https://doi.org/10.7840/kics.2023.48.7.803

# 전력 분할 기반 보안 릴레이의 보안 에너지 효율성 최대화

신 경 섭◆

# Secrecy Energy Efficiency Maximization of Power Splitting-Based Secure Relay

Kyungseop Shin◆

요 약

본 논문에서는 비신뢰적 릴레이가 존재하는 전력 분할 기반 보안 릴레이의 보안 에너지 효율성 최대화 문제를 수식화하고, 시뮬레이션을 통해 최적의 전력 분할 비율과 방해 잡음 전력 비율을 찾았다. 이 두 값을 상황에 맞게 최적화함으로써 제안방안은 기존방안에 비해 높은 보안 에너지 효율성을 달성함을 보였다.

**Key Words :** Information security, secrecy energy efficiency, power splitting, untrusted relay, jamming power

ABSTRACT

In this paper, we formulate the secrecy energy efficiency maximization problem of power splitting-based secure relay in the presence of an untrusted relay, and find the optimal power splitting ratio and jamming power ratio through simulation. By optimizing these two values in context, we show that the proposed scheme achieves higher secrecy energy efficiency than the existing schemes.

## Ⅰ. 서 론

암호키를 사용하는 기존 보안 기술의 대안으로 최근 물리계층보안에 대한 관심이 커지고 있다[1]. 물리계층보안의 경우 무선 채널의 물리적 특성을 이용하여 암호화 없이 도청자에게 방해 잡음을 전송하여 기밀 정보 유출을 막는 기술이다. 특히 비신뢰적 릴레이가 존재하는 환경의 경우 외부의 도청자가 존재하지 않아도 정보의 유실이 발생할 수 있다. 이를 막기 위해 송신 노드가 비신뢰적 릴레이에 데이터 신호를 전송할 때, 수신 노드도 함께 방해 잡음을 전송하는 destination-assisted jamming 방안에 대한 연구가 진행되었다[2,3]. 또한, 에너지 하베스팅이 가능한 비신뢰적 릴레이가 존재할 때 보안 전송률을 최대화하기 위한 최적의 에너지 하베스팅 비율을 도출 하였다[4-5].

보안과 관련된 스펙트럼 효율성 최적화에 집중한 기존 연구와는 다르게 본 논문에서는 전력 분할 기반 릴레이의 보안 에너지 효율성 최대화 문제를 다루고자 한다. 이를 위해 보안 릴레이 네트워크를 수학적으로 모델링하고, 보안 에너지 효율성을 최대화하는 최적의 전력 분할 비율과 방해 잡음 전력 비율을 수치적으로 찾았다. 또한, 시뮬레이션을 이용한 기존방안과의 성능 비교를 통해 효과적인 전력 분할 비율 및 방해 잡음 전력 비율 제어는 시스템의 보안 에너지 효율성을 향상시킬 수 있음을 보였다.

## Ⅱ. 시스템 모델 및 문제 정의

그림 1은 각각 한 개의 안테나가 장착된 송신 노드 (S), 릴레이 (R), 수신 노드 (D)로 구성된 two-hop 네트워크의 보안 릴레이 프로토콜을 보여준다. 송수신 노드 사이에는 무선 채널이 존재하지 않으며, 릴레이가 증폭-후-전달 (Amplify-and- Forward) 방식을 이용해 송신 노드의 데이터를 수신 노드에 전달한다[4-5]. 또한, 릴레이는 수신한 신호로부터 전력 분할 비율 $0 \le \alpha \le 1$를 조절하여 에너지를 수확하고 이를 이용하여 수신 노드에 신호를 전달하지만, 수신한 신호로부터 정보를 해석할 권한이 없는 비신뢰적 노드이다. 노드 $i$와 $j$ 사이의 채널인 $h_{ij} \sim CN(0\ ,\ \lambda_{ij})$와 Additive

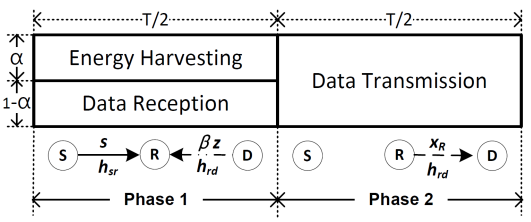


그림 1. 시스템 모델
Fig. 1. System model

◆ First Author : (0000-0002-3867-1921)Sangmyung University, Department of Computer Science, ksshin@smu.ac.kr, 조교수, 정회원
논문번호 : 202304-089-A-LU, Received April 25, 2023; Revised May 3, 2023; Accepted May 3, 2023

White Gaussian Noise(AWGN)인 $n \sim CN(0\ ,\ \sigma^2)$은 complex normal 분포를 따른다고 가정한다.

보안 릴레이 프로토콜은 전체 시간 $T$동안 동일한 주기 $\frac{T}{2}$를 갖는 두 개의 위상으로 구성되어 있다. 첫 번째 위상에서 송신 노드는 정규화된 데이터 신호 $s$를 전송 전력 $P_S$를 이용해 릴레이에 전송하고, 수신 노드 역시 정규화된 방해 잡음 $z$를 전송 전력 $\beta P_Z$를 이용해 릴레이에 전송한다. 여기서 $0 \le \beta \le 1$는 수신 노드의 방해 잡음 전력 비율이다. 이를 통해 비신뢰적 릴레이가 데이터 신호 $s$를 도청하는 것을 막을 수 있다. 릴레이는 수신한 신호의 전력 중 $\alpha$의 비율은 에너지를 수확하고 $1-\alpha$의 비율은 신호를 수신한다. 따라서 릴레이가 수확한 에너지는 다음과 같다.

$$E_R = \frac{\zeta \alpha T P_H}{2} = \frac{\zeta \alpha T\left(|h_{sr}|^2 P_S + |h_{rd}|^2 \beta P_Z\right)}{2}. \tag{1}$$

식 (1)에서 $\zeta$는 에너지 변환 효율이다. 또한, 릴레이에서 수신한 신호는 아래와 같다.

$$y_R = h_{sr}\sqrt{(1-\alpha)P_S}s + h_{rd}\sqrt{(1-\alpha)\beta P_Z}z + n. \tag{2}$$

만약 릴레이가 수신 신호로부터 데이터를 도청하는 경우의 Signal-to-Interference-plus-Noise-Ratio (SINR)는 다음과 같다.

$$\Gamma_R = \frac{(1-\alpha)P_S|h_{sr}|^2}{\beta(1-\alpha)P_Z|h_{rd}|^2 + \sigma^2}. \tag{3}$$

식 (3)를 이용하면 릴레이에서의 데이터 전송률은 다음과 같이 표현된다.

$$R_R = \frac{T}{2}\log_2(1+\Gamma_R). \tag{4}$$

두 번째 위상에서 릴레이는 수확한 전력 $P_R = \frac{E_R}{T/2} = \eta\alpha P_H$을 이용하여 다음과 같이 신호를 $A_R$만큼 증폭한 후 수신 노드에 전달한다.

$$x_R = A_R y_R = \sqrt{\frac{P_R}{(1-\alpha)P_H + \sigma^2}}\, y_R. \tag{5}$$

식 (5)를 이용하면 수신 노드가 릴레이로부터 수신한 신호는 다음과 같다.

$$\begin{aligned} y_D &= h_{rd}x_R + n \\ &= \frac{\sqrt{(1-\alpha)P_S P_R}h_{sr}h_{rd}s + \sqrt{P_R}h_{rd}n}{\sqrt{(1-\alpha)P_H + \sigma^2}} \\ &\quad + \underbrace{\frac{\sqrt{(1-\alpha)\beta P_Z P_R}h_{rd}^2 z}{\sqrt{(1-\alpha)P_H + \sigma^2}}}_{self-cancellation} + n. \end{aligned} \tag{6}$$

식 (6)에서 수신 노드는 자신이 보낸 방해 잡음을 제거할 수 있으므로[4,5] 결과적으로 수신 노드의 SINR은 다음과 같다.

$$\Gamma_D = \frac{(1-\alpha)P_S P_R|h_{sr}|^2|h_{rd}|^2}{\sigma^2\left(P_R|h_{rd}|^2 + (1-\alpha)P_H + \sigma^2\right)}. \tag{7}$$

식 (7)을 이용하면 수신 노드에서의 데이터 전송률은 다음과 같이 표현된다.

$$R_D = \frac{T}{2}\log_2(1+\Gamma_D) \tag{8}$$

따라서 데이터 링크과 도청 링크의 전송률 차로 정의되는 보안 전송률은 다음과 같다[1].

$$R_S = R_D - R_R = \left[\frac{T}{2}\log_2\left(\frac{1+\Gamma_D}{1+\Gamma_R}\right)\right]^+. \tag{9}$$

여기서 $[x]^+ = \max(x,0)$이다.

반면, 네트워크에서 사용하는 총 에너지는 다음과 같다.

$$E_{tot} = TP_C + \frac{T}{2}(P_S + \beta P_Z). \tag{10}$$

식 (10)에서 $P_C$는 전체 노드의 회로에서 소모되는 전력이다.

식 (9)과 (10)를 이용하여 단위 전력당 달성 가능한 보안 전송률을 나타내는 지표인 보안 에너지 효율성을 다음과 같이 정의할 수 있다.

$$\eta_S = \frac{R_S}{E_{tot}}. \tag{11}$$

본 논문에서는 비신뢰적 릴레이가 존재할 때 보안 에너지 효율성을 최대화하는 최적의 전력 분할 비율

및 방해 잡음 전력 비율을 도출하고자 한다.

$$\begin{aligned} \max_{\alpha,\beta} \quad & \eta_S \\ s.t. \quad & 0 \le \alpha \le 1, \\ & 0 \le \beta \le 1. \end{aligned} \tag{12}$$

위의 최적화 문제는 제약 조건을 만족하는 $\alpha$와 $\beta$의 범위에서 two-dimensional search를 통해 최적의 해를 수치적으로 찾을 수 있다.

## Ⅲ. 시뮬레이션 결과

시뮬레이션을 위한 시스템 변수는 $T=1s$, $\zeta=0.5$, $\sigma^2=-70dBm$, $P_S=43dBm$, $P_C=40dBm$으로 설정하였다[2-5]. 송수신 노드 사이의 거리는 20m이며, 릴레이는 중앙에 배치하였다. Path-loss exponent는 2.7로 선정하고, 평균이 1인 지수 확률 변수로 다중경로 페이딩을 만들어 최종적으로 랜덤한 무선 채널을 생성하였다.

그림 2는 최대 방해 전파 전력($P_Z$)에 대한 보안 에너지 효율성($\eta_S$)의 관계를 보여준다. 제안방안의 경우 $P_Z<37dBm$의 범위에서는 사용하는 방해 잡음 전력이 늘수록 보안 전송률도 크게 증가하기 때문에 결과적으로 $\eta_S$ 역시 증가한다. 하지만 $P_Z \ge 37dBm$인 경우 보안 전송률의 증가보다 소모되는 전력의 증가량이 더 크기 때문에 수신 노드가 $\beta$를 조절하여 일정한 크기의 전력으로 방해 잡음을전송하고, 그로 인해 일정한 $\eta_S$를 달성한다.

즉, 보안 에너지 효율성 측면에서 최적의 방해 잡음 전력이 존재함을 알 수 있다. 같은 이유로 ($\alpha=0.5$, optimal $\beta$)방안도 $P_Z$가 커지더라도 $\beta$를 조절하여 일정한 방해 잡음 전력을 사용하기 때문에 일정한 $\eta_S$로 수렴하는 것을 확인할 수 있다. 반면 (optimal $\alpha$, $\beta=0.5$)방안과 ($\alpha=0.5$, $\beta=0.5$)방안의 경우 $P_Z$가 커짐에 따라 사용되는 방해 잡음 전력도 커지기 때문에 에너지 효율성 측면에서 오히려 성능이 떨어지는 것을 확인할 수 있다. 제안방안은 모든 $P_Z$의 범위에서 비교방안에 비해 가장 높은 보안 에너지 효율성을 달성한다.

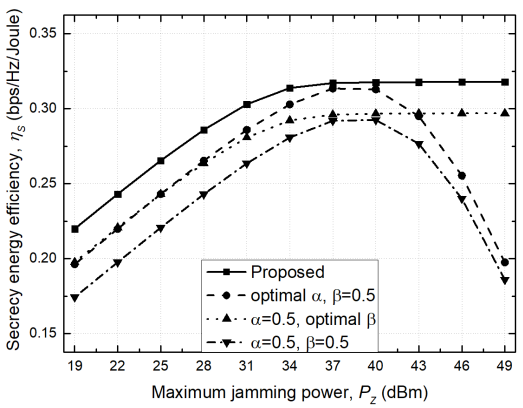


그림 2. 보안 에너지 효율성 vs. 최대 방해 잡음 전력
Fig. 2. Secrecy energy efficiency vs. Maximum jamming power

그림 3은 최대 방해 전파 전력($P_Z$)에 대한 최적의 전력 분할 비율($\alpha^*$)과 방해 잡음 비율($\beta^*$)을 보여준다. $P_Z$가 증가함에 따라 릴레이는 $\alpha$를 늘려 신호의 송수신 보다 에너지 하베스팅에 더 많은 전력을 할당하는 것을 확인할 수 있다. 또한, $P_Z$가 증가할수록 보안 에너지 효율성 측면에서 최적인 일정한 크기의 방해 잡음를 전송하기 위해 수신 노드는 $\beta$를 조절하는 것을 확인할 수 있다.

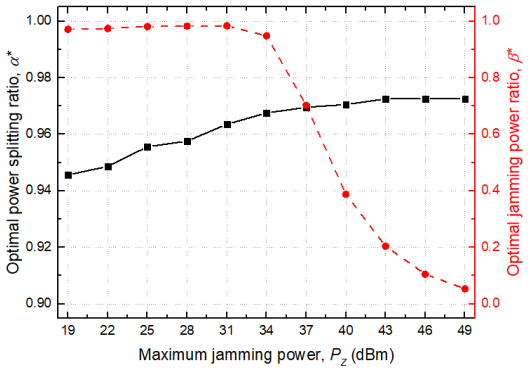


그림 3. 최적의 전력 분할 비율과 방해 전파 비율 vs. 최대 방해 전파 전력
Fig. 3. Optimal time switching ratio and jamming power ratio vs. Maximum jamming power

## Ⅳ. 결 론

본 논문에서는 비신뢰적 릴레이가 존재하는 환경에서 전력 분할 기반 보안 릴레이의 보안 에너지 효율성 최대화 문제를 수식화하고, 최적의 전력 분할 비율과 방해 잡음 전력 비율을 수치적으로 찾았다. 또한, 시뮬레이션을 통해서 제안방안이 비교방안에 비해 높은 보안 에너지 효율성을 달성할 수 있음을 확인하였다.

## References

[1] M. Bloch, J. Barros, M. R. D. Rodriques, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008. (https://doi.org/10.1109/TIT.2008.921908)

[2] 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. (https://doi.org/10.7840/kics.2019.44.7.1295)

[3] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741-1750, Sep. 2013. (https://doi.org/10.1109/JSAC.2013.130908)

[4] 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. (https://doi.org/10.1109/TVT.2016.2572960)

[5] K. Lee, J.-T. Lim, and H.-H. Choi, "Impact of outdated CSI on the secrecy performance of wireless-powered untrusted relay networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1423-1433, Jan. 2020. (https://doi.org/10.1109/TIFS.2019.2940906)