JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 11 : 2022~2028 Nov. 2017

에너지 하베스팅 네트워크에서 최소 요구 보안 용량을 최대화하기 위한 시간 전환 기반의 아날로그 네트워크 코딩

이기송[1] · 최현호[2*]

Time Switching-based Analog Network Coding for Maximizing the Minimum Required Secrecy Capacity in Energy Harvesting Networks

Kisong Lee[1] · Hyun-Ho Choi[2*]

[1]School of Information and Communication Engineering, Chungbuk National University, Cheongju 28644, Korea
[2*]Department of Electrical, Electronic and Control Engineering, Hankyong National University, Anseong 17579, Korea

요 약

최근 사물 인터넷 기술의 발달로 인해 사용되는 센서의 수가 늘어남에 따라 센서의 전원 부족 및 사적인 정보의 유출이 심각한 문제로 여겨지고 있다. 이러한 문제들을 해결하기 위해 외부의 RF 신호로부터 전력을 수집하는 RF 에너지 하베스팅과 물리계층 보안 기술의 중요성이 점차 커지고 있다. 본 논문에서는 소스가 전송하는 신호로부터 에너지 하베스팅이 가능한 릴레이가 존재하는 무선 네트워크에서 정보 보안을 향상시키기 위한 시간 전환 기반 네트워크 아날로그 코딩 기법을 제안한다. 소스가 전송하는 신호를 도청하려는 도청자가 존재하는 2-hop 릴레이 네트워크를 모델링하고, 수학적 분석을 통해 최소 요구 보안 용량을 최대화 할 수 있는 최적의 시간 전환 비율을 찾았다. 다양한 환경에서 시뮬레이션을 통해 제안 방안이 기존 방안에 비해 최소 요구 보안 용량을 개선함을 보인다.

ABSTRACT

Recently, the energy shortage of sensors and the leakage of private information are considered as serious problems as the number of sensors is increasing due to the technological advance in Internet-of-Things. RF energy harvesting, in which sensors collect energy from external RF signals, and physical layer security become increasingly important to solve these problems. In this paper, we propose a time switching-based network analog coding for improving information security in wireless networks where the relay can harvest energy from source signals. We formulate 2-hop relay networks where an eavesdropper tries to overhear source signals, and find an optimal time switching ratio for maximizing the minimum required secrecy capacity using mathematical analysis. Through simulations under various environments, it is shown that the proposed scheme improves the minimum required secrecy capacity significantly, compared to the conventional scheme.

키워드 : 에너지 하베스팅, 시간 전환, 보안 용량, 물리계층 보안, 아날로그 네트워크 코딩

Key word : Energy Harvesting, Time Switching, Secrecy Capacity, Physical Layer Security, Analog Network Coding

Received 14 September 2017, **Revised** 21 September 2017, **Accepted** 23 October 2017

* **Corresponding Author** Hyun-Ho Choi(E-mail:hhchoi@hknu.ac.kr, Tel:+82-31-670-5297)
Department of Electrical, Electronic and Control Engineering, Hankyong National University, Anseong 17579, Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.11.2022 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

전 방향으로 방사하는 RF 신호를 수집하여 센서의 전력을 충전하는 RF 에너지 하베스팅(Energy harvesting)은 최근 센서의 전원 부족 문제를 해결할 수 있는 유망한 기술로 각광받고 있다[1-4]. [1]에서는 에너지 하베스팅이 가능한 무전원 릴레이(Relay)에서 효율적으로 정보와 전력을 동시에 전송(Simultaneous Wireless Information and Power Transfer, SWIPT)하기 위한 릴레이 프로토콜을 제안하였다. [2]에서는 시간 전환 기반의 Amplify-and-Forward (AF) 와 Decode-and-Forward (DF) 릴레이 프로토콜을 제안하고, 각각의 프로토콜의 달성 가능한 용량을 분석하였다. [3, 4]에서는 채널 추정 오차가 존재하는 에너지 하베스팅 네트워크에서 SWIPT를 위한 저복잡도 파워 할당 및 분할 알고리즘을 제안하였다. 뿐만 아니라, 사물인터넷(Internet-of-Things) 기술의 발달로 인해 사용되는 센서의 수가 늘어남에 따라, 정보 보안이 중요한 이슈로 떠오르고 있다 [5-8]. [6]에서는 다수의 도청자(Eavesdropper)가 존재하는 환경에서 정보 보안 제약 조건을 만족시키기 위한 최적의 릴레이 선택 방안을 제안하였다. [7]에서는 셀룰러 시스템과 Device-to-device (D2D) 시스템이 공존하는 이기종 네트워크 환경에서 셀룰러 시스템의 통신 보안을 보장해 주기 위한 D2D 시스템의 파워 조절 방안을 제안하였다. [8]에서는 에너지 하베스팅 네트워크에서 물리계층 보안을 향상시키기 위한 파워 분할 기반의 아날로그 네트워크 코딩 기법을 제안하였다. 하지만 정보 보안을 향상시키기 위한 시간 전환 기반의 아날로그 네트워크 코딩은 구현이 간단하여 활용도가 높음에도 불구하고, 이에 대한 기존 연구는 존재하지 않는다.

본 논문에서는 에너지 하베스팅이 가능한 릴레이가 존재하는 무선 네트워크 환경에서 물리계층 보안(Physical layer security) 문제를 다루고자 한다. 양쪽에 위치한 두 소스(Source)로부터 신호가 전송되는 상황에서, 릴레이는 αT의 시간동안 에너지를 하베스팅하며, $(1-\alpha)T/2$의 시간동안 신호를 수신한다. 또한, 릴레이는 하베스팅한 에너지를 이용하여 $(1-\alpha)T/2$의 시간동안 수신한 신호를 증폭하여 두 소스에게 재전송한다. 이때, 주변의 도청자는 릴레이가 전송한 신호를 도청할 수 있다. 이러한 상황에서 도청자에게 도청을 당하지 않고 두 소스가 각자의 신호를 안정적으로 주고받을 수 있도록, 최저 요구 보안 용량 (Minimum required secrecy capacity)을 최대화 할 수 있는 최적의 시간 전환 기반 네트워크 아날로그 코딩(Time Switching-based Analog Network Coding, TS-ANC)을 제안한다. 또한, 다양한 시뮬레이션 환경에서 일정한 α를 사용하는 기존 방안과의 비교를 통해 제안 방안의 우수성을 검증한다.

Ⅱ. 시스템 모델

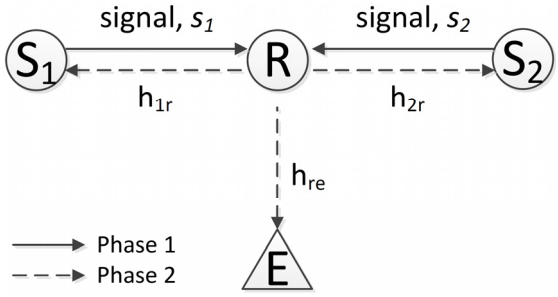

Fig. 1 System model of wireless-powered two-way relay networks

본 논문에서는 그림 1에서처럼 소스 1, 소스 2, 릴레이, 도청자가 존재하는 2-hop 기반의 무선 충전이 가능한 양방향 릴레이 네트워크를 고려한다. 소스1-릴레이, 소스2-릴레이, 릴레이-도청자 간의 채널은 각각 h_{1r}, h_{2r}, h_{re}로 정의하며, independent and identically distributed (i.i.d.) 플랫 페이딩 채널이라고 가정한다 [1-4]. 또한, 소스1-소스2, 소스1-도청자, and 소스2-도청자 간의 직접적인 무선 링크는 없으며, 각 노드의 수신부에는 $n \sim CN(0,\sigma^2)$의 동일한 Additive White Gaussian Noise(AWGN)이 존재한다고 가정한다 [6].

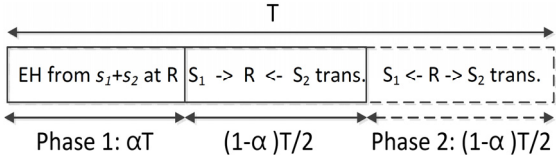

Fig. 2 TS-ANC protocol

그림 2는 본 논문에서 고려하고 있는 TS-ANC 프로토콜을 보여준다. 전체 블록 시간 T는 2단계로 이루어져 있으며, 첫 번째 단계는 릴레이에서 에너지 하베스팅을 위한 부분과 데이터 수신을 위한 부분으로 나뉜다. 예를 들어 첫 번째 단계에서 두 소스가 릴레이에게 각각 신호 s_1과 s_2를 전송하면, 릴레이는 αT의 시간동안 에너지를 하베스팅하여 전원을 충전하고, $(1-\alpha)T/2$의 시간동안 신호를 수신한다 [1, 2]. 나머지 $(1-\alpha)T/2$의 시간에 해당하는 두 번째 단계에서 릴레이는 하베스팅 한 에너지를 이용한 AF 기법을 통해 두 소스에게 다시 신호를 재전송한다. 릴레이가 전송한 신호는 도청자에게도 전달되어 도청이 가능하다.

첫 번째 단계에서 릴레이가 수신한 신호 y_r은 다음과 같다.

$$y_r = \sqrt{P_1}\,h_{1r}s_1 + \sqrt{P_2}\,h_{2r}s_2 + n. \tag{1}$$

수식 (1)에서 P_1과 P_2는 각각 소스 1과 2의 전송 파워이며, 신호 s_1과 s_2는 $E[|s_1|^2] = E[|s_2|^2] = 1$의 정규화된 파워를 갖는다. 또한, 릴레이가 하베스팅한 에너지는 다음과 같다.

$$E_h = T\eta\alpha(P_1|h_{1r}|^2 + P_2|h_{2r}|^2) = T\eta\alpha E_r. \tag{2}$$

수식 (2)에서 η는 에너지 변환 효율을 나타낸다.

두 번째 단계에서 릴레이는 하베스팅한 에너지 E_h를 이용하여 수신한 신호를 증폭하여 재전송한다. 여기서 릴레이가 전송에 사용하는 파워 P_r은 다음과 같이 표현된다.

$$P_r = \frac{E_h}{(1-\alpha)T/2} = \frac{2\eta\alpha E_r}{1-\alpha}. \tag{3}$$

또한, 릴레이가 전송하는 신호 x_r은 다음과 같다.

$$x_r = \frac{\sqrt{P_r}\,y_r}{\sqrt{E_r+\sigma^2}}. \tag{4}$$

소스 1이 릴레이로부터 수신한 신호 y_1는 아래와 같이 표현된다.

$$\begin{aligned} y_1 &= h_{1r}x_r + n \\ &= \frac{\sqrt{P_2P_r}\,h_{1r}h_{2r}s_2 + \sqrt{P_r}\,h_{1r}n}{\sqrt{E_r+\sigma^2}} \\ &\quad + \underbrace{\frac{\sqrt{P_1P_r}\,h_{1r}^2 s_1}{\sqrt{E_r+\sigma^2}}}_{self-cancellation} + n \\ &= \frac{\sqrt{P_2P_r}\,h_{1r}h_{2r}s_2 + \sqrt{P_r}\,h_{1r}n}{\sqrt{E_r+\sigma^2}} + n. \end{aligned} \tag{5}$$

또한, 소스 2가 릴레이로부터 수신한 신호 y_2는 아래와 같다.

$$\begin{aligned} y_2 &= h_{2r}x_r + n \\ &= \frac{\sqrt{P_1P_r}\,h_{1r}h_{2r}s_1 + \sqrt{P_r}\,h_{2r}n}{\sqrt{E_r+\sigma^2}} \\ &\quad + \underbrace{\frac{\sqrt{P_2P_r}\,h_{2r}^2 s_2}{\sqrt{E_r+\sigma^2}}}_{self-cancellation} + n \\ &= \frac{\sqrt{P_1P_r}\,h_{1r}h_{2r}s_1 + \sqrt{P_r}\,h_{2r}n}{\sqrt{E_r+\sigma^2}} + n. \end{aligned} \tag{6}$$

수식 (5)와 (6)에서 각각의 소스는 릴레이로부터 수신한 신호로부터 자신이 생성한 신호를 self-cancellation을 통해 제거함으로써, 다른 소스로부터 전송된 신호를 안정적으로 해석할 수 있다.

반면, 도청자가 릴레이로부터 도청한 신호 y_e는 아래와 같이 표현된다.

$$\begin{aligned} y_e &= h_{re}x_r + n \\ &= \frac{\sqrt{P_1P_r}\,h_{1r}h_{re}s_1 + \sqrt{P_2P_r}\,h_{2r}h_{re}s_2}{\sqrt{E_r+\sigma^2}} \\ &\quad + \frac{\sqrt{P_r}\,h_{re}n}{\sqrt{E_r+\sigma^2}} + n. \end{aligned} \tag{7}$$

수식 (7)에서 도청자가 특정 소스의 신호를 도청하려고 할 때 다른 소스의 신호가 간섭처럼 작용한다. 즉, 도청자가 소스의 신호를 해석하는 것을 방해하여, 결과적으로 소스 간의 통신 보안을 유지할 수 있다.

Ⅲ. 시간 전환 기반의 아날로그 네트워크 코딩 기법

수식 (5)와 (6)으로부터 소스 1과 2에서의 signal-to-noise ratio (SNR)은 다음의 수식 (8)과 (9)와 같이 표현할 수 있다.

$$\gamma_1 = \frac{\frac{2\eta\alpha E_r P_2 |h_{1r}|^2 |h_{2r}|^2}{(1-\alpha)(E_r+\sigma^2)}}{\frac{2\eta\alpha E_r |h_{1r}|^2 \sigma^2}{(1-\alpha)(E_r+\sigma^2)}+\sigma^2} = \frac{2\eta\alpha E_r P_2 |h_{1r}|^2 |h_{2r}|^2}{2\eta\alpha E_r |h_{1r}|^2 \sigma^2 + \sigma^2(1-\alpha)(E_r+\sigma^2)}. \quad (8)$$

$$\gamma_2 = \frac{\frac{2\eta\alpha E_r P_1 |h_{1r}|^2 |h_{2r}|^2}{(1-\alpha)(E_r+\sigma^2)}}{\frac{2\eta\alpha E_r |h_{2r}|^2 \sigma^2}{(1-\alpha)(E_r+\sigma^2)}+\sigma^2} = \frac{2\eta\alpha E_r P_1 |h_{1r}|^2 |h_{2r}|^2}{2\eta\alpha E_r |h_{2r}|^2 \sigma^2 + \sigma^2(1-\alpha)(E_r+\sigma^2)}. \quad (9)$$

또한, 수식 (7)로부터 도청자가 소스 1으로 전송되는 소스 2의 신호 s_2를 도청하려는 경우의 도청자에서의 SNR은 다음과 같이 표현된다.

$$\gamma_{e,1} = \frac{\frac{2\eta\alpha E_r P_2 |h_{2r}|^2 |h_{re}|^2}{(1-\alpha)(E_r+\sigma^2)}}{\frac{2\eta\alpha E_r P_1 |h_{1r}|^2 |h_{re}|^2 + 2\eta\alpha E_r |h_{re}|^2 \sigma^2}{(1-\alpha)(E_r+\sigma^2)}+\sigma^2} = \frac{2\eta\alpha E_r P_2 |h_{2r}|^2 |h_{re}|^2}{2\eta\alpha E_r |h_{re}|^2 (P_1 |h_{1r}|^2 + \sigma^2) + \sigma^2(1-\alpha)(E_r+\sigma^2)}. \quad (10)$$

반면, 도청자가 소스 2로 전송되는 소스 1의 신호 s_1을 도청하려는 경우의 도청자에서의 SNR은 다음과 같다.

$$\gamma_{e,2} = \frac{\frac{2\eta\alpha E_r P_1 |h_{1r}|^2 |h_{re}|^2}{(1-\alpha)(E_r+\sigma^2)}}{\frac{2\eta\alpha E_r P_2 |h_{2r}|^2 |h_{re}|^2 + 2\eta\alpha E_r |h_{re}|^2 \sigma^2}{(1-\alpha)(E_r+\sigma^2)}+\sigma^2} = \frac{2\eta\alpha E_r P_1 |h_{1r}|^2 |h_{re}|^2}{2\eta\alpha E_r |h_{re}|^2 (P_2 |h_{2r}|^2 + \sigma^2) + \sigma^2(1-\alpha)(E_r+\sigma^2)}. \quad (11)$$

수식 (8)과 (10)의 γ_1와 $\gamma_{e,1}$을 이용하여, 소스 1에서의 네트워크의 보안 용량은 소스 1에서의 통신 용량과 도청자에서의 통신 용량의 차로 표현할 수 있다 [6].

$$C_{S,1} = \left[\frac{(1-\alpha)T}{2}\{\log_2(1+\gamma_1) - \log_2(1+\gamma_{e,1})\}\right]^+. \quad (12)$$

수식 (12)에서 $[x]^+ = \max(0, x)$로 정의된다. 또한, 수식 (9)와 (11)의 γ_2와 $\gamma_{e,2}$로부터 소스 2에서의 네트워크의 보안 용량은 소스 2에서의 통신 용량과 도청자에서의 통신 용량의 차로 구할 수 있다.

$$C_{S,2} = \left[\frac{(1-\alpha)T}{2}\{\log_2(1+\gamma_2) - \log_2(1+\gamma_{e,2})\}\right]^+. \quad (13)$$

최종적으로 네트워크의 최소 요구 보안 용량은 C_{S1}과 C_{S2} 중 더 작은 값으로 결정 된다 [6].

$$C_S = \min(C_{S1}, C_{S2}). \quad (14)$$

수식 (14)의 C_S를 최대화 하는 최적의 α는 완결탐색 (Exhaustive search)를 통해 찾을 수 있다.

Ⅳ. 시뮬레이션 결과

시뮬레이션에서 $\eta = 0.5$ [9], $T = 1s$, $P_1 = P_2 = 23\,dBm$, $\sigma^2 = -174\,dBm/Hz$, $Bandwidth = 10MHz$, $Noise - figure = 9dB$, $m = 2.7$ [10]로 가정하였다. 또한, 평균 1을 갖는 exponentially distributed random variable을 이용하여 각각의 채널을 생성하였다 [3, 4]. 다양한 환경에서 C_S를 최대화 하는 최적의 α를 찾아 동작하는 제안 방안 (TS-ANC)과 특정 α 값을 사용하는 기존 방안의 성능을 비교하였다.

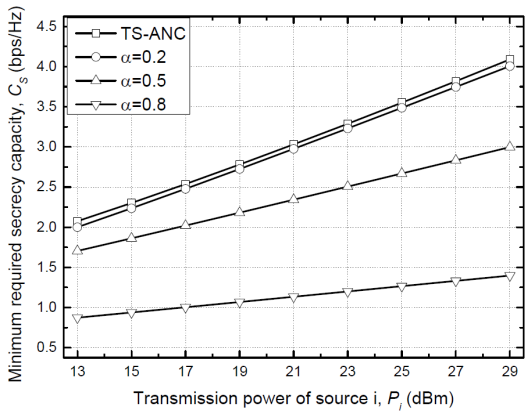

Fig. 3 Minimum required secrecy capacity vs. Transmission power of source i

그림 3은 각 소스의 전송 파워에 대한 최소 요구 보안 용량 성능을 보여준다. 여기서 $d_{12}=50m$, $d_{1r}=d_{2r}=d_{re}=25m$로 설정되었으며, d_{ij}는 노드 i와 j 사이의 거리를 의미한다. 각 소스가 큰 전송 파워를 사용할수록 릴레이는 안정적으로 신호를 수신할 수 있을 뿐만 아니라 많은 양의 에너지를 하베스팅 할 수 있다. 그러므로 P_i가 증가함에 따라 전 기법의 C_S가 향상된다.

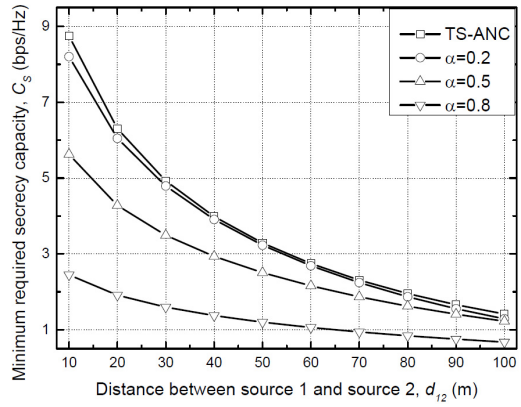

Fig. 4 Minimum required secrecy capacity vs. Distance between source 1 and source 2

그림 4는 소스 1과 소스 2 사이의 거리에 대한 최소 요구 보안 용량 성능을 보여준다. 여기서 $d_{1r}=d_{2r}=d_{12}/2$, $d_{re}=25m$로 설정하였다. d_{12}가 증가함에 따라, 첫 번째 단계 동안 양쪽 소스에서 릴레이로 전달되는 신호의 크기가 감소하게 된다. 또한, 두 번째 단계 동안 릴레이가 증폭하여 각각의 소스에 재전송해주는 신호의 크기도 감소하게 된다. 이에 따라 d_{12}가 증가할수록 전 기법의 C_S 성능은 저하된다.

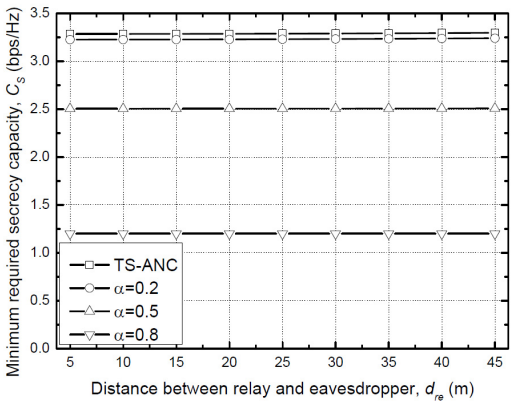

Fig. 5 Minimum required secrecy capacity vs. Distance between relay and eavesdropper

그림 5는 릴레이와 도청자 사이의 거리에 대한 최소 요구 보안 용량 성능을 보여준다. 여기서 $d_{12}=50m$, $d_{1r}=d_{2r}=25m$로 설정하였다. d_{re}가 커짐에 따라 도청자가 도청을 하기 어렵게 되어 전 기법의 C_S가 약간 향상된다. 하지만 d_{re}는 C_S 성능 변화에 큰 영향을 미치지 못함을 확인할 수 있다.

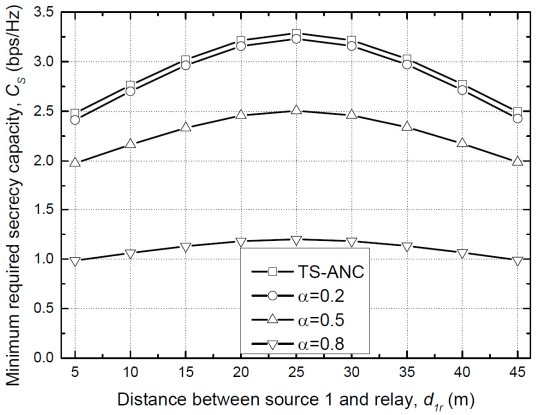

Fig. 6 Minimum required secrecy capacity vs. Distance between source 1 and relay

그림 6은 소스 1과 릴레이 사이의 거리에 대한 최소 요구 보안 용량을 보여준다. 여기서 $d_{12}=50m$, $d_{2r}=d_{12}-d_{1r}$, $d_{re}=25m$로 설정하였다. 릴레이가 d_{12}의 중앙에 위치할수록 전 기법의 C_S가 향상되고, 릴레이가 양 끝단에 위치할수록 전 기법의 C_S는 상대적으로 떨어지는 것을 확인할 수 있다. 또한, 그림 3-6에서 확인할 수 있듯이 제안 방안인 TS-ANC는 어떠한 채널 상황에서도 기존 방안에 비해 C_S를 향상시킨다.

Ⅴ. 결 론

본 논문에서는 양쪽에 위치한 두 소스가 전송하는 신호로부터 정보 송수신 및 에너지 하베스팅이 가능한 릴레이가 존재하는 무선 네트워크에서 최소 요구 보안 용량을 최대화하기 위한 TS-ANC를 제안하였다. 고려하는 네트워크 환경을 수식적으로 모델링하고, 수학적 분석을 통해 최소 요구 보안 용량을 최대화 할 수 있는 최적의 시간 전환 비율을 찾았다. 시뮬레이션을 통하여 제안 방안이 일정한 α를 사용하는 기존 방안에 비해 최소 요구 보안 용량을 개선하여, 도청이 가능한 환경에서도 안정적인 통신을 가능하게 함을 확인하였다.

ACKNOWLEDGMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2015 R1C1A1A01051747) and (2016R1C1B1016261)

REFERENCES

[1] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, “Relaying protocols for wireless energy harvesting and information processing,” *IEEE Transactions on Wireless Communication*, vol. 12, no. 7, pp. 3622-3636, July 2013.

[2] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, “Wireless-powered relays in cooperative communications: Time-switching relaying protocols and throughput analysis,” *IEEE Transactions on Communication*, vol. 63, no. 5, pp. 1607-1622, May 2015.

[3] K. Lee and J. Ko, “Power allocation and splitting algorithm with low-complexity for SWIPT in energy harvesting networks,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 20, no. 5, pp. 917-922, May 2016.

[4] K. Lee and J. Ko, “Power allocation and splitting algorithm for SWIPT in energy harvesting networks with channel estimation error,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 20, no. 7, pp. 1277-1282, July 2016.

[5] Jung Tae Kim, “Security and Privacy Issues in Internet of Things,” *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, vol. 6, no. 11, pp. 559-566, Nov. 2016.

[6] V. N. Q. Bao, N. L. Trung, and M. Debbah, “Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers,” *IEEE Transactions on Wireless Communication*, vol. 12, no. 12, pp. 6076-6085, Dec. 2013.

[7] K. Lee and J.-P. Hong, “Device-to-device communication power control technique for ensuring communication security of cellular system,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 21, no. 6, pp. 1100-1105, June 2017.

[8] K. Lee and H.-H. Choi, “Power splitting-based analog network coding for improving physical layer security in energy harvesting networks,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 21, no. 10, pp. 1849-1854, Oct. 2017.

[9] X. Lu, P.Wang, D. Niyato, D. I. Kim, and Z. Han, “Wireless networks with RF energy harvesting: A contemporary survey,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 757-789, May 2015.

[10] H. Meyr, M. Mseneclaey, and S. A. Fechtel, *Digital Communication Receivers, Synchronization, Channel Estimation, and Signal Processing*, J. G. Proakis, Ed. New York, NY: Wiley Series in Telecommunications and Signal Processing, 1998.

이기송(Kisong Lee)

2009년 KAIST 전기및전자공학과 석사
2013년 KAIST 전기및전자공학과 박사
2013년 ~ 2015년 ETRI 융합기술연구소 연구원
2015년 ~ 2017년 국립군산대학교 컴퓨터정보통신공학부 조교수
2017년 ~ 현재 충북대학교 정보통신공학부 조교수
※관심분야 : Wireless Power Transfer, Energy Harvesting Networks, Network Optimization 등

최현호(Hyun-Ho Choi)

2001년 KAIST 전기및전자공학과 공학사
2003년 KAIST 전기및전자공학과 공학석사
2007년 KAIST 전기및전자공학과 공학박사
2007년 ~ 2011년: 삼성종합기술원 전문연구원
2011년 ~ 현재: 국립한경대학교 전기전자제어공학과 부교수
※관심분야 : 매체접속제어, 분산자원관리, 저전력 프로토콜, 생체모방 알고리즘, 네트워크 최적화, 무선 에너지 하베스팅, 애드혹 네트워크, 차세대 이동통신 시스템 등