

다중 안테나 시스템에서 위상 왜곡을 활용한 물리계층보안 기법 성능 분석

홍영우, 황민, 송재영, 김수영*

전북대학교

{acehyw, gladiate01, jy.song, sookim}@jbnu.ac.kr

Performance Analysis of Phase Distortion Techniques for Physical Layer Security in MIMO system

Youngwoo Hong, Min Hwang, Jaeyoung Song, Sooyoung Kim*

Jeonbuk National University

요약

본 논문은 다중 안테나 시스템에서 위상 왜곡을 이용한 효율적인 물리계층보안 기법의 성능을 분석 제시한다. 제안된 기법을 알라무티 시공간 블록 부호화 및 공간 다중화 방식에 모두 적용하여, 각각의 보안성 및 성능을 평가한다. 인공잡음 또는 인공간섭 기반 기존 보안 기법과 달리 추가적인 전력 소모 문제없이 보안과 오류 성능을 달성함을 확인한다. 비트 오류율 그래프와 성상도 및 이미지 전송 시뮬레이션을 통해 위상 왜곡을 이용한 물리계층보안 기법의 성능을 평가한다.

I. 서론

다중 안테나(multi-input multi-output; MIMO) 시스템에서의 물리계층보안(physical layer security; PLS) 기법으로, 인공 잡음(artificial noise; AN) 및 인공 간섭(artificial interference; AI)을 활용한 PLS 기법에 대한 연구가 진행된 바 있다 [1][2]. 그러나 이 방식들은 추가적인 전력 소모, 최대전력 대 평균전력 비(peak-to-average power ratio; PAPR) 증가와 같은 한계가 존재한다. 이러한 한계를 극복하기 위해 MIMO 시스템에서 합법 수신자의 채널 위상 정보를 기반으로 효율적인 위상 왜곡을 활용한 PLS 기법이 제시된 바 있다 [3]. 본 논문에서는 이러한 위상 왜곡을 활용한 PLS 기법을 이미지 전송에 적용한 시뮬레이션을 진행하여 성능을 평가한다. 시뮬레이션 결과를 통해 추가적인 전력 소모나 PAPR 문제없이 합법 수신자에게는 기존 통신과 동등한 통신 품질을 제공하며, 불법 도청자의 정보 획득을 원천적으로 차단하는 특징을 보이는 것을 확인한다.

II. 위상 왜곡을 활용한 PLS 기법

본 기법은 알라무티 시공간 블록 부호화(space-time block coding; STBC) 방식의 송신 신호 행렬 또는 공간 다중화(spatial multiplexing; SM) 방식의 송신 신호 행렬에 채널의 위상 정보를 기반으로 한 사전 위상 왜곡(phase predistortion)을 적용하는 방식이다. 송신자(Alice)는 합법 채널의 위상 정보를 이용해 송신 신호의 각 성분에 사전 위상 왜곡을 가한다. 합법 수신자(Bob)의 경우, 전송 과정에서 채널 위상 정보는 제거되고 실수(real-number) 직교 채널 행렬을 전송받아 원래 신호를 복원할 수 있다. 반면에, 불법 도청자(Eve)가 수신하는 신호에서는 위상 왜곡 성분이 상쇄되지 않고 그대로 남아 원래 신호를 복원할 수 없다.

그림 1은 MIMO 시스템에서 위상 왜곡을 활용한 PLS 기법 시나리오를 나타낸다. Alice는 다중 안테나를 이용하여 부호화된 신호(S)에 위상 왜곡(P)으로 신호를 사전 왜곡하여 송신한다. 이때, P 정보는 Alice와 Bob의 채널 행렬 \mathbf{H} 의 성분으로 구성된다. 따라서 P 정보는 신호가 채널 \mathbf{H} 를 통

과하며 상쇄된다. 반면, Eve는 \mathbf{H} 의 정보를 알지 못하고, 신호가 Alice와 Eve의 채널인 \mathbf{G} 를 통과하여 전송되므로 위상 왜곡이 상쇄되지 않아 신호 복원에 실패한다 [3].

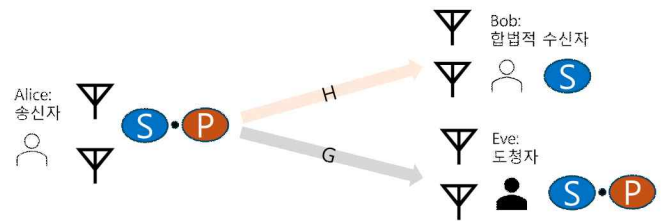


그림 1. 위상 왜곡을 활용한 PLS 기법 시나리오

III. 성능 평가 시스템

본 논문에서는 위상 왜곡을 활용한 PLS 기법의 성능을 평가하기 위해 그림 2와 같은 이미지 전송 시스템을 포함한 성능 평가 시스템을 구성하였다.

해당 시스템은 Alice의 이미지 데이터를 입력 데이터로 생성한다. 이를 위해, 픽셀 환경에서 픽셀로 구성된 이미지 데이터를 비트(0 또는 1)로 변환한다. 시뮬레이션에서 사용한 이미지는 가로 및 세로의 픽셀 수가 각각 256개이고 가산혼합 색상 모델인 RGB(red, green, blue) 채널로 구성되어 있으므로, 전체 바이트 수는 $196,608(\text{가로 픽셀 수} \times \text{세로 픽셀 수} \times \text{채널 수}) = 256 \times 256 \times 3$ 바이트이다. 이때, 바이트를 이미지 데이터 처리에 적합한 uint8 자료형으로 변환하면 각 바이트가 8비트 형태로 변환되므로, 이미지 데이터의 전체 비트 수는 1,572,864 비트이다. 이와 같이 생성된 비트는 QPSK(quadrature phase shift keying) 방식으로 변조되어 복소수 심볼로 변환된다. 이 변조된 심볼은 MIMO 프레임으로 구성되고, PLS 구현을 위한 사전 위상 왜곡이 적용된다. 즉, Alice는 합법 채널 행렬 \mathbf{H} 의 정보를 알 수 있다고 가정하기 때문에, \mathbf{H} 행렬의 성분으로 구성된

위상 왜곡 행렬을 부호화 신호에 곱하여 전송 신호를 생성한다 [3].

이후, 위상 왜곡이 적용된 신호는 주파수 비 선택적 MIMO 페이딩 채널을 통과하여 전송되고, 수신 신호는 각 수신자에 따라 복조 및 복조 과정을 거친다.

마지막으로, 복조 신호 데이터와 입력 데이터를 비교하여 신호 대 잡음 비(signal-to-noise ratio; SNR) 변화에 따른 BER 성능을 분석한다. 또한, Bob과 Eve의 수신 신호 정상도와 이미지 전송 시뮬레이션 결과를 바탕으로 제안 기법의 보안성 및 오류 성능을 평가한다.

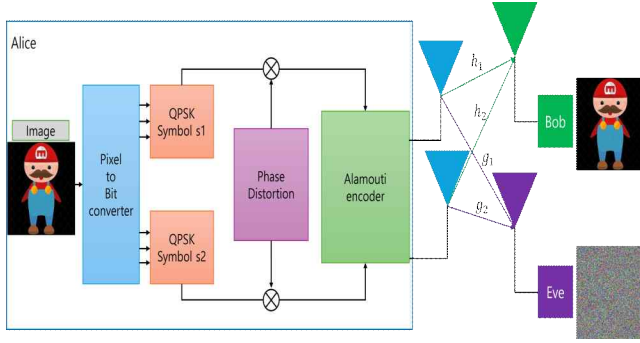


그림 2. 위상 왜곡이 적용된 이미지 전송 시스템

IV. 성능 평가 결과

그림 3은 SNR 변화에 따른 BER 성능을 비교한 결과이다. QPSK 변조를 적용한 2x2 SM 방식과 QPSK 변조를 적용한 2x1 STBC 방식에 대해 각각 평가를 진행하였다. Bob은 위상 왜곡을 활용한 PLS기법이 적용되지 않은 기존 SM 방식 및 STBC 방식과 동일한 BER을 보인다. 반면 Eve는 SNR이 증가함에도 BER이 약 0.5로 유지된다.

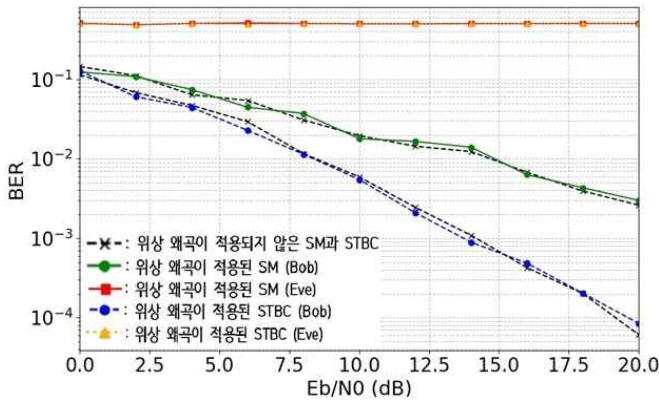


그림 3. BER 성능 그래프

그림 4는 Bob과 Eve에서 수신 신호 분포를 나타내는 정상도이다. 그림 4의 (a)는 Bob의 정상도로, 수신 신호에서 위상 왜곡 성분이 제거되어 이상적인 QPSK 심볼 위치(검은색 x) 주변에 수신 신호가 밀집되어 있음을 확인할 수 있다. 반면, 그림 4의 (b)는 Eve의 정상도로, 위상 왜곡 성분이 그대로 남아 수신 신호가 무작위로 분포함을 보인다.

그림 5는 이미지 전송 시스템의 시뮬레이션 결과이다. 해당 시뮬레이션은 SNR이 15 dB인 조건에서 수행하였다. Alice가 송신한 원본 이미지가 그림 5의 (a)와 같을 때, Bob의 경우 그림 5의 (b)와 같이 원본 이미지 정보를 손실 없이 복원할 수 있음을 보인다. 하지만, Eve는 그림 5의 (c)와 같이 수신 신호에 존재하는 위상 왜곡 성분으로 인해 원본 이미지의 정보

를 전혀 알 수 없는 잡음 형태로 복원됨을 알 수 있다.

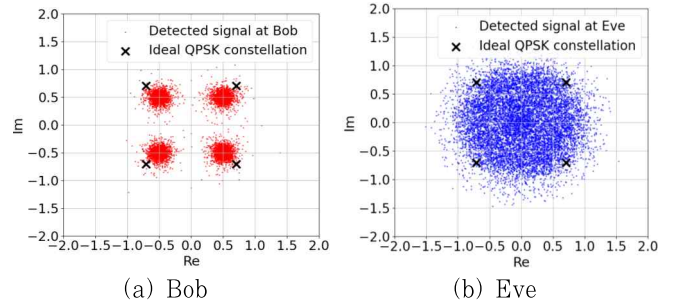


그림 4. 위상 왜곡 기법 적용 시 Bob과 Eve의 정상도 비교

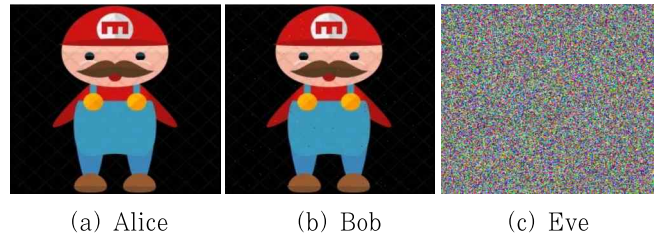


그림 5. 이미지 전송 시뮬레이션 결과

V. 결론

본 논문에서는 다중 안테나 시스템에서 위상 왜곡을 활용한 PLS 방식의 성능을 분석하였다. 해당 기법은 송신 신호에 합법적 채널의 위상 정보를 이용한 사전 위상 왜곡을 적용한 것으로, AN이나 AI를 활용한 PLS 방식 및 상위 계층 암호화와 달리 추가 자원 소모 없이 보안성과 오류 성능을 동시에 달성할 수 있음을 확인하였다. 따라서 해당 기법이 5G, 6G 및 IoT 등 차세대 초공간 네트워크 환경에서 효율적인 보안 기법으로 활용될 수 있을 것으로 기대된다.

ACKNOWLEDGMENT

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(RS-2024-00459799)

참고 문헌

- [1] P. Shang, W. Yu, K. Zhang, X.-Q. Jiang, and S. Kim, "Secrecy enhancing scheme for spatial modulation using antenna selection and artificial noise," *Entropy*, vol. 21, no. 7, pp. 626, Jun. 2019.
- [2] 채승호, "인공 잡음 및 송수신기 보호 구역을 활용한 보안 성능 향상," *한국정보통신학회논문지*, vol. 20, no. 3, pp. 558 - 564, Mar. 2016.
- [3] H. Lee, S. Chan, and S. Kim, "Efficient MIMO signal predistortion for secrecy-enhancing," *Electronics*, vol. 11, no. 9, pp. 1425, Apr. 2022.