무선LAN링크에서 스트림 암호시스템의 전송성능개선

*홍진근, **최은수, ***윤정오, **황찬식
*창신대학 정보통신과, **경북대학교 전자공학과, ***경운대학교 정보통신공학과
e-mail : jkhong@bongam.changshin-c.ac.kr

Transmission Performance Enhancement of Stream ciper system in Wireless LAN Link

*Jin-keun Hong, **Eun-soo Choi, ***Jeong-oh Yoon, **Chan-sik Hwang
*Dept. of Information & Telecommunication, Changshin college
**Dept. of Electronics, Kyungpook National University
***Dept. of Information & Communication Engineering, Kyungwoon University

요 약

본 논문은 복사전력에 제한을 받고 많은 잡음 채널로 전송채널이 심한 영향을 받는 이동통신망이나 위성통신망과 같은 무선 전송채널에서 버스트 오류로 인해 발생하는 통신불능 현상을 해결하기 위해 암호문에 인터리빙 기법을 제안하고 이 기법을 통해 전송성능을 개선한다. 전송성능을 개선하기 위해서는 송신되는 암호문을 암호문의 구조에 적합하도록 인터리빙기법[4]을 설계하여 전송함으로써 버스트 오류[3]가 발생할 경우에 안전하게 암호문을 수신함으로써 robust한 암호통신을 가능하도록 하였다. 본 논문은 무선채널에서 적합한 스트림암호 체계를 설계하였고 스트림암호를 통해 전송시 발생되는 동기패턴, 세션키, 암호문을 인터리빙 기법을 통하여 전송함으로써 버스트오류로부터 암호문을 보호하고 전송성능을 개선하였다.

I. 서 론

무선 LAN(Local Area Network)은 전송매체로 전파나 적외선을 이용하여 다중접속제어를 수행하며 수백Kbps이상의 전송속도를 가지고 컴퓨터망, 고속무선통신 및 각종 디바이스에 광범위한 기술이 종합적으로 응용된 시스템이다. 무선채널의 실내에서는 송신전파가 벽 등에서 반사합성되어 멀티패스 페이딩이 발생하고 지연 분산은 수십~100nsec 정도가 된다. 그러므로 본 논문에서는 2.4GHz 대역(중속 무선 LAN) 무선 LAN 시스템을 중심으로 실험을 수행하였다. 2.4GHz 대역의 무선 LAN 시스템이 확산스펙트럼 방식을 사용하므로써 멀티패스에 대한 주파수 선택성 페이딩 강함, 간섭방해파의 영향 적음, 신호의 은닉성 등으로부터 장점을 가지지만 상대방의 고의적인 재밍이나 버스트오류로부터 자유로울 수 없다.

이러한 가운데 무선통신망 서비스는 번개, 태풍, 홍수, 지진과 같은 자연재해와 환경으로부터의 위협, 전자파를 이용한 무선선로 청취로부터 정보노출이나 재밍(jamming), 정보유출, 파괴, 수정, 불법침투 등 인간의 의도적 위협, 인간의 부주의로 인한 오류 등에 관한 정보보호 대책이 해결해야 할 선결해야할 과제이다. 무선이동 서비스는 비인가자의 도용이나 도청 또는 정보파괴 및 변조 등으로부터 정보 보호를 위한 처리를 반드시 요구한다. 정보보호를 위한 암호화 방식은 대칭 암호체계와 비대칭암호체계로 구분하고 암호처리 형태에 따라 블록 암호체계와 스트림 암호 체계, 영상 정보에 대한 소유권 및 저작권보호에 관한 워터마킹, 광학을 이용한 영상암호체계 등 다양한 유형의 정보를 다양한 형태로 암호화하는 연구가 진행해 오고 있다.

스트림 암호 체계[1]는 키수열 발생기를 통해 발생된 난수를 이용하여 암복호화를 수행함으로써 오류 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 사용한다. 특히 복사전력에 제한을 받고 많은 잡음 채널로 전송채널이 심한 영향을 받는 이동통신망이나 위성 통신망과 같은 전송채널에서는 채널 오류정정 부호나 전송처리 방식을 이용하여 전송품질을 만족시켜야 한다. 좋은 성능의 채널정정 부호기법이 사용된다 하더라도 버스트오류에 대해서는 대책이 없기 때문에 최근에 사용되는 RS(Reed Solomon) 부호나 Turbo 부호같은 경우는 오류정정 부호기내에 인터리버를 두고 사용하여 오류를 정정하는 경우도 있다. 무선채널에서는 암호문 전송시 암호문이 무선채널의 다량의 비트가 버스트형태로 몰려와 오류가 발생하는 환경으로 인해 암호통신은 통신불능 현상이 발생한다. 본 논문은 이러한 버스트한 오류로 인해 발생하는 통신불능 현상을 해결하기 위해 암호문에 인터리빙 기법을 제안하고 이 기법을 통해 전송성능을 개선한다. 전송성능을 개선하기 위해서는 송신되는 암호문을 암호문의 구조에 적합하도록 인터리빙기법을 설계하여 전송함으로써 버스트 오류가 발생할 경우에 안전하게 암호문을 수신함으로써 robust한 암호통신을 가능하도록 하였다. 본 논문의 구성은 Ⅱ장에서 무선채널에서의 동기식 스트림 암호시스템의 시스템구조와 시뮬레이션 결과를 살펴본다. Ⅲ장에서 결론으로 맺고자 한다

Ⅱ. 시스템 설계 및 시뮬레이션

본 논문에서는 라이시안 페이딩 분포[2]를 갖는 채널로 가정하였다. 이는 무선통신 채널에서 다양한 형태로 적용이 가능하고 직접파 성분과 분산이 σ^2인 독립적인 가우시안 성분을 포함하는 반사파 성분으로 구성된다. 라이시안 페이딩 모델은 직접파 성분과 반사파 성분이 복합된 수신신호로 라이시안 페이딩 모델의 확률밀도함수 $P_R(\gamma)$ 는 다음 식(1),(2)에서와 같다. ρ 는 수신신호의 진폭을 정규화 시킨 진폭의 변동으로 수신신호의 순시진폭 R에 대해 $\frac{R}{\sqrt{R^2}}$의 값을 갖고, $I_0(\cdot)$는 0차 변형베셀 함수이다.

$$P_R(\rho)=2\rho(K+1)\,e^{-K-\rho^2(K+1)}\cdot I_0[2\rho\sqrt{K(K+1)}] \quad (1)$$

$$P_R(\gamma)=\frac{K+1}{\gamma_0}\,e^{\left[-K-\frac{\gamma(K+1)}{\gamma_0}\right]}\cdot I_0\left[2\sqrt{\frac{\gamma K(K+1)}{\gamma_0}}\right] \quad (2)$$

γ는 순시 수신반송파대 잡음전력비, γ_0는 평균 수신반송파대 잡음전력비를 나타내고 K는 직접파 대 반사파 전력비로서 $K=\frac{a^2}{2\sigma^2}$ 의 값을 갖는다. 평균 버스트 길이는 버스트 오류 성능을 평가하는 중요한 기준이다. 평균 버스트 길이 B는 모든 버스트의 전체 길이(L_t)를 버스트의 전체 수(N_t)로 나눈 값으로 결정된다.

$$B=\frac{L_t}{N_t} \quad (3)$$

이때 평균버스트 길이가 주어질 때 버스트 길이가 갖는 확률은 다음 식(4)로 정의될 수 있다.

$$p(L)=\frac{1}{B}(1-B)^{L-1} \quad (4)$$

이때 B는 평균 버스트 길이이고, L은 버스트 길이이며 $p(L)$은 버스트길이 L일 때 버스트 길이 L이 발생할 확률을 의미하고 이 확률에 근거하여 비트오류율 10^{-2}~10^{-7}까지 기하분포로 버스트 오류를 발생시켰다.

제안된 암호체계는 주요 부분인 주기적인 동기 패턴(Synchronization Pattern ; SP), 세션 키(Session Key; SK), 암호문(Ciphertext) 등으로 구성된다. 스트림 암호체계에서 키수열 발생기는 외부 키 입력을 시드 값(seed number)로 하여 무한 주기에 가까운 랜덤 키 수열을 발생시킨다. 그림 1에서는 스트림암호 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.

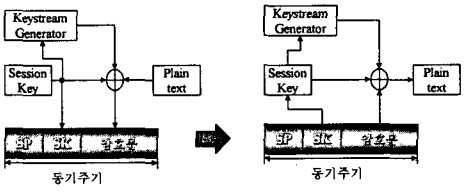

그림 1. 스트림 암호통신 체계

IEEE 802.11은 무선 LAN 시스템의 물리층과 다중접속하는 수단의 표준시방, 기밀 유지방법 및 적합성 시험의 규격등에 관한 검토를 수행하고 있으며 무선 매체로는 2.4GHz 대역의 직접확산스펙트럼, 주파수 호핑, 적외선매체가 있다. 액세스제어는 비동기패킷 통신을 기본으로하는 분산제어방식과 프로세스 제어, 음성 및 화상 등의 실시간전송으로 집중제어 방식으로 나누어 진다. IEEE 802. 11 분산제어기능은 비동기패킷 전송, 통신제어, 보안 등으로 CSMA-CA를 이용한다. 데이터 전송순서는 RTS(Request to send : 송신요구)패킷을 전송한 후 CTS(Clear to send : 송신가능)패킷, 데이터 전송 그리고 ACK(Acknow

-ledgement : 전송확인) 패킷이 전송된다. IEEE 802.11의 패킷형식은 RTS 제어패킷, CTS 제어패킷이고 그림3의 액세스 제어층의 패킷이 직접스펙트럼 확산되어 전송된다. 본 논문에서는 무선 LAN의 접속제어패킷을 동기식 스트림 암호체계로 암호화를 수행하였으며 이에 대한 인터리빙을 수행하지 않았을 때와 인터리빙을 수행했을 때의 결과를 그림 4에서 제시하였다.

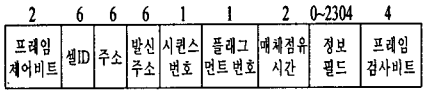

그림 2. 무선LAN 접속제어 패킷

일반적으로 사용되는 블록인터리빙 구조는 다음 그림 3에서와 같다. 비트열이 블록 4x4로 구성된 블록 인터리빙은 가로(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, ... 15, 16)방향 순으로 정보를 읽고 수신단에 송신할 때는 세로(1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 15, ..., 16)방향 순으로 출력하여 전송을 수행한다.

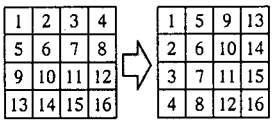

그림 3. 블록인터리빙 구조

블록인터리빙 방식을 적용할 때 적용구조는 헤더정보와 암호문을 구분하지 않고 프레임내의 전체 영역에 분산시켜서 블록인터리빙을 수행한다. 만일 하나의 동기주기를 갖는 동기패턴, 세션키, 암호문을 하나의 프레임으로 정할 때 프레임의 경계는 동기주기 단위로 결정한다. 이때 하나의 프레임 크기(N)을 2400bits로 정한다면 블록 인터리빙을 위한 블록의 크기는 50(m)x48(k)로 구성한다. 가로 방향은 블록인터리버의 간격으로 버스트오류가 발생할 때 오류없이 처리할 수 있는 버스트오류의 최대길이를 나타내고 세로 방향은 버스트 오류의 분산정도를 의미한다.

No 인터리빙과 블록 인터리빙을 적용한 결과는 그림 4에서와 같다. 동기주기를 4800비트로 하고 동기패턴 31비트, ML(51, 4)를 적용시 평균 버스트 길이가 20인 기하분포를 가질 때 비트오류율에 따른 오복호된 비트오류양을 나타내었다. No 인터리빙의 경우 10^{-2} 채널에서 $7.3637x10^{6}$, 10^{-3}에서 $7.436x10^{6}$, 10^{-4}에서 $1.763x10^{5}$, 10^{-5}에서 $1.740x10^{4}$, 10^{-6}에서 $3.0x10^{2}$의 결과를 얻을 수 있다. 블록 인터리빙의 경우 10^{-2}채널에서 $7.1389x10^{6}$, 10^{-3}에서 $1.049x10^{5}$, 10^{-4}에서 $3.101x10^{4}$, 10^{-5}에서 $2.334x10^{3}$, 10^{-6}에서 $2.92x10^{2}$의 비트오류양으로 블록 인터리빙을 통해 버스트 오류에 대해 개선된 전송성능을 얻을 수 있다.

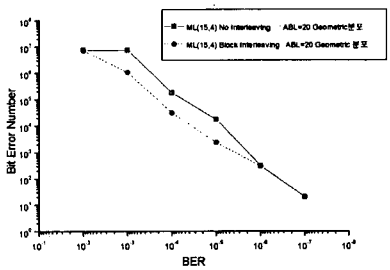

그림 4. No 인터리빙과 인터리빙 비트오류량

III. 결 론

본 논문에서는 무선LAN링크암호의 전송성능을 개선하기 위해서 송신되는 암호문을 암호문의 구조에 적합하도록 인터리빙기법을 설계하였으며 이로 인해 버스트 오류가 발생할 경우에도 안전하게 암호문을 수신할 수 있는 robust한 암호통신이 가능하도록 하였다. 본 논문은 무선채널에서 링크암호에 적용한 결과 No 인터리빙에 비해 10^{-3}~10^{-6}채널 환경에서 상당히 개선된 효과를 얻을 수 있었다. 스트림암호 체계에 인터리빙 기법을 제안함으로써 버스트 오류로부터 암호문을 보호하고 개선된 전송성능을 얻었다.

참고문헌

[1] B. schneier, Applied Cryptography 2nd ed., Protocols, Algorithm, and Source code in C, John Willy & Son, 1996.

[2] 안치훈, 김남, 박성균, "마이크로셀룰라 이동 무선시스템에서 Outage확률을 이용한 라이시안 페이딩과 로그노말 새도우잉 영향에 관한 분석," *전자파학회논문지 제9권 제1호*, pp. 60-71, 1998년 12월.

[3] A. Franchi & R. A. Harris, "On the Error Burst Properties of the "Standard" K=7, Rate-1/2 Convolutional Code with Soft-Decision Viterbi Decoding," *Submitted to European Transactions on Telecommunications.*

[4] H. Taub et al., *Principles of Communication Systems*, 2nd ed., McGraw-Hill, 1986.