

# MU-MIMO Wi-Fi 네트워크에서 물리계층보안을 위한 인공 잡음 설계

장철민, 소재우\*

서강대학교

cheilm314@sogang.ac.kr, \*jwso@sogang.ac.kr

## Artificial noise design for physical security in MU-MIMO Wi-Fi networks

Cheolmin Jang, Jaewoo So\*

Sogang Univ.

### 요약

본 논문은 MU-MIMO Wi-Fi 네트워크에서 인공 잡음에 대한 steering matrix 구성을 통해 보안 전송률을 높이는 방법을 제안한다. IEEE 802.11ac 표준 기반의 MU-MIMO 환경에서 정당한 사용자에게 기밀 신호를 보낼 때, 이에 대한 도청자의 비트 오류율과 보안 전송률을 분석하였다. 전체 신호 대비 인공 잡음비를 증가하면서 모의 실험을 진행하였을 때, 제안하는 기법을 통해 steering matrix를 구성하는 것이 인공 잡음비가 50%인 경우 85% 높은 성능을 보였다.

### I. 서론

무선 통신환경에서 진화하는 다양한 네트워크 공격 방법들로 인해 공격자의 연산 능력과 무관하게 보안을 유지할 수 있는 물리계층보안(Physical Layer Security) 기술에 대한 중요도가 높아지고 있다. 무선채널의 무작위성을 활용한 다양한 기술이 제시되어 왔으며, 최근에는 인공 잡음(Artificial Noise; AN)을 활용한 시스템에서 디코딩 방법에 대한 연구가 진행되었다[1, 2]. 본 논문에서는 IEEE 802.11ac 표준 기반의 MU-MIMO(Multi-User Multiple-Input Multiple-Output) 환경에서 AN에 대한 빔포밍 steering matrix의 구성 방법을 제안한다.

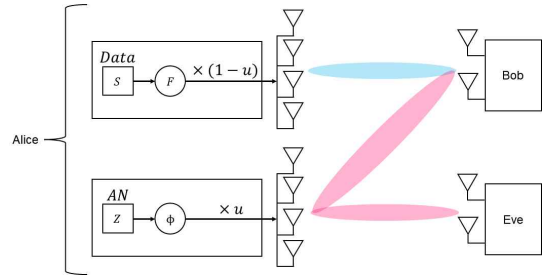


그림 1. AN 기반의 보안 통신 시스템

### II. 시스템 모델

IEEE 802.11ac MU-MIMO를 사용하는 실내 환경에서 기지국 역할을 하는 Alice가 정당한 사용자인 Bob에게 기밀 통신을 할 때, Eve가 이를 도청하는 환경을 고려한다. 이때, Eve는 Bob의 채널 환경을 완벽하게 알 수 있고, Alice는 Eve의 도청을 탐지했다고 가정한다.

그림 1은 AN에 빔포밍 steering matrix  $\phi$ 를 곱하여 송신하는 AN기반의 보안 통신 시스템이다. 이때, Bob의 데이터 전송률은 다음과 같다.

$$R = \log_2 \left( 1 + \frac{(1-u)|h_b^H f_b|^2}{(1-u)|h_b^H f_e|^2 + u(|h_b^H \phi_b|^2 + |h_b^H \phi_e|^2) + N_b/P} \right). \quad (1)$$

이때,  $h_b, h_e$ 는 각각 Bob과 Eve에 대한 채널 행렬이고,  $f_b, f_e$ 는 각각 Bob과 Eve에 대한 프리코딩 벡터,  $\phi_b, \phi_e$ 는 각각 Bob과 Eve에 대한 AN의 steering vector이다. 한편 Eve는 Bob의 채널 정보를 완전하게 알고 있으므로, Eve의 데이터 전송률은 다음과 같다[3].

$$R = \log_2 \left( 1 + \frac{(1-u)|h_e^H f_b|^2}{(1-u)|h_e^H f_e|^2 + u(|h_e^H \phi_b|^2 + |h_e^H \phi_e|^2) + N_e/P} \right). \quad (2)$$

수식 (1), (2)로부터 보안 전송률은 다음과 같이 계산한다.

$$R^s = R - R^e \quad (3)$$

이에 따른 최적화 수식은 다음과 같다.

$$\max_{u, \phi} R - R^e \quad (4a)$$

$$s.t. \quad 0 \leq u \leq 1 \quad (4b)$$

$$|f_b|^2 + |f_e|^2 + |\phi_b|^2 + |\phi_e|^2 \leq 1 \quad (4c)$$

### III. 제안하는 방법

MU-MIMO에서 대각 성분만을 사용한 프리코딩은 데이터 전송률을 향상에 기여한다[4]. 반면, 대각 성분을 제외하여 steering matrix를 구성할 경우, AN이 Bob에게 주는 영향을 감소시킬 것으로 기대할 수 있다. AN은 잡음의 크기에만 영향을 주고 디코딩 여부와 상관없이 없으므로 임의로 AN의 steering matrix를 변형할 수 있다. AN의 steering matrix  $\phi$ 는 프리코딩 행렬을 기반으로, 대각 성분을 뺀 행렬을 사용하면 다음과 같다.

$$\Phi = F - D(F) \quad (5)$$

이때  $D(\cdot)$ 는 행렬의 대각 성분만을 추출한 행렬이다.

#### IV. 모의 실험 결과

모의 실험은 WINNER II 채널 모델의 실내 시나리오를 사용하여 사용자 간 간섭이 높은 환경에서 진행하였다. Alice는 8x8 MIMO, Bob과 Eve는 각각 2x2 MIMO를 사용하는 것으로 구성하였다. 전송 전력이 30 dBm 일 때, AN을 사용하지 않았을 때와 AN을 사용하였을 때 steering matrix를 데이터 신호와 같이 설정한 경우와 제안하는 기법으로 설정하였을 때, Eve가 Bob의 데이터 신호를 추정하는 것에 대한 비트 오류(Bit Error Rate: BER)과 보안 전송률(secretcy rate)을 비교하였다.

그림 2는 도청자 Eve의 BER을 보여주고 있다. 이때 BER은 같은 payload 길이 1 k로 Bob에게 기밀 통신을 할 때 Bob의 채널 정보를 완전하게 알고 있는 Eve가 이를 디코딩하였을 때 비트 에러를 확인한 것이다. 시험 결과 AN 비율이 증가할수록 제안한 방법의 BER이 높은 것을 확인할 수 있다.

그림 3은 정당한 사용자 Bob의 보안 전송률을 보여주고 있다. 이때, 보안 전송률은 수식 (3)으로 계산된다. AN 비율이 증가할수록 제안한 방법의 보안 전송률이 높은 것을 확인할 수 있다.

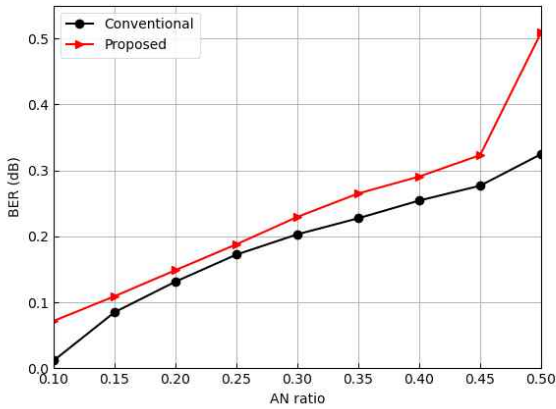


그림 2. 도청자 Eve의 BER

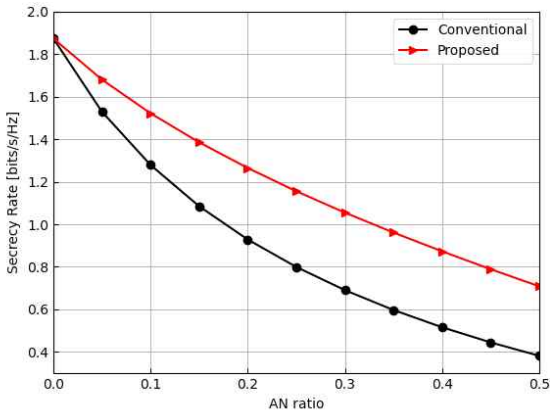


그림 3. 정당한 사용자 Bob의 보안 전송률

#### V. 결론

본 논문은 MU-MIMO Wi-Fi 네트워크에서 물리계층보안을 위한 AN 설계 방법을 제안하고 평가하였다. 제안하는 기법은 전체 송신 전력 대비 AN 비율이 높을수록 높은 성능을 내어 AN 비율이 50%일 때, 제안 기법이 85% 높은 성능을 보였다. 최근 RIS(Reconfigurable Intelligent Surface)를 활용한 물리계층보안 기술에 관한 연구가 활발하게 이루어지고 있는데, 추후 RIS를 사용하는 실외 환경에서 송신 전력에 따라 AN 비율과 이에 따른 steering matrix를 구성하는 방법을 연구할 계획이다.

#### ACKNOWLEDGMENT

본 연구는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2022R1F1A1062696). 본 논문의 교신저자는 소재우 임 (이메일: jwso@sogang.ac.kr).

#### 참고 문헌

- [1] E. Choi, M. Oh, J. Choi, J. Park, N. Lee, and N. Al-Dh "Joint precoding and artificial noise design for MU-MIMO wiretap channels," *IEEE Transactions on Communications*. vol. 71, no. 3, pp. 1564-1578, Dec. 2022.
- [2] J. Choi, J. Joung and Y. -S. Cho, "Artificial-Noise-Aided Space-Time Line Code for Enhancing Physical Layer Security of Multiuser MIMO Downlink Transmission," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1289-1300, March. 2022.
- [3] S. Lu, S. Zhao and Q. Shi, "Block-Diagonal Zero-Forcing Beamforming for Weighted Sum-Rate Maximization in Multi-User Massive MIMO Systems," in *Proc IEEE Symposium on Computers and Communications (ISCC)*, Rennes, France, 2020, pp. 1-6.
- [4] S. Arzykulov, A. Celik, G. Naurzybayev, and A. M. Eltawil, "Artificial noise and RIS-aided physical layer security: Optimal RIS partitioning and power control," *IEEE Wireless Communications Letters*. vol. 12, no. 6, pp. 992-996, Mar. 2023.