물리계층 보안 향상을 위한 이종 Rank 빔행렬 선택기반 의사-무작위 빔포밍 기법

손 웅(충남대학교), 정방철(충남대학교)

woongson@cnu.ac.kr, bcjung@cnu.ac.kr

A Pseudo-Random Beamforming Technique with Multiple Beam Matrices of Heterogeneous Rank for Improving Physical Layer Security

Woong Son(Chungnam National Univ.) and Bang Chul Jung(Chungnam National Univ.)

요 약

본 논문은 하향링크 셀룰라 네트워크에 다수의 공인단말들과 인접 셀에서는 인증되었으나, 공인 셀에 속하지 않아 수신이 허가되지 않은 비공인단말들이 존재하는 상황에서 물리계층 보안전송률을 향상시키기 위한 기지국에서의 이종 랭크(Rank)를 갖는 다수의 빔행렬 중 최적을 선택사용하는 의사-무작위 빔포밍 기법을 제안하였다. 컴퓨터 모의실험을 통해 기존의 완전한 랭크(Full Rank)를 갖는 다중 빔행렬 선택 기법과 제안한 기법의 성능을 비교 분석하였으며, 제안한 기법이 기존 기법 대비 보안전송률 성능이 우수함을 확인하였다.

Ⅰ. 서 론

최근 정보이론적으로 정의된 보안용량에 대해 활발하게 연구되고 있다. 관련연구 중에서 보안전송률을 극대화하기 위해 다중안테나 기지국에서 의사-무작위 빔행렬 후보들 중 최적을 선택하여 사용하는 기법 [1]이 제안되었다. 본 논문에서는 기존 기법 [1]을 기반으로 다양한 수의 빔벡터들로 구성하는 기법을 제안하였으며, 컴퓨터 모의실험으로 달성할 수 있는 보안전송률 측면에서 기존 기법과 함께 비교 분석하여, 성능이 향상됨을 검증하였다.

Ⅱ. 보안 전송률 향상을 위해 제안한 이종 Rank 빔행렬 선택 기반 의사-무작위 빔포밍 기법

N_t개의 안테나를 탑재한 기지국과 단일안테나 공인단말 N_{MS}개와 1개의 비공인단말이 존재하는 하향링크 셀을 고려한다. 기지국은 M개의 의사-무작위로 송신 빔행렬 후보 $\boldsymbol{V}^{[1]},...,\boldsymbol{V}^{[m]},...,\boldsymbol{V}^{[M]}$을 생성한다. 기존 기법 [1]에서는 N_t개의 빔벡터로 구성된 M개의 송신 빔행렬 후보들을 생성하며, $m\in\{1,...,M\}$번째 빔행렬 후보는 $\boldsymbol{V}^{[m]}=\left[\boldsymbol{v}^{[1]},...,\boldsymbol{v}^{[N_t]}\right]\in\mathbb{C}^{N_t\times N_t}$로 나타낼 수 있다. 그러나 본 논문에서 제안한 기법은 M개의 빔행렬 후보들 중 $M/2$개는 $\boldsymbol{V}^{[m]}=\left[\boldsymbol{v}^{[1]},...,\boldsymbol{v}^{[b]},...,\boldsymbol{v}^{[N_t]}\right]\in\mathbb{C}^{N_t\times N_t}$이며, 나머지 $M/2$개는 $\boldsymbol{V}^{[m]}=\left[\boldsymbol{v}^{[1]},...,\boldsymbol{v}^{[b]},...,\boldsymbol{v}^{[N_t/2]}\right]\in\mathbb{C}^{N_t\times(N_t/2)}$로 이종 랭크를 갖도록 생성한다. 이때, 각 빔행렬을 이루는 b번째 빔벡터는 $\boldsymbol{v}^{[b]}\in\mathbb{C}^{N_t\times 1}$의 크기를 갖는다. 예를 들면, 빔행렬 후보가 8개일 경우, $4(=M/2)$개의 빔행렬 후보는 $4(=N_t)$개의 빔벡터들, 나머지 $4(=M/2)$개는 $2(=N_t/2)$개의 빔벡터들로 구성된다. 또한 기지국은 공인단말과 생성한 빔 정보를 공유한다고 가정한다. 기지국으로부터 $i\in\{1,...,N_{MS}\}$번째 공인단말, 비공인단말까지의 무선채널벡터는 각각 $\boldsymbol{h}_{MS,i}\in\mathbb{C}^{N_t\times 1}$와 $\boldsymbol{h}_{EVE}\in\mathbb{C}^{N_t\times 1}$이며, 거리에 따른 채널감쇠는 고려하지 않는다. 공인단말들은 무선채널벡터를 통해 수신되는 신호의 유효 SINR값을 기지국으로 피드백하며, 기지국은 인접 셀에 속한 비공인단말과 통신하는 다른 인접 기지국을 통해 $\boldsymbol{h}_{EVE}$을 알고 있다고 가정한다. 무선채널들은 독립적이며 균등한 분포 (i.i.d.)를 따르며, 1개 시간슬롯 또는 프레임동안 변하지 않는 준정적 상태를 가정한다. 기지국이 B개의 공인단말들에게 동시 전송가능한 데이터신호벡터는 $\boldsymbol{x}=\left[x_{1,...,}x_B\right]^T\in\mathbb{C}^{B\times 1}$이며, 기지국에서 동시 전송가능한 데이터신호의 수는 사용하는 빔행렬을 이루는 빔벡터 수 $B\in\{(N_t/2),(N_t)\}$에 의해 결정된다. 또한, 데이터신호의 전력제한 $\mathbb{E}[\|\boldsymbol{x}\|^2]=P$를 만족한다. 이러한 상황에서 기지국이 m번째 빔행렬 후보를 사용하여 데이터신호벡터 $\boldsymbol{x}$를 전송한다면, i번째 공인단말과 도청단말에서의 b번째 빔벡터를 통해 수신되는 수신신호는 다음과 같이 표현된다.

$$y_{MS,i}^{[m,b]}=(\boldsymbol{h}_{MS,i})^T\boldsymbol{v}^{[m,b]}x_b+\sum_{l\neq b,l=1}^{B}(\boldsymbol{h}_{MS,i})^T\boldsymbol{v}^{[m,l]}x_l+z_{MS,i}\,, \quad (1)$$

$$y_{EVE}^{[m,b]}=(\boldsymbol{h}_{EVE})^T\boldsymbol{v}^{[m,b]}x_{b+}\sum_{l\neq b,l=1}^{B}(\boldsymbol{h}_{EVE})^T\boldsymbol{v}^{[m,l]}x_l+z_{EVE}, \quad (2)$$

이때 첫 번째 항은 원하는 신호의 크기, 두 번째 항은 빔간 간섭 신호들의 크기의 합이며, 세 번째 항 $z_{MS,i}$와 n_{EVE}는 공인단말과 비공인단말에서 발생하는 복소가우시안분포의 열잡음으로 $CN(0,N_0)$의 분포를 따른다고 가정한다. 이러한 상황에서 유효 SINR을 다음과 같이 계산할 수 있다.

$$\gamma_{MS,i}^{[m,b]}=\frac{\left|(\boldsymbol{h}_{MS,i})^T\boldsymbol{v}^{[m,b]}\right|^2}{\sum_{l\neq b,l=1}^{B}\left|(\boldsymbol{h}_{MS,i})^T\boldsymbol{v}^{[m,l]}\right|^2+N_0/P}, \quad (3)$$

$$\gamma_{EVE}^{[m,b]}=\frac{\left|(\boldsymbol{h}_{EVE})^T\boldsymbol{v}^{[m,b]}\right|^2}{\sum_{l\neq b,l=1}^{B}\left|(\boldsymbol{h}_{EVE})^T\boldsymbol{v}^{[m,l]}\right|^2+N_0/P}. \quad (4)$$

만약 $M=8$, $N_t=4$를 가정한다면, 모든 공인단말들과 비공인단말은 $(MN_t/2)+(MN_t/4)=3MN_t/4=3\times 8\times 4/2=48$개의 모든 빔벡터들에 대해 전부 계산할 수 있다. 이때, 기지국에서 m번째 빔행렬 후보를 사용하여 전송한다면, 달성가능한 보안전송률(Achievable Secrecy Sum-Rate)을 다음과 같이 계산할 수 있다.

$$R_{SEC}^{[m]}=\left[\sum_{b=1}^{B}\log_2\left(1+\max_i\gamma_{MS,i}^{[m,b]}\right)-\log_2\left(1+\max_l\gamma_{EVE}^{[m,l]}\right)\right]^+. \quad (5)$$

기지국은 모든 빔행렬 후보 M개에 대해 (5)를 계산한 후, 보안전송률을 극대화할 수 있는 빔행렬 후보의 인덱스 $\hat{m}$를 결정한다.

$$\hat{m}=\arg\max_m R_{SEC}^{[m]}. \quad (6)$$

최종적으로 얻을 수 있는 극대화된 보안전송률은 $R_{SEC}^{[\hat{m}]}$이다.

Ⅲ. 시뮬레이션 결과

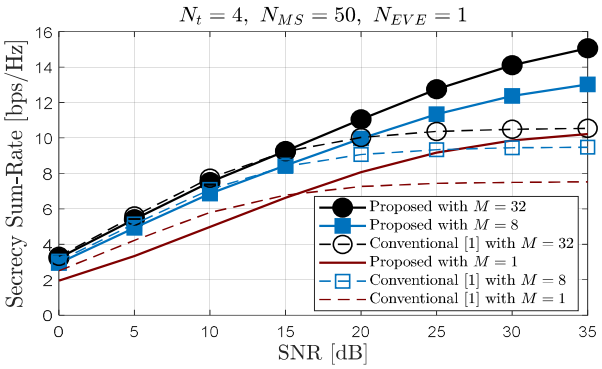

그림 1 제안한 기법과 기존 기법의 보안 전송률 성능 비교

그림 1은 본 논문에서 제안하는 기법과 기존 기법에 대해 기지국 안테나 수는 4개, 셀 내 공인단말 수는 50개, 셀 인접에 비공인단말 수는 1개일 때, 수신 SNR의 증가함에 따라 달성할 수 있는 보안 전송률을 보여준다. SNR이 낮은 영역에서 기존 기법의 보안전송률이 약간 우수하나, SNR이 높은 영역에서는 빔벡터를 더 적게 사용하는 제안한 기법이 기존 [1]의 성능보다 향상된다.

ACKNOWLEDGMENT

이 논문은 2019년도 과학기술정보통신부의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No.NRF-2019R1A2B5B01070697).

참 고 문 헌

[1] 손웅, 정방철, "하향링크 물리계층보안 향상을 위한 의사-무작위 빔포밍 기법,", in *Proc. of JCCI*, Mar. 2018.