무선 채널에서의 암호 통신을 위한 동기식 스트림 암호시스템 구현

정회원 홍 진 근*, 손 해 성*, 황 찬 식*, 김 상 훈**, 윤 희 철**

Implementation of Synchronized Stream Cryptosystem for Secure Communication in Radio Channel

Jin-keun Hong*, Hae-sung Son*, Chan-sik Hwang*, Sang-hyun Kim**, Hee-cheol Yun**
Regular Members

요 약

본 논문에서는 실제 무선 채널 환경에 효율적인 암호 통신을 제공하는 동기식 스트림 암호 통신 체계를 설계하였으며, 그 암호 시스템의 비도를 분석하였다. 제안된 시스템의 주요 구성 부분은 동기 패턴, 세션 키, 키 수열 발생기이며, 이에 대한 시스템 성능을 랜덤성, 주기, 선형 복잡도, 상관 면역도에 따라 비도 분석하여 무선 채널에 적합함을 판정하였다. 시뮬레이션 결과는 10-1과 10-2채널 오류 환경에서 영상 신호를 이용하여 암복호의 타당성으로 나타내었다.

ABSTRACT

In this paper, a synchronized stream cryptosystem for secure communication in radio channel is designed and its security level is analyzed. The main parts of the proposed crytosystem consist of synchronization pattern generator, session key generator, and key stream generator. The system performance is evaluated by analyzing the security level depending on the randomness, period, linear complexity, and correlation immunity. Experimental results with image data signal in the 10-1 and 10-2 channel error environment demonstrate the proper operation of the implemented crypto system.

I. 서 론

일반적으로 블록 암호 체계는 블록 단위로 평문을 암복호화함으로 암호문내에 1비트의 오류가 복호화 과정에서 블록 크기 만큼의 에러 확산을 유발하고 이로인해 채널 효율성이 떨어지고 비도 수준의 정량화가 불가능한 단점을 가진다. 이에 반해 스트림 암호 체계는 키수열 발생기를 통해 발생된 난수를 이용하여 암복호화를 수행함으로써 에러 확산이 없고 주기, 선형복잡도, 상관면역도 등과 같은 비도 수준에 대한 정량화가 가능하고 하드웨어 구현이 용이하며 통신 지연이 없다는 장점 등으로 인해 채널 구간의 암호 통신 방식으로 많이 사용된다.[1,2] 본 논문에서는 무선 통신환경에 적합한 암호 통신을 제공하는 스트림 암호 체계를 설계하였으며 제안된 암호 체계는 주요 부분인 주기적인 동기 패턴(Synchronization Pattern ; SP), 세션 키(Session Key; SK), 암호문(Ciphertext) 등으로 구성된다. 제안된 키수열 발생기는 종래의 Geffe 발생기[3]의 취약성인 상관 면역도를 보강한 피드백 메모리를 갖는 수열 발생기에 Meier[4], Dawson[5]이 제안한 합산 수열 발생기로 난수를 발생하며, 설계된 키수열 발생기를 주기, 선형 복잡도, 상관면역도 등의 비도요소를 분석하고, 골드 코드 특성을 이용한 동기 패턴을 발생시켜 이를 무

* 경북대학교 전자공학과 데이터통신시스템 연구실, ** LG정밀연구소
논문번호 : 98334-0803, 접수일자: 1998년 8월 3일

선 채널 환경에 적용시 타당성을 판정하며, 채널 환경에 따른 세션 키의 암복호 성능을 시뮬레이션을 통해 평가한다.

Ⅱ. 스트림 암호 체계

스트림 암호 체계에서 키수열 발생기는 외부 키 입력을 시드 값(seed number)로 하여 무한 주기에 가까운 랜덤 키 수열을 발생시킨다. 그림 1에서는 스트림 암호 시스템의 암복호 과정을 나타낸 것으로서 주기적으로 동기 패턴과 세션 키를 송신측에서 전송하고 수신측에서는 복호를 위해서 송수신측이 공유한 비밀키와 수신된 세션 키를 사용하여 키수열 발생기의 초기 상태 값을 결정하고 주기적으로 동일한 동기 패턴으로부터 동기를 유지한다.

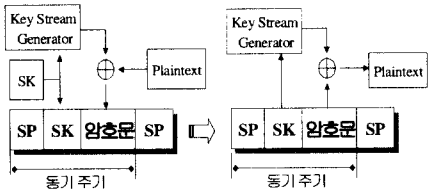


그림 1. 스트림 암호 통신 체계

먼저 주기적인 동기식 스트림 암호 통신 방식을 운용하기 위해서 요구되는 동기 패턴은 송수신이 동일한 값을 가져야 하며, Gold Code Generator [11-12]를 이용하여 발생시키고 그 패턴 길이는 사용하는 채널 환경에 적합하도록 결정되어야 한다. 암호기에서 일정 길이를 갖는 동기 패턴을 평균 BER이 주어진 통신 채널을 통해 전송하면 수신기에서 동기 검출 확률 P_D와 False Alarm 확률 P_{FA}를 유도하여 해당 동기 패턴의 허용 여부를 판별하게 된다. 세션키는 64비트 시드값을 세션키 발생기의 입력으로 하여 생성된 랜덤 수열을 각 64비트씩 분할하여 사용하며 각 세션에 해당하는 암호문을 생성하기 위한 키수열 발생기의 키중 일부분으로 해당 세션키를 이용한다. 세션키에서의 오류는 수신측에서 그 세션의 복호를 불가능하게 하므로 오류 확산을 방지하기 위해 3비트의 오류 정정 기능을 갖는 (15, 4) Maximal Length code[6-7]를 이용하여 64비트 세션키를 240비트로 부호화하여 전송한다. 복호기에서는 동기패턴을 검출하고 240비트 길이를 갖는 오류 정정 부호화된 세션키에서 64비트의 세션키를 복원하여, 송수신측이 공유하고 있는 비밀 키 64비트와 합하여 복호화를 위한 키수열 발생기의 시드 값을 정한다.

스트림 암호 체계에서의 비도 수준은 암호 공격에 강한 키수열 발생기의 설계에 의해 결정되므로 일반적으로 키 수열의 주기에 대한 최대값의 보장, 난수성이 좋음, 높은 상관 면역도를 가질 것, 큰 선형 복잡도를 지닐 것 등의 요구 사항을 만족해야 한다.

1. 주기(Period)

수열 발생기중 1973년 Geffe가 제안한 비선형 시스템은 그림 2와 같은 구조로 3개의 m-LFSR(Maximum Length Linear Feedback Shift Register)로 구성된다. 각 레지스터의 초기치가 0이 아니고, 각 출력 수열이 a_n, b_n, c_n이라하면 다음 식 (1)로 주어지는 출력 수열 g_n을 갖는다.

$$gn = anbn \oplus cn(bn \oplus 1) = anbn \oplus cnbn \oplus cn \qquad (1)$$

이때 m-LFSR1~m-LFSR3의 각 쉬프트 레지스터의 차수가 m, n, k일 때 각 쌍마다 서로 소의 조건에서 발생되는 출력 수열의 주기는 $(2^m - 1)(2^n - 1)(2^k - 1)$[1-2]로 결정된다.

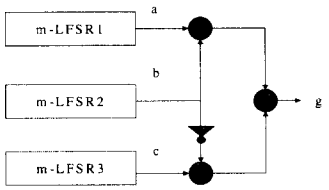


그림 2. m-LFSR로 구성된 Geffe 비선형 시스템

2. 선형 복잡도(Linear Complexity)

Massey[8]의 LFSR 합성법에 의해 얻을 수 있는 선형 복잡도는 임의의 키 수열 발생기가 발생시키는 난수와 동일한 난수를 발생하는 최단의 LFSR로 나타낼 수 있고 일반적으로 선형 복잡도를 증가하기 위해 후단에 비선형 결합기를 추가한다. 상기 비선형 시스템으로부터 유도되는 선형 복잡도는 각 차수가 m, n, k일 때 mn+nk+k의 값으로 결정된다.

3. 상관 면역도(Correlation Immunity)

"어떤 이진 수열이 m차 상관 면역이다"라는 것은 m개의 어떤 입력과도 생성자에 의한 출력 사이에는 통계적인 종속성이 존재하지 않음을 의미한다. 암호

분석과정에서 상관성 공격은 입출력 조합을 함수적으로 분리한 후 키 스트림의 분리 정복 공격을 통해 키를 검출하는 방법이다. J. Siegenthaler[9]는 키 스트림의 분리 정복에 의한 상관 공격에 대응할 수 있는 방법을, R. A. Rueppel[10]은 메모리를 갖는 생성자를 제안하였다. 메모리가 없는 비선형 차수와 상관 면역도 사이에는 k+m ≤ N-1, 1≤m≤N-2와 같은 trade-off 특성이 존재한다.

Ⅲ. 암호기 설계

1. 동기 패턴 발생기

동기 패턴 발생기는 자기 상관특성이 우수한 Gold Code Generator를 이용하여 동기 패턴을 발생시키고 복호기에서는 동기 패턴 검출 과정을 수행하여 수신한 동기 패턴이 검출되면 이어서 수신되는 세션 키를 수신하여 암호문을 복호한다. 무선 채널 구간이 갖는 평균 BER(Bit Error Rate) B는 1비트를 1회 전송시 에러가 발생할 확률을 나타낸다. 암호기에서 n비트의 동기 신호를 송신할 때 복호기에서는 0~n개의 오류를 가진 동기 신호를 수신할 수 있다. 이때 각 오류 개수에 대한 동기 검출 확률 P_{Di}는

$$PDi = nCi\ Bi(1-B)n-i\ i = 0, \quad ..., n \qquad (2)$$

을 통해 얻을 수 있고, 동기를 놓칠 확률 P_{Mi}는 다음과 같다.

$$PMi = 1 - PDi \qquad (3)$$

이때 m개까지의 오류가 발생했을 때의 동기 검출 확률 P_{Dm} 은

$$PDm = \sum_{i=0}^{m} PDi \qquad (4)$$

으로부터 얻는다.

각 오류 개수에 대한 False alarm 확률 P_{Fi}는 채널의 에러로 인해 동기 신호를 잘못 검출할 수 있는 오검출 확률로 다음 식 (5)와 같이 계산된다.

$$PFi = nCi\ (0.5)i(1-0.5)n-i$$
$$= nCi\ (0.5)n\ i=0, \ ..., \ n \qquad (5)$$

이때 m개까지의 오류가 발생했을 때의 False alarm 확률 P_{Fm} 은 다음 식 (6)으로 얻는다.

$$PFm = \sum_{i=0}^{m} nCi(0.5)n \qquad (6)$$

제안된 암호 체계에서는 무선 채널 환경 조건을 BER(Bit Error Rate)가 10^{-1}~10^{-3} 이고 전송속도 16~20Kbps에서 시뮬레이션을 수행하고 이때 각 검출 확률은 식 (4)와 식 (6)를 이용하여 P_{Dm}과 P_{Fm}을 얻을 수 있다. 표 1에서는 동기 패턴 길이를 31비트와 63비트를 사용할 때 무선 채널에서 주어지는 BER에 따라 동기 검출 확률과 False Alarm 에러가 발생하는 확률에 대해 계산한 것이다. 먼저 31비트의 동기 패턴 길이에서 동기 검출 확률은 10^{-1}에서 비트 여유를 2비트까지 허용할 때 검출 확률은 38.13%의 확률로부터 8비트까지 허용할 경우 해당 검출 확률은 99.27%에 해당한다. 그러므로 31비트의 동기 패턴을 사용할 경우 10^{-1}의 열악한 채널 환경에서 99%이상의 동기 검출 확률을 갖기 위해서는 적어도 8비트 이상의 오류를 허용해야만 한다. 통신 채널의 상태가 호전될수록 적은 허용 오류 개수에서 높은 검출 확

표 1. 31/63비트 동기 패턴 길이에서 각 BER에 따른 PDm, PFm

SP	31 bits					63 bits				
	10^{-1}	10^{-2}	10^{-3}	$P_{False\ Alarm}$		10^{-1}	10^{-2}	10^{-3}	$P_{False\ Alarm}$	
P_{D0}	0.0385	0.7323	0.9694	P_{F0}	4.6570E-10	0.00131	0.5309	0.9389	P_{F0}	1.084E-19
P_{D1}	0.1696	0.9616	0.9994	P_{F1}	1.4900E-08	0.01048	0.8687	0.9980	P_{F1}	6.938E-18
P_{D2}	0.3813	0.9963		P_{F2}	2.3140E-07	0.04206	0.9745		P_{F2}	2.186E-16
P_{D3}	0.6163	0.9997		P_{F3}	2.3240E-06	0.11342	0.9962		P_{F3}	4.524E-15
P_{D4}	0.7991	0.9999		P_{F4}	1.6970E-05	0.23235			P_{F4}	6.911E-14
P_{D5}	0.9088			P_{F5}	9.6090E-05	0.38829			P_{F5}	8.312E-13
P_{D6}	0.9617		99.94%	P_{F6}	4.3893E-04	0.49569		99.8%	P_{F6}	8.198E-12
P_{D7}	0.9827		↓	P_{F7}	1.6634E-03	0.64731	99.6%	↓	P_{F7}	6.818E-11
P_{D8}	0.9927	99.99%		P_{F8}	1.1105E-02	0.76517	↓		P_{F8}	4.881E-10
P_{D9}	0.9938	↓		P_{F9}	3.1704E-02	0.84520			P_{F9}	3.054E-09
P_{D10}	0.9933			P_{F10}		0.89326			P_{F10}	
P_{D11}	0.9933			P_{F11}		0.91897			P_{F11}	
P_{D12}	0.9933			P_{F12}		0.93135			P_{F12}	

률을 가질 수 있다.

표 2. 주어진 시간에서 채널율에 따른 False Alarm확률

시간간격 (T)	$P_{v \cdot T}$	Channel Rate(v)	
		16Kbps	20Kbps
10년	P'_{F1}	1.982E-13	1.585E-13
5년	P'_{F2}	3.964E-13	3.171E-13
1년	P'_{F3}	1.982E-12	1.585E-12
6개월	P'_{F4}	4.020E-12	3.215E-12
4개월	P'_{F5}	6.028E-12	4.823E-12
2개월	P'_{F6}	1.206E-11	9.645E-12
1개월	P'_{F7}	2.411E-11	1.929E-11
15일	P'_{F8}	4.822E-11	3.858E-11
10일	P'_{F9}	7.234E-11	5.787E-11
5일	P'_{F10}	1.447E-10	1.157E-10

실제 10^{-3}의 채널에서 동기 검출 확률은 2개 정도의 오류를 허용할 경우 99% 이상의 검출 확률을 갖는다. 복호화 과정에서 동기 패턴을 검출하고자 할 때 동기 패턴의 비트를 31비트를 사용한다고 가정하면, 동기 패턴 검출기에서는 전송되는 31비트와 자체적으로 발생기로부터 발생하는 31비트 동기

패턴에 대해 여유비트를 두고 비교를 하므로써 동기 패턴의 검출을 성공 또는 실패로 판별하게 된다. 이때 여유비트를 2비트로 결정한다고 하면, 31비트의 동기 패턴 가운데 적어도 2비트 이하의 패턴 불일치가 발생할 경우 동기 패턴의 검출을 성공한 것으로 판별한다. 그러므로 동기 패턴의 길이 31비트나 63비트를 사용할 경우 여유비트의 결정과 얼마의 통신 기간 동안 오검출 오류로부터 보장되는 통신을 제공할 것인가에 대한 결정이 암호체계의 신뢰성을 제공하는 요인이 된다. 동기 패턴의 여유비트에 대한 결정은 표 2에서 제공하는 16Kbps와 20Kbps채널 환경과 주어진 시간으로부터 유도할 수 있고 이것을 표 1에서 제공하는 오검출 확률과의 관계로부터 구할 수 있다. 16Kbps와 20Kbps 전송속도를 제공하고 63비트의 동기 패턴 길이를 사용하는 암호 체계에서 오검출이 발생하는 주기를 1년으로 할 때 P_{Fm}은 1.982×10^{-12}와 1.585×10^{-12}이고, 이때 표 1에서 P_{Fm}가 상기 확률을 만족할 조건은 63비트 가운데 여유 비트가 5~6비트 일때이다.

63비트의 동기 패턴을 사용할 경우 1년의 기간 동안 여유비트를 5~6비트 이상 두어 오 검출 비트가 발생하더라도 해당 동기 패턴으로 판별하는 데 반해, 31비트를 사용하는 경우 확률적인 계산으로부터 유도되는 식에서는 0비트의 여유 비트도 허용하지 않으며 해당되는 오검출 발생기간 또한 5일이하의 경우이므로 이론으로는 거의 매일 발생한다고 볼 수 있다. 그러나 실제 시스템에서 암호 통신 시간이 종래의 유선망을 이용하는 통신 시간과는 달리 상당히 짧은 시간 동안 이루어지고 자기 상관도의 특성을 이용하므로써 3비트의 여유 비트를 주어 동기를 검출할 경우 종래의 유사통신 방식을 고려해 볼 때 적용가능하리라 예측된다.

2. 세션키 발생기

세션키 발생기는 다음 그림 3과 같이 비선형 키수열 발생기로 한다.

출력함수 y_j는 LFSR1의 출력 수열 a_j와 LFSR2의 출력 수열 b_j, 이전 carry c_{j-1}(carry의 초기값은 0), 이전 피드백 메모리 비트 D_{j-1} 의 전가산기를 통해 비선형으로 구해지고 각 출력은 다음 식과 같이 표현된다.

$$yj = (aj \oplus bj \oplus Cj\text{-}1) \oplus Dj\text{-}1 \quad (7)$$

$$Cj = ajbj \oplus (aj \oplus bj)Cj\text{-}1 \quad (8)$$

$$Dj = bj \oplus (aj \oplus bj)Dj\text{-}1 \quad (9)$$

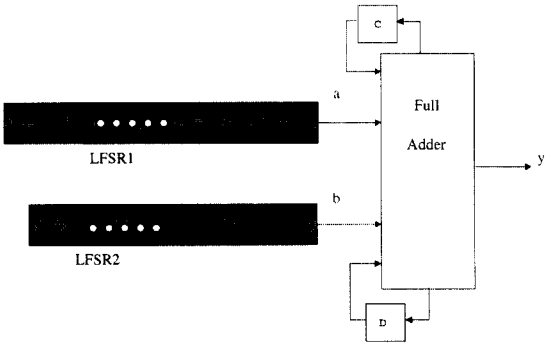


그림 3. 비선형 세션키 발생기

이때, j=0,1,2,...이다. 이 수열 발생기는 전가산기만으로 구성된 기존 발생기의 carry와 출력간의 상관 확률이 1/4로 매우 커서 상관공격에 취약하지만 feedback memory 함수를 추가하여 상관 확률이 1/2인 함수로 개선된 알고리즘을 사용하였다. 개선된 비선형 세션키 수열 발생기의 선형 복잡도는 주기 P가 (231-1)(261-1)에 근접하며 상관 면역도는 최고 차수를 갖는다.

3. 키수열 발생기

키수열 발생기는 출력 비트 수열의 선형 복잡도, 랜덤 특성, 상관 면역도 등을 고려하여 비선형 함수로 되어야 한다. 제안된 키수열 발생을 위해 사용된 비선형 키수열 발생기는 각 LFSR 주기의 단수가 31, 61, 91이 서로 소로서 전가산기를 통해 구성하였으며 다음 그림 4에서 제시한다.

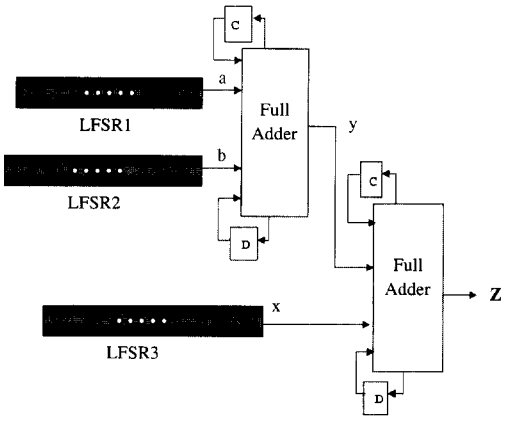


그림 4. 비선형 키수열 발생기

상기 그림 3에서의 세션키 발생기 원리와 동일하게 설계된 비선형 키수열 발생기는 비도측면에서 표 3에서 제시하는 바와 같이 무선 채널에 적용 가능한 비도 능력을 갖는다. 비선형 키수열 발생기가 갖는 비도는 주기가 $(2^{31}-1)(2^{61}-1)(2^{91}-1)$으로 10^{55}을 갖도록 설계하였으며, 선형 복잡도는 주기에 근접하도록 하였고 상관 면역도는 최고의 차수를 갖도록 하였다.

Ⅳ. 비도 요소 및 시뮬레이션 분석

암호체계를 설계하기 위해서는 랜덤 특성의 검정, 주기, 선형 복잡도, 상관 면역도, 키 수열의 수 등의 분석을 통해 적합성 판정이 요구된다. 본 장에서는 랜덤 특성을 검정하고 무선 환경에서의 암호체계를 시뮬레이션을 수행하고 이에따른 결과를 분석하고자 한다.

1. 랜덤 특성 검정

키수열 발생기의 전체 주기로부터 발생된 키 스트림으로부터 랜덤 특성을 검정하는 것은 불가능하므로 적당한 비트 길이를 사용하여 국부적인 랜덤 특성 검정을 수행한다. 이에 대한 검정 방법으로는 chi-square test를 사용하여 적합도를 평가하며 이에 대한 유의 수준 결정은 일반적으로 5%의 유의수준을 만족하게 되면 적합하다고 판정한다. 일반적인 검정 항목으로는 frequency test, serial test, t-serial test, poker test 및 autocorrelation test 등[12]이 있다.

다음 표3에서는 설계된 키수열 발생기를 이용하여 얻은 출력 비트 20만 비트를 초기치(initial seed number)를 달리하여 랜덤 검정을 수행한 결과를 나타낸 것으로 검정 항목에 따라 얻은 결과를 살펴볼 때 정의하는 유의 수준을 통과함으로써 시스템에 적용시 적합하다고 평가된다.

표 3. 설계된 키수열 발생기의 랜덤 특성 검정 결과

Test item	유의 수준 (5%)	test 결과	
		initial seed 1	initial seed 2
frequency test	3.841	0.891	1.414
serial test	5.991	2.135	1.520
generalized t-serial test(t=3)	9.488	4.090	1.855
〃 (t=4)	15.507	12.484	3.885
〃 (t=5)	26.296	20.755	9.446
poker test (length=3)	14.067	5.700	6.658
〃 (length=4)	24.996	19.930	11.340
〃 (length=5)	44.654	34.604	26.077

2. 무선 환경에 따른 암호 체계 시뮬레이션 및 분석

본 논문에서 제안하는 암호 체계의 암호화 구성도를 다음 그림 5에서 나타내고 있다.

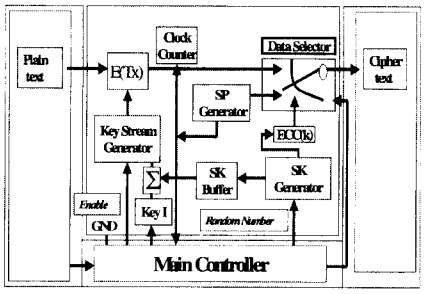


그림 5. 제안된 암호 체계의 암호화 구성도

먼저 주 제어기에서는 암호 체계를 구성하는 각

표 4. 31비트 동기패턴 길이를 사용할 때 채널환경과 검출 여유로 인한 오류비트

31bits SP길이	2400				4800				9600			
	BER1 (10^{-1})	BER2 (10^{-2})	BER3 (10^{-3})	BER4 (10^{-4})	BER1 (10^{-1})	BER2 (10^{-2})	BER3 (10^{-3})	BER4 (10^{-4})	BER1 (10^{-1})	BER2 (10^{-2})	BER3 (10^{-3})	BER4 (10^{-4})
m1(여유비트 1)	232828	15939	527	51	228595	21759	522	52	224130	22151	521	53
m2(여유비트 2)	219495	6217	527	51	212146	7331	522	52	217090	5240	521	53
m3(여유비트 3)	211305	5235	527	51	199944	7331	522	52	212808	5240	521	53
m4(여유비트 4)	257129	5235	527	51	245969	7331	522	52	248827	5240	521	53
m5(여유비트 5)	250477	5235	527	51	245399	7331	522	52	250490	5240	521	53
m6(여유비트 6)	250799	5235	527	51	258464	7331	522	52	250518	5240	521	53

부분 시스템의 동작 기능을 제어한다. 주 제어기의 신호를 통해 세션 키를 생성하고 생성된 그 세션키를 이용하여 랜덤 키수열을 발생시킨다. 이때 키수열 발생기를 통해 수열을 발생하기 위해서는 주 제어기에서의 신호를 받아야 한다. 평문은 발생된 키수열의 출력으로부터 암호화 과정을 수행하게 되고, 전송되는 주기적인 연속체계의 암호화 방식에서 주 제어기는 암호화된 암호문(E(Tx))과 동기패턴(SP Generator), 그리고 오류 정정 부호화된 세션 키(ECC SK)로 구성된 주기적인 동기 구조를 갖는 암호 체계의 타이밍(Data Selector)을 제어한다.

(1) 동기 패턴 발생기의 분석

부가 비트량은 정보량의 효율성 측면에서 고려되는 중요한 인자로 실제 발생되는 동기 패턴의 길이는 검출 확률과의 관계로부터 실제 통신에서 적합한 길이를 얻게 된다.

P_D에 따르면 31비트 동기 패턴 길이를 사용하고 비트 여유를 주지 않을 때, BER에 대한 동기 검출 확률은 10^{-1}채널 오류에서 3.8%, 10^{-2}채널 오류에서 73.2%, 10^{-3}채널 오류에서 96.9%의 검출 확률을 가진다. 실제 유선망 통신 환경과는 달리 짧은 기간 동안 통신이 이루어지므로 동기 패턴의 검출시 유효 여유 비트를 주게 되면 열악한 통신 환경인 10^{-1}채널 상태 이외에서는 정확성을 가지고 적용가능하리라 판단된다. 63비트 동기 패턴 길이를 사용하고 7비트의 여유 비트를 줄 때, BER에 대한 검출 확률은 10^{-1}채널 오류에서 64.7%, 10^{-2}채널 오류에서 99%, 10^{-3} 채널 오류에서 99%을 보장한다. 63비트 경우 16Kbps와 20Kbps에서 5~6개 오류가 발생할 경우 동기 검출시 오검출에 대한 오류가 1년이상을 보장한다. 그러나 실제 시스템에 적용할 때 표 4에서 살펴 볼 수 있듯이 동기 주기를 각 2400, 4800, 9600bits의 환경을 주고, 31비트로 구성된 동기 패턴 길이를 사용할 때 1~3비트의 비트 여유를 줌으로써 비트 여유에 대한 복호화된 데이터와 원래의 데이터 비트차에 관한 결과를 통해 동기 패턴 검출 가능성을 판단할 수 있다. 예를 들면 2400bits 경우 10^{-3} 환경에서 여유 비트를 1비트 주는 경우와 3비트 주는 경우 복호화 과정에서 동기 패턴은 검출가능하고 세션 키나 기타 데이터로부터 오류(527비트)가 발생한 것으로 판단할 수 있다. 31비트 동기 패턴을 사용할 경우 확률적인 계산에서 1비트의 여유를 허용하지 않으나 실제 시스템에서 동기 패턴을 검출함으로써 짧은 무선 통신 구간과 자기 상관성을 고려할 때 3비트의 여유를 허용할 경우에도 적용가능하리라 판단된다.

10^{-1}~10^{-4}의 채널 환경의 복호화 과정에서 발생되는 오류 비트양은 비트 여유에 따라서 달리 나타난

표 5. 63비트 동기패턴 길이를 사용할 때 채널환경과 검출 여유로 인한 오류비트

63bits SP길이	2400				4800				9600			
	BER1 (10^{-1})	BER2 (10^{-2})	BER3 (10^{-3})	BER4 (10^{-4})	BER1 (10^{-1})	BER2 (10^{-2})	BER3 (10^{-3})	BER4 (10^{-4})	BER1 (10^{-1})	BER2 (10^{-2})	BER3 (10^{-3})	BER4 (10^{-4})
m1(비트여유 1)	241869	39447	1449	51	243511	48714	523	51	243464	47469	521	53
m2(비트여유 2)	239760	12828	534	51	240417	13513	523	51	243464	22035	521	53
m3(비트여유 3)	236088	6200	534	51	237679	9428	523	51	240861	9447	521	53
m4(비트여유 4)	229571	5250	534	51	226055	7420	523	51	231830	5241	521	53
m5(비트여유 5)	215056	5250	534	51	221910	7420	523	51	222489	5241	521	53
m6(비트여유 6)	206997	5250	534	51	210418	7420	523	51	209536	5241	521	53

다. BER1 즉 10^{-1}의 채널에서는 ≒$6x10^5$데이터를 암호화시 평균 10회에 걸쳐 실험을 해본 결과 원 데이터의 40%에 해당하는 데이터 오류가 발생하고 발생된 비트 오류는 여유 비트에 따라 약간의 차이를 가지고 달리 나타난다. 그러나 BER2(10^{-2})의 경우 오복호 데이터의 비트량이 급격히 줄었다. 이는 채널 환경에 따라 동기 패턴, 세션키의 영향 정도를 나타내는 것으로 10^{-1}의 열악한 환경에서는 동기 패턴과 세션키의 오검출 확률이 상당히 높으므로 데이터 통신이 상당히 어렵다. 동기 패턴의 1회 검출 실패는 적게는 2400bits 동기 주기 구조에서 평균적으로 ≒1200bits에 달하는 오류가 발생하고, 9600bits의 동기 구조에서는 ≒4800bits 정도의 오검출을 초래한다. 63비트의 동기 패턴 길이를 사용할 경우 6비트의 여유 비트를 가지고 즉, 63비트의 비트중 57비트가 일치를 보이는 패턴에 대해 동기 패턴으로 인식하게 되고 동기 패턴이 검출되면 주 제어기에서는 세션키를 검출후 해당 암호문을 검출하여 복호화 과정을 수행하게 된다. 이때 무선 채널환경에서 암호 체계를 실험할 때 채널 환경에 따른 검출 여유에 대한 오류 비트량을 다음 표5에 나타내었다.

제시된 동기 주기가 9600비트이고 BER이 10^{-2} 인 열악한 통신 채널에서 동기 비트 검출시 여유 비트를 1비트를 주게되면 전체 복호 비트에서 47469비트의 오복호 데이터 오류를 얻게 되고 여유비트를 4~6비트로 주고 동기 패턴을 검출하면 이때 복호된 데이터 가운데 5241비트의 오복호 데이터를 얻게 된다. 실제 통신에서 아주 열악한 환경인 10^{-1}인 BER의 상태를 제외하고는 주기적인 암호 체계에서 동기 패턴의 검출 가능성은 높다고 판단한다.

(2) 무선 환경에서 암호 체계의 시뮬레이션 결과

무선 채널 오류에 따른 오복호 데이터 비트율은 각 BER의 상태 즉, 10^{-1}~10^{-4}에서 31비트 동기 패턴 중 비트 여유 2비트를 주고 동기 패턴을 검출하여 복호 과정을 수행했을 때 오복호 데이터를 그림 6에서 제시하고 있다. ≒$6x10^5$bits 중 40%에 해당하는 비트가 10^{-1} 채널에서 오류가 발생하고, BER2 즉, 10^{-2}에서 1%, 그 이외의 통신 채널 환경에서 거의 완전한 통신이 이루어지는 것으로 판단할 수 있다. 또한 2400, 4800, 9600bits 각각의 동기 주기에 따른 오복호 비트에 대한 분포는 2400bits의 경우 동기패턴, 세션키의 삽입 주기가 짧으므로 10^{-1}에서는 오히려 4800 bits 보다 많은 오복호 bits를 초래한다. 그러나 전반적으로 1회 동기가 깨어지거나 세션키가 깨어지면 그것은 다음 동기 데이터가 수신되기 이전까지 전구간이 오복호되는 경우가 발생한다. 세션키의 관리는 (15,4) Maximal Length Code를 통해 오류정정을 처리하므로써 10^{-1} 채널을 제외하고는 세션키의 정상적인 복호의 가능성이 높게 나타난다.

31비트와 63비트의 동기 패턴 구조를 갖는 암호 체계의 복호성능에 관하여 그림 7과 8에서 제시하였다. 10^{-1}채널의 경우 거의 줄무늬(검정색)가 나타나는 부분이 동기패턴의 검출 실패로 인한 오복호 부분이고, 다양한 명암의 차이가 나타나는 부분이 세션키의 오검출로 인한 부분이다. 10^{-2} 채널에서 동기 패턴은 거의 검출 성공이 이루어지고 세션키 부분은 일부 깨어지는 부분을 볼 수있다. 10^{-3}이상의 경우 정상적인 통신이 이루어지는 것을 볼 수 있다.

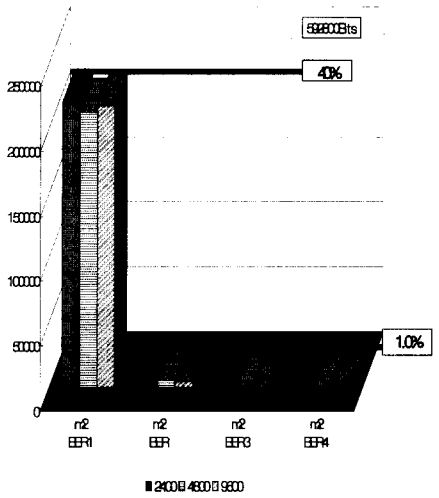
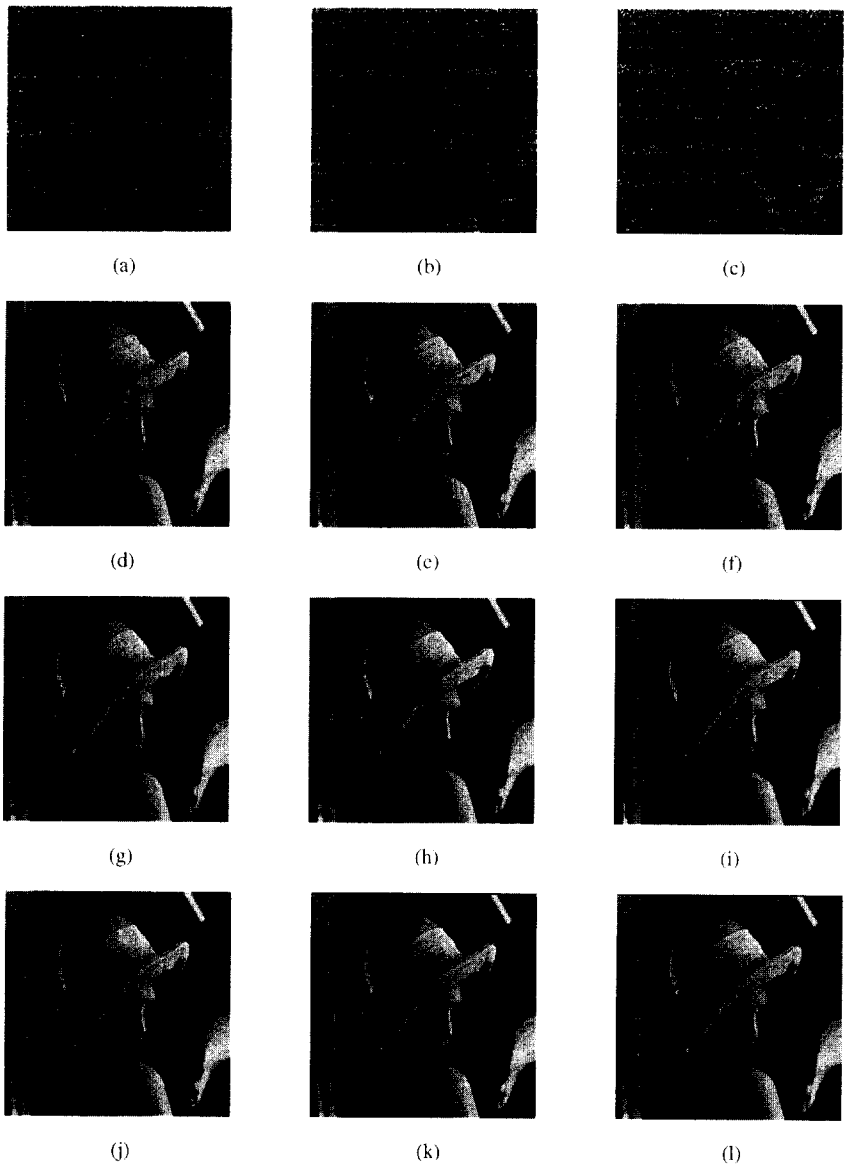


그림 6. 무선채널 에러에 따른 오복호 데이터 비트율

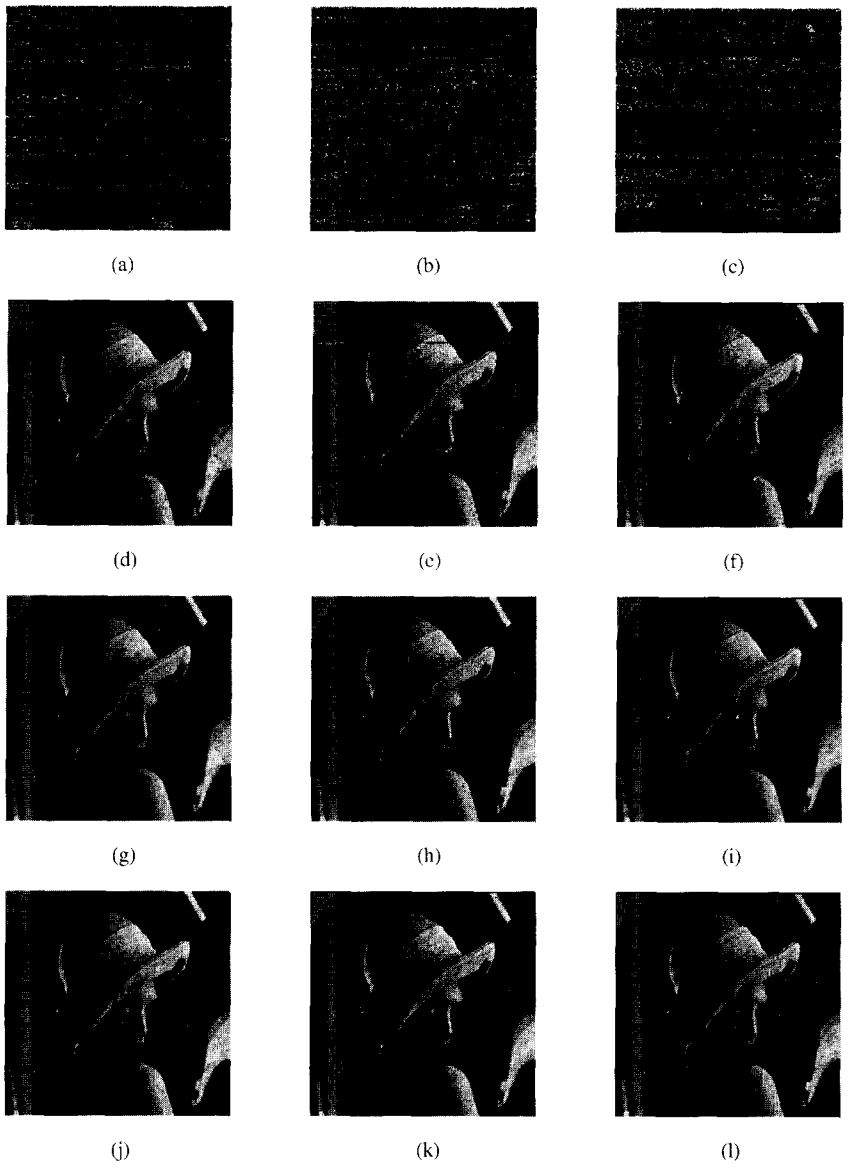
그림 7과 8은 무선 환경의 채널오류에 따른 오복호 데이터를 나타낸 것으로 암호체계가 채널 환경에 직접적인 영향을 받는 것을 볼 수 있다. 소요 비트중 무선 환경의 채널 오류가 10^{-1} 경우 각 2400/4800/9600비트의 동기 주기에 대해 거의 40%의 비트가 오복호된 데이터 비트량으로써 얻을 수 있지만 채널 상태가 호전됨에 따라 오복호된 데이터 비트 수는 급격히 감소한다. 이는 동기 비트의 정확한 검출이 암호 체계에서 복호의 정확성에 중대한 영향을 미치는 것을 볼 수 있다.

암호 체계에서 복호된 데이터는 채널의 오류로 인한 동기 패턴의 오검출, 세션 키의 오복호, 데이터의 변조 등의 영향을 받는다. 그림 7과 8에서는 31비트



(a) BER = 10^{-1}, 2400 bits
(b) BER = 10^{-1}, 4800 bits
(c) BER = 10^{-1}, 9600 bits
(d) BER = 10^{-2}, 2400 bits
(e) BER = 10^{-2}, 4800 bits
(f) BER = 10^{-2}, 9600 bits
(g) BER = 10^{-3}, 2400 bits
(h) BER = 10^{-3}, 4800 bits
(i) BER = 10^{-3}, 9600 bits
(j) BER = 10^{-4}, 2400 bits
(k) BER = 10^{-4}, 4800 bits
(l) BER = 10^{-4}, 9600 bits

그림 7. 31비트 동기 패턴에서 무선 채널에 따른 복호된 영상



(a) BER = 10^{-1}, 2400 bits
(b) BER = 10^{-1}, 4800 bits
(c) BER = 10^{-1}, 9600 bits
(d) BER = 10^{-2}, 2400 bits
(e) BER = 10^{-2}, 4800 bits
(f) BER = 10^{-2}, 9600 bits
(g) BER = 10^{-3}, 2400 bits
(h) BER = 10^{-3}, 4800 bits
(i) BER = 10^{-3}, 9600 bits
(j) BER = 10^{-4}, 2400 bits
(k) BER = 10^{-4}, 4800 bits
(l) BER = 10^{-4}, 9600 bits

그림 8. 3비트 동기 패턴에서 무선 채널에 따른 복호된 영상

와 63비트의 동기 패턴의 길이를 정의하여 설계된 암호체계에서 적정한 채널 오류를 삽입함으로써 복호시 발생하는 오류를 파악하고 있다. 일반적으로 긴 줄무늬형태의 선이 2400bits에서는 얇게, 4800bits에서는 9600bits보다는 가늘지만 어느 정도 굵기를 갖게 된다. 이것은 동기 패턴의 오검출로 인해 오복호된 데이터 비트량의 길이 정도를 나타낸 것으로 하나의 동기가 깨어지면 다음 동기를 맞추기까지 해당 데이터는 오복호된다. 채널 에러율에 따라 부분적으로 발견되는 포인터(점)들은 데이터에서 오복호된 것을 의미한다. 해당 암호 체계에서는 동기 패턴의 여유 비트를 31비트에서는 3비트를, 63비트에서는 6비트를 할당하여 여유 비트 이하의 경우 동기 패턴으로 판단한다. 10^{-1} 채널 오류 환경에서는 거의 통신이 어려운 상태로 파악되며 그 이외의 채널에서는 통신이 가능한 상태를 나타내고 있다. 또한, 동기 주기에 대한 결정은 2400bits 또는 4800bits가 적절할 것으로 판단되며, 이것은 16Kbps에서 샘플된 음성 데이터가 20Kbps로 전송될 때 4Kbps의 오버헤드에 대한 여유를 가진다는 것을 고려한다면 2400bits 또는 4800bits마다 동기 주기를 갖는 것이 적합하다. 동기 패턴 길이에 대한 결정은 오버헤드를 고려하거나 False Alarm의 확률적인 계산을 유도할 때, 그리고 짧은 무선 통신 시간을 고려할 때 31bits 또는 63bits의 길이를 사용하는 것이 적합할 것으로 판단된다.

V. 결 론

본 논문에서는 실제 무선 채널에 효율적인 암호 통신을 제공하는 동기식 스트림 암호 통신 체계를 설계하였다. 시스템의 주요 구성 부분인 동기 패턴, 세션 키, 키수열 발생기의 설계 및 이에 대한 시스템 성능을 랜덤성, 주기, 선형복잡도, 상관면역도에 따라 비도 측면에서 분석하여 무선 채널에 적용시 적합성을 판정하였다. 영상 샘플 데이터를 이용하여 시스템에 적용하여 수행한 결과 10^{-1}의 채널 오류 환경에서는 동기 검출의 효율성이 상당히 떨어지며 10^{-2}이상의 채널 오류 상태에서는 비교적 동기 검출이 무난할 것으로 판단된다. 세션 키의 검출은 (15,4) Maximal Length Code를 사용함으로써 오복호의 효율성이 나쁘지 않는 것으로 판단된다.

참 고 문 헌

[1] Van Til borg, H. C. A., An Introduction to Cryptology, KLUWER ACADEMIC PUBLISHERS, Boston, etc., 1988.

[2] H. J. Beker and F. C. Piper, Cipher Systems : The Protection of Communications, Northwood Books, London, 1982.

[3] P. R. Geffe, "How to Protect Data with Ciphers that are really hard to break," Electronics, pp. 99-101, Jan, 1973.

[4] W. Meier and O. Staffelbach, "Correlation Properties of Combiners with Memory in stream ciphers," Journal of Cryptology, vol. 5, pp. 67-86, 1992.

[5] E. Dawson, "Cryptoanalysis of Summation Generator," Advances in Cryptology AUSCRYPT '92, Lecture Notes in Computer Science, Springer -verlag, pp. 209-215, 1993.

[6] M. Simon, Spread Spectrum Communications Handbook, McGraw-Hill, 1994.

[7] M. Y. Lee, Error Correcting Coding Theory, McGraw-Hill, 1989.

[8] J. L. Massey, "Shift Register Synthesis and BCH Decoding," IEEE Trans. on Infor, Theo., Vol. IT-15, No. 1, pp. 122-127, Jan, 1969.

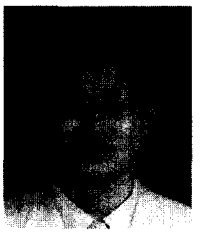
[9] T. Siegenthaler, "Correlation Immunity of Nonlinear Combining Function for Cryptographic Applications," IEEE Trans. on Infor, Theo, Vol.IF-30, NO. 5, pp. 776-780, Sep, 1984.

[10] R. A. Rueppel, "Correlation Immunity and the Summation Generator," Advances in cryptology, Proceedings of CRYPTO '85, pp.260-272, 1985.

[11] R. C. Dixon, Spread Sprectrum Systems, New York Wiley, 1976.

[12] M. Simon, Spread Spectrum communications Handbook, Mcgraw-Hill, 1994.

홍 진 근(Jin-keun Hong) 정회원



1994년 2월 : 경북대학교 전자 공학과 석사

1996년 3월~현재 : 경북대학교 전자공학과 박사과정

<주관심 분야> 초고속망, 암호통신

손 해 성(Hae-sung Son) 비회원

1997년 2월 : 경북대학교 전자공학과 졸업
1999년 2월 : 경북대학교 전자 공학과 석사
<주관심 분야> 암호통신

황 찬 식(Chank-sik Hwang) 정회원

1977년 2월 : 서강대학교 전자공학과 졸업
1979년 8월 : 한국과학기술원 전기전자공학과 석사
1996년 2월 : 한국과학기술원 전기전자공학과 박사
1991년 8월~1992년 8월 : UTA 방문교수
1979년 9월~현재 : 경북대학 교 전자전기공학부 교수
<주관심 분야> 초고속망, 암호통신, 영상통신

김 상 훈(Sang-hyun Kim) 비회원
1999년 현재 : LG정보통신(주) 선임연구원

윤 희 철(Hee-cheol Yun) 비회원
1999년 현재 : LG정보통신(주) 책임연구원