고정 타임슬롯 모드를 사용하는 PCM 시스템에서 디지털 음성 데이터 보안 기법

임성렬
충남대학교 전기정보통신공학부

e-mail : syim@cnu.ac.kr

Cipher method of digital voice data using fixed time slot mode in PCM system

Im Sung Yeal
Division of Electrical and Computer Engineering, Chungnam National University

요 약

본 논문은 연속된 음성 신호를 전송로 상에 전송하기 위해 음성 신호를 G.711 표준 권고인 PCM 으로 다중화한 후 고정 타임슬롯을 배정하여 전송하는 시스템에서 PCM 화된 디지털 음성 데이터를 실시간으로 암호화하여 전송하는 스트림 암호화 기법에 관한 것이다. 실시간으로 처리되는 음성 데이터의 암호화 시에는 하드웨어 방식이 적합한 데, 본 논문에서는 고정 타임슬롯을 배정받는 음성 데이터의 실시간 암호화 기법에 관한 것이다. 일반적으로 아날로그 음성 신호 코딩 시에 국내에서는 북미 방식인 μ-law 코딩 기법을 적용하는 데 이는 표본화한 음성 데이터를 양자화전에 압축하고 복호화 후 신장하는 비선형 양자화 기법을 적용하는 것으로 표본화된 값을 8 비트의 PCM 데이터로 변화하여 E1(2.048Mbps) 급 속도로 전송한다. 본 논문에서는 PCM 전송로 상에 전송되기 전의 직렬 입력 데이터를 암호화 장치를 거쳐 해당 타임슬롯에 해당하는 8 비트의 데이터를 실시간으로 암호화하여 전송로 상으로 전송하고 역으로 수신 단에서는 PCM 전송로를 거친 직렬 입력 데이터를 암호화된 타임슬롯을 판별하여 해당 타임슬롯의 데이터를 복호화하여 원래 데이터를 복원한다. 본 논문에서는 고정 타임슬롯을 배정받은 PCM 데이터를 암호화하여 전송한 후 수신 단에서 복호화 과정을 거친 후 타임슬롯 단위로 데이터 암호화/복호화가 가능함을 보여준다.

1. 서론

유선망을 이용한 음성 신호 전송시에 1972 년 ITU-T 의 권고 G. 711 에 근거한 64 Kbps PCM (Pulse Code Modulation)기술을 이용한 음성부호화 방식을 사용하며, 이는 파형 부호화 방식의 하나로, 아날로그 음성 신호를 표본화, 양자화, 부호화하여 디지털로 전송하고, 수신 측에서 복호화 함으로써 아날로그 음성 신호를 재생하는 방식이다.[1] 양자화 시에 양자화 잡음을 줄이기 위해 양자화 전에 압축하고, 복호화 후 신장하는 비선형 압축신장 기법을 사용하며 북미 μ-Law 방식과 유럽 A-Law 방식이 있으며 국내에서는 북미 방식인 μ-Law 방식을 사용한다.[2]

음성 데이터 같은 경우는 불법 침입자가 망에 접근하여 데이터를 취득하면 해석이 용이하므로 이에 대한 대비로 데이터를 암호화하여 전송하면 망에 접근하여 정보를 취득하더라도 해석이 불가능하게 함으로써 정보의 유출로 인한 피해를 줄일 수가 있다.

암호화 방식에는 블록 암호와 스트림 암호화 방식이 있다. 블록 암호는 평문을 블록 단위로 동일한 크기의 암호문 블록으로 암호화하는 방식이며 일반적으로 64 비트나 128 비트 크기의 블록을 사용한다. 스트림 암호화 방식은 암호화 키와 이진 데이터 스트림을 비트 단위나 바이트 단위로 직접 연산하는 방식이다. 말하자면 메시지 M 을 연속적인 몇 개의 문자나 수 비트 단위인 $m_1, m_2 \cdots$의 동일한 크기로 나누어서 각각의 m_i 를 키스트림 $K=k_1k_2\cdots$의 i 번째 키 k_i 로 암호화하는 방식이다. 스트림 암호화 방식에서는 동기식 스트림 암호화 방식과 자기 동기식 스트림 암호화 방식이 있다.[3]

동기식 스트림 암호화 방식에서는 키 스트림이 암호화할 평문 스트림과는 무관하게 생성된다. 이는 암호화문이 전송 중에 손상되거나 분실되었을 때 다음 작업을 위해 송신 측과 수신 측에서 키 발생기를 다시 동기시켜야 함을 의미한다.[4]

자기 동기식 스트림 암호화 방식에서는 앞서 입력된 n 개의 암호화문 데이터 스트림으로부터 키 생성 알고리즘을 거쳐 각각의 암호화 키 문자를 만든다. 이 방식에서는 전송 중에 분실되거나 변형된 1 개의 암호화 문자가 이보다 앞서 전송된 n 개의 문자에 에

러를 파급한다. 하지만 이 다음에 입력되는 n 개의 정확한 데이터에 의해 다시 동기를 복구하게 된다. 또한 각각의 키 문자가 앞서 입력된 전체 메시지 스트림에 함수적으로 연관되어 있으므로 암호화문은 비주기적이다.

디지털 음성 데이터 전송에서는 데이터를 TDM 망의 전송로 상에 타임슬롯 단위로 전송함으로 타임슬롯 상의 데이터가 손상되면 연속적인 데이터 스트림으로부터 키를 추출하는 자기 동기식 암호화 방식에서는 다시 동기를 맞추기가 어렵다. 이러한 형태의 데이터 스트림의 암호화에는 동기식 암호화 방식이 적합하다. 동기식 암호화 방식은 LFSR(Linear Feedback Shift Register) 방식과 계수기(Counter) 방식으로 분류된다.[5] 스트림 암호화 방식의 이점은 변환 속도가 빠르다는 것에 있다.

(그림 1) 동기식 스트림 암호화 방식

키 생성 알고리즘은 약정되어 있어 수신 측에서 복호화 시에도 키의 재생성이 가능하다. 키 발생기의 초기 상태는 초기값 IV 로 초기화된다. 키 발생 스트림은 송신 측 암호화 키 생성 알고리즘과 수신 측 복호화 키 생성 알고리즘이 동일해야 한다. (그림 1)에서 XOR 알고리즘을 이용한 간략한 암호화/복호화 과정을 보여주고 있다.

$$C_i = E_{ki}(m_i) = m_i \oplus k_i$$

여기서 m_i, k_i 와 C_i 의 단위는 1 비트나 1 바이트이다. 복호화 과정은 다음과 같다.

$$\begin{aligned} D_{ki}(m_i) &= C_i \oplus k_i \\ &= (m_i \oplus k_i) \oplus k_i \\ &= m_i \end{aligned}$$

동기식 암호화 방식에서는 1 비트나 1 바이트의 전송 에러가 연속된 다른 비트나 바이트에 영향을 미치지 않는다. 이 방식은 에러가 전파되지 않는다는 면에서 이점을 지닌다. 이제 동기식 암호화 방식인 LFSR 방식과 계수기 방식에 대해 살펴본다.

1.1 LFSR

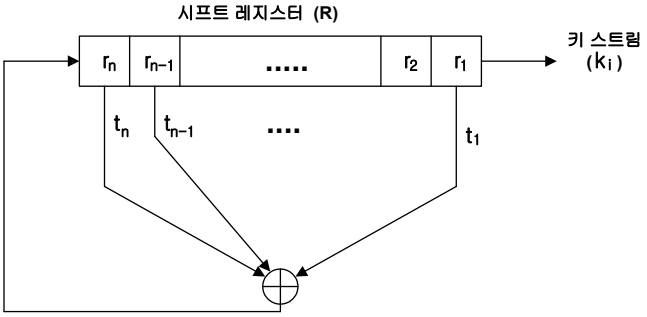
n 단의 LFSR 은 n 개의 시프트 레지스터 $R=(r_n, r_{n-1},\ldots, r_1)$ 과 n 개의 탭 시퀀스 $T=(t_n,t_{n-1},\ldots,t_1)$ 로 구성되어 있다. 여기서 r_1 와 t_1 는 1 비트의 2 진수이다. 각 단계마다 비트 r_1 이 키 스트림에 더해지고 비트 r_n ..... r_2 가 오른쪽으로 시프트 되며 T 와 R 조합으로부터 생성된 새로운 비트가 레지스터의 왼쪽 끝으로 입력된다. R 의 다음 상태인 R′은 다음 식 (1)과 같이 계산된다.

$$R' = HR \bmod 2 \qquad (1)$$

여기서 H 는 n x n 행렬이다.

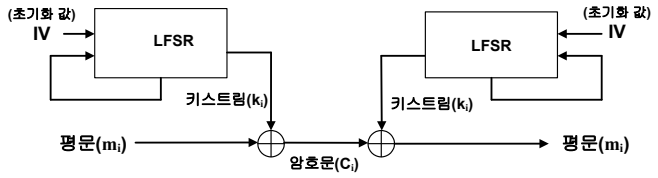
$$H = \begin{bmatrix} t_n & t_{n-1} & \ldots & t_2 & t_1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & & 0 \\ . & & & & \\ . & & & & \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

n 단의 LFSR 은 주기가 2^n-1 인 키 스트림(k_i)으로 사용되는 유사 무작위 비트 스트림을 생성한다. 이를 (그림 2)에 보여주고 있다.



(그림 2) LFSR

이진 평문 $M=m_1m_2\ldots\ldots$은 식 $C_i=m_i \oplus k_i$ 에 준해 암호화된다. (그림 3) 에서 보듯이 평문(m_i)을 LFSR 로 생성된 키 스트림(k_i)과 XOR 연산하여 전송하며 수신 단에서는 동기화된 키 스트림(k_i)과 암호문(C_i)를 XOR 연산하여 평문을 복구한다.

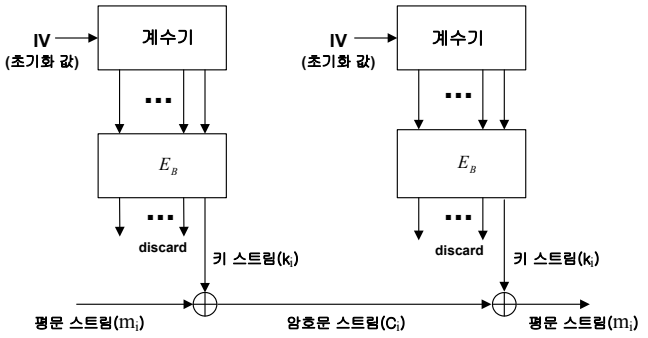


(그림 3) LFSR 을 이용한 암호화 방식

1.2 계수기 방식

계수기 방식에서는 연속적인 입력 블록들이 간단한 계수기로 생성된다. 계수기 방식을 적용하면 i 번째 키 k_i 를 초기의 i-1 번째 키 문자를 생성하지 않고도 만들 수 있다. 계수기 방식은 하드웨어나 소프트웨어적인 구현이 용이하며 구조가 ECB 나 CBC 방식에 비해 단순하다.[6] 계수기 방식을 이용한 동기식 스트림 암호화 방식을 (그림 4)에 보

여주고 있다.[7]

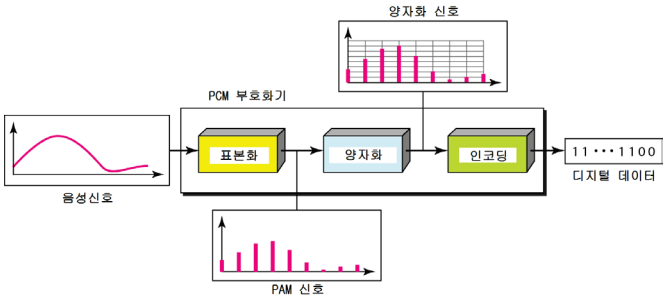


(그림 4) 계수기 방식 암호화

2. 음성 데이터 보안 기법

2.1 음성 코딩 방식

음성 신호의 디지털 변환 시에는 아날로그 음성 신호의 표본화, 양자화, 부호화 과정을 거치며 그 과정을 (그림 5)에 도시하였다. 음성 신호 대역폭이 300~3400Hz 이므로 8 KHz 의 속도로 표본화한 값을 8 비트의 디지털 신호로 변환한 64Kbps 속도의 PCM 데이터로 변환하여 준다.



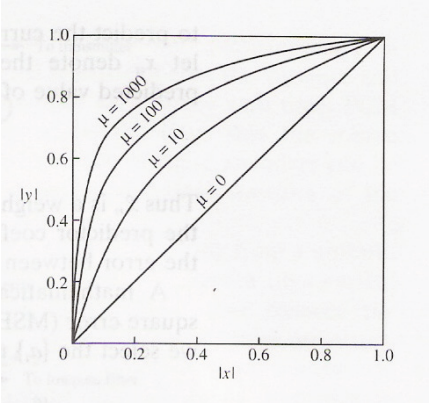
(그림 5) 음성 신호의 디지털 변환 과정

음성 신호의 경우는 큰 신호보다 작은 신호가 확률적으로 빈번함으로 양자화 잡음을 줄이기 위해 작은 신호 구간에서는 양자화 간격 구간크기를 작게 하고 큰 신호에서는 양자화 간격 구간크기를 크게 한 비선형 압축신장기법을 적용한다. 비선형 압축신장기법으로 국내에서는 북미 방식인 μ-Law 방식을 사용한다. (1) 식은 μ-Law 에 근거한 입력신호(x)과 양자화 값(y)의 관계식이며 (그림 6)은 μ 값에 따른 양자화 값(y)의 변화를 보여준다.[8] μ-Law 방식은 작은 신호 구간에서는 거의 선형 특성을 보이며 큰 신호 구간에서는 로그(logarithm) 특성을 지닌다.

$$|y| = \frac{\log(1+\mu|x|)}{\log(1+\mu)} \quad \cdots\cdots\cdots\cdots\cdots (1)$$

$$x = \frac{input}{x_{\max}} \le 1 \quad (\text{정규화된 입력 값})$$

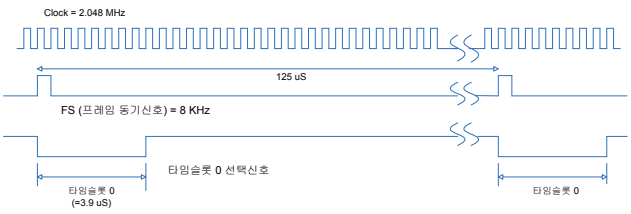
여기서 (1+ μ)=△$_{max}$/△$_{min}$, μ=255 이다.
(△: 양자화 간격 구간크기)



(그림 6) μ-law 압축신장기

2.2 PCM 전송

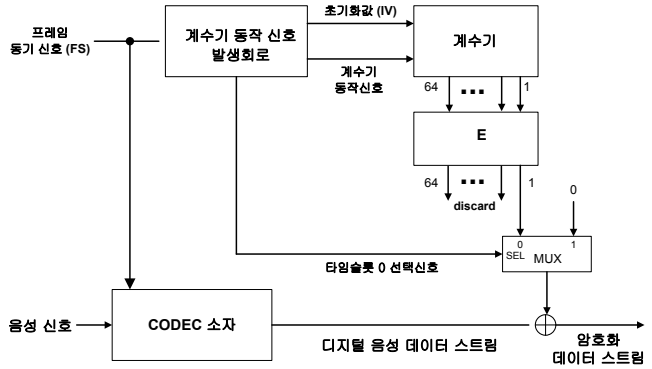
음성 신호를 PCM 디지털 신호로 변환·전송하는 소자로 음성 코덱소자를 사용하는 데 음성 신호를 μ-Law 변환을 거친 후 PCM 전송로 상으로 전송해 주어야 하는 데 PCM 전송로는 여러 개의 음성 신호를 다중화할 수 있도록 각 구간을 타임슬롯으로 나누어 음성 신호를 다중화하여 전송하고 있다. E1 전송로는 64Kbps 의 음성 데이터 32 채널을 각 타임슬롯 별로 다중화한 2.048Mbps 속도의 전송한다. 음성 신호 샘플링 속도와 동일한 8 KHz 속도의 프레임 동기(FS) 신호 구간을 32 개의 동일한 타임슬롯으로 나누어 배정한 구간에 PCM 화한 음성 신호를 실어준다. 음성코덱 소자는 제어단자를 통해 제어 데이터로 0~31 까지의 타임슬롯 지정이 가능하며 고정 타임슬롯 모드도 가능하다.[9] 고정 타임슬롯 모드를 사용할 경우에는 타임슬롯 0 을 배정받는다. (그림 7)에 음성 데이터 전송클럭과 프레임 동기신호 및 타임슬롯 0 구간을 보여준다. 본 논문에서는 고정 타임슬롯을 배정하는 시스템에서 암호화 기법을 소개한다.



(그림 7) 프레임 동기 신호와 고정 타임슬롯 구간

2.3 음성 데이터 보안 기법

음성 데이터를 암호화하여 전송하기 위해서는 음성 코덱을 거쳐 나온 데이터를 암호화한 후 암호화 과정을 거치기 전과 같은 타임슬롯에 전달하여 주어야 하므로 실시간으로 암호화한 후 동기를 맞추어 처리해야 한다. 본 논문에서는 동기식 암호화에 적합한 동기식 스트림 암호화 방식의 일종인 계수기 방식을 하드웨어로 구현하였다. (그림 8)에 디지털 음성 데이터의 동기식 스트림 암호화 장치의 블럭도를 도시하였다.



(그림 8) 디지털 음성 데이터의 동기식 스트림 암호화 장치

음성 데이터 스트림과 암호화 동기를 위해 코덱 소자에 인가되는 프레임 동기 신호와 동일한 신호를 계수기 동작 신호 발생회로에 인가하여 준다. 계수기 동작 신호 발생회로에서는 계수기가 무한 연속적으로 동작하지 않고 프레임 동기신호가 가해질 때마다 초기화되도록 신호를 가해준다. 프레임 동기 신호가 가해질 때 마다 계수기는 초기화되어 동작하며 이 계수기의 출력은 DES 암호화 소자의 64 비트 단위의 블록 입력으로 사용된다. 이 데이터를 암호화한 64 비트 단위의 출력 데이터 중 한 비트(비트 1)만 취하여 MUX 의 입력 단으로 가해준다. MUX 는 2 입력단자 MUX 를 사용하며 입력단자 0 에는 DES 출력단자의 비트 1 을 입력으로 입력단자 1 에는 ´0´값을 인가하여 준다. 계수기 동작신호 발생회로에서 타임슬롯 0 구간 동안만 논리´0´나머지 구간은 논리´1´인 신호를 발생시켜 MUX 의 선택단자로 인가하여 준다. 이 선택 입력 신호는 타임슬롯 0 구간 동안만 DES 암호화 소자의 출력 단자 비트 1 값을 선택하게 되고 이 값과 음성 데이터 스트림 출력을 비트 단위로 XOR 연산되도록 하여 암호화 과정을 수행한다. MUX 입력포트 1 의´0´값이 선택되는 구간에서는 디지털 음성 데이터 스트림과 XOR 한 값이 디지털 음성 데이터 스트림 값과 동일하므로 암호화가 되지 않는 것과 같다. 수신 측에서도 송신 측과 동일한 형태의 암호화 장치를 복호화용으로 사용하면 복호화가 수행되는 대칭적인 구조이다. 프레임 동기 신호는 송·수신 측이 동일한 신호를 사용한다.

3. 결론

본 논문에서는 일반적으로 암호화하지 않는 E1 급(2.048Mbps)속도의 음성 데이터 스트림을 동기식 암호화 기법을 적용하여 암호화하는 과정을 기술하였다. 동기식 암호화 방식에 적합한 계수기 방식의 암호화 기법을 사용하여 고정 타임슬롯을 배정받는 음성 데이터 스트림을 비트 단위로 암호화가 가능함을 보였다. 본 논문의 기법은 고정 타임슬롯을 배정함으로써 교환 기능이 배제된 점대점 통신을 많이 쓰는 군용통신 등에 적용이 가능할 것이다. 향후 과제로는 패킷 데이터의 하드웨어적인 암호화 구현에 관한 것이다.

참고문헌

[1] Jayant, N. S. and Noll, P., Digital Coding of Waveforms, Prentice-Hall, Englewood Cliffs, N.J., 1984.

[2] Jayant, N. S., “Digital Coding of Speech Waveforms: PCM, DPCM, and DM Quantizers,” Proc. IEEE, vol62, pp.611-632, May.

[3] Denning, D. E., Cryptography and Data Security, Addison-Wesley Publishing Co., pp. 135-138, 1983.

[4] Branstad, D. K.,“Security of Computer Communication,” IEEE, Comm. Soc. Mag. Vol. 16, No 6, pp. 33-40, Nov. 1978.

[5] Golumb, S. W., “Shift Register sequences,” Holden-Day, San Fransico, Calif., 1967.

[6] Lipmaa, H., Rogaway, P., and Wagner, D. “CTR Mode Encryption.” NIST First Mode of Operation Workshop, October 2000. http://csrc.nist.govc/encryption/modes.

[7] Hellman, M. E., “On DES-Based, Synchronous Encryption,” Dept. of Electrical Eng., Stanford Univ., Stanford, Calif., 1980.

[8] Jayant, N. S., Waveform Quantization and Coding, IEEE, Press, New York, 1976.

[9] TP3020 Data Sheet, National Semiconductor, (http//www.national.com/analog).