논문 17-42-10-13 The Journal of Korean Institute of Communications and Information Sciences '17-10 Vol.42 No.10
https://doi.org/10.7840/kics.2017.42.10.1955

보안 용량 최대화를 위한 시간 전환 기반 중계기

이 기 송◆, 최 현 호°

Time Switching-based Relaying for Maximizing Secrecy Capacity

Kisong Lee◆, Hyun-Ho Choi°

요 약

무선 RF 신호로부터 전력을 수집하는 RF 에너지 하베스팅은 향후 센서의 무전원화를 가능하게 하는 기술로써 최근 큰 관심을 받고 있다. 본 논문에서는 무전원 릴레이가 존재하는 2-hop 네트워크에서 물리계층 보안을 최대화하기 위한 시간 전환 기반 relaying 기법을 제안한다. 다양한 시뮬레이션 환경에서 기존 방안과의 비교를 통해, 제안 방안이 도청자의 도청을 막아 최적의 보안 용량을 달성함을 보인다.

Key Words : Energy Harvesting, Relay Protocol, Time Switching, Secrecy Capacity, Physical Layer Security

ABSTRACT

Recently, RF energy harvesting, in which energy is collected from the wireless RF signals, is considered as a technology to enable the implementation of wireless-powered sensors. In this paper, we propose a time switching-based relaying protocol for maximizing a physical layer security in 2-hop networks, in which a relay without a power source exists. Comparing with the conventional schemes under various simulation environments, it is demonstrated that the proposed scheme achieves an optimal secrecy capacity by disturbing the overhearing of eavesdropper.

Ⅰ. 서 론

버려지는 RF 신호로부터 전력을 수집하는 RF 에너지 하베스팅 기술은 센서의 전원 문제를 해결할 기술로 최근 각광받고 있다[1-3]. [1]에서는 런던에서 도시 규모의 실험을 통해 RF 신호로부터 초당 수 uW의 에너지 획득이 가능함을 보였다. [2]에서는 RF 신호를 이용하여 정보와 전력을 동시에 수신하기 위한 적응적 시간 전환 기법을 제안하였다. [3]에서는 불완전한 채널 추정이 가능한 에너지 하베스팅 네트워크에서 전력 효율성을 최대화하기 위한 자원할당 방안을 제안하였다. 또한, 최근 수많은 통신 노드가 주파수 대역을 공유하는 이기종 네트워크 (Heterogenous networks) 환경이 구현됨에 따라, 사용자의 정보가 원치 않는 대상에게 유출되는 문제가 상당히 심각해지고 있다[4-6]. [4]에서는 정보 보안을 최대화하기 위한 릴레이와 목적지 간의 협력적 파워 할당 기법이 제안되었다. 또한, [5]에서는 정보 보안 제약을 만족시키기 위한 최적의 릴레이 선택 방안이 연구 되었다. [6]에서는 무선 충전이 가능한 무전원 릴레이에서 정보 보안을 향상시키기 위한 파워 분할 기반 릴레이 프로토콜을 제안하였다.

본 논문에서는, 무전원 릴레이(Relay)가 존재하는 2-hop 네트워크 환경에서 네트워크의 물리계층 보안(Physical layer security)을 최대화하고자 한다. 릴레이는 무전원 노드로써, 발신원(Source)로부터 전송되는 신호로부터 전력을 획득하며, 이 전력을 이용하여 목적지(Destination)에 신호를 전달한다. 릴레이로부터 전송된 신호는 목적지 주변의 존재하는 도청자(Eavesdropper)에서 도청이 가능하다. 이러한 환경에서 발신원의 신호가 도청자에서 도청되는 것을 최소화하고 목적지에 안정적으로 전달될 수 있도록, 네트워크 보안 용량(Secrecy capacity)을 최대화하는 최적의 시간 전환 기반 릴레이 기법을 제안 한다. 제안하는 시간 전환 기반 릴레이 기법은 [6]에서 제안한 파워 분할 기반 릴레이 기법과는 릴레이 구조 및 동작 체계가 명확히 차별된다. 또한, 다양한 시뮬레이션 환

※ 이 논문은 2015 및 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임. (No. 2015R1C1A1A01051747, No. 2016R1C1B1016261)
◆ First Author : Chungbuk National University, School of Information and Communication Engineering, kslee85@cbnu.ac.kr, 정회원
° Corresponding Author : Hankyong National University, Department of Electrical, Electronic and Control Engineering, hhchoi@hknu.ac.kr, 정회원
논문번호 : KICS2017-09-248, Received September 12, 2017; Revised September 22, 2017; Accepted September 22, 2017

경에서 기존 방안과의 성능 비교를 통해 제안 방안의 효율성을 검증한다.

Ⅱ. 시간 전환 기반 릴레이 기법

본 논문에서는 그림 1에서처럼 발신원, 릴레이, 목적지, 도청자 등 4개의 노드가 존재하는 2-hop 네트워크를 고려한다. source-to-relay, relay- to-destination, relay-to- eavesdropper 간의 채널을 각각 h_{sr}, h_{rd}, h_{re}로 정의하고, 각 채널은 independent and identically distributed (i.i.d.) 플랫 페이딩 채널이며, source-to-destination, source-to -eavesdropper, and destination-to- eavesdropper 간의 직접적인 링크는 없다고 가정한다[4]. 각 노드의 수신 신호에는 $n \sim CN(0,\sigma^2)$의 동일한 Additive White Gaussian Noise가 존재한다고 가정한다. 본 논문에서 고려하고 있는 시간 전환 기반 릴레이 프로토콜(Time switching- based relaying protocol)은 전체 블록 시간 T 동안 2-phase로 이루어져 있다. Phase 1에서는 발신원이 릴레이에게 신호 s를 전송한다. 이때 릴레이는 무전원 노드이므로, 발신원으로부터 받은 신호 중 αT 에 해당하는 시간을 이용하여 에너지 하베스팅을 하고, $(1-\alpha)T/2$에 해당하는 시간을 이용하여 신호를 수신한다[1]. 나머지 $(1-\alpha)T/2$의 시간에 해당하는 phase 2에서 릴레이는 phase 1에서 충전한 파워를 이용하여 Amplify-and- forward (AF) 기법을 이용하여 목적지에 신호를 전달한다. 이때 전달된 신호는 역시 도청자에게도 전달이 되어 도청이 된다.

Phase 1에서 릴레이가 수신하는 신호 y_r은 다음과 같이 표현이 가능하다.

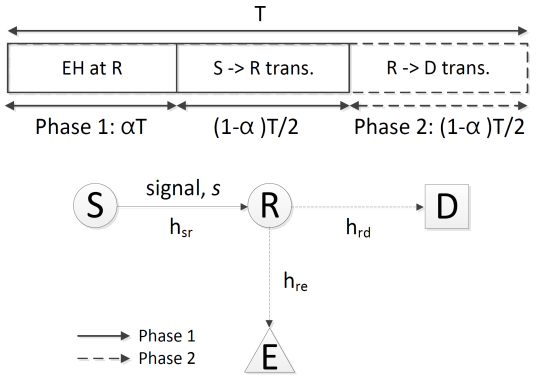

그림 1. 에너지 하베스팅이 가능한 시간 전환 기반 릴레이 시스템 모델
Fig. 1. System model of time switching- based relaying with energy harvesting

$$y_r = \sqrt{P_S} h_{sr} s + n. \tag{1}$$

또한, 릴레이에서 하베스팅된 에너지는 다음과 같다.

$$E_h = T\eta\alpha P_S |h_{sr}|^2. \tag{2}$$

Phase 2에서 릴레이에 의해 전송되는 신호 x_r은 다음과 같다.

$$x_r = \frac{\sqrt{P_r}\, y_r}{\sqrt{P_S |h_{sr}|^2 + \sigma^2}}. \tag{3}$$

여기서 릴레이가 전송에 사용하는 파워 P_r은 수식 (4)와 같이 표현될 수 있다.

$$P_r = \frac{E_h}{(1-\alpha)T/2} = \frac{2\eta\alpha P_S |h_{sr}|^2}{1-\alpha}. \tag{4}$$

또한, 목적지에서 수신되는 신호 y_d는 아래와 같이 표현된다.

$$\begin{aligned} y_d &= h_{rd} x_r + n \\ &= \frac{\sqrt{P_S P_r}\, h_{sr} h_{rd} s + \sqrt{P_r}\, h_{rd} n}{\sqrt{P_S |h_{sr}|^2 + \sigma^2}} + n. \end{aligned} \tag{5}$$

반면, 도청자에서 도청되는 신호 y_e는 아래와 같이 표현된다.

$$\begin{aligned} y_e &= h_{re} x_r + n \\ &= \frac{\sqrt{P_S P_r}\, h_{sr} h_{re} s + \sqrt{P_r}\, h_{re} n}{\sqrt{P_S |h_{sr}|^2 + \sigma^2}} + n. \end{aligned} \tag{6}$$

수식 (5)로부터 목적지에서의 signal- to-noise ratio (SNR)은 다음과 같이 표현할 수 있다.

$$\begin{aligned} \gamma_d &= \frac{P_r P_S |h_{sr}|^2 |h_{rd}|^2}{P_r |h_{rd}|^2 \sigma^2 + \sigma^2 (P_S |h_{sr}|^2 + \sigma^2)} \\ &= \frac{2\eta\alpha P_S^2 |h_{sr}|^4 |h_{rd}|^2}{2\eta\alpha P_S |h_{sr}|^2 |h_{rd}|^2 \sigma^2 + \sigma^2 (1-\alpha)(P_S |h_{sr}|^2 + \sigma^2)}. \end{aligned} \tag{7}$$

또한, 수식 (6)으로부터 도청자에서의 SNR은 다음과 같이 표현된다.

$$\gamma_e = \frac{P_r P_S |h_{sr}|^2 |h_{re}|^2}{P_r |h_{re}|^2 \sigma^2 + \sigma^2 (P_S |h_{sr}|^2 + \sigma^2)} = \frac{2\eta\alpha P_S^2 |h_{sr}|^4 |h_{re}|^2}{2\eta\alpha P_S |h_{sr}|^2 |h_{re}|^2 \sigma^2 + \sigma^2 (1-\alpha)(P_S |h_{sr}|^2 + \sigma^2)}. \quad (8)$$

결론적으로 γ_d와 γ_e로부터 네트워크의 보안 용량은 다음과 같이 구할 수 있다.

$$C_S = \left[\frac{(1-\alpha)T}{2} \{\log_2(1+\gamma_d) - \log_2(1+\gamma_e)\} \right]^+. \quad (9)$$

수식 (9)의 C_S를 최대화 하는 α는 exhaustive search를 통해 찾을 수 있다.

Ⅲ. 시뮬레이션 결과

시뮬레이션에서는 $T = 1s$, Transmit SNR ($\frac{P_S}{\sigma^2}$)=83dB, m(Path-loss exponent)=2.7, $d_{sd} = 30m$, $\eta = 0.5$[3]로 가정하였다. 또한, 평균 1을 갖는 exponentially distributed random variable을 이용하여 채널을 생성하였다[2]. 시뮬레이션을 통해 각 채널 상황에서 C_S를 최대화 할 수 있는 최적의 α를 찾는 Optimal time switching(OTS)과 채널 상황에 무관하게 일정한 α값을 사용하는 기존 방안의 성능을 비교하였다. 그림 2와 3에서는 각 노드 사이의 채널의 영향을 확인하기 위해 다음과 같은 3가지 경우에 대해 결과를 확인하였다; i) $d_{sr} = d_{rd} = 15m$, ii) $d_{sr} = 5m < d_{rd} = 25m$, iii) $d_{sr} = 25m > d_{rd} = 5m$.

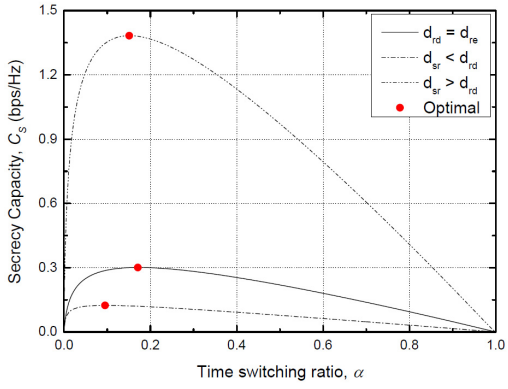

그림 2. 보안 용량 vs. 시간 전환 비율
Fig. 2. Secrecy capacity vs. Time switching ratio

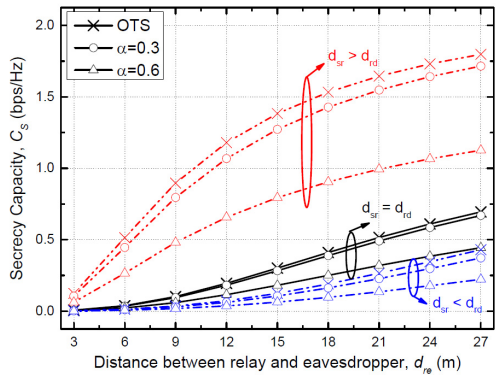

그림 3. 보안 용량 vs. 릴레이와 도청자 사이의 거리
Fig. 3. Secrecy capacity vs. Distance between relay and eavesdropper

그림 2는 시간 전환 비율에 대한 보안 용량을 보여준다. 여기서 $d_{re} = 15m$로 설정하였다. 각각의 경우에서 α에 대해 C_S는 concave한 형태를 지니며, 최적의 α값이 존재한다.

그림 3은 릴레이와 도청자 사이의 거리에 대한 보안 용량을 보여준다. d_{sr}이 커짐에 따라 C_S가 증가하는 것을 확인할 수 있다. 또한, d_{re}가 커짐에 따라 도청자로 전달되는 신호의 감쇠가 심해지고, 이에 따라 도청 감도가 떨어져 전 기법의 C_S가 향상된다. 또한, OTS가 일정한 α를 사용하는 기존 방안에 비해 성능을 크게 개선시키는 것을 알 수 있다.

Ⅳ. 결 론

본 논문에서는 발신원, 릴레이, 목적지, 도청자 등 4개의 노드가 존재하는 2-hop 네트워크에서 보안 용량을 최대화하기 위한 시간 전환 기반 릴레이 프로토콜을 제안하였다. 수학적 모델링 및 exhaustive search를 통해 보안 용량을 최대화 할 수 있는 최적의 시간 전환 비율을 찾았다. 시뮬레이션을 통하여 제안 방안이 기존 방안에 비해 보안 용량을 개선하여, 도청자가 존재하는 환경에서도 물리계층 보안을 향상시킬 수 있음을 확인하였다.

References

[1] M. Pinuela, P. Mitcheson, and S. Lucyszyn, "Ambient RF energy harvesting in urban and semi-urban environments," *IEEE Trans.*

Microwave Theory Tech., vol. 61, no. 7, pp. 2715-2726, Jul. 2013.

[2] L. Liu, R. Zhang, and K. Chua, "Wireless information transfer with opportunistic energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 288-300, Jan. 2013.

[3] K. Lee and J.-P. Hong, "Resource allocation for maximizing energy efficiency in energy harvesting networks with channel estimation error," *J. KIICE*, vol. 20, no. 3, pp. 506-512, Mar. 2016.

[4] 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, Sept. 2013.

[5] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, no. 15, pp. 1787-1791, Oct. 2010.

[6] K. Lee, and H.-H. Choi, "Power splitting-based relaying for improving physical layer security," *J. KICS*, vol. 42, no. 7, pp. 1352-1355, Jul. 2017.