Synchronization System for Crypto Initialization over GSM Voice Channel

WIRA FIRDAUS HJ YAAKOB
Microelectronics Dept
MIMOS Berhad
Technology Park Malaysia, 57000 Kuala Lumpur
MALAYSIA
wira@mimos.my http://www.mimos.my

Abstract: - Nowadays, GSM voice channel network is the most consumed by mobile communication users in the world [1]. However, the GSM voice channel network is currently vulnerable to hardware-based attacks and easy to be intercepted [2]. Current end-to-end secure communication solutions over the GSM voice channel network have a big challenge on how to get an efficient synchronization of cryptographic devices on both ends. The efficient synchronization method helps to recover fully the original voice after decryption with very minimize delay and distortion. This paper presents an enhanced synchronization system for the synchronization improvement by manipulating the Pulse Code Modulation (PCM) coded voice from/to the cryptographic devices at both ends. The system is developed for simple, low-cost and consumable by various segments of society such as public, banking, military and government.

Key-Words: - GSM voice channel network, Bluetooth, PCM, Synchronization, Stream Cipher Sequence, ciphertext, FPGA

1 Introduction

This paper presents an enhanced system on how to synchronize between transmitting and receiving crypto device for initialization using a voice channel of the transmission system. The importance of the synchronization is to ensure the receiving crypto device can decrypt back the encrypted PCM speech from the transmitter. The lack of the synchronization will make the encrypted speech signal to be unsuccessfully decrypted and results of failure having back the original voice [3]. Figure 1 shows the overall picture of the GSM voice channel encryption-decryption system. The encryption-decryption systems reside inside the Bluetooth headsets.

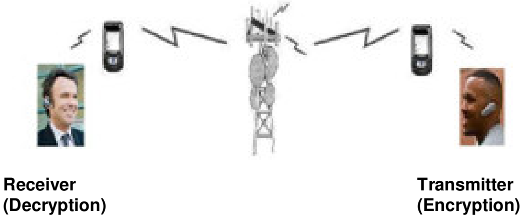


Fig. 1. The overall view of the GSM voice channel encryption decryption system presented in this paper

The present system can be applied to any wireless telephony applications such as mobile phones, PDAs, smart phones, military communications, pc to pc communication that are using GSM voice channel communication. The current solution for GSM encryption that is available in the market at the moment is mainly through the GSM data channel. However, the GSM data channel suffers from a number of disadvantages like interoperability problems and delay which exceeds the ITU-T specifications for one-way transmission times of 150ms for telephony services [4]. In addition, a user needs to pay extra for subscribing the data channel service from the service provider first like Celcom, Digi and Maxis (in Malaysia). Some Telco company does not provide the service.

2 Synchronization Methodology

The problem that is to be solved is the issue on how to start doing decryption in order to avoid unsuccessful decryption of the transmitted plaintext. The synchronization system that is presented in this paper helps to generate the stream cipher sequences at the receiver to be in the same sequence with the stream cipher sequences at the transmitter.

The other problems are the delay and some process that are introduced in the GSM voice channel make more difficult for the receiver to initialize the stream cipher sequences. In order to solve this problem, the transmitter is designed to transmit a few cycles of 32-bit digital zeros before transmitting the encrypted PCM data. At the receiver, the 32-bit digital zeros data is converted as positive full-scale PCM code. The magnitude bits for the positive full-scale PCM code is LOW for the sign bit that is the MSB (most significant bit) and HIGH for the remainder 12 bits. A delay module is also introduced at the transmitter in order to give some delay before the encrypted plaintext is propagated. The term for encrypted plaintext in this paper later on is called as ciphertext.

The overall diagram for the developed system in this project is shown in Figure 2. The PCB design of the developed system is shown in Figure 3. At the transmitter, before the plaintext is being transmitted, the synchronizer will generate 32-bit digital zeros for less than one second in order to ensure the receiver to be ready for initialization.

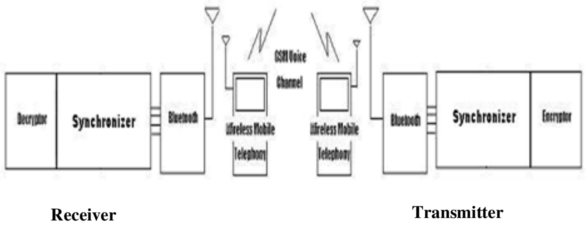


Fig. 2. Overview of The Developed Synchronization System [7]

Then the stream cipher sequence at the transmitter is generated once the plaintext is ready to be encrypted. Figure 4 shows a symmetrical encryption-decryption system on the basis of the mod2 operation, a cipher generating the random crypto sequence and sychronization being performed on the basis of the initial status of the cipher.

However, due to some delay and distortion from the GSM transcoding process in GSM voice channel communication [5], the ciphertext which is transmitted from the transmitter will not be synchronized with the ciphertext which is arrived at the receiver. Therefore, the symmetrical encryption-decryption system cannot be used straight away in the GSM voice channel encryption system since it has synchronization issue in GSM channel. The synchronization problem will affect whether the receiver can get back the original data or not.

At the receiver, some repetitive cycles of positive full-scale PCM code is received for less than one second when digital zeros are propagated from the transmitter. The delay module at the transmitter will give some delay for less than one second to give enough time for propagating the digital zeros before sending the ciphertext data. The purpose for sending the digital zeros is to give enough time for the receiver to be ready for receiving the ciphertext. Then, the stream cipher generator of the synchronizer at the transmitter starts to generate its stream cipher sequences. The ciphertext is propagated using the Bluetooth wireless communication to a wireless mobile telephony before it is sent through the wireless GSM voice channel communication [7].

Once the initializer module at the receiver detects the ciphertext, it will send a signal that will activate the stream cipher sequence generator to generate the stream cipher sequences.

Fig. 3. PCB Design of the System

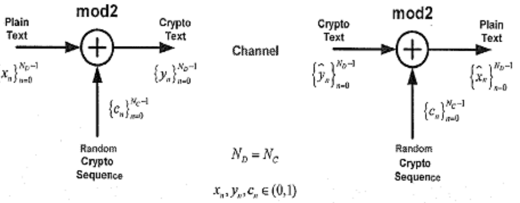


Fig. 4. A Symmetrical Encryption-Decryption System [7]

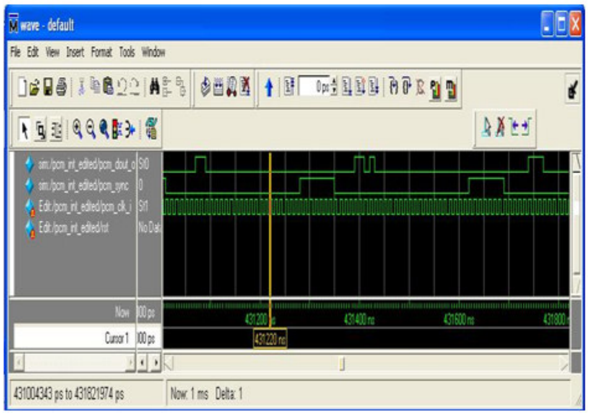
Then, the ciphertext is decrypted using the generated receiver's stream cipher sequences.

3 Simulation and FPGA Results

The functional testing was done in two parts; firstly in RTL Simulation using ModelSim™ and secondly in FPGA Implementation on Xilinx™. For the FPGA Implementation, the testing was done in a real environment through GSM voice channel and Bluetooth communication. The plaintext that was encrypted in the FPGA at the transmitter was propagated as Bluetooth signal to a mobile phone and then was transmitted through GSM voice channel to the other mobile phone at the receiver. The receiver's mobile phone transmitted the ciphertext to the receiver FPGA using Bluetooth communication. The stream cipher sequences that were generated in both FPGA at transmitter and receiver were taken out to their I/O pins and were probed to the DPO. The complete setup is shown in Figure 3. The probed results were viewed as shown in Figure 7 and 8.

3.1 Simulation Result

The simulation of the system has been done using ModelSim™. Figure 5 shows only the simulation result of the encryption's synchronization part.



sim:/pcm_int_edited/pcm_dout_o St0
sim:/pcm_int_edited/pcm_sync 0
Edit:/pcm_int_edited/pcm_clk_i St1
Edit:/pcm_int_edited/rst No Data
Now 100 ps
Cursor 1 100 ps
431004343 ps to 431821974 ps
Now: 1 ms Delta: 1

Fig. 5. Simulation Result of the Transmitter Using ModelSim™

The waveform shows that at every 8 kHz, the PCM synchronization flag was enabled. The PCM synchronization in the figure is named as *pcm_sync* while the signal *pcm_dout_o* represents the stream cipher sequences. The stream cipher sequence was generated and transmitted whenever the *pcm_sync* signal is activated. As shown in the figure as well, the stream cipher sequences kept changing at every sequence. The similar result was produced during FPGA implementation as captured from the DPO (Digital Phospor Oscilloscope) as shown in Figure 8. The PCM clock period that is indicated as pcm_clk in the figure was running at 256 kHz.

3.2 FPGA Result

The FPGA result of the stream cipher sequence generation at both transmitter and receiver are shown in Figure 6.

The result is achieved in the real time system through GSM voice channel and Bluetooth environment as shown in Figure 1. The waveform result is analyzed using Tektronix DPO4104 Digital Phosphor Oscilloscope.

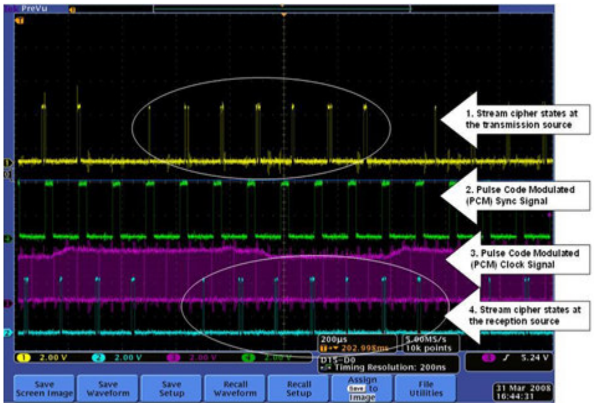


Fig. 6. FPGA Implementation Result of the Transmitter On Xilinx™ [7]

Both white ovals that surround the signals in the figure shows that the generated stream cipher sequences at the receiver are similar with the generated stream cipher sequences at the transmitter. Figure 7 shows the zoomed-in result of Figure 6.

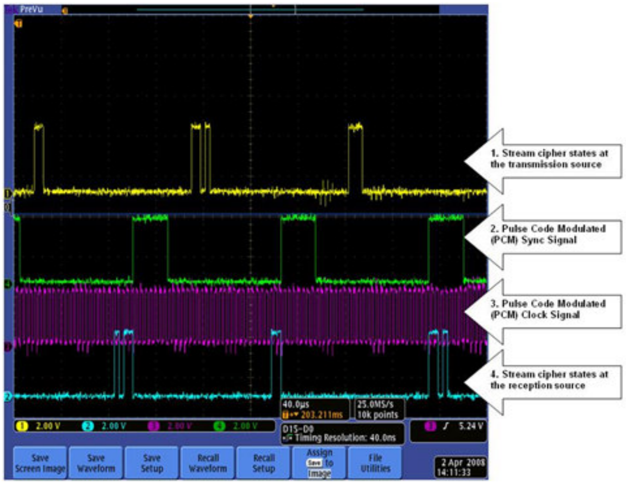

PreVu
1. Stream cipher states at the transmission source
2. Pulse Code Modulated (PCM) Sync Signal
3. Pulse Code Modulated (PCM) Clock Signal
4. Stream cipher states at the reception source
40.0µs
203.211ms
25.0MS/s
10k points
D15-D0
Timing Resolution: 40.0ns
1 2.00 V
2 2.00 V
3 2.00 V
4 2.00 V
5.24 V
Save Screen Image
Save Waveform
Save Setup
Recall Waveform
Recall Setup
Assign Save to Image
File Utilities
2 Apr 2008 14:11:33

Fig. 7. Zoomed-In FPGA Implementation Result of the Transmitter On Xilinx™ [7]

4 Conclusion

As we can see from Figure 6, the receiver generated the stream cipher sequences that were similar to the stream cipher sequences at the transmitter. The stream cipher sequences at the receiver could only be generated when once it was initialized. The generated stream cipher sequences then were used for decryption.

After the decryption, the original voice from the transmitter can be heard clearly. Therefore, the system proposed in this paper helps to get a perfect synchronization between transmitters and receivers.

Perfect synchronization between encryption and decryption is critical for decryption correctness and constitutes a vital challenge when communicating through noisy channels [6].

References:

[1] Rekha, A.B., Urnadevi, B., Solanke, Y.; Kolli, S.R., End-to-end security for GSM users [speech coding method], *IEE International Conference on Personal Wireless Communications*, Vol. X, No. X, 2005, pp. 434-437.

[2] Toorani, M., Beheshti Shirazi,A.A., Solutions to the GSM Security Weaknesses, *The Second International Conference on Next Generation Mobile Applications, Services and Technologies*, 2008, pp.576-581.

[3] N, Karugampala, S. Villeile, and A. M. Kondoz, Secure Voice over GSM and Other Low Bit Rate Systems, *IEE Secure GSM and Beyond: End to End Security for Mobile Communications,* 2003, pp. 3/1 – 3/4.

[4] N.N. Katugampala, K.T.Al-Naimi, S. Villette, A. Kondoz, Real time data transmission over GSM voice channel for secure voice and data applications, *IEE Secure Mobile Communications Forum: Exploring the Technical Challenges in Secure GSM and WLAN*, 2004, pp. 7/1 - 7/4.

[5] C. Lo and Y. Chen, Secure communication mechanisms for GSM networks, *IEEE Transactions on Consumer Electronics*, Vol. 45, No. 4, 1999, pp. 1074-1079.

[6]Zuquete, A., Barros, J., Physical-Layer Encryption with Stream Ciphers, *International Symposium on Information Theory*, vol. 2, 2008, pp.106-110.

[7]MIMOS Patent Pending (Wira Firdaus Hj Yaakob, Azhar bin Abu Talib, Ahmad Raif Mohamed Noor Beg, Raja Mohd Fuad Tengku Aziz); Synchroniation method for initialization of the crypto device for GSM Voice Channel Encryption, 2008.