물리계층 보안 강화를 위한 하향링크 의사-무작위 빔포밍 기법

손웅, 정방철
충남대학교 전자공학과
e-mail : *woongson@cnu.ac.kr, bcjung@cnu.ac.kr*

A Pseudo-Random Beamforming Technique for Improving Physical-Layer Security in Downlink Cellular Networks

Woong Son and Bang Chul Jung
Department of Electronics Engineering
Chungnam National University

Abstract

In this paper, we consider a downlink cellular network which consists of a single base station (BS) with multiple antennas, U_d legitimate mobile stations (MSs) with a single antenna, and U_e eavesdroppers. In particular, we propose a pseudo-random beamforming (PRBF) technique which exploits multiple candidates of BF vectors in order to improve the physical-layer security, while reducing feedback overhead from MSs. Simulation results show that the proposed PRBF improves the secrecy rate as the number of BF candidates increases.

I. 서론

최근 무선통신에서 보안성 강화에 대한 요구가 거세지고 있다. 특히, 군통신 네트워크에서의 보안성은 민간 유무선 통신에 비하여 그 중요성이 더욱 높다. 학계에서는 물리계층보안 (physical-layer security)의 개념이 정보이론적으로 정의 되었으며, 이 개념은 물리계층에서 공인된 사용자가 비공인 사용자들이 존재하는 상황에서 최대로 얻을 수 있는 보안 전송률을 나타내는 지표로 활용되고 있다. 한편, 의사 무작위 빔포밍 기법이 다중셀 다중사용자 다중안테나 환경에서 셀룰라 네트워크의 하향링크 전송률을 개선하는 기법으로 제안되었다 [2]. 의사 무작위 빔포밍 기법은 기존의 순수 무작위 빔포밍 기법에 비하여 신호절차가 간소하고 사용자 단말기로부터의 피드백 오버헤드를 감소시키는 장점이 있다. 이 무작위 빔포밍 기법을 활용하여 수신자 주변에 존재하여 전송을 엿듣는 비공인 단말이 존재할 때, 유출 전송률을 최소화하는 기회적 스케쥴링 기법이 셀룰라 하향링크에서 제안되었다 [3]. 또한 상향링크에서 물리계층보안을 향상시키기 위하여 최적 다중사용자 다이버시티 이득을 달성할 수 있는 임계값 기반의 다중사용자 스케쥴링 셀룰라 단일 셀 상향링크에서 제안되었다 [4]. [4]에서 제안된 임계값 기반의 물리계층보안 강화를 위한 사용자 스케쥴링 기법은 다중셀 상향링크 환경으로 확장되었다 [5]. 그러나, [4-5]에서는 기지국과 단말기가 모두 단일안테나를 가진다고 가정하였다.

본 논문에서는 하향링크 셀룰라 네트워크에 하향링크 전송을 엿듣는 다중 비공인 단말들이 존재할 때, 보안 전송률을 향상시킬 수 있는 다중 의사-무작위 빔포밍 후보 선택기반 물리계층보안 향상기법을 제안한다.

II. 다중빔 선택기반 의사-무작위 빔포밍기법

2.1 시스템 모델

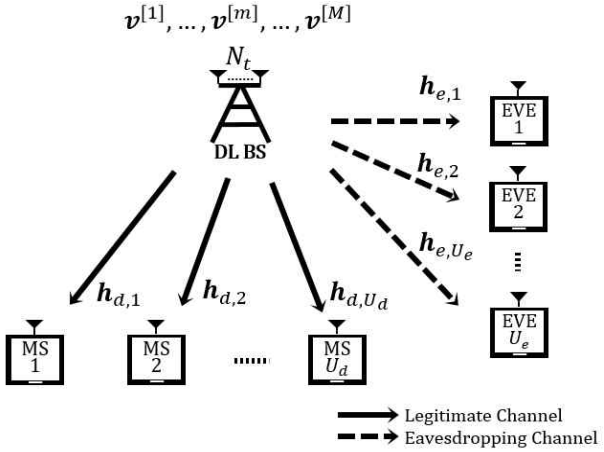

그림 1. 시스템 모델

본 절에서는 기밀 통신을 위한 의사-무작위 빔포밍 기법을 적용할 수 있는 하향링크 셀룰라 네트워크의 시스템 모델을 설명한다. N_t개의 송신 안테나를 갖는 하향링크 기지국과 단일 수신 안테나를 갖는 하향링크 단말이 U_d개 존재하며, 셀에 속하지 않은 비공인 단말 U_e개가 주변에 존재하여, 하향링크로 전송되는 신호를 엿들을 수 있고 엿들은 정보는 서로 공유하는 협력 구조를 갖는다고 가정한다. 또한, 기지국과 하향링크 단말들은 전송 전 M개의 의사-무작위 빔포밍 벡터 후보들인 $\boldsymbol{v}^{[1]},\ldots,\boldsymbol{v}^{[m]},\ldots,\boldsymbol{v}^{[M]}$에 대한 정보를 미리 공유하여 전송 전에 이미 알고 있다고 가정한다. 이때, m번째 빔포밍 벡터 $\boldsymbol{v}^{[m]} \in \mathbb{C}^{N_t \times 1}$를 선택하여 P의 전력 제한을 갖는 송신 신호 x를 전송한다고 가정하면, $i\left(i \in \{1,\ldots,U_d\}\right)$번째 하향링크 단말에서의 수신 신호는 다음과 같다.

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

이때, $\boldsymbol{h}_{d,i} \in \mathbb{C}^{1\times N_t}$는 기지국으로부터 i번째 하향링크 단말까지의 무선 채널 벡터를 의미하며, $n_{d,i}$는 i번째 하향링크 단말에서의 열잡음으로 $CN(0,1)$의 분포를 따른다.

유사하게 $j\left(j \in \{1,\ldots,U_e\}\right)$번째 비공인 단말에서의 수신 신호는 다음과 같다.

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

이때, $\boldsymbol{h}_{e,i} \in \mathbb{C}^{1\times N_t}$는 기지국으로부터 i번째 비공인 단말까지의 무선 채널 벡터를 의미하며, 이에 대해서는 기지국이 이미 알고 있다고 가정한다. 또한, j번째 비공인 단말에서의 열잡음 $n_{e,j}$는 $CN(0,1)$의 분포를 따른다.

2.2 기밀 통신을 위한 의사-무작위 빔포밍 기법 동작 절차

본 절에서는 기밀 통신을 위한 의사-무작위 빔포밍 기법에 대한 자세한 동작 절차를 설명한다.

2.2.1 기지국에서의 참조 신호 전송

하향링크 단말들이 기지국으로부터의 무선 채널 벡터를 획득할 수 있도록 기지국은 참조 신호를 방송한다.

2.2.2 하향링크 단말들의 SINR 피드백

참조 신호를 수신한 하향링크 단말들은 이미 알고 있는 기지국에서의 의사-무작위 빔포밍 벡터 M개에 대한 각 수신 SNR을 다음과 같이 계산하고 빔포밍 벡터 참조 번호를 함께 피드백한다.

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

2.2.3 비공인 단말에서의 수신 SINR 계산

기지국은 M개의 의사-무작위 빔포밍 벡터 후보들에 대해 이미 알고 있는 비공인 단말까지의 무선 채널 벡터를 이용하여 비공인 단말에서의 수신 SNR을 다음과 같이 계산한다.

$$SNR_{e,j}^{[m]} = \frac{|\boldsymbol{h}_{e,j}\boldsymbol{v}^{[m]}|^2 P}{N_0}, \quad \forall m. \quad (4)$$

2.2.4 기지국에서의 사용자 스케쥴링

기지국은 하향링크 단말로부터 수집된 정보를 기반으로 하향링크 전송률을 다음과 같이 계산한다.

$$R_{d,rate}^{[m]} = \log_2\left(1 + \max_{1 \le i \le U_d} SNR_{d,i}^{[m]}\right), \ \forall m. \quad (5)$$

또한, 비공인 단말로의 기밀 유출률을 다음과 같이 계산할 수 있다.

$$R_{e,rate}^{[m]} = \log_2\left(1 + \max_{1 \le i \le U_e} SNR_{e,i}^{[m]}\right), \ \forall m. \quad (6)$$

2.2.5 기밀 통신을 위한 최적의 의사-무작위 빔포밍 벡터 선택

기지국은 기밀 전송률을 극대화하는 최적의 의사-무작위 빔포밍 벡터의 참조 번호를 다음과 같이 선택한다.

$$\hat{m} = \arg\max_{m}\left(R_{d,rate}^{[m]} - R_{e,rate}^{[m]}\right). \quad (7)$$

2.2.6 하향링크로의 데이터 전송

기지국은 선택한 기밀 통신을 위한 최적의 의사-무작위 빔포밍 벡터 $\boldsymbol{v}^{[m]}$를 사용해서 하향링크로 전송하며, 이때의 물리계층 보안 전송률은 다음과 같이 얻는다.

$$R_{s,rate}^{[\hat{m}]} = R_{d,rate}^{[\hat{m}]} - R_{e,rate}^{[\hat{m}]}. \quad (8)$$

III. 시뮬레이션 결과 및 결론

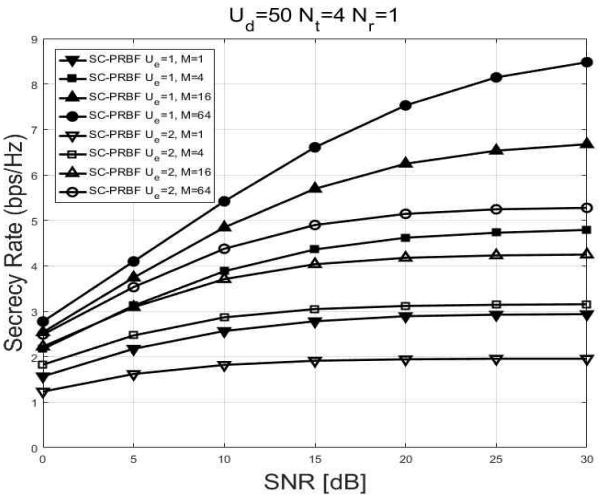

그림 2. 제안된 기법의 보안 전송률 성능

[그림2]는 1개의 셀 내부에 하향링크 단말이 50개 존재하고 이를 엿듣는 비공인 단말 수에 따른 시뮬레이션 결과를 보여준다. 빔포밍 벡터 후보 수가 증가할수록 보안 전송률이 향상된다.

본 논문에서는 물리계층 보안기밀 통신을 위한 의사-무작위 빔포밍 기법을 제안하고, 다양한 환경에서 시뮬레이션 실험을 통해 성능을 분석하였다. 특히 빔포밍 벡터 후보 수가 증가하면 보안 전송률이 향상되는 것을 확인하였다.

Acknowledgement

본 연구는 방위사업청과 국방과학연구소가 지원하는 미래전투체계 네트워크 기술 특화연구센터 사업의 일환으로 수행되었습니다. (UD160070BD)

참고문헌

[1] Y. -S. Shiu, *et al.*, "Physical layer security in wireless networks: A tutorial" *IEEE Wireless Commun.*, vol. 18, no. 2, Apr. 2011.

[2] W. Son, B. C. Jung, and W.-H. Chang., "다중 빔 포밍 행렬 선택기반 다중셀 의사-무작위 빔포밍 기법." *한국통신학회 논문지*, Vol. 42, No. 7, pp. 1356-1359, Jul. 2017.

[3] I. Krikidis and B. Ottersten, "Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling," *IEEE Signal Process. Lett.*, vol. 20, no. 2, pp. 141 - 144, Feb. 2013.

[4] H. Jin, W.-Y. Shin, and B. C. Jung, "On the multi-user diversity with secrecy in uplink wiretap networks," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1778 - 1781, Sep. 2013.

[5] H. Jin, B. C. Jung, and W.-Y. Shin "On the secrecy capacity of multi-cell uplink networks with opportunistic scheduling," *Proc. IEEE ICC,* May 2016.