잠재 도청자가 존재하는 다중안테나 하향링크 셀룰라 네트워크의 물리계층 보안 성능

오민규, 손웅, 정방철
충남대학교 전자공학과
dmb02048@o.cnu.ac.kr, woongson@cnu.ac.kr, bcjung@cnu.ac.kr

Physical-Layer Security Performance of MIMO Cellular Downlink Networks with Potential Eavesdroppers

Min Kyu Oh, Woong Son, Bang Chul Jung
Dept. of Electronics Engineering, Chungnam National University

요 약

본 논문에서는 다중 안테나를 탑재한 기지국과 이로부터 메시지를 수신할 수 있는 다수의 공인 사용자들(legitimate users)과 자신의 스케쥴에 따라 도청여부를 결정하는 다수의 잠재 도청자들로 이루어진 다중 사용자 하향링크 네트워크에서의 물리계층 보안 아웃티지 확률 (secrecy outage probability, SOP)를 분석하였다. 기지국으로부터 방송된 참조신호를 이용하여 각 사용자들은 채널상태정보를 파악하고, 자신의 무선 채널이득이 피드백 임계치 이상일 경우에만 기지국으로 피드백한다. 기지국은 채널상태정보를 피드백한 사용자들 중 각 사용자에게 대응하는 최대비전송 (maximum ratio transmission, MRT) 빔포밍을 수행한다는 가정하에 무선 채널이득을 극대화할 수 있는 사용자를 선택하여 메시지를 송신한다. 모의실험을 통해, 기지국에서 최대비전송 빔포밍을 수행하는 경우가 단일 안테나 기지국일 경우보다 보안 아웃티지 성능이 우수하고, 피드백 임계치가 큰 값임에도 불구하고 사용자 수가 충분히 존재할 경우에는 모든 사용자가 피드백하는 경우와 거의 유사한 보안 아웃티지 성능을 달성하는 것을 확인하였다.

Ⅰ. 서 론

사물인터넷 기술의 발전에 따라 개인 정보 유출 우려에 대한 보안 문제들이 대두되고 있다. 특히, 도청 문제를 해결을 위해서 비용효율적인 물리계층보안 기술들이 현재 부상중이며, 관련 연구들이 활발히 진행중이다 [1]. 최근에는 도청자의 스케쥴에 따라 도청여부를 결정하는 잠재 도청자를 수학적으로 정의하고 물리계층보안 성능을 분석한 연구가 발표되었다 [2]. 본 논문에서는 잠재 도청자가 존재할 경우에 기지국의 다중 안테나를 이용한 최대비전송 빔포밍 기술을 수행할 때, 기존 단일 안테나를 고려할 경우 [2]대비 보안 아웃티지 성능 향상을 확인하였다.

Ⅱ. 최대비전송 빔포밍을 고려한 하향링크 네트워크 시스템 모델 및 보안 아웃티지 성능 분석

N_t개의 안테나를 탑재한 하향링크 기지국과 단일 안테나를 탑재한 N_{MS}개의 사용자와 N_{E}개의 도청자가 존재하는 하향링크 네트워크를 고려한다. 기지국으로부터 $i\in\{1,2,...,N_{\mathrm{MS}}\}$번째 사용자까지의 무선 채널벡터는 $\boldsymbol{h}_{\mathrm{MS},i}\in\mathbb{C}^{1\times N_t}$이고, 각 성분은 $CN(0,\sigma_{\mathrm{MS}}^2)$을 따른다. 유사하게 $j\in\{1,2,...,N_{\mathrm{E}}\}$번째 도청자까지의 무선 채널벡터는 $\boldsymbol{h}_{\mathrm{E},j}\in\mathbb{C}^{1\times N_t}$이고, 각 성분은 $CN(0,\sigma_{\mathrm{E}}^2)$을 따른다. 모든 무선 채널벡터 성분들은 독립항등분포이고, 통신 중 변하지 않는 준정적 상태를 가정한다. 기지국이 i번째 사용자에게 메시지를 송신한다고 가정할 때, 기지국에서 $\mathbb{E}[|s_{\mathrm{MS},i}|^2]=P$의 전력 제한을 만족하는 최대비전송 빔포밍으로 전처리된 송신 메시지 벡터는 $\boldsymbol{s}_{\mathrm{MS},i}=(\sqrt{P}\boldsymbol{h}_{\mathrm{MS},i}^H/\|\boldsymbol{h}_{\mathrm{MS},i}\|)s\in\mathbb{C}^{N_t\times 1}$이다. i번째 사용자와 j번째 도청자에서의 수신 신호는 각각 다음과 같다.

$$r_{\mathrm{MS},i}=\boldsymbol{h}_{\mathrm{MS}}\boldsymbol{s}_{\mathrm{MS},i}+w_{\mathrm{MS},i}=\sqrt{P}\|\boldsymbol{h}_{\mathrm{MS},i}\|s+w_{\mathrm{MS},i},$$
$$r_{\mathrm{E},j}=\boldsymbol{h}_{\mathrm{E}}\boldsymbol{s}_{\mathrm{MS},i}+w_{\mathrm{E},j}=\left(\sqrt{P}\boldsymbol{h}_{\mathrm{E},j}\boldsymbol{h}_{\mathrm{MS},i}^H/\|\boldsymbol{h}_{\mathrm{MS},i}\|\right)s+w_{\mathrm{E},j}.$$

이때, $w_{\mathrm{MS},i}$와 $w_{\mathrm{E},j}$는 각각 i번째 사용자와 j번째 도청자에서의 열잡음으로 모두 $CN(0,N_0)$ 분포를 따른다. 기지국으로부터 참조신호를 수신한 사용자들은 유효 무선 채널이득이 $\|\boldsymbol{h}_{\mathrm{MS},i}\|^2\geq\zeta_{\mathrm{MS}}$를 만족하는 경우에만 메시지 수신을 위해 채널상태정보를 기지국으로 피드백한다. 이때, ζ_{MS}는 피드백 임계치이며, $\zeta_{\mathrm{MS}}=0$일 경우에는 사용자들이 항상 피드백 (full feedback, FF)하고, $\zeta_{\mathrm{MS}}>0$일 경우에는 조건을 만족하는 일부 사용자만 피드백(opportunistic feedback, OF)한다. N_{MS}개의 사용자들 중에서 피드백한 사용자들로 이루어진 집합을 $\mathcal{M}_{\mathrm{MS}}$로 정의한다. 도청자들은 도청확률 $P_{\mathrm{E}}\in[0,1]$을 기반으로 도청을 수행하며, $P_{\mathrm{E}}=1$일 경우에는 모든 도청자들이 도청을 수행(full eavesdropping, FE)하고, $0<P_{\mathrm{E}}<1$일 경우에는 일부 도청자들이 도청을 수행(random eavesdropping, RE)한다. N_{E}개의 도청자들 중에서 도청을 수행하는 도청자들로 이루어진 집합을 $\mathcal{M}_{\mathrm{E}}$로 정의한다. 위 시스템 모델에서 달성할 수 있는 보안 전송률과 보안 아웃티지 확률은 각각 다음과 같다.

$$R_s(|\mathcal{M}_{\mathrm{MS}}|,|\mathcal{M}_{\mathrm{E}}|)=\max_{j\in\mathcal{M}_{\mathrm{E}}}\left(\log_2\left(\max_{i\in\mathcal{M}_{\mathrm{MS}}}\left(\frac{1+\Gamma_{\mathrm{MS},i}}{1+\Gamma_{\mathrm{E},j}^{[i]}}\right)\right)\right),$$
$$P_{\mathrm{out}}=\Pr\left(R_s(|\mathcal{M}_{\mathrm{MS}}|,|\mathcal{M}_{\mathrm{E}}|)<R_0\right).$$

이때, i번째 사용자에서의 유효 수신대잡음비(signal to noise ratio)는 $\Gamma_{\mathrm{MS},i}=\rho\|\boldsymbol{h}_{\mathrm{MS},i}\|^2$, 기지국으로부터 선택된 i번째 사용자에게 대응하는 최대비전송 빔포밍으로 전처리된 메시지가 송신된다는 가정하에 j번째 도청자에서의 유효 수신대잡음비(signal to noise ratio, SNR)는 $\Gamma_{\mathrm{E},j}^{[i]}=\rho\left(\boldsymbol{h}_{\mathrm{E},j}\boldsymbol{h}_{\mathrm{MS},i}^H/\|\boldsymbol{h}_{\mathrm{MS},i}\|\right)^2$이며, $\rho=P/N_0$이다. 또한, 목표 보안 전송률은 R_0 [bps/Hz], $|\cdot|$은 집합의 성분 수를 의미한다. 최종적으로 기지국은 채널상태정보를 피드백한 사용자 중에서 각 사용자에 대응하는 최대비전송 빔포밍으로 전처리할 경우, 하향링크 전송률을 최대화할 수 있는 사용자를 선택하여 데이터 신호를 송신하며, 도청을 수행하는 도청자들에 의해 하향링크 송신 메시지가 도청된다.

Ⅲ. 모의실험 결과 및 결론

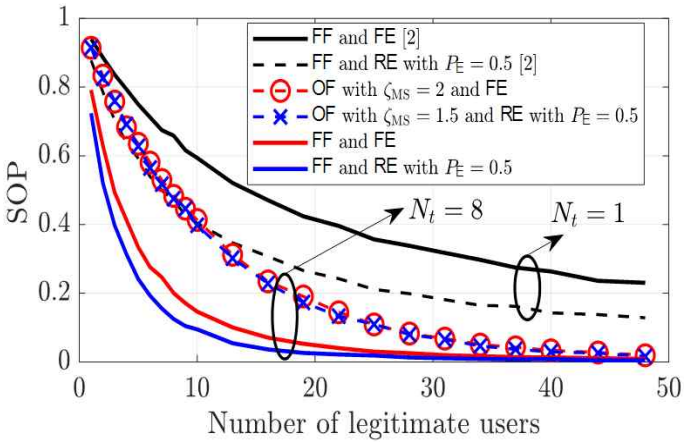

그림 1. 보안 아웃티지 확률 비교 결과

앞에서 고려한 시스템 모델에서 $\rho=0$ [dB], $N_{\mathrm{E}}=5$, $\sigma_{\mathrm{MS}}^2=1$, $\sigma_{\mathrm{E}}^2=0.5$, $R_0=1$ [bps/Hz]일 경우, 사용자 수에 따른 보안 아웃티지 확률을 분석하였다. 기지국 안테나 수가 최대비전송 빔포밍을 수행하는 $N_t=8$개일 경우가 $N_t=1$개일 경우 [2]보다 보안 아웃티지 확률이 우수하다. 또한 $\zeta_{\mathrm{MS}}>0$인 경우(OF), 충분한 수의 사용자가 존재한다면 다중 사용자 다중화 이득으로 $\zeta_{\mathrm{MS}}=0$의 경우(FF)와 거의 유사한 보안 아웃티지 확률을 달성한다.

ACKNOWLEDGMENT

본 연구는 미래창조과학부 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2019R1A2B5B01070697).

참 고 문 헌

[1] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun.. Survey & Tuts.*, vol. 21, no. 2, pp. 1773-1828, 2nd Quart. 2019.

[2] W. Son, H. Nam, W.-Y. Shin and B. C. Jung, "Secrecy outage analysis of multi-user downlink wiretap networks with potential eavesdroppers," *IEEE Systems Journal*, early access, Jul. 2020.