논문 19-44-11-11 The Journal of Korean Institute of Communications and Information Sciences '19-11 Vol.44 No.11
https://doi.org/10.7840/kics.2019.44.11.2070

비신뢰적 중계 네트워크에서 채널 추정 오류와 지연 채널 정보를 고려한 방해 신호 전력 제어

이 기 송◆, 최 현 호°

Jamming Power Control Considering Channel Estimation Error and Outdated Channel Information in Untrusted Relay Networks

Kisong Lee◆, Hyun-Ho Choi°

요 약

본 논문에서는 비신뢰적 중계 네트워크에서 채널 추정 오류와 지연 채널 정보를 고려하여 보안 전송률을 수학적으로 모델링 하고, 시뮬레이션을 통해 이를 최대화하는 최적의 방해 신호 전력 비율을 찾았다. 시뮬레이션 결과는 채널 추정 오류와 시간 지연으로 인하여 채널 정보가 심각하게 달라졌을 경우 방해 전력 비율을 줄이는 것이 시스템에서 보안 전송률을 향상시킬 수 있음을 보여준다.

Key Words : Physical layer security, outdated channel, channel estimation error, untrusted relay, jamming power control

ABSTRACT

In considerations of channel estimation error and outdated channel information, we formulate a secrecy rate in an untrusted relay network, and find the optimal jamming power ratio for maximizing the secrecy rate through simulations. The results show that it needs to reduce jamming power to improve the secrecy rate when the channel is severely outdated and has an estimation error.

Ⅰ. 서 론

최근 다양한 네트워크가 공존하게 되면서 정보 보안 문제가 더욱 더 중요해지고 있다. 특히 암호화 키 없이 무선 채널의 물리적 특성을 이용하여 정보의 기밀성을 보장해주는 물리 계층 보안 기술은 낮은 구현 복잡도를 가지므로 이에 대한 관심이 커지고 있다[1-4]. 물리 계층 보안의 기본 원리는 도청자에게 방해 신호를 전송함으로써 도청자가 기밀한 정보를 해석하는 것을 방해하는 것이다[1]. 특히 릴레이가 비신뢰성을 갖는 노드일 경우 보안 성능을 향상시키기 위하여 목적 노드가 방해 신호를 전송하는 기술이 연구되었다[2,3]. 뿐만 아니라 채널 추정 오류가 존재하는 비신뢰적 릴레이 환경에서 보안 전송률을 향상시키기 위한 방해 전파 전송 기술이 연구되었다[4].

하지만 비신뢰적 릴레이 환경에서 목적 노드가 방해 신호를 전송하는 동안의 채널과 목적 노드가 릴레이 신호를 수신하는 동안의 채널은 시간 지연으로 인해 일치하지 않는다[5]. 이 경우 목적 노드는 자신이 전송한 방해 신호를 완벽히 제거할 수 없으며, 이는 목적 노드에 잔류 방해 신호를 발생시켜 보안 전송률이 현저히 낮아진다. 본 논문에서는 채널 추정 오류와 지연 채널 정보를 고려하여 신뢰할 수 없는 릴레이가 존재하는 시스템의 보안 전송률을 수식적으로 도출하고, 시뮬레이션을 통해서 이를 최대화하는 최적의 방해 전력 비율을 찾는다. 또한, 기존 방안 대비 방해 신호 전력 제어를 사용하는 경우 시스템의 보안 성능이 크게 향상됨을 보였다.

Ⅱ. 시스템 모델

그림 1은 본 논문에서 고려하고 있는 발신 노드, 비신뢰성을 갖는 릴레이, 목적 노드로 이루어진 two-hop 네트워크를 보여준다. 각 노드들은 한 개의 송수신 안

※ 이 성과는 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2019R1A2C4070466).
◆ First Author : (ORCID:0000-0001-8206-4558)Chungbuk National University, School of Information and Communication Engineering, kslee85@cbnu.ac.kr, 정회원
° Corresponding Author : (ORCID:0000-0002-6785-2596)Hankyong National University, Department of Electrical, Electronic and Control Engineering, hhchoi@hknu.ac.kr, 정회원
논문번호 : 201908-154-A-LU, Received August 12, 2019; Revised September 16, 2019; Accepted September 19, 2019

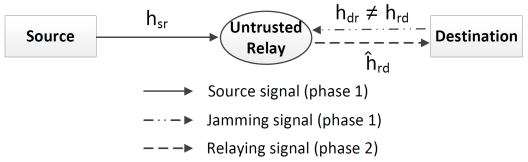

그림 1. 시스템 모델
Fig. 1. System model

테나를 갖으며, half-duplex 방식으로 동작한다. 또한, 발신 노드와 목적 노드 사이에 직접적인 채널 링크는 존재하지 않는다[3-4]. 릴레이는 증폭-후-전달(Amplify-and-Forward) 프로토콜을 통해서 발신 노드와 목적 노드 사이의 데이터 전달을 돕는다. 하지만 릴레이는 발신 노드와 목적 노드에 비해 낮은 보안 레벨을 가지므로 두 노드는 릴레이가 그들이 전송하는 데이터를 해석하기를 원치 않는다[1]. 노드 i와 j 사이의 채널은 h_{ij}로 표현하고, h_{ij}는 $CN(0\ ,\ \lambda_{ij})$의 complex Gaussian 분포를 따른다. 또한, 각 노드는 $n \sim CN(0\ ,\ \sigma^2)$를 따르는 동일한 Additive White Gaussian Noise(AWGN)를 갖는다고 가정한다.

첫 번째 위상에서 발신 노드는 데이터 신호 s를 전력 P로 릴레이에 전송 한다. 이와 동시에 목적 노드는 릴레이가 발신 노드의 데이터 신호를 해석하는 것을 막기 위해 방해 신호 z를 αP의 전력으로 릴레이에 전송한다. 이때, α는 방해 신호 전력 비율이며, 다음의 $0 \le \alpha \le 1$ 범위를 갖는다. 릴레이에서 수신한 신호는 다음과 같다.

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

식 (1)에서부터 릴레이의 Signal-to-Interference-plus- Noise Ratio(SINR)은 다음과 같이 나타낼 수 있다.

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

식 (2)에서 γ는 P/σ^2이다.

두 번째 위상에서 릴레이는 수신한 신호를 P의 전력을 이용하여 A_r만큼 증폭 후 목적 노드에 전달한다. 증폭된 릴레이 신호는 다음과 같다.

$$\begin{aligned} x_r &= A_r y_r \\ &= \sqrt{\frac{P}{|h_{sr}|^2 P + |h_{dr}|^2\alpha P + \sigma^2}} \cdot y_r. \end{aligned} \tag{3}$$

따라서 목적 노드가 수신한 신호는 다음과 같다.

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

식 (4)에서 첫 번째 위상과 두 번째 위상의 시간 지연으로 인해 h_{dr}는 h_{rd}와 정확히 일치하지 않는다. 따라서 h_{dr}과 h_{rd}의 관계는 다음과 같이 모델링이 가능하다[5].

$$h_{dr} = \sqrt{\Phi}\,h_{rd} + \sqrt{1-\Phi}\,e. \tag{5}$$

식 (5)에서 Φ는 h_{dr}과 h_{rd} 사이의 채널 상관 지수이며, e는 오차율로 h_{rd}와 같은 분포 $e \sim CN(0,\lambda_{rd})$를 따른다. h_{dr}과 h_{rd}가 정확히 일치하면 $\Phi = 1$이 되며, h_{dr}과 h_{rd}사이에 오차가 존재하는 경우 ($\Phi < 1$) 목적 노드는 수신 신호로부터 방해 신호를 완벽하게 제거하지 못한다. 그로 인해 목적 노드의 수신 신호에는 잔류 방해 신호가 발생하고 이는 목적 노드의 수신 성능을 떨어뜨린다. 식 (5)를 식 (4)에 대입하면 y_d를 다음과 같이 표현할 수 있다.

$$\begin{aligned} y_d = {} & A_r h_{sr}h_{rd}\sqrt{P}s + A_r h_{rd}^2\sqrt{\Phi}\,\sqrt{\alpha P}z \\ & + A_r h_{rd}\sqrt{1-\Phi}\,\sqrt{\alpha P}ze + A_r h_{rd}n + n. \end{aligned} \tag{6}$$

또한, 목적 노드에서 릴레이 신호의 pilot을 이용하여 h_{rd}를 추정한다. 하지만 채널 추정 오류가 존재하는 경우 추정된 채널 $\hat{h}_{rd}$은 식 (7)와 같이 표현할 수 있다[4].

$$\hat{h}_{rd} = h_{rd} + \hat{e}. \tag{7}$$

식 (7)에서 $\hat{e} \sim (0\ ,\ \lambda_{rd}\sigma_e^2)$이며, 추정된 채널 $\hat{h}_{rd}$를 이용하여 목적 노드는 수신된 신호 y_d에서 방해 신호의 일부분을 제거 할 수 있다.

$$\begin{aligned} \hat{y}_d = {} & y_d - A_r\hat{h}_{rd}^2\sqrt{\Phi}\,\sqrt{\alpha P}z \\ = {} & A_r h_{sr}h_{rd}\sqrt{P}s + A_r h_{rd}\sqrt{1-\Phi}\,\sqrt{\alpha P}ze \\ & + A_r h_{rd}n + n - A_r(2h_{rd}\hat{e} + \hat{e}^2)\sqrt{\Phi}\,\sqrt{\alpha P}z. \end{aligned} \tag{8}$$

식 (8)에서 $A_r h_{rd}\sqrt{1-\Phi}\,\sqrt{\alpha P}ze$는 지연 채널로 인한 잔류 방해 신호이며, $A_r(2h_{rd}\hat{e} + \hat{e}^2)\sqrt{\Phi}\,\sqrt{\alpha P}z$는 채널 추정 오류로 인한 잔류 방해 신호이다. 채널 추정 오류를 고려하여 정합 필터를 통과한 신호는 다음과 같이 나타낼 수 있다.

$$r_d = w_d \hat{y}_d = \frac{\hat{h}_{rd}^*}{|\hat{h}_{rd}|}\hat{y}_d$$
$$= \frac{A_r h_{sr}|h_{rd}|^2\sqrt{P}}{|h_{rd}+\hat{e}|}s + \frac{A_r h_{sr}h_{rd}\sqrt{P}}{|h_{rd}+\hat{e}|}s\hat{e}^* \quad (9)$$
$$+ A_r h_{rd}\sqrt{1-\Phi}\,\sqrt{\alpha P}\tilde{z}e + A_r h_{rd}\tilde{n} + \tilde{n}$$
$$- A_r(2h_{rd}\hat{e}+\hat{e}^2)\sqrt{\Phi}\,\sqrt{\alpha P}\tilde{z}.$$

식 (9)에서 $|w_d|=1$ 이고 n과 z가 circularly symmetric하므로 $\tilde{n}=w_d n\sim n$와 $\tilde{z}=w_d z\sim z$이 성립한다. 따라서 식 (9)로부터 목적 노드에서의 SINR은 식 (10)과 같이 표현된다. 또한, 식 (5)를 식 (2)에 대입하면 릴레이의 SINR 역시 식 (11)과 같이 표현 가능하다.

$$\Gamma_R = \frac{|h_{sr}|^2\gamma}{\left(\Phi|h_{rd}|^2+(1-\Phi)\lambda_{rd}\right)\alpha\gamma+1}. \quad (11)$$

결과적으로 식 (10)과 (11)를 이용하여 데이터 링크와 도청 링크의 전송률 차로 정의되는 보안 전송률을 다음과 같이 나타낼 수 있다[1].

$$R_S = \left[\frac{T}{2}log_2\left(\frac{1+\Gamma_D}{1+\Gamma_R}\right)\right]^+. \quad (12)$$

여기서 $[x]^+ = \max(x,0)$이다. 지연 채널 정보가 있는 환경에서 R_S을 최대화 하는 방해 신호 전력 비율 α는 시뮬레이션을 통해 수치해석적으로 찾고자 한다.

Ⅲ. 시뮬레이션 결과

시뮬레이션 환경은 다음과 같다[3-4]. 발신 노드와 릴레이 사이 거리, 릴레이와 목적 노드 사이의 거리는 각각 500 m로 같으며, 3GPP path-loss model ($L[dB]=128.1+37.6\log_{10}(distance[km])$), mean이 1인 exponential random 변수를 이용하여 multi-path fading를 발생시키고 최종적인 채널을 생성하였다. 또한, $T=1$, $\gamma=140$ dB로 설정하였다.

그림 2는 채널 추정 오차(σ_e^2)가 0.01과 0.001일 때

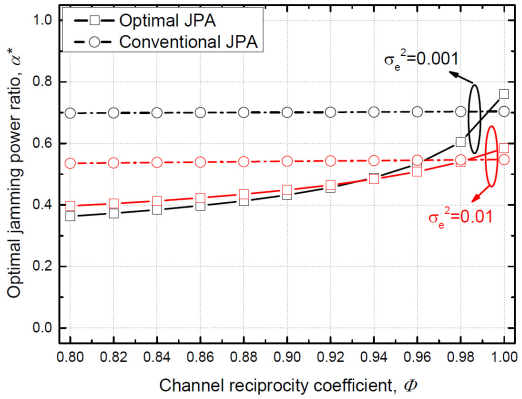

그림 2. 최적 방해 전력 비율 vs. 채널 상관 계수
Fig. 2. Optimal jamming power ratio vs. Channel reciprocity coefficient

채널 상관 계수(Φ)에 대한 최적의 방해 전력 비율(α^*)의 관계를 보여준다. 여기서 기존 방안(Conventional jamming power allocation, JPA)은 채널 추정 오류만을 고려하여 α^*를 결정하는 방안이다[4]. 기존 방안은 채널 지연을 고려하지 않기 때문에 Φ에 관계없이 일정한 α^* 값을 유지한다. 반면 제안 방안에서는 Φ가 작아질수록 α^* 역시 작아짐을 확인할 수 있다. 이는 h_{dr}과 h_{rd}사이의 상관도가 낮아질수록 목적 노드에서의 제거되지 않은 잔류 방해 신호가 커지므로 작은 전력으로 방해 신호를 전송하는 것이 보안 전송률 최대화 측면에서 최적임을 보여준다. 또한, 채널 추정 오류가 증가할수록 채널 지연의 영향이 상대적으로 작아져 α^*의 범위는 줄어드는 것을 확인할 수 있다.

그림 3은 σ_e^2가 0.01과 0.001일 때 채널 상관 계수(Φ)에 대한 보안 전송률(R_s)을 보여준다. 여기서 full JPA는 항상 최대 전력을 이용하여 ($\alpha=1$) 방해 신호를 전송하는 방안이다. Φ가 1에 다가갈수록 지연 채널 효과가 줄어들어 제안 방안과 conventional JPA와의 성능 차이가 줄어든다. 하지만 Φ가 작아질수록 제안 방안은 conventional JPA와 full JPA 보다 높은 R_s 성능을 보여준다. 이를 통해서 채널 추정 오류가 존재하는 환경에서 시간 지연으로 인해 채널이 달라진 경우 방해 신호 전송을 위한 전력을 적절한 값으로 제어하는 것이 보안 전송률 향상 측면에서 효과적임을 알

$$\Gamma_D = \frac{\dfrac{|h_{sr}|^2|h_{rd}|^4\gamma}{|h_{rd}|^2+\lambda_{rd}\sigma_e^2}}{\dfrac{|h_{sr}|^2|h_{rd}|^2\lambda_{rd}\sigma_e^2\gamma}{|h_{rd}|^2+\lambda_{rd}\sigma_e^2}+\Phi\lambda_{rd}\sigma_e^2(4|h_{rd}|^2+\lambda_{rd}\sigma_e^2)\alpha\gamma+\left\{(1-\Phi)\lambda_{rd}(|h_{rd}|^2\gamma+1)+\Phi|h_{rd}|^2\right\}\alpha+|h_{sr}|^2+|h_{rd}|^2+1/\gamma}. \quad (10)$$

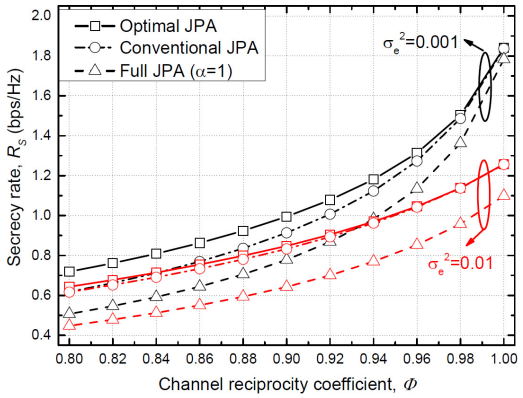

그림 3. 보안 전송률 vs. 채널 상관 계수
Fig. 3. Secrecy rate vs. Channel reciprocity coefficient

수 있다.

Ⅳ. 결 론

본 논문에서는 비신뢰적 중계 네트워크에서 채널 추정 오류와 시간 지연으로 인하여 릴레이와 목적 노드 사이의 채널 상태 정보가 릴레이 프로토콜의 두 위상 동안 일치하지 않는 경우, 시스템의 보안 전송률을 수식적으로 모델링 하였다. 또한, 시뮬레이션을 통해서 보안 전송률을 최대화 할 수 있는 최적의 방해 신호 전력 비율이 존재함을 보이고, 제안하는 최적의 방해 신호 전력 제어는 보안 전송률을 향상 시킬 수 있음을 확인하였다.

References

[1] X. He and A. Yener, “Cooperation with an untrusted relay: A secrecy perspective,” *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807-3827, Aug. 2010.

[2] 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.

[3] S. S. Kalamkar and A. Banerjee, “Secure communication via a wireless energy harvesting untrusted relay,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2199-2213, Mar. 2017.

[4] J. Lee and K. Lee, “Secure communication via untrusted relay with channel estimation error,” *J. KICS*, vol. 44, no. 7, pp. 1295-1298, Jul. 2019.

[5] D. Mi, M. Dianati, L. Zhang, S. Muhaidat, and R. Tafazolli, “Massive MIMO performance with imperfect channel reciprocity and channel estimation error,” *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3734-3749, Sep. 2017.