동기식 스트림 암호화 방식을 이용한 무선 암호 통신에서의 난수열 동기

손해성, 홍진근, 김강욱, 황찬식
경북대학교 전자공학과
대구광역시 북구 산격동 1370
shs@palgong.kyungpook.ac.kr

Random Sequence Synchronization for Radio Secure Communication Using Synchronous Stream Cipher

HaeSung Son, JinKeun Hong, KangWook Kim, ChanSik Hwang
Dept. of Electronics, Kyungpook National University
1370 Sankyuk-dong Puk-gu Taegu. KOREA
shs@palgong.kyungpook.ac.kr

Abstract

The synchronous stream cipher has the advantage that one bit error in the ciphertext only affects the corresponding bit in the plaintext, but it requires the perfect synchronization between encryptor and decryptor. For synchronization, a periodic resynchronization has been used in many applications. In this paper, we propose the periodic resynchronization scheme for radio secure communication and evaluate the performances according to the period of sync pattern and session key under radio channel environment having $10^{-2}\sim10^{-6}$ BER.

1.서론

최근 통신 및 컴퓨터 기술의 발달로 인하여 정보교환의 방법 및 양이 증가하고 있다. 이에 따라 송·수신자간의 정보교환에 대해 외부 침입자가 정보를 도청하거나 정보 파괴 및 변조를 방지하기 위한 방법이 요구되고 있으며 이에 대한 방법으로 암호화 기술이 제시되고 있다. 암호 시스템은 암호화를 수행하는 데이터의 형태에 의해 블록 암호(block cipher) 시스템과 스트림 암호(stream cipher) 시스템으로 나눌 수 있다. 블록 암호 시스템은 평문을 일정한 길이의 블록으로 나누어 암호화를 수행하는 것으로 블록간의 독립성이 유지될 수 있으나 전송 도중 블록내에 단순한 비트 오류가 발생하면 이 오류가 블록 전체로 확산되는 단점이 있으며 암호화 수행 속도가 늦어 고속 통신에 적합하지 않다. 반면에 스트림 암호 시스템은 정보를 비트 단위로 암·복호화 시키는 것으로 오류의 확산이 없거나 적고 고속 동작이 이루어지는 장점이 있으나 암·복호기간에 완벽한 난수 동기가 이루어져야 하는 요건이 있다. 따라서 본 논문에서는 스트림 암호 시스템에서 난수의 동기를 이루기 위한 방법으로 제시되고 있는 주기적 재동기 방식을 비트 에러율이 10^{-2} ~ 10^{-6}인 무선 환경에 적용했을 때 안정적인 음성 통신을 할 수 있도록 하기 위한 적절한 사용 방식을 제시하고 평가를 하도록 한다.

2. 스트림 암호 시스템

스트림 암호 시스템에서는 평문을 비트 단위로 암호화를 수행한다[1]. 그림 1은 스트림 암호 시스템의 전체적인 암호화 및 복호화 과정을 보여준다.

평문 P_i는 키스트림 발생기에서 발생한 난수열 K_i와 XOR에 의해 암호문 C_i를 형성하고, 암호문 C_i는 수신측에서 발생한 동일한 난수열 K_i에 의해 평문 P_i를 복호해

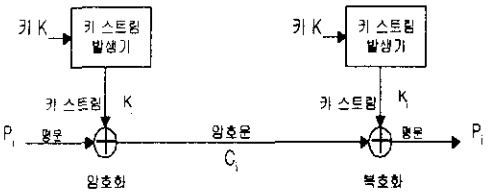

그림 1. 스트림 암호 시스템

낸다. 이를 간단히 나타내면 다음과 같다.

$$C_i = P_i \oplus K_i \quad : \text{암호화}$$

$$P_i = C_i \oplus K_i \quad : \text{복호화}$$

$$= (P_i \oplus K_i) \oplus K_i$$

$$= P_i$$

스트림 암호 시스템에서 그 안전성은 키스트림 발생기에서 발생하는 난수열의 랜덤성에 바탕을 두고 있으며 따라서 키스트림 발생기의 설계가 암호 시스템의 안전성을 결정하게 된다. 키스트림 발생기는 외부에서 입력하는 키 K에 의해 키스트림을 발생시키게 되는데, 이때 사용되는 키에 따라 스트림 암호 시스템은 동기식 스트림 암호(Synchronous stream cipher)와 자기 동기식 스트림 암호(Self-synchronous stream cipher)로 나눌 수 있다. 동기식 스트림 암호는 암호문 또는 평문과 무관한 별도의 키를 사용하여 난수열을 생성하는 것으로 오류의 확산이 발생하지 않아 통신 환경이 열악한 경우 유리할 수 있으나 난수열 동기를 위한 별도의 방법이 요구된다. 자기 동기식 스트림 암호는 암호문 또는 평문의 일부가 키스트림 발생기의 키로 사용되는 것으로 암·복호기간에 난수열 동기 이탈 현상이 발생하여도 일정 시간이 지나면 자동적으로 재동기를 이루는 장점이 있다. 하지만, 암호문에서 1비트의 오류가 발생하여도 수신측에서 복호시 오류 확산이 발생할 수 있어 통신 환경이 열악한 경우 불리하다. 따라서, 채널 환경이 열악한 무선 환경에서는 동기식 스트림 암호시스템을 사용하는 것이 적합하며 송·수신측 사이의 난수열을 동기시키기 위한 적절한 난수열 동기 방법이 요구된다.

3. 난수열 재동기 방법

동기식 스트림 암호에서 난수열 동기를 위한 방법으로 주기적 재동기 방식(periodic resynchronization method)이 많이 사용된다[2][3][4]. 주기적 재동기 방식은 암호문에 동기 패턴과 세션키를 주기적으로 삽입하여 동기를 이루는 방식으로 그 데이터 구성은 그림 2와 같다.

송신측은 동기 패턴과 세션키를 전송하고 이어서 세션

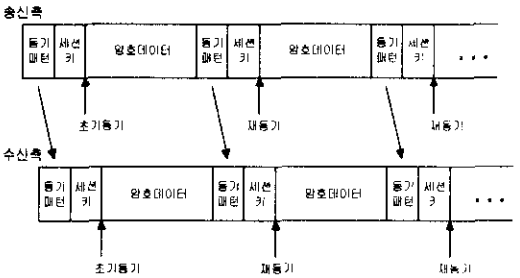

그림 2. 주기적 재동기 방식의 데이터 구조

키를 이용해 암호화된 데이터를 전송하게 되며 이러한 구조가 주기적으로 반복된다. 수신측은 먼저 동기 패턴을 검출하고 수신한 데이터가 동기 패턴이라는 것이 확인되면 이어서 수신되는 세션키를 받아서 난수열 발생기를 초기화 시키게 된다. 그리고, 초기화된 난수열 발생기에 의해 발생되는 난수열에 의해 암호화된 데이터를 복호하게 된다. 주기적 재동기 방식은 비교적 안정된 통신을 할 수 있으나, 주기적으로 동기 패턴과 세션키를 전송해야 하므로 전송 효율이 나빠지고 송·수신 시스템이 데이터를 처리할 때 부하가 많이 걸리는 단점이 있다. 따라서, 주어진 통신 환경과 통신 시스템의 특성을 고려하여 동기 패턴 및 세션키의 크기를 최소화하고 이의 삽입주기를 가능한 길게 해주어야 한다.

4. 무선 환경에 적합한 동기 패턴과 세션 키의 크기 및 삽입 주기 제안

본 논문에서는 무선 환경에서 음성 데이터의 암호 통신을 하기 위해 주기적 재동기 방식을 사용할 때 적합한 동기 패턴과 세션키의 이용 형태 및 삽입주기를 제안한다.

본 논문에서는 동기 패턴으로서 Gold code sequence generator의 출력을 사용하였다[5]. Gold code sequence generator는 많은 종류의 코드를 만들 수 있게 하며 그 출력 수열은 자기 상관(autocorrelation)특성이 우수하다. 그림 3의 [5, 2] generator와 [5, 4, 3, 1] generator의 초기값을 설정해 동작시키면 31비트열로 반복되는 code열이 발생되는데 이 반복되는 31비트를 동기 패턴으로 사용하였다.

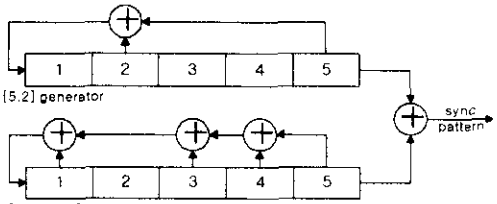

그림 3. Gold code sequence generator

송신측에서 n비트의 동기 신호를 전송하면 수신측에서는 0 ~ n개까지의 오류가 발생한 신호를 받을 수 있으며 m개까지의 오류를 허용할 때 동기 패턴 검출 확률 P_{Dm}은 다음과 같이 구할 수 있다.

$$P_{Dm} = \sum_{i=0}^{m} {}_nC_i \, B^i \, (1-B)^{n-i} \qquad (1)$$

where i = 0, 1, 2, ..., n

B : BER

BER이 10^{-2}일 경우 31비트의 동기 패턴중 1비트까지의 오류를 허용할 때 동기 패턴 검출 확률은 96.2%이며 2비트까지의 오류를 허용할 때 동기 패턴 검출 확률은 99.6%이다. 따라서 수신측에서는 2비트의 오류를 허용할 경우 BER이 10^{-2}일때도 동기 패턴을 거의 모두 검출할 수 있을 것으로 기대된다. 허용 오류 비트수를 너무 크게 하면 false alarm이 발생할 확률이 높아지는 문제점이 발생한다. 따라서, 동기 패턴 검출 확률과 false alarm의 발생 가능성을 고려하여 1비트 또는 2비트의 여분을 두는 것이 적당하며 그 이상의 여분을 두는 것은 바람직하지 않다. 본 논문에서는 31비트의 동기 패턴중 2비트의 여분을 두는 것으로 제안하였다.

세션키는 주기적으로 서로 다른 64비트의 세션키를 발생하여 전송하였는데, 세션키가 전송도중 오류가 발생하면 그 프레임의 암호화된 정보를 올바르게 복호할 수 없으므로 세션키에서의 오류를 줄이기 위해 최대 3비트의 오류 정정 기능을 갖는 (15,4) ML(Maximum-Length)코드로 오류 정정 부호화하여 전송하였다. m비트의 오류 정정기능을 가지는 (n, k)코드를 사용했을 때 L비트의 정보를 정확하게 수신할 확률은 다음 식과 같이 나타낼 수 있다.

$$P_{L(n,k)} = (P_{KEY(n,k)})^{L/k} \qquad (2)$$

where $P_{KEY(n,k)} = \sum_{i=0}^{m} {}_nC_i \, B^i \, (1-B)^{n-i}$

B : BER

BER이 10^{-2}일 때 64비트 세션키를 (15, 4) ML코드로 부호화하여 보낼 경우 위 식에 의하면 세션키를 정확하게 수신할 확률은 99.6%가 되므로 (15, 4) ML코드를 이용하면 세션키를 충분히 보호할 수 있을 것으로 생각된다.

동기 패턴 및 세션키의 삽입주기는 이들 데이터의 검출에 실패했을 때 잃어버리는 데이터가 많아지기 때문에 너무 길게 해서는 안된다. 음성 데이터를 전송할 경우 동기 데이터의 검출에 실패하더라도 그 영향을 최소화하기위해 동기 데이터의 삽입주기는 64kbps로 샘플된 음성의 경우 2400비트, 4800비트 또는 9600비트 정도가 적합할 것이다.

5. 실험 및 평가

무선 환경에서는 BER = 10^{-2} ~ 10^{-6}정도를 고려할 수 있다. 따라서 실험에서는 전송되는 데이터에 BER = 10^{-2}의 에러를 전체 데이터에 주었다. 이때 에러를 주는 위치를 랜덤하게 결정하기 위하여 이진 난수 발생기에서 발생하는 난수의 출력을 이용하여 에러의 위치를 정하였으며 이때 해당하는 위치의 비트를 반전시키는 방법을 이용하였다. 실험에서 동기패턴의 검출에 실패했을 때는 해당하는 만큼의 데이터에 대해 '0'비트를 삽입하였다.

실험은 65536byte의 영상과 64kbps로 샘플된 336000비트의 음성 신호에 대하여 행하였다. 영상에 대한 실험은 동기 패턴 및 세션키의 검출 실패에 따른 복호 데이터의 결과를 쉽게 알아볼 수 있어 제안한 방식에 의한 난수 동기의 성능을 파악하기 쉬운 장점이 있다. 그림 4는 동기 데이터의 삽입 주기를 2400비트로 했을 때 BER = 10^{-2}에서의 영상에 대한 복호된 결과이다.

(a) 원 영상 (b) 복호된 영상

그림 4. BER이 10^{-2}이며 동기 데이터의 삽입주기가 2400비트(247개의 전송프레임)일 때 영상의 복호

65536byte의 영상 데이터를 2400비트를 주기로 동기 데이터를 삽입하게 되면 247프레임의 데이터가 전송되게 된다. 그림 4 (b)의 복호 영상을 보면 검은 줄이 나타나는 부분은 동기패턴 검출에 실패한 경우이며 흰줄이 나타나는 부분은 동기패턴 검출은 성공하였으나, 세션키를 제대로 검출하지 못해 해당하는 암호 데이터를 틀리게 복호하였기 때문에 발생한 것이다. 실험 결과 동기 패턴 검출에 실패한 경우와 세션키 검출에 실패한 경우는 각각 한번 밖에 없었다. 247개의 전송 프레임중 2프레임의 검출에 실패하였으므로 전체 프레임의 수신률은 99.2%로서 만족할만한 수신률을 나타낸다. 복호 영상에서 줄이 나타나는 부분 이외의 랜덤하게 분포하고 있는 점들은 암호 데이터의 오류에 의한 것이다.

제안한 방식을 실제 음성에 적용해 본 결과는 그림 5와 같다. 실험에서는 64kbps로 음성을 5.25초간 녹음하여

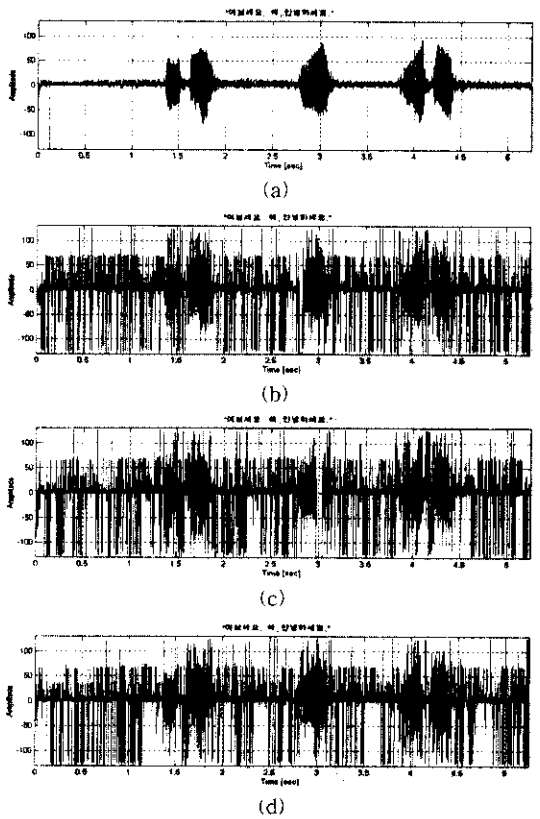

그림 5. BER이 10^{-2}일 때 동기데이터의 삽입주기에 따른 음성신호의 복호 (a)64kbps로 샘플된 원 음성 (b)주기 2400비트(158개의 전송프레임)일때의 복호음성, (c)주기 4800비트(75개의 전송프레임)일때의 복호음성, (d)주기 9600비트(37개의 전송프레임)일때의 복호음성

생성된 336000비트의 데이터를 이용하여 실험하였다. 실험 결과 일부 동기 데이터의 검출에 실패하는 경우는 발생하였지만, 실제 음성을 들어본 결과 모두 음성을 알아듣는데는 문제가 없었다. 주기를 9600비트로 하면 주어진 시간안에 전송되는 프레임의 수가 적어져서 동기 데이터가 에러의 영향을 받는 회수가 적어지므로 동기 데이터 검출에 실패하는 경우는 작아질 수 있다. 그러나, 한번 동기 데이터의 검출에 실패하게 되면 소리가 들리지 않는 구간이 길어져서 음성이 잠시 끊어지는 문제점이 발생하게 된다. 음성을 64kbps보다 더 낮은 rate로 샘플했을때는 그 영향이 더 커지게 될 것이다. 따라서, 64kbps보다 더 높은 rate로 음성을 샘플할때는 동기 패턴의 삽입주기를 9600비트 이상으로 하여도 전체 음성을 청취하는데는 큰 영향이 없으며 64kbps보다 낮은 rate로 음성을 샘플할때는 동기 패턴의 삽입주기를 9600비트보다 짧게 해야 한다.

6. 결론

동기 패턴의 길이를 길게 하고 허용하는 오류 비트의 수를 많이 하면 동기 패턴을 검출할 확률은 높아질 수 있으나 전송 효율이 떨어지는 문제점이 있으므로 본 논문에서는 동기 패턴의 크기를 31비트로 하고 2비트의 여유를 주는 것으로 제안하였다.

세션키는 64비트 세션키를 (15, 4) ML로 부호화하여 240비트를 전송하였다.

실험 결과 제안된 방식으로 데이터를 수신할 경우 비트 에러율이 10^{-2}일때도 99%이상의 높은 수신율을 나타내었다. 따라서, 제안된 방식을 이용하여 음성 데이터를 복호하는데 큰 무리가 없는 것으로 평가된다. 다만 동기 데이터의 삽입 주기를 너무 길게 할 경우 동기 데이터 검출에 실패할 때 잃어버리는 데이터가 많으므로 삽입 주기를 너무 길게 하는 것은 효율적이지 않다.

64kbps로 샘플된 음성에서 동기 패턴을 31비트로 하고 2비트의 오류를 허용하며 64비트 세션키를 (15, 4) ML로 오류 정정 부호화하여 전송한 결과 주기를 9600비트 이하로 하면 무선 환경에서 안정된 음성 통신이 가능하다는 것을 확인하였다.

참고 문헌

[1] Bruce schneier, Applied Cryptography 2nd edition : Protocols, Algorithms, and Source code in C, John Willy & Sons, 1996

[2] J. H Yoon, C. S Hwang, "Resynchronization technique by time synchronization for secure communication using stream cipher," Proceedings of 1997 International Conference on Information, Communications and Signal Processing, pp. 1129-1133, Sep. 1997.

[3] 윤장홍, 강건우, 황찬식 "동기식 스트림 암호 통신에 적합한 사이클 슬립 보상 알고리즘", 한국통신학회 논문지, 제 8권, 제 22호, pp. 1765-1773, 1997년 8월.

[4] 윤장홍, 안병호, 양상운, "점대점 비동기 스트림 암호 통신에서의 재동기 방법에 관한 연구" 제 6회 정보보호와 암호학에 관한 학술대회 논문집, pp.268-273, 1994년 10월.

[5] Harold B. Killen, Digital Communications with Fiber Optics and Satellite Applications, Prentice-Hall, 1988