Advance in Electronic and Electric Engineering
ISSN 2231-1297, Volume 3, Number 1 (2013), pp. 71-76
© Research India Publications
http://www.ripublication.com/aeee.htm

VOIP Media Stream Encryption Device

Anshu Shahdeo, G. Sahitya and N. Balaji

VNRVJIET (JNTU) Hyderabad, INDIA.
VNRVJIET (JNTU) Hyderabad INDIA
JNTU Kakinada Vijayanagar, INDIA.

Abstract

Our main aim is to design and develop VoIP media stream encryption device based on ARM9 microcontroller. It will be a low cost feature which will be based on embedded platform for VOIP media using ARM 32 bit Microcontroller and has feature of image/video processing by using various features and classification algorithms. The design can be used as VOIP media device communications platform for multiple applications areas. The device can be deployed between the VOICE OVER INTERNET PROTOCAL (VOIP) terminal, dedicatedly used for the encryption/de-encryption of the VoIP signal and the RTP voice packet. The encryption flow of the packet is described when the VoIP protocol is SIP and the encryption algorithm is RC4. Embedded system is designed for transferring voice through Internet protocol for low cost phone calls using SAMSUNG Corporation S3C2440 chips as core processor.

Keywords: Linux, S3C2440 (Friendly ARM), Application Language(C/C++), USB Drivers, Display Drivers.

1. Introduction

Voice over IP (VOIP) is the transmission of voice messages over a packet switched network using IP. Like most things associated with the Internet, this technology has the potential to change the way we communicate today. It offers a chip alternative to traditional telephone system. SAMSUNG's S3C2440A 16/32-bit RISC microprocessor. SAMSUNG’s S3C2440A is designed to provide hand-held devices and general applications with low-power, and high-performance microcontroller solution in small die size. The S3C2440A is developed with ARM920T core, 0.13um

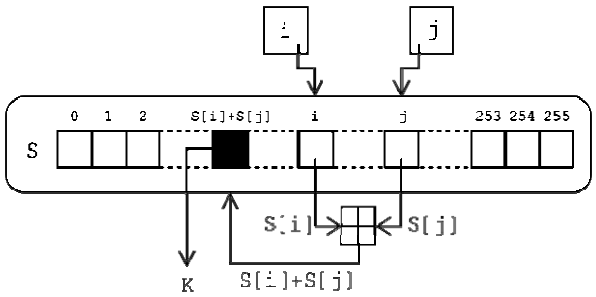
CMOS standard cells and a memory complier. Here we are using RC4 encryption algorithm and Session Initiation Protocol (SIP).

2. Description

2.1 RC4

RC4 is used as the encryption algorithm. RC4 was designed by Ron Rivest of RSA Security in 1987. It is officially termed as "Rivest Cipher 4. RC4 commonly used as encryption protocols and standards, including WEP and WPA for wireless cards and TLS. It is widely used due to its speed and simplicity and efficient implementations in both software and hardware are very easy to develop. RC4 generates a pseudorandom stream of bits (a keystream). As with any stream cipher, these can be used for encryption by combining it with the plaintext using bit-wise exclusive-or and decryption is performed the same way. To generate the keystream, the cipher makes use of a secret internal state which consists of two parts:

1. A permutation of all 256 possible bytes (denoted "S" below).
2. Two 8-bit index-pointers (denoted "i" and "j").



The lookup stage of RC4. The output byte is selected by looking up the values of S(i) and S(j), adding them together modulo 256, and then using the sum as an index into S; S(S(i) + S(j)) is used as a byte of the key stream, K.

2.2 Session Initiation Protocol

Session Initiation Protocol is an application layer control (signaling) protocol for creating, modifying and terminating session with one or more participants. This session include Internet Telephone calls, multimedia distribution and multimedia conferences. SIP supports five facts of establishing and terminating multimedia communication:

User location: Determination of the system to be used for communication.

User availability: Determination of the willingness of the called party to engage in communication.

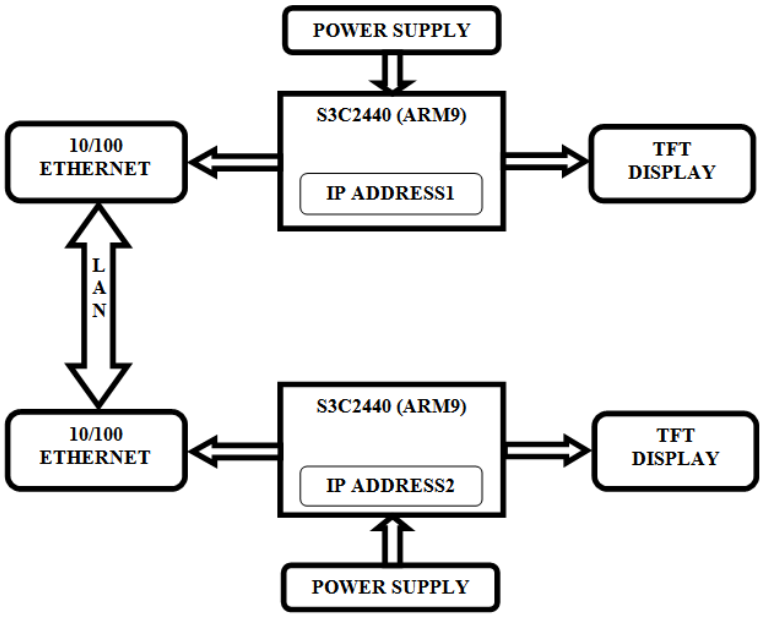
User capabilities: Determination of the media and media parameters to be used.

Session Setup: “Ringing”, establishment of session parameters at both called and calling party.

Session management: Including transfer and termination of session, modifying session parameters and invoking services. SIP architecture will include protocols such as the Real Time Transport protocol (RTP) for transporting Real Time data and providing QOS feedback, the real time streaming protocol (RTSP) (RFC) for trolling delivery of streaming media.

3. Imlementation

3.1 Internal working:



This project contains ARM9 board which is having in built memory where we store program. The ARM9 board uses a 1.8v power supply.

The board is programmed through DB9 connector to the PC. We have serial communication ports which are used to interface directly to the RS232 cable interfaced directly to the PC. The program is burned inside the controller by using the tool DNW.

The VoIP media stream system makes use of providing voice calls through internet which is interfaced to lower power consumptive and highly advanced micro controller like S3C2440. S3C2440 is a Samsung company’s microcontroller which is designed based on the structure of ARM 920T family. This microcontroller works for an voltage of +1.8V DC and at an operating frequency of 400 MHz The maximum frequency up to which this micro controller can work is 533 MHz

We cannot get S3C2440 microcontroller individually. We will get it in the form of FRIENDLY ARM board otherwise we can call it as MINI 2440 board.

In order to work with ARM 9 micro controllers we require 3 things. They are listed below.

1. Boot Loader
2. Kernel
3. Root File System

The essential programs that are required in order to work with MINI 2440 like Boot loader, Embedded Linux related Kernel, Root File System will be loaded into the NOR flash which is present on the MINI 2440 board itself. The program that is related with the application will be loaded into NAND flash which is also present on the MINI 2440 board itself. By using boot strap switch that is present on the MINI 2440 will help the user to select either NOR or NAND flash. After that by using DNW tool we can load Boot loader, Embedded Linux related kernel and Root File System into NOR flash by using USB cable and the application related program into NAND flash.

Once loading everything into MINI 2440 board it will work based on the application program that we have loaded into the NAND flash.

Voice over Internet Protocol (VoIP) is a technology that enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using IP rather than by traditional circuit transmissions of the PSTN. Here we are using two ARM9 boards which are used to communicate with each other by using VoIP technology. First ARM9 board having one IP address and second board having another IP address. The two ARM9 boards are connected through internet through Ethernet cable. By typing destination IP address the two devices can communicate and transfer the voice through VoIP. The voice can directly given by MIC which is present in the ARM9 board and voice can convert in the form of packets and transfer it to server through ARM9 board. The server will retransmit the packets to the destination IP address. At the other end the ARM9 board retrieves the packets into voice. Like that two devices can communicate over Internet Protocol.

4. Conclusion

The project “DESIGN OF A VOIP MEDIA STREAM ENCRYPTION DEVICE” has been successfully designed and tested. It has been developed by integrating features of all the hardware components and software used. Presence of every module has been reasoned out and placed carefully thus contributing to the best working of the unit. Secondly, using highly advanced ARM9 board and with the help of growing technology the project has been successfully implemented.

5. Acknowledgements

I would like to thank my guide G.Sahitya and Dr.N.Balaji for guiding me throughout the project. I am also thankful to my husband Sandeep Shahdeo who supported me during this project. In addition to that I would like to thank Prof. (Dr.) Ranjeet Kumar Singh HOD Chemistry BIT Sindri.

References

[1] Datasheets and the user manuals of S3C2440.
[2] http://www.ietf.org/html.charters/sip-charter.html
[3] http://www.cse.wustl.edu/~jain/refs/voi_book.htm