JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 10 : 1849~1854 Oct. 2017

에너지 하베스팅 네트워크에서 물리계층 보안을 향상시키기 위한 파워 분할 기반의 아날로그 네트워크 코딩

이기송[1] · 최현호[2*]

Power Splitting-based Analog Network Coding for Improving Physical Layer Security 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

외부의 RF 신호로부터 전력을 수집하는 RF 에너지 하베스팅은 무선 센서의 전원 부족 문제를 해결하는 기술로써 최근 큰 관심을 받고 있다. 뿐만 아니라, 사물 인터넷의 구현을 위해서는 센서 간의 보안 통신을 보장하는 것 역시 중요하다. 본 논문에서는 두 source로부터 전송되는 신호로부터 에너지 하베스팅이 가능한 relay가 존재하는 2-hop 네트워크에서 물리계층 보안을 최대화하기 위한 파워 분할 기반 네트워크 아날로그 코딩을 제안한다. 두 source, relay, eavesdropper가 존재하는 시스템을 수학적으로 모델링하고, exhaustive search를 통해 최소 요구 보안 용량을 최대화할 수 있는 최적의 파워 분할 비율을 찾았다. 다양한 환경에서 시뮬레이션을 통해 제안 방안은 기존 방안에 비해 eavesdropper에서의 도청을 막아 최소 요구 보안 용량을 개선함을 보인다.

ABSTRACT

Recently, RF energy harvesting, in which energy is collected from the external RF signals, is considered as a promising technology to resolve the energy shortage problem of wireless sensors. In addition, it is important to guarantee secure communication between sensors for implementing Internet-of-Things. In this paper, we propose a power splitting-based network analog coding for maximizing a physical layer security in 2-hop networks where the wireless-powered relay can harvest energy from the signals transmitted by two sources. We formulate systems where two sources, relay, and eavesdropper exist, and find an optimal power splitting ratio for maximizing the minimum required secrecy capacity using an exhaustive search. Through simulations under various environments, it is demonstrated that the proposed scheme improves the minimum required secrecy capacity by preventing the eavesdropper from overhearing source signals, compared to the conventional scheme.

키워드 : 에너지 하베스팅, 파워 분할, 보안 용량, 물리계층 보안, 아날로그 네트워크 코딩

Key word : Energy Harvesting, Power Splitting, Secrecy Capacity, Physical Layer Security, Analog Network Coding

Received 01 June 2017, **Revised** 15 June 2017, **Accepted** 21 June 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.2017.21.10.1849 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최근 무선 센서의 전원 부족 문제를 해결하기 위한 기술에 대한 요구가 커짐에 따라, 기존의 버려지는 RF 신호로부터 전력을 수집하여 센서의 전력을 충전하는 RF 에너지 하베스팅 (Energy harvesting) 기술에 대한 연구가 활발히 진행되고 있다[1-4]. [1, 2]에서는 정보와 전력을 동시에 전송(Simultaneous Wireless Information and Power Transfer, SWIPT)하기 위한 시간 전환 기법과 파워 분할 기법을 각각 제안하였다. [3]에서는 에너지 하베스팅이 가능한 relay에서 효율적인 SWIPT를 위한 relay 프로토콜을 제안하였다. [4]에서는 채널 추정이 불완전한 환경에서 SWIPT를 최적화하기 위한 파워 할당 및 분할 기법을 제안하였다. 뿐만 아니라, 사물인터넷 (Internet-of-Things) 기술이 발달함에 따라, 정보의 유출 없이 승인된 사용자 사이에서만 정보가 공유될 수 있도록 정보 보안이 중요한 이슈로 떠오르고 있다[5,6]. [5]에서는 다수의 eavesdropper가 존재하는 환경에서 정보 보안 요건을 만족시키기 위한 relay 선택 방안을 제안하였다. [6]에서는 양방향 relay 네트워크 환경에서 협력적 jamming이 있을 때와 없을 때 각각의 보안 용량을 최대화하기 위한 자원할당 방안을 제안하였다.

본 논문에서는, 무전원 relay가 존재하는 2-hop 네트워크 환경에서 물리계층 보안(Physical layer security)을 향상 시키고자 한다. Relay는 양쪽에 위치한 두 source로부터 전송되는 신호 중 ρ의 파워를 이용하여 에너지를 하베스팅하며, $1-\rho$의 파워를 이용하여 신호를 수신한다. 또한, relay는 충전된 전력을 이용하여 두 source에게 신호를 다시 전송한다. 이때, relay가 전송한 신호는 주변의 eavesdropper에게도 전달되어 도청이 가능하다. 이러한 환경에서 각각의 source에서 전달된 신호가 eavesdropper에게 도청 당하지 않고 안전하게 다른 source에 전달될 수 있도록, 최저 요구 보안 용량(Minimum required secrecy capacity)을 최대화 할 수 있는 최적의 파워 분할 기반 네트워크 아날로그 코딩(Power Splitting-based Analog Network Coding, PS-ANC)을 제안한다. 또한, 다양한 시뮬레이션 환경에서 일정한 ρ를 사용하는 기존 방안과의 비교를 통해 제안 방안의 우수성을 검증한다.

Ⅱ. 시스템 모델

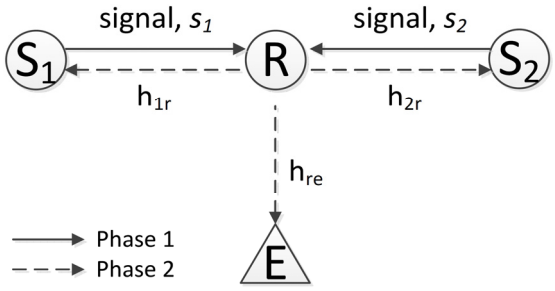


Fig. 1 System model of two-way relay networks

본 논문에서는 그림 1에서처럼 source 1, source 2, relay, eavesdropper가 존재하는 2-hop 네트워크를 고려한다. source1-to-relay, source2-to-relay, relay-to-eavesdropper 간의 채널은 independent and identically distributed (i.i.d.) 플랫 페이딩 채널이며, 각각 h_{1r}, h_{2r}, h_{re}로 정의한다[1,2]. 또한, source1-to-source2, source1-to-eavesdropper, and source2-to-eavesdropper 간의 직접적인 link는 없으며, 각 노드에서는 $n \sim CN(0,\sigma^2)$의 동일한 Additive White Gaussian Noise(AWGN)이 존재한다고 가정한다[3].

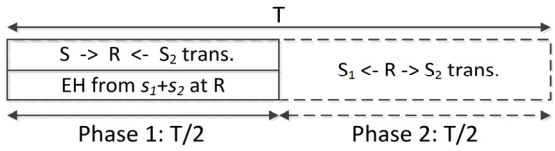


Fig. 2 PS-ANC protocol

그림 2에서처럼 본 논문에서 고려하고 있는 PS-ANC 프로토콜은 전체 블록 시간 T 동안 2-phase로 이루어져 있다. 먼저, T/2의 시간에 해당하는 phase 1에서는 두 source가 relay에게 각각 신호 s_1과 s_2를 전송한다. 여기서 relay는 무전원 노드로써, 두 source로부터 받은 신호 중 ρ 에 해당하는 파워를 에너지 하베스팅하여 전원을 충전하고, $1-\rho$에 해당하는 파워를 이용하여 신호를 수신한다[2-4]. 나머지 T/2의 시간에 해당하는 phase 2에서 relay는 phase 1에서 충전한 파워를 이용한 Amplify-and-Forward (AF) 기법을 통해 두 source에게 신호를 전송한다. 또한, relay로부터 전달된 신호는 eavesdropper에게도 전송 되어 도청이 가능한 상황

이다. Phase 1에서 relay가 수신하는 신호 y_r은 다음과 같다.

$$y_r = \sqrt{(1-\rho)P_1}\,h_{1r}s_1 + \sqrt{(1-\rho)P_2}\,h_{2r}s_2 + n. \quad (1)$$

수식 (1)에서 P_1과 P_2는 각각의 source의 전송 파워이며, 신호 s_1과 s_2는 $E[|s_1|^2] = E[|s_2|^2] = 1$의 정규화 된 파워를 갖는다. 반면에 relay에서 하베스팅된 에너지는 다음과 같다.

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

수식 (2)에서 η는 에너지 변환 효율이다.

Phase 2에서 relay는 E_h를 이용하여 수신 신호를 증폭한 후 전송한다. Relay에서 전송되는 신호 x_r은 다음과 같다.

$$x_r = \frac{\sqrt{P_r}\,y_r}{\sqrt{(1-\rho)E_r + \sigma^2}}. \quad (3)$$

또한, relay가 전송에 사용하는 파워 P_r은 수식 (4)와 같이 표현할 수 있다.

$$P_r = \frac{E_h}{T/2} = \eta\rho E_r. \quad (4)$$

Source 1에서 수신되는 신호 y_1는 아래와 같이 표현된다.

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

또한, source 2에서 수신되는 신호 y_2는 아래와 같다.

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

수식 (5)와 (6)에서 각각의 source는 자신이 생성한 신호를 self-cancellation을 통해 제거함으로써, 다른 source로부터 전송된 신호를 안정적으로 수신할 수 있다. 반면, eavesdropper에서 도청되는 신호 y_e는 아래와 같이 표현된다.

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

수식 (7)에서 eavesdropper가 특정 source의 신호를 해석하려고 할 때 다른 source의 신호가 간섭처럼 작용하여 eavesdropper의 도청을 방해한다. 이를 통해 source 간의 통신 보안을 유지할 수 있다.

Ⅲ. 파워 분할 기반의 아날로그 네트워크 코딩 기법

수식 (5)와 (6)으로부터 각각의 source에서의 signal-to-noise ratio (SNR)은 다음과 같이 표현된다.

$$\begin{aligned} \gamma_1 &= \frac{\dfrac{(1-\rho)P_2P_r|h_{1r}|^2|h_{2r}|^2}{(1-\rho)E_r + \sigma^2}}{\dfrac{P_r|h_{1r}|^2\sigma^2}{(1-\rho)E_r + \sigma^2} + \sigma^2} \\ &= \frac{\eta\rho(1-\rho)E_rP_2|h_{1r}|^2|h_{2r}|^2}{\eta\rho E_r|h_{1r}|^2\sigma^2 + \sigma^2((1-\rho)E_r + \sigma^2)}. \end{aligned} \quad (8)$$

$$\begin{aligned} \gamma_2 &= \frac{\dfrac{(1-\rho)P_1P_r|h_{1r}|^2|h_{2r}|^2}{(1-\rho)E_r + \sigma^2}}{\dfrac{P_r|h_{2r}|^2\sigma^2}{(1-\rho)E_r + \sigma^2} + \sigma^2} \\ &= \frac{\eta\rho(1-\rho)E_rP_1|h_{1r}|^2|h_{2r}|^2}{\eta\rho E_r|h_{2r}|^2\sigma^2 + \sigma^2((1-\rho)E_r + \sigma^2)}. \end{aligned} \quad (9)$$

또한, 수식 (7)로부터 eavesdropper가 source 1으로 전송되는 source 2의 신호 s_2를 도청하는 경우의 eavesdropper에서의 SNR은 다음과 같이 표현된다.

$$\gamma_{e,1}=\frac{\frac{(1-\rho)P_2P_r|h_{2r}|^2|h_{re}|^2}{(1-\rho)E_r+\sigma^2}}{\frac{(1-\rho)P_1P_r|h_{1r}|^2|h_{re}|^2+P_r|h_{re}|^2\sigma^2}{(1-\rho)E_r+\sigma^2}+\sigma^2}=\frac{\eta\rho(1-\rho)E_rP_2|h_{2r}|^2|h_{re}|^2}{\eta\rho E_r|h_{re}|^2((1-\rho)P_1|h_{1r}|^2+\sigma^2)+\sigma^2((1-\rho)E_r+\sigma^2)}. \quad (10)$$

반면, eavesdropper가 source 2로 전송되는 source 1의 신호 s_1을 도청하는 경우의 eavesdropper에서의 SNR은 다음과 같다.

$$\gamma_{e,2}=\frac{\frac{(1-\rho)P_1P_r|h_{1r}|^2|h_{re}|^2}{(1-\rho)E_r+\sigma^2}}{\frac{(1-\rho)P_2P_r|h_{2r}|^2|h_{re}|^2+P_r|h_{re}|^2\sigma^2}{(1-\rho)E_r+\sigma^2}+\sigma^2}=\frac{\eta\rho(1-\rho)E_rP_1|h_{1r}|^2|h_{re}|^2}{\eta\rho E_r|h_{re}|^2((1-\rho)P_2|h_{2r}|^2+\sigma^2)+\sigma^2((1-\rho)E_r+\sigma^2)}. \quad (11)$$

γ_1와 $\gamma_{e,1}$로부터 source 1에서의 네트워크의 보안 용량은 다음과 같이 source 1에서의 통신 용량과 eavesdropper에서의 통신 용량의 차로 구할 수 있다 [5].

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

또한, γ_2와 $\gamma_{e,2}$로부터 source 2에서의 네트워크의 보안 용량은 다음과 같이 source 2에서의 통신 용량과 eavesdropper에서의 통신 용량의 차로 구할 수 있다.

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

최종적으로 네트워크의 최소 요구 보안 용량은 $C_{S,1}$과 $C_{S,2}$ 중 더 작은 값으로 결정될 수 있다 [5].

$$C_S=\min(C_{S,1},C_{S,2}). \quad (14)$$

수식 (14)의 C_S를 최대화 하는 ρ는 exhaustive search를 통해 찾을 수 있다.

Ⅳ. 시뮬레이션 결과

시뮬레이션에서는 $\eta=0.5$ [7], $T=1s$, $P_1=P_2=23dBm$, $\sigma^2=-174dBm/Hz$, $Bandwidth=10MHz$, $Noise-figure=9dB$, m (Path-loss exponent) =2.7 [8]로 가정하였다. 또한 채널은 평균 1을 갖는 exponentially distributed random variable을 이용하여 생성하였다[1-3]. 또한, 제안 방안인 C_S를 최대화 하는 ρ를 찾아 동작하는 PS-ANC와 특정 ρ값을 사용하는 기존 방안의 성능을 비교하였다.

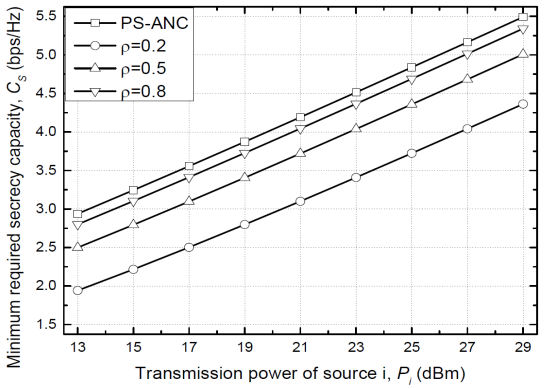


Fig. 3 Minimum required secrecy capacity vs. Transmission power of source i

그림 3은 source i의 전송 파워에 대한 최소 요구 보안 용량을 보여준다. 여기서 $d_{12}=50m$, $d_{1r}=d_{2r}=d_{re}=25m$로 설정되었으며, d_{ij}는 노드 i와 j 사이의 거리를 의미한다. P_i가 늘어남에 따라 relay는 source로부터 많은 양의 에너지를 하베스팅 할 수 있고, source로부터 전송되는 신호의 수신도 좋아지기 때문에 전 기법의 C_S가 향상된다.

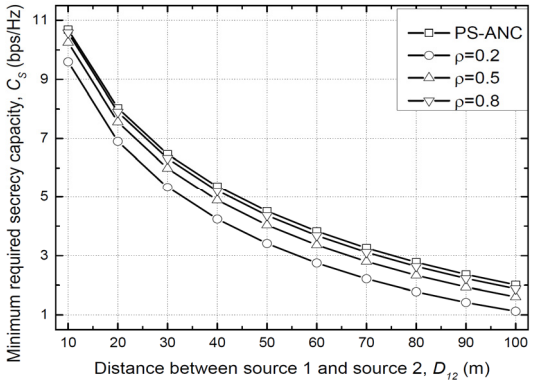


Fig. 4 Minimum required secrecy capacity vs. Distance between source 1 and source 2

그림 4는 source 1과 source 2 사이의 거리에 대한 최소 요구 보안 용량을 보여준다.

여기서 $d_{1r} = d_{2r} = d_{12}/2$, $d_{re} = 25m$로 설정하였다. d_{re}가 고정되어 있는 상황에서 d_{12}가 커지게 되면, 각각의 source가 주고받는 신호의 세기 감소하게 되어 전 기법의 C_S가 떨어지게 된다.

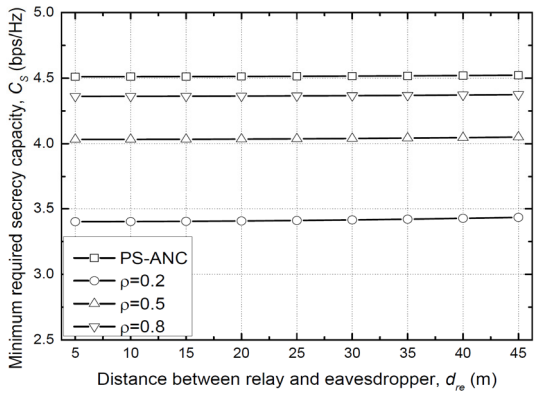


Fig. 5 Minimum required secrecy capacity vs. Distance between relay and eavesdropper

그림 5는 relay와 eavesdropper 사이의 거리에 대한 최소 요구 보안 용량을 보여준다. 여기서 $d_{12} = 50m$, $d_{1r} = d_{2r} = 25m$로 설정하였다. d_{re}가 커짐에 따라 eavesdropper로 전달되는 신호의 세기가 약해지고, 이에 따라 도청을 하기 어렵게 되어 전 기법의 C_S가 향상된다.

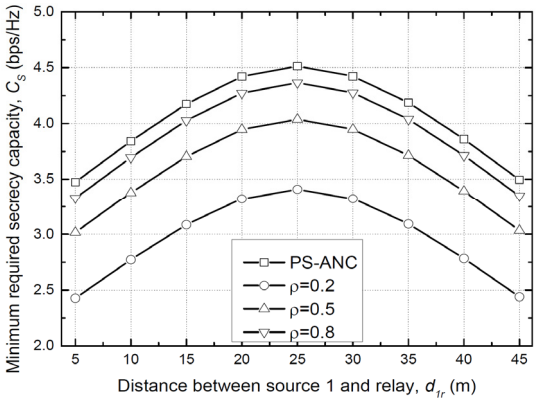


Fig. 6 Minimum required secrecy capacity vs. Distance between source 1 and relay

그림 6은 source 1과 relay 사이의 거리에 대한 최소 요구 보안 용량을 보여준다. 여기서 $d_{12} = 50m$, $d_{2r} = d_{12} - d_{1r}$, $d_{re} = 25m$로 설정하였다. Relay가 d_{12}의 중앙에 위치하면, 각각의 source로부터 비슷한 세기의 신호를 수신하고 이를 다시 증폭하여 전송한다. 이 경우 각각의 source는 자신이 생성한 신호를 제거하여 다른 source로부터의 전송된 신호를 안정적으로 수신 가능하다. 하지만 eavesdropper의 경우는 도청하려는 신호와 간섭 신호가 비슷한 세기로 존재하기 때문에 도청을 하기 어렵게 된다.

반면, relay가 특정 source에 가깝게 위치하면, 각각의 source로부터 수신하는 신호의 세기에 차이가 발생하게 된다. 이 경우 도청하고자 하는 신호의 세기는 커지고 간섭 신호의 세기는 작아지게 되어, eavesdropper가 큰 세기의 신호를 도청하기 유리해진다. 그러므로 relay가 d_{12}의 중앙에 위치하는 경우는 전 기법의 C_S가 향상되고, relay가 양 끝단에 위치할수록 전 기법의 C_S는 떨어지게 된다. 또한, 그림 3-6에서 확인할 수 있듯이 제안 방안인 PS-ANC는 기존 방안에 비해 전 구간에 대해서 C_S를 향상시킨다.

Ⅴ. 결 론

본 논문에서는 두 source로부터 전달되는 신호로부터 에너지 하베스팅이 가능한 relay가 존재하는 2-hop 네트워크에서 최소 요구 보안 용량을 최대화하기 위한 PS-ANC를 제안하였다. 두 source, relay, eavesdropper 등 4개의 노드가 존재하는 네트워크 환경을 수식적으로 모델링하고, exhaustive search를 통해 최소 요구 보안 용량을 최대화 할 수 있는 최적의 파워 분할 비율을 찾았다. 시뮬레이션을 통하여 제안 방안이 일정 비율의 ρ를 사용하는 기존 방안에 비해 최소 요구 보안 용량을 개선하여, source간의 통신 보안성을 향상시킬 수 있음을 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] L. Liu, R. Zhang, and K. Chua, "Wireless information transfer with opportunistic energy harvesting," *IEEE Transactions on Wireless Communication*, vol. 12, no. 1, pp. 288-300, Jan. 2013.

[2] L. Liu, R. Zhang, and K. Chua, "Wireless information and power transfer: a dynamic power splitting approach," *IEEE Transactions on Communication*, vol. 61, no. 9, pp. 3990-4001, Sep. 2013.

[3] 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.

[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] 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.

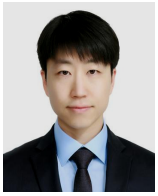
[6] H. Zhang, H. Xing, J. Cheng, A. Nallanathan, and V. C. M. Leung "Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1714-1725, Oct. 2016.

[7] 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.

[8] 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