever a Node receives RERR it looks at the Routing Table and removes all the routes that contain the bad Nodes.

The diagrams illustrate the three circumstances under which a Node would broadcast a RERR to its neighbors.

Forward but it does not have a route to the destination. The real problem is not that the Node does not have a route; the problem is that some other node thin in the first scenario the Node receives a Data packet that it is supposed to be that the correct Route to the Destination is through that Node.

In the second scenario the Node receives a RERR that cause at least one of its Route to become invalidated. If it happens, the Node would then send out a RERR with all the new Nodes which are now unreachable In the third scenario the Node detects that it cannot communicate with one of its Neighbors.[10]

When this happens it looks at the route table for Route that use the Neighbor for a next hop and marks them as invalid. Then it sends out a RERR with the Neighbor and the invalid routes.

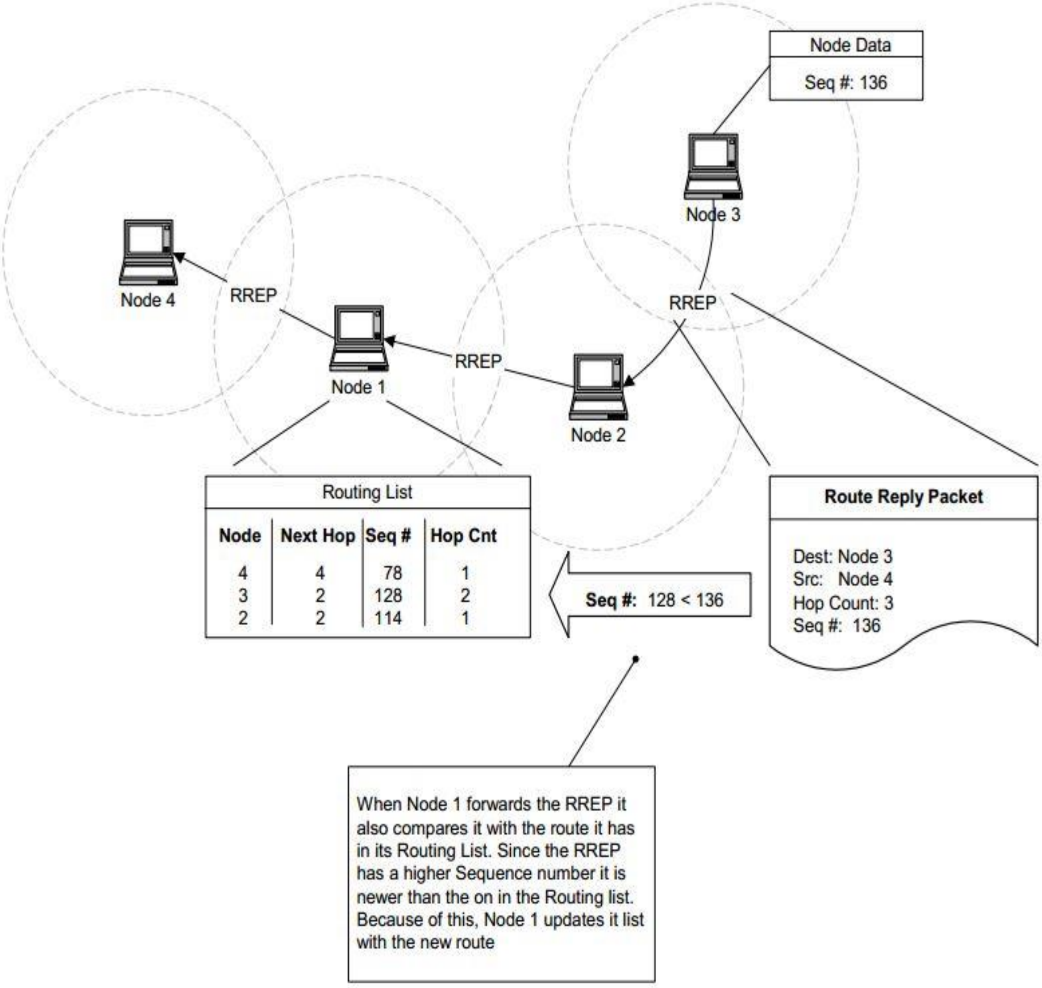

Figure 2.5 AODV error message

When we consider VoIP applications in general, they will probably become more widely used as time evolves. Currently, the main problem for such applications is the lack of QoS guarantees.

When QoS supporting protocols like RSVP are used on a larger scale, this will certainly make VoIP More popular since people can then communicate with the quality that they desire. On LANs, Where there is normally plenty of bandwidth, VoIP applications can already be used with little or no problems.

2.2 Related work

VoIP Traffic in Multi-Hop Ad Hoc Networks [2]. Multi-hop environments such as MANETs create situations not normally seen in wired networks. Armenia et al. study real-time audio traffic on multi-hop IEEE 802.11b ad hoc wireless networks via simulations and a test-bed including both proactive and reactive routing protocols, specifically OLSR and AODV. Figure 2.8 shows the test-bed topology, and Table 2.2 lists the specific configurations of the hosts. The test-bed consists of four stationary hosts and a 30 second audio file sampled at 8 kHz and 8-bit encoding. This VoIP file is sent using the Gnome Meeting tool and subsequently analyzed at the receiver using Ethereal [2].

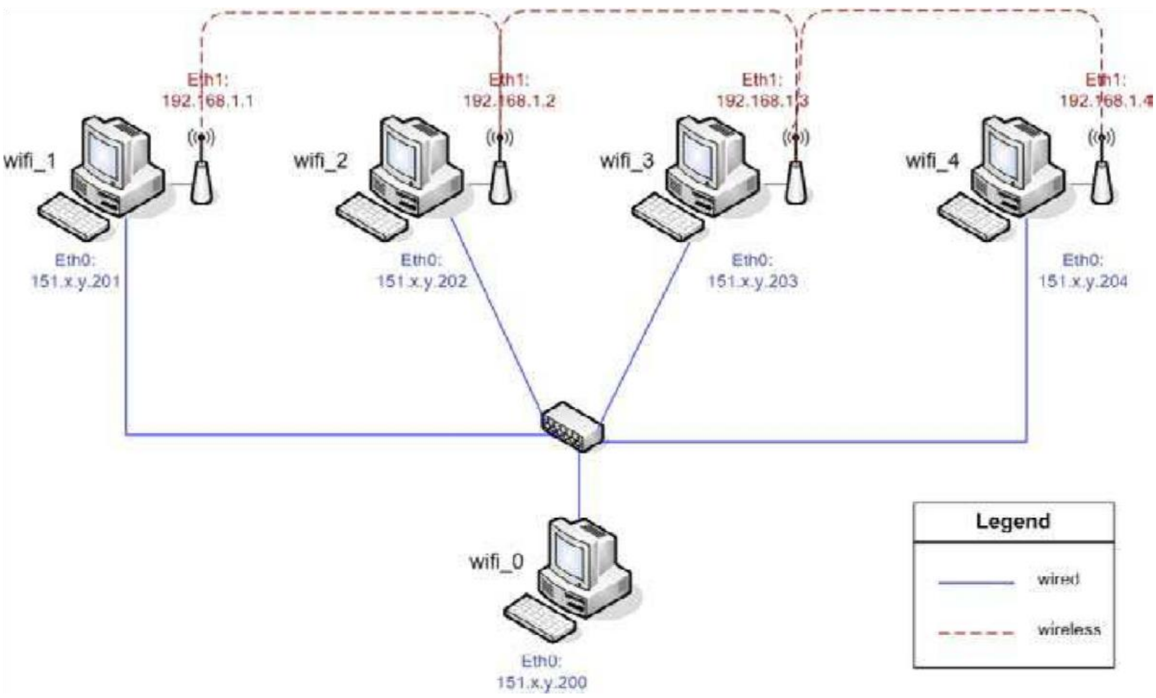

Figure 2.6 Test-bed Topology[2]

The codec does not affect the routing protocol performance nor is there a noticeable difference between OLSR and AODV throughput and delay jitter. However, varying the number of hops results in a noticeable difference between OLSR and AODV end-to-end delay. For all codecs studied, AODV returns an end-to-end delay averaging 0.07 seconds higher than OLSR [2]. These results are only for stationary hosts in an 802.11b ad hoc network. Mobile hosts have different results.

Table 2.2 : Test-bed Host Configurations[2]

CPU	AMD Duron 1.6 GHz, 64 KB cache Intel Pentium III 800 MHz, 256 KB cache
RAM	256 MB 128 MB
PCI Fast Ethernet Card	VIA Rhine II Fast Ethernet Adapter
Wireless PCI card	802.11b ADMtek

In [3] The author Discuss the set up a real 6-node multi-hop network. The experimental measurements confirm the existence of the optimal offered load. In addition He provide an analysis to estimate the optimal offered load that maximizes the throughput of a multi-hop traffic flow

In [4] The author review the basic principles behind multi-hop ad hoc networks and critically discusses approximately and summarize the main achievements and point out the limits of multi-hop ad hoc networks research and the research was conducted under the assumption that the networks mainly will be used for large-scale general consumer applications, and nodes would be ubiquitous, thus reasonably dense and active

In [5] the author present a multi-hop wireless ad hoc network implementation on Windows system based on 802.11 single-hop ad hoc mode. In the implementation we have adopted Ad hoc On-demand Distance Vector (AODV) protocol as the routing protocol.

In [6] the author attempts to provide a comprehensive overview of this dynamic field. First he explains the important role that mobile ad hoc networks play in the evolution of future wireless technologies. Then, he reviews the latest research activities in these areas, including a summary of MANETs characteristics, capabilities, applications, and design constraints. Also he representing a set of challenges and problems requiring further research in the future.

Chapter Three

Implementing of ad-hoc multi-hop routing protocol

Chapter Three

Implementing of ad-hoc multi-hop routing protocol

3.1 Preface

This chapter discusses the methodology for this research. Section 3.2 discusses system boundaries, including the component under test. The system services are described in this chapter, Section 3.3 discusses performance metrics, and Section 3.4 discusses system parameters. Workload parameters are discussed in Section 3.5, in 3.6 explains the evaluation technique.

3.2 System Boundaries

The System under Test (SUT) is the VoIP WMAN System. Figure 3.1 shows the components of the SUT. The VoWMAN system consists of four major components - ad hoc nodes, an ad hoc network, routing protocol, and the IEEE 802.11 MAC layer protocol.

3.2.1 Ad Hoc Nodes

Each node in the ad hoc network functions as both a client and a server. As clients, the nodes complete two tasks - send requests to the network and receive information from the network. As servers, the nodes process information received from the network and determine whether packets require forwarding. If so, the node services the packet accordingly. Thus, each node provides the services of both a router and an end unit.

3.2.2 Ad Hoc Network

The ad hoc network is measured by observing VoIP traffic as it travels through the network. This network provides the medium that transports VoIP traffic from one ad hoc node to another. The network is a test-bed implemented using the wireless network portable devices.

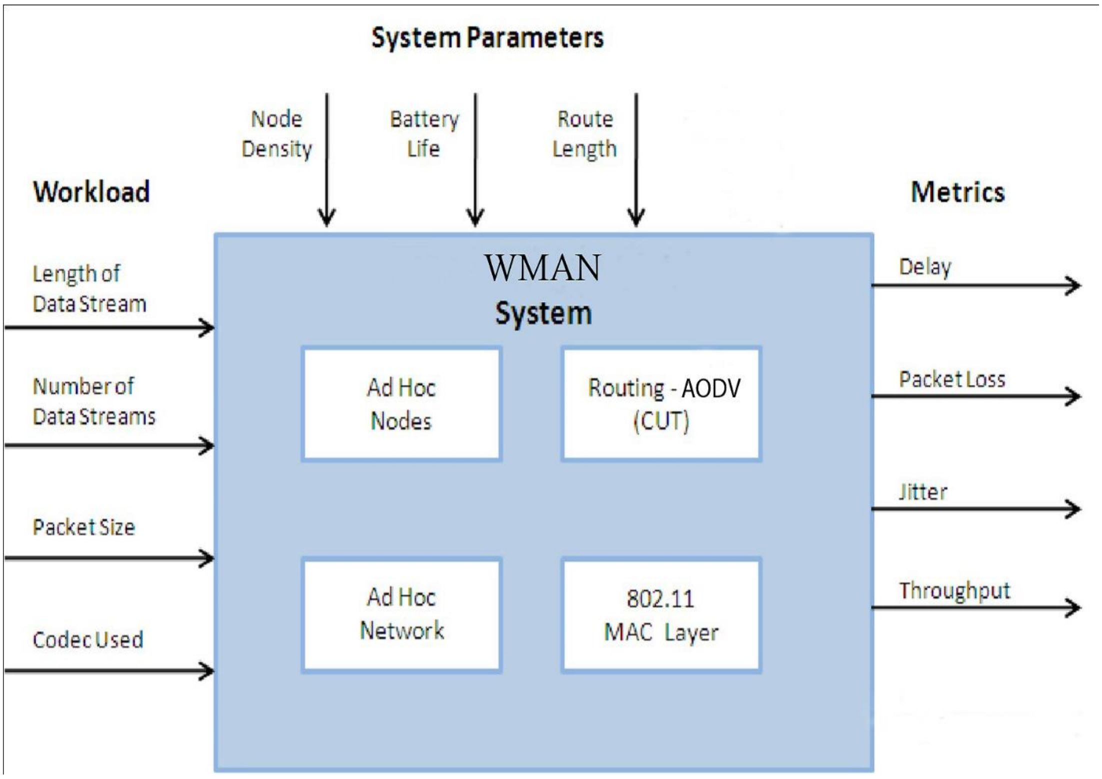

Figure 3.1 VoWMAN for System (SUT).

The service VoWMAN provides is VoIP calls over a WMAN. The system accepts VoIP data streams as input and transports the streams to the appropriate destination.

Figure 3.1 shows the possible outcomes of the WMAN system which are:

- The call is received with no errors and no re-routing is required.
- The call is received, but a new route is required resulting two possible outcomes:

- A valid route is found.
- A valid route is not found and the call is dropped.

- The call is dropped prior to being received because:

- No valid route is found.
- The call is dropped due to some other network error.

Since the AODV is the routing protocol, it is assumed the call is specified correctly by the sender and the receiver receives the call under normal conditions. That is, both the sender and receiver having compatible hardware and software and are able to communicate with each other (i.e., they are both part of the same WMAN). This excludes cases where calls are dropped due to application error and user error.

This experiment determines whether the routing protocol can obtain valid routes. Therefore, the outcomes considered are calls received when - no re-routing is required and re-routing required and a new valid route is calculated (all other outcomes are excluded).

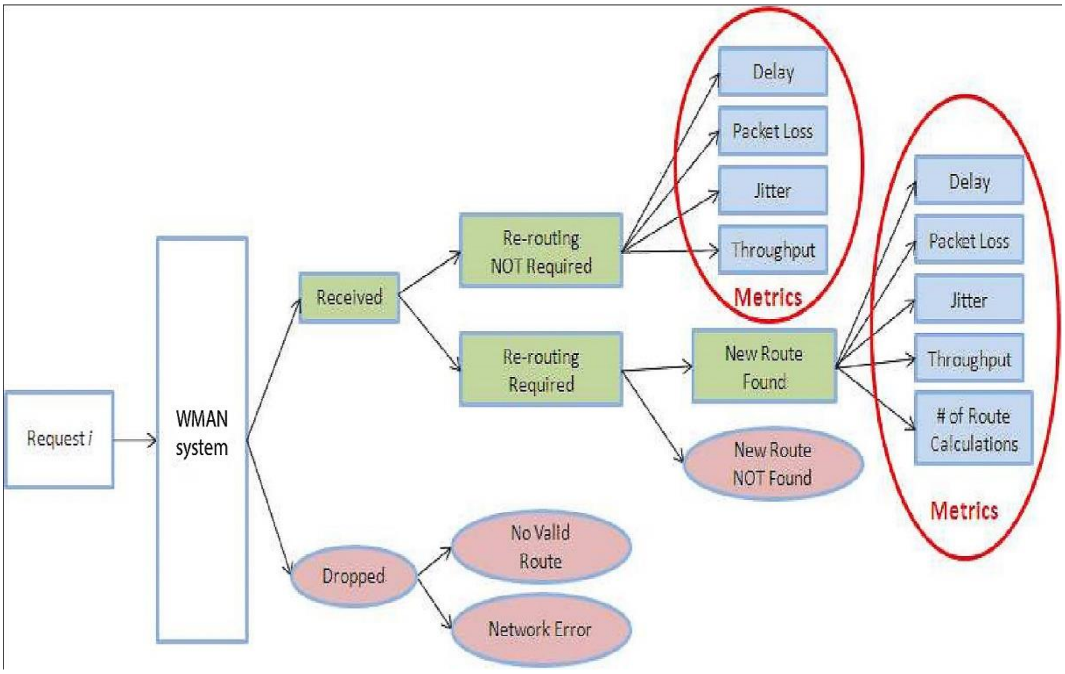

Figure 3.2 Possible Outcomes of the VoWMAN

3.3Performance Metrics

Performance metrics are used to establish the performance of systems. The performance metrics (circled in Figure 3.2) are delay, packet loss, jitter, throughput, and number of route calculations.

Evaluating performance in a MWAN for VoIP traffic requires end-to-end delay and packet loss be minimized since VoIP applications are sensitive to any type of latency and packet loss. These metrics are compared to the recommended values for each to determine whether AODV can support VoIP traffic in a MWAN.

3.3.1 End-to-End Delay

Delay is measured from the instant a packet leaves the sender's Network Interface Card (NIC) to the instant it is received at the destination's NIC. According to the International Telecommunications

Union (ITU) Recommendation G.114, delay in VoIP applications should never exceed 400 ms otherwise the quality of the VoIP stream is significantly degraded. However, the average delay for a VoIP stream should be less than 150 ms for acceptable perceived quality [7]. This end-to-end delay includes any time needed to calculate a new route and other routing delays such as router (i.e., another ad hoc node) processing and queuing delays.

3.3.2 Packet Loss

VoIP applications are sensitive to packet loss. Even though VoIP applications tolerate packet loss up to 10%, a packet loss of 1% still affects the quality of the VoIP stream [7]. Packet loss is measured as the percent of packets dropped at the receiver prior to data stream playback.

3.3.4 Jitter

When referring to VoIP applications, jitter occurs when packets are received with variances in delay. Packets can arrive out-of-order due to these delay variances or because of routing (i.e., a packet travels a different route than a prior packet). Variances in delay are due to packet position in queues along the path from source to destination. One packet could experience minimal queuing delays while the packet sent after it experiences long queuing delays along the same path. This affects the quality of streaming audio like VoIP. Jitter buffers at the receiver temporarily store packets to mask the variances in delay. Jitter, in this study,is measured at the receiver and does not assume any jitter buffers.

3.3.4 Throughput

Throughput is the total number of bits that are sent through the channel per second. The channel is the ad hoc network, thus, throughput is the maximum number of bits that can be sent per second through the ad hoc network.

3.4 System Parameters

The system parameters that affect the performance of the VoMAN system include number of nodes in a given area (node density), battery life, number of hops (route length), and mobility.

3.4.1 Node Density

Node density is the number of nodes .It is considered since AODV should perform better in a denser network. Hence, it is assumed that as the number of nodes in a fixed area increase, the performance of AODV improves.

3.4.2 Battery Life

Battery life is an important issue in WMAN. Since nodes are not always connected to power, batteries must have long life or include a mechanism that conserves energy while performing network tasks.

3.4.3 Route Length

If the sender and receiver are linked directly, then route length has minimal impact. However, if the sender and receiver do not have a direct link and the packets require routing through multiple hops, then route length plays a major role in the WMAN. Increased delay, jitter, and packet loss could result from a long route length. Route length is not observed in this study.

3.5 Workload Parameters

Workload parameters that affect performance on the WMAN system include the length of the VoIP data stream, number of data streams, packet size, and codec used.

3.5.1 Length of data stream

The number of packets in a VoIP data stream depends on the length of the original stream as well as the overhead associated with header data. Long data streams (i.e., streams containing large packets) result in higher transmission efficiency since less packets are transmitted. However, long streams also result in higher end-to-end delay and packet loss since a lost packet results in the inability to re-create the stream at the receiver. Shorter streams are more tolerant of packet loss and have shorter end-to-end delay, because a packet lost does not necessarily affect stream re-creation at the receiver. This results in better preserved voice quality [8]. The length of the data streams is fixed in this study to one VoIP packet coded using the G.711 codec.

3.5.2 Number of Data Streams

As the load on the MANET increases, OLSR performance is observed. Since VoIP traffic is sensitive to delay and packet loss, it is important to study the effects of increasing VoIP traffic over a MANET. As more traffic is injected into the network, the routing protocol must service multiple route requests. In addition to route requests, each node must accept traffic it receives and continue to forward packets through the network. Section 3.8 discusses the number of data streams as a factor for this study.

3.5.3 Packet size

In general, packet size can vary between data streams. However, VoIP packets do not vary significantly since VoIP packet size is constant prior to transmission due to the codec used [8]. If they did vary, it could affect the performance results of the WMAN. Packet size for this study is fixed at 200 bytes.

3.5.4 Voice Codecs

The rate at which the data stream is sampled is important since it affects the performance of the VoMAN system. Different codecs sample at different rates which results in various packet sizes [9]. Various compression ratios create variances in data streams such that two data streams carrying the same information sampled at different rates can vary greatly in size. The codec in this study is the ITU G.722 codec commonly used VoIP applications.

3.6 Evaluation Technique:

Measurement of an actual WMAN is expensive and infeasible. Therefore, the evaluation is done by using:

- Wireshark

Evaluation done by using wireshark on Linux (Ubuntu 10.04).

Table 3.1: Test-bed Host Configurations

CPU	AMD Duron 1.6 GHz, 64 KB cache Intel Pentium IIII 1 GHz, 256 KB cache Intel core 2 duo 2.2 GHz,512 kb cache
RAM	1 GB
PCI Fast Ethernet Card	VIA Rhine II Fast Ethernet Adapter
Wireless PCI card	802.11b ADMtek

Chapter Four

Results and Discussions

Chapter Four

Results and Discussions

4.1 Preface

Results discussed in this chapter cover the overall experiment and concentrate on the main results and analysis obtained from the study.

4.2 Results & Discussion

4.2.1 Delay & Jitter

4.2.1.1 Scenario 1

In this scenario two nodes has been connected to the ad-hoc network and result as follow

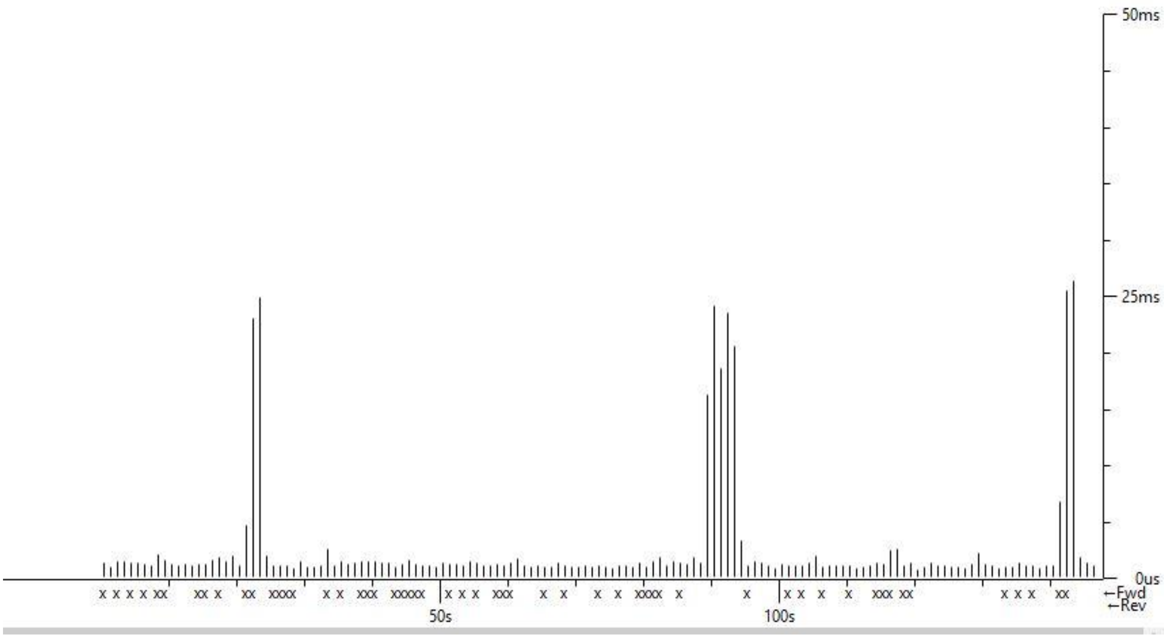

Figure 4.1

In figure 4.1 jitter occurs when packets received in variance in delay. The mean jitter from node 10.42.43.10 to node 10.42.43.11 is 1.58ms, and the max jitter in figure 4.1 is 26.27 ms .

The jitter in above figures occurs due the congestion on the network or the congestion at NIC interface.

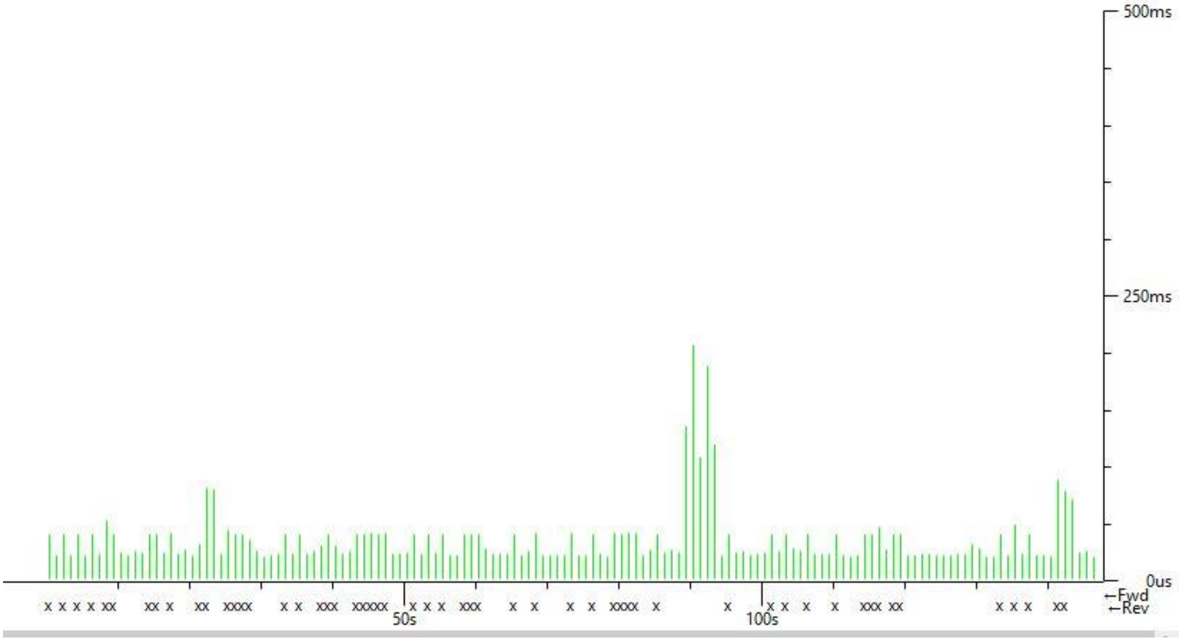

Figure 4.2

In figure 4.2 the max delta from 10.42.43.10 to 10.42.43.11 is 206.76 ms. the delta happened because number of nodes, distance between nodes and include any time needed to calculate routes.

- From figures 4.1 & 4.2 achieved the:

-Max delta = 206.76 ms at packet no. 35013

-Max jitter = 26.27 ms.

-Mean jitter = 1.58 ms.

-Max skew = -683.26 ms.

-Total RTP packets = 7391 (expected 7391)

-Lost RTP packets = 65 (0.88%)

-Sequence errors = 81

-Duration 147.79 s (-22527 ms clock drift, corresponding to 6781 Hz (-15.24%)

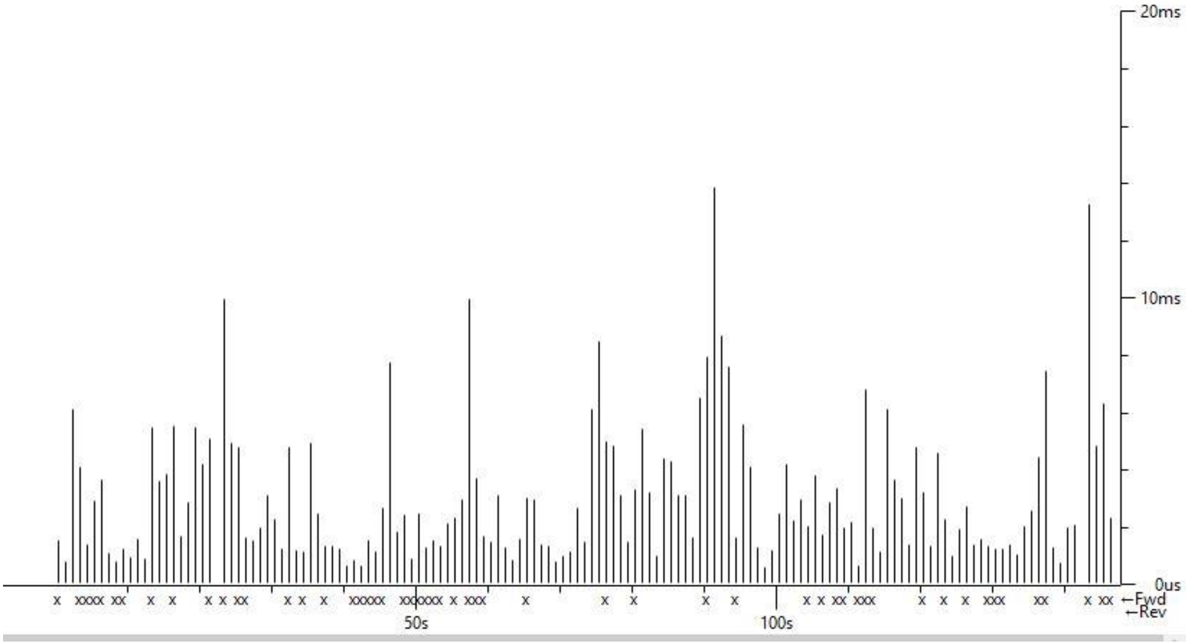

Figure 4.3

In figure 4.3 jitter occurs when packets received in variance in delay. The mean jitter from node 10.42.43.11 to node 10.42.43.10 is 1.53ms, and the max jitter is 13.8ms.

The jitter in above figures occurs due the congestion on the network or the congestion at NIC interface

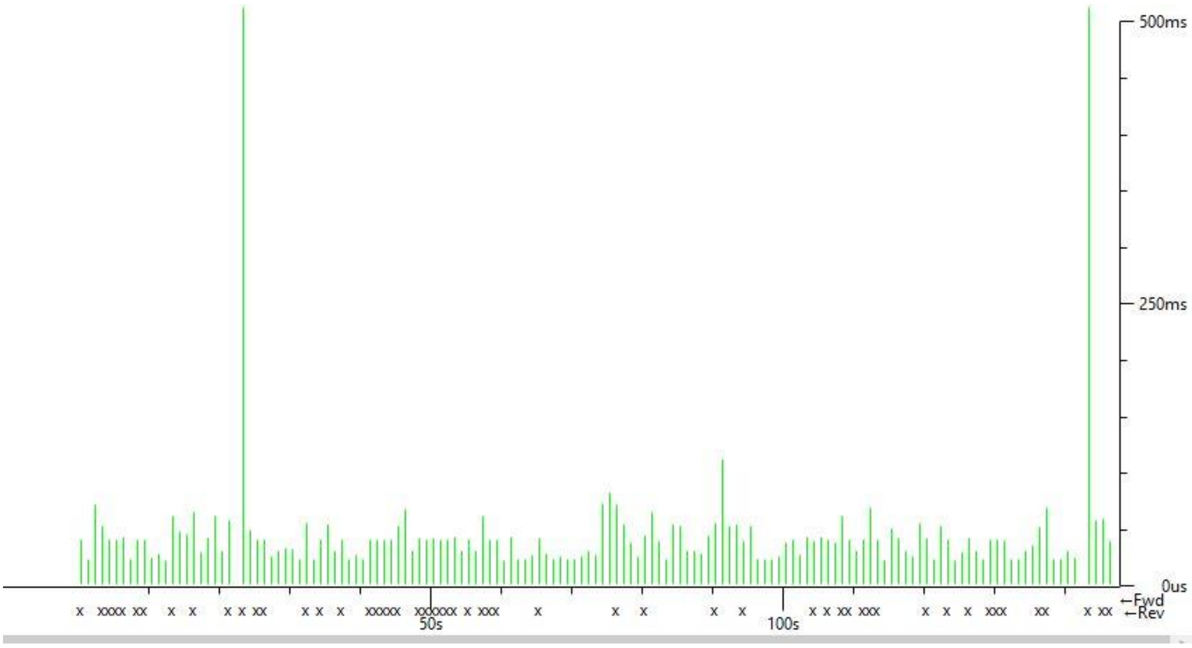

Figure 4.4

In figure 4.4 the max delta from 10.42.43.11 to 10.42.43.10 is 1565.74 ms. The delta happened because number of nodes, distance between nodes and include any time needed to calculate routes

❖ From figures 4.3 & 4.4 achieved the:

-Max delta = 1565.74 ms at packet no. 41728

-Max jitter = 13.80 ms.

-Mean jitter = 1.53 ms.

-Max skew = -113.39 ms.

-Total RTP packets = 7385 (expected 7385)

-Lost RTP packets = 222 (3.01%)

- Sequence -errors = 78

-Duration 147.67 s (-23420 ms clock drift, corresponding to 6731 Hz (-15.86%)

-Packet loss

The total stream from 10.42.43.10 to 10.42.43.11 was 7326 packets. The loss was 65 (0.88 %) packets, from 10.42.43.11 to 10.42.43.10 total number of packets was 7163 packets , loss was 222 (3.01%) packets.

The loss is occurred due to the functionality of UDP protocol because it's connectionless, and if packet is lost it's not send again, also the packet is dropped if it's miss arriving at receiver.

Table 4.1 scenario summary

Source	destination	Max jitter	Mean jitter	Max delta	Packet lost	Sequence error
10.42.43.10	10.42.43.11	26.27 ms	1.58 ms	206.76ms	65 (0.88%)	81
10.42.43.11	10.42.43.10	13.8 ms	1.53 ms	1565.74ms	222 (3.01%)	78

4.2.1.2 Scenario 2

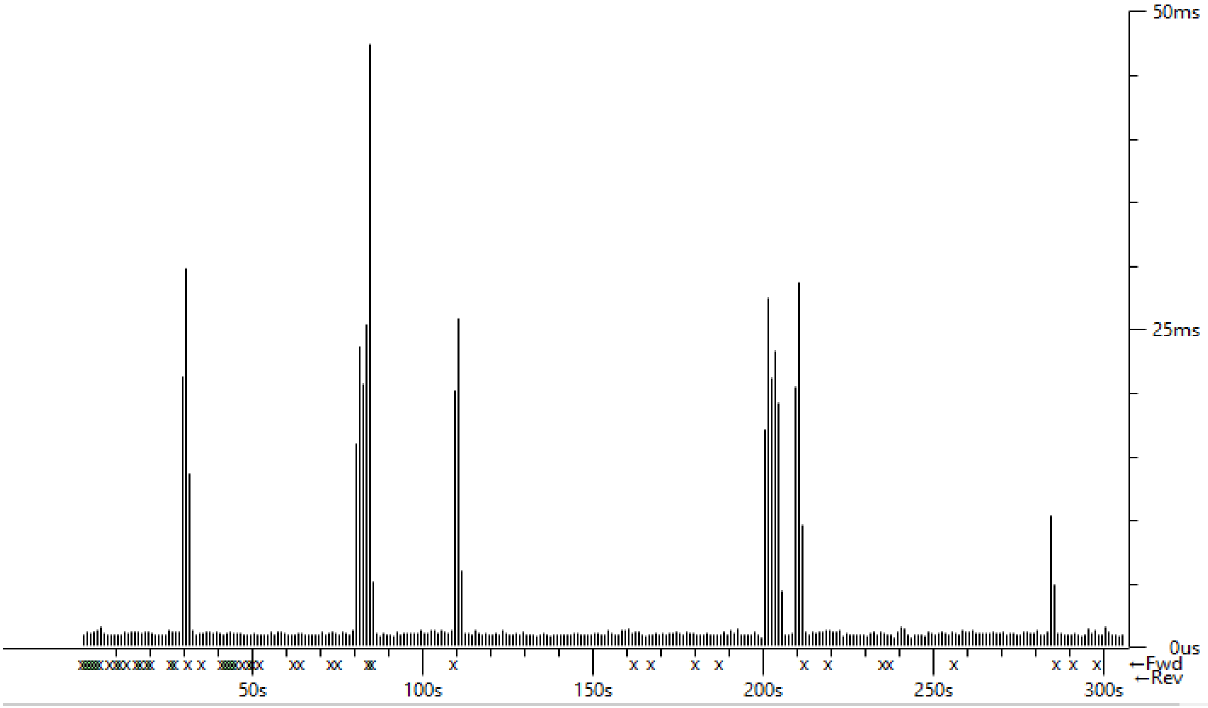

Figure 4.5

In figure 4.5 jitter occurs when packets received in variance in delay. The mean jitter from node 10.42.43.10 to node 10.42.43.11 is 1.47ms, and the max jitter in figure 9 is 47.33ms .

The jitter in above figures occurs due the congestion on the network or the congestion at NIC interface.

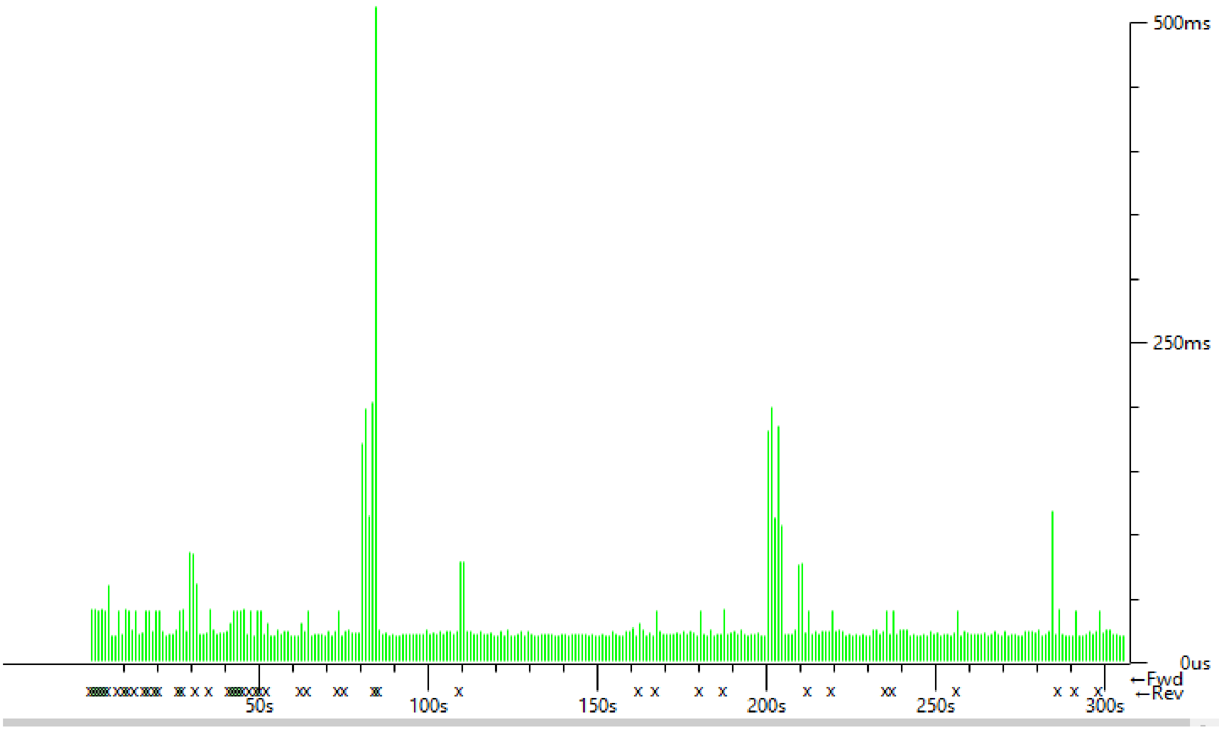

Figure 4.6

In figure 4.6 the max delta from 10.42.43.10 to 10.42.43.11 is 510.25 ms. The delta happened because number of nodes, distance between nodes and include any time needed to calculate routes.

❖ From figures 4.5 & 4.6 achieved the :

-Max delta = 510.25 ms at packet no. 13160 .

.-Max jitter = 47.33 ms. Mean jitter = 1.47 ms.

-Max skew = -874.76 ms.

-Total RTP packets = 15337 (expected 15337).

-Lost RTP packets = 70 (0.46%) .

-Sequence errors = 70 .+

-Duration 306.70 s (-39 ms clock drift, corresponding to 7999 Hz (-0.01%).

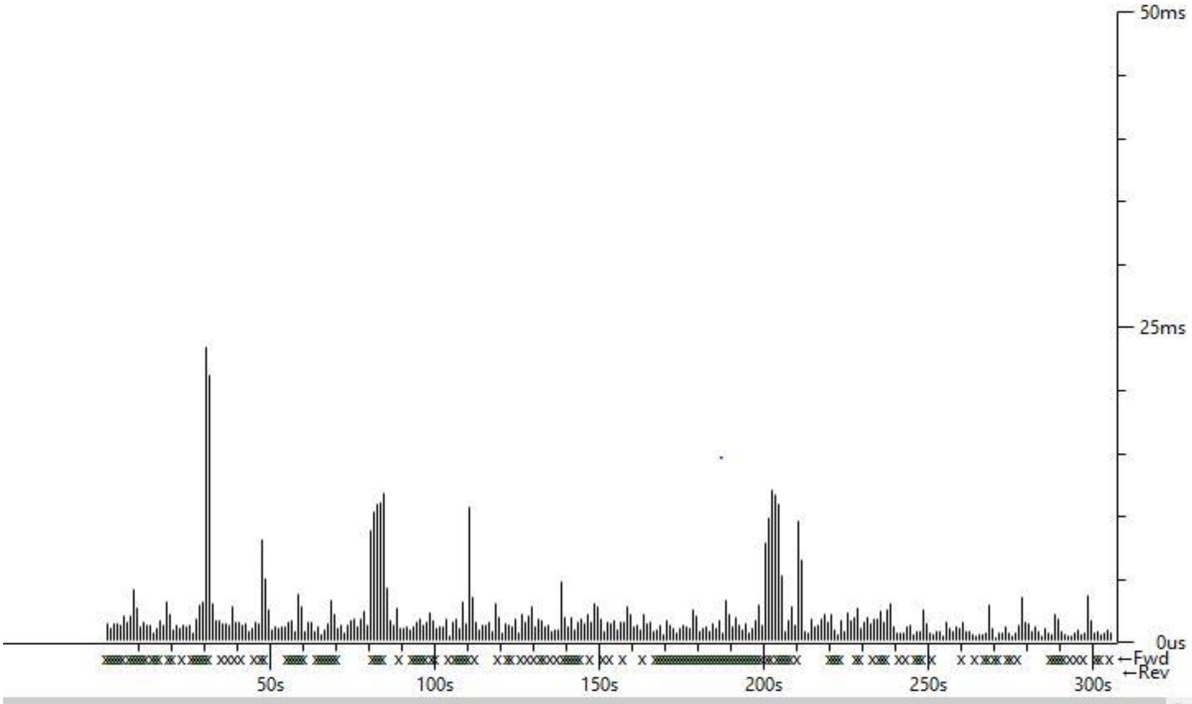

Figure 4.7

In figure 4.7 jitter occurs when packets received in variance in delay. The mean jitter from node 10.42.43.11 to node 10.42.43.10 is 1.11ms, and the max jitter is 23.28ms.

The jitter in above figures occurs due the congestion on the network or the congestion at NIC interface.

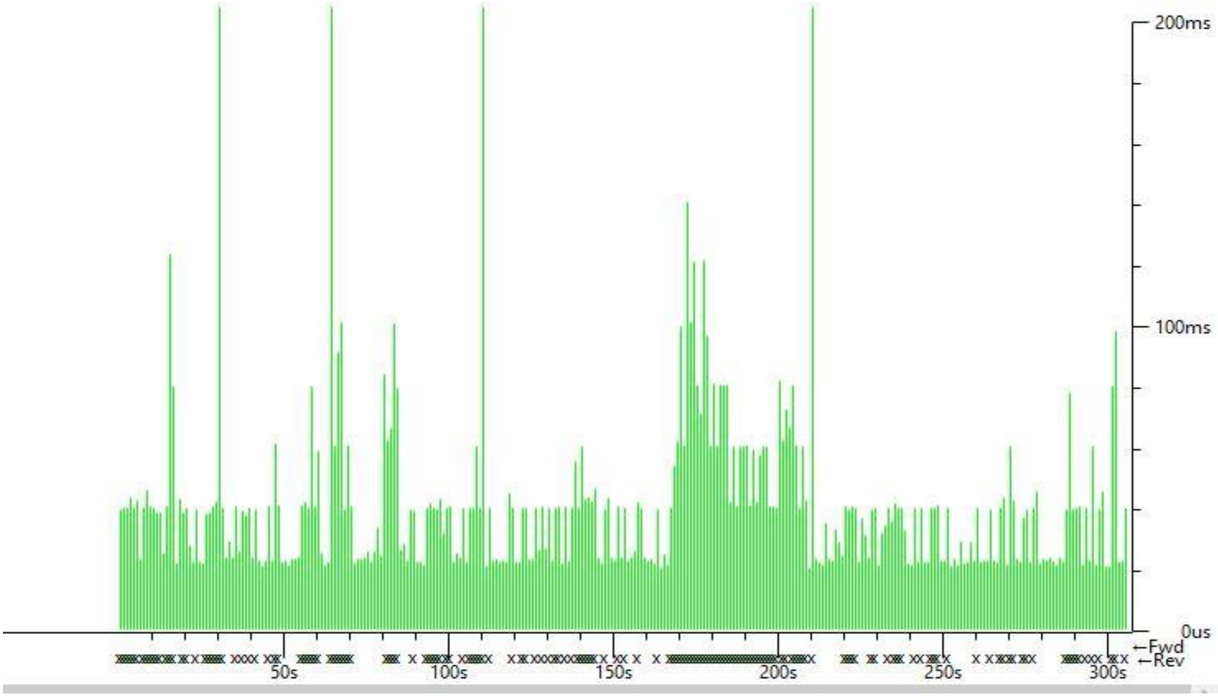

Figure 4.8

In figure 4.8 the max delta from 10.42.43.11 to 10.42.43.10 is 1871.00 ms. The delta happened because number of nodes ,distance between nodes and include any time needed to calculate routes.

❖ From figures 4.7 & 4.8 achieved the :

-Max delta = 1871.00 ms at packet no. 5052 .

-Max jitter = 23.28 ms. Mean jitter = 1.11 ms.

-Max skew = -314.12 ms.

-Total RTP packets = 15343 (expected 15343)

-Lost RTP packets = 1013 (6.60%) .

-Sequence errors = 606 .

-Duration 306.82 s (-43 ms clock drift, corresponding to 7999 Hz (-0.01%).

-Packet loss:

The total stream from 10.42.43.10 to 10.42.43.11 was 15372 packets. The loss was 70 (0.5 %) packets, from 10.42.43.11 to 10.42.43.10 total number of packets was 14330 packets , loss was 1013 (6.6%) packets.

The loss is occurred due to the functionality of UDP protocol because it's connectionless, and if packet is lost it's not send again, also the packet is dropped if it's miss arriving at receiver.

Table 4.2 : scenario summary

Source	destination	Max jitter	Mean jitter	Max delta	Packet lost	Sequence error
10.42.43.10	10.42.43.11	47.33 ms	1.47 ms	510.25 ms	70 (0.46%)	70
10.42.43.11	10.42.43.10	23.28 ms	1.11 ms	1871.00 ms	1013 (6.60%)	606s

Chapter five

Conclusion and Recommendation

Chapter five

Conclusion and Recommendation

5.1 Conclusion

This study observes the performance of WMAN running AODV while VoIP traffic is introduced into the network. It determines the suitability of AODV as a routing protocol for WMANs running a VoIP application. The goal of this research is to determine whether routing protocols affect VoIP end-to-end delay and packet loss in WMANs.

Representative VoIP traffic is submitted to a WMAN and end-to-end delay and packet loss are observed. Node density, and mobility are varied creating a full-factorial experimental design scenario.

Results show that node density, number of data streams, and mobility affect Delay and packet loss. Even with the increase in both packet loss and delay, AODV is still a suitable routing protocol for VoIP traffic. Delays between 20ms to 220ms are significantly below the recommended average 400ms for VoIP applications. This could increase as more traffic is introduced into the WMAN; however, it is still well below the recommended 400 ms. Background traffic is not considered in this experiment but would also increase delay. Packet loss is between 0.5% and 6.6%, which is less than the acceptable 10% for VoIP conversations.

These results show that routing protocols do, in fact, affect delay and packet loss in WMANs and that AODV is quite suitable for routing VoIP traffic in WMANs.

5.2 Recommendation

After experiment found that number of nodes affect the mean jitter according to receiving and retransmitting of packets and that lead to different arriving time of the packets, so as there is a less number of nodes there is low jitter.

References

[1] Ahmad, A. (2005). Wireless and mobile data networks. John Wiley & Sons.

[2] Armenia, S., Galluccio, L., Leonardi, A., & Palazzo, S. (2005, July). Transmission of VoIP traffic in multihop ad hoc IEEE 802.11 b networks: experimental results. In Wireless Internet, 2005. Proceedings. First International Conference on (pp. 148-155). IEEE.

[3] Varshney, U., Snow, A., McGivern, M., & Howard, C. (2002). Voice over IP.Communications of the ACM, 45(1), 89-96

[4] Oouch, H., Takenaga, T., Sugawara, H., & Masugi, M. (2002, November). Study on appropriate voice data length of IP packets for VoIP network adjustment. In Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE (Vol. 2, pp. 1618-1622). IEEE

[5] MURTHY, C. Siva Ram; MANOJ, B. S. Ad hoc wireless networks: Architectures and protocols. Pearson education, 2004.

[6] CONTI, Marco; GIORDANO, Silvia. Multihop ad hoc networking: The reality. Communications Magazine, IEEE, 2007, 45.4: 88-95.

[7] Thibodeau, E., Youssef, M., & Houle, A. C. (2006, May). Investigating MANET performance in a VoIP context. In Electrical and Computer Engineering, 2006. CCECE'06. Canadian Conference on (pp. 920-923). IEEE

[8] Yang, H., & Li, Z. Y. (2011, December). Simulation and analysis of a modified AODV routing protocols. In Computer Science and Network Technology (ICCSNT), 2011 International Conference on (Vol. 3, pp. 1440-1444). IEEE

[9] Maltz, D. A., Broch, J., & Johnson, D. B. (1999). Experiences designing and building a multi-hop wireless ad hoc network testbed. CARNEGIE-MELLON UNIV PITTSBURGH PA DEPT OF COMPUTER SCIENCE.

[10] Klein-Berndt, L. (2001). A quick guide to AODV routing. Wireless Communications Technologies Group, NIST (http://w3. antd. nist. gov/wctg/aodv_kernel/)

[11] Jain, R. (1998). Voice over IP: Issues and Challenges. Nortel, Canada, August,14.