# 잠재 도청자가 존재하는 무선 네트워크의 보안 성능 분석

손 웅 (충남대학교), 신원용 (연세대학교), 정방철 (충남대학교)
woongson@cnu.ac.kr, wy.shin@yonsei.ac.kr, bcjung@cnu.ac.kr

# Secrecy Performance Analysis of Wireless Network with Potential Eavesdroppers

Woong Son (CNU), Won-Yong Shin (Yonsei Univ.), Bang Chul Jung (CNU)

## 요 약

본 논문에서는 동일셀 또는 이웃셀에 등록되었으나, 스케쥴링되지 않은 다수의 잠재 도청자(potential eavesdropper)를 고려한 다중사용자 하향링크 무선 네트워크에서의 물리계층보안 성능을 분석한다. 특히, 하향링크 기지국은 다수의 공인 사용자뿐만 아니라 잠재 도청자까지의 채널상태정보 및 잠재 도청자 수, 도청여부를 알 수 있기 때문에, 이 정보들을 기반으로 최대 공인채널이득의 공인단말 1개를 선택하여 데이터를 하향링크로 전송한다. 한편, 공인 사용자들은 공인채널이득이 특정 임계치 이상일 경우에만 스케쥴링을 위한 유효채널이득을 피드백하는 기회적 피드백(opportunistic feedack, OF)과 간헐적으로 도청하는 무작위 도청(random eavesdropping, RE)을 함께 고려하였다. 모의실험을 통해 물리계층 보안 아웃티지 확률(secrecy outage probability, SOP)을 분석하였고, OF에서 채널 임계치가 높더라도 공인 사용자가 충분히 많이 존재할 경우, 스케쥴링을 위해 공인 사용자에서의 공인채널이득을 항상 피드백(full feedback, FF)하는 기법과 SOP 성능이 거의 동일한 수준을 유지하는 것을 확인했다.

## Ⅰ. 서 론

개인용 스마트 기기들의 수가 폭증함에 따라 보안통신이 매우 중요한 문제로 거듭나면서, 통신 계층별 다양한 보안통신 기술들이 연구되고 있다. 그 중 물리계층에서의 보안통신 기술들은 비용 및 에너지 효율적인 방법으로 잘 알려져있다 [1]. 특히, 기존에 잠재 도청자를 고려한 셀룰라 네트워크에서의 물리계층 보안 성능을 분석했다 [2][3]. 본 논문에서는 기존 정의된 잠재 도청자 [2][3]를 포괄하여 공인채널이득에 대한 임계치기반 기회적 피드백 기법(OF)을 제안하였으며, 잠재 도청자의 무작위 도청(RE)을 고려한 SOP 성능을 모의실험을 통해 분석하였다.

## Ⅱ. 잠재 도청자들이 존재하는 무선 네트워크

1개의 기지국과 $N_{\mathrm{MS}}$개의 공인 사용자 및 $N_{\mathrm{E}}$개의 잠재 도청자들이 존재하는 하향링크 네트워크 시스템 모델을 고려한다. 공인 기지국과 $i\in\{1,2,...,N_{\mathrm{MS}}\}$번째 공인 사용자와 기지국간 무선채널은 $h_{\mathrm{MS},i}\sim CN(0,\sigma^2_{\mathrm{MS}})$, $j\in\{1,2,...,N_{\mathrm{E}}\}$번째 잠재 도청자까지 무선채널은 $h_{\mathrm{E},i}\sim CN(0,\sigma^2_{\mathrm{E}})$로 정의되며, 독립적이고 균등한 분포 및 전송중 준정적상태를 가정한다. 한편, 기존 정의된 잠재 도청자 [2][3]들은 동일셀에 속하는 일부 또는 스케쥴링되지 않은 공인 사용자들을 잠재 도청자로 정의하였다. 그러나 본 논문에서는 동일셀뿐만 아니라 이웃셀의 공인 사용자들도 잠재 도청자가 될 수 있다. 또한 기지국은 공인 사용자들과 잠재 도청자들에 대한 채널상태정보를 알 수 있다고 가정한다. 기지국이 전력제한 $\mathbb{E}[|s|^2]=P$를 만족하는 데이터 신호 $s$를 하향링크로 전송할 때, $i$번째 공인 사용자와 $j$번째 잠재 도청자에서의 수신신호 모델은 다음과 같다.

$$r_{\mathrm{MS},i}=h_{\mathrm{MS},i}s+w_{\mathrm{MS},i},\qquad r_{\mathrm{E},j}=h_{\mathrm{E},j}s+w_{\mathrm{E},j},$$

이때 각 열잡음 $w_{\mathrm{MS},i}$와 $w_{\mathrm{E},j}$는 $CN(0,N_0)$ 분포를 따른다.

공인 사용자들의 스케쥴링을 위한 기회적 피드백(OF) 기법에서는 $i$번째 공인 사용자들은 $|h_{\mathrm{MS},i}|^2\geq\zeta_{\mathrm{MS}}$을 만족할 경우에만 기지국으로 무선채널이득을 피드백하며, $\zeta_{\mathrm{MS}}=0$일때에는 매 스케쥴링마다 무선채널이득을 피드백(FF)한다. 모든 잠재 도청자들은 각각 $P_{\mathrm{E}}\in[0,1]$의 확률로 무작위 도청(RE)을 시도하며, $P_{\mathrm{E}}=1$일때에는 항상 도청(full eavesdropping, FE)을 시도한다. 기지국은 최대 보안전송률을 달성할 수 있는 공인 사용자를 선택하여 데이터 신호를 전송한다. 최대 달성가능한 보안 전송률과 목표 보안전송률(target secrecy rate)이 $R_0$ [bps/Hz]일 경우의 SOP는 다음과 같다.

$$R_s(|\mathcal{M}_{\mathrm{MS}}|,|\mathcal{M}_{\mathrm{E}}|)=\log_2\left(\frac{1+\max_{i\in\mathcal{M}_{\mathrm{MS}}}|h_{\mathrm{MS},i}|^2\rho}{1+\max_{j\in\mathcal{M}_{\mathrm{MS}}}|h_{\mathrm{E},j}|^2\rho}\right),$$

$$P_{\mathrm{out}}(N_{\mathrm{MS}},N_{\mathrm{E}})=\Pr(R_s(|\mathcal{M}_{\mathrm{MS}}|,|\mathcal{M}_{\mathrm{E}}|)<R_0,)$$

이때 $|\mathcal{A}|$는 집합 $\mathcal{A}$의 cardinality이며, $\mathcal{M}_{\mathrm{MS}}$는 $N_{\mathrm{MS}}$개의 전체 공인 사용자들 중 스케쥴링을 받기위해 무선채널이득을 기지국으로 피드백한 사용자들의 집합이며, $\mathcal{M}_{\mathrm{E}}$는 $N_{\mathrm{E}}$개의 전체 잠재 도청자들 중 도청을 시도하는 도청자들의 집합이다. 또한 $\rho$는 수신 신호대잡음비(signal-to-noise ratio, SNR) [dB]이다.

## Ⅲ. 모의실험 결과 및 결론

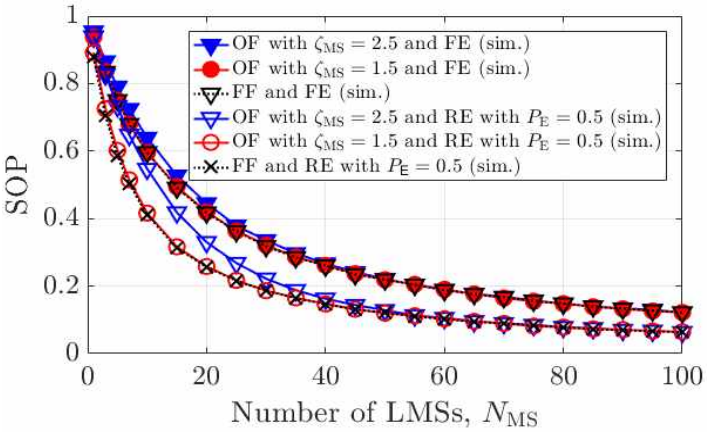


그림 1. SOP 성능 분석 결과

그림 1은 소개한 시스템 모델에서 $\rho=0$ [dB], $N_{\mathrm{E}}=5$, $\sigma^2_{\mathrm{MS}}=1$, $\sigma^2_{\mathrm{E}}=0.5$, $R_0=1$ [bps/Hz]일 경우, 공인사용자 수에 따른 SOP 성능에 대한 모의실험 결과를 보여준다. 공인링크 기준에서 살펴보면, 기회적으로 피드백하는 OF보다 FF에서의 SOP 성능이 항상 우수하며, 확률적 도청을 하는 RE보다 FE에서의 SOP 성능이 항상 낮다. 그러나 OF에서 채널 임계치 $\zeta_{\mathrm{MS}}$를 낮출수록 FF의 SOP 성능과 근접해진다. 또한 채널 임계치 $\zeta_{\mathrm{MS}}$가 높더라도 사용자 수 $N_{\mathrm{MS}}$가 충분히 많이 존재한다면, 다중-사용자 다이버시티 이득으로 FF의 SOP 성능 수준을 유지할 수 있다.

## ACKNOWLEDGMENT

This work was supported by the NRF through the Basic Science Research Program funded by the Ministry of Science and ICT under Grant NRF2019R1A2B5B01070697.

## 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] M. A. Abbas, H. Song, and J.-P. Hong, "Opportunistic scheduling for average secrecy rate enhancement in fading downlink channel wit potential eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 969-980, Apr. 2019.

[3] I. Bang and B. C. Jung, "Secrecy rate analysis of opportunistic user scheduling in uplink networks with potential eavesdroppers," *IEEE Access*, vol. 7, no. 1, pp. 127078-127089, Sep. 2019.