https://doi.org/10.7840/kics.2023.48.6.685

잠재적 도청자로부터 물리 계층 보안 성능 향상을 위한 시간 전환 기반 보안 릴레이

신 경 섭◆

Time Switching-Based Secure Relay for Enhancing Performance of Physical Layer Security from Potential Eavesdropper

Kyungseop Shin◆

요 약

본 논문에서는 에너지 하베스팅만 허용된 비신뢰적 노드가 존재할 때, 해당 노드의 최소 에너지 하베스팅 요구량을 보장해주면서 동시에 잠재적 도청을 막기 위한 보안 전송률 최대화 문제를 수식적으로 모델링 하였다. 시뮬레이션을 통해 보안 전송률을 최대화할 수 있는 최적의 시간 전환 비율을 찾았으며, 시간 전환 기반 보안 릴레이에서는 수신한 신호의 0.15~0.2 정도의 비율을 에너지 하베스팅 하는 것이 최적임을 확인하였다.

Key Words : Physical layer security, secrecy rate, time switching, untrusted node, jamming signal

ABSTRACT

In this paper, when there is an untrusted node that only energy harvesting is allowed, we formulate the problem that maximizes the secrecy rate to prevent potential eavesdropping while ensuring the minimum energy harvesting requirement of this untrusted node. Through simulations, we found the optimal time switching ratio for maximizing the secrecy rate, and confirmed that it is optimal to harvest energy at a ratio of 0.15~0.2 of the received signal for the time switching-based secure relay.

Ⅰ. 서 론

최근 사물인터넷 기술의 발달로 다양한 디바이스가 서로 다른 네트워크에 접속하게 되면서 정보 보안 문제가 중요해지고 있다. 이에 따라 별도의 암호화 없이 도청자에게 방해 전파를 전송하여 정보의 도청을 막는 물리 계층 보안 기술에 대한 관심이 커지고 있다[1]. 또한, 릴레이 전송 환경에서 자신이 보낸 신호는 self-cancellation이 가능하다는 점에 착안하여, 발신 노드가 데이터 신호를 전송할 때 목적 노드 역시 함께 방해 신호를 전송해주는 destination- assisted jamming 방안이 제안되었다[2-3]. 이 연구는 무선 충전이 가능한 환경으로까지 확장되었다[4-6]. 특히 통신 보안 용량을 최대화할 수 있는 시간 전환 기반 릴레이 기법이 제안되었으나, 도청 채널 정보를 안다는 비현실적인 가정에 기반하였다[6].

현재 에너지 하베스팅만 허용된 비신뢰적 노드가 존재하는 환경에서의 보안 릴레이에 대한 기존 연구는 없다. 사물인터넷 환경에서는 다양한 네트워크가 존재하고 사용하는 센서의 수도 기하급수적으로 늘어날 수 있기 때문에, 센서의 배터리 교체가 쉽지 않을 것으로 예상된다[7]. 즉, 통신을 하지 않는 센서는 주변 센서의 통신 신호로부터 에너지를 하베스팅하여 무전원으로 동작이 가능하여야 한다. 따라서 본 논문에서는 잠재적 도청자의 역할을 할 수 있는 에너지 하베스팅이 가능한 비신뢰적 노드가 존재할 때 시스템의 보안 전송률을 수식적으로 도출하고, 시뮬레이션을 통해서 에너지 하베스팅 요구사항을 만족하면서 보안 전송률을 최대화하는 최적의 시간 전환 비율을 찾았다. 또한, 기존 방안과의 비교를 통해 시간 전환 비율 제어는 시스템의 보안 성능을 향상시킬 수 있음을 보였다.

Ⅱ. 시스템 모델 및 문제 정의

그림 1은 본 논문에서 고려하고 있는 발신 노드(S), 릴레이 (R), 목적 노드 (D), 에너지 하베스팅만 허용된 비신뢰적 노드(EH)로 구성된 네트워크를 보여준다. 각 노드는 한 개의 안테나를 이용해 half-duplex 방식으로 신호를 송수신한다[2-3]. 또한, 발신 노드와

◆ First Author : (ORCID:0000-0002-3867-1921) Sangmyung University, Department of Computer Science, ksshin@smu.ac.kr, 조교수, 정회원
논문번호 : 202303-065-B-LU, Received March 30, 2023; Revised April 12, 2023; Accepted April 12, 2023

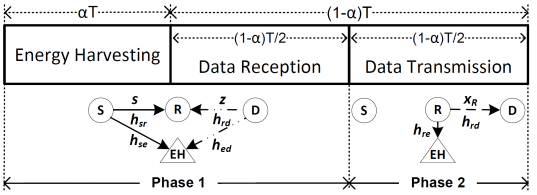

그림 1. 시스템 모델
Fig. 1. System model

목적 노드 사이에는 직접적인 무선 링크가 존재하지 않으므로, 릴레이가 증폭-후-전달 (Amplify-and-Forward) 프로토콜을 이용해 두 노드 사이의 데이터 전달을 돕는다[4-5]. 또한, 릴레이와 EH 노드는 수신한 신호로부터 시간 전환 비율 $0 \le \alpha \le 1$를 조절하여 에너지 하베스팅이 가능하다[2]. 하지만 EH 노드는 수신한 신호를 해석할 권한을 갖지 않는 비신뢰적 노드로써, 불법으로 신호를 도청할 수 있는 잠재적 도청자로 생각할 수 있다[8-9]. 또한, EH 노드의 에너지 하베스팅 요구량을 충족시켜주기 위해 다른 노드들은 EH 노드의 채널 정보를 알고 있다.

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

제안하는 보안 릴레이 프로토콜은 전체 시간 T동안 다음과 같은 2가지 위상으로 구성되어 있다. 첫 번째 위상은 $\alpha T + \frac{(1-\alpha)T}{2}$의 시간으로 구성되어 있으며, 발신 노드와 목적 노드는 αT 동안 각각 P_S와 P_Z의 전송 전력으로 릴레이에 전력을 보낸다. 이 시간 동안 릴레이가 수확한 에너지는 다음과 같다.

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

식 (1)에서 η는 에너지 변환 효율이다.

그 후 발신 노드는 $\frac{(1-\alpha)T}{2}$동안 정규화된 데이터 신호 s를 릴레이에 전송한다. 이 경우 신호 s가 EH 노드에 그대로 전달되면 도청의 위험이 있으므로, 이를 막기 위해 목적 노드 역시 동시에 정규화된 방해 신호 z를 릴레이에 전송한다. 따라서 릴레이에서 수신한 신호는 다음과 같다.

$$y_R = h_{sr}\sqrt{P_S}s + h_{rd}\sqrt{P_Z}z + n. \tag{2}$$

만약 EH 노드가 $\frac{(1-\alpha)T}{2}$동안 에너지 하베스팅 대신 신호를 도청하는 경우의 수신한 신호와 그로부터 얻을 수 있는 Signal-to-Interference-plus-Noise Ratio (SINR)은 각각 다음과 같다.

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

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

두 번째 위상에서 릴레이는 수신한 신호를 수확한 전력 $P_R = \frac{E_R}{(1-\alpha)T/2} = \frac{2\eta\alpha P_H}{(1-\alpha)}$을 이용하여 A_R만큼 증폭 후 목적 노드에 전달한다. 증폭된 릴레이 신호는 다음과 같다.

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

이때 목적 노드가 수신한 신호는 다음과 같다.

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

식 (6)에서 목적 노드는 자신이 보낸 방해 신호와 관련된 항을 제거할 수 있으므로[4-5] 목적 노드의 SINR은 다음과 같다.

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

식 (7)을 이용하면 목적 노드에서의 데이터 전송률은 $R_D = \frac{(1-\alpha)T}{2} log_2(1+\Gamma_D)$와 같이 표현된다.

반면, 두 번째 위상에서 EH 노드가 신호를 도청하는 경우 수신한 신호 및 SINR은 각각 다음과 같다.

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

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

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

결과적으로 R_D과 R_E를 이용하여 데이터 채널과 도청 채널의 전송률 차로 정의되는 보안 전송률은 다음과 같이 나타낼 수 있다[1].

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

여기서 $[x]^+=\max(x,0)$이다.

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

$$E_E=\eta\frac{(1+\alpha)T}{2}\left(|h_{se}|^2P_S+|h_{ed}|^2P_Z\right)+\eta\frac{(1-\alpha)T}{2}|h_{re}|^2P_R. \quad (11)$$

즉, 본 논문에서는 EH 노드의 에너지 하베스팅 요구량 $E_{\min}$을 보장해주면서, 동시에 보안 전송률을 최대화하여 EH 노드의 잠재적 도청을 막는 릴레이의 최적의 시간 전환 비율을 도출하고자 한다.

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

위의 최적화 문제는 제약 조건을 만족하는 feasible region에서 one-dimensional search를 통해 릴레이에서 수치적으로 찾을 수 있다. 이를 위해서 릴레이는 각 노드 사이의 채널 정보와 발신 노드와 목적 노드가 신호를 송신하는데 사용하는 전력에 대한 정보를 알아야 한다.

Ⅲ. 시뮬레이션 결과

기본적인 시뮬레이션 환경은 다음과 같이 $T=1s$, $\sigma^2=-70dBm$, $P_S=P_D=23dBm$, $E_{\min}=-20dBm$, $\eta=0.5$으로 설정하였다[2-7]. 또한, 발신 노드와 목적 노드의 거리는 20m이며, 릴레이는 중앙에 배치하였고 EH 노드는 발신 노드와 목적 노드 사이에서 임의 발생 시켰다. 무선 채널 생성을 위하여 path-loss exponent는 2.7로 설정하였으며, 다중경로 페이딩은 평균이 1인 지수 확률 변수로 생성하였다.

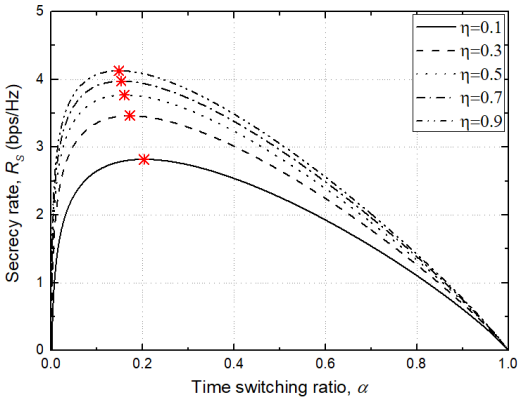

그림 2. 보안 전송률 vs. 시간 전환 비율
Fig. 2. Secrecy rate vs. Time switching ratio

그림 2는 시간 전환 비율(α)에 대한 보안 전송률(R_S)의 관계를 보여준다. 이 결과는 하나의 채널 상황에 대한 예시를 보여준다. R_S는 α에 대해 concave한 형태를 띄고 있으므로 one-dimensional search를 통해 최적값을 쉽게 찾을 수 있다. 채널 환경이 바뀔 때마다 최적의 α를 찾아 값을 조정해야 하며, 시뮬레이션 결과 정해진 채널 환경에 대해 one-dimensional search를 통해 최적의 α를 찾는데 약 1ms의 시간이 소요됨을 확인할 수 있었다. 또한, 에너지 변환 효율(η)이 커질수록 최적의 α가 작아지는 것을 확인할 수 있는데, 이는 η가 커질수록 작은 α에 대해서도 비슷한 에너지를 하베스팅할 수 있기 때문이다. 시간 전환 기반 보안 릴레이의 경우 α를 약 0.15~0.2 사이의 값으로 선정하는 것이 보안 전송률 측면에서 최적임을 알 수 있다.

그림 3은 에너지 변환 효율(η)에 대한 보안 전송률(R_s)을 보여준다. 여기서 최적의 α를 찾는 기법과 0.25, 0.5, 0.75의 고정된 α를 갖는 기법을 비교하였다. 그림 2의 결과에서 볼 수 있듯이 최적의 α가 0.2 근처였으므로 고정된 α를 갖는 기법은 α가 커질수록 성능이 열화됨을 확인할 수 있다. 또한, η가 커질수록 릴레이는 같은 신호에 대해 더 많은 양의 에너지를 획득할 수 있으므로 자유도가 높아져 보안 전송률이 상승한다.

그림 4는 에너지 하베스팅 요구량($E_{\min}$)에 대한 보안 전송률(R_s)을 보여준다. 제안방안의 $E_{\min}$이 커짐에 따라 최적의 α에서 제약조건을 만족시키지 못하게

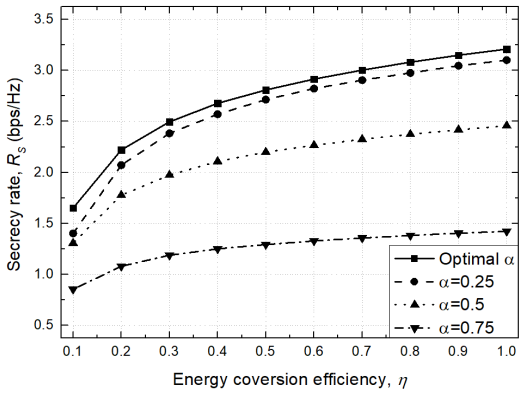

그림 3. 보안 전송률 vs. 에너지 변환 효율
Fig. 3. Secrecy rate vs. Energy conversion efficiency

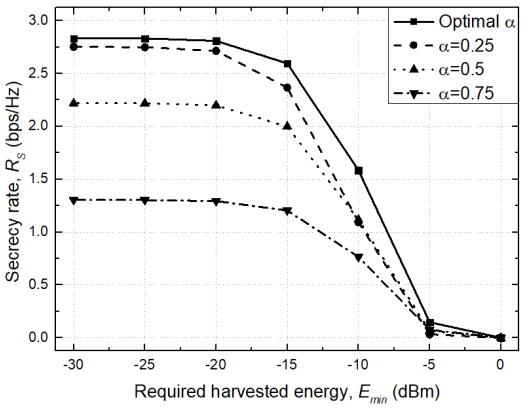

그림 4. 보안 전송률 vs. 에너지 하베스팅 요구량
Fig. 4. Secrecy rate vs. Required harvested energy

되고, 결과적으로 제약조건을 만족시키기 위해 α값을 증가시켜 보안 전송률이 감소한다. 고정된 α를 사용하는 기법의 경우 $E_{\min}$이 커질수록 제약조건을 보장하지 못하는 채널 환경이 늘어나고 이 경우 infeasible 한 상황으로 $R_s=0$이 되므로 결과적으로 보안 전송률이 감소한다. 모든 $E_{\min}$ 값에 대해 제안 방안이 가장 높은 성능을 달성함을 확인할 수 있으므로, 시간 전환 기반 보안 릴레이의 성능 향상을 위해서는 최적의 α 선정이 중요함을 확인할 수 있다.

Ⅳ. 결 론

본 논문에서는 에너지 하베스팅만 허용된 비신뢰적 노드가 존재할 때, 해당 노드의 최소 에너지 하베스팅 요구량을 보장해주면서, 동시에 잠재적 도청을 막기 위한 보안 전송률 최대화 문제를 수식적으로 모델링 하였다. 또한, 시뮬레이션을 통해서 보안 전송률을 최대화할 수 있는 최적의 시간 전환 비율이 존재함을 보이고, 효율적인 시간 전환 비율 선정을 통해 시스템의 보안 전송률을 향상시킬 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. (https://doi.org/10.1109/TIT.2010.2050958)

[2] 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. (https://doi.org/10.7840/kics.2019.44.4.678)

[3] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Secur.,* vol. 8, no. 4, pp. 682-694, Apr. 2013. (https://doi.org/10.1109/TIFS.2013.2248730)

[4] K. Lee, J.-P. Hong, H.-H. Choi, and M. Levorato, "Adaptive wireless-powered relaying schemes with cooperative jamming for two-hop secure communication," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2793-2803, Aug. 2018. (https://doi.org/10.1109/JIOT.2018.2830880)

[5] K. Lee, J. Bang, and H.-H. Choi, "Secrecy outage minimization for wireless-powered relay networks with destination-assisted cooperative jamming," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1467-1476, Feb. 2021. (https://doi.org/10.1109/JIOT.2020.3013573)

[6] 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. (https://doi.org/10.7840/kics.2017.42.10.1955)

[7] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surv. Tuts.*, vol. 17, no. 2, pp. 757-

789, Second Quart. 2015.
(https://doi.org/10.1109/COMST.2014.2368999)

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

[9] 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)