JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 7 : 1401~1410 Jul. 2017

최대길이 시퀀스를 이용한 암호동기신호 생성 기법

손영호[1] · 배건성[2*]

Cryptographic synchronization signal generation method using maximal length sequence

Young-ho Son[1] · Keun-sung Bae[2*]

[1]Attached Institute of ETRI, Daejeon, 34129, Korea
[2*]School of Electronics Engineering, Kyungpook National University, Daegu, 41566, Korea

요 약

암호통신에서 암호기와 복호기 간의 암호 알고리즘 내부 상태 동기와 스트림 동기를 일치시키는 암호동기 기능은 암호통신 품질에 많은 영향을 준다. 암호통신 중 송신기와 수신기 간에 동기 이탈이 발생하면 재동기를 이루기까지 통신 불능 상태가 된다. 특히 BER이 높은 무선 채널에서 이루어지는 암호통신에서는 암호동기 성능이 암호통신의 품질을 좌우하는 요소가 된다. 본 논문에서는 BER이 높은 잡음 환경에서도 동기 성능을 향상시킬 수 있는 새로운 형태의 암호동기신호 생성 및 검출 기법을 제안하였다. 제안한 방법에서는 최대길이 시퀀스 기반의 마스킹 구조 형태로 동기신호를 생성하고, 최대길이 시퀀스의 상관함수 특성을 이용하여 동기신호를 검출한다. 다양한 모의실험을 통해 제안한 마스킹 구조 형태의 동기신호가 기존의 연접 형태의 동기신호에 비하여 잡음환경에서 우수한 동기 성능을 보임을 확인하였다.

ABSTRACT

Cryptographic synchronization which synchronizes internal state of cryptographic algorithm and ciphertext stream between an encryptor and a decryptor affects the quality of secure communication. If there happens a synchronization loss between a transmitter and a receiver in a secure communication, the output of the receiver is unintelligible until resynchronization is made. Especially, in the secure communication on a wireless channel with high BER, synchronization performance can dominate its quality. In this paper, we proposed a novel and noise robust synchronization signal generation method as well as its detection algorithm. We generated a synchronization signal in the form of a masking structure based on the maximal length sequence, and developed a detection algorithm using a correlation property of the maximal length sequence. Experimental results have demonstrated that the proposed synchronization signal outperforms the conventional concatenated type synchronization signal in a noisy environment.

키워드 : 암호동기, 암호통신, 동기신호, 최대길이 시퀀스, 마스킹

Key word : Cryptographic synchronization, secure communication, synchronization signal, m-sequence, masking, etc

Received 16 March 2017, **Revised** 16 March 2017, **Accepted** 25 March 2017

* **Corresponding Author** Keun-sung Bae(E-mail:ksbae@ee.knu.ac.kr, Tel:+82-53-950-5527)
School of Electronics Engineering, Kyungpook National University, Daegu, 41566, Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.7.1401 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

공개된 유무선 네트워크를 이용한 정보 교환이 증가하면서 제 3자에 의한 도청을 방지하기 위한 수단으로 암호통신의 사용이 증가하고 있는 추세이다. 암호통신은 송신자가 전송한 정보가 전송 구간에서 제 3자에게 누설되거나 임의로 조작되는 것을 방지하기 위하여 송신자가 암호기를 이용하여 데이터를 제 3자가 알아보기 어려운 형식으로 암호화하여 보내고 정당한 수신자만 복호기를 이용하여 암호문을 해독함으로써 유효한 정보를 얻도록 하는 방법이다.

암호통신에서 수신된 암호문이 제대로 복원되기 위해서는 암호기와 복호기 간의 암호 알고리즘 내부 상태 동기와 스트림 동기가 일치해야 한다. 암호 알고리즘의 내부 상태 동기는 암호 알고리즘을 동작시키는 세션키를 암호기와 복호기 간에 공유하는 키 교환을 통하여 이루어진다. 초기 암호통신에서는 사전에 오프라인 방식으로 사용자 간에 전송 데이터를 암호화하는 키수열을 직접 공유하였다. 그러나 암호통신의 확대에 따른 통신 대상과 전송 데이터 양의 급격한 증가로 오프라인 방식의 사전 키 교환은 불가능하게 되었다. 따라서 최근에는 오프라인 방식으로 사전에 공유하는 키 요소를 최소화하고, 새로운 통신 세션마다 온라인으로 추가적인 가변 요소를 동기신호에 포함하여 교환함으로써 세션키를 공유하는 방법을 사용한다[1,2]. 암호통신에서 스트림 동기는 암호기에서 출력되는 암호문과 복호기로 입력되는 암호문의 암호 알고리즘에 대한 입출력 관계를 일치시키는 기능으로, 동기식 암호통신에서는 암호기에서 동기신호를 전송하고 복호기에서 검출하여 스트림 동기를 일치시키는 방법을 주로 사용한다[3,4]. 암호통신 시작 단계에서 일치된 스트림 동기는 통신 중 채널 잡음, PLL(phase lock loop)의 정밀도 차이 등에 기인한 사이클 슬립(cycle slip) 현상 등으로 동기가 어긋나는 동기 이탈 현상이 발생할 수 있다[4-6].

동기 방식에 대한 기존 연구에서는 송신기에서 동기신호를 신호 검출에 필요한 동기 패턴과 키 교환에 필요한 동기 데이터를 연접하는 형태로 구성하여 암호문과 동일한 채널로 전송하고, 수신기에서 동기 패턴의 상관특성을 이용하여 동기신호를 검출하는 방식을 사용한다[3,4]. 이러한 동기 방식에서는 수신기에서 동기 패턴을 검출하여 동기신호 이후의 암호문 위치를 검출함으로써 송신기와 암호문에 대한 스트림 동기를 일치시킨다. 그리고 동기 패턴에 연접된 동기 데이터 구간에서 동기 데이터를 복원하고 세션키를 생성하여 공유함으로써 암호 알고리즘의 내부 상태 동기를 일치시킨다. 그러나 비트 오류율(bit error rate, BER)이 높은 무선통신 환경에서는[7,8] 채널에서 발생하는 높은 수준의 오류 때문에 동기 패턴 검출률과 동기 데이터 검출률이 낮아지게 되고, 이로 인한 통신 불능 현상으로 암호통신의 품질이 평문통신에 비하여 상당히 떨어지게 된다. 또한 기존의 동기 방식에서는 동기신호를 부가정보로 암호문과 동일한 채널로 전송하기 때문에 암호통신은 평문통신에 비하여 데이터 전송률이 낮아지게 된다. 특히 열악한 무선 환경에서 운용되는 암호 시스템에서 암호통신의 생존성을 높이고, 방송통신 모드를 지원하는 암호 시스템에서 late-entry[4,9]를 지원하기 위하여 주기적인 재동기 방식 적용이 필요한 경우에 기존 동기 방식은 낮은 동기신호 검출률과 전송 효율 저하 문제 등으로 적용에 어려움이 있다[3,4]. 이처럼 암호통신에서 동기 검출에 사용하는 동기신호의 검출 성능과 전송 효율은 암호통신의 품질을 좌우하는 주요 요소가 된다. 따라서 암호통신의 품질을 개선하기 위하여 BER이 높은 잡음 환경에서 동기신호 검출 성능을 높이면서도 전송 효율을 향상시킬 수 있는 동기신호 생성 방법에 대한 연구가 필요하다.

본 연구에서는 암호통신에서 기존 동기 방식에서 사용하던 연접(concatenation) 형태의 동기신호 구조에 비하여 잡음 환경에서 동기 성능을 향상시킬 수 있는 최대길이 시퀀스(maximal length sequence, m-sequence)[10-12]를 이용한 마스킹 구조 형태의 동기신호 생성 방법과 검출 알고리즘을 제안하고, 동기신호 검출 성능을 이론적으로 분석하였다. 그리고 다양한 잡음 환경에서 제안한 동기신호와 기존의 동기신호를 이용한 동기 검출 모의실험을 실시하고, 결과를 비교·분석하여 제안한 마스킹 구조 형태의 동기신호가 잡음 환경에서 동기 검출 성능이 우수함을 보였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 연접 형태의 동기신호 구조에 대하여 설명하고, 3장에서 최대길이 시퀀스를 이용한 동기신호 생성 기법과 검출 알고리즘에 대하여 설명한다. 4장에서는 다양한 잡음 환경에서 제안한 동기신호를 이용한 동기신호 검출 모의실험 결과를 제시하고, 5장에서 결론을 맺는다.

Ⅱ. 기존 연구에서의 동기신호 구조

일반적으로 암호통신에서 사용하는 동기신호는 동기 패턴과 동기 데이터로 구성된다[3,4]. 동기 패턴은 송신기에서 보낸 동기신호를 수신기에서 검출하기 위한 식별자로서, 자기상관 특성이 우수한 시퀀스를 사용한다. 동기 데이터는 암호기와 복호기 간에 세션키 등을 공유하기 위하여 필요한 키 교환 데이터에 해당한다.

그림 1은 동기 방식에 관한 기존 연구에서 제시한 동기신호 구조를 나타낸 것으로, 동기신호를 동기 패턴(SP)에 동기 데이터(SKD)를 연접하는 형태로 구성하였다. 동기 패턴에 단일 동기 데이터를 연접하여 보내는 구조(a)는 동기신호를 짧게 구성할 수 있다는 장점이 있으나, BER이 높고, 전송 중 연집 오류(burst error) 발생 가능성이 높은 무선 환경에서는 동기 검출 성능이 급격히 낮아지는 단점이 있다. 이러한 단점을 보완하기 위하여 송신기에서는 동기 데이터에 오류정정부호(error correcting code, ECC)를 적용하고, 수신기의 동기 패턴 검출기에서는 입력 스트림이 동기 패턴과 일정 비트 이상 일치하면 동기 패턴으로 간주하여 동기신호 검출률을 높이는 방법을 사용한다. 그림 1의 (b)에서 제시한 동기신호는 (a)에서 제시한 동기신호 구조에서 동기 데이터를 홀수 번 반복 전송하는 방식으로, 수신기에서는 다수결 논리 복호기(majority logic decoder)를 이용하여 동기 데이터를 검출한다. BER이 높은 무선 환경에서 동기 검출 성능을 향상시킬 수 있으나, 동기신호 길이 증가로 인해 전송 효율이 낮아지고 전송 지연이 커지는 단점이 있다.

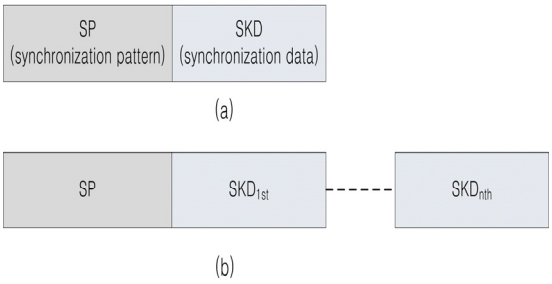

Fig. 1 Concatenated synchronization signal structure used in a conventional synchronization method (a) Single transmission (b) Repetitive transmission

그림 2와 3은 63비트의 동기 패턴에 42비트의 동기 데이터를 단순히 연접하여 전송하는 경우와 동기 데이터에 BCH(127,43)을 적용하여 전송하는 경우의 이론적인 동기 검출 확률을 각각 보인 것으로, 동기 데이터를 단순히 전송하는 경우는 BER 증가로 동기 성능이 급격히 떨어지는 것을 볼 수 있다. 그림에서 T는 상관특성 기반의 동기 패턴 검출기[3,4]에서 입력 수열을 동기 패턴으로 검출하기 위한 오류 개수 문턱값을 의미한다.

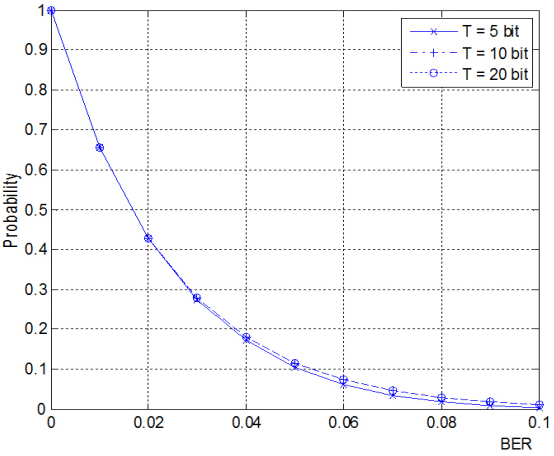

Fig. 2 Detection probability of cryptographic synchronization with a conventional method in random error environment (without ECC)

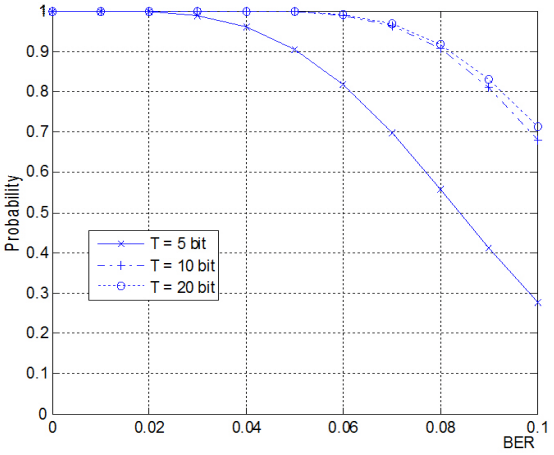

Fig. 3 Detection probability of cryptographic synchronization with a conventional method in random error environment (with BCH(127,43))

Ⅲ. 최대길이 시퀀스를 이용한 동기신호

3.1. 최대길이 시퀀스를 이용한 동기신호 생성 방법

최대길이 시퀀스는 잡음과 유사한 특성을 가지면서 이상적인 자기상관함수 특성을 지닌 PN(pseudo noise) 시퀀스의 한 종류로서, CDMA(code division multiple access) 방식의 이동통신에서 사용자의 송신 정보 확산과 기지국 구분 등에 사용되고 있다[10,11]. 최대길이 시퀀스는 시프트 레지스터를 이용하여 효과적으로 생성할 수 있다. 시프트 레지스터는 데이터 저장소인 레지스터들이 선형으로 연결된 구조로서, 클럭이 입력될 때마다 레지스터에 저장된 모든 비트를 다음 레지스터로 이동시키는 방식으로 입출력을 서로 연결하는 구조이다[10-12].

그림 4는 n개의 연속적인 레지스터들로 구성된 n차의 시프트 레지스터를 보인 것이다. 제시된 시프트 레지스터에서는 클럭이 n번 활성화된 후 모든 레지스터가 '0'으로 채워지는 것을 방지하기 위하여, 이전 상태값들의 선형 함수로 이루어지는 궤환회로를 구성하여 그 결과값을 첫 번째 레지스터로 입력하게 하였다. 이러한 시프트 레지스터를 LFSR(linear feedback shift register)이라고 한다[10-12]. 궤환회로가 부가된 LFSR은 결정적 장치이면서, 레지스터들이 가질 수 있는 값의 조합이 유한하기 때문에 출력수열은 일정한 주기로 반복되게 된다. 특히 LFSR에서 궤환함수를 적절히 선택하면 출력수열의 주기가 최대인 $2^n - 1$이 되면서, 랜덤하게 보이는 이진수열을 생성할 수 있는데, 이러한 이진수열을 최대길이 시퀀스라고 한다[10-12].

그림 5는 제안한 최대길이 시퀀스를 이용하여 생성한 동기신호 구조를 보인 것으로, 상관특성이 우수한 최대길이 시퀀스와 홀수 번 반복된 동기 데이터 간의

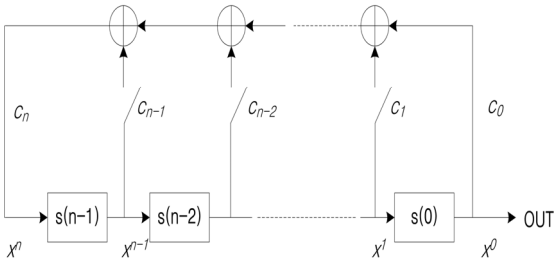

Fig. 4 Linear feedback shift register of degree n

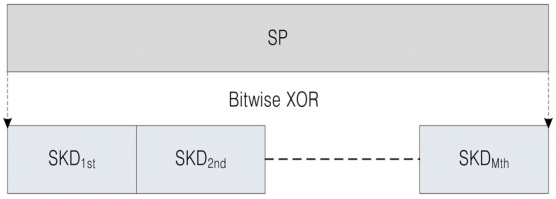

Fig. 5 Synchronization signal structure using m-sequence

bitwise xor 연산으로 동기신호를 생성한다[13]. 동기 패턴으로 동기 데이터를 비트 단위로 마스킹하는 방식으로 동기신호를 생성하기 때문에 동기 패턴 영역과 동기 데이터 영역이 별도로 구분되지 않는 특징을 갖게 된다. 동기신호를 생성하는 과정은 다음과 같다.

Step 1: L비트의 동기 데이터를 생성한 후 홀수 번(M회) 반복한다.

Step 2: 길이가 L x M 비트 이상인 최대길이 시퀀스를 생성한다.

Step 3: 생성된 최대길이 시퀀스의 길이가 반복 부호화된 동기 데이터의 길이를 초과할 경우 동기 데이터의 끝부분에 초과한 비트 수만큼 '0' 으로 채운다.

Step 4: 생성된 최대길이 시퀀스와 반복된 동기 데이터를 bitwise xor 연산을 수행하여 동기신호를 생성한다.

3.2. 최대길이 시퀀스를 이용한 동기신호 검출 방법

기존 연구에서 제시한 연접 형태 동기신호의 경우는 상관특성을 이용하는 동기 패턴 검출기[3,4]를 이용하여 동기 패턴을 검출함으로써 동기신호 전체를 검출하게 된다. 그러나 본 연구에서 제안한 구조의 동기신호는 최대길이 시퀀스에 동기 데이터가 비트 단위로 마스킹되어 난수열로 변형되기 때문에 상관특성을 이용하는 동기 패턴 검출기를 사용할 수 없다.

그림 6은 송신기에서 최대길이 시퀀스를 이용하여 동기신호를 생성하고, 수신기에서 동기신호를 검출하는 과정을 보인 것이다. 송신기에서는 M회 반복된 동기 데이터를 최대길이 시퀀스와 bitwise xor 연산을 수행하여 동기신호를 생성한 후 암호문에 연접시켜 출력한다. 이때 송신기에서 출력되는 동기신호(SYNC)와 암호문(R_1, R_3)은 모두 난수성을 갖게 되는데, 이것은 암호문

과 최대길이 시퀀스가 갖는 유사난수성 때문이다. 수신기에서는 동일한 최대길이 시퀀스를 이용하여 입력 스트림과 bitwise xor 연산을 수행한다. 이때 동기신호와 정확히 일치하는 구간에서는 동기신호에 포함된 최대길이 시퀀스가 제거되어 반복된 동기 데이터(*SKD*$_{1st}$ ~ *SKD*$_{Mth}$)가 출력되고, 그 외 구간에서는 난수열이 출력되는 특징을 이용하여 동기신호 구간을 검출하게 된다.

일반적으로 반복 전송된 데이터는 다수결 논리 복호기를 이용하여 검출할 수 있다. 다수결 논리 복호기는 수신된 비트 스트림에서 가장 많이 발생한 값을 해당 비트의 대푯값으로 결정하는 방식으로, 부호 이론에서 반복 부호의 복호기로 사용된다[14].

그림 7은 5회 반복 전송된 데이터에서 각 비트 값을 다수결 논리 복호기를 이용하여 결정하는 과정을 개념적으로 보인 것이다. 식 (1)은 다수결 논리 복호기에서 *M*번 반복 수신된 동기 데이터 비트 값을 결정하는 수식을 나타낸 것이다.

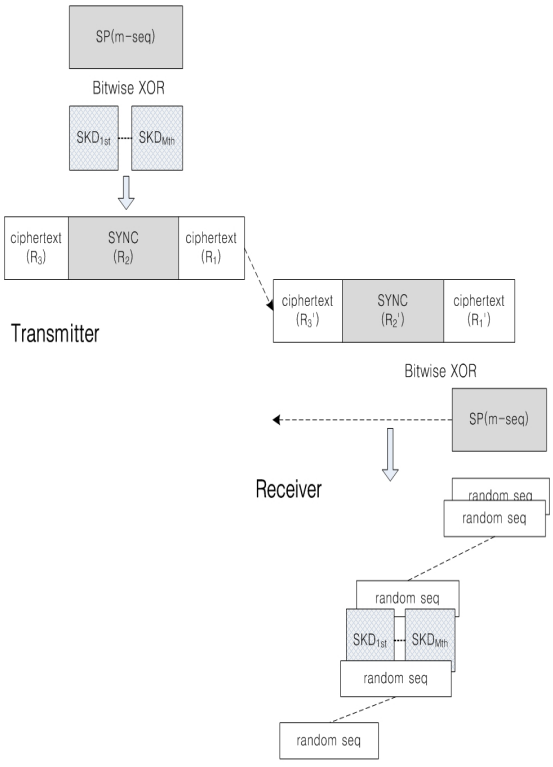

Fig. 6 Synchronization signal generation and detection procedure using m-sequence

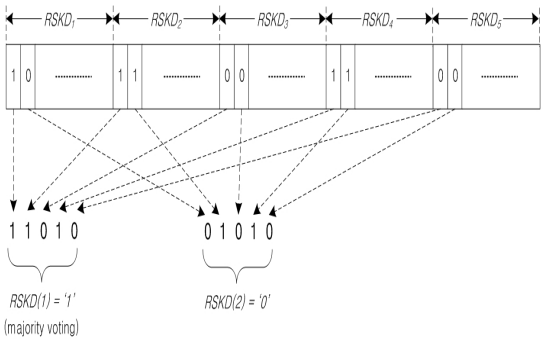

Fig. 7 Synchronization data detection procedure in majority logic decoder

$$\begin{aligned} &\text{if} \quad \sum_{i=1}^{M} RSKD_i(j) > \frac{M-1}{2}, SKD(j) = 1 \\ &else \qquad\qquad\qquad\qquad\quad , SKD(j) = 0 \end{aligned} \tag{1}$$

식에서 *RSKD*는 *L* x *M* 비트 크기의 수신 데이터 저장 레지스터를 의미하며, *SKD*는 다수결 논리 복호기로 복호한 동기 데이터를, *i*와 *j*는 각각 반복 횟수와 동기 데이터를 구성하는 비트의 위치를 의미한다.

그림 8은 최대길이 시퀀스로 마스킹된 구조의 동기신호를 검출하는 알고리즘의 개략적인 흐름도를 보인 것이다. *L* x *M* 비트 크기의 입력 스트림을 최대길이 시퀀스로 bitwise xor 연산을 하고, 다수결 논리 복호기에 입력하여 *L*비트의 데이터를 검출한다. 이때 각 비트의 대푯값을 결정하는 과정에서 검출된 오류 개수의 합(*Error*)이 설정된 문턱값(*T*) 이하인 경우에 동기신호가 검출된 것으로 판단하고, 검출된 데이터를 동기 데이터(*SKD*)로 결정한다.

본 연구에서는 최대길이 시퀀스로 마스킹된 구조의 동기신호를 검출하기 위하여 다수결 논리 복호기에서 검출된 오류 개수의 분포 특성을 이용한다. 반복 부호화된 비트를 다수결 논리 복호기로 결정할 때, 대푯값과 다른 비트의 개수를 오류 개수로 정의하면, *L*비트의 *SKD* 결정 과정에서 발생할 수 있는 전체 오류 개수(*Error)*는 식 (2)와 같다.

$$\begin{aligned} &Error = \sum_{j=0}^{L} error(j) \\ &where\ error(j) = \sum_{i=1}^{M} |SKD(j) - RSKD_i(j)| \end{aligned} \tag{2}$$

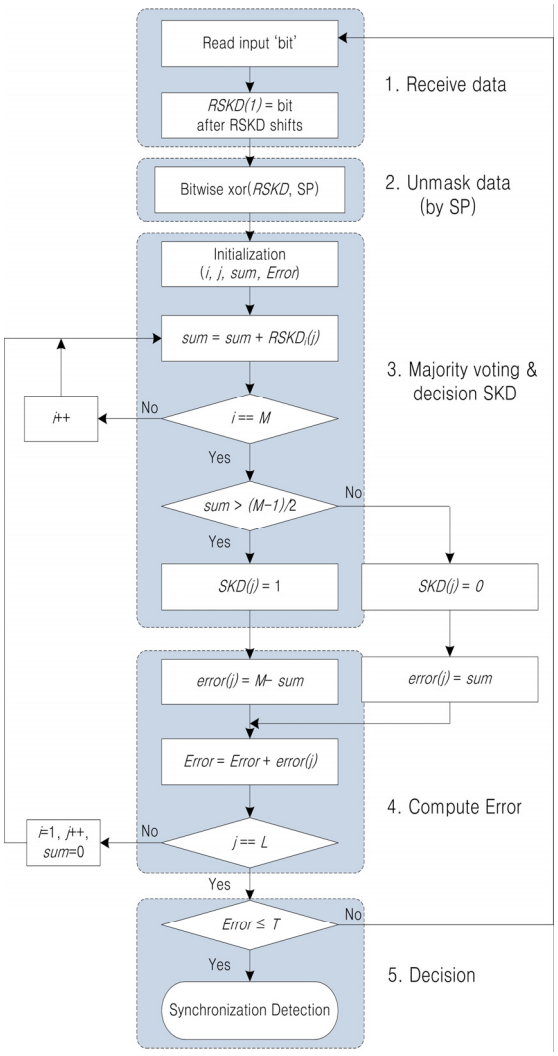

Fig. 8 Synchronization signal detection algorithm using m-sequence

최대길이 시퀀스의 상관함수 특성과 유사난수성 특성으로 다수결 논리 복호기에서 검출되는 오류 개수는 동기신호 구간($Error_{syn}$)과 그 외 신호 구간($Error_{other}$)에서 각각 식 (3), (4)와 같이 정의할 수 있다. 따라서 동기신호 검출 여부를 결정하기 위한 오류 개수 문턱값을 식 (5)와 같이 설정할 수 있다. 식에서 B는 동기신호가 전송되는 채널의 BER을 의미한다.

$$Error_{syn} = B \times L \times M \tag{3}$$

$$Error_{other} = L \times Max(error(j))$$
$$where\ Max(error(j)) = \frac{M-1}{2} \tag{4}$$

$$Error_{syn} < T < Error_{other} \tag{5}$$

최대길이 시퀀스로 마스킹된 구조의 동기신호를 이용하는 동기 방식에서는 수신된 데이터 스트림을 다수결 논리 복호기에 입력하여 동기신호를 검출하고, 대푯값으로 결정된 L비트의 데이터를 동기 데이터로 결정한다. 따라서 암호통신에서 동기 검출에 성공할 확률(P_{SKD})은 식 (6)과 같이 동기신호 검출 확률(P_D)과 동기 데이터 검출 확률(P_L)의 곱으로 정의될 수 있다.

$$P_{SKD} = P_D \times P_L$$
$$where\ P_D = \sum_{j=0}^{T} P_{dj},\quad P_L = (P_{bit})^L \tag{6}$$

식에서 P_{dj}는 다수결 논리 복호기에서 발생할 수 있는 오류 개수 j에 대한 확률밀도함수를 의미하며, P_{bit}는 1비트의 데이터를 M번 반복 전송할 때, 수신기에서 해당 데이터가 정확히 수신될 확률을 나타낸다.

Ⅳ. 실험 결과

본 연구에서 제안한 최대길이 시퀀스로 마스킹한 동기신호의 동기 검출 성능을 분석하기 위하여 동기신호를 생성하여 다양한 수준의 잡음이 부가되는 채널로 전송하고 검출하는 모의실험을 실시하고 그 결과를 분석하였다. 채널 잡음은 BER 값에 해당하는 오류 개수만큼 전송 데이터의 비트 위치를 랜덤하게 선택한 후 해당 비트의 값을 반전하는 방식으로 부가하였다.

그림 9는 최대길이 시퀀스로 마스킹하여 생성한 127비트 동기신호가 포함된 암호문에 랜덤 잡음을 부가하여 전송하고, 수신기에서 그림 8에서 제안한 알고리즘으로 동기신호를 검출할 때 다수결 논리 복호기에서 검출되는 오류 개수를 BER 값별로 비교하여 보인 것이다. 동기신호 구간에서 오류 개수는 BER 증가와 함께 증가하지만, 그 외 구간에서는 유사하게 나타나는 것을 볼 수 있다. 이러한 현상은 다수결 논리 복호기에 동기신호 구간에서는 랜덤 잡음이 부가된 반복 부호화된 동기

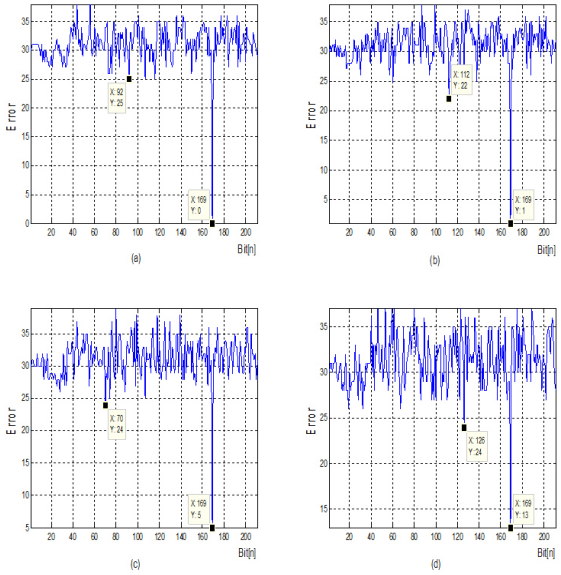

Fig. 9 Error distribution for BER in the majority logic decoder (a) BER = 0, (b) 0.01, (c) 0.05, (d) 0.1

데이터가 입력되고, 그 외 구간에서는 최대길이 시퀀스로 마스킹되어 유사난수성을 갖는 이진수열이 입력되기 때문이다. 따라서 동기신호 구간을 검출하기 위한 오류 개수 문턱값을 식 (3)에서와 같이 채널의 BER을 반영하여 적응적으로 설정하여야 한다. 예로 BER이 0.1인 경우 오류 개수 문턱값은 식 (5)와 실험 결과를 고려할 때 13에서 24 사이의 값으로 설정할 수 있다.

그림 10은 그림 9에서 사용한 127비트 동기신호를 이용한 동기 검출 실험으로 얻은 동기신호 검출률을 식 (6)에서 정의한 검출 확률 P_D와 비교하여 보인 것으로, 동기신호 검출률이 식 (3)에서 유도된 최소 문턱값 13에서는 79% 수준이나, 19 이상에서는 100%로 상당한 차이가 있는 것을 볼 수 있다. 이것은 동기신호 구간에서 발생할 수 있는 랜덤 오류 개수에 차이가 있을 수 있기 때문이다. 그리고 오류 개수 문턱값 20까지는 실험상의 동기신호 검출률이 이론상의 동기신호 검출 확률과 거의 일치하지만, 초과하는 경우에는 실험상의 검출률이 급격히 떨어지는 것으로 나타났다. 이것은 동기신호 구간으로 결정하는 오류 개수 문턱값이 커질수록 원래 동기신호가 아닌 구간을 동기신호에 문턱값 이내의 오류가 발생한 것으로 판단하여 동기신호로 오검출(false alarm)[4]하는 빈도가 증가하기 때문이다.

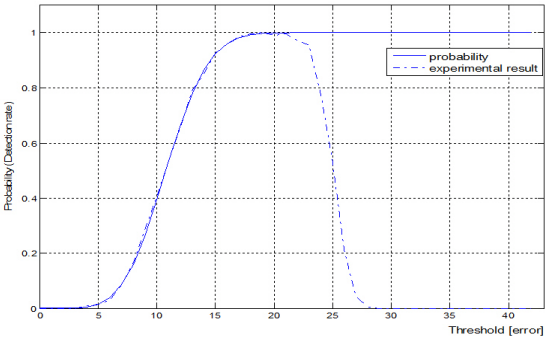

Fig. 10 Comparison of detection probability and measured detection rate of a synchronization signal (BER=0.1)

그림 11은 동기신호 검출 후 동기 데이터의 정확한 복원까지 반영하는 암호동기 검출률을 식 (6)에서 정의한 검출 확률인 P_{SKD}와 비교하여 보인 것으로, 동기 데이터를 단순히 3회 반복하여 구성하는 경우에는 BER 0.1인 채널에서 동기 검출률이 30% 이하로 상당히 낮게 나타났다. 이것은 전송 중 동기신호 구간에 발생한 오류로 인하여 동기신호 구간은 검출하였으나, 동기 데이터의 정확한 복원에는 실패하였기 때문이다. 비밀키 기반의 암호통신에서 수신기에서 동기신호 구간을 검출하여 스트림 동기에 성공하여도 동기 데이터 검출에 실패하면 암호기와 복호기에서 사용하는 세션키가 불일치하여 수신기에서 암호문 해독에 실패하게 된다. 따라서 제안한 최대길이 시퀀스로 마스킹한 구조의 동기신호를 BER이 높은 무선 환경에 적용하기 위해서는 동기 데이터에 발생한 오류를 정정할 수 있는 오류정정기법 등의 적용이 필요하다.

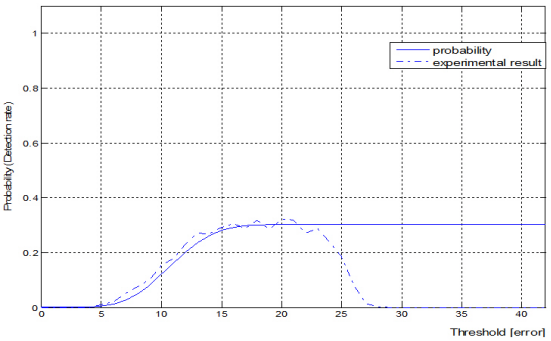

Fig. 11 Comparison of cryptographic synchronization detection probability and measured detection rate (BER=0.1)

표 1은 최대길이 시퀀스를 이용하여 동기신호를 생성할 때, 42비트의 동기 데이터를 단순 반복하는 경우에 반복 횟수에 따른 암호동기 검출 확률(P_{SKD})을 나타낸 것이며, 표 2는 동기 데이터에 다양한 BCH 부호를 적용하여 3회 반복하는 경우에 적용한 BCH 부호에 따른 암호동기 검출 확률을 나타낸 것이다.

BER이 0.1인 채널에서 동기 검출 목표값을 89% 이상으로 할 때, 동기 데이터를 단순 반복하는 경우는 7회 이상 반복이 필요하기 때문에 동기신호 길이는 최소 294비트에 달한다. 그러나 동기 데이터에 BCH(31, 21)를 적용하고, 3회 반복하는 경우는 동기신호를 186비트로 줄일 수 있다. 이러한 결과는 최대길이 시퀀스로 마스킹한 동기신호를 이용하는 동기 방식에서 동기 데이터를 단순 반복하는 것보다 오류정정부호를 적용하고, 반복 횟수를 최소화하는 것이 동기 성능 개선에 효과적임을 보여준다.

Table. 1 Cryptographic synchronization detection probability with repetition

Repetition	P_{SKD}(%) with $P_D = 1$		Length (bit)
	BER = 0.01	0.1	
3	98.756	30.338	126
5	99.959	69.693	210
7	99.999	89.160	294
9	100	96.326	378
11	100	98.766	462
13	100	99.584	546
21	100	100	882

Table. 2 Cryptographic synchronization detection probability with ECC

BCH	P_{SKD}(%) with $P_D = 1$		Length (bit)
	BER = 0.01	0.1	
	3 times	3 times	
BCH(15,11)	99.996	76.536	180
BCH(31,21)	100	89.279	186
BCH(63,45)	100	89.978	189
BCH(15, 7)	100	95.434	270
BCH(127,43)	100	100	381

Table. 3 Synchronization signal composition for synchronization methods

Method	SYNC(190 bit)	
	SP(bit)	SKD(42 bit)
m-sequence based	190	BCH(63,45), 3 repetition
concatenation based	127	BCH(63,45)
	63	BCH(127,43)

그림 12는 최대길이 시퀀스로 마스킹한 동기신호와 기존 연접 형태의 동기신호의 동기 검출 성능을 비교하기 위하여 표 3에서와 같이 동기신호를 생성하여 랜덤 오류가 발생하는 채널로 전송하고 검출하는 모의실험을 반복하여 얻은 암호동기 검출률을 비교하여 보인 것이다. 동기신호 검출에 사용한 오류 개수 문턱값은 동기신호 검출 확률(P_D)이 99% 이상이 되는 오류 개수 중 최소값으로 설정하였다. 동기신호별 동기 검출 성능이 BER이 0.01 이하인 경우에는 비슷하지만 BER이 증가할수록 제안한 동기신호의 검출률에 비하여 기존 연접 형태 동기신호의 검출률이 급격히 떨어지는 것을 볼 수 있다. 이것은 동기신호 영역을 동기 패턴과 동기 데이터로 분할하여 사용하는 기존 동기신호 구조에 비하여 제안한 동기신호는 동기신호 전 구간을 동기 패턴과 동기 데이터 영역으로 확장함으로써 동기 데이터에 오류정정 성능이 좋은 오류정정부호 적용이 가능하기 때문이다.

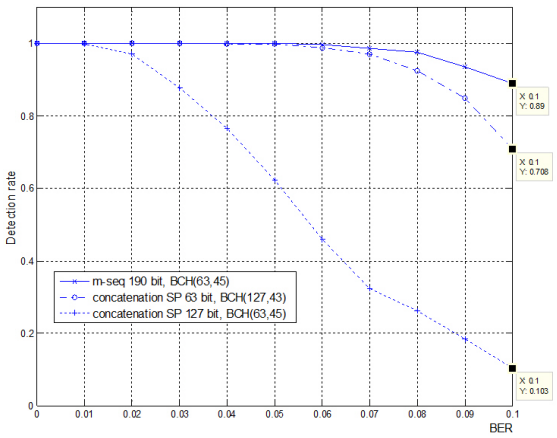

Fig. 12 Detection rate of cryptographic synchronization depending on synchronization methods in random error environment

그림 13은 표 3에서 제시한 동기신호들을 BER 0.1인 채널로 전송할 때 동기신호 검출기에서의 이론상의 암호동기 검출 확률을 비교하여 보인 것이다. 그래프에 표시한 좌표는 동기신호 검출 확률이 99% 이상이 되는 오류 개수 문턱값 중 최소값에서의 암호동기 검출 확률을 나타낸 것으로, 그림 12에서 BER 0.1일 때 모의실험으로 얻은 암호동기 검출률 89%, 70.8%, 10.3%를 거의 비슷하게 반영하는 것을 볼 수 있다.

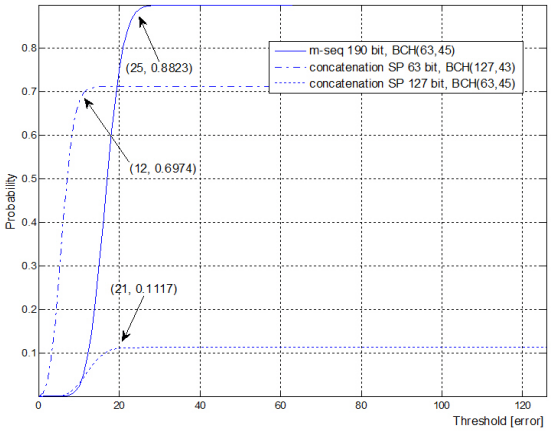

Fig. 13 Detection probability of cryptographic synchronization depending on synchronization methods in random error environment

Ⅴ. 결 론

본 논문에서는 암호통신에서 BER이 높은 잡음 환경에서 기존의 연접 형태 동기신호 구조에 비하여 암호동기 검출 성능을 향상시킬 수 있는 최대길이 시퀀스를 이용한 마스킹 구조 형태의 동기신호 생성 방법과 검출 알고리즘을 제안하였다. 그리고 다양한 잡음 환경에서의 동기신호 검출 모의실험을 통하여 제안한 동기신호와 기존 동기신호의 검출 성능을 비교·분석하였다. 실험 결과로부터 BER이 증가할수록 최대길이 시퀀스로 마스킹한 제안한 방식의 동기신호 검출 성능이 기존 연접 형태의 동기신호 검출 성능에 비하여 상대적으로 더 우수함을 확인할 수 있었다. 제안한 동기신호 생성 및 검출 방법은 특히 BER이 높은 무선 채널에서 운용되는 암호 시스템에 응용이 가능할 것으로 기대된다.

REFERENCES

[1] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, *Handbook of Applied cryptography*, Boca Raton, FL: CRC press, 1996.

[2] W. Stallings and M. P. Tahiliani, *Cryptography and Network Security: Principles and Practice (6th edition)*, London: Pearson, 2014.

[3] H. J. Lee, "Highly reliable synchronous stream cipher system for link encryption," in *Proceedings of International Conference on Computational Science and Its Applications*, pp. 269-278, 2006.

[4] J. H. Yoon, "A non-periodic random sequence resynchronization method using the address data of LAPB and HDLC," Ph. D. Dissertation, Kyungpook National University, Daegu, Korea, 1997.

[5] G. Ascheid and H. Meyr, "Cycle slips in phase-locked loops: a tutorial survey," *IEEE Trans. Communications*, vol. 30, no.10, pp. 2228-2241, 1982.

[6] V. Smirnova and A. V. Proskurnikov, "Phase locking, oscillations and cycle slipping in synchronization systems," in *Proceedings of European Control Conference*, pp. 873-878, 2016.

[7] P. Eliardsson, E. Axell, P. Stenumgaard, K. Wiklundh, B. Johansson, and B. Asp, "Military HF communications considering unintentional platform-generated electromagnetic interference," in *Proceedings of International Conference on Military Communications and Information Systems*, pp. 1-6, 2015.

[8] Witvliet, Ben A. and Rosa Ma Alsina-Pagès. (2017). Radio communication via Near Vertical Incidence Skywave propagation: an overview. *Telecommunication Systems* [Online]. pp. 1-15. Available: http://link.springer.com/article/10.1007/s11235-017-0287-2.

[9] R. J. Sutton, *Secure Communications: Applications and Management*, Chichester, U.K.: John Wiley & Sons, 2002.

[10] S. W. GOLOMB. *Digital communications with Space Applications*, Englewood Cliffs, NJ: Prentice-Hall, 1964.

[11] A. Ahmad, S. S. Al-Busaidi, M. J. Al-Musharafi, "On properties of PN sequences generated by LFSR - A generalized study and simulation modeling," *Indian Journal of Science and Technology*, vol. 6, no 10. pp. 5351-5358, Oct. 2013.

[12] N. S. Abinaya and P. Prakasam, "Performance analysis of maximum length LFSR and BBS method for cryptographic

application," in *Proceedings of International Conference on Electronics and Communication Systems*, pp. 1-5, 2014.

[13] Y. H. Son, J. K. Hong and K. S. Bae, "Authentication masking code against DoS of T-MAC protocol," *Journal of Central South University*, vol. 20, no. 7, pp. 1889-1895, Jul. 2013.

[14] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*, Amsterdam: North-Holland, 1977.

손영호(Young-ho Son)

저자의 요청으로 사진 생략

1999년 2월: 경북대학교 전자공학과 석사
2017년 2월: 경북대학교 전자공학과 박사
2000년~현재: 한국전자통신연구원 부설연구소 책임연구원
※ 관심분야 : 음성신호처리, 디지털신호처리, 정보보호 등

배건성(Keun-sung Bae)

1977년 2월: 서울대학교 전자공학과 학사
1979년 2월: 한국과학기술원 전기 및 전자공학과 석사
1989년 5월: University of Florida 공학박사
1979년~현재: 경북대학교 전자공학부 교수
※ 관심분야 : 음성신호처리, 디지털신호처리, 적응필터링, 패턴인식, 소나/레이더신호처리 등