

# 분산형 인공잡음 삽입 기반 물리계층 보안 기법

## Physical Layer Security Algorithm Based on Distributed Artificial Noise Injection

장근영, 유병하, 정해준, 신현동  
경희대학교 전자정보융합공학과

{wkdrmsduddl, syeon2513, haejoonjung, hshin} @khu.ac.kr

### 요약

6G 통신에서는 대규모 사물인터넷(Internet of things, IoT) 노드가 초고밀도로 존재해 5G 통신에 비해 10 배 더 높은 연결성을 제공할 것으로 전망된다. 그러나, 인공지능 기술의 발전과 양자 컴퓨팅의 발전으로 정보 보안을 위협하는 공격 형태 또한 다양해지고, 정교해질 것으로 예측된다. 이에 따른 6G 보안의 핵심 후보 기술 중 하나로서 물리계층 보안 기술이 고려되고 있다. 따라서, 본 논문에서는 추가적인 인공잡음을 삽입하는 협력적 빔형성 기반의 물리계층 보안기술을 제시하며 시뮬레이션 결과를 통해 성능을 분석한다.

#### I. 서론

물리계층 보안은 무선 통신의 고유한 무작위성을 이용하기에 수신자에게 데이터를 안전하게 송신하는 동시에 도청자가 존재하는 방향에선 잡음과 같은 신호로 관측되게 된다. 따라서 도청자의 수신 감도를 낮춰 정보 유출을 막는 기법이 주류를 이루고 있는데 저복잡도의 IoT 노드에서는 전력과 하드웨어 제약으로 인하여 다중 안테나를 적용하기 어려운 문제가 있다.

이러한 대규모 IoT 네트워크에서는 여러 IoT 노드들이 가상 안테나 배열 (virtual antenna array, VAA)을 생성하는 협력 빔형성을 사용하여 선택적으로 정보 전송을 달성할 수 있다. 그러나 매 송신 시간 간격 (transmit time interval, TTI)마다 VAA 요소가 무작위로 선택되기 때문에 모든 VAA 요소의 채널상태정보 (channel state information, CSI)를 수집하고, 프리코딩 벡터를 공유하는 것은 매우 큰 오버헤드가 발생한다. 본 논문에서는 이러한 한계를 극복하기 위해 노드들의 위치를 VAA의 통계적인 정보로 활용하여 CSI와 프리코딩 벡터 공유를 요구하지 않는, 완전히 분산된 방식의 협력적 빔형성 기법을 제시한다.

기존 협력적 빔형성 기반 물리계층 보안 알고리즘은 도청자가 수신자 근처 가까이에 존재할 경우 보안율이 매우 낮다는 문제점이 존재하였다 [1]. 이러한 문제점을 극복하기 위해, 본 논문에서는 프리코더에 인공잡음 주입 빔포머를 추가한다. 제안한 프리코더는 데이터 빔포머와 인공잡음 빔포머로 구성되며, 두 빔포머의 비율에 따른

성능을 시뮬레이션을 통해 분석하고 기존 다중안테나 기반 물리계층 보안 알고리즘들과 secrecy rate 성능을 비교한다.

#### II. 본론

##### II-1. 시스템 모델

단일 안테나를 장착하고 있는 N 개의 IoT 노드들이 지상에 균일하게 분포하여 2 차원 원 형태의 VAA를 형성한다고 가정한다. VAA 요소들은 수신자의 각도 위치를 이용하여 위상을 조정하는 개방형 루프 접근 방식의 협력적 빔형성을 수행한다.

$k$  번째 TTI에서 수신자가 받는 신호는  $y(\rho, \varphi, k) = \sqrt{P}h(\rho, \varphi, k)w(k)s(k) + z(k)$ 로 표현되며  $P$ 는 전송전력,  $h$ 는 채널벡터,  $w$ 는 빔형성 벡터,  $s$ 는 메시지 그리고  $z$ 는 Gaussian 잡음으로 이루어진다. 데이터 빔포머와 인공잡음 빔포머로 이루어져 있는 빔포밍 벡터는  $w(k) = \sqrt{t}w_D(k) + \sqrt{1-t}w_{AN}(k)\epsilon(k)$ 로 표현되며  $w_D(k)$ 가 수신자에게 원하는 메시지를 보내는 데이터 빔포머,  $w_{AN}(k)$ 가 도청자가 존재하는 방향으로 인공잡음을 삽입하는 인공잡음 빔포머이다.  $\epsilon(k)$ 는 인공잡음이며 가우시안 분포를 따른다. 이 두 빔포머를  $t$ 를 이용하여 비율을 조정한다. 이 빔포머는 매 TTI마다 무작위되는 노드들의 위치이 빔포머는 매 TTI마다 무작위되는 노드들의 위치 정보를 공유해야 되는 오버헤드가

존재한다. 이를 해결하기 위해서 노드들이 VAA 내에 완전히 분산하여 각각의 위치 정보를 VAA의 통계적인 정보로 이용하여 대체하는 분산적 빔포밍 벡터는 다음과 같다.

$$\begin{aligned} \tilde{w}(k) &= \frac{\sqrt{t}}{\sqrt{N}} v(\varphi_B, k) \\ &+ \frac{\epsilon(k)\sqrt{1-t} \left( v(\varphi_{AN}, k) - 2 \frac{J_1\left(\frac{4\pi R}{\lambda} \sin\left(\frac{\varphi_{AN} - \varphi_B}{2}\right)\right)}{\frac{4\pi R}{\lambda} \sin\left(\frac{\varphi_{AN} - \varphi_B}{2}\right)} v(\varphi_B, k) \right)}{\sqrt{N - 4N \frac{J_1\left(\frac{4\pi R}{\lambda} \sin\left(\frac{\varphi_{AN} - \varphi_B}{2}\right)\right)^2}{\left(\frac{4\pi R}{\lambda} \sin\left(\frac{\varphi_{AN} - \varphi_B}{2}\right)\right)^2}}} \end{aligned}$$

$\varphi_B$ 와  $\varphi_{AN}$ 는 각각 수신자와 도청자의 각도,  $v(\varphi_B, k)$ 와  $v(\varphi_{AN}, k)$ 는 각각 수신자, 도청자의 방향 벡터를 의미하며,  $J_1$ 는 제 1 베셀함수이다. 분산적 빔형성 벡터를 통해 기존에 노드 개수의 두배만큼 요구되었던 노드간 상호 통신은 1 번밖에 이뤄지지 않으며, 벡터 정규화는 더 이상 필요하지 않게 된다.

## II-2. Secrecy Rate 분석

II-1장에서 언급한 수신된 신호에서 전송전력과 채널 벡터, 그리고 빔형성 벡터로 이루어진 array factor,  $F(\rho, \varphi, k)$ 의 평균과 분산을 이용하여 신호 대 잡음비 (signal to noise power ratio, SNR)을 도출한다. 수신자와 도청자의 SNR은 각각  $\gamma_B = \frac{|E[F(\rho_B, \varphi_B, k)]|^2}{\text{Var}[F(\rho_B, \varphi_B, k)] + \sigma^2}$ 와  $\gamma_E = \frac{|E[F(\rho_E, \varphi_E, k)]|^2}{\text{Var}[F(\rho_E, \varphi_E, k)] + \sigma^2}$ 으로 구할 수 있고 이를 통해 secrecy rate을 도출하여 물리계층 보안 성능을 분석할 수 있다 [2].

## II-3. 시뮬레이션 결과

노드의 개수  $N = 32$ , carrier frequency는 5GHz, 파장 0.06m로 설정된 시뮬레이션은 총  $10^4$ 번 반복 시행되었다. VAA의 반지름은 1m이며, VAA 중심과 수신자, 도청자와의 거리는 모두 1km이다. 그림 1은 수신자가  $120^\circ$ , 도청자는 수신자 근처인  $122^\circ$ 에 존재할 때, 다중안테나 기반의 기법들과 제안한 기법에 대해 secrecy rate을 비교한 그림이다. 도청자가 존재하는  $122^\circ$ 에서 협력 빔형성을 사용한 기법이 기존 다중안테나 기반의 기법보다 더 높은 secrecy rate을 도출한다. 그러나 인공잡음 삽입이 없는, 기존 협력 빔형성 기법인  $t = 1$ 의 결과도 수신자의 근처에선 낮은 secrecy rate을 보이는 것을 알 수 있다. 하지만 인공잡음이 적절하게 이루어진  $t = 0.5$  또는  $t = 0.8$ 의 결과는  $122^\circ$ 에서  $t = 1$ 일 때보다 약 1.5배의 secrecy rate 향상을 보인다.

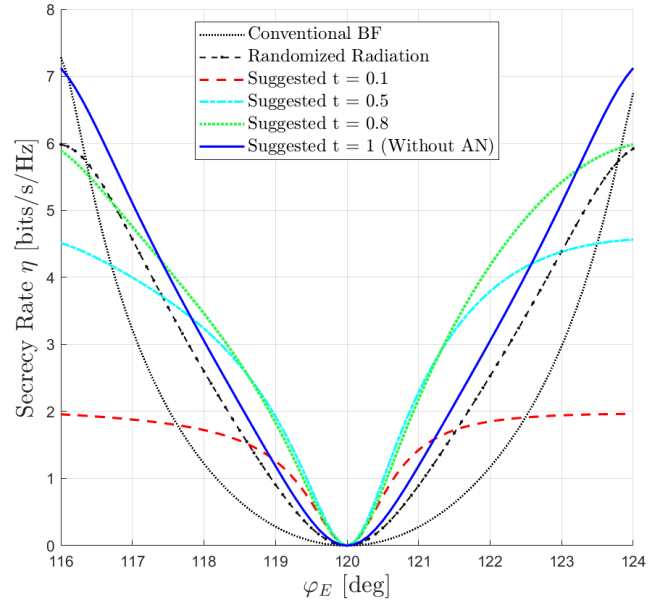


그림 1. Secrecy rate 시뮬레이션 결과

## III. 결론

IoT 네트워크에서 VAA의 통계적인 정보를 이용해 오버헤드를 줄인 분산형 인공잡음 삽입 기반 협력 빔형성 기법을 제시하였다. 제안한 기법은 분산적 빔형성 벡터로 인하여 노드간 상호 통신과 computing 오버헤드가 현저히 줄어들었다. 또한, 인공잡음 빔포머의 비율이 적절하게 설정되었을 때, 데이터 빔포머로만 이루어진 기존의 협력 빔형성 기법보다 더 높은 secrecy rate을 얻을 수 있는 것을 확인하였다.

## ACKNOWLEDGMENT

This work was supported by the MSIT, Korea, in part under the National Research Foundation of Korea grants (RS-2023-00303757, NRF-2022R1F1A1065367 and NRF-2022R1A4A3033401) and in part under the ITRC support programs (IITP-2024-2021-0-02046) and in part under the Convergence security core talent training business support program (IITP-2023-RS-2023-00266615) supervised by the IITP.

## 참고 문헌

- [1] H. Jung and I.-H. Lee, "Analog cooperative beamforming with spherically bound random arrays for physical-layer secure communications," *IEEE Commun. Lett.*, vol. 22, no. 3, pp. 546–549, Mar. 2018.
- [2] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri and R. W. Heath, "Enhancing Secrecy with Multiantenna Transmission in Millimeter Wave Vehicular Communication Systems," in *IEEE Trans. Veh. Tech.*, vol. 66, no. 9, pp. 8139–8151, Sept. 2017.