ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Clandestine VOIP Communications Using Steganography Technique over Smart Grid Applications

V.Krishnaiah
M.Tech,
Department of ECE,
Aurora's Technological and Research Institute,
Hyderabad, Telangana, India.

T.Shirisha
Assistant Professor,
Department of ECE,
Aurora's Technological and Research Institute,
Hyderabad, Telangana, India.

Abstract:

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. In this project, I am using Stegnography encryption algorithm. The encryption algorithm provides secure communication between the participants. This algorithm is used for both encryption and decryption.During the entire process a protocol like SIP is used to control the call (e.g. setting up connection, dialing, disconnecting etc.) and RTP is used for reliable transmission of data packets and maintain quality of service. Here I am using two ARM9 boards which are used to communicate with each other by using VoIP technology. The 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 using SIP protocol. By typing destination IP address on the TFT display and press the CALL button then the two devices can communicate and transfer the voice through RTP protocol. 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. If anyone wants to terminate the communication press END button which will disconnect the SIP session.

Keywords:

ARM microcontroller, Stegnography encryption algorithm, encrypted data, secret data.

I.INTRODUCTION:

Smart grids use the information and communication technology to collect and process information aiming at improving the efficiency, reliability, economy and the sustainability of electric power production and distribution. Smart grids collect information by using some measurement systems, and exchange a great deal of information in real time. Because of its advantages, smart grids have been spread worldwide, and many countries are investing in smart grids. However, smart grids have real difficulty with data security, because they do not provide secure exchange of information between the stations. Stegnography is a method of embedding secret data into a cover, which never causes unacceptable distortion and observers' attention. Stegnography and encryption technology both keep the confidentiality of secret data, but there is a difference in the idea. Encryption technology only protects the content of secret data, making it unreadable. Unauthorized users can know the existence except the specific details about the secret data. Stegnography hides the existence of secret data; unauthorized users know neither the existence of secret data nor the details. Stegnography is one of the most important parts of information security, becoming more and more widely applied in various fields. For example, military communication systems usually need higher security level. It not only needs to encrypt messages exchanged, but also hide the existence of messages. Attackers even can't perceive it. For protecting the intellectual property of digital products, merchants usually embed their trade mark or unique logo into digital products with Stegnography. These are some applications of Stegnography.

II.LITERATURE SURVEY:

In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

There are many possible ways to transmit data using the internet: via e-mails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the „security threat it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. In order to improve the security features in data transfers over the internet, many techniques have been developed like: digital watermarking Cryptography and Steganography. While Cryptography is a method to conceal information by encrypting it to cipher texts and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats.

III.AES ALGORITHM:

AES (the Advanced Encryption Standard) is a fundamental building block of the encryption within 1Password and most everything else that uses encryption in the modern world. It takes a key and some data (plaintext) as input and transforms that data into something that looks entirely random (ciphertext). The only way to get meaning out of the ciphertext is to use AES and the same key to transform it back into the plaintext. A key is just a number, and AES can work with keys of three different sizes, 128 bits, 192 bits, and 256 bits.AES, by the way, is always a 128-bit cipher operating on 128-bit chunks of data (blocks) at a time; so when I use expressions like “AES256″ or “256-bit AES” in what follows; I’m just talking about key size.

The numbers that we need to talk about are just too big to write out normally. When we are dealing with numbers like 65536, I can opt whether to express it as “65536” or “216“, depending on what is most useful in the context. And maybe when dealing with a number like 232 I can say things like “4.3 billion”.But the numbers we deal with in cryptography are so big that I have to write them in exponential form.

The number of possible keys that a 128-bit key allows is just too enormous to write otherwise. Sure, I could write out 2128 in words with the help of a numbers to words converter, but it is neither informative nor manageable. Nor would it be useful for me to write out the number in decimal, as it would be 39 digits long. Briefly, there is a long-known problem with how AES deals with 256-bit AES keys. (Of course in this business a “long-known problem” means about 10 years old.) AES does multiple rounds of transforming each chunk of data, and it uses different portions of the key in these different rounds.

The specification for which portions of the key get used when is called the “key schedule”. The key schedule for 256-bit keys is not as well designed as the key schedule for 128-bit keys. And in recent years there has been substantial progress in turning those design problems into potential attacks on AES 256. This is the basis for Bruce Schneier’s advice on key choice.

IV.EXISTING SYTEM:

Voice over Internet Protocol (VoIP) is one of the most popular real-time services on the Internet. VoIP has more advantages than traditional telephony, since the Internet allows VoIP to provide low-cost, high-reliability and global services. With the increasing percentage of VoIP streams in all of the Internet traffic, VoIP is a better cover for information hiding. Besides, VoIP connection is usually short, it is uneasy for attackers to detect. However the existing system is not provided the security of secret information and it does not allow too many operations, making it difficult to add more operations to improve the security level.

V.PROPOSED SYSTEM:

To overcome the drawback present in existing system we are proposing a VoIP Stegnography method based on AES to achieve a real-time covert communication over smart grids. There are many literatures in researching VoIP Stegnography; we can divide them into two categories. One is embedding secret data into some free or unused fields of TCP/IP protocol headers. The other one is embedding secret data into the payload of VoIP packets.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

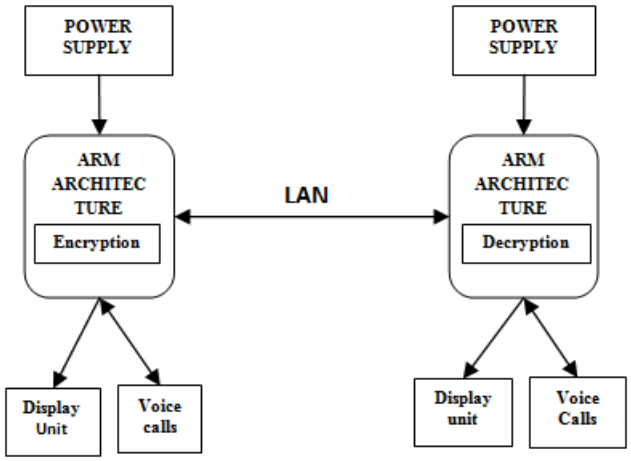
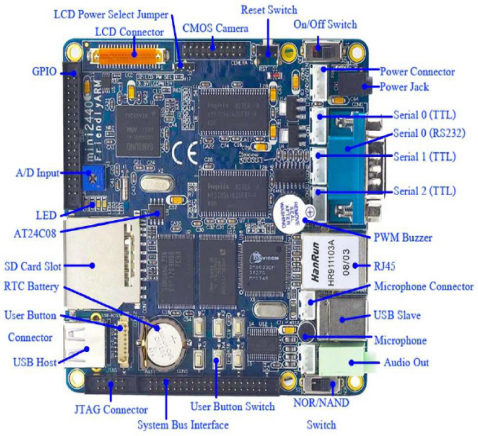


Fig.1: Block Diagram for Proposed system

In order to meet the requirement of real-time, we encrypt the secret message and embed it with different algorithms into audio packets before sending them. So observers cannot detect it by using a simple statistical analysis. At the receiving end, we employ the corresponding method to retrieve the secret message, and then decrypt it to get the original message. For implementing this project we are using 32-bit ARM micro controller. In this we are using different embedding methods; each packet has a different capacity for embedding the secret message.

VI.HARDWARE IMPLEMENTATION

Mini2440 Development board:



Mini2440 is a practical low-cost ARM9 development board, is currently the highest in a cost-effective learning board. It is for the Samsung S3C2440 processor and the use of professional power stable core CPU chip to chip and reset security permit system stability.

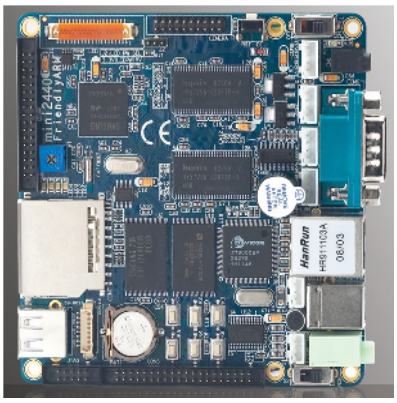


Fig2. Mini2440 Development board

The mini2440 Immersion Gold PCB using the 4-layer board design process, professional, such as long-wiring to ensure that the key signal lines of signal integrity, the production of SMT machine, mass production; the factory have been a strict quality control, with very detailed in this manual can help you quickly master the development of embedded Linux.

VII.SOFTWARE IMPLEMENTATION:

A.Linux Operating System:

Linux or GNU/Linux is a free and open source software operating system for computers. The operating system is a collection of the basic instructions that tell the electronic parts of the computer what to do and how to work. Free and open source software (FOSS) means that everyone has the freedom to use it, see how it works, and changes it.

There is a lot of software for Linux, and since Linux is free software it means that none of the software will put any license restrictions on users. This is one of the reasons why many people like to use Linux.A Linux-based system is a modular Unix-like operating system. It derives much of its basic design from principles established in UNIX during the 1970s and 1980s.

Such a system uses a monolithic kernel, the Linux kernel, which handles process control, networking, and peripheral and file system access. Device drivers are either integrated directly with the kernel or added as modules loaded while the system is running.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

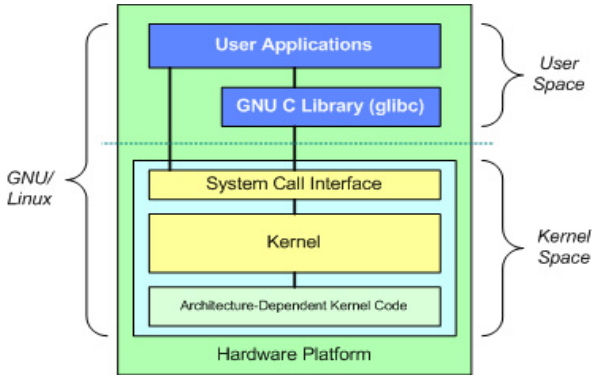


Fig.3: Architecture of Linux Operating System

B.Qt for Embedded linux:

Qt is a cross-platform application framework that is widely used for developing application software with a graphical user interface (GUI) (in which cases Qt is classified as awidget toolkit), and also used for developing non-GUI programs such ascommand-line tools and consoles for servers. Qt uses standard C++ but makes extensive use of a special code generator (called the Meta Object Compiler, or moc) together with several macros to enrich the language.

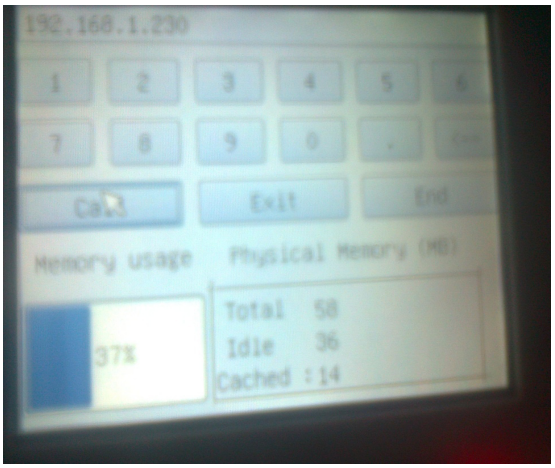
Qt can also be used in several other programming languages via language bindings. It runs on the major desktop platforms and some of the mobile platforms. Non-GUI features include SQL database access, XML parsing, thread management, network support, and a unified cross-platform application programing interface for file handling.It has extensive internationalization support.

VIII.RESULTS:

The hardware kit of project:

Performance of board:

Performance of board at calling time:



IX. CONCLUSION:

The project "Clandestine Voip Communications-Using Steganography Technique Over Smart Grid Applications" 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 ARM board and with the help of growing technology the project has been successfully implemented.

X.REFERENCES:

[1] C. H. Yang, C. Y. Weng, S. J. Wang, Etc." Adaptive Data Hiding In Edge Areas Of Images With Spatial Lsb Domain Systems," Ieee RansactionsOn Information Forensics And Security, Vol. 3, Pp. 488-497, Sep. 2008.

[2] Y. K. Lee, L. H. Chen, "High Capacity Image Steganographic Model," Iee Proceedings-Vision Image And Signal Processing, Vol. 147, Pp. 288-294, Jun. 2000.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[3] LM. Marvel, CG. Boncelet, CT. Retter, "Spread spectrum image steganography," IEEE TRANSACTIONS ON IMAGE PROCESSING,vol. 8, pp. 1075-1083, Aug. 1999.

[4] R. Darsana, A. Vijayan. "Audio Steganography Using Modified LSB and PVD," TRENDS IN NETWORKS AND COMMUNICATIONS, vol. 197, pp. 11-20, 2011.

[5] N. Cvejic,T. Seppanen, "Increasing the capacity of LSB-based audio steganography," in Proc. 5th IEEE Workshop on Multimedia Signal Processing (MMSP 2002), ST THOMAS, 2002, pp. 336-338.

[6] O. Cetin, F. Akar, A. T. Ozcerit, etc. "A blind steganography method based on histograms on video files," IMAGING SCIENCE JOURNAL,vol. 60, pp. 75-82, Apr. 2012.

[7] W. Mazurczyk, K. Szczypiorski, "Steganography of VoIP streams," Lecture Notes in Computer Science, vol. 5332, pp. 1001-1018, 2008.

[8] Y. F. Huang, S. Tang, C. Bao, Y.j. Yip. "Steganalysis of compressed speech to detect covert voice over Internet protocol channels," IET INFORMATION SECURITY, vol. 5, lss.1, pp. 26-32, 2011.

[9] R. Miao,Y. F. Huang, "An Approach of Covert Communication Based on the Adaptive Steganography Scheme on Voice over IP," Proc. IEEE Int Conf. on Communications, Kyoto, Japan, JUN 05-09, 2011.

[10] C. Kratzer, J. Dittmann, T. Vogel and R. Hillert. "Design and evaluation of steganography for Voice -over-IP," Proc. IEEE Int. Symp. on Circuits and Systems, Kos, GREECE, 21-24 May 2006, pp. 2397-2340.

[11] H. Tian, K. Zhou, Y. F. Huang, etc. "A Covert Communication Model Based on Least Significant Bits Steganography in Voice over IP," Proc. 9th Int. Conf. for Young Computer Scientists, Zhangjiajie, PEOPLES R CHINA, NOV 18-21, 2008, pp.647-652.

[12] C.Y. Wang, Q. Wu, "Information Hiding in Real-time VoIP Streams," Proc. 9th IEEE Int. Symp. on Multimedia, Taichung, Taiwan, DEC 10-12 2007, pp. 255-262.

[13]Daemen, Joan; Rijmen, Vincent (9/04/2003)."AES Proposal: Rijndael". National Institute of Standards and Technology. p. 1. Retrieved 21 February 2013.

[14] FIPS 197, Announcing the advanced encryption standard (AES), 2001.