



Securing VoIP in SIP Mobil Network

By

Zaid Salah Munef

Supervisor

Prof. Dr. Alaa Alhamami

**This Thesis is submitted as the Partial Fulfillment of the Requirements for the
Master Degree in Computer Science**

College of Computer Sciences and Informatics

Amman Arab University

Nov 2014



تأمين الصوت المنقول عبر الأنترنت في شبكة الموبايل SIP

إعداد

زيد صلاح منيف

إشراف

الأستاذ الدكتور علاء الحمامي

قدمت هذه الرسالة لأستكمال متطلبات الحصول على درجة الماجستير

في علم الحاسوب

قسم علوم الحاسوب - كلية العلوم الحاسوبية والمعلوماتية

جامعة عمان العربية

تشرين الثاني ٢٠١٤

Authorization

I, Zaid Salah Munef, authorize Amman Arab University to reproduce this thesis in whole or in part for research purposes.

Name: Zaid Salah Munef

Signature: 

Date: 4/11/2014

Resolution & The examining committee

This dissertation, titled "Securing VoIP in SIP Mobil Network ", has been defended and approved.

Examining committee

Title

Signature

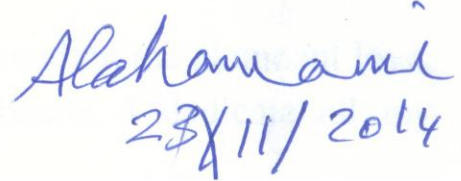
Prof. Dr. Riyad Al-Shalabi

Chair



Prof. Dr. Alaa Al-Hamami

Supervisor



Prof. Dr. Ahmad Kayed

Member



Dedication

I dedicate this thesis to:

My Family,

My Sisters,

My fiancée Sarah Al-Ramli,

My Colleagues Rafal Al-Khashab and Dhura Al-Azawi,

and My favorite friends.

Finally I would like to thank all members for sending me abundant love, encouragement and support from all their hearts. I dedicate all my success to each one of them.

Acknowledgment

I would like to express my warm thank to my supervisor Prof. Dr. Alaa Al-Hamami who provided me with his full support, encouragement and guidance to get this dissertation in its present form .Without his help and support, this work would not see the light. He was available at all times I needed his help, I would therefore like to convey my sincere gratitude to him.

My grateful appreciation goes to the Dean of College of Computer Sciences and Informatics, all of the lecturers, administration and staff of Amman Arab University.

List of Abbreviations

Abb.	Meaning
2G	Second Generation
AES	Advanced Encryption Standard
AR2SS	AES & RSA Speed and Security
ARP	Address Resolution Protocol
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DEFSOP	Digital Evidence Forensics Standard Operating Procedures
DoS	Denial of Services
EAP-SIM	Extensible Authentication Protocol - Subscriber Identity Module
GB	Giga Byte
GK	Gate Keepers
GW	Gate Ways
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSec	Internet Protocol Security
ITU-T	International Telecommunication Union and Telephony
MAC	Media Access Control
MCU	Multipoint Control Units
OAEP	Optimal Asymmetric Encryption Padding
PCT	Private Communication Technology
PSTN	Public Switched Telephone Network
RAM	Random Access Memory
RSA	Rivest-Shamir-Adleman
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
Wi-Fi	Wireless Fidelity

List of Tables

No.	Description	
Table (1-1)	Comparison between SIP and H.323	
Table (4-1)	The first experiment	
Table (4-2)	The second experiment	
Table (4-3)	The third experiment	
Table (4-4)	The forth experiment	
Table (4-5)	The fifth experiment	
Table (4-6)	The sixth experiment	

Contents

Authorization.....	III
Dedication	V
Acknowledgment.....	VI
List of Abbreviations	VII
List of Tables	VIII
Abstract	XI
المخلص	XIII
Chapter One:Introduction &Background.....	1
1-1Introduction.....	2
1-2VoIP Service	3
1-3VoIP Components	6
1-4Contribution	17
1-5Statement of Problem.....	18
1-6Thesis Organization.....	19
Chapter Two:Literature Review	20
2-1Introduction.....	21
2-2Literature Review	22
2-3Summary	36
Chapter Three:Theoretical Design	37
3-1Introduction.....	38
3-2Tools	41
3-3Used Algorithms	42
3-4Summary	52
Chapter Four:Experimental Works	53
4-1Introduction.....	54

4-2Interfaces Execution	55
4-3Experiment	66
Chapter Five:Conclusion and Future works	75
Introduction.....	76
5-1Conclusion	76
5-2Future works.....	78
References.....	79

Abstract

Lately, the development and progress have become significant in the field of information technology, especially in the field of data transmission via internet. One kind of the data transfer is voice. In addition to that, the development in the field of mobile devices, which is possibility supplying the device by internet service became a paradigm shift, that grabs people in hugely way to be used widely.

These developments in the field of technology are concurring many problems, where it had a direct impact on this development and the turnout by the users. Some of these problems: eavesdropping call between the two parties, they must choose secured way to transfer audio to the other party. As well as when untrusted users enter the program which supports audio transfer, the administrators can deal with this problem by identifying a list of authorized users to enter this program.

In this thesis, the model's implementation has done on a mobile device (Which is operating by (Android) system). Because recently it has been widely used among different people, dealing with sound transfer process has been via the internet using the SIP server to authenticate the communication process between two parties, and to make sure the reliability of persons and this process, after that RSA algorithm (key size used 1024 bit) is using of increased the encryption keys strength and exchanged between the two parties and to ensure that the packet transmitted every time. (AES) algorithm used to encrypt the package, the reason of choosing this algorithm that is very effective, which is associated with the encryption speed. Key size used in the proposed model with AES is (256 bit) to ensure the secured and speed of the proposed operation.

Results of experiments showed that the sent 20016 byte to each sender packet size, which is including 16 byte for key. It will be receiving 20000 bytes, and the total time between the encryption and decryption process for each packet is 2-5millisecond. These results depend on the quality of service (Internet) from one side and by the number of users from the other side where the commensurate is affecting of extrusive.

المخلص

مؤخراً ، اصبح التطور والتقدم الحاصل في مجال تكنولوجيا المعلومات ملحوظ بشكل كبير ، وخصوصاً في مجال نقل البيانات عبر الإنترنت، أحد انواع هذه البيانات هو الصوت. يضاف الى ذلك التطور في مجال الاجهزة الخلوية ، حيث اصبح بالامكان تزويد الجهاز بخدمة الانترنت والتي تعتبر نقلة نوعية له وادى ذلك الى الاقبال الهائل على استخدامه من قبل المستخدمين بشكل واسع.

أدى التطور في مجال التكنولوجيا الى ظهور العديد من المشاكل، التي كان لها التأثير المباشر على هذا التطور وعلى العديد من مستخدميه. والبعض من هذه المشاكل : هو التتصت على المكالمات ما بين طرفين ، فيجب اختيار طريقة آمنة لنقل الصوت الى الطرف الآخر. كذلك عندما يقوم احد المستخدمين الغير مخولين بالدخول على احد برامج نقل الصوت، حيث يمكن للمسؤول عن البرنامج التعامل مع هذه المشكلة عن طريق تحديد قائمة للمستخدمين المخولين بالدخول الى هذا البرنامج.

في هذه الأطروحة، تم تنفيذ النموذج على جهاز الهاتف النقال (والذي يعمل بنظام تشغيل (Android)). لأنه في الاونة الاخيرة ، انتشر استخدامه على نطاق واسع بين مختلف الاشخاص، وتم التعامل مع عملية نقل الصوت عبر الإنترنت باستخدام خادم SIP لضمان عملية الاتصال ما بين الطرفين والتأكد من موثوقية هذه العملية والاشخاص ، بعد ذلك يتم استخدام خوارزمية RSA (حجم المفتاح المستخدم ١٠٢٤ بت) لزيادة قوة مفاتيح التشفير وتبادلها بين الطرفين وضمان الحزمة التي تنتقل في كل مرة. تستخدم خوارزمية (AES) لتشفير الحزمة، والسبب في اختيار هذه الخوارزمية هو فعاليتها الكبيرة التي ترتبط مع سرعة التشفير. حجم المفتاح المستخدم في النموذج المقترح مع AES هو (256 بت) لضمان أمنية وسرعة العملية المقترحة.

أظهرت نتائج التجارب من النموذج المقترح ان حجم الحزمة المرسله ٢٠٠١٦ بايت منها ١٦ بايت حجم المفتاح ، لتكون الحزمة عند المستقبل ٢٠٠٠٠ بايت، وان الوقت الاجمالي بين العمليتين (التشفير وفتح التشفير) هو ٢-٥ جزء من الثانية لكل حزمة. هذه النتائج تعتمد على نقطتين مهمتين: النقطة الاولى هي جودة الخدمة (الإنترنت)، والثانية هي عدد الاشخاص المستخدمين لها، ويكون تأثير كل نقطة على الاخرى هو تأثير طردي.

Chapter One: Introduction & Background

1-1 Introduction

In our world fields the significant developments occurred in different of life such as (Medicine, Engineering, Cultivation, Science, Technology etc.). The development of technology domain represents computer, communication, and mobile. Especially new generation of mobile, led to increase number of mobile users, and revolutionize the domain usage of new mobile because it works to present service on widely used.

The mobile is more than just device for making phone calls; it gives developments in hardware and software. Mobile phones use have been expanded such as send messages, check emails, process of shopping, banking service, store contacts, select map's, store important dates, camera service and other uses.

Part of the most useful is mobile Wireless Fidelity (Wi-Fi) that led to develop new services in domain transfer of media, including voice transfer known as Voice over Internet Protocol (VoIP).

VoIP service is providing very low-cost or semi-free voice calls. Through internet, and draws of attention many internet users. The VoIP services are generate from fixed sized packets. The size of VoIP packet is relatively small compared to other video or web packets, and the redundant header size of a VoIP packet is larger than the size of the payload including voice information (Jung & et al, 2013).

VoIP is subjected to various types of attacks that called capturing packets, eavesdropping communications and many other types. For that transmissions of media need different factors like confidentiality, authentication, and integrity with replay protection to the media stream.

The confidentiality of the data means that the encrypted data is indistinguishable by anyone who does not have the key. Message authentication implies that if second part as a user agent server receives a datagram apparently sent by first party as a user agent client, then it was indeed sent by first party. Data integrity implies that any modification of the data during transmission will be detected by the recipient (Rakotondraina & et al, 2013; Kumar & Chauhan, 2013).

1-2VoIP Service

To explain some concepts that dealing with the VoIP, the concept and their meaning:-

1.1.1 Types of VoIP service

There are different types of VoIP based on the infrastructures employed by the owner of the network. There are three known services used in VoIP (Alo & Firday, 2013):-

1.1.1.1 Computer to Computer

Computer to Computer service provides internet telephony free using the same softphone software such as Skype, Instant Messaging, AOL etc. this type provides voice transfer from caller to receiver by internet protocol, and both parties must be using their computers in order to place calls. The following requirement must be met to use computer to computer VoIP service: softphone software, a sound card and good internet service, and the caller with receiver should be online, as shown in Figure (1-1).



Figure (1-1): Computer to Computer

1.2.1.2 Computer to Phone and Vice Versa

This is a software-based and hardware-based service. Softphone software is used to route the call an Internet Protocol (IP) and hands off to a conventional telephone network. To use the service, one needs to subscribe and be charged at a low rate. Examples include Skype, MSN and Google Talk that provides the service to enable their customers to call landline from their computer.

Computer to phone requirements are internet-enabled phone and computer, VoIP service subscription, modem and analog terminal adapter to convert the call signal to digital signal and also back to analog signal. Computer to phone does not allow emergency call users and the computer needs to have a computer connected to the internet, as shown in Figure (1-2).

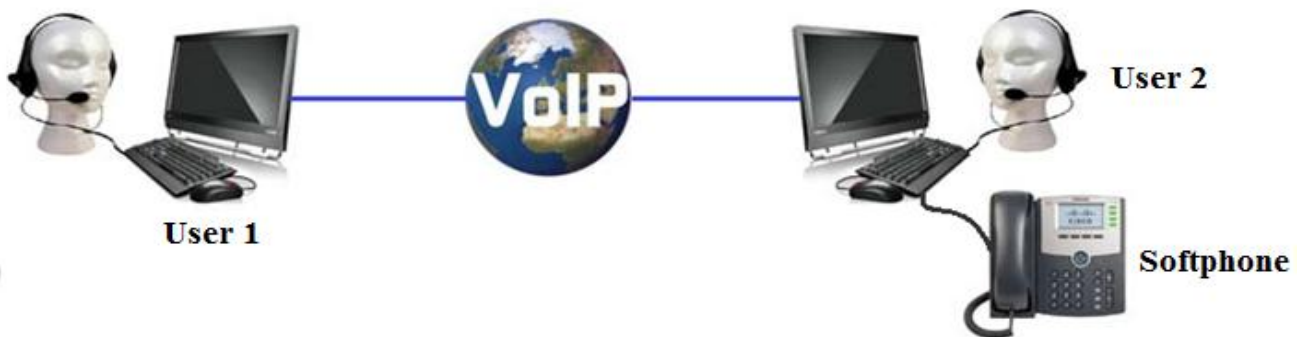


Figure (1-2): Computer to Phone Service

1.2.1.3 Phone to Phone

This is a hardware-based service that allows the caller and receiver to call each other using the internet. Different companies in the world use this type to handle long distance calls. In this type, voice converts to the packets and transfer it over the IP. It allows emergence calls and does not need Public Switched Telephone Network (PSTN) for begin and termination of calls as shown in Figure (1-3).



Figure (1-3): Phone to Phone Service

1.2.2 VoIP Security Threats

There are different key elements of VoIP threat, such as the following (Keromytis, 2009):

- 1.2.2.1 Social Threats:** this type targeted directly against humans. Such as, misconfigurations, bugs or bad protocol interactions in VoIP systems may enable or facilitate attacks that misrepresent the identity of malicious parties to users.
- 1.2.2.2 Eavesdropping, Interception, and Modification Threats:** this type is cover situations, when the intruder can listen in on the signaling (call setup) or the content of a VoIP session, and possibly modify aspects of that session indirectly while avoiding detection.

- 1.2.2.3 Denial of Service Threats:** this type is denial the user from access to the VoIP services. This may be particularly problematic in the case of emergencies, or when a DoS attack affects all of user's or organization communication capabilities. It may be occurred by VoIP protocol. They may also involve attacks through computing or other infrastructures (e.g., shutting down power).
- 1.2.2.4 Service Abuse Threat:** this type is covering the improper use of VoIP services, especially in situations where such services are offered in a commercial setting. Such as threats that include toll fraud and billing avoidance.
- 1.2.2.5 Physical Access Threat:** this type is referring to inappropriate/unauthorized.
- 1.2.2.6 Physical Access** to VoIP equipment, or to the physical layer of the network.

1-3VoIP Components

There are different elements of VoIP components, such as the following:

1.3.1 End-user Equipment

The end-user equipment is used to access the VoIP system to communicate with another end point. Connection to the network may be physically cabled or may be wireless, therefor it is considered the most important part in the VoIP component.

The end-user equipment may be a phone that sits on a desk or a softphone that is installed a program on PC, it include voice and possibly video communication, and may contain instant messaging, monitoring and surveillance capabilities (Sans, 2014).

1.3.2 VOIP Protocol

There are different types of VoIP protocols in network, but only the most commonly used ones are UDP, TCP, H.323 and SIP :-

1.3.2.1 User Datagram Protocol (UDP)

The UDP is defined to make available a datagram mode of packet communication between two devices in the networks. This protocol sent packet without wait any response from second party.

The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed. And it is containing checksum field, which is processing errors that occur between transmitter and receiver (Forouzan, A. B., 2006), as shown in Figure (1-4):-

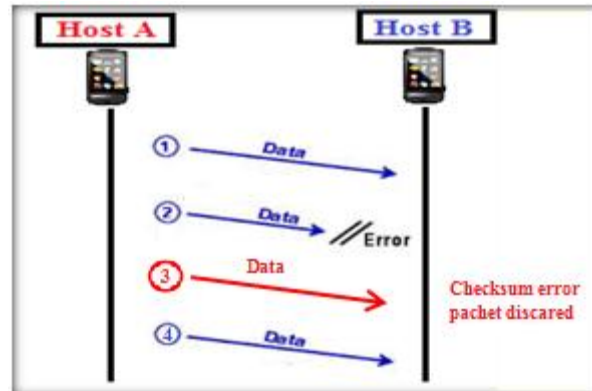


Figure (1-4): UDP Protocol

1.3.2.2 Transmission Control Protocol (TCP)

The TCP protocol before two terminals establish a connection, they will execute a process called handshaking that is a process of negotiation. TCP will establish a specific connection between source and destination for the communication.

The transfer packet should be in sequence and does not send any packet before make sure the arrival of the prior packet, because the TCP packet depends on:-

Sequence number: each endpoint of a TCP connection establishes a starting sequence number for packets it sends from source.

Acknowledgement number: it is contained receive packet response from destination, if the response is positive then source sent the next packet. But the response is negative; the source resent the same packet (Forouzan, A. B., 2006).

As a result of handshaking, TCP will establish in connection between two terminals for this communication, so that TCP will cost more time depends on network traffic condition than UDP to finish it. But the ensure safety arrival of packet in TCP is better than UDP, as shown in Figure (1-5):-

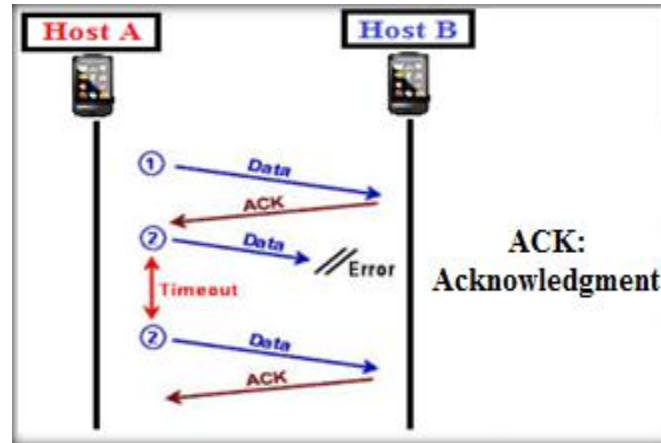


Figure (1-5): TCP Protocol

1.3.2.3 H.323 Protocol

H.323 is developed by International Telecommunication Union and Telephony (ITU-T) that define the protocols to provide audio communication sessions on any packet network. The H.323 makes it possible to create and deploy new services quickly and to take advantage of multimedia capabilities.

It is defining several network elements that work together in order to deliver rich multimedia communication capabilities. Those elements are Terminals, Multipoint Control Units (MCUs), Gateways (GW), Gatekeepers (GK), and border elements. Collectively, terminals, multipoint control units and gateways are often referred to as endpoints.

The H.323 is widely used within various internet real-time applications like NetMeeting and is widely deployed worldwide by service providers and enterprises for VoIP networks. The H.323 standard addresses call signaling, multimedia transport, and bandwidth control for point-to-point and multi-point conferences. Therefore the H.323's strength depends on data important (Malhotra & Kaur, 2011), as shown in Figure (1-6).

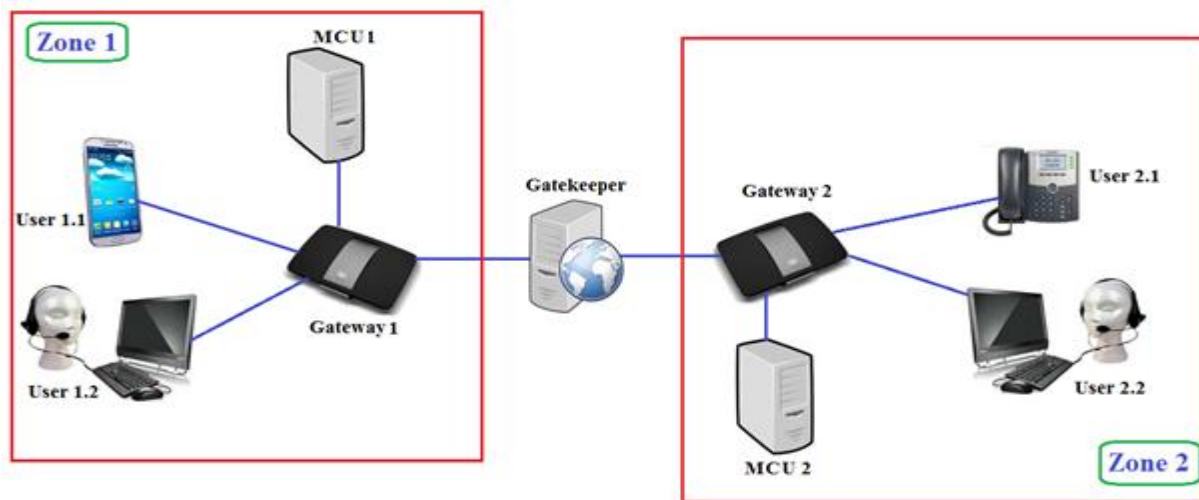


Figure (1-6): H.323 Protocol

1.3.2.4 Session Initiation Protocol (SIP)

The SIP is a standardized Internet Engineering Task Force (IETF) signaling /controlling protocol, for initiating, manipulating, managing and terminating interactive communication sessions between users, these sessions may include voice, video, instant messaging (Voznak & Rozhan, 2013; Krishna, 2013).

SIP is used to setup IP based multimedia services such as audio and video streaming, instant messaging, and other real-time communication across commonly used packet networks. This protocol is becoming widely use in coming years and more popular than the H.323 family, because it is simpler nature and flexible design (Voznak & Rozhan, 2013; Krishna, 2013), as shown in Figure (1-7).



Figure (1-7): SIP Protocol

The SIP is mediator between two parties and it is transfer data between two clients, the SIP server is receive the data from sender in packet form like Hypertext Transfer Protocol (HTTP), so opens many opportunities for several attacks such as registration hijacking, impersonating a proxy and Denial of Services (DoS). SIP is a signaling protocol, and during the signaling phase several parameters are exchanged between the end users. These parameters contain the sensitive information like the user name and the location of the user.

Security concept of SIP are becoming a main problem due to adoption to the SIP based VoIP system, when being established call between two parties, the conversation should be protected and the information should not be revealed to an outsider by applying different security parameters. These parameters are (Voznak & Rozhan, 2013; Krishna, 2013):-

- (1) Confidentiality and Integrity

SIP can use confidentiality to prevent malicious users from call monitoring, which contains the information such as caller presence status, buddy list and contact address. The system would be vulnerable to many attacks like message tampering, and eavesdropping.

To provide confidentiality in SIP server, there are different encryption techniques, which provide user authentication, such as: symmetric encryption and asymmetric encryption.

While the integrity service using to protect the source of data and providing the authentication service, without integrity control to drive to any system is non-trusted has the ability to modify the different contents without any notice.

(2) Authentication and Privacy

The users should know what kind of information is used in transfer through the communication, and it should be encrypted for access successfully to other party. The SIP server can use authentication and privacy concepts for protect data from unauthorized access, interruption, delay or modification.

This concepts present many threats to the applications such as message tampering, and eavesdropping, so that required an implementation of a set of secure interfaces, which provide authentication, authorization and integrity.

(3) Availability

SIP is need availability of secured voice resources on ability to access desired data or required services; this means when user requires or requests any services, a system should ensure the user can access the required service without any problem.

But sometimes this parameter is not possible due to various attacks such as Denial of Service (DoS) attacks or Distributed Denial of Service (DDoS) attacks.

These parameters offer suitable environment to threats, A SIP system is vulnerable to common IP and VoIP threats. That threats are represent of intruder, this intruder provide data by eavesdropping through know the IP between user and SIP server.

So that should be to find the sip security mechanism, different numbers of security protocols or schemes that should be integrated with the SIP protocol or used together with the SIP, to improve the security. These protocols and schemes are suggested and recommended by IETF, but most of them originated from communications communities.

1.3.2.5 Comparison between SIP and H.323

After explain the all commonly protocols, choosing the SIP server for the following reasons through that declared the most important difference between the SIP and H.323. Additionally, the SIP server is having more flexible design to make activity security (Forouzan, A. B., 2006 ; Voznak & Rozhan, 2013; Krishna, 2013), as shown in Table (1-1):

Table (1-1) Comparison between SIP and H.323

Type	SIP	H.323
Transport	Either TCP, UDP or both, The UDP protocol is mostly used for signaling.	Either TCP or UDP (mostly TCP for signaling).
Security	Supports authentication and encryption.	Uses H.235 for security mechanisms.
Capability Exchange	Uses Session Description Protocol (SDP) for ensure arrival data to the other party.	Uses H.245 for call control.
Memory	Uses low memory.	Uses high memory.
Data	Text, voice or video.	Multimedia only.

1.3.3 Security Methods of VoIP

There are different types of VoIP security through encryption algorithm, but only used in this thesis the most commonly ones are AES and RSA:-

1.3.3.1 Advanced Encryption Standard (AES) Algorithm

The AES is use to provide security for sensitive data, and it is based on Substitution and Transposition methods. The AES is used in many password-protected documents and wireless communications such as wireless sensor networks, and also in top secret government files, for which it was first built (Cho & et al, 2013; Pradhan & Bisoi, 2013).

This algorithm is take the input data block of size 128 bit and a variable key size of 128, 192 or 256 bits for 10, 12 or 14 rounds respectively. Each round consists of several processing steps, including the encryption step itself. Similarly, set of reverse rounds are performed to transform ciphertext back into plaintext, the pictorial representation of the AES encryption process to encrypt 128-bit in plaintext to 128-bit in ciphertext. When the plaintext size is more than 128-bits, it will be divided into blocks of 128-bit plaintext (Cho & et al, 2013; Pradhan & Bisoi, 2013), as shown in Figure (1-8).

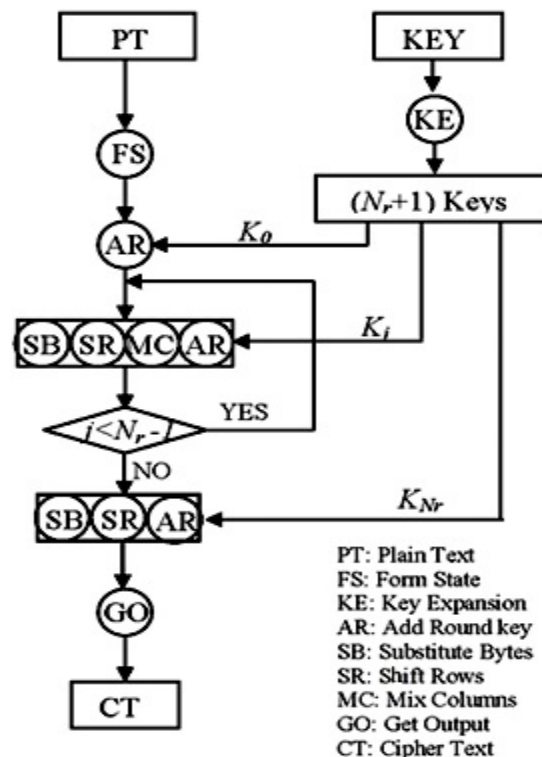


Figure (1-8): AES Encryption Flowchart (Stein, Y. and Malepati, H., 2008)

In such situation, AES encryption will be done for each block separately. So, the sensitive part of the algorithm is the secret key. Therefore should be motivated to do some processing to give more security to this key (Cho & et al, 2013; Pradhan & Bisoi, 2013), as shown in Figure (1-9).

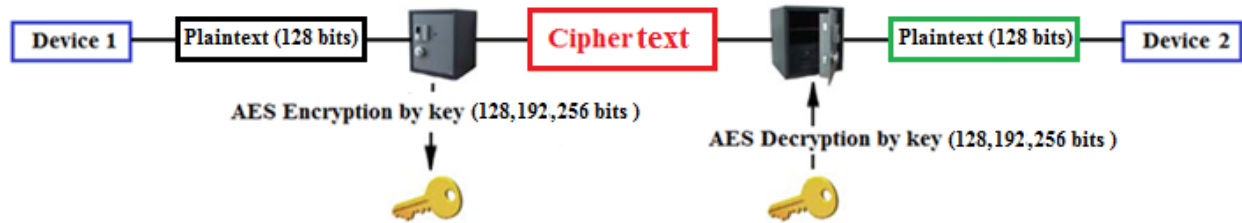


Figure (1-9): AES

1.3.3.2 Rivest-Shamir-Adleman (RSA) Algorithm

The RSA algorithm is one of the most popular public-key encryption and it is kind of asymmetric encryption methods. It is can be used both for encryption and signature. The importance of this algorithm resides in the fact that it underlies well known systems such as Secure Sockets Layer (SSL) and Private Communication Technology (PCT), as well as many of the firewall and network security products currently available.

The handheld devices such as mobile phones or some other development devices such as sensors will not have enough resources to provide adequate levels of security if RSA is used.

In addition to that, VoIP networks are growing very fast, so a larger volume of VoIP traffic is expected and this will significantly increase the cost of supporting RSA computations.

Depending on the RSA algorithm in the future means increasing the corresponding keys sizes in order to cope with the improvement of processors speeds that the attackers might use to attack this algorithm. Unfortunately, increasing the keys sizes will worsen the performance (Naqi & et al, 2013; Kumar & et al, 2013), as shown in Figure (1-10).

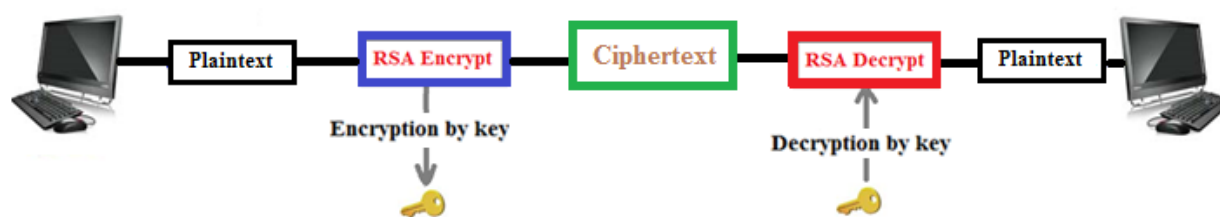


Figure (1-10): RSA

Therefore in this case, the proposed model is using RSA and AES to reduce the intruder attacks and problems of get data during the process of transportation, as discussed in statement of problem.

1-4Contribution

The main contribution in this thesis is focusing to present a suitable solution for reducing problem of the voice transmission, and these contributions summarized as the following:

1. Quality of service which represent process speed of the voice transmission for delivering the voice to the second party, which it is depending of the service provider.

2. Data integrity from any types of intruders, which the intruder is eavesdropping or monitoring on the voice by RSA and AES encryption algorithms.
3. Non-repudiation that represented the third party which ensuring the calling process between the two parties by SIP server.

1-5Statement of Problem

In these days, the development of voice transmission field generates many problems especially, the evolution is of mobile technology, which they have many benefits that represent as ease of communication, easy to use and speed to connection, all these benefits leads when the consumer to use mobile nested of other device such as personal computer, iPad and so on.

The intruder problem considered from dangerous problem because the voice transferred might have important and sensitive information. Therefore the protection of data from misused is essential, and needed the encryption and decryption to provide the protection. So, the problems of intruders notes through eavesdropping or monitoring the data.

The VoIP is considered one types of voice transmission, so it needs to protect. Therefore, in this thesis, the encryption is applied on the voice to produce the cipher voice and the decryption is applied to retrieve the original voice.

1-6 Thesis Organization

This thesis includes four chapters in addition to chapter one. The following is a summary for the chapters:

- Chapter two: it presents the main problem that discussed in this research, and summary of the most important related works.
- Chapter three: it introduces a description of a proposed solution of the problem, explained by flowcharts and algorithms.
- Chapter four: it discusses the experimental works and results.
- Chapter five: it introduces conclusions and future works for this research.

Chapter Two:Literature Review

2-1 Introduction

During the last decades, the development technology was occurred the information of technology field generally, and the communication field specifically that represented on mobile technology. The biggest technology development was achieved especially in transferring the information and data through the internet.

The development caused many problems; the main problem is how to avoid the intruder in addition to other problems, as the following:

1. The intruder can discover the important information or data through reading the text or eavesdropping on the voice.
2. The delayed time occurred through the transferring process.
3. To ensure that interruption problem not occurred between the two parties.

The transmission process from sender to receiver should protect data through a specific secure method because data is very important.

In this thesis, we will choose one type of the data transmission techniques which is voice transmission. Because it is threatened by the intruder, so it should transfer the data between two parties with high protection and suitable speed here.

We will try to achieve this by designing a model to secure data before send it to other party, as shown in Figure (2-1).

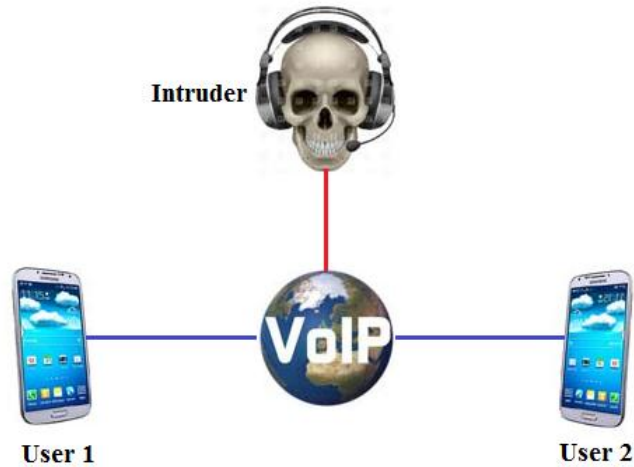


Figure (2-1): VoIP Threats

2-2 Literature Review

Caimu Tang and Dapeng Oliver Wu (Tang & Oliver, 2007): In this paper, the authors proposed a novel and efficient mobile authentication scheme which is suitable for low-power mobile devices, and its security property has been analyzed. It uses an elliptic-curve-cryptosystem based trust delegation mechanism to generate a delegation passcode for mobile station authentication, and it can effectively defend all known attacks to mobile networks including the denial-of-service attack.

Moreover, the scheme requires one scalar point multiplication operation and two short messages on mobile stations for each session establishment after the initial one-time delegation key verification.

. This station only need to receive one message and send one message to authenticate itself to a visitor's location register, and the scheme only requires a single elliptic-curve scalar point multiplication on a mobile device. Therefore, this scheme enjoys both computation efficiency and communication efficiency as compared to known mobile authentication schemes.

R. Vargic, et al (Vargic & et al, 2013): The authors are proposed a solution for two issues in current communications: **Firstly**, that IP Multimedia Subsystem (IMS) suffers from lack of clients. **Secondly**, the mobile operators want to give the subscriber a possibility to access their VoIP network and efficiently cover special, densely populated areas like airports. To address these problems, they developed a novel service architecture, which allows second Generation (2G) subscriber access to a SIP based VoIP network via Wi-Fi complying security standards, such an approach can be used especially in highly-populated areas, such as airports and business centers.

The user authentication and authorization is based on algorithm used the Extensible Authentication Protocol and prove the user identity by owning a Subscriber Identity Module, this algorithm called EAP-SIM algorithm. The integrity and confidentiality is provided by Internet Protocol Security (IPSec) connection established using parameters derived from authentication triplets.

They tested secured and not secured SIP sessions. The latter ones were tested for non-IPSec enabled clients, and verified the proposed architecture with a mobile phone and have proven the correctness of their approach..

The main drawback that remains is the difficulty of IPSec implementation that can be by passed by a special application. The lack of IMS clients and special requirements of the mobile operators have forced researchers and industry to develop new service architectures.

M. Preetha and M. Nithya (Preetha & Nithya, 2013): This paper is discussing the important idea about the few end-users today who make use of real security applications. These applications tend to be too complicated, exposing too much detail of the cryptographic process. Users need simple inherent security that doesn't require more of them simply clicking the secure checkbox. Cryptography is a first abstraction to separate specific algorithms from generic cryptographic processes in order to eliminate compatibility and upgradeability problems.

Since the RSA provides highest security to the business application. Moreover, this scheme can be used for encryption of long messages without employing the hybrid and symmetric encryption.

The core idea in this paper is the public key algorithm RSA and enhanced RSA are compared analysis is made on time based on execution time. And use the technique of encoding a message with Optimal Asymmetric Encryption Padding (OAEP) and then encrypting it with RSA, this method is called (RSA-OAEP).

Ahmad Reza Montazerolghaem and Mohammad HosseinYaghmaee (Montazerolghaem & Yaghmaee, 2013): The main idea in this paper is create end-to-end connection, and being independence from the type of transmitted data, SIP protocol is a good choice for signaling protocol in order to set up a connection between two users of an IP network. Although utilization of SIP protocol in a wide range of applications has made various vulnerabilities in this protocol, amongst which overload could make serious problems in SIP servers. A SIP is overloaded when it does not have sufficient resources (majorly Central Processing Unit (CPU) processing power and memory) to process all messages. The studies accomplished in this paper show that SIP protocol is not efficient enough in facing with congestion, so that when call request rate increases, the delay of call establishment increases suddenly, proxy's throughput falls, and consequently resend rates and unsuccessful calls increase.

In this paper window-based control method is developed, implemented, and tested on a real platform and also the efficiency of SIP proxy in case of overload is studied by using window-based distributed overload control method, which is developed on Asterisk open source proxy. Studying the charts of throughput, delay, and resend rate of INVITE and BYE messages in Asterisk proxy shows that the algorithm is able to maintain the throughput at up to twice of the downstream proxy's capacity. This is clearly observable in average memory and CPU utilization charts.

Seungpyo Hong, et al (Hong & et al, 2013): This paper explains the Address Resolution Protocol (ARP) is used to resolve the Media Access Control (MAC) address of a host given its IP address. ARP is stateless, as there is no authentication when exchanging a MAC address between hosts. Hacking methods using ARP spoofing are being continuously abused in various ways, and there have been many prior studies of the prevention of such attacks.

Numerous methods have been developed to prevent ARP spoofing attacks. However, no single system is popular due to difficulties in their practical application to the current network or monetary issues. However, prevention requires the modification of the basic network protocol or expensive additional equipment, so it is hard to apply these methods to the current network. In this paper, they examine the protection of users from ARP spoofing attacks.

In addition, they suggest a defense mechanism that does not require changes to the network protocol or expensive equipment. The proposed system automatically renews the reliable MAC address information to the ARP table as a static type to protect users from ARP spoofing. This suggested method is based on the host environment and does not require protocol modification or any additional equipment. It requires a physically separated PC with a MAC-Agent, but it is a light application, and thus the suggested system can be widely used under the current network environment.

Yun-Sheng Yen, et al (Yen & et al, 2011): This paper discusses the use of communication technology to commit crimes, including crime facts and crime techniques. The development of the internet is fuelled by numerous commercial intentions; it is no longer simple information delivery. Many criminals try to earn profits through the internet. Thus, the use of the internet should be under the protection of information security to ensure honest users. The main problems include internet phone fraud and internet phone attacks. In addition to the analysis and management of internet security vulnerabilities, penetration testing should be added to test security in a practical internet environment.

This paper focuses on the security analysis VoIP, a prevention method against VoIP call attack and the attention points for setting up an internet phone. The importance of digital evidence and digital forensics are emphasized. This paper consults related works on the VoIP Digital Evidence Forensics Standard Operating Procedures (DEFSOP) and correlative digital evidence from different scholars and develops a higher quality and more suitable DEFSOP. This paper discusses the security problems faced by the VoIP, lists prevention policies and designs a VoIP DEFSOP to help forensics operators. This paper shows how VoIP DEFSOP works in the operation stage through experiments and provides investigators with suggestions for the future.

Byounghee Son et al (Son & et al, 2013): The authors present the VoIP encryption module was designed to prevent eavesdropping on internet telephones communications and involved encoding/decoding the output data at the transmitter and receiver of the internet telephone.

The VoIP encryption proposed module for securing privacy. In encoding communication using the proposed module, the AES advised that should be used which resulted in the overall verification of the system performance and delay times through experiments. In the experiments, a high speed symmetric 128 bit AES method was used to reduce the voice delay of the VoIP telephone. In the beginning, the call process using a mutual key exchange in the encryption system, an asymmetric encoding method RSA algorithm was used to improve security. The speech quality demonstrated good performance with a Mean Opinion Score (MOS) of 4.18~4.20 (Good) and an R-factor of 91.25~93.00 (Good).

Yacine Rebahi et al (Rebahi & et al, 2008):The authors presented a SIP standard for managing IP multimedia sessions in the internet. Identity management in SIP is a crucial security field that deals with identifying users in SIP networks and controlling their access to the corresponding resources. RFC 4474 describes a mechanism, based on certificates, for dealing with the SIP users identities. This RFC recommends the use of the RSA algorithm as it is currently the most popular public key cryptography system. The proliferation of small and simple devices as well as the need to increase the capacity of the SIP servers to handle the increasing VoIP traffic will make continued reliance on RSA more challenging over time. The implementation is described of the current RFC 4474.

This paper discusses the integration of Elliptic Curve Cryptography (ECC) into SIP identity management schemes. In fact, RFC 4474 that describes a certificate-based mechanism for dealing with SIP users identities is implemented using RSA as well as Elliptic Curve Digital Signature Algorithm (ECDSA). The experiment is shown the superiority of ECDSA over RSA in terms of performance. Due to its computational efficiency, ECDSA can be used in constrained environments where traditional public key mechanisms are impractical. Further, the paper also analyzed the security issues related to the identity management mechanism. Although this mechanism is helpful to authenticate the SIP identities, the performance of it poses security threats to SIP services. Thus, it is necessary to optimize the performance of this mechanism from different aspects, which can be considered as a first step in standardizing the use of elliptic curves in the identity management for SIP.

Jaspreet kaur and Er.Kanwalpreet Singh (Kaur & Singh, 2013): Now-a-days, communication is most popular now days. Everyone wants secure communication that's way use encrypts and decrypt data scheme. It is basically used for military and business purpose. People want high security level during their communication. The numbers of algorithms are used for speech encryption and decryption. However in this paper In this paper discussed about cryptography, speech cryptography, encryption or decryption of data by working done on three different kinds of algorithms i.e. NTRU, RSA and RINJDAEL these three popular algorithms are used for speech encryption and decryption approach. Basically NTRU and RSA algorithms are asymmetric in nature and RINJDAEL algorithm is symmetric in nature..

In speech encryption, first the speech is converted into text then further the text is converted into cipher text. The cipher text is sent to be particular receiver in which transmitter want to communicate. At the receiver end, receiver receives the original data through decryption process.

At the end the performance is analyzed of these three approaches respectively. The parameters calculated are encryption, decryption and delay time are varying according to the number of bits per seconds, complexity, and packet lost are approximately same, security level is important in wireless environment. There is no packet lost during transmitting and receiving the data. After the analysis of these three algorithms, NTRU is provided better result so it will improve the current security level, fastest speed and provide reliable message at receiver end with respect to key generation, encryption and decryption with small key size. The android platform are used for these three algorithm to find the results in which algorithm took less time for encrypt or decrypt the data and help to evaluate the performance in speech encryption algorithms.

H.Hakan Kilinc and Tugrul Yanik (Kilinc & Yanik, 2014): The authors presented a survey of authentication and key agreement protocols are critical security services to implement a secure SIP protocol which is a common part of the VoIP architecture. Performance and security of the authentication and key agreement schemes are two critical factors that affect the VoIP applications with large number of users. Therefore, the performance of the authentication and key agreement protocols is of great importance.

In this survey, they are identified, categorized and evaluated various SIP authentication and key agreement protocols according to their performance and security evaluation. They are examined schemes according to four different categories which can be denoted as Password Authenticated Key Exchange (PAKE) based, Hash based, Public Key Cryptography (PKC) based and ID based.

On the other hand, most SIP implementations today still employ the Hypertext Transfer Protocol (HTTP) Digest Authentication. The simplicity of implementation and the lower performance overhead seem to be the major reasons. But with the increasing number of security breaches in VoIP systems this choice might change in the near future. Although the performance is inversely proportional to the security features provided in general, they observed that there are successful schemes from both the performance and security viewpoint.

The discussed schemes are mostly designed for client/server architectures. Most of the proposed schemes do not consider delays introduced by network and database access. When designing authentication and key agreement protocols it would be appropriate to consider the delays in a distributed environment. For Peer-to-Peer (P2P) and Next Generation Networks (NGN) architectures, new authentication and key agreement protocols that consider the various overheads introduced by the distributed network structure are necessary.

Tahina Ezéchiél Rakotondraina and et al. (Rakotondraina & et al, 2013): In this study, the authors are contributed of the security voice in IP network, which will become in the near future, a universal standard of voice and video networks telecommunications. As with any phone call, it is need to encrypt communication to respect the rights and privacy of each person. The security of voice implemented in IP packets and study material resource consumption on the establishment of this system. This is the major problem with this kind of technology that is currently experiencing various attacks threatening all communication systems.

It is clear that the module data encryption in VoIP is not yet fully implemented in the server, since the use of a real-time requires a minimum treatment period of service. The results showed that they can properly secure the data to the risk of a maximum use of resources such as CPU and memory, the server and increased the latency of the system.

Based on analysis, they are found a slight difference between normal communication and encrypted communication. These differences lie in the fact that encrypted communication consumes a lot more resources that the implementation of the encryption module, both the secure transport of cryptographic keys on the packets in the Asterisk server requires adding a process where the need for additional resource.

Amor Lazzez (Lazzez, 2013): The author presented the technology of Voice over IP (VoIP) is allowing voice and multimedia transmissions as data packets over a private or a public IP network. Thanks to the benefits that it may provide, the VoIP technology is increasingly attracting attention and interest in the industry. Actually, VoIP allowed significant benefits for customers and communication services providers such as cost savings, rich media service, phone and service portability, mobility, and the integration with other applications.

The deployment of the VoIP technology encounters many challenges such as architecture complexity, interoperability issues, QoS issues, and security concerns. Among these disadvantages, VoIP security issues are becoming more serious because traditional security devices, protocols, and architectures cannot adequately protect VoIP systems from recent intelligent attacks. After that talked about the security profiles of the VoIP protocols, and the countermeasures are presented that should be considered to help the deployment of a reliable and secured VoIP systems.

A deep analysis is presented of the security concerns of the VoIP technology. Firstly, a brief overview is presented about the basics of the VoIP technology. Then, they discussed the security vulnerabilities and attacks related to VoIP protocols and devices. A future work will address another important issue in the deployment of VoIP technology; the ability to support the QoS constraints of the voice and video applications.

HarjitPal Singh et al., (Singh & et al, 2014): In this paper, the authors presented and discussed many issues that the Internet has revolutionized the telecommunication systems by supporting new applications and services. Voice over Internet Protocol (VoIP) is one of the most prominent telecommunication services based on the Internet Protocol (IP). The signal quality of the VoIP system depends on several factors such as networking conditions, coding processes, speech content and error correction schemes. From the very beginning of transferring the voice data over packet switched networks, the journey of the packet based communications to modern VoIP and advancements to improve the service of the VoIP system. The VoIP system has been established as the best alternative to the traditional Public Switched Telephone Network (PSTN) telecommunication system for providing the voice services to the users.

The author summarized the merits/demerits, compression schemes and measurement schemes for the VoIP system. Further, the progress in improving the signal quality of the VoIP system in the last four decades had been reviewed. The possibility of the VoIP communication over satellite link, security issues and the role of digital filters to improve signal quality had been highlighted.

Alessandro Barengi et al. (Barengi & et al, 2013): The authors presented a full characterization of an effective low-cost, non-invasive and effective technique to inject transient faults into a general purpose processor through lowering its feeding voltage, and to characterize the effects on the computing system..

The technique chosen to induce the faults consists of constantly underfeeding the general purpose RISC CPU that carries out the computations. They validated the effectiveness of the fault model through attacking Open SSL implementations of the RSA and AES cryptosystems. A new attack against AES, able to retrieve the full 256-bit key, is described, and the number of faults to be collected is delineated. In addition to, they designed two new attack techniques, one for each cryptosystem, and have been able to validate their practical effectiveness with a thorough experimental campaign. They were able to successfully break the AES cipher employing less than 30 KiB of faulty cipher texts, to retrieve an RSA encrypted plaintext using at most 5 faulty cipher texts and to factor the RSA modulus employing at most two faulty signatures.

The experimental results showed no signs of tampering were left on the attacked device, thus proving that the employed technique is not invasive and does not alter the further functioning of the device.

Mr. S.Thiruppathi (Thiruppathi, 2012): The main idea in this paper that discussed, today the customer care in telecommunication using the Voice over Internet Protocol (VOIP) is a way to carry out telephone conversation over a data network for free. VoIP products promise converged telecommunications data services that are cheaper, more versatile and provide good voice quality as compared to traditional offerings. Although VoIP is widely used, VoIP on mobile devices is still in infancy. Currently there are a number of VoIP solutions for mobile phones. However, VoIP solutions developed using Java 2 platform Micro Edition (J2ME) are not available .Java based solutions are widely compatible with many devices.

The author focused and granted to devices compatibility through the use of the widely supported J2ME framework for the people using environment. The implementation details of VoIP client using J2ME and deploy on a mobile phone with the necessary features. The features of the implemented client are suitable for mobile devices. Although the implemented client is compatible with the VOIP standard, the client is not implemented completely.

2-3Summary

Recently, there have been many researches who presented suitable transfer method in the VoIP field, which is representing the protocol for transmitting voice data using the internet.

Several techniques and algorithms have been presented to improve the quality of VoIP transmission, but these techniques have been focused on one side of the transmission aspects, such as security, quality or speed.

In this thesis, attempted to handle all the important aspects of the VoIP field and this has been achieved through focusing on two important points:-

- **The first point:** - the transmission VoIP process occurred through SIP server, who works as a monitoring on the communication session between two parties (sender and receiver).

- **The second point:** - providing transmission security by depending on the characteristics of two algorithms (RSA and AES), as declared in next chapter.

Chapter Three: Theoretical Design

3-1 Introduction

The intruder problems lately became serious result enormous of technology development in general and specifically on the field of voice transfer. The process of voice transfer may contain important and personal information, or data that related to both sender and receiver. So the information or data must be secured and known only by authorized parties.

Various models have been proposed to solve the problem of VoIP security. Many of these models were very weak in secured operation in order not to effect on the voice's speed. On others hand some models were very secured operation, but fetch the attention to the intruders.

This thesis is focused on two main points:

- The model proposes and generates method to reduce the threats during transfer operation. This model should be secured and without drawing any attention to the intruders.
- The proposed security algorithm will depend on two characteristics AES algorithm (high speed and reasonable security) and RSA algorithm (Strong Security and reasonable speed). This proposal is using the advantages of AES speed with RSA security to produce an algorithm that called AR2SS (AES & RSA Speed and Security).

The proposed model includes three procedures:-

1. SIP Server procedure: this procedure's function is to make a connection between two parties, it is elaborate when receiving extension request and check it if available or not, then open session will depend on available or not (sender and receiver).
2. Sender procedure: this procedure's function is to encrypt the audio in the sender side, and then sends it to the receiver. Which is working after the extension is available.
3. Receiver procedure: this procedure's function is to receive the encryption audio from sender, and then decrypts it in the receiver side. Which elaborating after the SIP server is opening session.

Note: (all steps above work together and the chart illustrate working of every step).

Figure (3-1) explains the three procedures and the main steps in each procedure

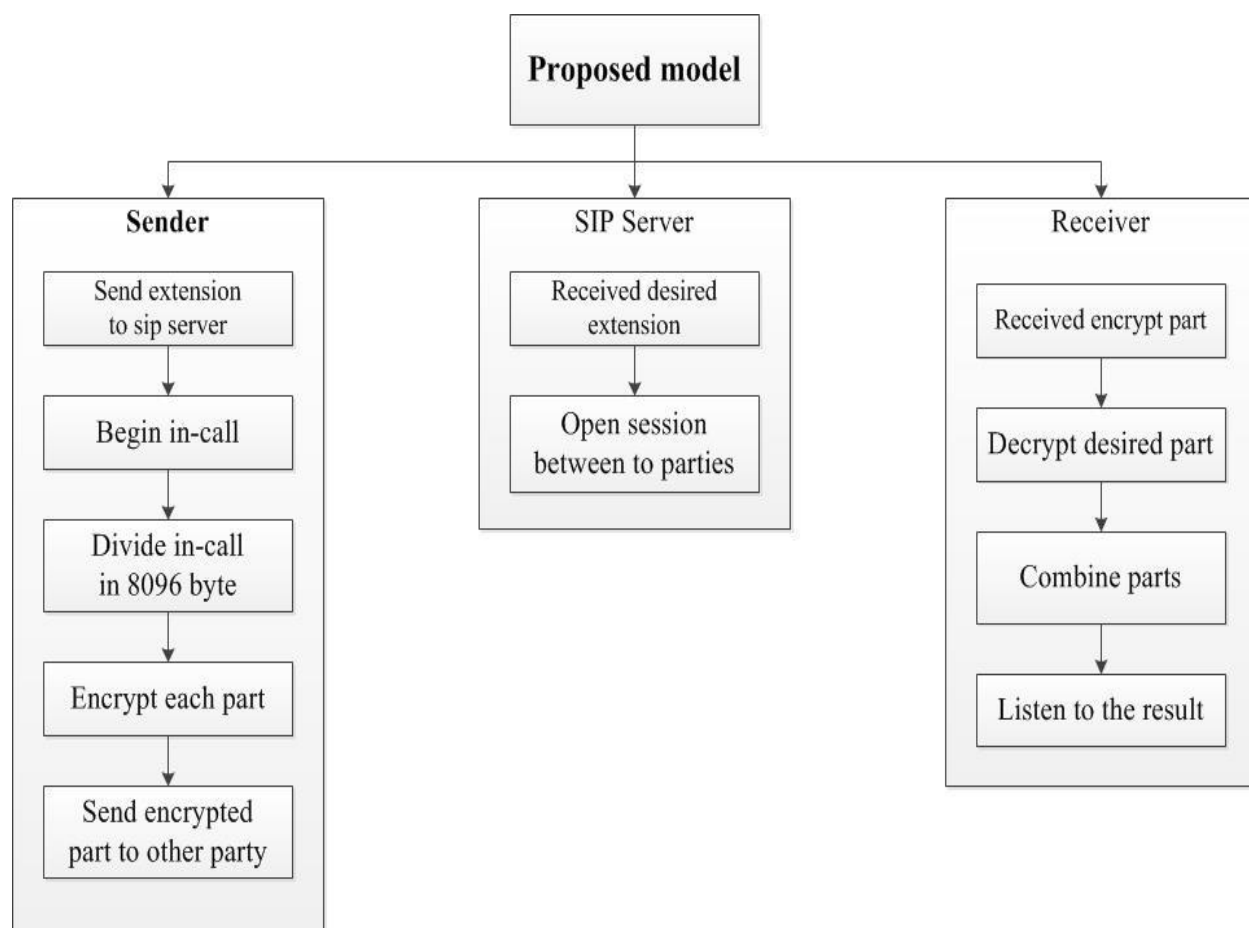


Figure (3-1) The Proposed Model

3-2Tools

3.2.1 SIP Server (3CX)

3CX Phone System is a SIP server used for Windows that works with popular VoIP Gateways and SIP phones allow you to setup a complete IP. SIP servers are responsible for setting up the calls between SIP devices and usually combine several of the SIP server functions such as SIP proxy and SIP register into one piece of software.

3.2.2 Two mobile devices by using Android operating system version (4.1.2)

Android is an operating system based on the Linux kernel with user interface. Android's source code is released by Google under open source licenses.

Android 4.1 (Jelly Bean) is announced by Google at the conference on 27 June 2012. Jelly Bean was an incremental update with the primary aim of improving the functionality and performance of the user interface. There are many features as listed in the following that updating the features from the previous versions:

1. Lock/home screen rotation support for the Nexus 7.
2. One-finger gestures to expand/collapse notifications.
3. Bug fixes and performance enhancements

3.2.3 Type of device using

- 1- HTC Desire 600 (Operating system: Android, CPU: 1.2GHz and RAM: 8GB).
- 2- HTC Desire 500 (operating system: Android, CPU: 1GHz and RAM: 4 GB).

3- Samsung i9300 (operating system: Android, CPU: 1GHz and RAM: 8 GB).

3-3 Used Algorithms

There are many algorithms used in this thesis for providing suitable security in transmission voice, these algorithms are divided into three procedures and each procedure includes many steps to execute a specific function.

3.3.1 Major Flowchart

This part is used to transmit audio between the sender and the receiver, in addition to third-party in safely form, as shown in the Figure (3-2).

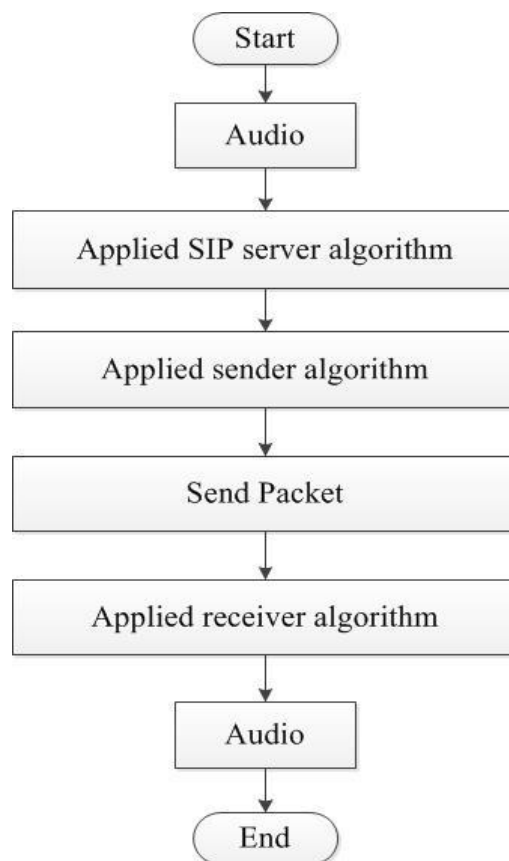


Figure (3-2) Major Flowchart

Algorithm: Major algorithm

// Input: audio.

Output: audio. //

- Step1: Call (SIP-Server algorithm).
- Step2: Call (AR2SS-Encrypt Algorithm).
- Step3: Send encrypt packet
- Step4: Call (AR2SS-Decrypt Algorithm).
- Step5: Return (audio).

3.3.2 SIP-Server Flowchart

This part is used to receive the required extension from the sender, then make sure this extension is available case or not. Based on the case, the server decides to open the session or not. As shown in the Figure (3-3).

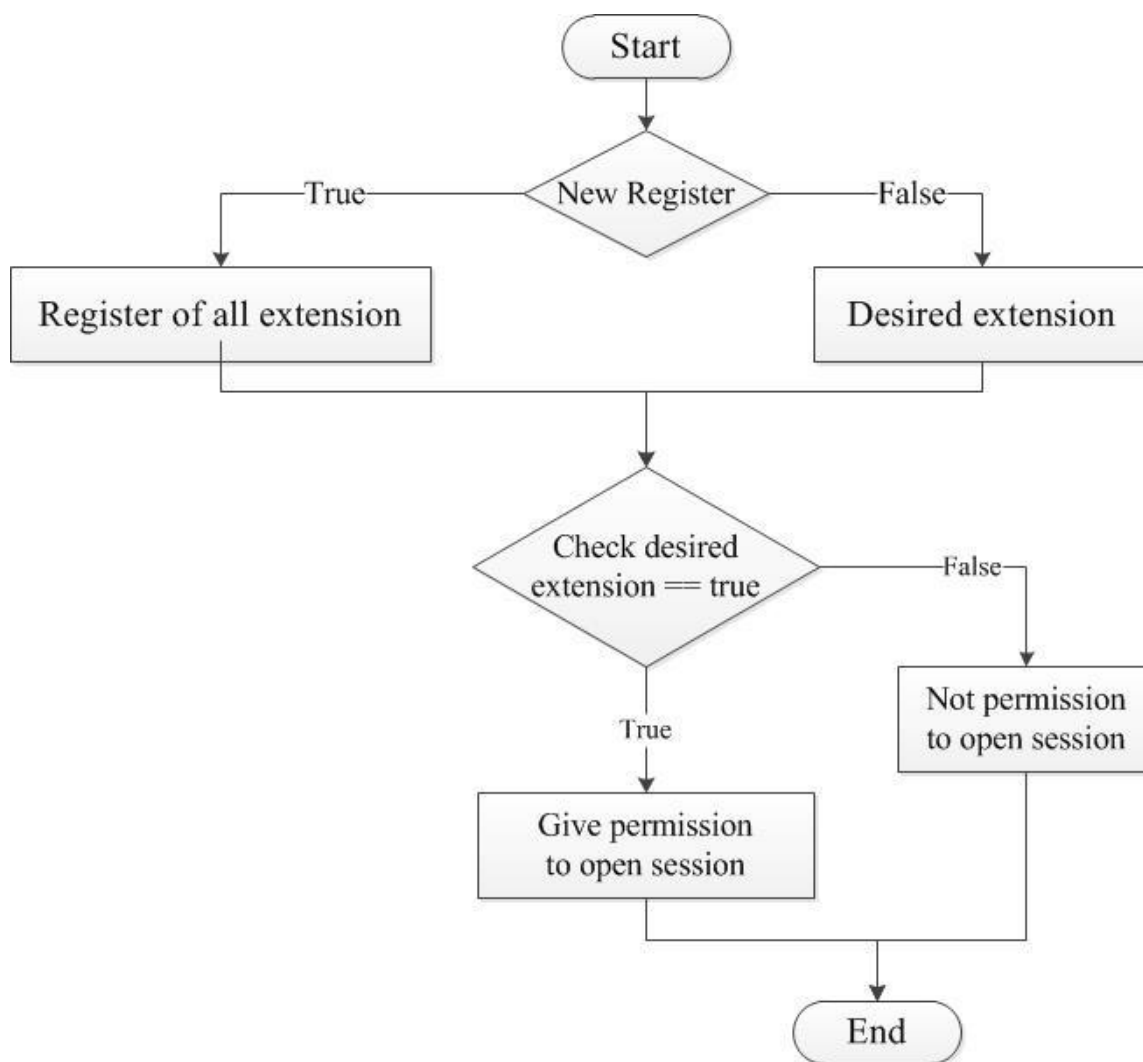


Figure (3-3) SIP-Server Flowchart

Algorithm: SIP-Server algorithm

// Input: desired extension.

Output: give permission or not. //

- Step1: Step1: IF (New Register ==True) Then
- Step2: X ← register include all extension
- Step3: Else
- Step4: Y ← desired extension from sender
- Step5: If (Y == True in X) Then
- Step6: Z ← give permission and open session between parties
- Step7: ELSE
- Step8: Z ← not permission to open session
- Step9: End If
- Step10: Return (Z)

3.3.3 AR2SS-Encrypt Flowchart

The AES & RSA Speed and Security (AR2SS) algorithm will depend on two characteristics of AES algorithm (high speed and reasonable security) and the RSA algorithm (Strong Security and reasonable speed). AR2SS is using the advantages of AES speed with RSA security.

This part is used to open the session with the SIP server, also make sure the second party is existing or not. After that, the sender is encrypting the audio then sent it to the recipient side. As shown in Figure (3-4).

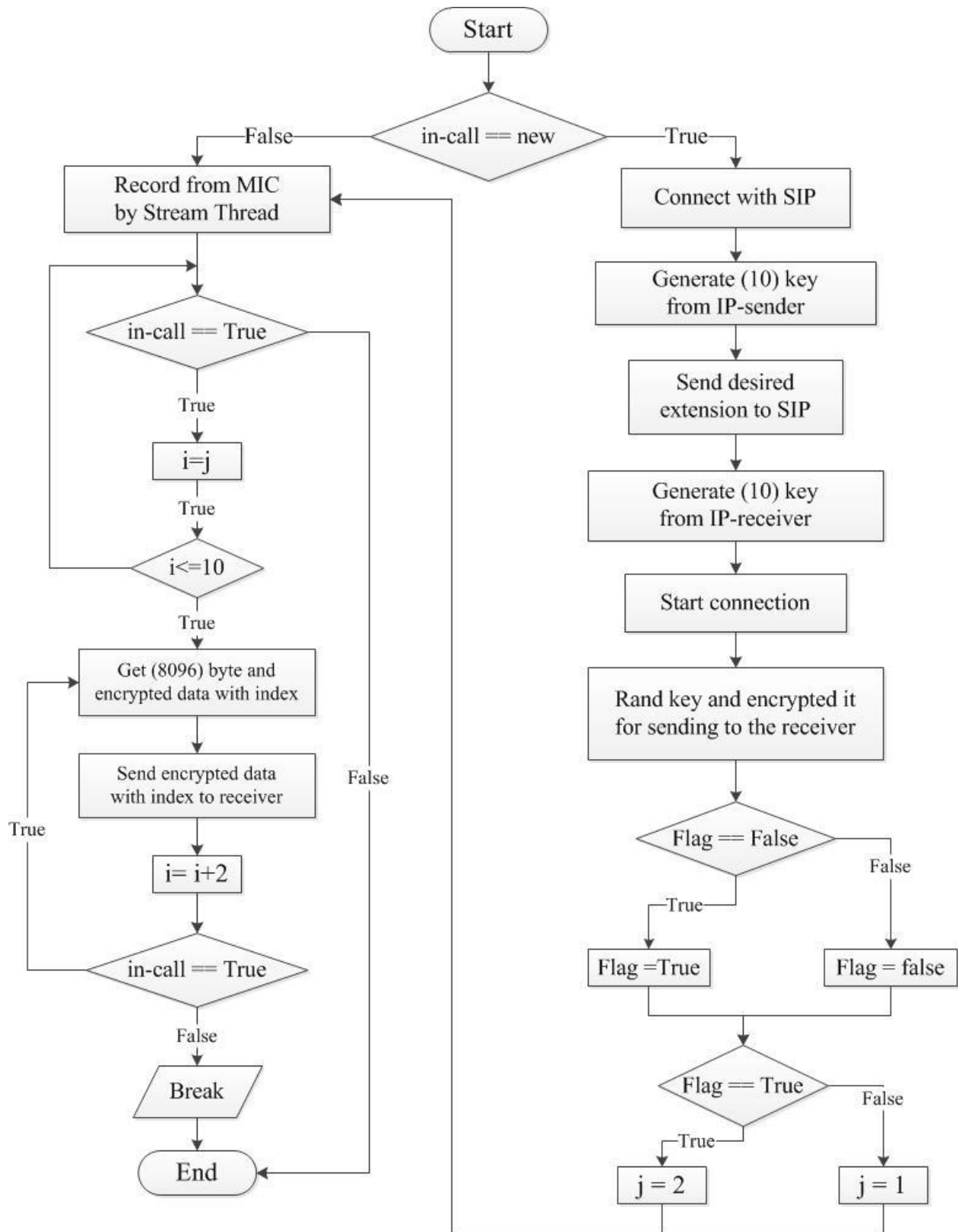


Figure (3-4) Encryption Flowchart

AR2SS-Encrypt Algorithm

// Input: original audio.

Output: encrypted audio with index of encrypted key //

- Step1: IF (in-call == New Call)
- Step2 : Connect with SIP server
- Step3: Generate (10 Keys) from IP-Sender
- Step4 : Send desired extension to the SIP as (Ext# receiver @ IP address sip server)
- Step5 : Receive IP-Receiver from SIP server
- Step6 : Generate (10 Keys) from IP- Receiver
- Step7 : Start connection between parties
- Step8 : $X \leftarrow \text{Rand (Key)}$
- Step9 : $X1 \leftarrow \text{encrypt by RSA}(X)$
- Step10 : Send (X1) to the receiver
- Step11 : IF (Flag == False) Then
- Step12 : Flag \leftarrow True

- Step13 : ELSE
- Step14 : Flag \leftarrow False
- Step15 : END IF
- Step16 : IF (Flag ==True)
- Step17 : J \leftarrow 2
- Step18 : ELSE
- Step19 : J \leftarrow 1
- Step20 : END IF
- Step21 : END IF
- Step22 : Record from MIC by Stream Thread
- Step23 : While (in-call == True)
- Step24 : For I=J:2:10 // by using key receiver
- Step25 : X2 \leftarrow 8096 byte (data)
- Step26 : X3 \leftarrow Encrypt by AES_{Key_i} [X2] //X3: data encrypted
- Step27 : X4 \leftarrow Encrypt by $AES_{Key_{X_1}}$ [index Key_i] //X4: index key encrypted
- Step28: Send (X4,X3) to the second party by Audio Streamer Send Sound to port (50505).

- Step29 : IF(in-call== True) Then
- Step30 : Continue
- Step31 : ELSE
- Step32 : Break
- Step33 : END IF
- Step34 : END FOR
- Step35 : END While
- Return (X3,X4)

3.3.4 AR2SS-Decrypt Flowchart

This part is used to receive encrypted data from the sender, then decrypt this data and combine it, as shown in the Figure (3-5).

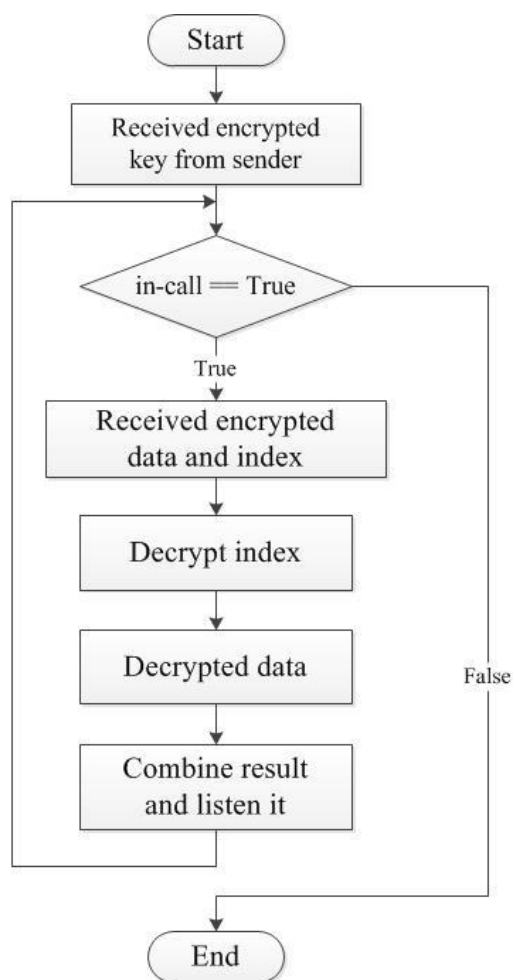


Figure (3-5) Decryption Flowchart

AR2SS-Decrypt Algorithm

// Input: encrypted audio with index of encrypted key.

Output: original audio //

- Step1: $R \leftarrow$ Received (X1) from sender
- Step2 : $R1 \leftarrow$ RSA (R)
- Step3 : While (in-call == True)
- Step4 : Received (X3) and (X4) from sender by Audio Receiver from port (50505).
- Step5 : $R2 \leftarrow X3$ //R2: encrypted data
- Step6: $R3 \leftarrow$ decrypt by $AES_{Key R1}$ [index Key_{X4}] //R3: index key
- Step7 : $R4 \leftarrow$ decrypt by $AES_{Key R3}$ [R2] //R4: data decrypted
- Step8: $R5 \leftarrow$ combine (R5,R4) //R5:result data
- Step9: Listen (R5)
- Step10 : END While
- Return (X5)

3-4Summary

Chapter three discussed the suitable method for suggested problem, and declared the proposed model through algorithms and flowcharts. Each of them explains one of the parts in the model. Also this chapter focused on the model aims for accepting achieved results, as below:

- 1- The fast encryption process by AES algorithm, which it is handling delay in transfer voice with quickly sent to receiver.
- 2- The strong encryption packet by RSA algorithm, where was encrypted packet for anti-eavesdropping on clients.

Chapter Four: Experimental Works

4-1 Introduction

Data communication is important issue in the recently days. Therefore data's protection from misusing is essential. So, the voice is the most important types of data transmitted that needs to be protected.

VoIP is the protocol for transmitting voice data using the internet. It has already achieved wide acceptance in the world. At the same time, the VoIP targeted by various types of attacks, namely capturing packets, eavesdropping communications, and many others.

The weakness in management is one of the threats in the VoIP technologies which deal with two parties (sender and receiver) for controlling their access to sensitive data. For that purpose the sender and receiver share a session key with the server before any communication. Therefore, this key is exchanged over the network for using it to be based in the providing secure channel.

IP telephony is an emerging technology, enabling a range of new service possibilities. Although, if is used various protocols such as (UDP and TCP) underlying this technology is adding to the SIP server, which seems to be the standard that is being widely adopted by the different VoIP communities. The services that the VoIP providers offer to their customers need to reach a certain security maturity level.

There are different algorithms dealing with SIP server, this thesis choosing RSA and AES algorithms to provide suitable method for protecting the audio transmission.

The RSA algorithm is the most widely used public key technology today; AES is based on design principle known as substitution-permutation network, and it is fast in both software and hardware. This method is depending on high speed, reasonable security in AES algorithm and strong security, reasonable speed in RSA algorithm.

The model is implemented by additional new interface between two parties. It will build outside the SIP server. The sender part is used the AR2SS algorithm for encrypt voice before transmission to other party by SIP server, and receiver will use the same algorithm in reverse to decrypt the voice, as shown in Figure (4-1):

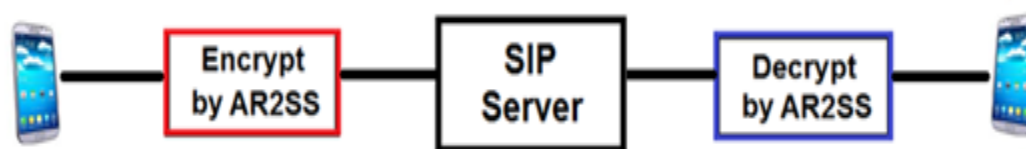


Figure (4-1) Framework

4-2 Interfaces Execution

The execution of application is divided into four procedures:

1. Admin Procedure.
2. Register Procedure.
3. Call Procedure.
4. Fail Procedure.

4.2.1 Admin Procedure

The main interface showed in SIP server is the admin interface. It includes (Language, User name and Password), as shown in Figure (4-2).

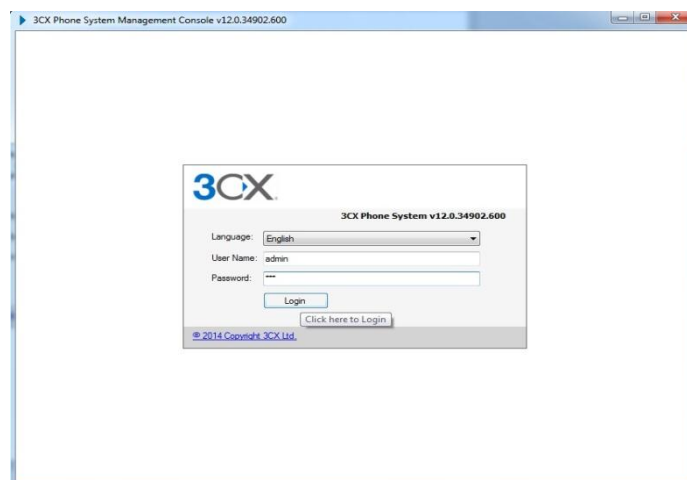


Figure (4-2) The Main Interface of Admin

After pressing the log-in button, the next interface will include all the register users in SIP server. The green point is for online or active user, the red is point for offline user, as shown in Figure (4-3).

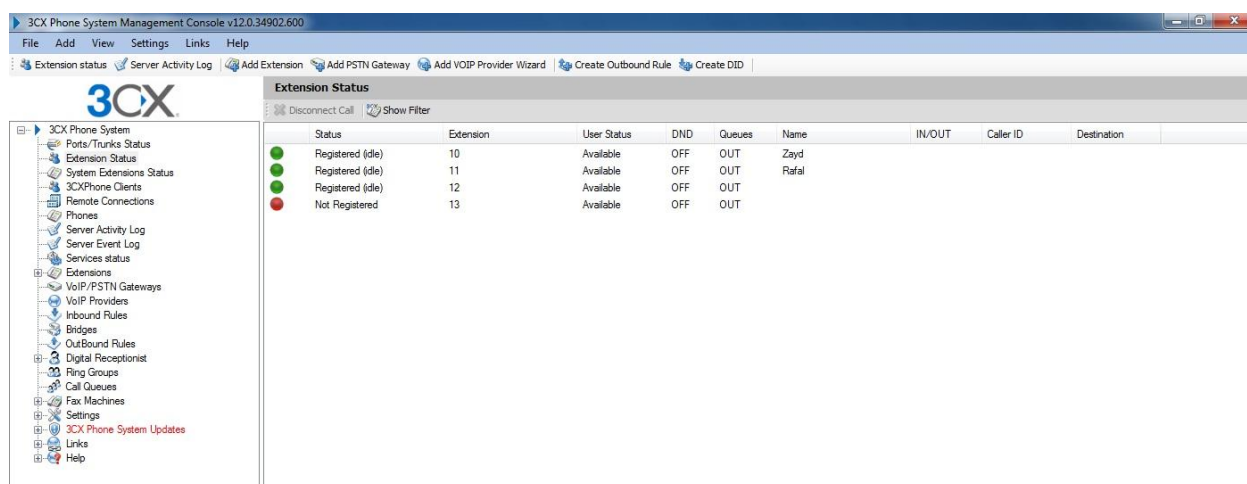


Figure (4-3) Status of Users

When the user choose the extensions option, then the next interface will appear for adding new extension to the SIP server by filling the required information in this interface, as shown in Figure (4-4).

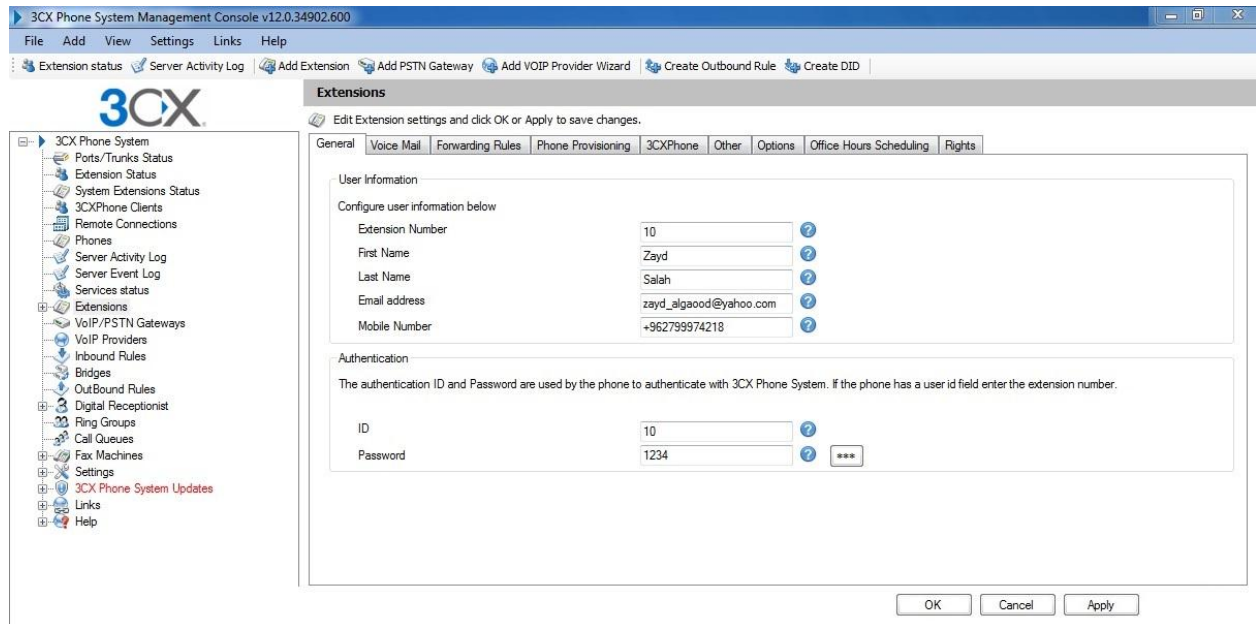


Figure (4-4) Extensions Interface

After the admin click the apply button, the below inter face will appear, as shown in Figure (4-5).

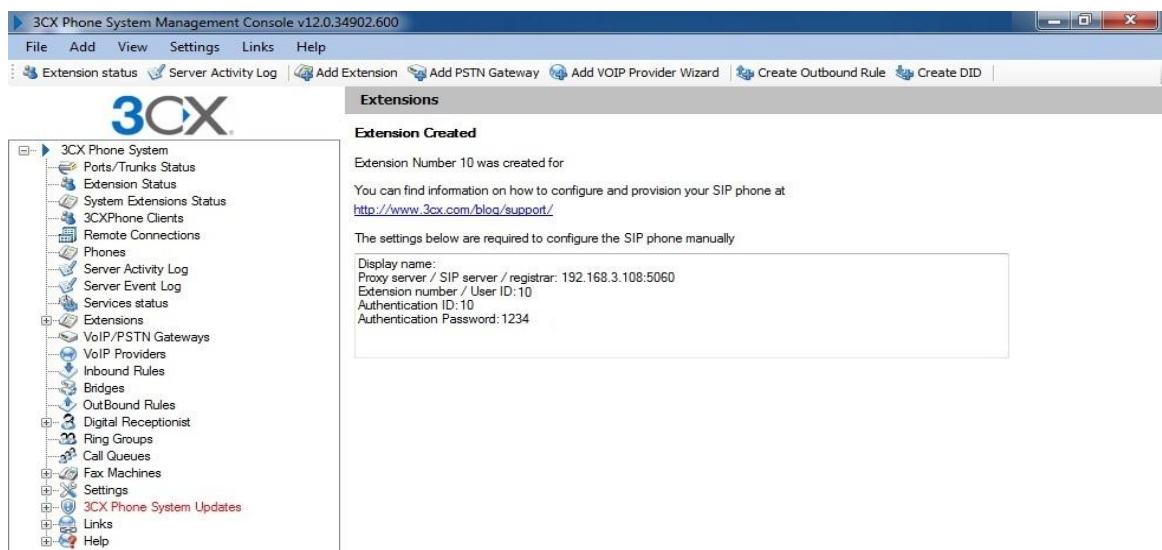


Figure (4-5) Created New User

The admin can edit any extension in SIP server by choosing the user who wants to edit the information, as shown in Figure (4-6) after that the Figure (4-4) interface will appear and the admin can edit any information.

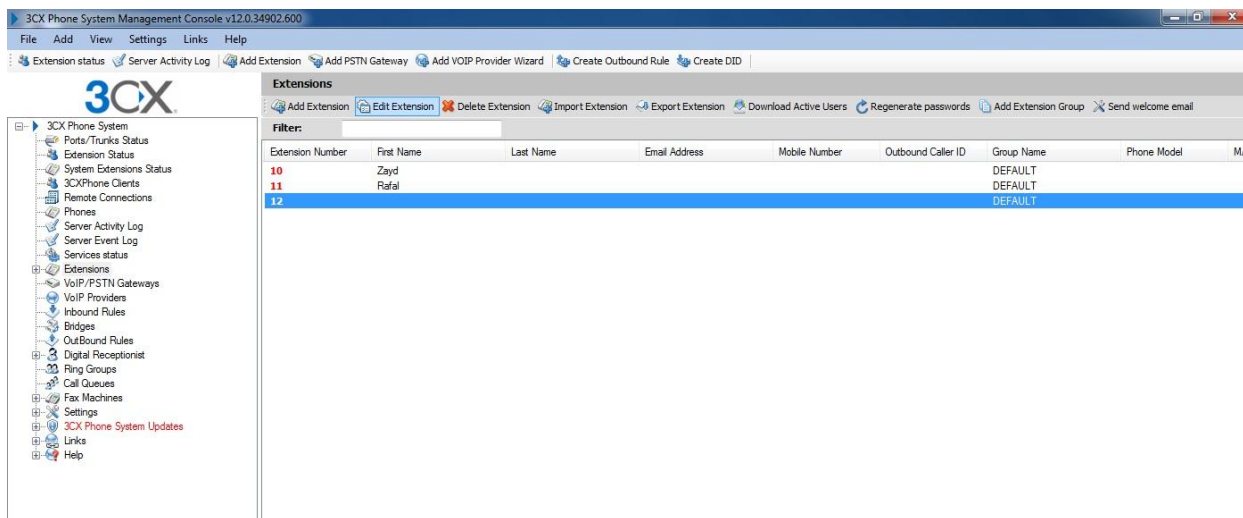


Figure (4-6) Editing Extension Interface

When the one of parties decided to call another party, the following interface will appear, as shown in Figure (4-7).

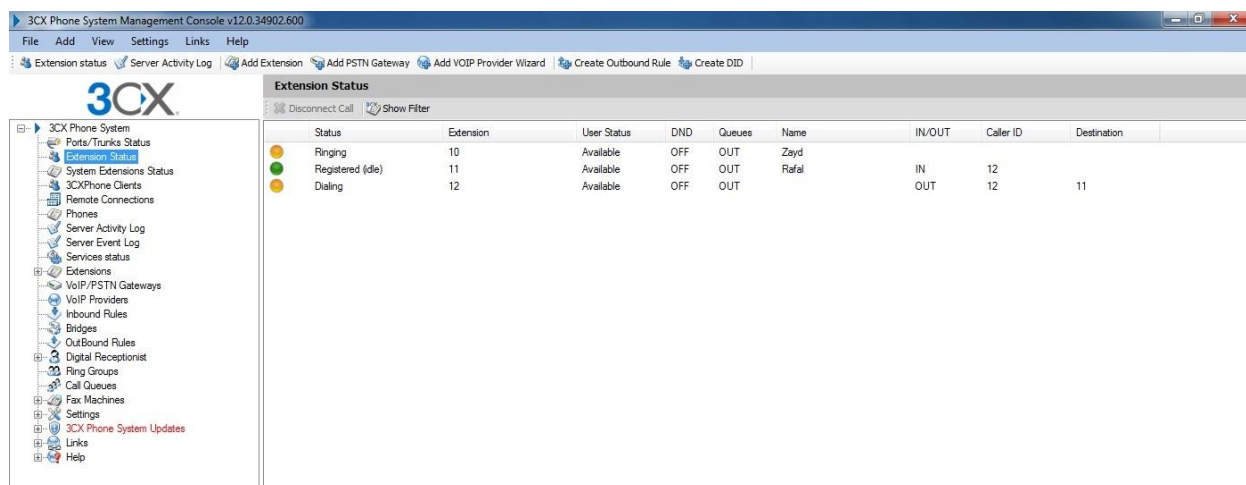


Figure (4-7) Before Calling Process

Through the calling process between two parties such that from 12 extensions to 10 extensions, the following interface will appear, as shown in Figure (4-8).

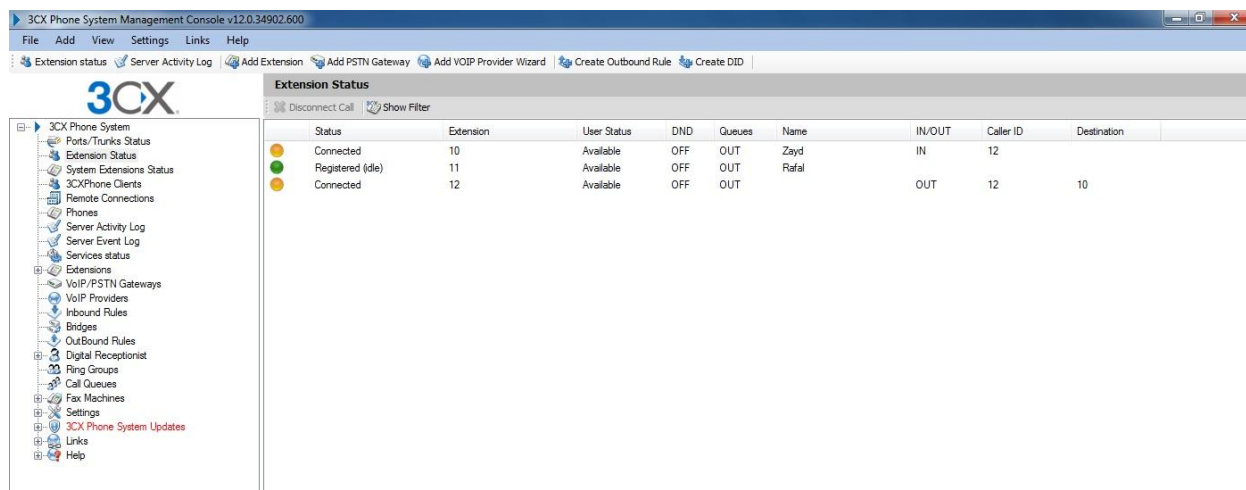


Figure (4-8) After Calling Process

4.2.2 Register Procedure:

The main interface during installation the application in the mobile, the following interface will appear message that declared the user is not registered as shown in Figure (4-9).

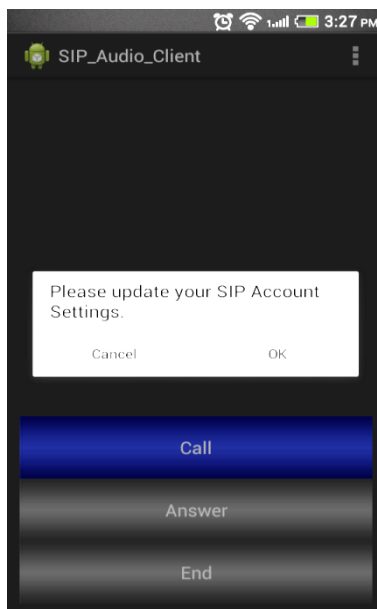


Figure (4-9) Main Interface of Installation Application Process

When the user click on ok button, the following interface will appear and includes (Enter Username, Enter Domain and Enter Password), as shown in Figure (4-10).

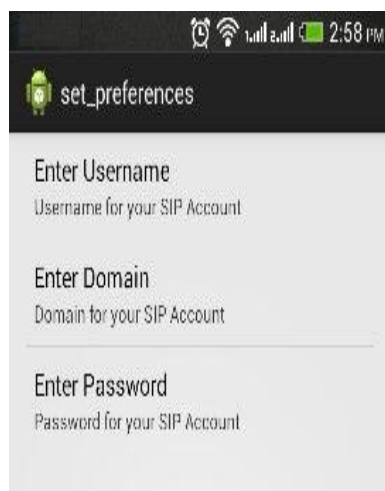


Figure (4-10) Set-Preferences Interface

When the user enters the username, the following interface will appear and it can enter the username as number or characters, as shown in Figure (4-11).



Figure (4-11) Enter Username Interface

The user enters the SIP name through the IP of the SIP server, as shown in Figure (4-12).



Figure (4-12) Enter Domain Interface

The user enters the password, as shown in Figure (4-13).



Figure (4-13) Enter Password Interface

4.2.3 Call Procedure

At the end of registration process, the work of call procedure will begin, the following interface shows ready notification to the user and ready to make call between the parties, as shown in Figure (4-14).

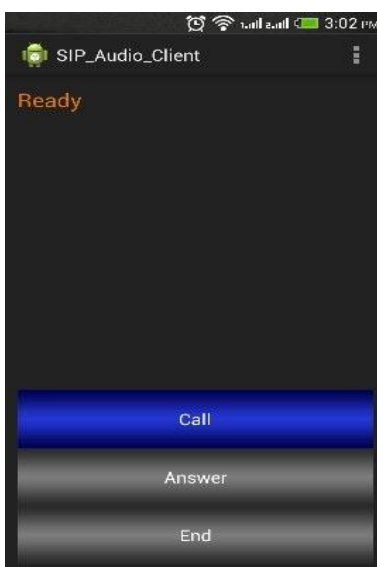


Figure (4-14) Ready Interface

The application can make calling process, either by IP domain of the receiver as shown in Figure (4-15)

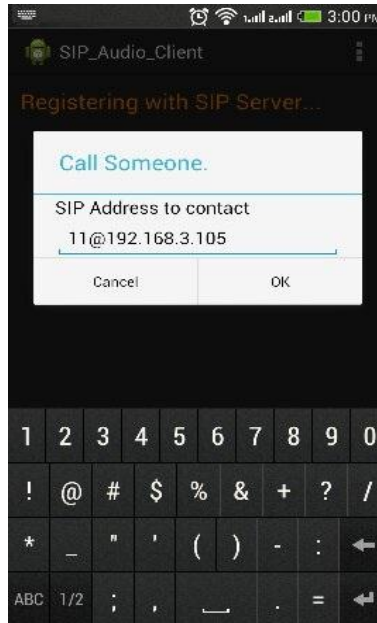


Figure (4-15) IP Domain of the Receiver Interface

Or add by name receiver as shown in Figure (4-16).

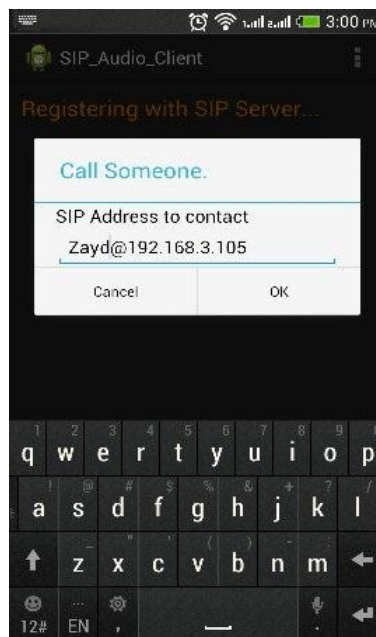


Figure (4-16) Name Receiver Interface

When the calling process is begging between the sender and receiver, the following interface will appear as shown in Figure (4-17).

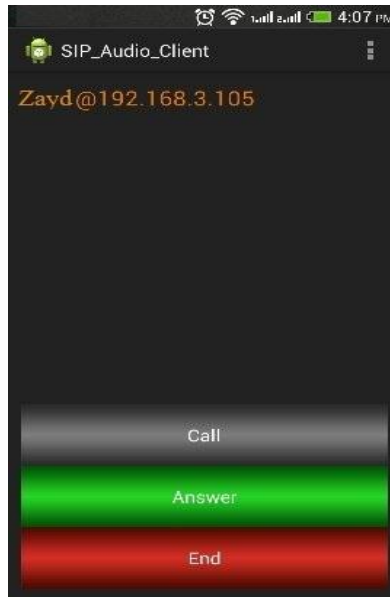


Figure (4-17) Calling Process Interface

4.2.4 Fail Procedure

If the SIP server is turned off or the registration process is failed, the application will appear message to the user for editing information in settings, as shown in Figure (4-18).

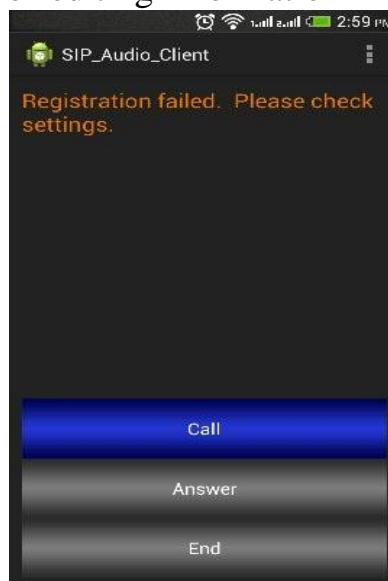


Figure (4-18) Failed Registration

The edit interface will appear as shown in Figure (4-19).

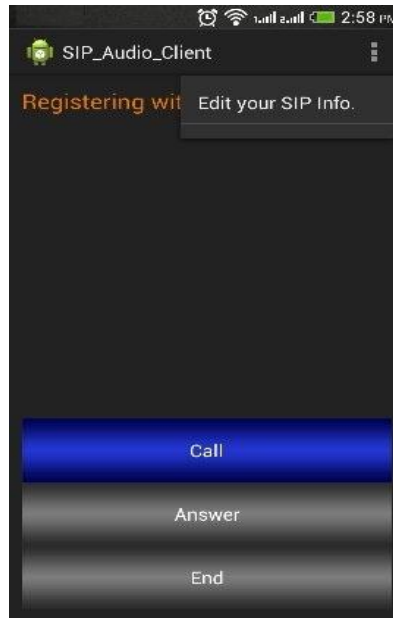


Figure (4-19) Editing SIP Info

4-3Experiment

This part will explain the results which were obtained through the implementation of the program on PC (CPU 3120 GHz, RAM 8 GB) with Samsung mobile device. This type is (i9300), which CPU 1GHz and RAM 8 GB with also a router of 108 megabyte per second the speed of transmitting data. The experiments are clarified as follows:

The first experiment: A key size of 128 bit was used with a packet size of the sender was 20016 byte, including 16 byte for key. It will be receiving 20000 byte. The following Table (4-1) shows estimated time to make the encryption and decryption.

Table (4-1) ... The first experiment

Process No.	Encryption Time (ms)	Decryption Time (ms)
1	4	6
2	4	6
3	4	7
4	3	5
5	4	7
6	3	6
7	3	5
8	3	4
9	4	8
10	4	7
11	4	5
12	4	7
13	3	4
14	3	8
15	3	6
16	4	7
17	4	11
18	4	10
19	3	6
20	3	6
Total range time	71	131
Average Time	3.55	6.55

The second experiment: A key size of 192 bit was used with a packet size of the sender was 20016 byte, including 16 byte for key. It will be receiving 20000 byte. The following Table (4-2) shows estimated time to make the encryption and decryption.

Table (4-2) ... The second experiment

Process No.	Encryption Time (ms)	Decryption Time (ms)
1	8	10
2	4	8
3	5	9
4	3	7
5	4	8
6	4	8
7	4	8
8	4	6
9	4	8
10	4	6
11	4	8
12	3	5
13	4	8
14	5	5
15	5	9
16	4	8
17	4	7
18	3	7
19	5	9
20	4	8
Total range time	85	152
Average Time	4.25	7.6

The third experiment: A key size of 256 bit was used with a packet size of the sender was 20016 byte, including 16 byte for key. It will be receiving 20000 byte. The following Table (4-3) shows estimated time to make the encryption and decryption.

Table (4-3) ... The third experiment

Process No.	Encryption Time (ms)	Decryption Time (ms)
1	6	12
2	5	8
3	5	10
4	5	8
5	4	7
6	4	6
7	4	7
8	4	10
9	5	7
10	6	9
11	5	8
12	5	6
13	4	7
14	5	7
15	5	8
16	4	7
17	5	8
18	4	7
19	4	10
20	4	7
Total range time	93	159
Average Time	4.65	7.95

The forth experiment: A key size of 256 bit was used with a packet size of the sender was 10016 byte, including 16 byte for key. It will be receiving 10000 byte. The following Table (4-4) shows estimated time to make the encryption and decryption.

Table (4-4) ... The forth experiment

Process No.	Encryption Time (ms)	Decryption Time (ms)
1	4	8
2	3	9
3	3	7
4	3	7
5	3	8
6	2	6
7	2	6
8	2	11
9	6	10
10	2	6
11	3	7
12	3	7
13	5	9
14	3	10
15	3	7
16	3	7
17	2	6
18	3	7
19	2	10
20	3	7
Total range time	60	155
Average Time	3	7.75

The fifth experiment: A key size of 256 bit was used with a packet size of the sender was 40016 byte, including 16 byte for key. It will be receiving 40000 byte. The following Table (4-5) shows estimated time to make the encryption and decryption.

Table (4-5) ... The fifth experiment

Process No.	Encryption Time (ms)	Decryption Time (ms)
1	8	11
2	8	15
3	11	14
4	10	13
5	8	12
6	8	11
7	9	12
8	9	14
9	9	12
10	9	12
11	9	10
12	8	11
13	10	13
14	8	11
15	8	14
16	8	11
17	8	13
18	9	12
19	8	11
20	7	10
Total range time	172	242
Average Time	8.6	12.1

In addition to the table mentioned above, noted the average time between the encryption and decryption process is 2.25 - 4.75 millisecond. It is depending on quality of service (Internet), with a service users' numbers, which used the fixed packet size (20000) byte and changed key size (128,192 and 256) bit, as shown in Figure (4-20).

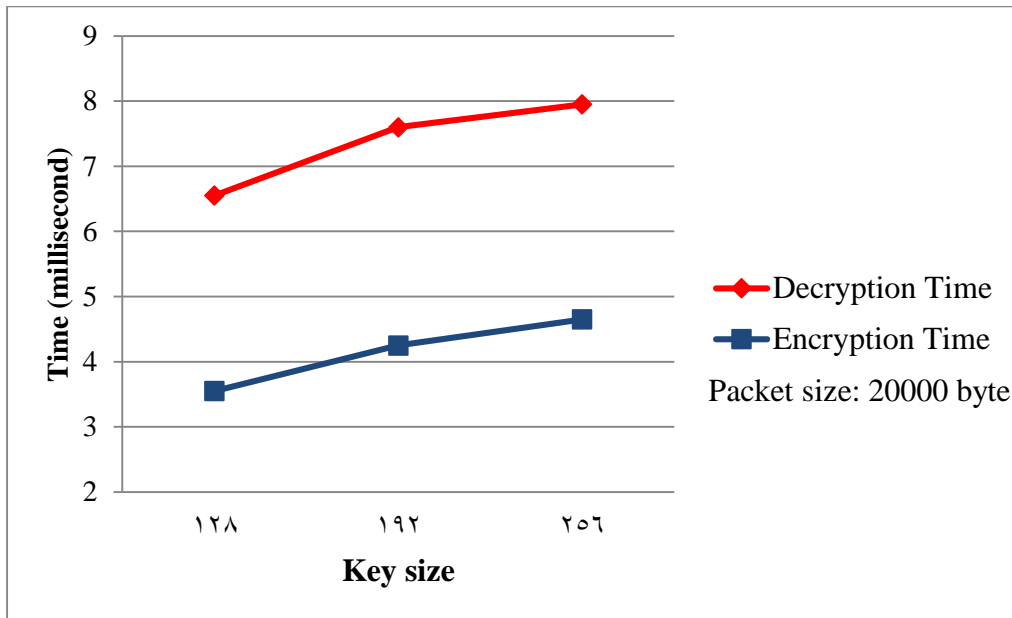


Figure (4-20) The results show for the effects of the key size on the Encryption & Decryption average time.

While is using the fixed key size (256) bit and changed packet size (10000, 20000 and 40000) byte, as shown in Figure (4-21).

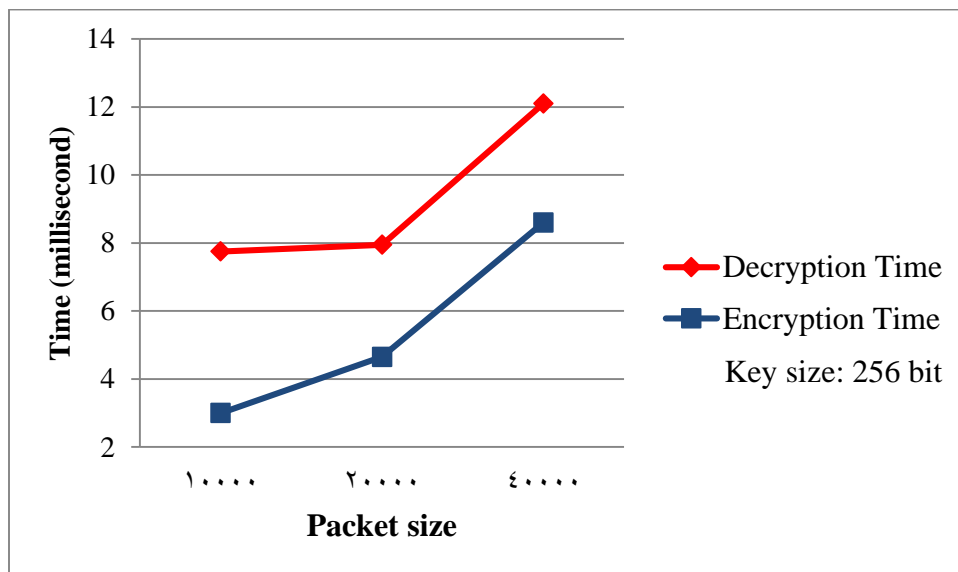


Figure (4-21) The results show for the effects of the packet size on the Encryption & Decryption average time.

The sixth experiment: It has used the same key size, packet in the fourth experiment, but on different devices which are router 54 megabyte per second, and PC with different properties (CPU 1800 GHz, RAM 2GB), HTC mobile device. This device is (Desire 500) CPU 1 GHz, RAM 4 GB. The following table (4-6) shows estimated time to make the encryption and decryption.

Table (4-6) ... The sixth experimen

Process No.	Encryption Time (ms)	Decryption Time (ms)
1	11	14
2	11	13
3	10	13
4	12	16
5	11	12
6	11	14
7	11	13
8	10	13
9	9	12
10	11	12
11	11	15
12	12	13
13	10	13
14	8	12
15	11	12
16	11	15
17	12	13
18	11	13
19	11	15

20	10	12
Total range time	214	265
Average Time	10.7	13.25

The following was observed after implementing these experiments, where in each one a different key were used more than the other one with similar packet or the opposite:

- In the 1st experiment obtained a high speed but unacceptable security is in data transfer.
- In the 2nd experiment obtained unacceptable security and unacceptable speed is in data transfer.
- In the 3rd experiments got insufficient security one time and insufficient speed on the other time.
- In the 4th experiment obtained acceptable speed and security is in data transfer.
- In the 5th experiment obtained a high security but unacceptable speed is in data transfer.

Consequently a key size of 256 bit and packet of 20000 bytes was selected as a proposed solution for acceptable security and speed, where the packet contains the data that the receiver can listen to the audio without delay. In addition, having enough time to decrypt the following packets and listen to it. Based on must take into account the effect of quality and service, as well as the number of users. Where affect the speed of transport directly.

Chapter Five: Conclusion and Future works

Introduction

This thesis has summarized the important points as a conclusion, and suggested some ideas for future works after the explanation of important general issues of VoIP, SIP server, RSA algorithm and AES algorithm.

5-1 Conclusion

VoIP service is providing very low-cost or semi-free voice calls through the internet, so it has get attention from many internet users. VoIP is subjected to various types of attacks called capturing packets, eavesdropping communications and many other types. So transmissions of media need different factors; these factors are confidentiality, authentication, and integrity with replay protection to the media stream.

Some users allowed listening on the transferred voice and dealing with this issue through adding any secured methods to supporter program during the transmission process. These secured methods; it could be through encryption or hiding the information to transmit data in a secured way. Some other problems such as delay of total time for the transmission process, that could be appeared through transmission or listening process.

In this thesis, mobile device is transmit in the voice through call process, call process based on SIP server, which used to setup IP based multimedia services such as audio and video streaming, instant messaging, and other real-time communication across commonly used packet networks.

The voice transmission process is providing in secured way by using two algorithms RSA, AES through advantages of each algorithm, the characteristics of AES algorithm is declared as high speed and reasonable security. In addition, a characteristic of RSA algorithm is declared as strong security and reasonable speed.

This thesis is using the advantages of AES speed with RSA security to produce an algorithm that called AR2SS (AES & RSA Speed and Security).

The proposed model implemented multi experiments in three procedures: SIP server procedure, sender procedure and receiver procedure which executing through a call between two phones. The model obtained many results that shown in chapter four, and declared difference of time for encryption and decryption processes.

The time difference is depending on the packet size from sender to receiver, with comparing the encryption and decryption processing time that declared possibility data encryption in suitable time. Results of experiments showed that the sent 20016 byte to each sender packet size, which is including 16 byte for key. It will be receiving 20000 bytes, and the total time between the encryption and decryption process for each packet is 2-5millisecond. It is depending on quality of service (Internet), with how to use a service in case of increasing number of user. But this difference is not effect on transfer voice.

5-2Future works

Even though, work in this thesis improved, that proposed solution enhanced security of VoIP; there are further research that can be done to enhance or support the presented solution such as:

1. Applied this program on other Mobile operating systems.
2. Applied this program to send messages on live chat programs and video calls.
3. It can use other techniques of exchanging key such as Diffi-Hellman exchange key algorithm.
4. The user can connect to global network rather than local network.

References

Alo, U., R., and Firday, N., H., (2013). Voice over Internet Protocol (VOIP): Overview, Direction and Challenges. Journal of Information Engineering and Applications, Vol.3, No.4.

Barengi, A., Bertoni, G., M., Breveglieri, L., and Pelosi, G., (2013). A fault induction technique based on voltage underfeeding with application to attacks against AES and RSA. Journal of Systems and Software, Vol. 86, Issue 7, page 1864-1878.

Cho, J., Soekamtoputra, S., Choi, K., and Moon, J., (2013). Power dissipation and area comparison of 512-bit and 1024-bit key AES. Computers and Mathematics with Applications.

Forouzan, A., B., (2006). Data Communications & Networking (sie). Tata McGraw-Hill Education.

Hong, S., Myeungjin Oh., M., and Lee, S., (2013). Design and implementation of an efficient defense mechanism against ARP spoofing attacks using AES and RSA. Mathematical and Computer Modeling.

Jung J., Y., Kang, H., S., Lee, J., R., (2013). Performance evaluation of packet aggregation scheme for VoIP service in wireless multi-hop network. Ad Hoc Networks.

Kaur, J., and Singh, K., P., (2013). Comparative Study of Speech Encryption Algorithms Using Mobile Applications. *International Journal of Computer Trends and Technology (IJCTT)*, Vol. 4, Issue 7.

Keromytis, A., D., (2009). Voice over IP: Risks, threats and vulnerabilities. *Cyber Infrastructure Protection*.

Kilinc, H., H., and Yanik, T., (2014). A Survey of SIP Authentication and Key Agreement Schemes. *IEEE Communications Surveys & Tutorials*, Vol. 16, No. 2, Second Quarter.

Krishna, S., (2013). Safety Dimensions of Session Initiation Protocol. *International Journal of Computer Science and Mobile Computing*, Vol. 2, Issue. 8, page 63 – 69.

Kumar, S., Narasimham Ch, and Setty, P., (2013). Small Secret Exponent Attack on Multiprime RSA. *International Journal of Soft Computing and Engineering*, Vol. 3, Issue. 2.

Kumar¹, R., and Chauhan, S., (2013). A Survey and Analysis of Media Keying Techniques in Session Initiation Protocol (SIP). *International Journal of Computer Science and Mobile Computing*, Vol. 2, Issue. 5, page 289 – 301.

Lazzez, A., (2013). VoIP Technology: Security Issues Analysis. arXiv preprint arXiv:1312.2225.

Malhotra, S., and Kaur, P., (2011). Comparison of Call Signaling Protocols for Ad-hoc Networks. *International Journal of Computer Applications*, Vol. 27, No.10.

Montazerolghaem, A., R., and Yaghmaee, M., H., (2013). Sip Overload Control Testbed: Design, Building And Evaluation. International Journal of Ambient Systems and Applications, Vol.1, No.2.

Naqi, Wei, W., Zhang, J., Wang, W., Zhao, J., Li, J., Shen, P., Yin, X., Xiao, X., and Hu, J., (2013). Analysis and Research of the RSA Algorithm, Information Technology Journal.

Pradhan, C., and Bisoi, A., K., (2013). Chaotic Variations of AES Algorithm. International Journal of Chaos, Control, Modeling and Simulation, Vol.2, No.2.

Preetha, M., Nithya, M. (2013). A Study and Performance Analysis of RSA Algorithm. International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 6, page.126 – 139.

Rakotondraina, T., E., Ravonimanantsoa, N., M., and Randriamitantsoa A., A., (2013). Contribution to Securing Communications on VOIP. International Journal of Computer Science and Network, Vol. 2, Issue. 3.

Rebahi, Y., Minh, N., T., and Zhang, G., (2008). Performance Analysis of Identity Management in the Session Initiation protocol (SIP). Computer Systems and Applications, AICCSA, IEEE/ACS International Conference, page. 711-717.

Sans, (2005). Voice Over Internet Protocol (VoIP) and Security, <https://www.sans.org/reading-room/whitepapers/voip/voice-internet-protocol-voip-security-1513>, Accessed by 15-1-2014.

Singh, H., P., Singh, S., Singh, J., and Khan, S., A., (2014). VoIP: State of art for global connectivity—A critical review. Journal of Network and Computer Applications, Vol.37, page 365-379.

Son, B., Nahm, E., and Kim, H., (2013). VoIP encryption module for securing privacy. Multimedia tools and applications Vol. 63 No.1, page. 181-193.

Stein, Y. and Malepati, H. (2008). Implementation of the AES algorithm on Deeply Pipelined DSP/RISC Processor, <http://www.embedded.com/design/connectivity/4007659/Implementation-of-the-AES-algorithm-on-Deeply-Pipelined-DSP-RISC-Processor>. Accessed by 15-7-2014.

Tang, C., and Oliver Wu, D., (2007). An Efficient Mobile Authentication Scheme for Wireless Networks. Transactions on Wireless Communications, IEEE.

Thiruppathi, M., S., (2012). Improving Quality in Voice Over Internet Protocol (VOIP) on Mobile Devices in Pervasive Environment”, Journal of Computer Applications ISSN: 0974 – 1925, Vol.5, Issue EICA2012-4.

Vargic, R., Kotuliak, I., Vrábel, A., and Husák, F., (2013). Provisioning of VoIP services for mobile subscribers using Wi-Fi access network. Telecommunication System.

Voznak, M., and Rozhon, J., (2013). Approach to stress tests in SIP environment based on marginal analysis. Telecommunication System.

Yen, Y., Lin, I., and Wu, B., (2011). A study on the forensic mechanisms of VoIP attacks: Analysis and digital evidence. Digital Investigation.

