Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 14(3): 171-176, Sep. 2016 **Regular paper**

Physical Layer Secrecy Performance of RF–EH Networks with Multiple Eavesdroppers

Tien-Vu Truong [1*], Nhan-Van Vo[1], Dac-Binh Ha[2], and Duc-Dung Tran[2], *Member, KIICE*

[1]Information Technology Faculty, Duy Tan University, Da Nang 550000, Vietnam
[2]Electrical & Electronics Engineering Faculty, Duy Tan University, Da Nang 550000, Vietnam

Abstract

In this study, we investigate the physical layer secrecy performance of RF energy harvesting (EH) networks over Rayleigh fading channels. The RF–EH system considered here consists of one power transfer station, one source, one destination, and multiple passive eavesdroppers. The source harvests energy from the power transfer station and transmits the information to the destination by using a time switching-based relaying protocol. The eavesdroppers try to extract the transmitted information without an active attack. By using the statistical characteristics of the signal-to-noise ratio (SNR), the exact closed-form expressions of the existence probability of the secrecy capacity and the secrecy outage probability are derived. Further, we analyze the secrecy performance of the system with respect to various system parameters, such as the location of the system elements and the number of eavesdroppers. Finally, the equivalent Monte Carlo simulation results are provided to confirm the correctness of our calculations.

Index Terms: Existence probability of secrecy capacity, RF–EH networks, Secrecy capacity, Secrecy outage probability

I. INTRODUCTION

The RF energy harvesting (EH) technique has recently been used as an alternative method to power next-generation wireless networks [1]. This technique is considered a potential solution to the energy constraints of wireless networks, such as the limited lifetime of wireless sensor networks that significantly constrains network performance. In RF–EH networks, wireless devices can harvest energy from an RF signal and convert it into electricity for information processing and transmission. Recently, this technique has received a considerable amount of attention by both academia and industry [2-5]. However, the open nature of this environment has led to certain security problems; for instance, eavesdroppers can now harvest energy and simultaneously wiretap information. To solve this problem, physical layer security is required to guarantee a perfectly secure information transmission by exploiting the physical characteristics of a wireless communication channel on the basis of the information theory [6]. Accordingly, the authors of [7-10] have investigated physical layer secrecy in RF–EH networks. The authors of [7] have proposed a solution for optimizing transmit beamforming and power allocation by applying the technique of semi-definite relaxation (SDN) in a multiuser multiple-input single-output (MISO) simultaneous wireless information and power transfer (SWIPT) system. A multiple antenna technique has also been exploited to enhance the secrecy performance [8, 9]. In particular, these researchers have investigated the wireless information and power transfer (WIPT) tradeoffs on the basis of two typical multi-antenna

Received 29 July 2016, **Revised** 31 July 2016, **Accepted** 08 August 2016
***Corresponding Author** Tien-Vu Truong (E-mail: truongtienvu@dtu.edu, Tel: +84-914083188)
Information Technology Faculty, Duy Tan University, Da Nang 550000, Vietnam.

Open Access **http://dx.doi.org/10.6109/jicce.2016.14.3.171** print ISSN: 2234-8255 online ISSN: 2234-8883

techniques, namely a limited feedback multi-antenna technique for short-distance transfer and a large-scale multiple-input multiple-output (LS-MIMO, also known as massive MIMO) technique for long-distance transfer. In [10], the researchers investigated the impact of power transfer selection on the physical layer secrecy performance of RF–EH networks; here, the best power transfer station was selected among multiple power transfer stations in EH networks to increase the harvested power of the energy-constrained users.

In the present study, we focus on analyzing the secrecy performance of an RF–EH network with one power transfer station, one energy-constrained information source, one destination, and multiple passive eavesdroppers over Rayleigh fading channels. The main contributions of this paper are as follows:

- The exact closed-form expressions of the joint cumulative distribution function (CDF) are derived for further calculations.
- For evaluating the secrecy performance of the considered system, the exact closed-form expressions of the existence probability secrecy capacity and the secrecy outage probability are derived by using the statistical characteristics of the signal-to-noise ratio (SNR).
- Further, the impact of some parameters, such as the number of eavesdroppers and the location of the energy receiver, information receiver, and eavesdroppers, on the secrecy performance is analyzed.

The rest of this paper is organized as follows. Section II presents the system and the channel model. The physical layer secrecy performance of the considered system is analyzed in Section III. Section IV presents the numerical results and some discussion. Finally, we conclude this work in Section V.

II. SYSTEM AND CHANNEL MODEL

We consider a wireless network with RF–EH as illustrated in Fig. 1. The system consists of one power transfer station denoted by P, one energy-constrained source denoted by S, and one destination denoted by Din the presence of N passive eavesdroppers. The source S harvests energy from the power transfer station P and transmits the information to the destination by using a time switching-based relay (TSR) protocol [6]. We assume that all the channels undergo Rayleigh fading and that all transmitters and receivers are equipped with a single antenna.

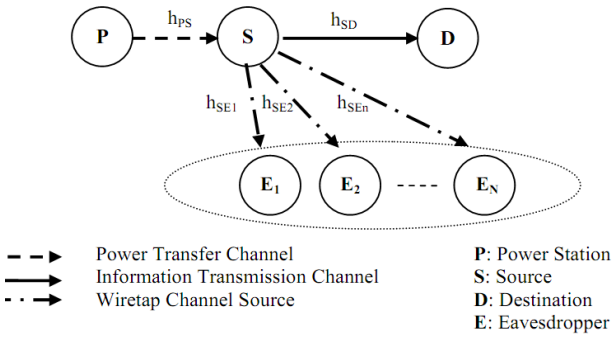

Fig. 1. System and channel model.

First, the source S harvests energy from the power transfer station P in the duration of αT as follows:

$$P_S = \frac{E_h}{(1-\alpha)T} = \frac{\eta\alpha P_0 |h_{PS}|^2}{(1-\alpha)d_S^\theta} = \frac{\eta\alpha P_0}{(1-\alpha)}\gamma_S , \quad (1)$$

where $[0 < \eta < 1]$ denotes the energy conversion efficiency, which depends on the rectification process and the energy harvesting circuitry; P_0 represents the transmit power of the power station; T indicates the block time; α refers to a fraction of the block time, $0 < \alpha \le 1$; $|h_{PS}|^2$ stands for the channel power gain of the link from the power station to the source; d_S denotes the distance from P to S; θ represents the path loss exponent; and $\gamma_S = \frac{|h_{PS}|^2}{d_S^\theta}$.

In the remaining duration of $(1-\alpha)T$, the source transmits the signal $x(t)$ to the destination and the signal received at D is expressed as follows:

$$y(t) = \sqrt{\frac{P_S}{d_D^\theta}} h_{SD} x(t) + n_D , \quad (2)$$

where h_{SD} and d_D denote the channel coefficient and the distance from S to D, respectively. Further, n_D represents an additive white Gaussian noise, $n_D \in \mathcal{CN}(0, N_1)$.

The eavesdroppers try to extract the transmitted information at S without an active attack. The received signal at E_i can be expressed as follows:

$$z_i(t) = \sqrt{\frac{P_S}{d_{E_i}^\theta}} h_{SE_i} x(t) + n_{E_i}, 1 \le i \le N , \quad (3)$$

where h_{SE_i} and d_{E_i} denote the channel coefficient and the distance from S to E_i, respectively. Further, n_{E_i} represents an additive white Gaussian noise of the channel from S to E_i. Assume that all n_{E_i} are equal and $n_{E_i} \in \mathcal{CN}(0, N_2)$. For simplicity, we suppose $N_1 = N_2 = N_0$.

The instantaneous received SNR at the destination D is given as follows:

$$\gamma_{SD} = \frac{P_S |h_{SD}|^2}{d_D^\theta N_0} = a\gamma_S\gamma_D , \quad (4)$$

where $a = \frac{\eta\alpha P_0}{(1-\alpha)N_0}$ and $\gamma_D = \frac{|h_{SD}|^2}{d_D^\theta}$.

Similarly, the instantaneous received SNR per eavesdropper E_i is given as follows:

$$\gamma_{SE_i} = \frac{P_S |h_{SE_i}|^2}{d_{E_i}^\theta N_0} = a\gamma_S \gamma_{E_i}, \quad (5)$$

where $\gamma_{E_i} = \frac{|h_{SE_i}|^2}{d_{E_i}^\theta}$.

Since all channels follow a Rayleigh distribution, the probability density function (PDF) of a random variable (RV) $U = \{\gamma_S, \gamma_D, \gamma_{E_i}\}$ is as follows:

$$f_U(x) = \frac{1}{\lambda_U} e^{-\frac{x}{\lambda_U}}, \quad (6)$$

where $\lambda_U = \{\lambda_S, \lambda_D, \lambda_{E_i}\}$, $\lambda_S = \frac{\mathbb{E}\left[|h_{PS}|^2\right]}{d_S^\theta}$, $\lambda_D = \frac{\mathbb{E}\left[|h_{PS}|^2\right]}{d_D^\theta}$, $\lambda_{E_i} = \frac{\mathbb{E}\left[|h_{PS}|^2\right]}{d_{E_i}^\theta}$, and $\mathbb{E}(.)$ denotes an expectation operator.

The CDF of RV $U = \{\gamma_S, \gamma_D, \gamma_{E_i}\}$ is as follows:

$$F_U(x) = 1 - e^{-\frac{x}{\lambda}}. \quad (7)$$

The CDF of $V = \{\gamma_{SD}, \gamma_{SE_i}\}$ is calculated as follows:

$$F_V(x) = \int_0^\infty F_U\left(\frac{x}{az}\right) f_{\gamma S}(z)dz = 1 - 2\sqrt{\frac{x}{a\lambda_1\lambda_2}} K_1\left(\sqrt{\frac{x}{a\lambda_1\lambda_2}}\right), \quad (8)$$

where $U = \{\gamma_S, \gamma_D\}$ and $\lambda_{1,2} = \begin{cases} \{\lambda_S, \lambda_D\}, if V = \gamma_{SD} \\ \{\lambda_S, \lambda_{E_i}\}, if V = \gamma_{SE_i} \end{cases}$.

From the above result, we obtain the PDF of $V = \{\gamma_{SD}, \gamma_{SE_i}\}$ as follows:

$$f_V(x) = \frac{2}{a\lambda_1\lambda_2} K_0\left(\sqrt{\frac{x}{a\lambda_1\lambda_2}}\right). \quad (9)$$

III. PHYSICAL LAYER SECRECY PERFORMANCE ANALYSIS

A. Preliminaries

The instantaneous channel capacity of the S–D link can be expressed as follows:

$$C_{SD} = \log_2(1+\gamma_{SD}). \quad (10)$$

The instantaneous channel capacity of the S–E_i link is as follows:

$$C_{SE_i} = \log_2(1+\gamma_{SE_i}), 1 \le i \le N. \quad (11)$$

The instantaneous secrecy capacity of each E_i is given as follows:

$$C_{S_i} = \left[C_{SD} - C_{SE_i}\right]^+ = \begin{cases} \log_2\left(\frac{1+\gamma_{SD}}{1+\gamma_{SE_i}}\right), \gamma_{SD} > \gamma_{SE_i} \\ 0, \gamma_{SD} \le \gamma_{SE_i} \end{cases}. \quad (12)$$

LEMMA 1. Under Rayleigh fading, the joint CDF of γ_{SD} and γ_{SE_i} is given as follows:

$$F_{X,Y}(x,y) = 1 - uK_1(u) - vK_1(v) + tK_1(t). \quad (13)$$

Proof. See Appendix A.

B. Existence Probability of Secrecy Capacity

The existence probability of the secrecy capacity is an important measure useful for system designers to evaluate the secrecy performance of a wireless communication system. Assuming that the main channel and the eavesdropper channel are independent of each other, we can define the existence probability of the secrecy capacity as follows:

$$P_{CS} = \Pr(C_S > 0). \quad (14)$$

THEOREM 1. Under Rayleigh fading, the existence probability of secrecy capacity P_{CS_i} is given as follows:

$$P_{CS_i} = \frac{\lambda_D}{\lambda_D + \lambda_{E_i}}. \quad (15)$$

Proof. See Appendix B.

In a system with multiple eavesdroppers, the existence probability of the secrecy capacity is defined as follows:

$$P_{CS_i} = P\left(C_{S_i} > 0\right) = \Pr(C_{S_1} > 0, C_{S_2} > 0 \cdots C_{S_N} > 0)$$
$$= \prod_{i=1}^{N} P(C_{S_i} > 0) = \prod_{i=1}^{N} \frac{\lambda_D}{\lambda_D + \lambda_{E_i}} \quad . \tag{16}$$

C. Secrecy Outage Probability

Secrecy outage probability P_{out} is also an important performance metric generally used for characterizing the secrecy performance of a wireless communication system. It is defined as the probability that the instantaneous secrecy capacity C_S falls below a predetermined secrecy rate threshold $R > 0$ and can be expressed as follows:

$$P_{out} = P(C_S < R) \quad . \tag{17}$$

THEOREM 2. Under Rayleigh fading, the secrecy outage probability P_{out_i} is expressed as follows:

$$P_{out_i} = 1 - \frac{\lambda_D}{m\lambda_E 2^R + \lambda_D} bK_1(b) \quad , \tag{18}$$

where $b = 2\sqrt{\frac{(n+1)(2^R - 1)m}{a\lambda_S \lambda_D}}$.

Proof. See Appendix C.

In a system with multiple (K) eavesdroppers, the secrecy outage probability is calculated as follows:

$$P_{out} = P(C_S < R)$$
$$= 1 - \prod_{i=1}^{N} P(R \le C_{S_i})$$
$$= 1 - \prod_{i=1}^{N} \left[1 - P(C_{S_i} < R)\right]$$
$$= 1 - \prod_{i=1}^{N} \left[1 - \left(1 - \frac{\lambda_D}{2^R \lambda_{E_i} + \lambda_D} bK_1(b)\right)\right]$$
$$= 1 - \prod_{i=1}^{N} \left[\frac{\lambda_D}{2^R \lambda_{E_i} + \lambda_D} bK_1(b)\right] \quad . \tag{19}$$

IV. NUMERICAL RESULTS AND DISCUSSION

In this section, the numerical results in terms of the existence probability of the secrecy capacity and the secrecy outage probability are provided to analyze the system secrecy performance. Fig. 2 depicts the variation of P_{CS} with respect to d_D for different values of the number of eavesdroppers N. This figure shows that when N increases, P_{CS} decreases.

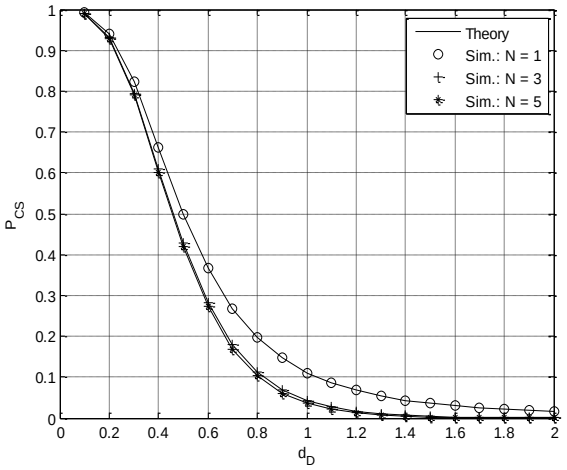

Fig. 2. Existence probability of secrecy capacity as a function of d_D for different values of N.

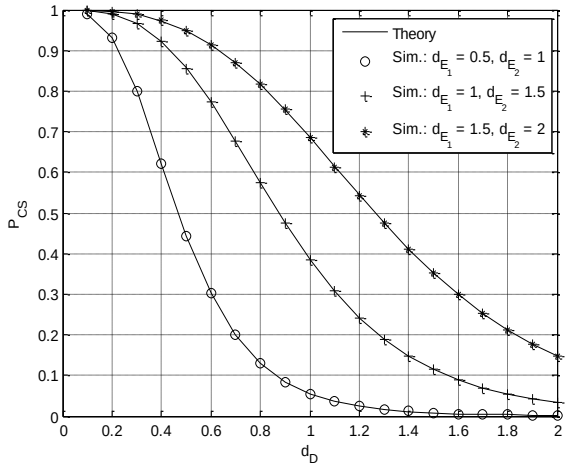

Fig. 3. Existence probability of secrecy capacity as a function of d_D for different values of d_E.

Fig. 3 depicts the variation of P_{CS} with respect to the distance from the source to the destination d_D for different values of the distance from the source to the eavesdropper d_E. It shows that P_{CS} increases when d_D decreases and d_E increases. This can be attributed to the fact that when d_D scales down and d_E scales up, the received signal at D is better than that at E. Thus, the capacity of a legal channel is larger than that of an illegal channel.

Fig. 4 shows that when the number of eavesdroppers N and the distance from the source to the destination d_D increases, the outage probability P_{out} increases.

Fig. 5 depicts the variation of P_{out} with respect to the distance from the source to the destination d_D for different values of the distance from the source to the eavesdropper d_E. It shows that the outage probability P_{out} increases when

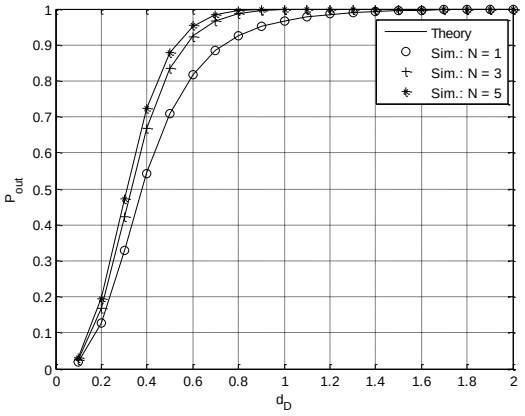

Fig. 4. Secrecy outage probability as a function of d_D for different values of *N*.

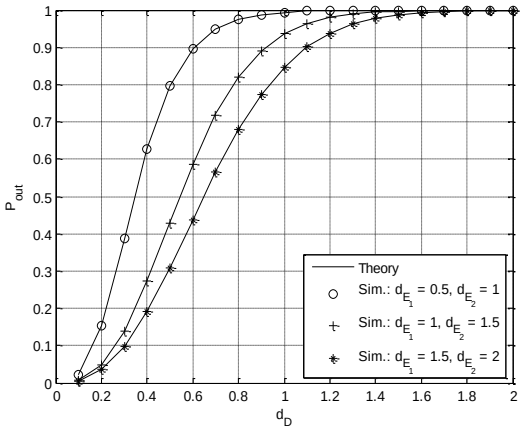

Fig. 5. Secrecy outage probability as a function of d_D for different values of d_E .

d_D increases and d_E decreases because the received signals at the eavesdroppers are better than those at the destination.

As can be clearly observed from all these figures, the good agreement between analytical and simulation results verifies the correctness of our analysis.

V. CONCLUSIONS

In this study, the secrecy performance of an RF–EH network with multiple eavesdroppers was investigated. The exact closed-form expressions of the secrecy existence probability and the outage probability of the considered system were derived. On the basis of these expressions, we evaluated the impact of some parameters on the secrecy performance. A Monte Carlo simulation verified the correctness of the derived mathematical analysis. Our numerical results indicated that the secrecy performance of the considered system depended on the location of the energy receiver as well as that of the eavesdroppers.

APPENDIX

Appendix A

$$\begin{aligned} F_{X,Y}(x,y) &= \lambda_S - \int_0^\infty e^{-\frac{x}{a\lambda_D^2}-\frac{z}{\lambda_S}} dz \\ &\quad - \int_0^\infty e^{-\frac{y}{a\lambda_{E_i}^2}-\frac{z}{\lambda_S}} dz + \int_0^\infty e^{-\left(\frac{x}{\lambda_D}+\frac{y}{\lambda_{E_i}}\right)\frac{1}{az}-\frac{z}{\lambda_S}} dz \\ &= 1 - uK_1(u) - vK_1(v) + tK_1(t), \end{aligned} \tag{20}$$

where $X = \gamma_{SD}$, $Y = \gamma_{SE_i}$, $u = 2\sqrt{\frac{x}{a\lambda_S\lambda_D}}$,

$v = 2\sqrt{\frac{y}{a\lambda_S\lambda_{E_i}}}$, and $t = 2\sqrt{\frac{(\lambda_{E_i}x + \lambda_D y)}{a\lambda_S\lambda_D\lambda_{E_i}}}$

Appendix B

$$\begin{aligned} P_{CS} &= \int_0^\infty \int_0^x f_{\gamma_{SD},\gamma_{SE_i}}(x,y)dxdy \\ &= \int_0^\infty \left[\frac{\partial F_{\gamma_{SD},\gamma_{SE_i}}(x,y)}{\partial x}\right]_{y=x} dx \\ &= \int_0^\infty \left[K_0\left(2\sqrt{\frac{x}{a\lambda_S\lambda_D}}\right) - K_1\left(2\sqrt{\frac{(\lambda_{E_i}+\lambda_D)x}{a\lambda_S\lambda_D\lambda_{E_i}}}\right)\right] dx \\ &= \frac{\lambda_D}{\lambda_D + \lambda_{E_i}} \quad . \end{aligned} \tag{21}$$

Appendix C

$$\begin{aligned} P_{out} &= P(C_S < R) \\ &= \int_0^\infty \int_0^{2^R(1+y)-1} f_{\gamma_{SD},\gamma_{SE}}(x,y)dxdy \\ &= \int_0^\infty \left[1 - uK_1(u) - vK_1(v) + tK_1(t)\right]_{x=2^R(1+y)-1} dy \\ &= 1 - \frac{\lambda_D}{2^R\lambda_{E_i} + \lambda_D} bK_1(b) \quad , \end{aligned} \tag{22}$$

where $b = 2\sqrt{\frac{2^R - 1}{a\lambda_S\lambda_D}}$.

REFERENCES

[1] H. J. Visser and R. J. M. Vullers, "RF energy harvesting and transport for wireless sensor network applications: principles and requirements," *Proceedings of the IEEE*, vol. 101, no. 6, pp. 1410-

1423, 2013.

[2] K. Huang and V. K. N. Lau, "Enabling wireless power transfer in cellular networks: architecture, modeling and deployment," *IEEE Transactions on Wireless Communications*, vol. 13, no. 2, pp. 902-912, 2014.

[3] H. Nishimoto, Y. Kawahara, and T. Asami, "Prototype implementation of ambient RF energy harvesting wireless sensor networks," in *Proceedings of IEEE Sensors*, Kona, HI, pp. 1282-1287, 2010.

[4] X. Zhang, H. Jiang, L. Zhang, C. Zhang, Z. Wang, and X. Chen, "An energy-efficient ASIC for wireless body sensor networks in medical applications," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 4, no. 1, pp. 11-18, 2010.

[5] H. Liu, "Maximizing efficiency of wireless power transfer with resonant inductive coupling," 2011 [Internet]. Available: http://hxhl95.github.io/media/ibee.pdf.

[6] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[7] L. Liu, R. Zhang, and K. C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Transactions on Signal Processing*, vol. 62, no. 7, pp. 1850-1863, 2014.

[8] X. Chen, Z. Zhang, H. H. Chen, and H. Zhang, "Enhancing wireless information and power transfer by exploiting multi-antenna techniques," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 133-141, 2015.

[9] B. He and X. Zhou, "On the placement of RF energy harvesting node in wireless networks with secrecy considerations," in *Proceedings of 2014 IEEE Globecom Workshops*, Austin, TX, pp. 1355-1360, 2014.

[10] D. B. Ha, D. D. Tran, T. V. Truong, and N. V. Vo, "Physical layer secrecy performance of energy harvesting networks with power transfer station selection," in *Proceedings of the 6th International Conference on Communications and Electronics (ICCE)*, Ha Long Bay, Vietnam, pp. 451-456, 2016.

Tien-Vu Truong
received his B.S, M.S., and Ph.D. candidate in Computer Science in 1999, 2009, 2012 respectively. Since 2000, he has been taught and researched at Duy Tan University, Vietnam. His research interest includes information security, physical layer secrecy, RF-EH and other advanced communication systems security. He a member of IEEE, VNISA, DSA.

Nhan-Van Vo
received the B.E. and M.Sc. degrees of Computer Science in 2006 and 2014, respectively. Since 2009, he has been taught and researched at Duy Tan University, Vietnam. His research interests include information security, physical layer secrecy, RF-EH and other advanced communication systems security. He is member of Cisco System, Juniper System, ComPTIA System.

Dac-Binh Ha
received the B.S. degree in Radio Technique, the M.Sc. and Ph.D. degrees in Communication and Information System from Huazhong University of Science and Technology (HUST), China in 1997, 2006, and 2009, respectively. He is currently the Dean of Faculty of Electrical & Electronics Engineering, Duy Tan University, Da Nang, Vietnam.

Duc-Dung Tran
received the B.E. degree in electronics and telecommunications from Hue University of Sciences, Vietnam, in 2013, the M.Sc. degree in computer sciences from Duy Tan University, Vietnam, in 2016. He works for the Institute of R&D, Duy Tan University as an assistant researcher. His research interests include secrecy physical layer communications, wireless communications, UWB communication systems, MIMO systems, wireless energy harvesting networks.