다중안테나 통합 센싱 및 통신 와이어탭 채널의 보안 빔포밍 기법

정성규, 박정훈*
연세대학교

wjdtjd963@yonsei.ac.kr, *jhpark@yonsei.ac.kr

Secure Beamforming for MIMO ISAC Wiretap Channels

Seongkyu Jung, Jeonghun Park,
Yonsei Univ.

요 약

본 논문은 본 논문은 다중 안테나 (MIMO)를 사용하는 통합 센싱 및 통신 (ISAC) 시스템에서 통신 보안 문제를 다룬다. 특히, 합법적인 통신 수신자와 센싱 대상이 존재하는 동시에 악의적인 도청자가 통신 내용을 엿듣는 와이어탭 채널 환경을 고려한다. 이러한 ISAC MIMO 와이어탭 채널에서, 우리는 통신 사용자에게 높은 데이터 전송률을 제공하고 센싱 성능을 유지하면서 도청자에게 유출되는 정보량을 최소화하여 보안 용량(secrecy capacity)을 극대화하는 것을 목표로 한다. 이를 위해 일반화된 특이값 분해 (GSVD)에 기반한 새로운 송신 빔포밍 기법을 제안한다. 제안하는 기법은 합법적인 사용자의 채널과 도청자의 채널을 동시에 고려하여 신호 공간을 효과적으로 분리하고, 이를 통해 센싱 빔과 통신 빔을 정교하게 설계하여 보안 성능과 센싱 성능을 동시에 최적화한다.

Ⅰ. 서 론

최근 6G 및 미래 무선 통신 시스템에서 제한된 무선 자원의 효율적인 활용을 위해 통합 센싱 및 통신(Integrated Sensing and Communication, ISAC) 기술이 큰 주목을 받고 있다 [1]. ISAC 은 단일 하드웨어 플랫폼과 공유된 스펙트럼을 사용하여 통신 기능과 레이더와 같은 센싱 기능을 동시에 수행함으로써 시스템 효율성을 크게 향상시킬 수 있다 [2]. MIMO 기술은 빔포밍을 통해 공간적 자유도를 활용하여 ISAC 시스템의 성능을 더욱 향상시키는 핵심 요소로 간주된다 [3].

그러나 무선 채널의 개방적인 특성으로 인해 ISAC 시스템 역시 통신 정보 유출의 위협에 노출될 수 있다. 특히, 통신 데이터가 민감한 정보를 포함하는 경우, 악의적인 도청자(eavesdropper)의 존재는 심각한 보안 문제를 야기한다. 물리 계층 보안(Physical Layer Security, PLS)은 이러한 위협에 대응하기 위한 효과적인 접근 방식으로, 암호화 기법에 의존하지 않고 채널의 물리적 특성을 활용하여 보안 통신을 달성한다 [4,6]. 와이어탭 채널 모델은 PLS 연구의 기본적인 프레임워크를 제공하며, 보안 용량(secrecy capacity)은 합법적인 사용자와 도청자 간의 채널 용량 차이를 통해 정의된다 [5].

ISAC 시스템에서 센싱 기능과 통신 기능을 동시에 수행하면서 통신 보안까지 고려하는 것은 매우 도전적인 과제이다. 송신 빔은 통신 사용자에게 강한 신호를 전달하고, 센싱 대상에게 충분한 에너지를 방사하며, 동시에 도청자에게는 신호 유출을 최소화하도록 설계되어야 한다. 기존의 많은 연구들은 ISAC 에서의 빔포밍 최적화 [1,3] 또는 보안 통신을 위한 프리코딩/빔포밍 [4,6]을 개별적으로 다루었으나, 이 세 가지 요구사항(통신, 센싱, 보안)을 통합적으로 고려한 연구는 아직 초기 단계이다.

본 논문에서는 ISAC MIMO 와이어탭 채널 환경에서 일반화된 특이값 분해(Generalized Singular Value Decomposition, GSVD)를 활용한 새로운 보안 빔포밍 설계 기법을 제안한다. GSVD 는 두 개 이상의 행렬을 동시에 분해하여 공유된 신호 부공간과 개별적인 신호 부공간을 식별하는 데 효과적인 수학적 도구이다. 우리는 GSVD 를 합법적인 사용자의 채널 행렬과 도청자의 채널 행렬에 적용하여, 합법적인 사용자에게는 강한 신호를 전달하고 도청자에게는 약한 신호를 전달하는 통신 빔, 센싱 대상 방향으로 에너지를 집중시키는 센싱 빔을 체계적으로 설계한다.

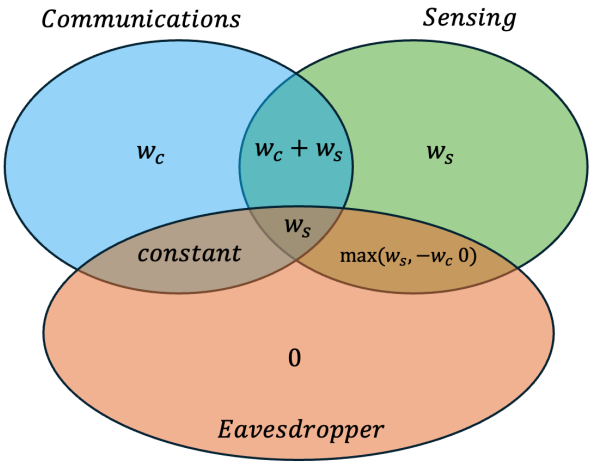
Ⅱ. 본론

A. 시스템 설정

모든 링크(통신, 센싱, 도청자)를 잡음 분산이 1 인 AWGN(Additive White Gaussian Noise) 채널로 모델링한다. 합법 수신자 채널 행렬을 $H_c \in C^{N_r \times N_t}$로 정의하며, 도청자 채널 행렬을 $H_e \in C^{N_e \times N_t}$로, 센싱 채널은 공분산 R_s의 Cholesky 분해를 통해 얻은 $H_s = R_s^{1/2} \in C^{N_s \times N_t}$로 모델링한다. 통신 성능은 보안 용량

$C_{\text{secrecy}} = \log|I + F^H H_c^H H_c F|$ 으로, 센싱 성능은 센싱 상호 정보량 (sensing mutual information) $C_{\text{sensing}} = \log|I + F^H H_s^H H_s F|$ 으로 측정하며, 센싱에 대한 가중치가 통신에 대한 가중치보다 작다고 가정한 후 $C_{\text{joint}} = w_c C_{\text{secrecy}} + w_s C_{\text{sensing}}$로 평가한다.

B. 직교 direct sum 에서의 최적 전력 할당



[그림 1. 3 개의 채널이 만드는 8 개의 부분공간]

[그림 1]에서 각각의 원은 해당 채널 영공간(null space)의 수직 여공간을 나타낸다. 이를 통해 전체 송신공간을 총 8 개의 부분공간으로 구분할 수 있으며, 이들 부분공간의 합으로 전체 송신공간이 표현됨을 알 수 있다. 만약 이 8 개의 부분공간이 서로 직교하는 형태의 direct sum 을 이룬다면, [그림 1]과 같이 전력 할당(power allocation) 을 하면 KKT 조건을 만족하는 최적 전력 할당이 됨을 보일 수 있다. 하지만 실제로는 해당 부분공간들이 서로 직교하지 않으므로, 이러한 방식을 직접적으로 적용하여 최적의 전력 할당을 수행하는 것은 불가능하다.

C. GSVD 기반 통신/센싱 빔 설계

제안하는 빔 설계 기법은 합법 수신자·도청자 채널 행렬에 대해 GSVD 를 수행하여 공통 우측 기저 행렬 V와 개별 특이값 행렬 Σ_c, Σ_e를 동시에 도출한다. $H_c = U_c \Sigma_c \left[\Omega^{-1} 0\right] V^H, H_e = U_e \Sigma_e \left[\Omega^{-1} 0\right] V^H$로 분해한다. 여기서 $\Omega = \begin{bmatrix} \Omega_1^{-1} & 0 & 0 \\ T_{21} & \Omega_2^{-1} & 0 \\ T_{31} & T_{32} & \Omega_3^{-1} \end{bmatrix}$는 하삼각 행렬이고 $\Sigma_c^2 + \Sigma_s^2 = I$를 만족하게 된다. $\begin{bmatrix} H_e \\ H_c \end{bmatrix}$의 rank 수를 k 라고 할 때, V의 $k+1$번째부터 n_t 번째 열은 합법 수신자와 도청자의 공통 영공간을 span 하는 기저 벡터이다. 이 부분공간에서 그람-슈미트 과정(Gram-Schmidt process) 을 통해 H_s의 영공간과의 교집합 및 나머지 직교공간에 해당하는 기저를 추출할 수 있다. 이 기저들에 대해 전력을 w_c 씩 균등 할당해주면 센싱 개인 채널에 대한 전력을 분배할 수 있다. 이후 GSVD 에서 공통 행공간(row space)에 대해서는 $\Omega_2\sqrt{(P)}$의 전력할당을 해주고, 합법 도청자의 개인 채널에 대해서는 w_c 만큼의 균등 전력 할당을 해주면 o(P)의 손실만을 갖는 준최적 해(suboptimal solution)이 됨을 확인할 수 있다.

Ⅲ. 결론

본 논문에서는 MIMO ISAC 와이어탭 채널 환경을 대상으로, 일반화된 특이값 분해(GSVD)를 이용한 새로운 보안 빔포밍 설계 기법을 제안하였다. 제안 기법은 합법 수신자와 도청자 채널을 동시에 고려하여 공통 및 전용 채널을 명확히 분리하고, 통신 성능(보안 용량)과 센싱 성능(상호 정보량)을 가중치 기반으로 균형 있게 최적화할 수 있도록 설계되었다.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. RS-2024-00397216, Development of the Upper-mid Band Extreme massive MIMO(E-MIMO)).

참 고 문 헌

[1] Choi, J., Park, J., Lee, N., and Alkhateeb, A. "Joint and Robust Beamforming Framework for Integrated Sensing and Communication Systems," IEEE Transactions on Wireless Communications, vol. 23, no. 11, pp. 17602-17618, Nov. 2024.

[2] Kim, N., Han, J., and Park, J. "Integrated Sensing and Communications in FDD MIMO Without CSI Feedback: Towards FDD MIMO ISAC," Proc. 22nd International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt '24), Seoul, Korea, Republic of, pp. 132-137, 2024.

[3] Choi, E., Park, S., Choi, J., Park, J., and Lee, N. "Beamforming Optimization for Integrated Sensing and Communication Systems with SCNR Consideration," Proc. 22nd International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt '24), Seoul, Korea, Republic of, pp. 146-153, 2024.

[4] Choi, E., Oh, M., Choi, J., Park, J., Lee, N., and Al-Dhahir, N. "Joint Precoding and Artificial Noise Design for MU-MIMO Wiretap Channels," IEEE Transactions on Communications, vol. 71, no. 3, pp. 1564-1578, March 2023.

[5] Choi, J., and Park, J. "Sum Secrecy Spectral Efficiency Maximization in Downlink MU-MIMO: Colluding Eavesdroppers," IEEE Transactions on Vehicular Technology, vol. 70, no. 1, pp. 1051-1056, Jan. 2021.

[6] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas—Part II: The MIMOME Wiretap Channel," in IEEE Transactions on Information Theory, vol. 56, no. 11, pp. 5515-5532, Nov. 2010