https://doi.org/10.7840/kics.2023.48.6.681

보안 전송률 최대화를 위한 무선 충전이 가능한 전력 분할 기반 보안 릴레이

신 경 섭◆

Wireless-Powered Power Splitting-Based Secure Relay for Maximizing Secrecy Rate

Kyungseop Shin◆

요 약

본 논문에서는 비신뢰적 노드의 에너지 하베스팅 요구량을 보장해주면서 동시에 잠재적 도청을 막기 위한 전력 분할 기반 보안 릴레이를 제안하였다. 보안 전송률 최대화를 위한 최적의 전력 분할 비율을 찾는 최적화 문제를 수식화하고, 시뮬레이션을 통해 최적의 전력 분할 비율을 찾았다. 전력 분할 기반 보안 릴레이에서는 수신한 신호의 0.9 이상의 비율을 에너지 하베스팅 하는 것이 보안 성능을 향상시킴을 보였다.

Key Words : Information security, secrecy rate, power splitting, untrusted node, jamming signal

ABSTRACT

In this paper, we propose a power splitting-based secure relay to prevent potential eavesdropping while guaranteeing the energy harvesting requirement of an untrusted node. We formulated an optimization problem to find the optimal power splitting ratio for maximizing the secrecy rate, and found the optimal power splitting ratio through simulation. In the power splitting-based secure relay, energy harvesting of a ratio of 0.9 or more of the received signal improves security performance.

Ⅰ. 서 론

최근 무선 디바이스와 활용되는 네트워크가 다양해짐에 따라 프라이버시 및 기밀한 정보의 보안 문제에 대한 관심이 커지고 있다. 이에 따라 암호화 과정 없이 도청자에게 방해 잡음을 전송하여 정보의 해석을 막는 물리 계층 보안 기술에 대한 중요성이 커지고 있다[1]. 특히 릴레이 환경에서 송신 노드가 데이터 신호를 전송할 때 수신 노드 역시 함께 방해 잡음을 전송한 후, 릴레이 신호로부터 자신이 보낸 방해 잡음을 제거하고 데이터 신호를 복원하는 수신 노드의 방해 잡음 전송 방안이 제안되었다[2-3]. 또한, 관련 연구는 에너지 하베스팅이 가능한 릴레이 환경으로도 확장되었다[4-5]. 에너지 하베스팅이 가능한 비신뢰적 릴레이가 존재하는 환경에서 보안 전송률과 보안 아웃티지 확률 측면에서 최적의 에너지 하베스팅 비율을 도출하였다[4]. 또한, 이 연구를 확장하여 동일한 환경에서 채널 정보가 오래되어 오류가 있을 때 보안 전송률과 보안 아웃티지 확률 측면에서 최적의 에너지 하베스팅 비율과 방해 전파 전력 비율을 동시에 도출하였다[5]

이러한 기존 연구와는 다르게 본 논문에서는 에너지 하베스팅만 허용된 별도의 비신뢰적 노드가 존재하는 환경에서 무선 충전이 가능한 전력 분할 기반 보안 릴레이를 고려하였다. 비신뢰적 노드의 에너지 하베스팅 요구량을 보장해주면서 동시에 잠재적 도청을 막기 위한 보안 전송률 최대화 문제를 수식적으로 도출하고, 시뮬레이션을 통해서 최적의 전력 분할 비율을 찾았다. 또한, 기존 방안과의 비교를 통해 효과적인 전력 분할 비율 제어는 시스템의 보안 전송률을 향상시킬 수 있음을 보였다.

Ⅱ. 시스템 모델 및 문제 정의

그림 1은 송신 노드 (S), 릴레이 (R), 수신 노드 (D), 비신뢰적 노드(EH)로 구성된 two-hop 네트워크를 보여준다. 각 노드에는 한 개의 안테나가 장착되어 있으며, half-duplex 방식으로 신호를 송수신한다. 또한, 송신 노드와 수신 노드 사이에는 직접적인 무선 채널이 존재하지 않으며, 릴레이가 증폭-후-전달 (Amplify -and-Forward) 방식을 이용해 두 노드 사이의 데이터를 전달한다[4-5]. 또한, 릴레이와 비신뢰적 노드는 별도의 에너지원이 없는 무전원 노드로써 송

◆ First Author : (0000-0002-3867-1921)Sangmyung University, Department of Computer Science, ksshin@smu.ac.kr, 조교수, 정회원
논문번호 : 202303-066-S-LU, Received March 30, 2023; Revised April 12, 2023; Accepted April 12, 2023

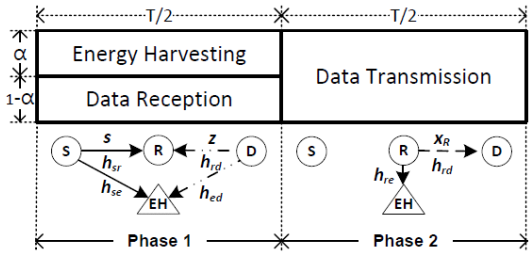

그림 1. 시스템 모델
Fig. 1. System model

신 노드와 수신 노드가 전송하는 신호를 수신하고 이 수신 신호로부터 전력 분할 비율 $0 \le \alpha \le 1$를 조절하여 에너지 하베스팅을 수행한다. 하지만 비신뢰적 노드는 수신한 신호로부터 정보를 해석할 권한이 없으며, 에너지 하베스팅 중 불법으로 신호를 도청할 수 있는 잠재적 도청자로 간주한다 [6-7].

노드 i와 j 사이의 무선 채널은 h_{ij}로 표기하고, $h_{ij} \sim CN(0\ ,\ \lambda_{ij})$ complex normal 분포를 따른다고 가정한다. 또한, 각 노드에서 수신한 신호에는 $n \sim CN(0\ ,\ \sigma^2)$의 Additive White Gaussian Noise(AWGN)가 존재한다고 가정한다.

제안하는 보안 릴레이 프로토콜은 전체 시간 T동안 동일한 주기 $\frac{T}{2}$를 갖는 두 개의 위상으로 구성되어 있다. 첫 번째 위상에서, 송신 노드는 전송 전력 P_S로 정규화된 데이터 신호 s를 릴레이에 전송한다. 이와 동시에 신호 s가 비신뢰적 노드에 도청당하는 것을 막기 위해 수신 노드 역시 전송 전력 P_Z로 정규화된 방해 잡음 z를 릴레이에 전송한다. 릴레이는 수신한 신호의 전력을 나눠 α의 비율은 에너지 하베스팅에 사용하고 $1-\alpha$의 비율은 신호를 수신하는데 사용한다. 따라서 릴레이가 수확한 에너지는 다음과 같다.

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

식 (1)에서 η는 에너지 변환 효율이다. 또한, 릴레이에서 수신한 신호는 다음과 같다.

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

만약 첫 번째 위상에서 비신뢰적 노드가 에너지 하베스팅 대신 신호를 도청하는 경우의 수신한 신호와 Signal-to-Interference-plus-Noise-Ratio (SINR) 는 각각 다음과 같다.

$$y_E^{[1]} = h_{se}\sqrt{P_S}s + h_{ed}\sqrt{P_Z}z + n. \quad (3)$$

$$\Gamma_E^{[1]} = \frac{P_S|h_{se}|^2}{P_Z|h_{ed}|^2 + \sigma^2}. \quad (4)$$

두 번째 위상에서 릴레이는 수확한 전력 $P_R = \frac{E_R}{T/2} = \eta\alpha P_H$을 이용하여 신호를 A_R만큼 증폭 후 수신 노드에 전달한다. 이때 증폭된 릴레이 신호는 다음과 같다.

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

또한, 수신 노드가 수신한 신호는 다음과 같다.

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

식 (6)에서 수신 노드는 수신한 신호로부터 자신이 보낸 방해 잡음과 관련된 항을 제거할 수 있으므로 수신 노드의 SINR은 다음과 같다[4,5].

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

식 (7)로부터 수신 노드에서의 데이터 전송률은 $R_D = \frac{T}{2}log_2(1+\Gamma_D)$와 같이 표현된다.

반면, 두 번째 위상에서 비신뢰적 노드가 도청 하는 경우 수신한 신호 및 SINR은 각각 다음과 같다.

$$\begin{aligned} y_E^{[2]} &= h_{re}x_R + n \\ &= \frac{\sqrt{(1-\alpha)P_S P_R}\,h_{sr}h_{re}s + \sqrt{(1-\alpha)P_Z P_R}\,h_{rd}h_{re}z}{\sqrt{(1-\alpha)P_H + \sigma^2}} \\ &\quad + \frac{\sqrt{P_R}\,h_{re}n}{\sqrt{(1-\alpha)P_H + \sigma^2}} + n. \end{aligned} \quad (8)$$

$$\Gamma_E^{[2]} = \frac{(1-\alpha)P_S P_R|h_{sr}|^2|h_{re}|^2}{(1-\alpha)P_Z P_R|h_{rd}|^2|h_{re}|^2 + \sigma^2\left(P_R|h_{re}|^2 + (1-\alpha)P_H + \sigma^2\right)}. \quad (9)$$

식 (4)와 (9)를 이용하면 비신뢰적 노드에서의 데이터 전송률은 $R_E = \frac{T}{2} log_2\left(1+I_E^{[1]}+I_E^{[2]}\right)$와 같다.

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

$$R_S = R_D - R_E = \left[\frac{T}{2} log_2\left(\frac{1+\Gamma_D}{1+I_E^{[1]}+I_E^{[2]}}\right)\right]^+. \quad (10)$$

여기서 $[x]^+ = \max(x,0)$이다.

만약 비신뢰적 노드가 도청을 하지 않고 전체 시간 T동안 에너지 하베스팅을 하는 경우 수확 가능한 에너지는 다음과 같다.

$$E_E = \eta\frac{T}{2}\left(|h_{se}|^2 P_S + |h_{ed}|^2 P_Z + |h_{re}|^2 P_R\right). \quad (11)$$

즉, 비신뢰적 노드의 최소 에너지 하베스팅양 $E_{\min}$을 보장해주면서, 동시에 비신뢰적 노드의 잠재적 도청을 막을 수 있는 릴레이의 최적의 전력 분할 비율을 도출하고자 한다.

$$\begin{array}{ll} \max\limits_{0\le\alpha\le 1} & R_S \\ s.t. & E_E \ge E_{\min}. \end{array} \quad (12)$$

위의 최적화 문제는 제약 조건을 만족하는 구간에서 1차원 탐색를 통해 수치적으로 찾을 수 있다. 이를 통해 비신뢰적 노드가 에너지 하베스팅을 수행하는지 도청을 하는지 정확히 모르는 상황에서도 비신뢰적 노드의 에너지 하베스팅 요구량과 신뢰적 노드들의 통신 보안을 동시에 만족시켜 줄 수 있다.

Ⅲ. 시뮬레이션 결과

시뮬레이션을 위한 시스템 변수는 $T=1$, $P_S = P_D = 23dBm$, $E_{\min} = -20dBm$, $\sigma^2 = -70dBm$, $\eta = 0.5$으로 설정하였다[2-5]. 송수신 노드 사이의 거리는 20m이며, 릴레이는 중앙에 배치하였고 비신뢰적 노드는 송수신 노드 사이에서 임의 발생 시켰다. Path-loss exponent는 2.7로 선정하였으며, 다중경로 페이딩은 평균이 1인 지수 확률 변수로 반영하여 최종적으로 무선 채널을 생성하였다.

그림 2는 전력 분할 비율(α)에 대한 보안 전송률(R_S)의 관계를 보여준다. 이 결과는 하나의 채널 상황에 대한 예시를 보여준다. R_S는 α에 대해 위로 복록한

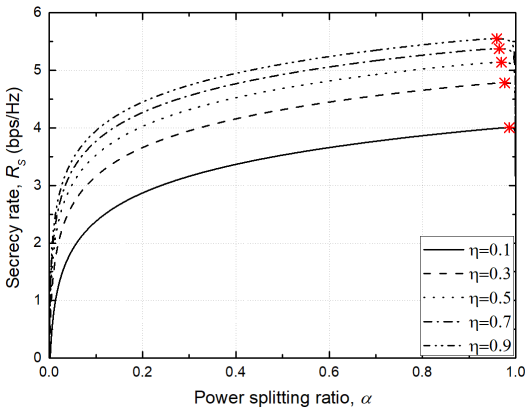

그림 2. 보안 전송률 vs. 전력 분할 비율
Fig. 2. Secrecy rate vs. Power splitting ratio

형태이므로 1차원 탐색를 통해 최적의 α 및 최대 R_S 값을 찾을 수 있다. 또한, 큰 에너지 변환 효율(η)에 대해 작은 α로도 비슷한 에너지를 수확할 수 있기 때문 η가 커질수록 최적의 α가 작아지는 것을 확인할 수 있다. 전력 분할 기반 보안 릴레이의 경우 α를 0.9 이상의 값으로 선정하여 릴레이가 에너지 수확을 많이 하는 것이 보안 전송률 측면에서 최적임을 알 수 있다.

그림 3은 에너지 변환 효율(η)에 대한 보안 전송률(R_s)을 보여준다. 여기서 비교 방안으로는 0.25, 0.5, 0.75의 고정된 α를 갖는 기법으로 선정하였다. 그림 2의 결과에서 볼 수 있듯이 최적의 α가 0.9 이상이었으므로 비교 방안은 α가 커질수록 성능이 향상됨을 알 수 있다. 또한, η가 커질수록 릴레이는 같은 신호에 대해 더 큰 에너지를 수확하여 이를 신호 전송에 사용할 수 있으므로 보안 전송률이 높아진다. 이 결과를 통해

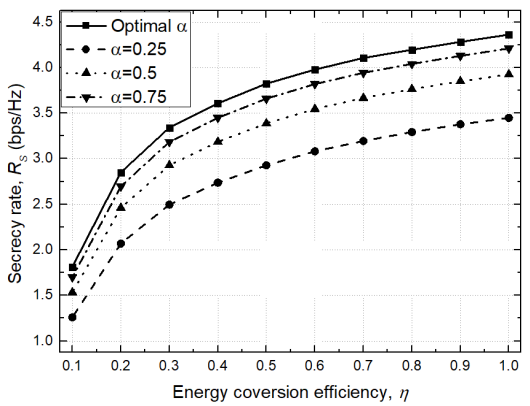

그림 3. 보안 전송률 vs. 에너지 변환 효율
Fig. 3. Secrecy rate vs. Energy conversion efficiency

최적의 α 선정은 전력 분할 기반 보안 릴레이의 성능 향상에 큰 영향을 미치는 것을 확인할 수 있다.

그림 4는 에너지 하베스팅 요구량($E_{\min}$)에 대한 보안 전송률(R_s)을 보여준다. 최적의 α는 보안 전송률을 최대화하는 방향으로 결정이 되기 때문에 에너지 하베스팅 요구량을 상대적으로 쉽게 만족할 수 있는 범위인 $E_{\min} \leq -20dBm$에서 α는 거의 비슷한 값을 가지며, 그에 따라 제안 방안은 상대적으로 일정한 R_s를 달성한다. 하지만 $E_{\min}$이 커지게 되면 보안 전송률에서 손해를 보더라도 α를 늘려서 $E_{\min}$을 만족시켜줘야 하므로 제안 방안의 R_s는 감소한다. 고정된 α를 갖는 기법의 경우도 역시 $E_{\min}$이 커지면 $E_{\min}$을 보장해주지 못하는 채널 환경이 더 빈번히 발생하게 되고, 이 경우 최적화 문제 (12)가 infeasible 하게 되어 결국 해당 채널에서 보안 전송률이 0이 된다. 그 결과 여러 채널에 대해 얻은 보안 전송률의 평균을 취한 값인 R_s가 급격히 감소한다.

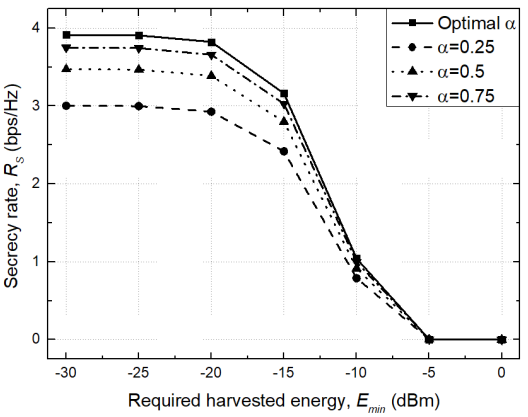

그림 4. 보안 전송률 vs. 에너지 하베스팅 요구량
Fig. 4. Secrecy rate vs. Required harvested energy

Ⅳ. 결 론

본 논문에서는 비신뢰적 노드가 존재하는 무선 충전이 가능한 전력 분할 기반 보안 릴레이를 고려하였다. 비신뢰적 노드의 에너지 하베스팅 요구량을 보장해주면서, 동시에 잠재적 도청을 막기 위한 보안 전송률 최대화 문제를 수식화하였다. 또한, 시뮬레이션을 통해서 보안 전송률 측면에서 최적의 전력 분할 비율을 찾고, 이를 통해 시스템의 보안 성능을 향상시킬 수 있음을 확인하였다. 추후 확장 연구로써 최적화 기법을 이용하여 제안한 보안 전송률 최대화 문제를 수학적으로 풀고 시뮬레이션을 통해 도출한 해의 정확성을 확인하고자 한다.

References

[1] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451-456, Jul. 1978. (https://doi.org/10.1109/TIT.1978.1055917)

[2] K. Lee and J.-T. Lim, "Effects of outdated channel on secrecy performance of power splitting-based relaying protocol," *J. KICS*, vol. 44, no. 5, pp. 829-834, May 2019. (https://doi.org/10.7840/kics.2019.44.5.829)

[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] J.-T. Lim, K. Lee, and Y. Han, "Secure communication with outdated channel state information via untrusted relay capable of energy harvesting," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11323-11337, Oct. 2020. (https://doi.org/10.1109/TVT.2020.3010008)

[6] Z. Deng and Y. Pan, "Optimal beamforming for IRS-assisted SWIPT system with an energy-harvesting eavesdropper," *Electronics*, vol. 10, no. 20, pp. 2536, Oct. 2021. (https://doi.org/10.3390/electronics10202536)

[7] K. Lee, J. -P. Hong, and W. Lee, "Deep learning framework for secure communication with an energy harvesting receiver," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 10121-10132, Oct. 2021. (https://doi.org/10.1109/TVT.2021.3103521)