通信情報保護學會論文誌
第 11 券 第 1 號, 2001. 2

무선암호시스템에서 전송성능 개선을 위한 동적할당 알고리듬

홍 진 근*, 윤 장 홍*, 장 병 화*, 황 찬 식**

Dynamic Allocation Algorithm for enhancement of transmission performance on a radio encryption system

Jinkeun Hong*, Janghong Yoon*, Byunghwa Jang*, Chansik Hwang**

요 약

본 논문은 무선채널에서 안전한 암호통신을 위해 동기식 스트림 암호시스템을 설계하였다. 페이딩 채널에서 설계된 스트림 암호를 통해 암호문을 전송할 때 한 주기 동안 발생하는 동기패턴, 세션키, 암호문 정보에 적합한 인터리빙 기법을 설계하여 전송함으로써 버스트 오류로부터 암호문을 보호하고 전송성능을 개선하여 robust한 암호통신을 가능하도록 하였다. 본 논문에서는 동적인 인터리빙 depth를 갖는 DAA를 적용함으로써 정적인 인터리빙 depth를 갖는 SAA (static allocation algorithm)보다 전송성능 개선을 얻었다.

ABSTRACT

In this paper, a synchronized stream encryption system for secure link layer communication in a radio channel is designed. Interleaving scheme which is used to enhance the transmission performance over a fading channel is applied to the encrypted information. A designed synchronous stream cipher system consists of a keystream generator, a synchronization pattern generator and a session key generator. The structure of a synchronous stream cipher system with periodic synchronization is composed of the encrypted information which consists of a synchronization pattern, an error correcting coded session key, an encrypted data in a period of synchronization. In this paper, interleaving scheme using dynamic allocation algorithm(DAA) is applied the encrypted information. The BER of the DAA has been slightly higher than that of the SAA(static allocation algorithm).

keyword : *synchronous stream cipher system, interleaving scheme*

Ⅰ. 서 론

최근 이동중에 장소와 거리에 제약없이 데이터 송수신에 관한 무선 데이터통신 시스템 개발에 대한 관심이 고조되고 있다. 이러한 가운데 무선 데이터통신의 서비스 요구에 발맞추어 선결해야 할 과제는 보안에 대한 위협요소들로부터 보호대책 수립이다.[1~2] 무선 데이터통신에서 고려되는 보안 위협요소에는 불법사용, 도청(eavesdropping), 가로채기(interception), 전파교란(jamming), 정보유출, 파괴, 수정 등이 있다. 블록 암호시스템의 경우 블록단위로 평문을 암복호화함으로써 암호문내에 1비트의 오류가 복호화 과정에서 블록 크기 만큼의 오류 확산을 유발하고 이로 인해 채널 효율성이 떨어지고 비도 수준의 정량화가 불가능한 단점을 가진다. 이에 반해 스트림 암호시스템의 경우 키수열 발생기를 통해 발생된 난

* ETRI 부설 국가보안기술연구소(jkhong@etri.re.kr)
** 경북대학교 전자전기공학부

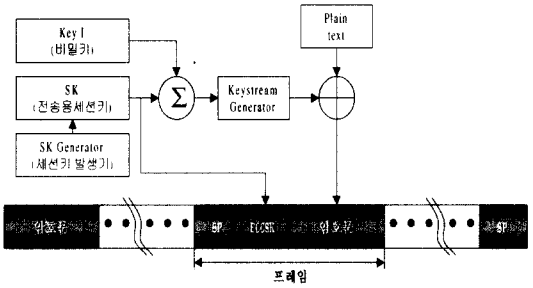
수를 이용하여 암복호화를 수행함으로써 오류 확산이 없고 주기, 선형복잡도, 상관면역도 등과 같은 비도 수준에 대한 정량화가 가능하고 하드웨어 구현이 용이하며 통신 지연이 없다. 이와 같은 암호시스템의 특성으로 인해 스트림 암호시스템은 송수신 링크의 암호통신 방식에 많이 사용되고 있다.[3] 스트림 암호정보를 무선 전송로에 적용하면 다중경로 페이딩, 간섭 등의 열악한 채널 환경으로 인해 다량의 버스트 오류가 발생할 수 있는데 특히 레일레이 페이딩(Rayleigh fading)과 같이 반사파로만 구성된 전파환경의 경우 페이딩 영향으로 인해 버스트 오류가 수십~수백 비트에 걸쳐서 발생한다. 인터리빙 기법은 통신채널에서 발생하는 버스트 오류특성을 고려하여 송신측에서 전송하고자 하는 정보를 확산시켜 전송함으로써 버스트 오류를 랜덤 오류의 특성을 갖도록 처리하여 전송성능을 개선한다. 본 논문에서는 암호통신을 위해 동기식 스트림 암호시스템을 설계하였고 동기패턴, 오류정정 부호화된 세션키, 암호문으로 구성되는 암호정보에 인터리빙 기법을 적용하여 전송성능을 개선하였다. 이때 적용된 동기식 스트림 암호시스템의 적용구조는 한 주기단위의 동기패턴, 오류정정 부호화된 세션키, 암호문으로 이루어진다. 주기적인 동기식 스트림 암호시스템의 경우 한 동기주기내의 동기패턴의 손실과 세션키의 오류는 한 프레임의 암호문 손실을 초래한다. 그런데 버스트 오류의 경우 채널환경에 따라 수십비트 이상의 오류비트가 연속적으로 발생하게 되므로 전송되는 암호정보의 한 프레임내에 이와 같은 버스트 오류가 발생하게 되면 특히 동기패턴 부분이나 세션키 부분에 발생하게 되면 프레임 손실 및 오복호로 인해 암호통신이 불가능하게 된다. 이를 해결하기 위해 채널의 전송성능을 개선하기 위한 기법으로 사용되는 인터리빙을 암호정보에 적용하였다. 수십비트이상 발생하는 버스트 오류를 랜덤 오류로 확산시킴으로써 동기패턴과 세션키 부분에 버스트 오류가 발생하여 프레임이 손실될 확률을 감소시켜 전송성능을 개선하고자 한다. 동기패턴의 경우 한 프레임의 시작과 끝을 지시하는데 만일 동기패턴에 버스트 오류가 발생하면 동기패턴을 검출할 수 없음으로 해당 프레임은 손실이 발생한다. 따라서 인터리빙을 통해 버스트 오류를 랜덤 오류로 확산함으로써 동기패턴의 손실을 감소시킬 수 있고 이를 통해 프레임의 손실률을 감소할 수 있다. 세션키의 경우 오류정정능력을 갖는 비트이상의 버스트 오류가 발생하면 해당 세션의 암호정보는 정상적인 복호가 불가능하다. 그러므로 인터리빙을 통하여 세션키 부분에서 발생되는 버스트 오류를 랜덤 오류로 확산함으로써 세션키에서 발생하는 오류율을 감소시킬 수 있다. 버스트 오류로 인한 전송성능의 열화를 해결하기 위해 암호정보에 인터리빙 기법을 적용하여 전송함으로써 암호문의 전송성능을 평가하였다. 적용된 동기식 스트림 암호시스템의 프레임은 9600비트 프레임 구조에서 실험하였다. 전송성능은 채널환경에 따라 인터리빙 depth를 고정한 정적할당 알고리듬(static allocation algorithm) 방식보다 제안된 인터리빙 depth를 고정하지 않은 동적할당 알고리듬(dynamic allocation algorithm) 방식에서 개선된 전송성능을 얻었다.

Ⅱ. 동기식 스트림 암호시스템

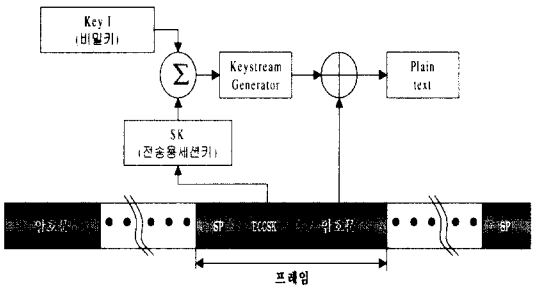
본 논문에서 암호통신을 제공하기 위한 동기식 스트림 암호시스템은 동기패턴(Synchronization Pattern, SP) 부분, 세션키(Session Key, SK) 부분, 키수열 발생기(Keystream Generator) 부분 등으로 구성된다.[3,7] 스트림 암호시스템은 동기식 스트림 암호시스템(synchronous stream cipher system)과 자체 동기식 스트림 암호시스템(self-synchronous stream cipher system)으로 나눌 수 있다.[2~3] 동기식 스트림 암호시스템은 키수열과 평문이 독립적으로 생성되고 오류확산이 없다는 장점을 갖는다. 그러나 암호통신을 위해서는 송수신측이 동기가 이루어져야 하고 키수열 동기를 위한 별도의 장치가 요구된다. 자체 동기식 스트림 암호시스템은 암호문 또는 평문의 일부가 키수열 발생기의 키로 사용된다. 암복호동안에 키수열의 불일치가 발생할 경우 일정시간이 지나면 자동적으로 재동기를 이루는 장점을 갖는다. 그러나 암호문내에서 1비트의 오류가 발생하더라도 복호시 오류확산이 발생할 수 있으므로 열악한 통신환경에서는 적합하지 않다. 따라서 본 논문에서는 페이딩 채널과 같은 열악한 통신환경에 적합한 동기식 스트림 암호시스템을 설계하였다.

2.1 동기식 스트림 암호시스템 설계

스트림 암호시스템에서 키수열 발생기는 외부 키입력을 시드값(seed number)으로 하여 무한주기에 가까운 랜덤 키수열을 발생시킨다. 본 논문에서 설계한 스트림 암호시스템의 암호기 및 복호기는 [그림 1]에서 나타내었다. 암호기에서 전송되는 프



(a) 암호화기



(b) 복호하기

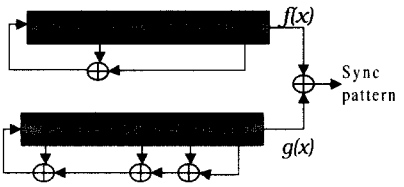
〔그림 1〕 주기적인 동기방식을 이용한 스트림 암호시스템

레임의 구조는 동기패턴(SP), 오류정정 부호화된 세션키(ECCSK), 암호문(encrypted data)으로 구성된다. 주기적인 동기식 스트림 암호통신 방식을 운용하기 위해서 요구되는 동기패턴은 송수신이 동일한 값을 가져야 하며, 골드코드 발생기(*Gold code generator*)를 이용하여 발생시킨다.[8]

전송용 세션키는 64비트 시드값을 세션키 발생기의 입력으로 하여 생성된 랜덤수열을 각 64비트씩 분할하여 사용한다. 이때 분할된 64비트의 랜덤수열은 오류정정 부호화된 세션키로서 동기패턴 및 암호문과 함께 전송된다. 수신측에서는 복호를 위해서 송수신측이 공유한 비밀키(Key I)와 전송된 오류정정 부호화된 세션키를 사용하여 키수열 발생기의 초기상태 값을 결정하고 주기적으로 동일한 동기패턴으로부터 동기를 유지한다.

2.2 동기패턴 발생기

동기식 스트림 암호시스템에서 동기부는 동기패턴 발생기와 동기패턴 검출기로 구성된다. 동기부는 동기식 스트림 암호의 송수신 키수열을 일치시켜 정상적인 암호 통신이 이루어지게 한다. 복호기에서는 동기패턴 검출 과정에서 수신된 동기패턴이 정상적으로 검출되면 오류정정 부호화된 세션키를 수신하여 암호문을 복호한다. 동기패턴 발생기는 자기상관 특성이 우수한 골드코드 발생기를 이용하여 동기패턴을 발생시킨다. 골드코드로 구성된 31비트의 동기패턴 발생기는 〔그림 2〕에서 나타내었다. 31비트의 키 길이를 갖는 동기패턴 발생기는 각 *LFSR1*, *LFSR2*를 *XOR*과정을 통해 동기패턴을 얻게된다. 원시다항식은 식 (1), (2)에서와 같이 구성된다.



〔그림 2〕 골드코드 구조를 이용한 31비트 동기패턴 발생기

$$f(x)=x^5+x^2+1 \tag{1}$$

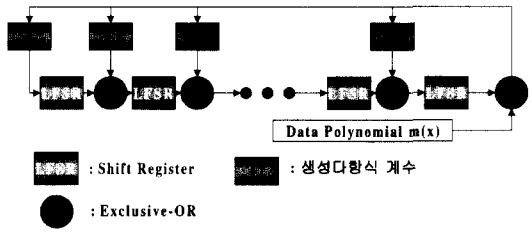
$$g(x)=x^5+x^4+x^3+x+1 \tag{2}$$

2.3 세션키 발생기

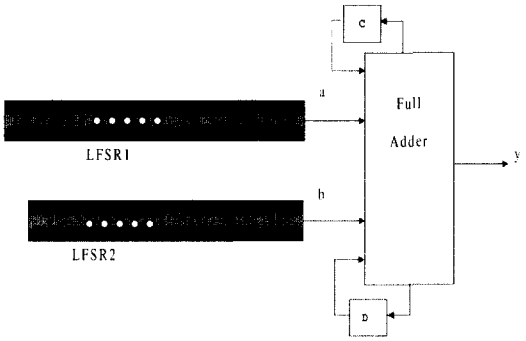
암호시스템에서 전송되는 세션키에 오류가 발생하면 암호정보의 오복호로 인해 한 주기동안 암호통신이 불가능하게 된다. 그러므로 전송되는 세션키를 보호하기 위해 무선통신의 버스트 채널에 적합한 *RS* (*Reed Solomon*)부호를 사용하여 오류정정을 수행하였다. *RS*부호는 1960년 *Reed*와 *Solomon*에 의해 제안되었으며 버스트 오류정정 능력이 뛰어난 비이진 부호로서 사용된다.[9~11] RS부호는 확장된 *BCH* (*Bose-Chaudhuri Hoquenghem*)부호로 길이가 q^m-1인 q^m-ary 부호어이다. *RS*부호는 (n, k, t)로 표현되고 n은 부호어의 길이, k는 정보어의 길이, t는 오류정정 능력을 의미한다. 부호어의 길이 n은 $k+2t$로 표현되고 오류정정 능력 t는 $\frac{n-k}{2}$이다. 부호화에서 각 부호심볼은 m비트로 구성되고 부호어는 $x^{n-k}m(x)+r(x)$로 만들어지고 식 (3)와 같다.

$$\frac{x^{n-k}m(x)}{g(x)}=q(x)+r(x) \tag{3}$$

이때 부호기는 생성다항식 $g(x)$에 따라 피드백이 연결된 *LFSR*(*Linear Feedback Shift Register*)과 각각의 피드백 연결부분에 생성다항식 $g(x)$의 계수를



〔그림 3〕 RS 채널부호기의 블록도



〔그림 4〕 비선형 세션키 발생기

곱함으로써 구성된다.

세션키 발생기는 〔그림 4〕에서와 같이 비선형 키 수열 발생기로 구성된다. 수신측에서 복호화 과정은 동기패턴을 검출한 후 전송용 세션키를 복원하고 이 복원된 키 값과 송수신측이 공유하고 있는 64비트의 비밀키 값으로부터 키수열 발생기의 시드값을 결정한다. 이때 사용되는 전송용 세션키는 64비트를 *RS*(31, 13) 부호기로 부호화하여 155비트로 전송된다. 세션키 발생기는 2비트 메모리를 갖는 이진 합산수열 발생기로서 *carry*와 메모리 지연소자로 구성된다.[3,6] 출력함수(Y_j)의 출력 수열은 *LFSR1*의 출력 수열 a_j와 *LFSR2*의 출력 수열 b_j, 이전 *carry* c_{j-1}(*carry*의 초기값은 0), 이전 피드백 메모리 비트 D_{j-1}의 전가산기를 통해 비선형으로 구해지고 각 출력 수열은 식 (4)~(6)과 같이 얻어진다.

$$Y_j=(a_j \oplus b_j \oplus C_{j-1}) \oplus D_{j-1} \quad (4)$$

$$C_j=a_j b_j \oplus (a_j \oplus b_j) C_{j-1} \quad (5)$$

$$D_j=b_j \oplus (a_j \oplus b_j) D_{j-1} \quad (6)$$

이때, j는 0, 1, 2, ... 이다.

2.4 키수열 발생기

키수열 발생기는 출력비트 수열의 비도 척도인 선형 복잡도, 랜덤 특성, 상관 면역도 등을 고려하여 설계되고 비선형 함수로 구성된다.[3,7] 키수열 발생기는 각 *LFSR*이 서로 소인 29단, 59단, 89단, 109단으로 전가산기를 통해 구성되고 〔그림 5〕에서 나타내었다. 함수 X_j는 *LFSR1*의 출력 수열 A_j와 *LFSR2*의 출력 수열 B_j, 이전 *carry* CX_{j-1}(*carry*의 초기값은 0), 이전 피드백 메모리 비트 DX_{j-1}의 전가산기를 통해 비선형으로 구해지고 식 (7)~(9)에서 나타내었다.

$$X_j=(A_j \oplus B_j \oplus CX_{j-1}) \oplus DX_{j-1} \quad (7)$$

$$CX_j=A_j B_j \oplus (A_j \oplus B_j) CX_{j-1} \quad (8)$$

$$DX_j=B_j \oplus (A_j \oplus B_j) DX_{j-1} \quad (9)$$

함수 Y_j는 *LFSR2*의 출력 수열 P_j와 *LFSR3*의 출력 수열 R_j, 이전 *carry* CY_{j-1}(*carry*의 초기값은 0), 이전 피드백 메모리 비트 DY_{j-1}가 전가산기를 통해 식 (10)~(12)에서와 같이 비선형으로 구해진다.

$$Y_j=(P_j \oplus R_j \oplus CY_{j-1}) \oplus DY_{j-1} \quad (10)$$

$$CY_j=P_j R_j \oplus (P_j \oplus R_j) CY_{j-1} \quad (11)$$

$$DY_j=R_j \oplus (P_j \oplus R_j) DY_{j-1} \quad (12)$$

따라서 출력 Z_j는 식 (10)~(12)를 통해 식 (13)~(15)와 같이 얻을 수 있다.

$$Z_j=(X_j \oplus Y_j \oplus CZ_{j-1}) \oplus DZ_{j-1} \quad (13)$$

$$CZ_j=X_j Y_j \oplus (X_j \oplus Y_j) CZ_{j-1} \quad (14)$$

$$DZ_j=Y_j \oplus (X_j \oplus Y_j) DZ_{j-1} \quad (15)$$

이때, j=0,1,2,...이다.

2.5 비도 수준

스트림 암호체계에서 비도 수준은 암호 공격에 강한 키수열 발생기의 설계에 의해 결정되므로 일반적

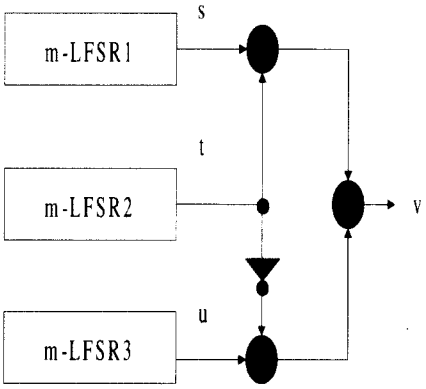
으로 키수열의 주기에 대한 최대 값 보장, 좋은 난수성 특성, 높은 상관 면역도의 특성을 지닐 것, 큰 선형복잡도를 가질 것 등의 요구사항을 만족해야 한다.

2.5.1 주기(Period)

Geffe가 제안한 비선형 키수열 시스템[12]은 [그림 6]과 같은 구조로 3개의 m-LFSR(Maximum Length Linear Feedback Shift Register)로 구성된다. 이 경우 각 레지스터의 초기 값이 0이 아니고, 각 출력 수열이 s_n, t_n, u_n이라 할 때 식 (16)으로 주어지는 출력수열 v_n을 갖는다.

$$v_n = s_n t_{n-1} u_n (t_{n-1} \oplus 1) = s_n t_{n-1} u_n t_{n-1} \oplus u_n \quad (16)$$

이때 m-LFSR1~m-LFSR3의 각 쉬프트 레지스터의 차수가 m, n, k일 때 각 쌍마다 서로 소의 조건에서 발생되는 출력 수열의 주기는 $(2^m-1)(2^n-1)(2^k-1)$[17]로 결정된다.



[그림 6] m-LFSR로 구성된 Geffe 비선형시스템

2.5.2 선형복잡도(Linear Complexity)

임의의 키수열 발생기가 발생시키는 난수와 동일한 난수를 발생하는 최단의 LFSR은 Massey[18]가 제안한 LFSR 합성법에 의해 얻을 수 있고 이때 선형 복잡도를 증가하기 위해 후단에 비선형 결합기를 추가한다. 선형복잡도에서 비선형 시스템으로부터 유도될 경우 각 차수가 m, n, k이면 $mn+nk+k$의 값으로 결정된다.

2.5.3 상관면역도(Correlation Immunity)

암호 분석과정에서 상관성 공격은 입출력 조합을 함수적으로 분리한 후 키수열의 분리정복 공격을 통해 키를 검출하는 방법이다. 만일 어떤 이진 수열이 m차 상관 면역이라고 하면 이것은 m개의 어떤 입력과도 생성자에 의한 출력 사이에는 통계적인 종속성이 존재하지 않음을 의미한다. J. Siegenthaler[18]의 경우 키수열 분리정복에 의한 상관공격에 대응할 수 있는 방법을 제안하였으며, R. A. Rueppel[19]은 메모리를 갖는 생성자를 제안하였다. 메모리가 없는 비선형 차수와 상관 면역도 사이에는 $k+m \le N-1$, $1 \le m \le N-2$와 같은 trade-off 특성이 존재한다.

Ⅲ. 제안된 인터리빙 depth의 동적할당 알고리듬(DAA)

3.1 인터리빙 기법

인터리빙 기법[21]은 정보전송 중에 발생하는 버스트 오류를 분산시키는 방법으로 정보를 전송하기 전에 발생된 전송 비트열을 달리 배열하여 전송하고 복호측에서 원래의 순서대로 재배열하는 방식이다. 이는 전송중에 발생가능한 버스트 오류를 랜덤 오류와 같은 형태로 분산시키는 기능으로서 오류정정이 가능한 비트의 수가 제한된 순방향 오류정정 부호화의 효율을 극대화할 수 있다. 본 논문에서는 높은 보안수준을 유지하기 위해 무선채널에서 암호시스템을 적용할 때 무선채널 특성상 발생하는 버스트 오류에 대해 송신되는 암호정보를 보호하고 전송성능을 개선하기 위해 인터리빙 기법을 제시하였다. 무선 통신시스템에서 전송성능 개선을 위한 인터리빙 기법에 관한 연구는 Hamouda의 경우 위성링크에서 ATM 셀을 전송시 순방향 오류정정(forward error correction) 부호기법 설계에 블록 인터리빙 기법을 도입함으로써 위성링크의 버스트 오류에 대해 성능을 개선하였다.[22] Couleaud는 우주통신에 적용가능한 고이득 부호기에 관한 연구논문에서 다양한 오류정정 부호기법을 도입하고 버스트 오류로부터 오류정정부호기의 성능을 개선하기 위해 다양한 인터리빙 기법을 설계하고 적용함으로써 성능평가를 수행하였다.[23] 그러나 무선링크에서 적용된 인터리빙 방식은 인터리빙 depth가 고정된 정적할당 알고리듬(Static Allocation Algorithm) 방식이다. 본 논문은 페이딩 환경에 인터리빙 depth를 가변하는 동적할당 알고리듬을 적용하고 인터리빙 depth를 고정한 정적할당 알고리듬(static allocation algorithm)과 성능을 평가한다. 정적할당 알고리듬

은 이동국이 페이딩 채널의 이동상황에도 고정된 인터리빙 depth를 사용함으로써 채널환경에 적응적으로 대처할 수 있도록 설계하기 위해서는 채널환경을 고려하여 충분한 인터리빙 depth를 갖도록 설계되어야 한다. 이동국이 개활지에서 도심지역으로 접어들거나 도심지역에서 개활지로 이동할 때 전파환경은 달라진다. 따라서 페이딩 채널환경에 따라 인터리빙 depth를 동적으로 할당함으로써 페이딩 영향이 적고 수신전력 변이가 작은 지역에서 인터리빙 depth를 감소시키고 상대적으로 수신전력 변이가 큰 지역에서 인터리빙 depth를 증가시킴으로써 전송성능을 개선할 수 있다.

3.2 동적할당 알고리듬(DAA)

본 논문은 페이딩 환경에 인터리빙 depth를 동적으로 적응할 수 있는 동적할당 알고리듬을 제안하였다. 정적할당 알고리듬은 이동국이 페이딩 채널의 이동상황에도 고정된 인터리빙 depth를 사용함으로써 채널환경에 적응적으로 대처할 수 없다. 이동국이 개활지에서 도심지역으로 접어들거나 도심지역에서 개활지로 이동할 때 전파환경은 달라진다. 페이딩 채널에서 전송성능은 페이딩 영향이 적고 수신전력 변이가 작은 지역에서 인터리빙 depth를 감소시키고 상대적으로 수신전력 변이가 큰 지역에서 인터리빙 depth를 증가시킴으로써 개선할 수 있다. $K=0$에서 라이시안 페이딩 수신전력 함수 n_L은 Le^{-L^2}과 같이 주어지고 순시 수신전력 함수 n_L은 식 (17)과 같이 나타낼 수 있다.

$$\begin{pmatrix} n_{L_0} \\ \cdots \\ n_{L_{n-1}} \end{pmatrix} = \begin{pmatrix} L_0 e^{-L_0} \\ \cdots \\ L_{n-1} e^{-L_{n-1}} \end{pmatrix} (\text{K=0일 때}) \qquad (17)$$

가로축은 시간변이를 나타내고 세로축은 수신전력 변이를 나타낸다. 주어진 시간 x_0에서 국소평균 $m(x)$를 구하기 위해 결정되는 길이 w는 $40\lambda \sim 200\lambda$ 사이가 적합하다.[4~6] 수신된 페이딩 신호는 $\frac{\lambda}{2}$마다 Null 값이 발생하고 주파수 대역이 850MHz이고 이동속도가 24Km/h일 때 평균적으로 0.5초단위로 20정도의 페이드(10λ)가 발생한다. 이동속도는 페이딩 발생률에 반비례하므로 이동속도가 감소할수록 길이 w는 증가하고 반대로 이동속도가 증가할수록 w는 감소한다. 인터리빙 depth의 결정은 80개마다 국소평균 전력을 얻는다. 동적할당 알고리듬은 다음 Step1~Step 8의 절차로 수행된다.

Step 1. Detection of Received Power
Step 2. Calculation of λ, ν, k
Step 3. N_0, n_L, LCR
Step 4. CPD, ADF
Step 5. *Verification of Burst Length*
Step 6. $n@2L$
Step 7. *Decision of ADF, ABL, K*
Step 8. *Decision of MBL @Depth*

Step 1에서는 수신전력 변동을 순시적으로 검출한다. 레벨교차율은 정규화 인자 n_0와 n_L값으로부터 결정되고 평균 페이딩 구간은 $\frac{1}{n_0}$과 $\frac{CPD}{n_L}$의 인자로 결정된다. 평균 페이딩 구간을 구하고 평균 페이딩 구간에 전송속도를 곱하여 평균 버스트 길이를 얻는다. 구해진 평균 버스트 길이를 근거하여 인터리빙 depth를 결정한다. 이때 적용구간($x \le w$)내의 값을 평균하고 이로부터 얻은 평균값을 이용해서 다음의 인터리빙 depth를 결정한다. 국소평균 수신전력 m(x)는 식 (18)과 같이 주어진다.

$$m(x) = \frac{1}{\omega} \sum_{y=0}^{n-1} n_L(y) \qquad (18)$$

순시 페이딩 영향을 구하고자 할 때 순시 수신전력 변이가 L_0, L_1, L_2, ..., $L_{(n-1)}$ 값으로 주어지면 국소평균 수신전력은 식 (18)에서 국소평균 $m(x)$를 m_0, m_1, m_2, ..., m_{n-1}과 같이 나타낼 수 있다. 그러므로 레벨교차율 $n(L)$은 식 (19)와 같이 나타낼 수 있다.

$$\begin{pmatrix} n(L_0) \\ \cdots \\ n(L_{(n-1)}) \end{pmatrix} = \begin{pmatrix} n_0 \cdot m_0 \\ \cdots \\ n_0 \cdot m_{(n-1)} \end{pmatrix} \qquad (19)$$

여기서 n_0는 $2.5\frac{v}{\lambda}$이다. 누적확률분포와 평균 페이딩 구간 $t(L)$은 식 (20), 식 (21)과 같이 구할 수 있다.

$$\begin{pmatrix} CPD_0 \\ \cdots \\ CPD_{n-1} \end{pmatrix} = \begin{pmatrix} P(\gamma \le L_0) \\ \cdots \\ P(\gamma \le L_{n-1}) \end{pmatrix} \qquad (20)$$

$$\begin{pmatrix} t(L_0) \\ \cdots \\ t(L_{n-1}) \end{pmatrix} = \begin{pmatrix} \frac{1}{n_0} \cdot F(L_0) \\ \cdots \\ \frac{1}{n_0} \cdot F(L_{n-1}) \end{pmatrix} \quad (21)$$

따라서 평균 버스트 길이 MBL은 전송속도 B bps와 평균 페이딩 구간(ADF)로 표현되고 식 (22)와 같이 나타낼 수 있다.

$$\begin{pmatrix} MBL_0 \\ \cdots \\ MBL_{n-1} \end{pmatrix} = \begin{pmatrix} B \cdot t(L_0) \\ \cdots \\ B \cdot t(L_{n-1}) \end{pmatrix} \quad (22)$$

한 블록이 k 비트로 구성될 때 평균 버스트 오류길이 MBL과 인터리빙 depth(D)의 곱은 k비트 이상의 값으로 결정될 때 오류를 정정할 수 있으므로 이를 고려하여 인터리빙 depth를 결정하였다.[24]

$$\begin{pmatrix} k_0 \\ \cdots \\ k_{n-1} \end{pmatrix} \le \begin{pmatrix} MBL_0 \\ \cdots \\ MBL_{n-1} \end{pmatrix} \cdot \begin{pmatrix} D_0 \\ \cdots \\ D_{n-1} \end{pmatrix} \quad (22)$$

Ⅳ. 암호시스템 비도 분석 및 실험 결과 고찰

4.1 암호시스템 실험 환경

첫째, 전송속도는 9600bps에서 실험을 수행하였다. 둘째, 암호시스템은 암호부, 인터리빙부, 송수신부로 구성된다. 암호부에서 프레임은 동기패턴, 오류정정 부호화된 세션키, 암호문으로 구성되고 한 프레임의 크기는 9600비트로 구성된다. 셋째, 라이시안 채널 환경에서 실험하였다. 평균 비트오류율은 10^{-1}~10^{-3} 이다. 이때 발생되는 비트오류율은 라이시안 페이딩 분포를 고려한 평균 버스트 오류길이로 발생된다. 발생된 평균 버스트 오류길이는 기하분포를 갖는다. 넷째, 정보는 1.5×10^7 비트량을 사용하였다.

4.2 비도 분석 및 랜덤성 검정

본 논문에서 제시된 키수열 발생기는 주기성, 선형복잡도, 상관면역도 등을 고려하여 설계되었다. 설계된 키수열 발생기의 주기는 $(2^{29}-1)(2^{59}-1)(2^{89}-1)(2^{109}-1)$으로 거의 10^{86} 값을 갖는 충분한 긴 주기성을 갖도록 설계되었다.[3,17] 선형복잡도는 주기에 근접하도록 설계되었고 상관면역도는 1차수를 갖도록 하였다. 이때 키수열 발생기는 피드백 메모리 소자를 추가하여 1/2인 상관확률을 갖도록 함으로써 상관성 공격에 강한 특성을 갖도록 설계되었다. 키수열 발생기의 전체 주기에 대한 랜덤성 검정은 불가능하므로 적합한 비트 길이를 사용하여 국부검정을 수행하였다.[3,17] 세션키수열 발생기의 선형복잡도는 주기 P인 $(2^{31}-1)\cdot(2^{61}-1)$ 값에 근접하고 상관 면역도는 최고차수 1차수[12~16]로 설계함으로써 적용시 적합한 것으로 판정된다. 동기패턴 발생기는 자기 상관특성이 우수한 Gold Code Generator를 이용하였으며 실제 시스템에서 짧은 무선망 통신에서 자기 상관도의 특성을 고려하여 3비트 여유를 주어 동기를 검출하도록 설계하였다.[25] 검정방안은 카이제곱검정(χ_2-*chi-square test*)을 사용하여 적합도를 평가하며 유의수준 결정은 일반적으로 5%의 유의수준을 만족하게 되면 적합하다고 판정한다. 적용된 검정 항목은 *frequency test, serial test, t-serial test, poker test* 및 *autocorrelation test* 등이 있다.[17] 설계된 키수열 발생기를 이용하여 얻은 출력 비트 20만 비트를 초기 값(initial seed number)을 달리하여 랜덤 검정을 수행한 결과를 [표 1]에서 제시하였다. 이때 검정 항목에 따라 얻은 결과를 살펴볼 때 정의하는 유의 수준을 통과함으로써 시스템에 적용될 때 적합하다고 평가한다.

4.3 정적할당알고리듬(SAA)과 동적할당알고리듬(DAA)의 성능비교

정적할당 알고리듬은 인터리빙 depth를 고정함으로써 채널환경에 적합한 인터리빙 depth를 결정하여 적용하는 것이 중요하다. 이동환경의 경우 페이딩 채널이 순시적으로 변화하기 때문에 적절한 인터리빙 depth를 결정하여 적합한 인터리빙 depth를 설계하는 것은 사실상 어렵다. 동적할당 알고리듬은 인터리빙 depth를 순시적으로 변화하는 페이딩 채널환경에 동적으로 적용함으로써 인터리빙 depth의 결정에 다소 유연하다. 동적할당 알고리듬과 정적할당 알고리듬의 성능비교는 [표 2]에서 나타내었고 220MHz 대역의 24Km/h 이동속도환경에서 9600bps 전송속도 환경에서 수행하였다.

동적할당 알고리듬의 평균 인터리빙 depth의 결정은 40λ를 기준으로 적용하였다. 무선 채널환경이 10^{-1}~10^{-3} 비트오류율을 갖는 페이딩이 심한 채널에서 인터리빙을 적용하지 않았을 경우 42.8% 정도의

〔표 1〕 설계된 키수열 발생기의 랜덤특성 검정결과

Test item	유의 수준 (5%)	test 결과	
		initial seed 1	initial seed 2
Frequency test	3.841	0.22	1.829
Serial test	5.991	0.277	1.835
Generalized t-serialtest(t=3)	9.488	0.489	1.928
〃 (t=4)	15.507	9.29	7.626
〃 (t=5)	26.296	12.508	14.154
Poker test (length=3)	14.067	3.88	12.173
〃 (length=4)	24.996	15.955	12.371
〃 (length=5)	44.654	37.906	33.992
Autocorrelation test	Max.≤0.05	0.008949	0.008398

오류비트 수를 발생하였다. 인터리빙 depth를 100으로 고정한 정적할당 알고리듬의 블록 인터리빙 성능결과는 1729535비트(9.5%)의 비트오류율이 발생하고 인터리빙 depth를 200으로 고정한 정적할당 알고리듬의 성능은 1376455비트(7.17%)의 오류비트 수를 발생한다. 이 경우 정적할당 알고리듬은 인터리빙 depth의 결정에 따른 2.33%의 성능차이를 발생시키지만 동적할당 알고리듬은 거의 성능차이가 없으며 페이딩 채널환경에 유연하게 적용된다. 적용된 동적할당 알고리듬은 인터리빙 depth를 채널환경에 따라 평균 버스트 오류길이가 100비트 이하의 환경에서는 인터리빙 depth를 100으로, 평균 버스트 오류길이가 100~200비트 환경에서는 인터리빙 depth를 200으로, 평균 버스트 오류길이가 300비트 이상의 환경에서는 인터리빙 depth를 300으로 동적으로 적용시켰다. 이때 동적할당 알고리듬의 오류비트 수는 1194025비트(5.96%)로 정적할당 알고리듬의 성능에 비해 동적할당 알고리듬이 1.21% 전송성능 차이를 보이고 인터리빙 depth의 범위를 확장하여 적용할 경우 인터리빙을 통한 전송성능이 개선될 것으로 예측된다.

〔표 2〕 동적할당 알고리듬과 정적할당 알고리듬의 비교 (비트오류율 : 10^{-1}~10^{-3})

인터리빙유형 / 인터리빙depth	Non-인터리빙	정적할당 알고리듬	동적할당 알고리듬
정적(100), 동적(80,200,300)	6721440 (42.8%)	1729535 (9.5%)	1194560 (5.96%)
정적(200), 동적(100,200,300)		1376455 (7.17%)	1194025 (5.96%)

〔표 3〕 동적할당을 통한 인터리빙 유형의 결과(비트오류율 : 10^{-1}~10^{-3})

인터리빙유형 / 인터리빙depth	Non 인터리빙	블록	랜덤	확장랜덤
동적(80,200,300)	6721440 (42.8%)	1194560 (5.96%)	1328574 (6.85%)	1324038 (6.83%)
동적(100,200,300)		1194025 (5.96%)	1279935 (6.53%)	1225268 (6.17%)

동적할당 알고리듬을 블록, 랜덤, 확장랜덤 인터리빙의 성능 비교는 〔표 3〕에서 나타내었다.

동적할당 알고리듬을 블록, 랜덤, 확장랜덤 구조에 적용한다. 인터리빙 depth를 80, 200, 300비트로 동적으로 적용한 블록의 성능은 1194560비트(5.96%), 랜덤은 1328574비트(6.85%), 확장랜덤은 1324038비트(6.83%)의 오류비트 수를 발생시키고, 인터리빙 depth를 100, 200, 300비트로 동적으로 적용한 인터리빙에서 블록은 1194025비트(5.96%), 랜덤은 1279935비트(6.53%), 확장랜덤은 1225268비트(6.17%)의 오류비트 수를 발생한다. 인터리빙 depth를 동적으로 할당하여 적용할 때 블록 인터리빙의 성능이 랜덤 인터리빙에 비해 평균적으로 0.89%와 0.57%, 확장랜덤에 비해 0.87%와 0.21%의 성능차이를 얻었다.

V. 결 론

본 논문은 무선채널에서 페이딩 채널을 고려한 스트림 암호시스템을 설계하였고 설계된 스트림 암호를 통해 암호문을 전송할 때 한 주기 동안 발생하는 동기패턴, 세션키, 암호문 정보를 인터리빙 기법을 적용하여 전송함으로써 버스트 오류로부터 암호문을 보호하고 전송성능을 개선하여 robust한 암호통신을 가능하도록 하였다. 제안된 인터리빙 기법을 적용하기 위해 라이시안 페이딩 채널을 고려하여 페이딩 지수에 따른 평균적으로 발생하는 버스트 오류를 이론적으로 유도하였으며 주기적인 동기식 스트림 암호시스템에 인터리빙을 적용할 때 한 주기의 동기패턴, 세션키, 암호문으로 구성된 프레임 정보에 인터리빙을 수행함으로써 전송성능 측면에서 개선된 결과를 보였다.

동기식 스트림 암호시스템의 동기구조는 9600비트를 갖도록 설계하였고 이 동기구조를 갖는 암호정보에 DAA를 적용함으로써 채널환경의 변화에도 유연하고 개선된 전송성능을 갖도록 설계하였다.

참 고 문 헌

[1] Van Til borg, H. C. A., *An Introduction to Cryptology*, KLUWER Academic Pub., Boston, 1988.

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

[3] B. Schneier, *Applied Cryptography 2nd ed.: Protocols, Algorithm, and Source code in C*, John Willy & Son, New York, 1996.

[4] W. C. Y. Lee, *Mobile Cellular Telecommunications: Analog and Digital Systems*, 2nd ed., McGraw-Hill, Singapore, 1996.

[5] William C. Y. Lee, *Mobile Communications Engineering*, McGraw-Hill, New York, 1982.

[6] William C. Y. Lee, *Mobile Communications Design Fundamentals*, John Willey & Sons, New York, 1993.

[7] Rainer A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, Berlin, 1986.

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

[9] M. H. Lee, S. B. Choi, "A High Speed Reed-Solomon Decoder," *IEEE Trans. on Comsumer Elect.*, Vol. 41, No. 4, pp. 1142~1146, Nov. 1995.

[10] 노재성, 김영철, 박기식, 조성언, 조성준, "마이크로 셀룰러 시스템에서 MRC 다이버시티와 Reed-Solomin 부호를 적용한 Trellis Coded QPSK 신호의 오율해석,"전자파학회논문지 제9권 4호, pp. 427~438, 1998년 8월.

[11] J. K. Wolf, "ECC Performance of Interleaved RS Codes with Burst Errors," *IEEE Trans. on Magnetics*, Vol. 34, No. 1, pp. 75~79, Jan. 1998.

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

[13] W. Meier and O. Staffelbach, "Correlation Properties of Combiners with Memory in stream ciphers," *Journal of Cryptology*, Vol. 5, pp. 67~86, 1992.

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

[15] R. A. Rueppel, "Correlation Immunity and the Summation Generator," *Advances in Cryptology Proceedings of CRYPTO'85, Lecture Notes in Computer Science*, Springer-verlag, pp. 260~272, 1985.

[16] T. Siegenthaler, "Correlation Immunity of Nonlinear Combining Function for Cryptographic Applications," *IEEE Trans. on Inform. Theory*, Vol. IT-30, No. 5, pp. 776~780, Sept., 1984.

[17] Helen May Gustafson, "Statistical Analysis of Symmetric Ciphers," *Thesis submitted in accordance with the regulations for Degree of Doctor of Philosophy*, Queensland University of Technology, Jul. 1996.

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

[19] 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.

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

[21] J. Y. Couleaud, "High Gain Coding Schemes for Space communications," *University of South Australia Signal Processing Research Institute Final Year Project*, Mar.-Sept. 1995.

[22] W. A. Hamouda, *Efficient Coding Schemes For ATM Transmission Via Geostationary Satellite Networks*, M.Sc. thesis, Queen's University, 1997.

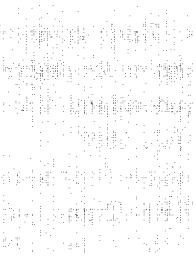
[23] J. Y. Couleaud, "High Gain Coding

Schemes for Space communications," *University of South Australia Signal Processing Research Institute Final Year Project*, Mar.-Sept. 1995.

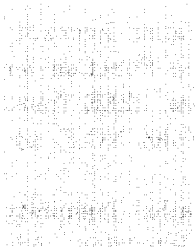
[24] King Ip Chan and Justin C-I Chuang, "Required Interleaving Depth in Rayleigh Fading Channels," *Proceedings of the Globelcom'96*, Vol. 2, pp. 1417~1421, 1996.

〈著者紹介〉

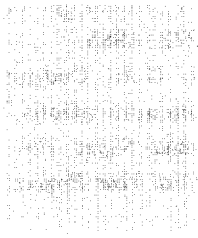
홍 진 근(Jin-Keun Hong) 정회원
1994년 2월 경북대학교 전자공학과 석사
2000년 2월 경북대학교 전자공학과 박사
2000년 9월~2001년 3월 ETRI 부설 국가보안기술연구소 선임연구원



윤 장 홍(Jang-Hong Yoon) 정회원
1987년 2월 : 경북대학교 전자공학과 석사
1998년 2월 : 경북대학교 전자공학과 박사
1987년 2월~2000년 1월 : ADD 선임연구원
2000년 2월~현재 : ETRI 부설 국가보안기술연구소 책임연구원(응용2팀장)



장 병 화(Byung-Hwa Jang) 정회원
1975년 2월 : 연세대학교 전자공학과 학사
1978년 2월 : 한국과학기술원 전기및전자공학과 석사
1988년 2월 : 한국과학기술원 전기및전자공학과 박사
1975년 11월~1983년 3월 : 한국과학기술연구소 전자공학부 선임연구원
1983년 3월 ~ 2000년 1월 : 국방과학연구소 책임연구원
2000년 2월~현재 : ETRI 부설 국가보안기술연구소 책임연구원(응용기술연구부장)



황 찬 식(Chan-Sik Hwang) 정회원
1977년 2월 서강대학교 전자공학과 졸업(공학사)
1979년 8월 한국과학기술원 전기전자공학과 졸업(공학석사)
1996년 2월 한국과학기술원 전기전자공학과 졸업(공학박사)
1991년 8월~1992년 8월 UTA 방문교수
1979년 9월~현재 : 경북대학교 전자전기공학부 교수