보안-에너지 효율 향상을 위한 잠재적 도청자 기반 기회적 전송 기법

오민규, 손웅, 정방철
충남대학교 전자공학과
e-mail : dmb02048@o.cnu.ac.kr, woongson@cnu.ac.kr, bcjung@cnu.ac.kr

Opportunistic Transmission Technique against a Potential Eavesdropper for Improving Secrecy Energy-Efficiency

Min Kyu Oh, Woong Son and Bang Chul Jung
Department of Electronics Engineering
Chungnam National University

Abstract

We investigate a wire-tap network, in which a transmitter, a receiver and a potential eavesdropper. We also propose an opportunistic transmission (OT) for maximizing secrecy energy-efficiency (SEE). In the proposed OT, the legitimate transmitter attempts to transmit a data signal with a scaled transmission power using a transmission probability based on channel thresholds for legitimate and eavesdropping channel gain to the legitimate receiver. Computer simulation results shown that the optimal SEE can be achieved in the proposed OT with the optimal threshold.

I. 서론

통신 기술의 발달로 5세대 이동 통신의 상용화와 함께 무선 통신 시스템은 일상생활을 비롯하여 다양한 분야에 필수적인 요소로 자리 잡고 있다 [1]. 이에 따라, 무선 통신 시스템에서의 개인 정보 유출 우려에 대한 보안 문제들이 대두되고 있다. 기존에는 애플리케이션 및 네트워크 계층 등의 상위 계층에서 적용할 수 있는 보안 기법들이 중심이 되었지만, 최근에는 mmWave 및 THz 통신 기술이 발달하면서 물리 계층에서 원천적으로 악의적인 단말이 보안성이 중요한 메시지를 수신할 수 없도록 할 수 있는 물리 계층기반의 보안 통신 기술들이 떠오르고 있다 [2]. 따라서, 물리 계층 보안 (physical-layer security)은 도청자가 존재하는 상황에서 무선 채널의 무작위성 및 기회성을 이용하여 공인단말간의 채널과 도청자까지의 채널의 비대칭성을 이용하여 통신하여 무선 통신 시스템의 보안 용량을 향상시킨다. 이와 관련하여 최근에는 잠재도청자까지의 채널 정보를 기반으로 채널 이득 임계치 기반의 기회적 사용자 스케쥴링 기법 [3] 및 기회적 피드백 기법 [4]을 제안하고 물리계층보안 성능을 분석한 연구가 발표되었다. 본 논문에서는 잠재도청자가 존재하는 무선 네트워크에서의 송신기로부터 수신기까지의 채널 이득 임계값과 도청자까지의 채널 이득 임계값을 동시에 고려한 기회적 전송 기법을 제안하고, 이에 대한 보안 에너지 효율성을 분석하였다.

II. 보안-에너지 효율성 향상을 위한 기회적 전송 기법

2.1 시스템 모델

단일 안테나를 탑재한 송신기와 수신기, 도청자가 존재하는 무선 네트워크를 고려한다. 이 논문에서 고려하는 도청자는 공인단말들 중 하나이며, 의도치 않게 엿듣는 잠재도청자로 가정한다. 송신기로부터 수신기까지의 무선 채널은 h이고, $CN(0,\sigma_h^2)$의 분포를 따른다. 기지국으로부터 도청자까지의 무선 채널은 g이고, 채널 성분은 $CN(0,\sigma_g^2)$의 분포를 따른다. 모든 무선 채널 성분들은 독립항등분포이고, 통신 중 변하지 않는 준정적 상태를 가정한다. 송신기는 수신기로 메시지 s를 전송할 때, 수신기와 도청자에게서의 수신 신호는 각각 다음과 같다.

$$y_{\mathrm{R}} = hs + w_{\mathrm{R}}, \qquad y_{\mathrm{E}} = g\,s + w_{\mathrm{E}}.$$

이때, w_R와 w_E는 각각 수신기와 도청자에게서의 열잡음으로 모두 $CN(0,N_0)$ 분포를 따른다.

2.2 기회적 전송 기법

송신기는 수신기 및 도청자까지의 무선채널 이득을 고려하여, $|h|^2 \geq \alpha$와 $|g|^2 \leq \beta$를 동시에 만족하는 경우에만 기회적으로 메시지를 전송한다. 이때, α는 수신기까지의 무선채널 이득에 대한 임계값, β는 도청자까지의 무선채널 이득에 대한 임계값이다. 이때 송신기가 메시지 전송 확률 γ은 다음과 같다.

$$\gamma = \Pr(|h|^2 \geq \alpha, |g|^2 \leq \beta) = \Pr(|h|^2 \geq \alpha)\Pr(|g|^2 \leq \beta).$$

이때 α가 작아지면 공인링크의 채널 품질이 낮을 때에도 전송한다. 반면, β가 커지면 도청링크의 채널 품질이 높을 때에도 전송한다. 기회적 전송 기법을 적용하면, 송신기는 위 조건을 만족하는 순간마다 송신전력 $\gamma^{-1}P$로 메시지를 송신한다.

2.3 물리계층보안 성능

위 시스템 모델과 기회적 전송 기법을 고려하였을 때, 시스템에서 평균 달성할 수 있는 보안 전송률 R_s와 보안 에너지 효율성 η는 다음과 같다.

$$R_s = \gamma\ \mathbb{E}\left[\log_2\left(\frac{1+|h|^2\gamma^{-1}\rho}{1+|g|^2\gamma^{-1}\rho}\right)\right], \qquad \eta = \frac{R_s}{P},$$

이때 수신기에서의 유효 수신 신호대잡음비 (signal to noise ratio)는 $|h|^2\gamma^{-1}\rho$, 도청자에서의 유효 수신 신호대잡음비는 $|g|^2\gamma^{-1}\rho$이고, $\rho = P/N_0$이다.

Ⅲ. 시뮬레이션 분석 및 결론

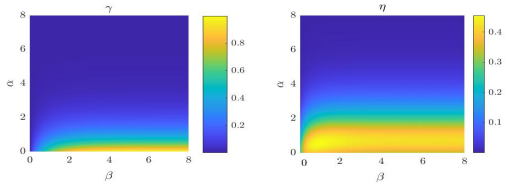

그림 1. 임계치에 따른 전송확률 γ(좌) 및 보안 에너지 효율성 η(우)

그림 1은 $\rho = 0$ [dB], $\sigma_h^2 = \sigma_g^2 = 1$인 시스템 모델에서 기회적 전송 기법을 적용하였을 때의 송신기에서 수신기까지의 무선채널 이득에 대한 임계값 α와 도청자까지의 무선채널 이득에 대한 임계값 β에 따른 전송확률 및 보안 에너지 효율성을 보여준다. α가 작아지거나 β가 커질 경우 전송확률이 1에 가까워진다. 반면, 보안 에너지 효율성 측면에서는 $\alpha = 0.7$ 및 $\beta = 1.2$일 경우, 보안 에너지 효율성 η는 약 0.4522 [bit/Hz/Joule] 으로 극대화되며, 이때 송신기의 전송확률 γ는 약 0.347의 값을 갖는다.

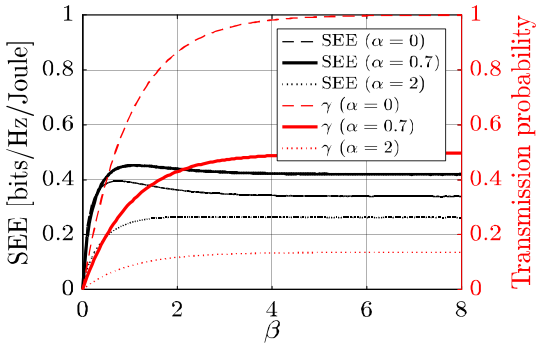

그림 2. 전송 확률 및 보안 에너지 효율성 분석 결과

그림 2는 β에 따른 전송확률 및 보안 에너지 효율성 분석 결과를 보여준다. β가 커질수록 도청자까지의 무선채널 이득이 커지는 것을 허용하는 수준이 증가하므로, 전송확률이 증가한다. 그러나 α가 주어졌을 경우, 보안 에너지 효율성을 극대화하는 β가 존재한다. 따라서 공인링크의 채널과 도청링크의 채널정보를 기반으로 기회적 전송 기법을 적용하면, 기존 대비 보안 에너지 효율성을 향상시킬 수 있다.

Acknowledgement

이 논문은 2021년도정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (2019-0-00964, 스펙트럼 챌린지를 통한 기존 무선국 보호 및 주파수 공유기술 개발).

참고문헌

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679-695, April. 2018.

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

[3] I. K. Bang and B. C. Jung, "Secrecy rate analysis of opportunistic user scheduling in uplink networks with potential eavesdroppers," *IEEE Access*, vol. 7, pp. 127078-127089, 2019

[4] W. Son, H. Nam, W.-Y. Shin and B. C. Jung, "Secrecy outage analysis of multiuser downlink wiretap networks with potential eavesdroppers," *IEEE Syst. J.*, Vol. 15, No. 2, pp. 3093-3096, Jun. 2021.