ISSN: 2250-3676
Volume-3, Issue-4, 160-164

IMPLEMENTATION OF A VOIP MEDIA STREAM ENCRYPTION DEVICE

M.SUSHEEL KUMAR[1], M.SUDHAKAR [2]

1M.Tech, Department of ECE, CMR College of Engineering &Technology, Hyderabad, AP-India,
e-mail: susheelkumar8921@gmail.com
2 Professor in Dept of ECE, CMR College of Engineering & Technology, Hyderabad, AP-India.
email: vp@cmrcet.org

Abstract

This paper is to implement of a VoIP media stream encryption device for secure audio communication between the participants based on Mini S3C2440 (ARM 9) as a processor. Here we undergo RC4 encryption algorithm for secure data (audio) communication, to enable the VoIP protocol we use SIP, RTP protocol. The device can be placed between the soft switch or IP-PBX and the VoIP terminal, the encryption flow of data packetization is described when the VoIP protocol is SIP. Finally the device is tested and compares the voice signal at sender side and receiver side, the effectiveness in terms of clarity and security of the design is proved.

Index Terms: *ARM 9 Mini S3C2440, SIP, RTP, RC4 Encryption algorithm, VOIP.*

I.INTRODUCTION

VOIP (VoIP over internet protocol) communication technology is used to make phone calls through the internet cost effective. VoIP transmits packet via packet-switched based network, on the other hand the traditional public switched telephone network is based on circuit switched network. The differences are as follows.

In circuit-switching network the path is decided up on before the data transmission starts. Where as in packet switching network each packet has to find it own route to the destination and there is no pre determined path.

Circuit switching is a connection-oriented data transmission where as packet switching network is a connectionless-oriented data transmission.

Circuit switching is outdated and expensive where as packet switching is more modern and cheaper.

Circuit switching establishes fixed bandwidth circuits/channels between nodes and terminals before the users communicate. Where as in packet switching is a communication method the packets are routed between nodes over data links shared with other traffic.

Voice over IP (voice over Internet Protocol, VoIP) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, IP communications, and broadband phone service.

Voice over Internet Protocol (VoIP) which is also referred to as internet telephony is a technology that transmits voice signal in real time using the protocol (IP) over a public internet or private data network. In a simpler term, it converts voice signal which is analog to a digital signal in the device before compressing and encoding it into long strings of IP packets for upward transmission over the IP network to the receiver. At the receiving end, the received IP packets reassembles in order before decompressing and processing through the use of a Digital to Analogue Converter (DAC) to generate the initial signal transmitted [1].

VoIP systems employ session control and signaling protocols to control the signaling, set-up, and tear-down of calls.

They transport audio streams over IP networks using special media delivery protocols that encode voice, audio, video with audio codec's and video codec's as Digital audio by streaming media.

VoIP ARCHITECTURE

The major goal of the VOIP technology is establishing and managing communication sessions for transmitting both voice and data over a IP network. Some additional data format like video, text or images may also be supported by VoIP transmission. During this process, a stable and reliable transmission is maintained and the session can be put to end when any of the parties decide to. The two widely used protocols through the world today are the H323 and SIP protocol. For the purpose of the system and our VOIP deployment SIP protocol is used [1].

II. RELATED WORK

In this section SIP protocol, RTP protocol, mini S3C2440 processor, RC4 Encryption algorithm, are reviewed.

ARM9: (Mini2440 | S3C2440 ARM9 Board):

The MINI2440 Development Board is based on the Samsung S3C2440 microprocessor. Its PCB is 4-layer boarded, equipped with professional equal length wiring which ensures signal integrity. MINI2440 boards are Manufactured in mass production and released with strict quality control. On startup it directly boots preinstalled Linux by default. There are no extra setup steps or configuring procedures to start the system . It is easy for users to get started. Anyone with very basic knowledge about the C language can become proficient. The Mini2440 consist of on board 64M SDRAM and NAND Flash, 2M NOR flash with preinstalled BIOS, 100M Ethernet RJ-45 port (powered by the DM9000 network chip). The MINI2440 development board currently supports Linux 2.6.29, WinCE.NET 5.0 and Android.

SAMSUNG S3C2440 uses 16/32 bit ARM920T RISC technology for the core. Its main Frequency is 400M Hz. It provides an Ethernet controller DM9000 and audio codec UDA1341TS which are useful for this paper.

Ethernet controller:

The DM9000 is a fully integrated and cost-effective single chip fast Ethernet MAC controller with a general processor interface, a 10/100M PHY and 4k Dword SRAM. It is designed with low power and high performance process. The DM9000 supports 8-bit, 16-bit and 32-bit micro processor interface to internal memory access for different processors .the DM9000 also supports IEEE802.3X full- duplex flow control.

AUDIO CODEC:

The UDA1341TS is a single-chip stereo Analog-to-Digital Converter (ADC) and Digital-to-Analog Converter (DAC) with signal processing features employing bit stream conversion techniques. Its fully integrated analog front end, including Programmable Gain Amplifier (PGA) and a digital Automatic Gain Control (AGC). Digital Sound Processing (DSP) featuring makes the device an excellent choice for primary home stereo Minidisc applications, but by virtue of its low power and low voltage characteristics it is also suitable for portable applications such as MD/CD boom boxes, notebook PCs and digital video cameras.

Head phones: The head phone is used for giving audio input and audio output to the Mini S3C2440 processor. For VoIP communication between any two parties.

In this paper the system use two protocols SIP, RTP for the design of VOIP.

Session Initiation Protocol (SIP)

In this paper we are using session initiation protocol which was designed by IETF (internet engineering task force). It is an application layer protocol that establishes, manages, and terminates a multimedia session (call). It can be used to create two-party, multiparty, or multicast sessions. SIP is designed to be independent of the underlying transport layer; it can run on either UDP, TCP, or SCTP. The major driving force behind SIP is to enable VoIP [2].

.

Real-time Transport Protocol

This protocol is designed to handle real time traffic on the internet. RTP doesn't have a delivery mechanism. It must be used with UDP. RTP stands between UDP and the application program. RTP supports the transfer of real-time media (audio and video) over packet switched networks. It is used by both SIP and H.323. The transport protocol must allow the receiver to detect any losses in packets and also provide timing information so that the receiver can correctly compensate for delay jitter [2].

RC4 ALGORITHM

In this paper the system uses RC4 encryption /decryption algorithm for secure voice communication between any two participants. The algorithm is divided into two stages: initialization and operation. The RC4 is a stream cipher and a symmetric key algorithm the same algorithm is used for both encryption and decryption. The logic used in the RC4 algorithm data stream is simply XORed with the generated key Sequence. The key stream is independent of the plaintext is used. To initialize a 256-bit state table we use a variable length key from 1 to 256 bit. The state table is used for generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text [6].

The initialization process is shown by pseudo-code below

```
j = 0;
for i = 0 to 255:
S[i] = i;
for i = 0 to 255:
j = (j + S[i] + K[i]) mod 256;
swap S[i] and S[j];
```

In above code swapping of location of the numbers 0 to 255 in the state table is done. After the initialization process is completed then operation process is followed it is shown by pseudo code below

```
i = j = 0;
for (k = 0 to N-1) {
i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
Swap S[i] and S[j];
pr = S[ (S[i] + S[j]) mod 256]
Output M[k] XOR pr
}
```

M [0...N-1] is the input message consisting of N bits finally the algorithm produces a stream of pseudo-random values. The input stream is XORed with these values, bit by bit. The encryption and decryption process is same as the data stream is simply XORed with the generated key sequence.

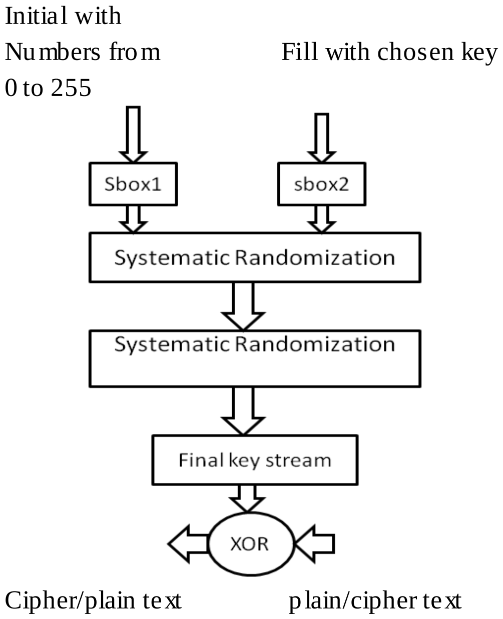


Figure1: RC4 Encryption Algorithm

RC4 Steps

The steps for RC4 encryption algorithm is as follows:

1- Get the data to be encrypted and the selected key.

2- Create two string arrays.

3- Initiate one array with numbers from 0 to 255.

4- Fill the other array with the selected key.

5- Randomize the first array depending on the array of the key.

6- Randomize the first array within itself to generate the final key stream.
7- XOR the final key stream with the data to be encrypted to give cipher text.

III. IMPLEMENTATION & RESULTS

In the implementation of the system as shown in the figure2. Firstly load operating system WIN CE 5.0 software in to MINI 2440 ARM 9 board using DNW tool for creating platform. The S3C2440 processor is ported with required modules like Ethernet controller, LCD TFT display, head phones, RJ45.

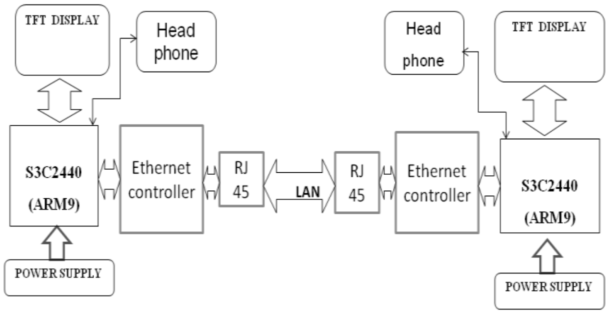
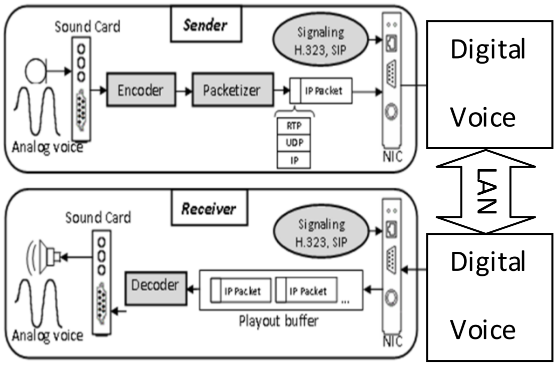


FIGURE 2: Hardware diagram of the system

SIP (session initiation protocol) is a signaling protocol and also a text based protocol like HTTP to establish a call connection between any two participants or to terminate the call. Then necessary SIP message commands should write in the code
In SIP there are six messages each command message used for different purpose.

1 The caller initializes a session with the INVITE
Message.
2 After the callee answers the call the caller sends an
ACK message for confirmation.
3 BYE message terminates a session
4 OPTIONS message queries a machine capabilities.
5 CANCEL message cancels an already started
Initialization process.
6 REGISTER message makes a connection when the
Callee is not available.



If a connection is establish the voice of a sender side is act as an input to the device. The voice is converted analog to digital data by using audio codec UDA1341TS. For secure voice communication between caller and callee the system use a RC4 algorithm. The data stream which is available from audio codec is XORed with the generated key sequence. At the receiver side data is decrypted and also audio CODEC is used to get original voice of the caller. At packetization level the system use RTP protocol because it supports the transfer of real –time media (audio and video) over packet switched networks. The RTP is used by both SIP and H.323. In this way there will be secure voice conversion between the caller and the callee.

Caller (HOST)

Callee

The device is tested by taking a sample voice. The tests results have shown that sample voice at the sender side is replicated at receiver side and vice - versa. The system can Support full-duplex secure communication of voice by taking 3 or 4 callees (nodes) with the help of LAN. If there is any peer - peer communication the third person should not hear voice conversation of others as the system used RC4 encryption algorithm.

CONCLUSION:

VOIP media stream encryption device is mainly implemented for defence sector, R&D, and also for public domain for secured voice communication at lower costs.

REFERENCES

[1] David Endler, “Hacking Exposed VoIP: Voice Over IP security Secrets & Solutions,” McGraw Hill Osborne Media.

[2] Behrouz A.Forouzan, TCP/IP protocol suite Tata McGraw-Hill publication.

[3] D.Richard Kuhn, “Security Consideration for Voice Over IP Systems,” NIST Special Publication 800-58.

[4] http:// www.Friendly ARM MINI 2440.com - Datasheet.

[5] http:// www.Friendly ARM MINI 2440.com Programming Guide.

[6] X.Lai, “ on the Design and security of Block Ciphers,” ETH Series in Information processing,vol.1 Konstanz:Hartung_ Georre Verlag, 1992.

[7] A.F Webster and S.E.Tavares, “ on the Design of S-box. Advances in Cryptology-crypto 85,” Springer-verlag.

BIOGRAPHIES

M.SusheelKumar received Bachelor Degree in Electronics and Communications from JNTUH college of Engg and Technology, HYDERABAD. Presently he is pursuing his M.Tech (Embedded systems) in CMRCET college of Engg and Technology, Hyderabad.

Prof. M. Sudhakar is currently working as Professor & vice principal in CMRCET college of Engg and Technology. Graduated (B.Tech) from JNTU College of Engineering, Hyderabad with the specialization of ECE. Post graduation (M.Tech) from Indian Institute of Technology, Madras with the specialization of Instrumentation, Control & Guidance. He also did his PG Degree in Aeronautical Engineering (Electronics) from Air Force Technical College, Bangalore. Presently pursuing his research in “Intelligent and Adaptive Control Systems, in JNTU Hyderabad.