**Sudan University of Science and Technology**

**College of Engineering**

**School of Electronic Engineering**

# Implementation of Test-Bed for VoIPv6 Encryption

A Research Submitted in Partial fulfillment for the Requirements of the Degree of B.Sc. (Honors) in Electronics Engineering

**Prepared By:**

Alkhansaa Abdallah Mohammed

Doaa Salim Mohammed

Walaa Faisal Mohammed

Yusra Osman Alhaj

**Supervised By:**

Dr. Sami Hassan Omer

**September 2014**

قال تعالى:

﴿رَبِّ قَدْ ءَاتَيْتَنِي مِنَ الْمُلْكِ وَعَلَّمْتَنِي مِن تَأْوِيلِ الْأَحَادِيثِ فَاطِرَ السَّمَاوَاتِ وَالْأَرْضِ أَنتَ وَلِيِّي فِي الدُّنْيَا وَالْآخِرَةِ تَوَفَّنِي مُسْلِمًا وَأَلْحِقْنِي بِالصَّالِحِينَ﴾

[ سورة يوسف – 101]

# DEDICATION

To our parents, thank you for all the unconditional dua, guidance, and support that you have always given us.

To our friends, thank you for the support along the way.

# ACKNOWLEDGEMENT

First and above all, we praise God.

Dr. Sami Hassan Omer thanks you for your assistance throughout this research.

This Thesis appears in its current form due to the assistance of several people. We would therefore like to offer our sincere thanks to all of them.

Eng. Mustafa Mohammed Ahmed we deeply appreciate your assistance.

Our families thank you for everything. We warmly thank and appreciate our parents for their material and spiritual support in all aspects of our life.

Thank for everyone who helped to achieve this thesis.

# ABSTRACT

Internet Protocol (IP) has been used for most of modern communication systems standards as a networking protocol. It survived for over 30 years and has been an essential part of the Internet evolution. Today's Internet is a much different than it was 30 years ago. Most traditional communications media -including telephone -are being restructured by the Internet, giving new services such as voice over Internet Protocol (VoIP).

As a result of increased demand for these services, the number of Internet-connected users and devices are growing at a rapid way.

Adopting IP to support new services introduces many challenges such as managing networking resources efficiently and true end-to-end functionality (i.e. end-to-end security, QoS, etc.) which is not feasible with IPv4.

IPv6 designed to be the successor to IPv4 with 128 bit to provide large address space. Additional features are impeded within the design to meet the demands of future networks. Implementing voice over IPv6 network with addition of encryption introduces an assortment of ways configurations.

In this research The Secure Real-Time Transport Protocol (SRTP) will be used for media encryption and Transport Layer Security (TLS) for secure signaling.

Testing Scenario will be conducted using soft-phones and Asterisk free PBX server running in Linux. It is expected that applying an encryption technique on VoIP will degrade QoS parameters.

# المستخلص

استخدم بروتوكول الانترنت كبروتوكول للاتصال في معظم معايير أنظمة الإتصالات الحديثة, لأكثر من ثلاثين عاما ومثّل جزء أساسي في تطور الانترنت . اصبح الانترنت في الآونة الأخيرة مختلفاً عن ما كان عليه قبل ثلاثين عاما إذ أن معظم الخدمات التقليدية من ضمنها خدمات الاتصال الهاتفي أعيد بناؤها بالانترنت مما انتج خدمات جديدة مثل الاتصال الهاتفي عبر برتكول الانترنت. نتيجة لازدياد الطلب على هذه الخدمات اصبح عدد المستخدمين المتصلين بالانترنت ينمو باضطراد.اعتماد هذه الخدمات الجديدة على بروتوكول الانترنت ادى لمواجهة عدة تحديات مثل إدارة موارد الشبكة بكفاءة و التوصيل بين الأجهزة المتصلة دون الحاجة إلى وسيط مع تحقيق السرية وجودة الخدمة..الخ.

تم تصميم الإصدار السادس من بروتوكول الانترنت الذي يستخدم مساحة عنوان بطول 128 بت - ليحل محل الإصدار الرابع من بروتوكول الانترنت لزياده مساحة العناوين مع إضافة الكثير من الخصائص الجديدة والتي ستشكل حاجة في مستقبل الشبكات.

تطبيق خدمة الاتصال الهاتفي عبر بروتوكول الانترنت وإضافة خاصية أمنية له - مثل التشفير- له عدة طرق للإعداد. في هذا البحث سيتم استخدم بروتوكول تأمين النقل بالزمن الفعلي بالإضافة لاستخدام بروتوكول أمن طبقة النقل. سيناريو الاختبار سيتم إجراؤه في هذا البحث باستخدام Asterisk كمخدم في بيئة Linux و الهواتف الرقمية.

يتوقع تراجع معاملات جودة الخدمة (زمن التأخير, نسبة فقدان حزم البيانات...الخ) عند تطبيق بروتوكول السرية.

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# LIST OF APPENDICE

# ABBREVIATIONS

| | |
|---|---|
| 1, 2, 3G | First, Second, Third Generation |
| ADPCM | Adaptive Deferential Pulse Code Modulation |
| AES | Advanced Encryption Standard |
| ARP | Address Resolution Protocol |
| CATNIP | Common Architecture for the Internet |
| CIDR | Classless Inter-Domain Routing |
| CLNP | Connectionless Network Layer Protocol |
| Codecs | Coders/Decoders |
| DoS | Denial of Service |
| DHCPv6 | Dynamic Host Configuration Protocol version 6 |
| DNS | Domain Name System |
| GUI | Graphical User Interface |
| HTTP | Hybrid Text Transfer Protocol |
| IANA | Internet Assigned Numbers Authority |
| ICMP | Internet Control Message Protocol |
| ICMPv6 | Internet Control Message Protocol for IPv6 |
| IETF | Internet Engineering Task Force |
| IGMPv3 | Internet Group Management Protocol version 3 |
| IP | Internet Protocol |
| IPAE | IP Address Encapsulation |
| IPng | Internet Protocol Next Generation |
| IPsec | Internet Protocol Security |
| IPTV | IP Television |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |

| | |
|---|---|
| IPX | Internetwork Packet Exchange |
| ISDN | Integrated Services for Digital Network |
| ISP | Internet Service Provider |
| ITU-T | International Telecommunication Union-Telecommunication Standardization Sector |
| IVR | Interactive Voice Response |
| LAN | local Area Network |
| MCUs | Multipoint Control Units |
| MLD | Multicast Listener Discovery |
| MTU | Maximum Transmission Unit |
| NAT | Network Address Translation |
| NAT-PT | Network Address Translation - Protocol Translation |
| NAT6 | Network Address Translation 6 |
| NAT64 | Network Address Translation 64 |
| ND | Neighbor Discovery |
| OSI | Open System Interconnection |
| PAT | Port Address Translation |
| PBX | Private Box Exchange |
| PCM | Pulse Code Modulation |
| PSTN | Public Switched Telephone Network |
| QoS | Quality of Service |
| RARP | Reverse Address Resolution Protocol |
| RAS | Registration Admission and Status |
| RIR | Regional Internet Registry |
| RTCP | Real Time Control Protocol |
| RTP | Real-time Transport Protocol |
| SDP | Session Description Protocol |
| SIP | Session Initiation Protocol |
| SIP | Simple Internet Protocol |

| | |
|---|---|
| SIPP | Simple Internet Protocol Plus |
| SLAAC | Stateless Address Autoconfiguration |
| SRTP | Secure Real Time Transport Protocol |
| SSRC | Synchronization Source |
| TCP | Transport Control Protocol |
| TCP/IP | Transport Control Protocol/Internet Protocol |
| TCP/UDP | Transport Control Protocol/User Datagram Protocol |
| TLS | Transport Layer Security |
| TUBA | TCP/UDP over CLNP Addressed Networks |
| UA | User Agents |
| UAC | User Agent Clients |
| UAS | User Agent Servers |
| UDP | User Datagram Protocol |
| VoIPv6 | Voice over IP version 6 |
| VPNs | Virtual Private Networks |

# CHAPTER ONE

# INTRODUCTION

# 1. INTRODUCTION

## 1.1 Preface

For a while the range of applications that operate over the Internet, has been dominated by e-mail, and file transfer, and Web interfaces that emphasized text and images, etc.

The abundance of broadband access to the Internet has increased the interest in Internet-based multimedia applications. Multimedia applications which are involve massive amounts of data for visualization and support of real-time interactivity. One of the most widespread multimedia applications is Voice over IP (VoIP).

VoIP allows a user to make long-distance phone calls for a slight investment. The voice is digitized, compressed and sent over the network, then recovered at the other side. [1]

The advent of VoIP followed PSTN due to the need of carrying voice over their data networks.

Each device on an Internet must have a unique IP address to identify the network ID as well as the host's own ID. The Internet is a dynamic environment, the usage of the Internet is differed greatly since IPv4 was developed, which it has a theoretical upper limit of about 4.3 billion unique addresses. The actual number

of devices has been increased dramatically, considering the multiple Internet-enabled devices such as smart phones, tablets and laptops. Thus there is inefficiency in the allocation of IPv4's addresses over the years. NAT had been put forward as substantial solution, but it emerged an issue about the end-to-end nature of IP computing.

IPv6 had been presented as the best hope to meet the demands of Internet users. IPv6 provides enormous number of addresses which it enables globally unique IPs for all devices, which called off the need for NAT. IPv6 header has two QoS-related fields; flow label, and traffic class identifier, which improved QoS.

Cellular telephone systems present a large deployment field for Internet Protocol devices as mobile telephone service transiting to "next-generation" 4G technologies, in which voice is provisioned as a Voice over Internet Protocol (VoIP) service. This mandates the use of IPv6 for such networks. And add acceptable level of security.

Overall, it seems a sensible idea to implement VoIP on an IPv6 network to contribute to its widespread, and to make use of IPv6 features. This project emphasizes the implementation of TLS and SRTP, and the measurement of QoS parameters for the secure and unsecure telephony calls.

## 1.2 Problem Statement

All fourth generation (4G) telecommunication standards are mainly based on packet switching infrastructure. Moreover IPv6 is being mandatory for such standards since the number of connected devices is growing and the bandwidth requirements are increasing. Furthermore, for most of new services true end-to-end functionality is needed which is viable only through IPv6. Thus, various configuration scenarios have been proposed to standardize an optimum scenario for implementing voice over IPv6 and adding an acceptable level of security.

## 1.3 Proposed Solution

An implementation of test-bed platform for voice over IPv6 is needed to evaluate various scenarios and define the optimum architecture for encrypted voice over IPv6 components.

## 1.4 Objective

- To implement a Test bed.
- To configure IPv6 on the network nodes and asterisk server.
- To make voice over IPv6 calls.
- To sniff the voice over IPv6 conversations between two nodes.
- To implement secure calls based on SRTP and TLS as voice security protocols.

## 1.5 Methodology

An inductive approach is concerned with data analysis to generate new theory while the deductive method begins with hypothesis.

Deductive approach is adopted in this thesis to implement encrypted voice over IPv6 testing environment. Both virtual and physical platform are used to assure maximum flexibility, adaptability and reusability.

The VoIP communication was tested on a LAN with installed soft- phones to make calls through it .they were selected so as to support IPv6, SIP as signaling protocol and both SRTP ,TLS as VoIP security support protocols.

Free PBX server AsteriskNow version was used in order to forward the calls between two soft-phones. Wireshark version 1.10.6 was used as a packet sniffer tool to capture packets, displays message exchanges and reports performance data such as quality of service parameters.

## 1.6 Thesis Outlines

Chapter Two and chapter Three illustrate the literature review. The former give an overview of IPv6 based networks while the later describe voice over IP and an encryption technique. An explanation of testing platform for VoIPv6 and result are described in chapter Four. Then Conclusion and recommendation of future works are drawn in chapter Five.