논문 19-44-07-08 The Journal of Korean Institute of Communications and Information Sciences '19-07 Vol.44 No.07
https://doi.org/10.7840/kics.2019.44.7.1295

채널 추정 오류를 고려한 비신뢰적 릴레이를 통한 보안 통신

이 준 섭•, 이 기 송°

Secure Communication Via Untrusted Relay with Channel Estimation Error

JunSeob Lee•, Kisong Lee°

요 약

본 논문에서는 채널 추정 오류를 반영하여 신뢰할 수 없는 릴레이가 존재하는 시스템의 보안 전송률을 수식적으로 모델링 하였으며, 시뮬레이션을 통해 이를 최대화 할 수 있는 최적의 방해 신호 전력 비율을 찾았다. 시뮬레이션 결과는 채널 추정 오류가 존재하는 시스템에서 보안 전송률을 향상시키기 위해서는 효율적인 방해 전력 제어가 필요하다는 것을 보여준다.

Key Words : Physical layer security, secrecy rate, channel estimation error, secure relaying

ABSTRACT

In this paper, we formulate the secrecy rate of an untrusted relay system with channel estimation error, and find the optimal jamming power ratio for maximizing the secrecy rate through simulations. The results show that it is required to control jamming power effectively to improve the secrecy rate in the system with channel estimation error.

Ⅰ. 서 론

무선 신호는 전방향으로 방사한다는 특성 때문에 필연적으로 도청의 위협에 노출되어 있다. 최근 무선 통신의 보안을 향상시키기 위해서, 기존의 암호화 기반 보안 기술의 대안으로써 물리 계층 보안에 대한 연구가 활발히 수행 되고 있다.

물리 계층 보안의 가장 대표적인 방안으로는 송신단의 신호와 함께 인위적인 방해 신호를 전송함으로써 도청자가 송신단의 신호를 해석하는 것을 방해하게 하는 협력적 방해 신호 전송이 있다[1]. 특히 수신단에서 방해 신호를 전송하는 방식은 방해 신호 전송을 위한 추가적인 노드나 안테나가 필요하지 않아 비용적인 면에서 효과적이다[2]. 하지만 릴레이와 수신단 사이 채널의 정확한 Channel State Information(CSI)를 알지 못하면 수신단은 릴레이 신호로부터 방해 신호를 완벽하게 제거할 수가 없다. 실제 무선 통신 환경에서는 채널을 완벽하게 추정하는 것은 불가능하며, 이는 수신단 측에 잔류 방해 신호를 발생시켜 시스템의 성능이 현저히 감소하게 된다[3-5]. 본 논문에서는 채널 추정 오류를 고려하여 신뢰할 수 없는 릴레이가 존재하는 시스템의 보안 전송률을 수식적으로 도출하고자 한다. 또한, 시뮬레이션을 통해서 보안 전송률을 최대화하는 최적의 방해 전력 비율이 존재함을 확인하고, 기존의 방안과 비교하여 방해 전력 제어가 시스템의 성능 향상에 미치는 효과를 보이고자 한다.

Ⅱ. 시스템 모델

본 논문에서는 그림 1에서 보는 바와 같이 송신단, 수신단, 신뢰할 수 없는 릴레이로 구성된 시스템을 고려한다. 각 노드들은 half-duplex로 동작하며, 한 개의 송수신 안테나를 갖는다. 또한, 송신단과 수신단 사이의 직접 링크는 존재하지 않으므로, 릴레이는 증폭-후-전달 (Amplify-and-Forward) 프로토콜을 통해서 송신단과 수신단 사이의 통신을 돕는다[2,5]. 노드 i와 j 사이의 채널은 h_{ij}로 표현하고, $h_{ij} \sim CN(0\ ,\ \lambda_{ij})$이다. 여기서 $\{i,j\} \in \{s,r,d\}$이며, s,r,d는 각각 송신단, 릴레이, 수신단을 나타낸다. 또한, 수신단은 송신단과 릴레이 사이의 채널 h_{sr}의 CSI를 완벽하게 알고 있으며, 릴레이와 수신단 사이의 채널 h_{rd}에는 채널 추정 오류가 존재한다고 가정한다.

※ 이 성과는 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2018R1C1B6003297).
• First Author : (ORCID:0000-0001-6097-5369)Chungbuk National University, School of Information and Communication Engineering, ljs30671@cbnu.ac.kr, 학생회원
° Corresponding Author : (ORCID:0000-0001-8206-4558)Chungbuk National University, School of Information and Communication Engineering, kslee85@cbnu.ac.kr, 정회원
논문번호 : 201905-065-A-LU, Received May 2, 2019; Revised May 23, 2019; Accepted May 23, 2019

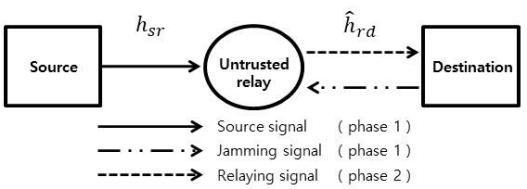

그림 1. 시스템 모델
Fig. 1. System model

첫 번째 위상에서 송신단은 심볼 s을 전송 전력 P로 릴레이에 전송 한다. 이와 동시에 릴레이가 송신단의 신호로부터 정보를 해석하는 것을 방해하기 위해서, 수신단에서는 방해 신호 z를 αP의 전송전력으로 릴레이에 전송한다. 이때, α는 방해 신호 전력 비율이며, $0 \le \alpha \le 1$이다. 릴레이에서 수신된 신호 y_r는 다음과 같이 표현할 수 있다.

$$y_r = h_{sr}\sqrt{P}s + h_{rd}\sqrt{\alpha P}z + n_r. \tag{1}$$

식 (1)에서 $n_r \sim CN(0\ ,\ \sigma^2)$이며, 릴레이에서의 Additive White Gaussian Noise(AWGN)를 나타낸다. 또한, 릴레이의 Signal-to-Interference-plus-Noise Ratio(SINR)인 Γ_R는 다음과 같이 나타낼 수 있다.

$$\Gamma_R = \frac{|h_{sr}|^2 P}{|h_{rd}|^2 \alpha P + \sigma^2} = \frac{|h_{sr}|^2 \gamma}{|h_{rd}|^2 \alpha\gamma + 1}. \tag{2}$$

식 (2)에서 γ는 P/σ^2이며 시스템의 전송 Signal-to-Noise Ratio(SNR)이다.

두 번째 위상에서 릴레이는 수신된 신호를 P의 전송 전력으로 증폭 후 수신단에 전달한다. 증폭된 릴레이 신호는 다음과 같다.

$$x_r = A_r y_r = \sqrt{\frac{P}{|h_{sr}|^2 P + |h_{rd}|^2 \alpha P + \sigma^2}}\, y_r. \tag{3}$$

식 (1)과 식 (3)을 이용해서 수신단에서 수신된 신호 y_d는 다음과 같이 쓸 수 있다.

$$\begin{aligned} y_d &= h_{rd}x_r + n_d \\ &= A_r h_{sr} h_{rd}\sqrt{P}s + A_r h_{rd}^2\sqrt{\alpha P}z + A_r h_{rd} n_r + n_d. \end{aligned} \tag{4}$$

이때 $n_d \sim CN(0\ ,\ \sigma^2)$이다. 수신단은 릴레이 신호 안의 pilot을 통해서 채널 h_{rd}의 CSI를 추정 할 수 있다. 하지만, 실제 무선 통신 시스템에서는 채널을 완벽하게 추정 할 수 없으므로 채널 추정 오류가 존재한다. 채널 추정 오류를 포함하는 추정된 채널 $\hat{h}_{rd}$은 식 (5)와 같이 표현할 수 있다[4].

$$\hat{h}_{rd} = h_{rd}(1+e) = h_{rd} + \hat{e}. \tag{5}$$

여기서 $e \sim (0\ ,\ \sigma_e^2)$이고, 분산 σ_e^2는 추정된 채널과 실제 채널 사이의 차이를 비율로 표현한 것이며, 채널 추정 오류의 정도를 나타내는 지표가 된다. e는 h_{rd}와 독립적이다. 그러므로 $\hat{e} \sim (0\ ,\ \lambda_{rd}\sigma_e^2)$이며, 수신단은 추정된 채널 $\hat{h}_{rd}$를 바탕으로 수신된 신호 y_d에서 방해 신호 부분을 제거 할 수 있다. 방해 신호 제거 후 수신단에서 수신된 신호는 다음과 같다.

$$\begin{aligned} \hat{y}_d &= y_d - A_r\hat{h}_{rd}^2\sqrt{\alpha P}z \\ &= A_r h_{sr} h_{rd}\sqrt{P}s + A_r h_{rd} n_r + n_d - A_r(2h_{rd}\hat{e} + \hat{e}^2)\sqrt{\alpha P}z. \end{aligned} \tag{6}$$

식 (6)에서 $A_r(2h_{rd}\hat{e} + \hat{e}^2)\sqrt{\alpha P}z$는 채널 추정 오류 때문에 생긴 수신단에서의 잔류 방해 신호이다. 불완전한 CSI를 고려하여 정합 필터를 통과한 신호 $\hat{y}_d$는 다음과 같이 나타낼 수 있다.

$$\begin{aligned} r_d &= w_d\hat{y}_d = \frac{\hat{h}_{rd}^*}{|\hat{h}_{rd}|}\hat{y}_d \\ &= \frac{A_r h_{sr}|h_{rd}|^2\sqrt{P}}{|h_{rd}+\hat{e}|}s + \frac{A_r h_{sr} h_{rd}\sqrt{P}}{|h_{rd}+\hat{e}|}\hat{e}^* \\ &\quad + A_r h_{rd}\tilde{n}_r + \tilde{n}_d - A_r(2h_{rd}\hat{e} + \hat{e}^2)\sqrt{\alpha P}\tilde{z}. \end{aligned} \tag{7}$$

식 (7)에서 $|w_d| = 1$ 이고 n_r, n_d, z가 circularly symmetric하므로 $\tilde{n}_r = w_d n_r \sim n_r$, $\tilde{n}_d = w_d n_d \sim n_d$,

$$\Gamma_D = \frac{\dfrac{|h_{sr}|^2|h_{rd}|^4\gamma}{|h_{rd}|^2 + \lambda_{rd}\sigma_e^2}}{\dfrac{|h_{sr}|^2|h_{rd}|^2\lambda_{rd}\sigma_e^2\gamma}{|h_{rd}|^2 + \lambda_{rd}\sigma_e^2} + \lambda_{rd}\sigma_e^2(4|h_{rd}|^2 + \lambda_{rd}\sigma_e^2)\alpha\gamma + (1+\alpha)|h_{rd}|^2 + \dfrac{1}{\gamma}}. \tag{8}$$

$\tilde{z}=w_d z \sim z$이 성립한다. 식 (7)을 이용하여, 수신단에서의 SINR은 식 (8)과 같이 나타낼 수 있다. 결과적으로 통신 링크와 도청 링크의 전송률의 차로 정의되는 보안 전송률은 다음과 같이 나타낼 수 있다.

$$R_s = \left[\frac{T}{2} log_2\left(\frac{1+\Gamma_D}{1+\Gamma_R}\right)\right]^+. \quad (9)$$

여기서 $[x]^+ = \max(x,0)$이고, T는 전체 블록 시간을 나타낸다. 수식 (9)를 이용하여 최적의 α는 bisection 알고리즘을 통해 빠르게 찾을 수 있다.

Ⅲ. 시뮬레이션 결과

시뮬레이션 환경은 다음과 같다[4,6]. 송신단과 릴레이 사이 거리, 릴레이와 송신단 사이의 거리는 각각 500m로 같으며, path-loss exponent는 2.7, multi-path fading은 mean이 1인 exponential random 변수를 이용하여 생성하였다. 또한, $T=1$, $\gamma=113$ dB로 설정하였다.

그림 2는 채널 추정 오류 σ_e^2가 0.01, 0.05, 0.1일 때, 보안 전송률(R_s)과 방해 전력 비율(α)의 관계를 보여준다. R_s는 α에 대해 concave하기 때문에 R_s를 최대화 할 수 있는 최적의 방해 전력 비율 α^*가 존재한다. 또한, α^*은 채널 추정 오류와 함께 증가한다. 이를 통해서 방해 신호는 Γ_D보다 Γ_R에 더 부정적인 영향을 미치는 것을 알 수 있다.

그림 3은 채널 추정 오류(σ_e^2)에 대한 보안 전송률(R_s)을 보여준다. 여기서 항상 최대 전력을 이용하여

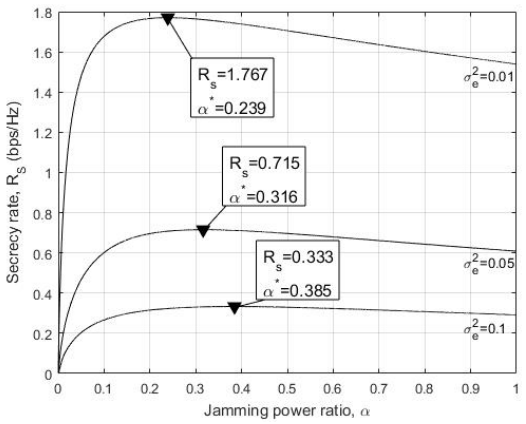

그림 2. 보안 전송률 vs. 방해 전력 비율
Fig. 2. Secrecy rate vs Jamming power ratio

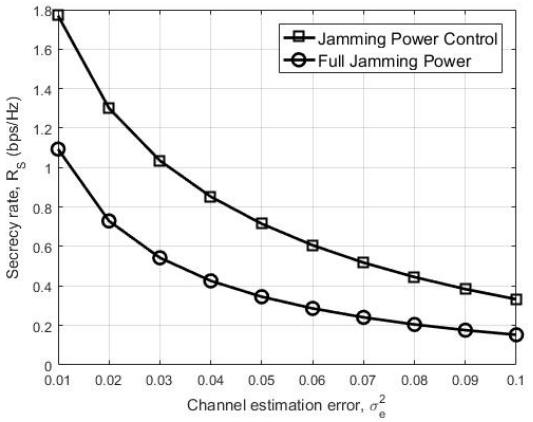

그림 3. 보안 전송률 vs. 채널 추정 오류
Fig. 3. Secrecy rate vs Channel estimation error

($\alpha=1$) 방해 신호를 전송하는 Full Jamming Power scheme을 비교 방안으로 선정하였다. σ_e^2가 증가 하면서 2가지 방안 모두 R_s이 감소한다. 또한, Full Jamming Power scheme에 비해 α를 최적의 값으로 제어하는 제안 방안이 약 40%가량 더 좋은 R_s 성능을 보였다. 이를 통해서 채널 추정 오류가 존재할 때는 방해 신호 전송을 위한 전력을 제어 하는 것이 보안 전송률 향상 측면에서 효율적임을 알 수 있다.

Ⅳ. 결 론

본 논문은 채널 추정 오류를 고려하여 신뢰할 수 없는 릴레이가 존재하는 시스템의 보안 전송률을 수식적으로 모델링 하였다. 또한, 시뮬레이션을 통해서 이를 최대화 할 수 있는 최적의 방해 신호 전력 비율이 존재함을 보이고, 효율적인 방해 전력 제어는 시스템의 보안 전송률을 약 40% 정도 향상 시킬 수 있음을 확인하였다.

References

[1] R. Negi and S. Goal, “Secret communication using artificial noise,” in *Proc. IEEE VTC’05*, pp. 1906-1910, Dallas, USA, Sep. 2005.

[2] K. Lee and H.-H. Choi, “Time switching-based relaying for maximizing secrecy capacity,” *J. KICS*, vol. 42, no. 10, pp. 1955-1958, Oct. 2017.

[3] B. Yang, W. Wang, B. Yao, and Q. Yin,

"Destination assisted secret wireless communication with cooperative helpers," *IEEE Sign. Process Lett.*, vol. 20, no. 11, pp. 1030-1033, Nov. 2013.

[4] C. Wang, T.-K. Liu, and X. Dong, "Impact of channel estimation error on the performance of amplify-and-forward two-way relaying," *IEEE Trans. Veh. Technol*, vol. 61, no. 3, pp. 1197-1207, Mar. 2012.

[5] J.-T. Lim, K. Lee, and I.-H. Ra, "Secrecy performance analysis and enhancement scheme for time switching-based relaying protocol under outdated channel state information," *J. KICS*, vol. 44, no. 4, pp. 678-684, Apr. 2019.

[6] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Wireless-powered relays in cooperative communications: Time-switching relaying protocols and throughput analysis," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1607-1622, May 2015.