https://doi.org/10.7840/kics.2023.48.7.826

보안 에너지 효율성 최적화를 위한 시간 전환 기반 보안 릴레이

신 경 섭•

Time Switching-Based Secure Relay for Optimizing Secrecy Energy Efficiency

Kyungseop Shin•

요 약

본 논문에서는 에너지 수확이 가능한 비신뢰적 중계 노드가 존재할 때, 보안 에너지 효율성을 정의하고 이를 최대화하는 문제를 수식화 하였다. 시뮬레이션을 통해 보안 에너지 효율성을 최대화 할 수 있는 최적의 시간 전환 비율과 방해 전파 전력 비율을 찾았으며, 이 값을 최적화함으로써 네트워크의 성능을 크게 향상시킬 수 있음을 확인하였다.

Key Words : Physical layer security, secrecy energy efficiency, time switching, untrusted relay, jamming signal

ABSTRACT

In this paper, we define the secrecy energy efficiency and formulate the problem of maximizing it in the presence of untrusted relay that is capable of energy harvesting. Through simulations, we find the optimal time switching ratio and jamming power ratio to maximize the secrecy energy efficiency, and show that by optimizing these values, the performance of the network can be significantly improved.

Ⅰ. 서 론

기존 암호화 방식은 암호키 공유에 추가적인 비용과 절차가 필요한 반면 물리 계층 보안 기술은 암호화 없이 도청자에게 방해 전파를 전송하여 도청을 막을 수 있으므로 이 기술에 대한 관심이 커지고 있다[1]. 특히 비신뢰적 중계 노드가 존재하는 환경에서 발신 노드가 데이터 신호를 전송할 때 목적 노드 역시 방해 전파를 전송하는 destination- assisted jamming 방안이 연구되었다[2,3]. 이를 통해 목적 노드는 추후 중계 노드가 전달한 신호로부터 자신이 보낸 방해 전파는 self-cancellation 함으로써 데이터 신호를 복원할 수 있는 반면 중계 노드는 방해 전파로 인해 데이터 신호를 복원할 수 없다. 또한, 이 연구는 RF 에너지 하베스팅이 가능한 환경까지 확장되어 보안 전송률을 최대화하기 위한 최적의 에너지 하베스팅 비율을 도출하였다[4,5].

하지만 보안 전송률 최대화를 주로 고려한 기존 연구와는 다르게 무선 노드는 제한된 전력량을 가지고 있다는 점을 감안하여 본 논문에서는 에너지 하베스팅이 가능한 비신뢰적 중계 노드가 존재할 때 시스템의 보안 에너지 효율성을 수식적으로 모델링하고, 시뮬레이션을 통해서 이를 최대화하는 최적의 시간 전환 비율과 방해 전파 전력 비율을 함께 찾았다. 또한, 기존방안과의 성능 비교를 통해 보안 에너지 효율성 관점에서 제안방안의 우수성을 보였다.

Ⅱ. 시스템 모델 및 문제 정의

본 논문에서는 그림 1과 같이 발신 노드 (S), 중계 노드 (R), 목적 노드 (D)로 구성된 네트워크를 고려한다. 각 노드에는 단일 안테나가 부착되어 있으며, 반이중 방식으로 신호를 송수신한다. 발신 노드와 목적 노드 사이에는 신호를 직접적으로 전송하기 위한 무선 링크가 존재하지 않기 때문에, 중계 노드가 증폭-후-전달 릴레이 (Amplify-and-Forward Relay) 기법을 이용해 두 노드 사이의 신호를 전달한다[5]. 또한, 중계 노드는 무전원 노드로써, 발신 노드와 목적 노드에게 수신한 신호로부터 시간 전환 비율 $0 \le \alpha \le 1$를 조절하여 에너지를 하베스팅하고 이 에너지를 사용하여

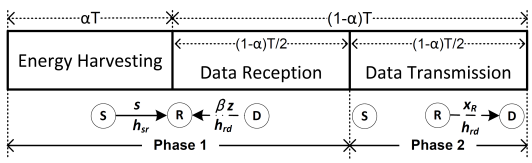

그림 1. 시스템 모델
Fig. 1. System model

• First Author : (0000-0002-3867-1921)Sangmyung University, Department of Computer Science, ksshin@smu.ac.kr, 조교수, 정회원
논문번호 : 202307-081-B-LU, Received March 30, 2023; Revised April 13, 2023; Accepted April 13, 2023

신호를 전달한다[5]. 이때 중계 노드는 발신 노드의 데이터 신호 해석이 허용되지 않은 비신뢰적 노드로써, 불법으로 신호를 도청할 수 있는 잠재적 도청자로 생각할 수 있다.

임의의 두 노드 i와 j 사이의 채널은 h_{ij}로 나타내고, $h_{ij} \sim CN(0\ ,\ \lambda_{ij})$는 복소 정규 분포를 따른다고 가정한다. 또한, 각 노드에서 수신한 신호에는 복소 정규 분포 $n \sim CN(0\ ,\ \sigma^2)$를 따르는 Additive White Gaussian Noise(AWGN)가 존재한다고 가정한다.

시간 전환 기반 보안 릴레이 프로토콜의 전체 시간은 T로 표현하며, 다음과 같은 2가지 위상으로 구성된다. 첫 번째 위상의 αT동안 발신 노드와 목적 노드는 각각 P_S와 βP_Z의 전송 전력으로 중계 노드에 전력을 보내고 중계 노드는 이 신호들로부터 전력을 획득한다. 여기서 $0 \le \beta \le 1$는 목적 노드의 방해 전파 전력 비율이며, 이 시간 동안 중계 노드가 획득한 에너지는 다음과 같다.

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

식 (1)에서 ζ는 에너지 변환 효율이다.

그 후 첫 번째 위상의 $\frac{(1-\alpha)T}{2}$동안 발신 노드는 정규화된 데이터 신호 s를 중계 노드에 전송한다. 이 경우 중계 노드에 데이터 신호 s만 전달되면 도청의 위험이 있으므로, 이를 막기 위해 목적 노드 역시 정규화된 방해 신호 z를 중계 노드에 전송한다. 따라서 중계 노드에서 수신한 신호는 다음과 같이 표현된다.

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

만약 중계 노드가 수신 신호로부터 데이터 신호 s를 도청한 경우 Signal-to-Interference-plus-Noise Ratio (SINR)은 다음과 같다.

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

식 (3)을 이용하면 중계 노드에서의 스펙트럼 효율성은 다음과 같이 표현된다.

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

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

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

식 (5)를 이용하면 두 번째 위상에서 목적 노드가 수신한 신호는 다음과 같다.

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

식 (6)에서 목적 노드는 자신이 보낸 방해 신호는 이미 알고 있는 정보이므로 이와 관련된 항을 제거할 수 있다[3,5]. 따라서 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 스펙트럼 효율성은 다음과 같다.

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

수식 (4)와 (8)에 정의된 R_R과 R_D를 이용하면 보안 스펙트럼 효율성은 다음과 같다[1].

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

여기서 $[x]^+ = \max(x,0)$이다.

반면, 네트워크에서 사용하는 총 에너지는 다음과 같다.

$$E_T = TP_C + \frac{(1+\alpha)T}{2}(P_S + \beta P_Z). \tag{10}$$

식 (10)에서 P_C는 전체 노드의 회로에서 소모되는 전력이다.

식 (9)과 (10)을 이용하여 단위 전력당 얼마나 효율

적으로 보안 스펙트럼 효율성을 달성하는가를 나타내는 지표인 보안 에너지 효율성을 다음과 같이 정의할 수 있다.

$$\eta_S = \frac{R_S}{E_T}. \tag{11}$$

본 논문에서는 비신뢰적 중계 노드를 고려하여, 보안 에너지 효율성을 최대화하는 최적의 시간 전환 비율과 방해 전파 전력 비율을 동시에 도출하고자 다음과 같은 최적화 문제를 수식화하였다.

$$\max_{0 \le \alpha \le 1, 0 \le \beta \le 1} \eta_S \tag{12}$$

위의 최적화 문제에서 제약 조건을 만족하는 범위에서 이차원 탐색를 통해 수치적으로 최적의 α와 β를 찾을 수 있다. α와 β를 각각 N등분 한다면 이차원 탐색의 복잡도는 N^2이다.

Ⅲ. 시뮬레이션 결과

시뮬레이션 환경은 다음과 같이 $T=1s$, $\zeta=0.5$, $\sigma^2=-70dBm$, $P_S=43dBm$, $P_C=40dBm$으로 설정하였다[2-5]. 또한, 발신 노드와 목적 노드의 거리는 20m이며, 중계 노드는 중앙에 배치하였다. Path-loss exponent는 2.7로 설정하였으며 다중경로 페이딩은 평균이 1인 지수 확률 변수로 생성하여 최종적으로 랜덤한 값을 갖는 무선 채널을 생성하였다.

그림 2는 최대 방해 전파 전력(P_Z)에 대한 보안 에너지 효율성(η_S)의 관계를 보여준다. 제안방안의 경우 $P_Z<37dBm$의 범위에서 P_Z가 증가함에 따라 η_S가 증가한다.

하지만 P_Z가 $37dBm$보다 커지는 경우 일정한 η_S를 보이는데 이는 P_Z가 커지더라도 목적 노드가 β를 조절하여 일정한 크기의 전력으로 방해 전파를 전송하기 때문이다. 방해 전파 전력을 늘리면 보안 스펙트럼 효율성이 증가하지만 그보다 더 소모되는 에너지양이 증가하게 된다. 즉, 보안 에너지 효율성 측면에서 최적의 방해 전파의 크기가 존재함을 알 수 있다. 같은 이유로 ($\alpha=0.5$, optimal β)방안도 P_Z가 커지더라도 β를 조절하여 일정한 η_S로 수렴하는 것을 확인할 수 있다. 반면 (optimal α, $\beta=0.5$)방안과 ($\alpha=0.5$, $\beta=0.5$)방안의 경우 P_Z가 커짐에 따라 사용되는 방해 전파의 전력도 커지기 때문에 오히려 η_S가 감소하는 것을 확인할 수 있다. 제안방안과 각 기존방안의 성능 비교를 통해 각각의 파라미터 α와 β가 성능에 미치는 영향을 알 수 있으며, 모든 P_Z의 범위에서 제안방안이 가장 높은 성능을 달성하는 것을 확인할 수 있다.

그림 3은 최대 방해 전파 전력(P_Z)에 대한 최적의 시간 전환 비율(α^*)과 방해 전파 비율(β^*)을 보여준다. P_Z가 증가할수록 중계 노드는 α를 줄여 에너지 하베스팅을 적게 하고 신호의 송수신에 더 많은 시간을 할당하는 것을 알 수 있다. 또한, P_Z가 증가할수록 목적 노드는 β를 조절하여 보안 에너지 효율성 측면에서 최적인 일정한 크기의 방해 전파를 전송하는 것을 확인할 수 있다.

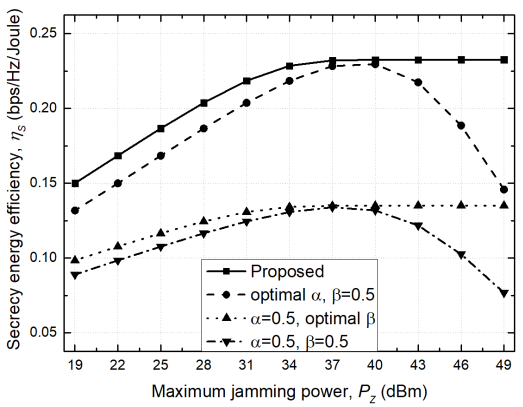

그림 2. 보안 에너지 효율성 vs. 최대 방해 전파 전력
Fig. 2. Secrecy energy efficiency vs. Maximum jamming power

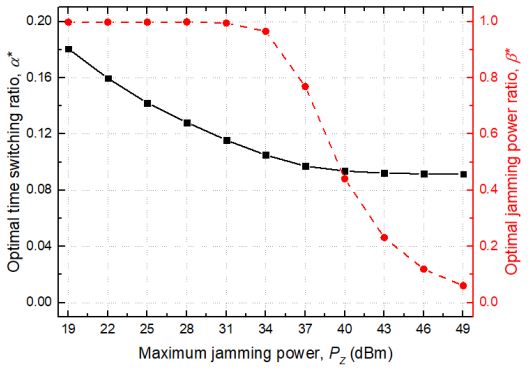

그림 3. 최적의 시간 전환 비율과 방해 전파 비율 vs. 최대 방해 전파 전력
Fig. 3. Optimal time switching ratio and jamming power ratio vs. Maximum jamming power

Ⅳ. 결 론

본 논문에서는 에너지 하베스팅이 가능한 비신뢰적 중계 노드가 존재할 때, 보안 에너지 효율성 최대화 문제를 수식적으로 모델링 하였다. 또한, 시뮬레이션을 통해서 보안 에너지 효율성을 최대화할 수 있는 최적의 시간 전환 비율과 방해 전파 전력 비율을 찾고, 이를 통해 시스템의 보안 에너지 효율성을 크게 향상시킬 수 있음을 확인하였다. 추후 확장 연구로써 파워 분할 기반 보안 릴레이를 고려할 수 있다.

References

[1] A. Mukherjee, “Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints,” in *Proc. IEEE,* vol. 103, no. 10, pp. 1747-1761, Oct. 2015. (https://doi.org/10.1109/JPROC.2015.2466548)

[2] 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)

[3] K. Lee, J.-P. Hong, and H.-H. Choi, “Adaptive jamming power control for untrusted relay networks with imperfect channel reciprocity,” *IEEE Syst J.*, vol. 14, no. 3, pp. 4217-4220, Sep. 2020. (https://doi.org/10.1109/JSYST.2019.2937963)

[4] 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)

[5] 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)