Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 5 pp. 2313-2318, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.5.2313

End-to-End Digital Secure Speech Communication over UHF and PSTN

Ki Hong Kim[1*]

[1]**The Attached Institute of ETRI**

UHF와 PSTN간 단대단 디지털 음성보안통신

김기홍[1*]

[1]한국전자통신연구원 부설연구소

Abstract With the widely applications of tactical radio networks, end-to-end secure speech communication in the heterogeneous network has become a very significant security issue. High-grade end-to-end speech security can be achieved using encryption algorithms at user ends. However, the use of encryption techniques results in a problem that encrypted speech data cannot be directly transmitted over heterogeneous tactical networks. That is, the decryption and re-encryption process must be fulfilled at the gateway between two different networks. In this paper, in order to solve this problem and to achieve optimal end-to-end speech security for heterogeneous tactical environments, we propose a novel mechanism for end-to-end secure speech transmission over ultra high frequency (UHF) and public switched telephone network (PSTN) and evaluate against the performance of conventional mechanism. Our proposed mechanism has advantages of no decryption and re-encryption at the gateway, no processing delay at the gateway, and good inter-operability over UHF and PSTN.

요 약 전술무선통신망의 급격한 증가로 이기종망간 단대단 음성보안통신은 매우 중요한 보안이슈가 되어왔다. 일반적으로 고비도의 단대단 음성보안통신은 사용자 통신단말에 고비도의 암호알고리즘을 적용함으로써 가능하나, 이는 이기종망간 암호화된 데이터를 직접 전송할 수 없는 문제점을 필수적으로 야기시킨다. 다시 말해, 서로 다른 전술통신망 사이에 위치하는 망연동 게이트웨이에서 암호화 데이터에 대한 복호화 및 재암호화와 같은 부가절차가 필연적으로 요구된다. 본 논문에서는 이기종 전술통신환경에서 게이트웨이에서의 복호화 및 재암호화에 따른 문제점을 해결하고, 최적의 단대단 음성보안체계를 수립하기 위해 UHF와 PSTN 통신망간 단대단 음성보안통신 메커니즘을 제안하고 기존 메커니즘 대비 제안 메커니즘의 성능을 비교, 분석한다. 제안된 메커니즘은 망연동 게이트웨이에서의 복호화 및 재암호화에 따른 부가지연이 전혀 없고, 이기종망간 우수한 연동특성을 가진다.

Key Words : Digital Secure Speech, Speech Coder, Modem, Gateway, UHF, PSTN, Inter-operability

1. Introduction

With the advent of tactical wireless communication technology, UHF radio communication has been the focus of much attention. UHF channel (300 ~ 3,000MHz) is of great importance to the military wireless communications. UHF has many advantages, related mostly to signal penetration, worldwide coverage, broadcast networks, and assured access [1]. High-grade narrow band digital speech security for UHF radio channel can be achieved using modern low rate speech coder and strong encryption algorithm.

For guaranteed end-to-end speech security over UHF and PSTN, however, the encrypted speech signal must be

*Corresponding Author : Ki Hong Kim
Tel: +82-42-870-2205 email: hong0612@ensec.re.kr
Received February 22, 2012 Revised (1st March 26, 2012, 2nd March 29, 2012) Accepted May 10, 2012

decrypted and re-encrypted at the gateway between UHF and PSTN before entering the other network system. Since each network has different communication security mechanism appropriate for its communication environment, it cannot guarantee a continuous and seamless end-to-end secure speech communication to each end user. Another problem caused by decryption and re-encryption is the fatal security vulnerability at the UHF-PSTN gateway. And thus, these result in severe disadvantages such as non-reliable transmission of digital encrypted speech data, security vulnerability, additional processing delay, and poor inter-operability.

There have been several previous related works regarding secure communication techniques and security issues for heterogeneous network topology such as global system for mobiles (GSM)-to-PSTN. The modulation scheme and prototype that enables the transmission of encrypted speech data over the GSM voice channel has been introduced in [2]. The work in [3] described the technique for secure communication over GSM as well as PSTN networks. In [4], encrypted speech transmission scheme using a modem based on linear predictive coding (LPC) on GSM was presented. The scheme using quadrature amplitude modulation (QAM) and orthogonal frequency division multiplexing (OFDM) modulation for secure communications over voice dedicated channels of GSM was proposed in [5].

There have also been several researches in the field of secure speech communication mechanisms for tactical wireless network and PSTN. The [6] presented the APCO Project 25 (P25) waveform for improving public security inter-operability between the civilian forces and the military forces over a radio channel, while the [7] presented the test results of an investigation of the performance and efficiency of the secure communications inter-operability protocol (SCIP) over tactical very high frequency (VHF)/UHF channels. The study in [8] analyzed the transmission and quality performance of digital secure voice over high frequency (HF) radio channel. The secure speech and data communication over PSTN was suggested in [9][10]. However, the most secure communication mechanisms are focused on efficient end-to-end secure speech transmission schemes over GSM and PSTN and digital signal processing techniques such as speech coding and modulation for tactical radio and PSTN security. No work was done in security communication mechanism for end-to-end digital secure speech transmission over UHF and PSTN heterogeneous network.

In this paper, a novel end-to-end digital secure speech communication mechanism over UHF and PSTN is presented and its transmission performance is analyzed for the first time. An experimental real-time test system for proposed end-to-end secure speech transmission mechanism using mixed excitation linear prediction (MELP) vocoder over UHF and PSTN is developed and its transmission performance, in terms of synthetic speech quality, transmission delay, and spectrum characteristics, is evaluated and analyzed. Using our enhanced mechanism, we were able to improve mean opinion score (MOS) over 0.85 ~ 1.04 compared with the conventional mechanism. Of particular note is that the proposed mechanism reduces end-to-end transmission delay by up to 50% compared with conventional mechanism over UHF and PSTN environment. This work differs from previous works in that it concentrates on one significant aspect of a tactical heterogeneous UHF secure speech communication environment, namely end-to-end transmission of encrypted digital speech over UHF and PSTN network. To our knowledge, this is the first proposal and comprehensive analysis of an end-to-end secure speech communication mechanism over UHF and PSTN. Our results can be used to design technique of efficient and reliable secure communication for a variety of other wireless tactical heterogeneous networks.

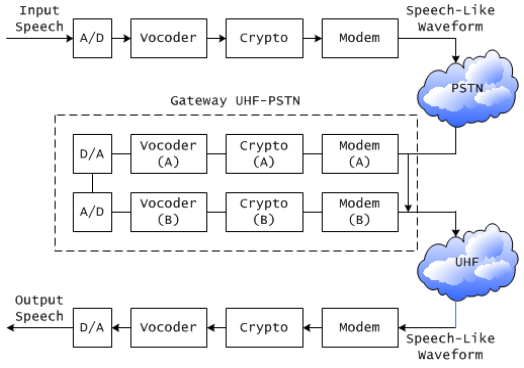
The remainder of this paper is organized as follows. In the next section, a brief description of the conventional end-to-end secure speech communication mechanism over UHF and PSTN is given. In section 3, the proposed secure speech communication mechanism is described. Some experimental results are presented in section 4, and concluding remark and future work is provided in section 5.

2. Conventional End-to-End Secure Speech Communication Mechanism

For the end-to-end digital secure speech communication, digital speech data should be encrypted at user ends. A

conventional mechanism for digital secure speech transmission over UHF and PSTN is illustrated in [Fig. 1]. In this conventional mechanism, end-to-end digital secure speech communication over UHF and PSTN is accomplished using UHF-PSTN gateway.

In PSTN transmitting, input speech signal is converted by analogue to digital (A/D) module to pulse code modulation (PCM) as input for PSTN speech encoder *A*. After analysis of each input speech data frame, fixed-length bits of coded speech parameters are transferred to the encryption module *A* suitable for PSTN environment and then to the PSTN modulation module *A*. After passing through the PSTN, it is received by the UHF-PSTN gateway. The demodulation module *A* in gateway demodulates the modulated encrypted speech data signal. After demodulation at the gateway, PSTN-suitable decryption *A* is performed and speech decoding *A* is carried out. The synthetic speech signal from the PSTN speech decoder in the gateway is also compressed using an UHF-suitable speech encoder *B* in order to accommodate in the available UHF radio channel. Then the output bitstream of UHF speech encoder is encrypted using the encryption module *B* appropriate for UHF radio environment, and then fed into UHF modem *B*. The UHF modem modulates the encrypted digital speech data into a form suitable for transmission over UHF wireless media. At the UHF receiver, the UHF modem *B* receives the speech signal from UHF radio link and demodulates it to an encrypted digital speech data, and feeds it to the decryption module *B* in turn. Then the encrypted digital speech data is decrypted and decoded by the UHF speech decoder *B* to reconstruct the output speech signal.



[Fig. 1] Conventional mechanism for end-to-end secure speech communication between UHF and PSTN

For the end-to-end secure speech communication over UHF and PSTN, the conventional mechanism has some disadvantages. First, it has inevitably security vulnerability at the UHF-PSTN gateway because the encrypted data must be decrypted and re-encrypted at the gateway before entering the other communication network. Second, it has additional larger processing delay for decryption and re-encryption at the gateway, and thus it results in poor real-time communication. Third, it has poor inter-operability. Since each network has different security mechanism as well as speech coder and modem appropriate for its communication characteristics such as data rate, bit error rate (BER), and delay, it cannot provide a continuous and reliable secure communication to each network user. In a world, the way of conventional transmission has very poor performances.

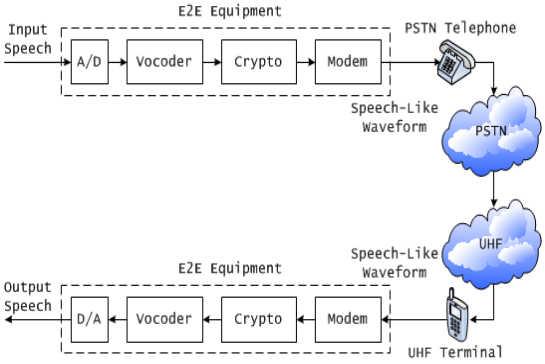
3. Proposed End-to-End Secure Speech Communication Mechanism

To overcome the problems inherent in conventional end-to-end secure communication over UHF and PSTN, we propose a new and efficient end-to-end transmission mechanism for digital encrypted speech data.

A block diagram of the proposed communication mechanism is shown in [Fig. 2]. The example shown is a typical PSTN terminal, e.g. PSTN telephone, to UHF radio terminal communication path. As shown in this figure, there are no additional processes in UHF-PSTN gateway, namely decryption and re-encryption and data format conversion suitable for transmitting in each network environment.

The input speech signal is first compressed using a very low bit rate speech encoder, e.g. 1.2/2.4kbps MELP, in order to accommodate in the available bandwidth. The output parameter bitstream of the speech encoder can be encrypted. The encrypted speech data is fed into the modem module, which converts it into a speech-like waveform to feed into the PSTN telephone handset. That is, the modem accurately converts the encrypted speech data into an unique analogue speech-like waveform, which possesses speech characteristics and transmits through speech channel with sufficient accuracy. The resulting analogue waveform is transmitted over the

communications channel, which includes a PSTN and an UHF radio link. On the other side, modem receives the transmitted signal from the handset port of UHF radio terminal. It also demodulates the transmitted speech-like waveform to extract the original transmitted data. Then the received encrypted speech data is decrypted and decoded by the speech decoder. The speech decoder at the receiver uses the decrypted speech bitstream to regenerate the synthetic speech output. For simplicity, only PSTN-to-UHF communication is illustrated, however, the reverse end-to-end secure speech communication is possible using the same mechanism.



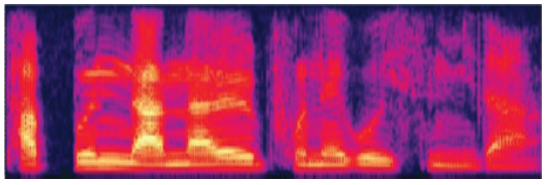
[Fig. 2] Proposed mechanism for end-to-end secure speech communication between UHF and PSTN

The proposed transmission mechanism has many advantages. First, there is no security vulnerability caused by the decryption and re-encryption at the UHF-PSTN gateway. Second, it has short processing delay. The end-to-end delay equals to the sum of the processing delays in the end-to-end (E2E) equipment connected to the PSTN telephone and the UHF radio terminal. This will be much lower than conventional transmission because of no extra processes in the UHF-PSTN gateway, such as modulation and demodulation, decryption and re-encryption, and speech encoding and decoding. Third, it has also good inter-operability. When the speech-like signal representing the encrypted speech data transmits from the transmitting E2E equipment to the receiving E2E equipment, it is taken as a general analogue speech signal by heterogeneous communication channel.

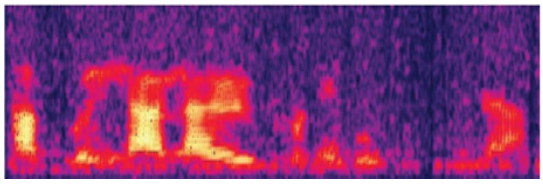
4. Experimental Results

In this paper, to prove the efficiency of the proposed mechanism, we compared and analyzed the perceptual evaluation of speech quality (PESQ) test [11], objective synthetic speech quality test, and the end-to-end transmission delay for end-to-end secure communication of our proposed mechanism with conventional mechanism. The performance of the proposed end-to-end secure speech communication mechanism has also been evaluated in terms of spectrum characteristics of output synthetic speech. In order to ensure consistency and accuracy of our experimental test results, we averaged each of the results over several iterations for each mechanism.

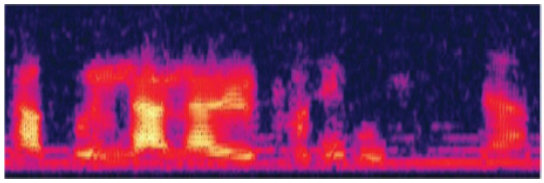
In the conventional mechanism as shown in [Fig. 1], we used a 2.4kbps advanced multi-band excitation (AMBE) speech coder [12] and existing 2.4kbps V.22bis modem [13] for PSTN environment, and 2.4kbps MELP speech coder and 8-PSK UHF modem using waveform defined in MIL-STD-188-110B [14] were used for UHF radio channel. In the PSTN security, we used advanced encryption standard (AES) [15], and in the UHF security, academy research institute agency (ARIA) [16] was used. For the proposed mechanism as shown in [Fig. 2], we developed a real-time experimental test system, which consists of 2.4kbps MELP speech coder, 4-QAM [5] for speech-like waveform design, and ARIA algorithm.



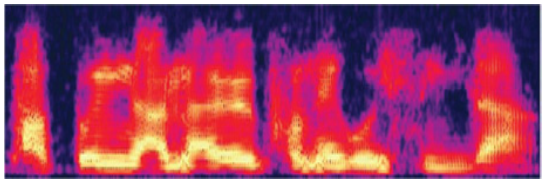
(a) Original speech signal



(b) Synthetic speech signal using conventional mechanism (UHF to PSTN)



(c) Synthetic speech signal using conventional mechanism (PSTN to UHF)



(d) Synthetic speech signal using proposed mechanism

[Fig. 3] Spectrum of original and synthetic speech signals according to mechanism

The spectrum of the original and synthetic speech signals according to end-to-end secure speech communication mechanism is illustrated in [Fig. 3]. In this figure, we can see that the spectrum of the synthetic speech signal using the proposed mechanism approximates even more accurately that of the original speech signal.

[Table 1] PESQ of the synthetic speech signal and end-to-end secure communication delay between UHF and PSTN

Mechanism		MOS	Delay(ms)
Conventional	UHF→PSTN	1.77	1273.89
	UHF←PSTN	1.96	1221.13
Proposed	UHF↔PSTN	2.81	586.44

Table 1 show the result of the objective speech quality test, the PESQ test, and the end-to-end transmission delay according to each mechanism for end-to-end secure speech communication over UHF and PSTN. In the transmission environment from UHF to PSTN, if the conventional mechanism is used, the MOS is only about 1.77. In the case of transmission mode from PSTN to UHF, the MOS is about 1.96. In the proposed mechanism, however, the MOS is even higher 2.81, providing that the synthetic speech quality from the proposed mechanism is better than that from the conventional mechanism. It is demonstrated that the proposed mechanism increases speech quality performance, namely MOS by about 60% when compared with the conventional mechanism. The main reason is because unlike the conventional mechanism, there is no degradation of synthetic speech quality caused by tandemming environment between UHF and PSTN.

In addition, when measuring the end-to-end communication delay, the delay in each mechanism is provided: 1273.89ms in transmission mode from UHF to PSTN using conventional mechanism, 1221.13ms in transmission mode from PSTN to UHF using conventional mechanism, and 586.44ms in the proposed mechanism. This means that the proposed mechanism reduces end-to-end transmission delay by more than 50% when compared with the conventional mechanism. The reason is that there are no additional procedures in the UHF-PSTN gateway for end-to-end secure speech communication between UHF and PSTN, namely modulation and demodulation, decryption and re-encryption, and speech encoding and decoding.

5. Conclusion and Future Work

This paper presented the novel communication mechanism for the end-to-end digital secure speech transmission over UHF and PSTN. An experimental test system was developed to inspect the proposed mechanism and to analyze the transmission performance. Test results showed that the proposed mechanism achieve better performance in terms of synthetic speech quality, transmission delay, and spectrum characteristics than conventional mechanism. Using our proposed mechanism, we manage to improve MOS over 0.85 ~ 1.04 compared with the conventional mechanism. Moreover, this mechanism is able to reduce the end-to-end transmission delay by up to 50% when compared with conventional mechanism.

This work is the first proposal and comprehensive analysis of the end-to-end secure speech communication over UHF and PSTN. Application of this secure communication mechanism provides the efficient and reliable end-to-end secure communication without any security vulnerabilities, additional processing delay, and poor inter-operability via the UHF-PSTN environment. This work can be significant first step toward designing

of inter-operable secure communication mechanism for tactical heterogeneous networks. It also can be extended to a variety of other tactical heterogeneous environment, including VHF, aeronautical mobile network, among others.

In the future, the authors will attempt to test a same test system in an actual on-air UHF network using the UHF radio terminal in order to investigate the transmission performance in an actual scenario. The plan is then to examine the effect that actual UHF radio channel environment has on the performance and efficiency of the end-to-end digital secure speech transmission.

References

[1] J. Ingerski and A. Sapp, "Mobile Tactical Communications, The Role of The UHF Follows-on Satellite Constellation and Its Successor, Mobile User Objective System," IEEE MILCOM '02, pp. 302-306, 2002.

[2] N. N. Katugampala, K. T. Al-Naimi, S. Villette, and A. M. Kondoz, "Real-Time End-to-End Secure Voice Communications over GSM Voice Channel," EURASIP EUSIPCO '05, 2005.

[3] S. Islam, F. Ajmal, S. Ali, J. Zahid, and A. Rashdi, "Secure End-to-End Communication over GSM and PSTN Networks," IEEE IET '09, pp. 323-326, 2009.

[4] Y. Yang, S. Feng, W. Ye, and X. Ji, "A Transmission Scheme for Encrypted Speech over GSM Network," IEEE ISCSCT '08, pp. 805-808, 2008.

[5] T. Chmayssani, G. Baudoin, and G. Hendryckx, "Secure Communications through Speech Dedicated Channels Using Digital Modulations," IEEE ICCST '08, pp. 312-317, 2008.

[6] P. Kiley and T. Benedett, "Public Safety Interoperability with an SCA Military Radio Using the P25 Waveform," IEEE MILCOM '07, pp. 1-8, 2007.

[7] J. M. Alvermann and M. T. Kurdziel, "The Secure Communication Interoperability Protocol (SCIP) over a VHF/UHF Radio Channel," IEEE SSST '10, pp. 1-6, 2008.

[8] K. Kim and J. Hong, "Evaluation of Transmission and Quality Performance of Digital Secure Voice Communications in an HF Network," IEEE ICDT '09, pp. 20-25, 2009.

[9] N. M. Anas, Z. Rahman, A. Shafii, M. N. A. Rahman, and Z. A. M. Amin, "Secure Speech Communications over Public Switched Telephone Network," IEEE Asia-Pacific Conference on Applied Electromagnetics '05, pp. 336-339, 2005.

[10] T. Chmayssani and G. Baudoin, "Data Transmission over Voice Dedicated Channels Using Digital Modulations," IEEE RADIOELEK '08, pp. 1-4, 2008.

[11] ITU-T Recommendation P. 862, 2002.

[12] http://www.dvsinc.com/index.htm

[13] ITU-T Recommendation V. 22 bis, 1993.

[14] US DoD, "MIL-STD-188-110B, Military Standard - Interoperability and Performance Standards for Data Modems," 2000.

[15] FIPS PUBS 197, 2001.

[16] IETF RFC 5794, 2010.

Ki Hong Kim [Regular Member]

- Feb. 1998 : Kyungpook National University, B.S.
- Feb. 2000 : Kyungpook National University, M.S.
- Aug. 2007 : Korea University, Ph.D.
- Dec. 1999 ~ Sept. 2000 : LG Electronics, Engineer
- Sept. 2000 ~ Current : The Attached Institute of ETRI, Senior Engineer

<Research Interests>
Communication Security, Physical-Layer Security, Signal Processing