Journal of Naval Science and Engineering
2011, Vol.7 , No.1, pp. 37-47

A ROBUST REAL-TIME SECURE COMMUNICATION APPROACH OVER PUBLIC SWITCHED TELEPHONE NETWORK

Ahmet KARACA
Technical Education Faculty,
Computer Systems Education,
Esentepe Campus, Serdivan, Sakarya, 54187,Turkey
akaraca@sakarya.edu.tr

Özdemir ÇETIN
Asst.Prof.
Technical Education Faculty,
Computer Systems Education,
Esentepe Campus, Serdivan, Sakarya, 54187,Turkey
ocetin@sakarya.edu.tr

Abstract

In this paper, a secure phone system implemented over Public Switched Telephone Network (PSTN). Speech data is sent through a dial-up modem over PSTN to receiver after converted digital form and ciphered. In this study, Scalable Encryption Algorithm (SEA) is used. SEA is developed for systems have low level memory and low power process. Also in this system, a text file can be embedded into speech data before encrypted voice data. By this means, security of system is increased. During a text file is embedding into speech data, distortion in speech data is kept low level according to Human Auditory System (HAS). Even if eavesdroppers can get decrypted speech data they must detect hidden data in speech data. And then malicious people have to use steganalysis techniques to get secret data.

A Robust Real-Time Secure Communication Approach Over Public Switched Telephone Network

AÇIK ANAHTARLAMALI TELEFON HATTI ÜZERİNDEN GERÇEK ZAMANLI DAYANIKLI BİR GÜVENLİ HABERLEŞME YAKLAŞIMI

Özetçe

Bu çalışmada Public Switched Telephone Network (PSTN) üzerinden güvenli haberleşme amaçlı bir sistem gerçekleştirilmiştir. Konuşma sinyali dijital sinyale çevrilip şifrelendikten sonra bir dial up modem aracılığıyla PSTN üzerinden alıcıya gönderilmektedir. Burada şifreleme için düşük bellek ve işlem gücüne sahip sistemler için geliştirilmiş SEA kullanılmıştır. Gerçekleştirilen sistem ile aynı zamanda konuşma sinyali şifrelenmeden önce bu sinyalin üzerine bir metin dosyası gizlenebilmektedir ve bu sayede sistemin güvenliği arttırılmıştır. Metin dosyası ses sinyali üzerine gömülürken ses sinyalindeki bozulmalar kulakla algılanmayacak seviyede tutulmaktadır. Hattı dinleyen yetkisiz kişiler şifrelemeyi çözüp ses sinyalini elde etseler bile ses içinde gizlenmiş bir veri olduğunu algılayıp steganaliz yöntemleri ile bunu çözmeleri gerekmektedir.

Keywords: PSTN, SEA, secure communication, steganography, steganalysis
Anahtar Kelimeler: PSTN, SEA, güvenli Haberleşme, stenografi, steganaliz

1. INTRODUCTION

In the present day, information technologies are developing rapidly. The result of this, secure communication between individuals and corporations becomes an important issue among researchers. So far many secure communication techniques have been developed about audio, video or text data cipher [1-5]. The important aim for these techniques is to protect privacy of communication.

Nowadays, people commonly use voice communication resources are becoming a big part of life in their very important works such as Internet

banking. Because of this, ensuring reliability of communication media is becoming important issue. Wireless secure communication techniques are different than wire secure communication techniques. Wireless techniques are more open to attack than wire techniques [8-11]. Because security of wireless communication is more vulnerable than wire to use wire communication when high security level is necessary is more convenient.

In the proposed study, a secure communication implementation is aimed over wire phone lines. However choosing wire phone lines for secure communication bring some restriction. For instance, bandwidth is between 300 Hz and 3500 Hz for voice communication in switchboard [9,10]. Therefore, voice data is sent after compression over the phone line. Compression process causes decrease sample number and also reduces voice quality. Hereby, secret communication possibility is reduced.

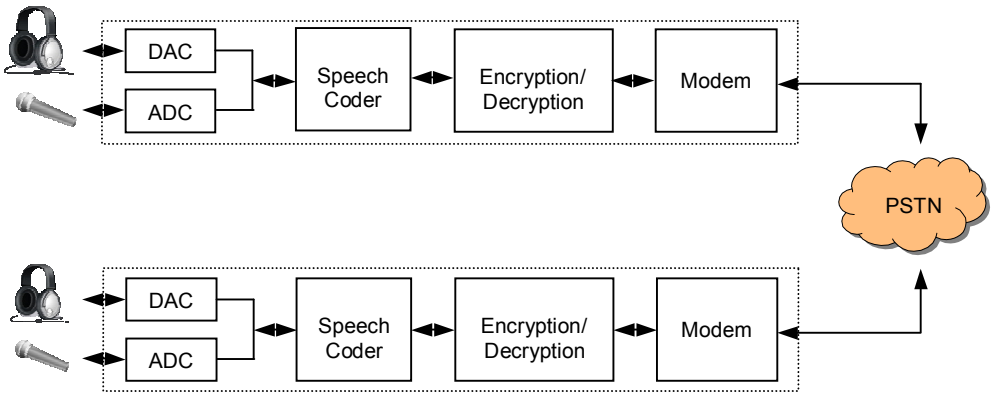
In this study, voice data is sent over phone line after ciphered and also an important data is embedded to voice data by steganography technique can be sent at the same time. By this way, security of communication can be high level. So it is almost impossible to Access secret data.

Paper organization is: related works are given in the second part. In the third part, developed security system and its implementation are described. In the last part, results of the study are given.

2. BASIC OF SECURE PHONE SYSTEMS

At the present time, there are a few techniques using for speech communication as Public Switch Telephone Network (PSTN), Integrated Services Digital Network (ISDN) and Asymmetric Digital Subscriber Line (ADSL). Communication lines using ISDN and ADSL techniques also can perform data communications by speech communication. PSTN, which creates the basis of used telephone lines today, is a communication technique that has been improved to use for speech communication. Since the purpose of this technique is only speech communication, voice quality is

not very important. Although Human Earing System (HES) is sensitive for voices between 20 and 20000 Hz, bandwidth of PSTN between 300-3500 Hz is enough for a comprehensible communication. In secure phone applications, dial-up modems which are working on this channel and were used for internet connection in the past have been used for data transfer. Here, after analogue speech information had been converted to digital information, it has been encrypted and sent by modem.



Figue 1. General block diagram of secure communication system

Block diagram representing secure communication generally is shown in Figure 1. For speech signals can be encrypted, they need to be digital. The ADC unit in the block diagram is used for converting analogue signal coming from microphone to digital for the encryption can be done. In speech encoder unit compression process is performed for the speech signal converted to digital information can be encrypted more quickly. Since the bandwidth of communication line is limited, this process has been also provided advantages sending data. After compressed speech data are encrypted with selected encryption algorithm, they have been sent over phone line by a dial-up modem working full duplex. In the receiver unit reverse of these processes are performed.

In subsections speech coder, encryption and modem units which create secure phone system will be explained briefly.

2.1 Speech Coder Block

Selection of cabled telephone lines for secure communication has been brought along some limitations also. Because the number of data can be sent over telephone line by modem in a certain time is limited, the compression of speech signal with speech coder is purposed. The works in literate Code-Excited Linear Prediction (CELP) coder had been mostly used as speech coder. Since decreasing number of used samples with speech coding saves extra time for encryption algorithm, this allows the use of more powerful encryption algorithm.

CELP coder had been used as speech coder in the work performed by L. Diez-del-Rio and the others [3]. These researchers had performed 9600 bps and 4800 bps coding according to voice quality. In the other work J. Calpe and the others had used two different CELP speech coders as 9600 bps and 7200 bps [2]. Anas and the others had used a 4800bps rate speech coder which was termed ICELP by them in their work [1].

2.2 Encryption block

Encryption block is the most important part of the system. Durability of the used encryption algorithm is the most significant fact which determines the system reliability. In the work performed by L. Diez-del-Rio and the others, an asymmetric encryption based technique named Tiche had been used to encrypt communication information [3]. In microcontroller systems with low memory capacity and process power, It cannot be expected that asymmetric encryption, which needs high process power, works with full performance. A type of RSA algorithm had been used in the work of J. Calpe and teh others [2]. Anas and the others had been used DES algorithm as encryption algorithm [1]. DES is appropriate for low power process microcontroller systems; its security of encryption is not enough, though.

2.3 Modem

In applications of secure phone, modem is used for transfer of encrypted speech data on cabled communication line over PSTN. Running on rate of 9600 bps and full duplex modem with CCITT V32 standard had been used in works performed by Luiz Diez-del-Rio, Javier Calpe, Anas.

3. DESCRIPTION OF THE PROPOSED SYSTEM

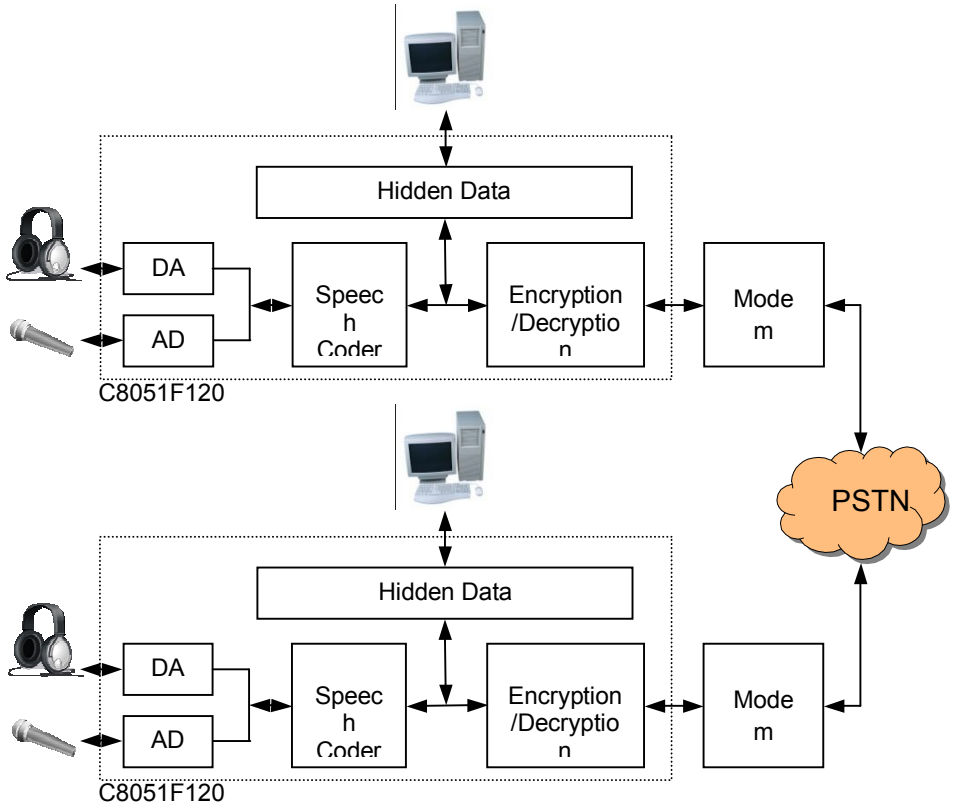


Figure 2. Block diagram of the designed secure communication system

The block diagram of the proposed system presented in the paper is as shown in Figure 2. Designed system includes hidden data embedding (stenography) unit which is different from present secure phone systems. Therefore, even though encrypted voice communication might be subjected to an attack, it would not be discerned as it is send by stenographical method. Although attackers might capture the voice communication they wouldn't reach the actual hidden information. Another contribution of the designed system is that it uses recently developed an encryption algorithm called Scalable Encryption Algorithm (SEA).

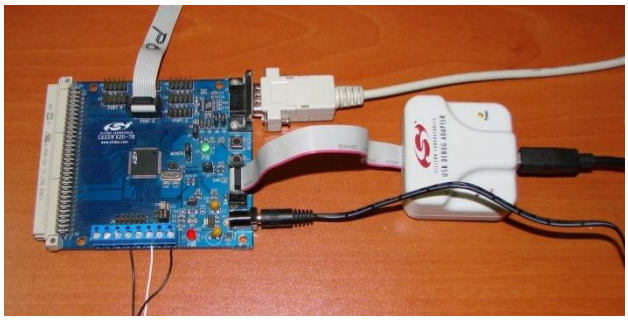


Figure 3. C8051F120DK development board

For the implementation of the designed system, C8051F120DK development board produced by SILABS is utilized. The microcontroller on the board has 100 Mips of computing power. Microcontroller includes the units of ADC and DAC having 12 bit resolution. Apart from modem, all other blocks are implemented on this development board. Speech coder, data embedding and encryption algorithms were written using C language for C8051F120 microcontroller.

3.1 Encryption block

SEA is an encryption algorithm developed in 2006 by François-Xavier Standaert and etc. for embedded systems having restricted resources

such as memory size and computing power [6-8]. SEA's design criteria's depending on symmetric block encryption approximation are small memory utilization, small code size and limited instruction set. For these reasons, only bit operations like Exclusive OR, bit/word rotations, mod 2b sum and s-box are used. Having quite flexible structure, SEA is expressed by SEA(n,b) and it can work on different text, key/word lengths.

In addition, SEA relaying on Fiestel structure with variable rotation count is described by the following parameters:

- n: raw text and key size
- b: word
- $n_b = n/2b$: the number of words per Feistel branch
- n_r: the number of encryption tour

In the realization of SEA algorithm, the parameters of n and b are selected according to target processor's features. On the other hand key and raw text size should be multiples of 6, like; 48, 96, …, 192 bit. Another important points for providing a effectual safety level are that word length should be $b \geq 8$ and rotation count should be at least $n_r = 3n/4+2(n_b + [\ b/2])$ [6-8]. In addition to being up to date and having powerful structure against attacks, one of the most important reasons why SEA algorithm was utilized in this study is that it is designed for embedded systems having limited resources such as memory size and computing power. SEA which has a considerable flexible structure can be used easily with microcontrollers working with simple logical and arithmetic instructions. In addition, previous studies show that SEA encryption algorithm wasn't utilized in the secure voice communication applications before. Figure 4 shows the structure of SEA algorithm.

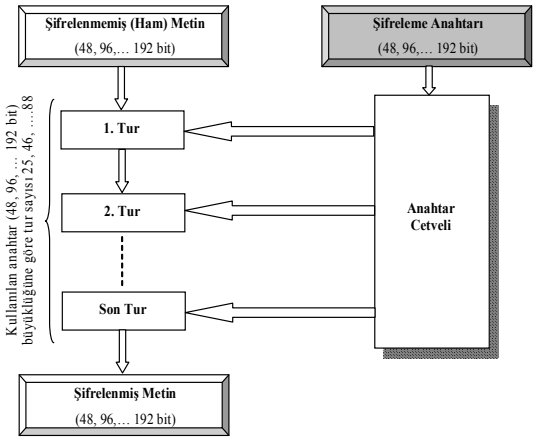


Figure 4. Scalable encryption algorithm (SEA)[8].

3.2 Hidden Data embedding block

The function of data embedding block is to send a secret data embedded in the voice signal to the target. In order to realize this function, hidden data coming from computer is added to voice signal by changing the bits that do not disturb the voice data obtained from the output of speech coder. Because the main goal of stenography is to prevent attackers from perceiving the hidden information, embedded voice signal wouldn't be discerned by unauthorized persons. Therefore an additional safety level which wasn't used in the previous studies is added to system. In order for attackers to reach the hidden data, it is necessary for them to apply steganalysis methods to signal obtained by decoding encrypted voice information.

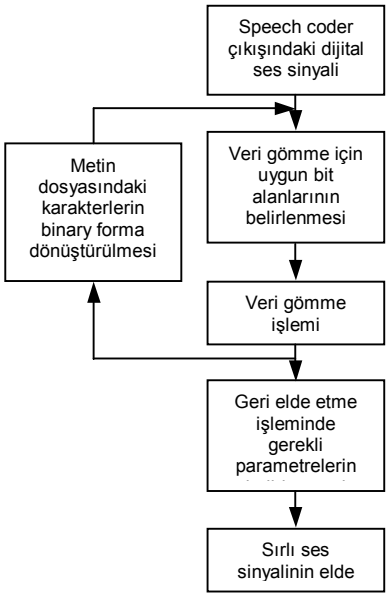


Figure 5. Flow diagram of data embedding algorithm

4. CONCLUSION

In this paper, we implemented secure communication over wired phone link. The proposed system provides two advantages compared to other systems in literature. Firstly, it use a new encryption algorithm namely Scalable Encryption Algorithm. Secondly, the implemented system presents hidden file transferring with voice stenography technique. DES and RSA encryption algorithms used in existing works have a several disadvantages. Although DES algorithm is fast algorithm, it has lost reliability nowadays. However, RSA algorithm that is asymmetric encryption algorithm is not suitable for systems based on microcontroller due to requirement high processing load. SEA is designed for microcontroller systems. Also, it presents high fast and security. In addition to voice encryption for secure communication, we presented hidden file transfer application in this work. Hidden file transferring is realized embedding file within voice data using stenography methods. Attackers will spend to solve encrypted

communication during attacking time. Even if the encryption communication is solved, this solution will not be sufficient to obtain hidden file. Consequently, employing of the implemented system will be provided high security in wired communication links.

REFERENCES

[1] Anas N.M.,Rahman Z., Shafii A.,Rahman M.N.A.,Amin Z.A.M., "Secure Speech Communication over Public Switched Telephone Network", Asia-Pacific Conference on Applied Electromagnetics Procedings, pp. 336-339, MALAYSIA, 2005.

[2] Calpe, J.; Magdalena, J.R.; Guerrero, J.F.;Frances, J.V., "Toll-quality digital secraphone" Electrotechnical Conference, 1996. MELECON '96, 8th Mediterranean pp. 1714 - 1717 Volume 3, 1996.

[3] Diez-Del-Rio, L.; Moreno-Perez, S.; Sarmiento, R.; Parera, J.; Veiga-Perez, M.; Garcia-Gomez, R., "Secure speech and data communication over the public switching telephone network", Acoustics, Speech, and Signal Processing, 1994. ICASSP-94., 1994 IEEE International Conference on Volume II, pp. 425-428, 1994.

[4] Uma Devi.G, "Steganography-Survey on File Systems", Research – CSE I I I T Hyderabad, 2006.

[5] Christian Cachin, "Digital Steganography", IBM Research Zurich Research Laboratory, Rüschlikon, Switzerland, 2005.

[6] Standaert, F. -X., Piret, G., Gershenfeld, N., Quisquater, J.-J., "SEA: A Scalable Encryption Algorithm for Small Embedded Applications", Lecture Notes in Computer Science, Vol. 3928, April 2006, pp. 222-236.

[7] Macé, F., Standaert, F.-X., Quisquater, J.-J., "FPGA Implementation(s) of a Scalable Encryption Algorithm", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 16, No.2, Nov. 2007, pp. 212 – 216.

[8] Çakıroğlu M., Bayılmış C., "SEA Şifreleme Algoritması Kullanarak Güvenli Kablosuz Algılayıcı Ağ Haberleşmesinin Gerçekleştirilmesi", 3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı", 173-177, 25-27 Aralık 2008.

[9] Chowdhury D.D., "Unified IP Internet-Working", ISBN 3-540-67370-9, Springer-Verlag, Germany, 2001.

[10] Valin M.J., Lefebure R., "Bandwidth Extension Of Narrowband Speech For Low Bit-Rate Wıdeband Coding", pp. 130-132, Speech Coding Conf., 2000.

[11] Ahmadian Z., Salimi S., Salahi A., "Security enhancements against UMTS–GSM interworking attacks" pp. 2256–2270 Computer Networks 54 (2010).