Development of a Cryptographic Dongle for Secure Voice Encryption over GSM Voice Channel

Tae Yong Kim, Won-Tae Jang, Hoon-Jae Lee, Member, KIMICS

Abstract—A cryptographic dongle, which is capable of transmitting encrypted voice signals over the CDMA/GSM voice channel, was designed and implemented. The dongle used PIC microcontroller for signals processing including analog to digital conversion and digital to analog conversion, encryption and communicating with the smart phone. A smart phone was used to provide power to the dongle as well as passing the encrypted speech to the smart phone which then transmits the signal to the network. A number of tests were conducted to check the efficiency of the dongle, the firmware programming, the encryption algorithms, and the secret key management system, the interface between the smart phone and the dongle and the noise level.

Index Terms—Cryptographic dongle, PIC microcontroller, secure voice, CDMA, GSM, Smart Phone.

I. INTRODUCTION

GSM is the most widely used mobile communications system in the world. However the security of the GSM voice traffic is not guaranteed especially over the core network [1-3]. If encryption is enabled by the GSM operator, then the voice is only encrypted between the GSM mobile phone handsets and the base station, the rest of the communication is send in clear. To achieve maximum security especially from eavesdropping, it is highly desirable to have end-to-end secure communications [4]. In order to achieve end-to-end security, speech must be encrypted before it enters the GSM network.

Encrypting GSM voice communication is a real challenge. At the moment, encrypted GSM voice is send through the circuit switch data channel (CSD). However, this approach suffers from a number of disadvantages; the GSM network channel gives priority to voice instead of data. Theoretically, it takes longer time to establish a connection between the GSM handset and network when using the CSD channel.

The aim of this research and development is to transmit encrypted voice over the GSM voice channel. Sending encrypted voice over channel is a very challenging task [4]. It is thought that this approach is not a good approach and suffers from noise and synchronization problems. This research project will investigate such claims and would help providing some insights into how to solve the problems. To achieve this, a real-time prototype is designed, tested and implemented. A real network test is also conducted first in the CDMA network and then in the GSM network.

II. HARDWARE DEVELOPMENT

A. Design of a Secure Dongle

Development and cooperative research for secure dongle is to confirm the availability before production. So some constraints for secure dongle development have to be considered. Firstly secure dongle can be limited to communicator capable of transmitting and receiving a secure voice signal by using simple crypto algorithm. The crypto algorithm is applied to encrypt/decrypt a voice signal [5-7]. But voice signal from smart phone cannot be directly because voice channel should be protected from many mobile-phone venders. Hence the following constraint conditions are considered:

(a) Power consumption
(b) Power supply constraint
(c) Interface requirement
(d) Packaging
(e) Cost constraint
(f) Synchronizing problem for communicating between secure dongs
(g) Time delay and bit errors over CDMA/GSM mobile network
(h) An ability to transmit and receive secure voice signal
We describe some pictures in Figure 1, as the front of Dongle and connectors’ and switches’ names. In Figure 1, ‘Phone connector,’ specified by TTAS.KO-06.0028/R4 standard, is connector to interconnect with 20-pin connector in Smart-Phone [8]. ‘Ear-set connector,’ specified by PJ-204, is connector to interconnect with commonly-used ear-set. ‘Reset’ switch is used for power-on reset and “Synchronization Switch” is useful for cipher synchronization between the sender and the receiver.

**Fig. 1 Developed secure dongle.**

**Table 1 Electronic Specifications**

<table>
<thead>
<tr>
<th>PCB Size</th>
<th>56 x 29.5 (mm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro Controller</td>
<td>PIC18F2610</td>
</tr>
<tr>
<td>Power Driving</td>
<td>3.6V in/ 3V out (MIC5205)</td>
</tr>
<tr>
<td>ADC</td>
<td>10 bit ADC</td>
</tr>
<tr>
<td>DAC</td>
<td>DAC2512 (12bit)</td>
</tr>
<tr>
<td>Connector</td>
<td>TTAS.KO-06.0028/R4</td>
</tr>
<tr>
<td>Earset</td>
<td>PJ-204</td>
</tr>
<tr>
<td>Display</td>
<td>LED (power status)</td>
</tr>
<tr>
<td>Switch</td>
<td>SEND/END RESET</td>
</tr>
</tbody>
</table>

**B. Specification of a secure dongle**

There are requirements to perform the pilot project for a secure dongle; they have been summarized in Table 1. To reduce the size of a secure dongle, the microcontroller was chosen over the PIC series at the recommendation [9]. They both contain serial interfaces and a sufficient number of pins. This MPU consumes small power and support 10 bit ADC for converting analog to digital signal.

The size of double layered PCB (Printed Circuit Board) by using this device is 56 by 29.5 mm shown in Figure 1. The Table 1 summarizes the overall functionality of dongle PCB according to circuit design.

**III. TEST AND RESULTS**

**A. Local Loop-back in signal channel**

In order to confirm dongle which is working well, the ADC, DAC and the encryption functions were tested in one dongle.

The voice is first feed into the dongle through an earpiece microphone, and then the voice gets converted to a digital format using the DAC before it is encrypted. Once the encryption is performed, the signal gets decrypted and converted back to an analog format before it is passed to the speaker, as shown in Figure 2 and 3.

The results of this test are as the follows:
(a) The voice signal was send/received correctly.
(b) There was some noise associated with the voice.
(c) It is expected that the main reason for noise occurrence is amplifying both voice as well as noise.

**B. Communication test between two dongles**

In this test, the ADC, DAC and the encryption functions were tested in two identical dongles. The voice is first feed into the sending dongle through an earpiece microphone, and then the voice gets converted to a digital format using the DAC before it
is encrypted. Once the encryption is performed, the signal gets decrypted on the receiving dongle and converted back to an analog format before it is passed to the speaker. The Figure 4-5 illustrates the process of this test.

As a result, the voice signal was send/received correctly although the signal level is different slightly each other.

![Fig. 4 Signal flow diagram for testing two dongles.](image)

![Fig. 5 Communication test between two dongles.](image)

**C. Real network test**

In this test, the two dongles are tested in the CDMA network. The signal flow for testing two dongles which are attached to smart phone each other, as shown in Figure 6 and 7.

In this test, some noise occurred which made it difficult to hear the other party. Strangely, the noise level verifies from one keystreams to another keystreams. It is predicted that the noise level is low if the results of the eXORing of the plain signal with the keystreams is close to the original plain signal.

Therefore, some values of keystreams were selected in such a way that they generate low noise when encrypted with the plain signal. The reason behind this is to test the quality of the encrypted voice over the voice channel without having added extra overheads such as the use of synchronization pattern.

![Fig. 6 Signal flow diagram for testing two dongles attached to smart phone.](image)

![Fig. 7 Real network test in CDMA.](image)

**D. Key management using smart phone**

Voice Encryption Key management system is a system designed for T-Omnia smart phones that encrypt the voice through a dongle connected to it via the serial port. The system is used to send keys to dongle to be used in the encryption algorithm. The system is user friendly. Only authorized people can use this system.
IV. CONCLUSIONS

A cryptographic dongle was developed and tested for sending encrypted voice using the CDMA voice channel with the aim of testing this in the GSM channel. A cryptographic dongle with a simple encryption algorithm was used.

The dongle used PIC18F2610 (28-pins) microcontroller for signals processing including AD conversion and DA conversion, encryption and communicating with a smart phone.

A number of tests were conducted to check the performance of the dongle hardware, the firmware programming, the encryption algorithms, the VEKMS (Voice Encryption Key Management System), the interface between the smart phone and the dongle and the noise level.

In the future, further investigation and improvement is needed to transmit a secure voice over GSM/CDMA network voice channel.

ACKNOWLEDGMENT

This work was supported in part by the Dongseo Frontier 2009 and the research fund of Dongseo University in 2009.

REFERENCES


Tae Yong Kim was born in Korea, on November 14, 1965. He received a Ph.D. at Okayama University, Graduate School of Natural Science and Technology, in 2001 and is presently an assistant professor at Dongseo University, Korea. He was worked on analysis of antenna device, flow sensor system, numerical modelling, and simulation for various fields. Member of Institute of Control, Robotics and System and The Korea Institute of Maritime Information & Communication Sciences.

Won-Tae Jang received BS Degree in electronic engineering from SungKyunKwan University, Seoul, Korea in 1985, and received MS Degree in electronic engineering from University of Seoul, Korea in 1995. He is currently an assistant professor in the School of Computer and Information Engineering at Dongseo University. From 1989 to 2000, he was a research associate at the Korea Telecom International. His current research interests include developing mobile communication system, RFID system.

Hoon-Jae Lee received BS, MS, and PhD Degrees in electronic engineering from Kyungpook National University, Daegu, Korea in 1985, 1987, and 1998, respectively. He is currently an associate professor in the School of Computer and Information Engineering at Dongseo University. From 1987 to 1998, he was a research associate at the Agency for Defense Development (ADD). His current research interests include developing secure communication system, side-channel attack and USN/RFID security.