A REAL-TIME SPEECH CRYPTOGRAPHY METHOD BASED ON ADPCM CODING AND CHAOTIC MAP FOR VOIP SYSTEM

BY

MOHAMMAD SHAHABUDDIN

A dissertation submitted in fulfilment of the requirement for the degree of Master of Science (Communication Engineering)

Kulliyyah of Engineering
International Islamic University Malaysia

OCTOBER 2019

ABSTRACT

The Voice over Internet Protocol (VoIP) system is an open access mobile communication service over the Internet. It has become popular in recent years because of constant development of high-speed internet, available software and comparatively cheap method of mobile communication. VoIP communication became the new priority for its easy audio, video, image and data exchange. In the era of digitalization, VoIP is the modern digital communication system, where business, education and research came to a strong bond. Although, it sounds good in teems the matter of cost and good features but, still now it is the most unsafe communication method for high hacking rates and easy to lose important data. Even though recent software's are becoming more intelligent for data, it requires more security in real-time environment. Safety may achieve by introducing comparatively large security method but it has to compromise the real-time environment. For VoIP system, real-time is a necessary requirement element, where most of the free software compromise with the security for real-time communication.

In this research, an approximately efficient encryption structure based on chaotic maps method and Adaptive Differential Pulse Code Modulation (ADPCM) coding technique as combined algorithm is proposed, to provide real-time secure for VoIP communication, conform to ITU-T Recommendation point G.726, and ANSI T1.303 – 1989 standard's connections 16, 24, 32 and 40 kbps for ADPCM transcoding algorithms. The chaotic map encryption has chosen for its high secure encoding with random values. ADPCM method has proposed for its transcoding energy efficiency and described small memory capable of two parallel encode functions per frame. The small memory of ADPCM holds the user define security keys. The proposed method of the encryption algorithm should have the adaptability of three main operations, 1. First, to generate chaotic values from independent initial conditions using two chaotic logistic maps, 2. The second step is to transform them into binary tables using random encoding condition and the final is 3. To execute basic proposed ADPCM process to increase more security.

The simulation analysis was performed on conventional maximised data encoding speed, ITU standard single ADPCM transcoding and proposed combined method to test the packet loss ratio, delay, jitter and channel quality performance of the proposed system.

خلاصة البحث

Voice over Internet Protocol (VoIP) هو خدمة اتصالات متنقلة مفتوحة الوصول عبر الإنترنت. لقد أصبح شائعًا في السنوات الأخيرة بسبب التطوير المستمر للإنترنت فائق السرعة ، والبرمجيات المتاحة وطريقة رخيصة نسبيا للاتصال المحمول. أصبحت الاتصالات عبر بروتوكول الإنترنت أولوية جديدة لسهولة تبادل الصوت والفيديو والصور والبيانات. في عصر الرقمنة ، أصبح VoIP هو نظام الاتصالات الرقمية الحديث ، حيث أصبحت الأعمال التجارية والتعليم والبحوث قوية. على الرغم من أنه يبدو جيدًا في مسألة التكلفة والميزات الجيدة ، إلا أنه لا يزال يمثل وسيلة الاتصال الأكثر أمانًا لمعدلات القرصنة العالية ومن السهل فقدان البيانات المهمة. على الرغم من أن البرامج الحديثة أصبحت أكثر ذكاءً بالنسبة للبيانات ، إلا أنها تتطلب مزيدًا من الأمان في بيئة الوقت الفعلي. قد تحقق السلامة من خلال إدخال طريقة أمان كبيرة نسبيًا ولكن يتعين عليها الإخلال بالبيئة في الوقت الفعلي. بالنسبة لنظام الصوت عبر بروتوكول الإنترنت (VoIP) ، يعد الوقت الفعلي عنصرًا ضروريًا للمتطلبات ، حيث تتعارض معظم البرامج المجانية مع أمان الاتصال في الوقت الفعلي.

في هذا البحث ، يُقترح هيكل تشفير فعال تقريبًا يعتمد على طريقة الخرائط الفوضوية وتقنية تشفير تشفير شفرة النبض التفاضلي التكيفي (ADPCM) وفقًا لخوارزمية مدمجة ، لتوفير وقت آمن للاتصال عبر بروتوكول الإنترنت ، وفقًا لنقطة التوصية ITU-T G. 726 و ANSI T1.303 - 1989 اتصالات القياسية 16 و 24 و 32 و 40 كيلو بايت في الثانية لخوارزميات ترميز ADPCM. اختارت تشفير الخريطة الفوضوية لترميزها عالي الأمان بقيم عشوائية. اقترحت طريقة ADPCM كفاءة ترميز الطاقة ووصفت ذاكرة صغيرة قادرة على وظيفتين تشفير متوازيين لكل إطار. ذاكرة صغيرة من ADPCM يحمل المستخدم تعريف مفاتيح الأمان. يجب أن يكون للطريقة المقترحة لخوارزمية التشفير القدرة على التكيف مع ثلاث عمليات رئيسية ، 1. أولاً ، لإنشاء قيم فوضوية من الشروط الأولية المستقلة باستخدام خريطتي لوجستية فوضويتين ، 2. والخطوة الثانية هي تحويلها إلى جداول ثنائية باستخدام شرط الترميز العشوائي والأخير هو 3. لتنفيذ عملية ADPCM الأساسية المقترحة لزيادة الأمن.

أجري تحليل المحاكاة على السرعة التقليدية المشفرة لترميز البيانات ، الشفرة الموحدة ADPCM الموحدة للاتحاد الدولي للاتصالات والطريقة المدمجة المقترحة لاختبار نسبة خسارة الرزم ، التأخير ، الارتعاش ، وجودة القناة في النظام المقترح.

APPROVAL PAGE

I certify that I have supervised and read this study and that in my opinion, it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Science (Communication Engineering.)

…………………………………..
Khaizuran Abdullah
Supervisor

…………………………………..
Ahmad Zamani Bin Jusoh
Co-Supervisor

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Science, (Communication Engineering.)

…………………………………..
Nurul Fariza Zulkurnain
Internal Examiner

…………………………………..
Ami Liza Asnawi
Internal Examiner

This dissertation was submitted to the Department of Electrical and Computer Engineering and is accepted as a fulfilment of the requirement for the degree of Master of Science, (Communication Engineering.)

…………………………………..
Mohamed Hadi Habaebi
Head, Department of Electrical
and Computer Engineering.

This dissertation was submitted to the Kulliyyah of Engineering and is accepted as a fulfilment of the requirement for the degree of Master of Science, (Communication Engineering.)

…………………………………..
Ahmad Faris Ismail
Dean, Kulliyyah of Engineering.

DECLARATION

I hereby declare that this dissertation is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Mohammad Shahabuddin

Signature.. Date.......................................

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

A REAL-TIME SPEECH CRYPTOGRAPHY METHOD BASED ON ADPCM CODING AND CHAOTIC MAP FOR VOIP SYSTEM

I declare that the copyright holder of this dissertation is the joined owned by the student and IIUM.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below

1. Any material contained in or derived from this unpublished research may be used by others in their writing with due acknowledgement.

2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.

3. The IIUM library will have the right to make, store in a retrieved system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that, I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Mohammad Shahabuddin

……..…………………….. ………………………..
Signature Date

ACKNOWLEDGEMENTS

In the name of Allah, the Most Gracious, the Most Merciful. This thesis is the result of my work as a master student of Electrical & Computer Engineering (IIUM). First, I thank my God (Allah S.W.T) who supplies all my needs. Thank you for inspiration and perseverance. Thank you, for the incomparable gift of salvation and the eternal hope you offer all who would place their trust in you.

I would like to thank my thesis supervisor, Associate Prof. Ir. Dr. Khaizuran Abdullah, for sharing her knowledge, guidance, patience and support me throughout this thesis. I would also like to thank Assist. Prof. Dr. Ahmad Zamani Bin Jusoh for giving supportive feedback on how to improve this work.

I truthfully present my appreciation to all of my friends and faculty members for supporting me on my thesis and publications.

Finally, I would like to thank my family for the endless encouragement in my academic pursuits.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AID	Analog-to-Digital
AC	Authentication Canters
ACELP	Algebraic Code Excited Linear Predictive
ADPCM	Adaptive Differential Pulse Code Modulation
AES	Advanced Encryption Standard
CA	Certificate Authorities
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CRHF	Collision Resistant Hash Function
CRL	Certificate Revocation List
CS-ACELP	Conjugate Structure Algebraic Code Excited Linear Predictive
CLM	Chaotic Map or Chaotic Lorenz Map.
CODEC	Compression/Decompression.
DA	Destination Address
Dl A	Digital-to-Analog
Dual-C	Dual-Core
DES	Data Encryption Standard
DS	Differential Service
DHCP	Dynamic Host Configuration Protocol
DIX	DEC, Intel, Xerox
DSP	Digital Signal Processing
DSLAM	Digital Subscriber Line Access Multiplexer
ECN	Explicit Congestion Notification
EF	Expedited Flow
ENT	ENTROPY
IPDV	Internet Protocol Packet Delay Variation
ITU	International Telecommunication Union
SLA	Service Level Agreements

LIST OF SYMBOLS

λ	Control parameter
x_0, X_0	Arbitrary initial condition for 1st process
y_0, Y_0	Arbitrary initial condition for 2nd process
n	Number of iterations with the time frame
s(k)	Input signal
k	Sampling index
$s_e(k)$	Estimated predicted
d(k)	Differential signal
y(k)	Scaling factor
α	Constant
β	Line slope or gradient
ε	Difference between two neighboring trajectories generating values.
F, G	Two logistic chaotic maps are denoted as f and g
$R_{F,0}$	Encryption scheme key shift register for f
$R_{G,0}$	Encryption scheme key shift register for g
λ_p	Variable control parameter for 1st logistic chaotic maps
μ_q	Variable control parameter for 2nd logistic chaotic maps
X_{i+1}, Y_{j+1}	Produced values of
m	Assigned variable
r	Number of bits binary code
I_k	Number of code word
$F_{k,r}$, $G_{k,r}$	Free spectral range (fsr)
S_{BF}, S_{BG}	Dynamic substitution process
$d_{ln(K)}$	Level of quantization
d_0, d_1	Distance parameter
d_k	Binary words transformation for k number of samples
$B_{k,r}$	Transformed into r-bit words for 1st logistic chaotic maps
$D_{k,r}$	Transformed into r-bit words for 2nd logistic chaotic maps
T_F, T_G	Encoding tables for f and g
$B_{k,o}$	Transformed encryption plot for o-bit binary
$D_{k,o}$	Transformed encryption plot for o-bit binary
$T(n)$	Transfer function of n number of bits
y_n, x_n	Initial conditions for *n* number iterations
$s_l(k)$	Converted into 16-bit pcm uniform signal

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

Modern telecommunication technologies are developing rapidly because of high number quality research and proper development. The rapid growth in telecommunication technologies is ahead of others because of digitalization, uses high frequency and robust security systems. Nowadays, internet over telephone is becoming the backbone of all communications. This research aimed to develop a secured and high performance method for the voice transmission or speech processing over the internet communication system known as VoIP.

The speech processing is a science related to the development of telecommunication technologies. Modern techniques of speech processing are designed to perform the analysis functions, synthesis, compression and security coding. This research is a part of development of speech security coding using ADPCM and Chaotic map. The choice of compression algorithm depends on the application domain (telephone, military radio, satellite communication) and the used equipment performance (software or hardware, DSP). In this research study, the encoding and decoding method using ADPCM (Adaptive Differential Pulse Code Modulation) technique is proposed. ADPCM is a coding technique mainly used for voice music and sound compression. The ADPCM algorithm technique that was designed previously for multimedia games and animations, (Purwar RK, Priyanka (2013) released into the public domain by several companies such as Oracle (Anees A, 2014) and IMA (Interactive Multimedia Association), also used by Apple and Microsoft for its simple structure of implementation and has low computational complexity.

Chaotic map was chosen for robust security where, the challenging task in the design of chaotic map as cryptographic techniques is to generate key streams of high randomness and statistical properties. In chaotic map the quality of the key stream generated by the security system determines its strength from cryptographic viewpoint. The importance of a careful design of cryptographic key stream generators cannot be underestimated as these generators are becoming particularly useful to ensure secure multimedia data transmission over an insecure communication channel. Generating key streams with high randomness is a vital part of many cryptographic operations.

The security method or secure processing of the voice encoding, and decoding is still a very important and indispensable process to protect voice communication against illegal access. The GSM, VoIP, telephone, analogue radio, and military communication system is generally based on same voice security processing rules and techniques. The increased need for confidentiality in the communication systems and telecommunications' always leads to develop of new techniques and algorithms for encryption.

1.2 PROBLEM STATEMENT

In this research, we have proposed ADPCM combined with Chaotic map for better performance. However, the ADPCM is a technique that uses the principle of proposed predictive coding which is based on a sequence of samples to predict the next sample. The Institute of Standards and Technology (ITU) standardized a 32 kbps ADPCM, known as G721 protocol, which gave reconstructed speech almost as good as the 64 kbps PCM codec (Phillippa Biggs, "The satus of voice over internet protocol (VoIP) worldwide, 2007)

On the other hand, the Chaotic map uses public key scheme for user authentication to server, secure key exchange, and symmetric stream cipher encryption scheme for speech data that encoded and compressed by ITU G.729 standard. The protocol comprises of four stages; User Connection Stage, User Authentication Stage, Distributed chaotic initial parameters Stage and Communication Stage (Mohamed Amine Ferrag, 2017). Use of two encoding tables for parallel method of speech conversion with selective number of binary words is difficult to implement.

The cryptographic system for speech conversion should not be vulnerable.

1.3 RESEARCH OBJECTIVES

The main aim of this research is to enhance secure control using ADPCM and Chaotic Mapping method for speech encryption system. The detailed objectives are:

1- To investigate and enhance a secure method design based on ADPCM and chaotic Map.

2- To simulate chaotic map based ADPCM method for speech encrypting to enhance packet loss, delay, Jitter in real time communication.

3- To evaluate the packet loss ratio, delay, and jitter and channel quality of the proposed algorithm with the existing algorithms.

1.4 PROPOSED DEVELOPMENT

- Secured ADPCM method.
- Introducing Chaotic-mapping system.
- Real-time operation scheme for encryption and decryption.

1.5 SCOPE OF THE RESEARCH

The operation of ADPCM method is to predict the current signal value from the previous transmitted values and to calculate only the difference between the real and the predicted value. The difference of the result may be quite small, so that it can produce fewer bits than the corresponding PCM encoded value. However, the efficient purpose of communication system is always to transmit maximum information using the minimum value of bit rate. ADPCM method is appropriate for signals, sound and images; those have strong correlations between successive samples values. The main scope is to –

1. Develop a new algorithm based on chaotic maps and ADPCM algorithm to implement predefine cyphers.
2. Evaluate the controller performance is evaluated for comparison with other controllers. Finalize the controller design and simulation output. Record benchmark performance for software compilation.

1.6 THESIS OUTLINE

To achieve the purposes of this thesis, the descriptions of ADPCM and Chaotic map method has been given (in chapter 2) for VoIP protocol. In addition, the previous study performance of individual method on VoIP system for the secure encoding and decoding has been described where, description of some good method also shown. Chapter 2 partly discussed the theoretical study. Chapter 3 contains the methodology of the research. Chapter 4 presents the results and discussion based on the methodology proposed in this research. Chapter 5 summarises the outcome of the research and conclude the findings.

1.7 THESIS CONTRIBUTION

In this research, we introduced a method for VoIP system based on combined secured chaotic method with ADPCM. Though both methods are not new, we have combined both method in a series with cross checking mechanism to get low packet loss ratio, low delay, low jitter and better channel quality then single performance of the methods. The simulation analysis was performed on maximised data encoding speed versus ITU standard ADPCM transcoding bits to test the cryptographic performance of the combined method over the single use of ADPCM or not aggregated signals in VoIP. The results have shown an improved performance than single ADPCM transcoding because, the proposed system have dual channel ADPCM transcoding operation to increase data encoding rate. Higher value of data encoding rate means higher value of compressed transcoded data ready to transfer through a single connection.

1.8 CHAPTER SUMMARY

This chapter has presented and discussed the background of the study about proposed systems for the Voice over Internet Protocol (VoIP). It explained why combined method is vital for the highly secure environment where fast communication is the main concern. Finally, it can say that the concept of combined method is one of the step-up proposals in VoIP system.

CHAPTER TWO

LITERATURE REVIEW

2.1 INTRODUCTION

Voice over Internet Protocol (VoIP) is a fast-growing service in communication technology. Due to the cost-effectiveness, many organizations have been deploying VoIP technology for their teleconferencing and video conferencing services. In recent decades, various types of unsecured applications have been developed, and different application protocols have been standardized but without providing any confidentiality to voice stream when traveling on the open or shared networks. However, most of VoIP applications were developed for transmitting voice data over an insecure network. The increasing demand for VoIP services results in increasing number of users who need a secure, a reliable, high quality of service, and efficient communication. In this research, a VoIP system speech encryption has been designed and implemented which is optimized for best real-time service delivery and increases the confidentiality and authority. It has also focused on studying the performance of VoIP system and encryption quality by using multiple data at the same time based on the chaotic Lorenz map and ADPCM method.

2.2 VOIP STRUCTURE

VoIP is one of the most common and cheap technology to communicate in short and long distance. It transmits the digitized voice data over IP network which provides a user to have a telephonic conversation over the existing Internet; this voice signal is appropriately encoded at one end of the communication channel transmitted using IP packets, and then decoded at the receiving end which transformed back into a voice signal.

The simple diagram, which is shown in Figure 2.1, can easily illustrate the idea of using VoIP calls. VoIP calls start from a Location A, traverse Router A if it is an IP based call otherwise routed towards PBX box, which further placed it to PSTN Voice network. This network switches it back to the destination PBX and then placed it to Location C. Whereas the IP call goes from Router A to Router C by the help of IP WAN DATA; they are diverted to the router and terminate over the destination location.

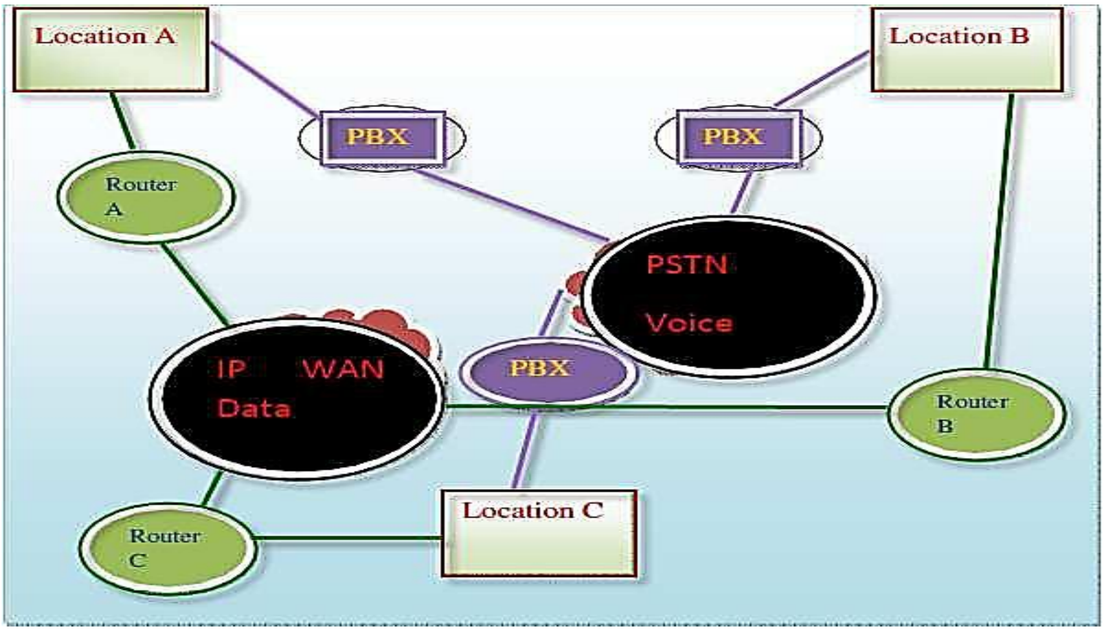

Figure 2.1 Illustration of a VoIP system (Amor Lazzez and Thabet Slimani. 2013)

Figure 2.2 shows the internal structure of VoIP calls made by IP phone. It starts from the IP phone; the first user presses the digital number on the dialling pad, which translate these digital numbers into binary codes. These binary codes are converted into IP packets and transmits towards the Local Area Network (LAN). They further transmit it towards the router, which analyses the IP address of the destination, and transmit further through the IP Network. The call has been treated according to the destination, for instance if it’s meant for an ordinary telephony then it will be directed towards a

PSTN Gateway which further switches towards the right destination. But if it's a VoIP call then it will go to the relevant router which analyses the IP address and direct towards a relevant LAN and then which further could be attended by an IP phone or a soft phone (software in computer or in a phone).

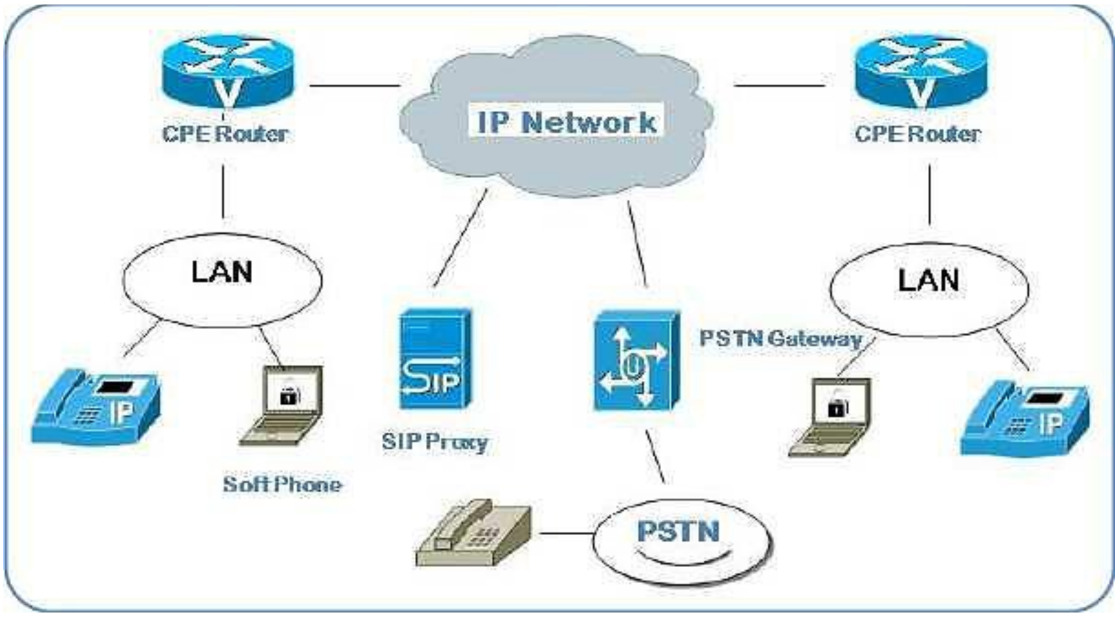

Figure 2.2 VoIP internal structure (Phillippa Biggs, 2007)

2.3 WORKING PRINCIPAL OF VOIP

VoIP uses Internet Protocol for transmission of voice as packets over IP networks. The process involves digitization of voice, the isolation of unwanted noise signals and then the compression of the voice signal using compression algorithms/codecs. After the compression, the voice is packetized to send over an IP network. Each packet needs a destination address sequence number and data for error checking. The signalling protocols are added at this stage to achieve these requirements along with the other call management requirements. When a voice packet arrives at the destination, the sequence number enables the packets to be place in order and then the decompression algorithms are applied to recover the data from the packets. Here the synchronization and delay management need to be taken care of to make sure that there is proper spacing. Jitter buffer is used to store the packets arriving out of order through different routes, to wait for the packets arriving late (Bakshi, 2016). There are many intermediate devices which serve the purpose as shown in the Figure 2.3.

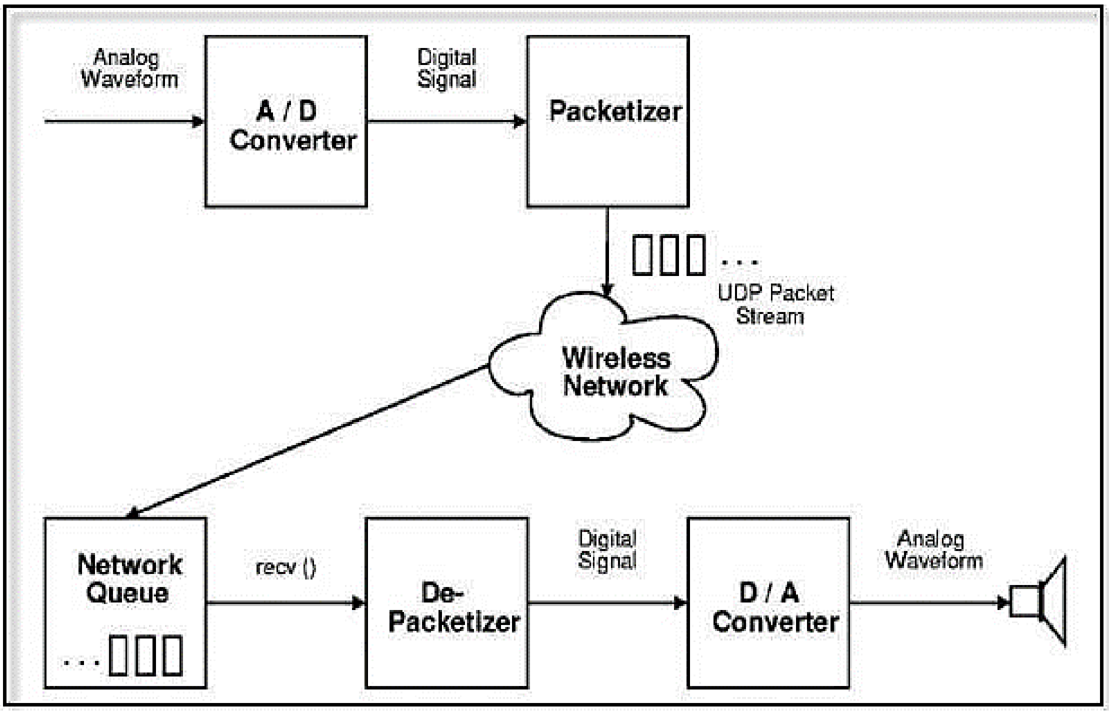

Figure 2.3 VoIP process (Mona Soliman Habib and Nirmala Bulusu ,2002)

2.4 SUMMARY OF VOIP WORKS

The overall working of VoIP is summarized at the following steps.

- Voice Capture: VoIP uses Internet Protocol for transmission of voice as packets over IP networks. VoIP communication needs an audio input device, like in ordinary PSTN system, such as a microphone, to send the audio signal. An analog-to-digital converter is used to transform that audio signal into digital bytes packets.

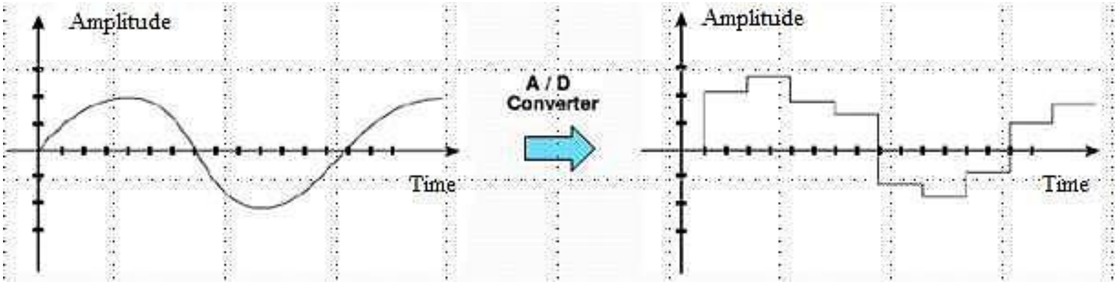

Figure 2.4 Analog to Digital conversion. (Mohamed Amine Ferrag, Volume 2017)

- Audio Data Encoding: Before sending the digital signal, it is important in packet-switched networks to prioritize voice data to be encoded. Then speech compression is engaged at this stage. Traditional telephone networks use pulse code modulation (PCM) at 8K samples per second. 12-bit samples are compressed and expanded by a nonlinear look-up table into 8-bit words giving a transmitted rate of 8kbit/s. The compression typically used by an Internet phone today is of the order of 16 to 1 (128kbit/s to 8kbit/s). Such compression is beyond PCM, ADPCM (32kbit/s, used in CT-2 cordless phones), or sub-band coding (down to 16kbit/s for speech bandwidths, normally used for music at higher bit rates).

- Packetization: After the compression, the voice is packetized to send over an IP network. The first packetization is implemented at application level by using RTP protocol. The voice packets are converted into data packets with RTP protocol. RTP data packets are sent to transport layer.

- For transport Layer (UDP): The transport layer provides the rules required for sending the data. Most data travelling over the Internet uses the Transmission Control Protocol (TCP) for the transport layer because it guarantees data delivery and integrity. VoIP does not need the kind of delivery guarantee which