DBpia

논문 21-46-07-06 The Journal of Korean Institute of Communications and Information Sciences '21-07 Vol.46 No.07
https://doi.org/10.7840/kics.2021.46.7.1146

누적 인공 부호어 가산 기반 물리계층 보안 기법

박 상 준◆°

Accumulated Artificial Codeword Addition Based Physical-Layer Security Scheme

Sangjoon Park◆°

요 약

본 논문에서는 도청자가 존재하는 채널 환경을 위한 누적 인공 부호어 가산 기반 물리계층 보안 기법을 제안한다. 제안 기법은 매 전송시간마다 정상적인 송수신단 사이에 교환된 정보를 이용하여 인공 부호어를 생성하고, 현재까지 생성된 인공 부호어들을 합한 누적 인공 부호어를 정상 부호어와 가산하여 전송한다. 이 때 누적 인공 부호어로 인한 오류는 부호어의 형태이므로 도청자의 미검출 복호 오류 확률을 증가시킬 수 있다. 모의실험 결과 제안 기법이 채널 부호화가 적용된 시스템에서 도청자의 오류 확률을 크게 증가시킬 수 있음을 확인하였다.

Key Words : Artificial Codeword, Secrecy Performance, Physical-Layer Security, Wiretap Channel, Undetected Error

ABSTRACT

In this letter, an accumulated artificial codeword addition based physical-layer security scheme is proposed for wiretap channels with an eavesdropper. In each time slot, the proposed scheme generates an artificial codeword based on the information exchanged between the legitimate transmitter and receiver, and the artificial codewords generated until the current time slot are added to make the accumulated artificial codeword, which will be added to the normal data codeword for transmission. Because the error by the accumulated artificial codeword is in the form of a codeword, the undetected decoding error probability of the eavesdropper is increased. Simulation results confirm that the proposed scheme can significantly increase the error probability of the eavesdropper in channel coded systems.

Ⅰ. 서 론

무선 통신 시스템에서는 송신단 및 수신단간 전달되는 데이터가 무선 채널을 통해 도청자에게 유출될 수 있다. 물리계층 보안 (physical-layer security) 기법은 채널 등 물리 계층의 특성을 이용하는 보안 기법으로 기존 상위 계층에서 적용되는 인증 및 암호화 기법 등의 보완 혹은 대체 방식으로 많은 연구가 진행되고 있다.[1-4]

무선 통신 시스템에서는 송수신단 사이의 채널에서 발생한 오류를 보상하기 위하여 채널 부호화 기법이 널리 적용되고 있다. 하지만 채널 부호화 기법이 적용된 데이터가 도청자에게 전달된 경우, 도청자 또한 복호 과정을 통해 도청된 신호의 오류를 정정할 수 있다. 즉, 채널 부호화가 적용된 시스템에서는 도청자 또한 채널 부호화 기법으로부터 오류 정정 이득을 얻어 도청 성공 확률을 증가시킬 수 있다.

이러한 채널 부호화 시스템에서의 보안 성능 향상을 위해, 본 논문에서는 정상 송수신단 사이에 교환된 정보를 이용하여 도청자의 오류 정정 이득 획득을 방지하기 위한 누적 인공 부호어 기반 물리계층 보안 기법을 제안한다. 제안 기법은 TDD (Time-Division Duplex) 시스템 등과 같이 매 전송시간별 송신단 및 수신단에서 공유되는 정보가 존재할 때, 이를 이용하여 인공 부호어 (artificial codeword)를 생성하고 또한 현재 전송시간까지 생성된 모든 인공 부호어를 합한 새로운 누적 인공 부호어 (accumulated artificial codeword)를 생성한다. 송신단은 해당 누적 인공 부호어를 매 시간별 정상적으로 보낼 데이터를 부호화한 정상 부호어에 가산하여 전송한다. 이 때 누적 인

※ 이 논문은 2019년도 과학기술정보통신부의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2019R1C1C1003202).
◆° First and Corresponding Author : (ORCID:0000-0002-6684-9803)Kyonggi University, Department of Electronic Engineering, sj.park@kgu.ac.kr, 조교수, 정회원
논문번호 : 202104-077-A-LU, Received April 7, 2021; Revised April 22, 2021; Accepted April 23, 2021

www.dbpia.co.kr

공 부호어로 인한 오류는 부호어의 형태이므로 제안 기법은 도청자의 미검출 오류 (undetected error) 발생 확률을 증가시켜 채널 부호화 기법에 의한 도청자의 오류 정정을 방지할 수 있다.

Ⅱ. 시스템 모델

본 논문에서는 그림 1과 같이 송신단, 수신단, 그리고 도청자가 존재하는 기본적인 와이어탭 (wiretap) 채널 환경을 고려하였다. 도청자는 수동 도청자 (passive eavesdropper)로 송수신단 사이에서 전달되는 파일럿 신호 (pilot signal) 및 데이터 신호 (data signal) 등의 모든 정보들을 수신할 수 있다.

송수신단에서는 데이터 신호의 전송을 위해 이진 선형 채널 부호 (binary linear channel code)를 사용한다. 먼저 송신단에서는 t번째 전송시간에서 K 비트의 데이터 비트열 $\boldsymbol{d}_t = [d_1, \cdots, d_K]$를 $N(> K)$ 비트의 부호어 $\boldsymbol{c}_t = [c_1, \cdots, c_N]$로 부호화한다.

$$\boldsymbol{c}_t = \mathrm{ENC}(\boldsymbol{d}_t) \tag{1}$$

식 (1)에서 $\mathrm{ENC}(\cdot)$는 시스템에서 사용된 채널 부호를 이용한 부호화 과정을 나타낸다. 이 후 송신단은 $\boldsymbol{c}_t$에 대한 변조를 통해 생성된 송신 심볼들을 전송하며, 이는 채널을 통해 수신단 및 도청자 모두에게 전달된다. 이 때 도청자는 자신과 송수신단간 채널에 대한 CSI (Channel State Information)를 알고 있으며, 또한 송신단에서 사용한 부호 및 변조 방식을 알고 있다.[1-3] 따라서 복조 및 복호 과정을 통해 얻어진 경판정 (hard-decision) 부호어는 수신단 및 도청자 모두에서 다음과 같이 표현된다.

$$\hat{\boldsymbol{c}}_t = \boldsymbol{c}_t + \boldsymbol{e}_t \tag{2}$$

식 (2)의 $\boldsymbol{e}_t$는 복호된 경판정 부호어 $\hat{\boldsymbol{c}}_t$에 남아있는 오류를 나타내는 이진 오류 벡터 (binary error vector)

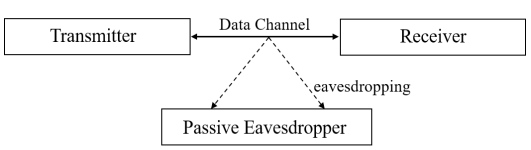

그림 1. 와이어탭 채널 모델 및 도청 환경
Fig. 1. Wiretap channel model and eavesdropping environment

이며, $+$는 이진 가산 (binary addition) 연산을 나타낸다. 즉 수신단 및 도청자 각각에서 복호된 경판정 부호어 $\hat{\boldsymbol{c}}_t$는 원본 부호어 $\boldsymbol{c}_t$에 오류 벡터 $\boldsymbol{e}_t$가 이진 가산된 형태로 나타나며, 이 때 $\boldsymbol{e}_t$는 수신단 및 도청자의 SNR (Signal-to-Noise Ratio) 및 채널 상태 등에 따라 달라질 수 있다. 이후 수신단 및 도청자는 각각의 $\hat{\boldsymbol{c}}_t$로부터 데이터 비트열 $\hat{\boldsymbol{d}}_t$를 얻고 t번째 전송시간에서의 수신 과정을 종료한다.

Ⅲ. 제안 기법

제안 기법을 위해 먼저 매 전송시간마다 정상 송수신단에게 길이 B의 비트열 $\boldsymbol{b}_t$가 공유되며 도청자는 해당 비트열 $\boldsymbol{b}_t$를 완벽히 추정할 수 없는 상황을 가정한다. 이러한 상황에 맞는 대표적인 예로는 RCKG (Reciprocal Channel Key Generation) 방식과 같이 TDD 시스템에서 송수신단이 서로가 보낸 파일럿 신호를 통해 각각의 CSI를 얻는 경우를 들 수 있다.[1,2] 이 경우 송수신단은 송신단과 수신단 간의 데이터 채널에 대한 동일한 CSI를 얻을 수 있으나, 도청자는 자신과 송신단 사이 및 자신과 수신단 사이의 도청 채널들에 대한 CSI만을 얻게 되며 송수신단 사이의 데이터 채널에 대한 CSI는 얻을 수 없다. 따라서 송수신단은 서로 동일한 $\boldsymbol{b}_t$를 생성할 수 있는 반면, 도청자는 자신이 송신단 또는 수신단에 매우 근접하게 위치하는 등 데이터 채널과 도청 채널이 매우 높은 상관관계 (high correlation)를 이루지 않는 한 송수신단과 동일한 $\boldsymbol{b}_t$의 생성이 어렵다. 다른 예로는 송수신단 중 한쪽에서 $\boldsymbol{b}_t$를 생성한 후 $\boldsymbol{b}_t$의 신드롬 (syndrome) 등 부분적인 정보만을 상대방과 공유하여 서로가 생성한 정보를 동기화하는 방식을 들 수 있다.[3]

제안 기법에서는 이렇게 송수신단 사이에 $\boldsymbol{b}_t$가 오류 없이 동기화되었음을 가정하여 t번째 전송시간에서의 인공 부호어 $\boldsymbol{g}_t$를 생성한다. 이 때 $\boldsymbol{b}_t$의 길이 B가 길수록 송신단 및 수신단에서 오류가 없는 동일한 $\boldsymbol{b}_t$를 갖기 위한 동기화 과정이 보다 어려워질 수 있다.[1-3] 이에 본 논문에서는 $B << K$, 즉 공유된 비트열 $\boldsymbol{b}_t$의 길이는 데이터 비트열 $\boldsymbol{d}_t$의 길이보다 크게 짧다고 가정한다. 따라서 서술의 편의상 B가 K의 약수임을 가정하면, 인공 부호어 $\boldsymbol{g}_t$는 $\boldsymbol{b}_t$로부터 다음과 같이 생성될 수 있다.

www.dbpia.co.kr

$$\boldsymbol{g}_t = \mathrm{ENC}(\boldsymbol{b}_t \times \mathbf{1}_{K/B}) \quad (3)$$

식 (3)의 $\times$는 크로네커 곱 (Kronecker product) 연산이며 $\mathbf{1}_{K/B}$는 K/B개의 원소가 모두 1인 벡터를 나타낸다. 즉, $\boldsymbol{g}_t$는 $\boldsymbol{b}_t$를 K/B번 반복한 길이 K의 벡터 $[\boldsymbol{b}_t,\cdots,\boldsymbol{b}_t]$를 부호화하여 얻어질 수 있다.

이렇게 생성된 인공 부호어 $\boldsymbol{g}_t$는 데이터 비트에 대한 부호어 $\boldsymbol{c}_t$에 더하여 전송될 수 있다. 하지만 t번째 전송시간에서 도청 채널과 데이터 채널과의 상관관계가 높은 경우 송수신단 사이의 $\boldsymbol{b}_t$의 동기화 과정에서 유출된 정보 등을 조합하여 도청자가 $\boldsymbol{b}_t$ 및 $\boldsymbol{g}_t$를 매우 정확하게 추정할 수 있다. 즉, 도청자의 추정 정확도에 따라 인공 부호어 사용에 의한 보안 성능 향상 정도가 크지 않을 수 있다.

따라서 도청자의 추정 오류를 보다 증가시키기 위해, $\boldsymbol{g}_t$를 생성한 이후 송신단은 현재까지 얻어진 모든 인공 부호어를 가산하여 t번째 전송시간에서의 누적 인공 부호어 $\boldsymbol{a}_t$를 다음과 같이 생성한다.

$$\boldsymbol{a}_t = \sum_{i=1}^{t} \boldsymbol{g}_i = \boldsymbol{a}_{t-1} + \boldsymbol{g}_t \quad (4)$$

식 (4)에서 $\boldsymbol{a}_0$는 영벡터 (all-zero vector)이다. 이 때 각 $\boldsymbol{g}_i (1 \le i \le t)$가 시스템에서 사용된 이진 선형 부호의 부호어이므로, 각 $\boldsymbol{a}_i (1 \le i \le t)$ 또한 해당 이진 선형 부호의 부호어이다.

송신단은 이러한 $\boldsymbol{a}_t$를 정상 데이터의 부호어 $\boldsymbol{c}_t$에 가산하여 고의적인 오류를 포함시킨다. 즉 송신 심볼 블록은 $(\boldsymbol{c}_t + \boldsymbol{a}_t)$를 변조하여 생성되며, 이는 채널을 통해 수신단 및 도청자에게 전달된다. 따라서 복조 및 복호 과정을 거친 경판정 부호어는 다음과 같이 표현될 수 있다.

$$\hat{\boldsymbol{c}}_t^{\mathrm{pr}} = \boldsymbol{c}_t + \boldsymbol{e}_t + \boldsymbol{a}_t = \hat{\boldsymbol{c}}_t + \boldsymbol{a}_t \quad (5)$$

수신단은 송신단에서 사용한 $\boldsymbol{b}_t$를 알고 있으므로, 송신단과 동일한 $\boldsymbol{a}_t$를 생성한 한 후 이를 식 (5)에 가산하는 보상 과정을 통해 $\boldsymbol{a}_t$의 영향을 제거하여 식 (2)와 동일한 결과를 얻을 수 있다. 반면, 도청자의 경우 추정된 $\hat{\boldsymbol{b}}_t$가 $\boldsymbol{b}_t$와 동일하지 않으므로, $\hat{\boldsymbol{b}}_t$로부터 생성한 $\hat{\boldsymbol{a}}_t$은 $\boldsymbol{a}_t$와 동일하지 않다. 보다 구체적으로, 누적 방식의 적용으로 인해 도청자가 t번째 전송시간까지의 모든 $\boldsymbol{b}_t$를 완벽하게 추정하지 않는 한 특정 전송시간에서의 $\boldsymbol{b}_t$를 완벽하게 추정하여도 정확한 $\boldsymbol{a}_t$를 추정해낼 수 없다. 따라서 보상 이후 도청자의 경판정 부호어는 다음과 같다.

$$\hat{\boldsymbol{c}}_t^{\mathrm{pr,eve}} = \boldsymbol{c}_t + \boldsymbol{e}_t + \boldsymbol{a}_t + \hat{\boldsymbol{a}}_t = \hat{\boldsymbol{c}}_t + (\boldsymbol{a}_t + \hat{\boldsymbol{a}}_t) \quad (6)$$

즉 도청자는 $\boldsymbol{e}_t$ 이외에 $(\boldsymbol{a}_t + \hat{\boldsymbol{a}}_t)$로 인한 추가적인 오류를 겪는다. 이 때 $\boldsymbol{a}_t$ 및 $\hat{\boldsymbol{a}}_t$가 모두 $\boldsymbol{c}_t$와 동일한 이진 선형 부호의 부호어들이므로, 제안 기법은 도청자의 미검출 오류를 증가시키게 된다. 이는 도청자가 $\hat{\boldsymbol{a}}_t$를 보상하지 않고 식 (5)의 $\hat{\boldsymbol{c}}_t^{\mathrm{pr}}$을 최종 경판정 부호어로 사용하였을 때도 동일하다.

Ⅳ. 모의실험 결과

모의실험을 위해 $K=1152$, $N=2304$인 LDPC (Low-Density Parity-Check) 부호를 고려하였다. 매번 1000개의 블록을 전송하는 버스트 전송 환경을 고려하였으며, 누적 인공 부호어는 다음 버스트에서 초기화됨을 가정하였다. 또한 송수신단에서 $\boldsymbol{b}_t$는 완벽하게 동기화되어 인공 부호어 생성 및 보상 과정에서 사용되는 $\boldsymbol{a}_t$가 항상 동일한 상황을 고려하였다. QPSK (Quadrature Phase Shift Keying) 변조 및 준정적 레일리 감쇄 채널이 고려되었으며, 수신단 및 도청자의 수신 안테나 수는 8로 수신단에서는 MRC (Maximum-Ratio Combining)를 사용하였으며, $B=8$로 설정되었다. 복호기의 최대 반복 복호 횟수는 40번이다.

그림 2 및 3은 도청자의 추정 확률에 따른 평균 BER (Bit Error Rate) 및 BLER (Block Error Rate) 성능을 보여준다. $p = \mathrm{Prob}(\hat{\boldsymbol{b}}_t = \boldsymbol{b}_t)$이며 인공 부호어 방식이 적용되지 않은 기존 기법의 성능은 정상 수신단의 오류 성능과 동일하다. 그림 2와 3은 제안 기법이 기존 기법 대비 도청자의 오류 확률을 크게 증가시킴을 보여준다. 특히 제안 기법에서 누적 인공 부호어 대신 단일 인공 부호어를 사용한 경우 도청자의 평균 BER이 p에 수렴하는 반면, 누적 인공 부호어의 경우 $p=0.9$인 경우에도 평균 BER이 0.5에 수렴하는 것을 확인할 수 있다. 이는 앞서 설명한 바와 같이 누적 방식에서 추정 오류에 의한 효과가 지속적으로 누적

www.dbpia.co.kr

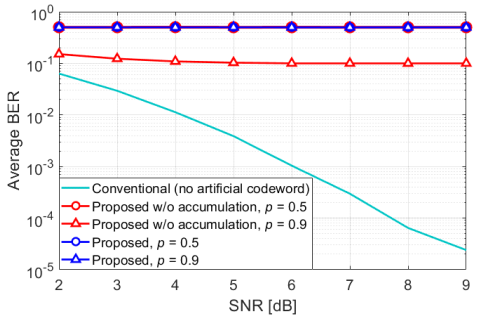

그림 2. 제안 기법의 평균 BER 성능
Fig. 2. Average BER of the proposed scheme

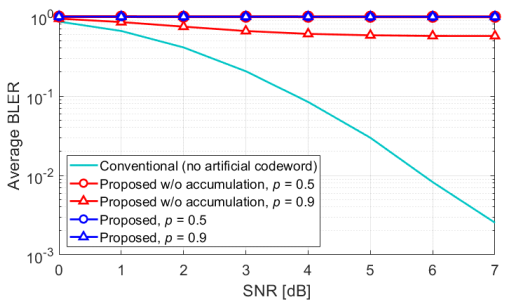

그림 3. 제안 기법의 평균 BLER 성능
Fig. 3. Average BLER of the proposed scheme

되기 때문이다. 또한 그림 3에서 기존 기법의 블록 오류는 모두 검출 가능한 복호 오류(e_t)인 반면, 해당 비율을 제외한 제안 기법의 모든 블록 오류는 가산된 누적 인공 부호어에 의해 발생되어 도청자의 검출이 불가능한 미검출 복호 오류이다. 이를 통해 제안 기법이 채널 부호화가 적용된 시스템을 위한 효율적인 물리계층 보안 기법임을 확인할 수 있다.

V. 결 론

본 논문에서는 도청자가 존재하는 채널 환경을 위한 누적 인공 부호어 가산 기반 물리계층 보안 기법을 제안하였다. 모의실험 결과를 통해 제안 기법이 채널 부호화가 적용된 시스템의 보안 성능을 크게 향상시킬 수 있음을 확인하였다. 본 논문에서는 공유된 비트열의 길이를 메시지 길이만큼 단순 반복 확장함을 가정하였으며, 또한 현재까지 얻은 인공 부호어를 모두 누적하는 방식을 가정하였다. 이러한 확장 및 누적 방식에 대한 추가적인 연구를 통해 제안 기법의 성능을 보다 향상시킬 수 있다. 이와 함께, 본 문에서는 송신단 및 수신단에서 인공 부호어 생성을 위해 공유된 정보가 오류 없이 동기화되어 있는 상황을 가정하였다. 공유할 정보의 길이가 길어지는 등 동기화 과정에서 오류가 발생하여 송수신단에서 서로 다른 정보를 갖게 되는 경우 제안 기법은 도청자뿐만 아니라 정상 수신단의 복호 성능도 열화시킬 수 있다. 이러한 동기화 과정의 오류 역시 고려한 제안 기법의 확장 방식에 대한 연구는 향후 과제로 남는다.

References

[1] J. W. Wallace and R. K. Sharma, “Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis,” *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 3, pp. 381-392, Sep. 2010.

[2] J. Zhang, et al., “Key generation from wireless channels: a review,” *IEEE Access*, vol. 4, pp. 614-626, Mar. 2016.

[3] S. Park and H. Son, “Near-perfect code scrambling with limited key information for wiretap channels,” *IEEE Trans. Veh. Tech.*, vol. 69, no. 11, pp. 13410-13423, Nov. 2019.

[4] I. Bang and S. Kim, “A role of small cells in heterogeneous networks for physical-layer security: Jamming or cooperation,” *J. KICS*, vol. 43, no. 4, pp. 619-628, Apr. 2018.

www.dbpia.co.kr