

물리계층보안 향상을 위한 빔 선택기반 의사-무작위 빔포밍 및 기회적 피드백 기법

손 웅(충남대학교), 정방철(충남대학교)

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

A Pseudo-Random Beamforming with Beam Selection and Opportunistic Feedback for Improving Physical-Layer Security

Woong Son(CNU), Bang Chul Jung(CNU)

요약

본 논문은 하향링크 셀룰라 네트워크에서 물리계층보안 향상을 위하여 빔 선택기반 의사-무작위(pseudo-random) 빔포밍 기법과 기회적 피드백 기법을 제안한다. 시뮬레이션 결과를 통하여 제안한 기법이 물리계층보안을 향상시키면서도 상향링크 제어신호를 효과적으로 줄일 수 있음을 확인하였다.

I. 서론

최근 통신 네트워크에서 보안 성능 향상을 위하여 물리계층보안(physical-layer security) 개념이 정보이론을 이용하여 정립되었고 물리계층보안은 통신 네트워크의 보안성에 대한 중요한 지표가 되었다 [1]. 본 논문은 무선통신 네트워크에서 물리계층보안 향상을 위하여 빔 선택기반 다중 의사-무작위 빔포밍 기법을 제안하고 기회적 피드백 방법도 제안한다.

II. 제안하는 빔 선택기반 의사-무작위 빔포밍 및 기회적 피드백 기법

1. 시스템 모델

N_t 개의 안테나를 갖는 기지국과 단일 안테나를 갖는 공인 단말들이 N_u 개로 이루어진 하향링크 셀을 고려한다. 또한 셀 주변에 단일 안테나를 갖는 N_e 개의 도청 단말(eavesdropper)들이 존재한다. 기지국에서는 M 개의 의사-무작위 송신 빔 벡터 후보 $\{\mathbf{v}^{[1]}, \dots, \mathbf{v}^{[m]}, \dots, \mathbf{v}^{[M]}\}$ 들을 미리 생성하고 공인 단말들과 이를 공유한다. $\mathbf{v}^{[m]} \in \mathcal{C}^{1 \times N_t}$ 는 $m(m \in \{1, \dots, M\})$ 번째 빔 벡터 후보를 나타낸다. 기지국은 $i(i \in \{1, \dots, N_u\})$ 번째 공인 단말까지의 무선 채널 벡터 $\mathbf{h}_{u,i} \in \mathcal{C}^{1 \times N_t}$ 와 인접에 존재하는 $j(j \in \{1, \dots, N_e\})$ 번째 도청 단말까지 무선 채널 벡터 $\mathbf{h}_{e,j} \in \mathcal{C}^{1 \times N_t}$ 를 알고 있다고 가정한다. 기지국에서 m 번째 빔 벡터 후보를 이용하여 전송하였을 경우, i 번째 공인된 하향링크 단말에서의 수신 신호와 j 번째 도청 단말에서의 수신 신호는 다음과 같다.

$$y_{u,i}^{[m]} = \mathbf{h}_{u,i} (\mathbf{v}^{[m]})^H x + n_{u,i}, \quad (1)$$

$$y_{e,j}^{[m]} = \mathbf{h}_{e,j} (\mathbf{v}^{[m]})^H x + n_{e,j}, \quad (2)$$

여기서 $x \in \mathcal{C}$ 는 기지국에서 공인 단말로 전송하는 데이터 신호를 나타낸다. $n_{u,i} \sim \mathcal{CN}(0, N_0)$ 와 $n_{e,j} \sim \mathcal{CN}(0, N_0)$ 는 각각 공인 단말과 도청 단말에서 발생하는 가우시안 열잡음을 나타낸다.

2. 동작 절차

1) 기지국에서의 참조 신호 전송

기지국에서 참조 신호를 전송하면 공인 단말에서는 기지국으로부터의 공인 단말까지의 무선 채널 벡터를 추정한다.

2) 공인 단말에서의 SNR 계산 및 피드백

공인 단말들은 얻은 무선 채널 벡터와 기지국의 M 개의 빔 벡터 후보들을 이용하여 수신 SNR을 다음과 같이 계산하여 기지국으로 피드백한다.

$$SNR_{u,i}^{[m]} = \frac{|\mathbf{h}_{u,i} (\mathbf{v}^{[m]})^H|^2 P}{N_0}, \quad \forall m. \quad (3)$$

이때 기존 피드백 방법을 적용하면 M 개의 빔 벡터 후보들에 대한 모든 SNR값을 피드백한다. 이 SNR을 Q 비트로 양자화한다면 기존 피드백 방법에서의 단말 당 피드백 비트 수는 다음과 같다.

$$F_{conv} = \log_2 M + Q. \quad (4)$$

한편, 기회적 피드백 방법을 적용하면 M 개의 빔 벡터 후보들에 대해 모두 피드백 하는 것이 아닌 가장 높은 수신 SNR부터 낮은 순으로 $n(n < M)$ 개에 대해서만 피드백한다. 기회적 피드백 방법에서의 단말 당 피드백 비트 수는 다음과 같다.

$$F_{prop} = \log_2 n + Q. \quad (5)$$

3) 기지국에서의 도청 단말의 수신 SNR 계산

기지국에서는 도청 단말들에 대한 무선 채널 벡터 $\mathbf{h}_{e,j}$ 를 이용하여 수신 SNR을 다음과 같이 계산한다.

$$SNR_{e,j}^{[m]} = \frac{|\mathbf{h}_{e,j} (\mathbf{v}^{[m]})^H|^2 P}{N_0}, \quad \forall m. \quad (6)$$

4) 기지국에서의 최적의 빔 벡터 선택

기지국에서는 공인 단말들로부터 수집한 수신 SNR과 계산한 도청 단말에서의 수신 SNR을 기반으로 M 개의 빔 벡터 후보들을 사용하였을 경우 달성 가능한 전송률과 유출률을 다음과 같이 계산한다.

$$R_{u,rate}^{[m]} = \log_2 \left(1 + \max_{1 \leq i \leq N_u} SNR_{u,i}^{[m]} \right), \quad \forall m, \quad (7)$$

$$R_{d,rate}^{[m]} = \log_2 \left(1 + \max_{1 \leq j \leq N_e} SNR_{e,j}^{[m]} \right), \quad \forall m. \quad (8)$$

이를 이용하여 최적의 빔 벡터 참조번호 $\hat{m}$ 을 다음과 같이 결정한다.

$$\hat{m} = \underset{1 \leq m \leq M}{\operatorname{argmax}} (R_{u,rate}^{[m]} - R_{d,rate}^{[m]}). \quad (9)$$

5) 데이터 전송

기지국은 빔 벡터 후보 중, 최적의 빔 벡터 $\mathbf{v}^{[\hat{m}]}$ 을 이용하여 데이터를 전송한다.

III. 시뮬레이션 결과

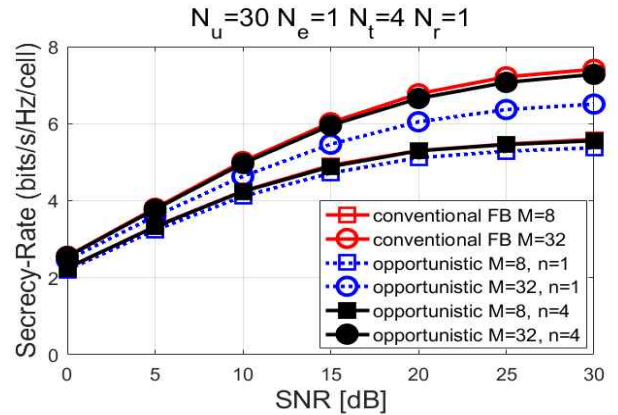


그림 1 제안한 기법의 보안 전송률 성능

그림 1은 제안하는 기법의 보안 전송률 성능을 보여준다. 제안한 기법에서 M 이 증가할수록 보안 전송률은 향상되고 기회적 피드백 기법에서는 상향링크 피드백 오버헤드와 성능사이에 Trade-Off가 존재한다.

ACKNOWLEDGMENT

이 논문은 2016년도 과학기술정보통신부의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.NRF-2016R1A2B4014834).

참고 문헌

- [1] Y. -S. Shiu, et al., "Physical layer security in wireless networks: A tutorial" *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66-74, Apr. 2011.
- [2] W. Son, B. C. Jung, and W.-H. Chang., "다중 빔포밍 행렬 선택기반 다중셀 의사-무작위 빔포밍 기법." *한국통신학회 논문지*, vol. 42, no. 7, pp. 1356-1359, Jul. 2017.