인공잡음을 이용한 알라무티 부호 기반 보안 방식의 성능평가

채가람, 박근수, 정예준, 이혜인, 김수영*

전북대학교

{irlsgaram200, qkrrmstn3365, yejun011120. leehyein96, sookim}@jbnu.ac.kr

Evaluation of Alamouti-coded Security Scheme using Articificial Noise

Garam Chea, GuenSu Park, Yejun Jung, Hyein Lee, Sooyoung Kim*

Jeonbuk National University

요 약

본 논문은 알라무티 시공간 부호화 행렬에 인공 잡음을 삽입하는 물리 계층 보안 방식을 다루며, 신호 전력과 인공 잡음 전력의 비율에 따른 수신 이미지의 품질 변화를 분석하여 해당 방식의 보안 성능을 평가하고, 신호 전력과 인공 잡음 전력이 상충 관계임을 보인다. 인공 잡음 삽입에 따른 전력 소모 문제를 보완하기 위해 제안된 전력 조절 인공 잡음 방식과 기존 인공잡음 방식의 성상도를 비교하고, 다양한 인공 잡음 기반 물리 계층 방식 기법의 성능을 평가한다.

Ⅰ. 서론

물리 계층 보안 (physical layer security; PLS)은 별도의 추가 장비 없이 통신 채널의 물리적 특성을 이용해 보안을 강화하는 방식이다. 알라무티 시공간 부호화 행렬 (space time block code; STBC)과 인공잡음 (artificial noise; AN)을 더하는 PLS 방식은 합법 수신자(Bob)에게는 AN의 영향을 최소화하고, 불법 수신자(Eve)의 비트 오류율 (bit error rate; BER)을 증가시켜 보안을 강화하는 방식임이 증명됐다 [1][2]. 본 논문은 AN 기반 방식과 전력 조절 (power-balanced; PB) AN방식의 송신 신호 성상도를 비교 분석하여, PB-AN 방식이 기존 AN방식의 전력 효율 저하 문제를 개선함을 보인다. 또한, 이미지 전송 시스템에서 신호 전력 (p_s)과 인공 잡음 (p_{an})비율을 변화시키며 합법 수신자 (Bob)와 불법 도청자 (Eve)가 수신한 이미지의 품질을 분석한 결과, 신호 품질과 보안성은 신호와 인공 잡음의 전력 분배에 따라 반비례한다는 점을 보인다.

Ⅱ. AN을 이용한 물리 계층 보안 방식

알라무티 시공간 부호화 행렬에 AN을 삽입하는 PLS 기법은, 송신자 (Alice)가 Bob의 채널 정보를 기반으로 AN을 설계하여, Bob은 AN이 제거된 신호를 수신한다. 반면 Eve는 Bob의 채널 정보를 알 수 없으므로, 삽입된 AN을 제거하지 못해 송신 신호를 정확하게 복원하기 어렵다 [1]. 이러한 기존의 AN 기반 물리 계층 보안 방식은 랜덤 분포를 따르는 AN과 채널 정보를 이용하여 설계되기 때문에, 첨두 전력 대 평균 전력비 (peak-to-average power; PAPR)가 증가한다. 이를 해결하기 위해 제안된 PB-AN 방식은, 각 타임 슬롯의 전송 전력을 최소화 하는 위상 회전 인자를 AN에 곱함으로써, PAPR 문제를 개선 한다 [2].

Ⅲ. 성능 평가 시스템

그림 1 은 AN/PB-AN을 적용하여 이미지를 전송하는 시스템을 도시한 것 이다. 먼저, Alice는 전송하고자 하는 이미지의 밝기 (Y) 성분과 색차 성분 (Cr, Cb)을 추출하여 이미지의 정보를 YCrCb 색 공간으로 변환한다. 이어서, 변환된 이미지의 밝기 (Y) 성분에는 Sobel 필터를 적용하여

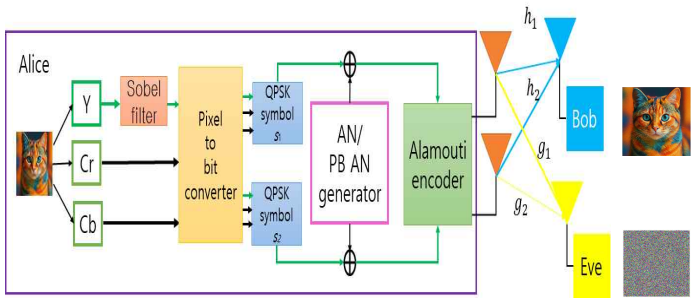


그림 1. AN/PB-AN이 적용된 이미지 전송 시스템.

밝기 변화가 급격한 윤곽 정보를 추출하고, 색차 성분 (Cr, Cb)과 함께 픽셀 값을 비트로 전환한다. 이렇게 얻어진 이미지 정보를 포함하는 비트스트림을 QPSK 심볼에 대응시킨 후 생성된 AN와 결합하여 알라무티 시공간 부호화 행렬로 구성하여 송신한다. 최종적으로, 송신 신호는 Rayleigh 페이딩 채널을 통해 전송되며 Bob과 Eve 모두 수신할 수 있다.

Ⅳ. 시뮬레이션 결과

1. PB-AN의 전력 효율 성능

그림 2 는 AN과 PB-AN을 적용한 송신 신호의 성상도를 비교한 것이다. AN을 적용한 전송신호의 성상도 (a)의 경우, 송신 신호가 PLS을 적용하지 않은 QPSK 신호를 중심으로 넓게 확산되어 있으며, 이는 송신신호에 AN이 더해짐으로써 위상 및 진폭 왜곡이 발생했음을 의미한다. 반면, PB-AN을 적용한 전송신호 성상도 (b)는 송신 신호가 QPSK 신호좌표를 중심으로 비교적 작은 반경 내에 집중적으로 분포하여 AN방식에 비해 낮은 평균전력과 PAPR을 가지는 것을 알 수 있다. 예를 들어, p_s=1 W, p_{AN}=1 W이면 AN과 PB-AN을 적용한 송신 신호의 평균 전력은 각각 $p_{t,AN} \simeq 2$ W, $p_{t,PB\text{-}AN} \simeq 0.9$ W 이다.

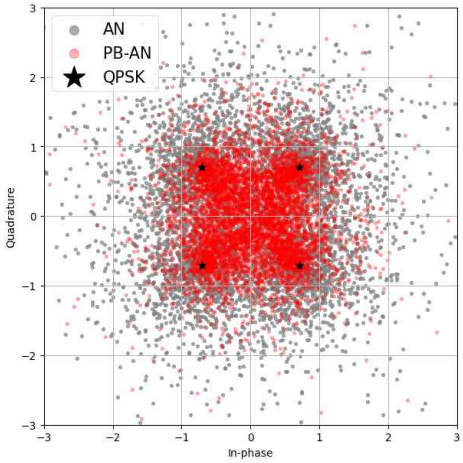


그림 2 인공 잡음 기반 PLS를 적용하여 왜곡된 송신 신호의 성상도

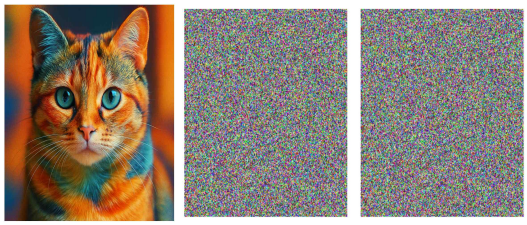
2. 신호 전력과 인공 잡음 전력 비율에 따른 수신 이미지 분석

그림 3 은 PLS를 적용하지 않은 원본 이미지 (a)와 AN과 PB-AN을 적용했을 때의 송신 이미지 (b), (c)를 각각 도시한 것이다. 보이는 바와 같이, PLS를 적용한 이미지 (a)와 (b) 모두 원본 이미지 (a)를 추측하기 어려울 만큼 충분히 왜곡된 것을 확인 할 수 있다. 따라서, PB-AN 방식은 AN방식과 비교하여 나은 전력 효율을 가지면서도 견줄만한 보안성능을 보임을 확인 할 수 있다.

그림 4와 그림 5는 신호 전력과 인공 잡음 전력 비율 $\chi = p_s/p_{an}$를 각각 0.01 , 1, 99 에 대해, Bob과 Eve의 수신 이미지를 각각 비교한 것이다. 이 때, 채널의 신호 대 잡음비는 30 dB라고 가정한다.

그림 4에서 도시된 바와 같이, Bob은 χ과 상관없이 그림 3의 (a)이미지에 가까운 이미지를 수신한다. 이는 Alice와 Bob의 채널정보 영공간에서 설계된 AN이 해당 채널을 통해 전송되는 과정에서 AN이 소거되기 때문이다.

반면, 그림 5는 Eve가 AN을 제거하지 못하므로, χ에 따라 수신 이미지의 품질이 크게 달라진다. 예를 들어, 그림 5의 (c)와 같이 신호 전력이 AN의 전력보다 충분히 클 경우 ($\chi = 99$), AN의 영향이 감소하여 Eve도 일정 수준 이상의 정보를 복원할 수 있다. 반대로, 그림 5의 (a)와 같이 신호 전력이 AN 전력보다 현저히 작은 경우 ($\chi = 0.01$), Eve는 수신 신호로부터 유의미한 정보를 복원할 수 없다. 이로써, χ는 보안성과 이미지 품질 간의 상충 관계(trade-off)를 형성한다.

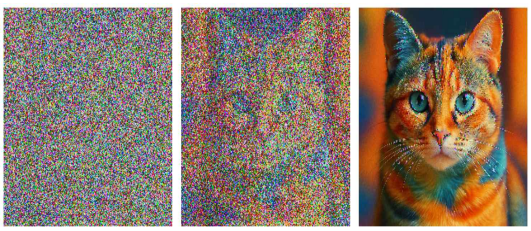


(a)원본 이미지 (b) AN 기법 (c) PB-AN기법

그림 3. 원본 이미지와 인공 잡음 기반 PLS를 적용하여 왜곡된 이미지

(a) χ=0.01 (b) χ=1 (c) χ = 99

그림 4. 신호 전력과 인공잡음 전력 비율 χ에 따른 Bob의 수신 이미지 비교



(a) χ=0.01 (b) χ=1 (c)χ = 99

그림 5. 신호 전력과 인공 잡음 전력 비율 에 따른 Eve의 수신 이미지 비교

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. RS-2024-00459799).

참 고 문 헌

[1] P. Shang, S. Kim, and X.-Q. Jiang, “Efficient Alamouti-coded spatialmodulation for secrecy enhancing,” in Proc. Int. Conf. Inf. Commun.Technol. Converg., 2019, pp. 860 - 864.

[2] S. Chan, S. Kim, H. W. Kim, B. J. Ku, and D. Oh, “Energy-efficient physical layer security schemes for low Earth orbit satellite systems,” In*ternational Journal of Satellite Communications and Networking,* vol. 42, no. 5, pp. 374-396, Sept/Oct. 2024.