# Wireless Power Transfer Under Secure Communication with Multiple Antennas and Eavesdroppers

Duc-Dung Tran[1], Dac-Binh Ha[1(✉)], and Anand Nayyar[2]

[1] Faculty of Electrical and Electronics Engineering, Duy Tan University, Danang, Vietnam
dung.td.1227@gmail.com, hadacbinh@duytan.edu.vn
[2] Graduate School, Duy Tan University, Danang, Vietnam
anandnayyar@duytan.edu.vn

**Abstract.** In this paper, we analyze the physical layer secrecy performance of a 5G radio frequency energy harvesting (RF-EH) network in the presence of multiple passive eavesdroppers. In this system, the source is considered as an energy-limited node, hence it harvests energy from RF signals generated by a power transfer station to use for information transmission. Additionally, in order to enhance the energy harvesting and system performance, the source is equipped with multiple antennas and employs maximal ratio combining (MRC) and transmit antenna selection (TAS) techniques to exploit the benefits of spatial diversity. Given these settings, the exact close-form expressions of existence probability of secrecy capacity and secrecy outage probability are derived. Furthermore, the obtained results indicate that multiple antennas technique applied at the source not only facilitates energy harvesting but also improves secrecy performance of the investigated network. Finally, Monte-Carlo simulation is provided to confirm our analytical results.

**Keywords:** Energy harvesting · Maximal ratio combining
Secrecy capacity · Transmit antenna selection · Wireless power transfer

## 1 Introduction

In recent years, a new solution, namely Radio Frequency (RF) energy harvesting (EH) has ben proposed for powering wireless devices in 5G network [1–3]. This technology helps to prolong the lifetime of the devices without recharging or replacing the batteries which is usually inconvenient or even impossible (e.g., medical devices embedded inside human bodies). More importantly, it can bring energy-constrained communication nodes the possibility of collecting energy and receiving information simultaneously.

On the other hand, many recent research works have been devoted to physical layer security (PLS) [4–6]. Unlike the traditional secure methods (e.g., upper-layer cryptographic protocols), which provide security under the assumptions

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2019
Published by Springer Nature Switzerland AG 2019. All Rights Reserved
T. Q. Duong and N.-S. Vo (Eds.): INISCOM 2018, LNICST 257, pp. 208–220, 2019.
https://doi.org/10.1007/978-3-030-05873-9_17

of limited computational capability at the eavesdroppers and error-free physical link, PLS regarded as a complement to the cryptographic technology, improves secrecy performance of wireless networks by exploiting the nature of wireless channels [7,8].

As to the RF-EH network, PLS has been studied to evaluate the information security ability of this network [8–14]. Specifically, the works in [8,10] have addressed secure cooperative communication in RF-EH networks. He et al. [11] has investigated the optimal placement of the EH node with PLS considerations by solving two optimization problems: maximizing the average EH power subject to a secrecy outage constraint and minimizing the secrecy outage probability subject to an EH constraint. In [12], PLS in single-input single-output (SISO) simultaneous wireless information and power transfer (SWIPT) system has been evaluated by analyzing the optimization problems of transmit power allocations and power splitting ratios. Moreover, to utilize the advantages of spatial diversity, multiple antennas technique has been studied in [13,14]. In particular, the work in [13] has investigated a MIMO information-energy broadcast system. The authors have supposed that a multi-antenna source can transmit information and energy simultaneously to a multi-antenna information receiver and a multi-antenna energy receiver, where the energy receiver is considered as an eavesdropper. Also, they has proposed global optimal solutions to the secrecy rate maximization (SRM) problem. Furthermore, the authors in [14] have formulated the resource allocation algorithm design for secure MISO communication systems with RF energy harvesting receivers as a non-convex optimization problem. Given these studies, it can be concluded that besides reducing the received signal at eavesdroppers, multiple antennas technique can improve the received signals at both IRs and ERs. As a result, it can enhance the secrecy performance and RF-EH. However, to the best of our knowledge, the secrecy performance analysis for multi-antenna information source considered as energy harvesting nodes has not been studied.

In this paper, we focus on anlyzing the secrecy performance of a wireless power transfer system with multiple antennas at the source over Rayleigh fading channels. In particular, the network consists of one power transfer station, one energy-constrained source and one destination in the presence of multiple passive eavesdroppers. The source is equipped with multiple antennas to facilitate the energy harvesting and information transmission processes, meanwhile all the remaining nodes have a single antenna. Our contributions can be summarized as follows. First, we propose a communication protocol which helps to improve energy collecting capability of the source and secrecy performance of the system. Second, we derive the exact close-form expressions of existence probability of secrecy capacity and secrecy outage probability. Third, we evaluate the secrecy performance of the considered system under the influence of various system parameters, namely energy harvesting time, energy conversion efficiency, source location, and average transmit signal-to-noise ratio (SNR). Finally, we confirm the analytical results by using Monte-Carlo simulation.

The remainder of this paper is organized as follows. System and channel model is presented in Sect. 2. Secrecy performance of the considered system is analyzed in Sect. 3. The numerical results are discussed in Sect. 4. We conclude our work with future scope in Sect. 5.

*Notation:* boldface lowercase letters are used to denote vectors. $\mathcal{CN}(0, N_0)$ is a scalar complex Gaussian distribution with zero mean and variance $N_0$. $\mathbb{E}[\cdot]$ indicates the expectation operator. $|\cdot|$ and $\|\cdot\|$ denote the absolute value and the Euclidean norm, respectively. $\mathcal{K}_\nu(\cdot)$ stands for the $\nu^{th}$ – order modified Bessel function of the second kind.

## 2 System and Channel Model

In this paper, we investigate a secure communication system with energy harvesting, as illustrated in Fig. 1. The network consists of one power transfer station denoted by $P$, one energy-constrained information source denoted by $S$, one destination denoted by $D$ and $K$ passive eavesdroppers denoted by $E_k (1 \leq k \leq K)$. It is assumed that $P$, $D$, and $E_k$ are equipped with a single antenna, meanwhile $S$ has $N_S$ antennas. Our proposed protocol divides the overall communication process into two phases. In the first phase, source $S$ harvests energy from the power transfer station $P$ by using MRC scheme to combine the received signals from $N_S$ antennas. In the second phase, source $S$ transmits information to destination $D$ by employing TAS scheme to reduce the signal processing cost and choose the best antenna which maximizes the instantaneous SNR at the destination (i.e., maximize channel coefficient of $S \rightarrow D$ link) [7]. Moreover, we assume that all the channels subject to Rayleigh distribution.

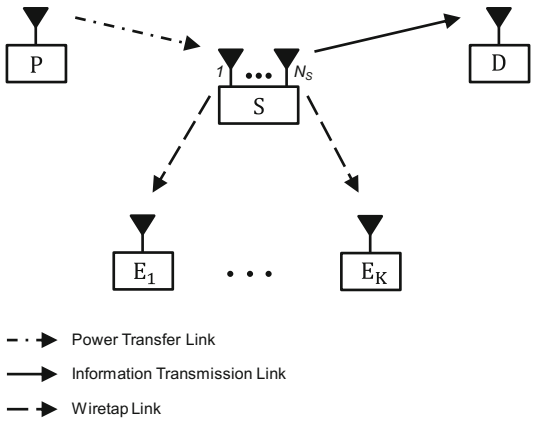


**Fig. 1.** System model for secure communication with energy harvesting.

First, the source S harvests energy from the power station P in the time duration of by using MRC technique. The power used for the second phase is

given by [15]

$$P_S = \frac{E_h}{(1-\alpha)T} = \frac{\eta\alpha P_0 \|\mathbf{h}_{PS}\|^2}{(1-\alpha)d_S^{\theta_S}} = \frac{\eta\alpha P_0}{1-\alpha}\gamma_S, \tag{1}$$

where, $1 < \eta \leq 1$ is the energy conversion efficiency which depends on the rectification process and the energy harvesting circuitry; $P_0$ is the transmit power of the power station; $T$ is the block time in which a certain block of information is conveyed from the source node to the destination node; $\alpha$ is the fraction of the block time in which source $S$ collects energy from the RF signal produced by the power station $P$, $0 < \alpha < 1$. Considering the link from the power station to the source, $\|\mathbf{h}_{PS}\|^2$ is the channel power gain following exponential distribution, with $\mathbf{h}_{PS}$ is $1 \times N_S$ channel vector between an antenna at the power station $P$ and $N_S$ antennas at the source $S$, $\gamma_S = \frac{\|\mathbf{h}_{PS}\|^2}{d_S^{\theta_S}}$, $d_S$ is the distance, $\theta_S$ is the path-loss exponent. The probability density function (PDF) of $\gamma_S$ has the following form [7]

$$f_{\gamma_S}(x) = \frac{x^{N_S-1}e^{-\frac{x}{\lambda_S}}}{\Gamma(N_S)\lambda_S^{N_S}}, \tag{2}$$

where, $\Gamma(\cdot)$ is the Gamma function, $\lambda_S = \frac{\left[\|\mathbf{h}_{PS}\|^2\right]}{d_S^{\theta_S}}$.

In the remaining duration of $(1-\alpha)T$, the source transmits signal $x(t)$ to the destination by applying TAS scheme and the signal received at $D$ can be presented as

$$y(t) = \frac{\sqrt{P_S}h_{SD}}{\sqrt{d_D^{\theta_D}}}x(t) + n_D, \tag{3}$$

where, $h_{SD}$ is the channel coefficient of $S \rightarrow D$ link with $|h_{SD}|^2 = \max_{1\leq i\leq N_S}\left\{|h_{SD,i}|^2\right\}$, $d_D$ and $\theta_D$ are the distance and path-loss exponent of $S \rightarrow D$ link, respectively, $n_D$ is white complex Gaussian noise, $n_D \sim \mathcal{CN}(0, N_0)$.

The eavesdroppers try to extract the transmitted information at $S$ without active attack. The signal received at $E_k$ $(1 \leq k \leq K)$ is given by

$$z_k(t) = \sqrt{\frac{P_S}{d_{E,k}^{\theta_{E,k}}}}h_{SE,k}y(t) + n_{E,k}, \tag{4}$$

where, $h_{SE,k}$ is the channel coefficient of $S \rightarrow E_k$ link, $d_{E,k}$ and $\theta_{E,k}$ are the distance and path-loss exponent from source $S$ to the eavesdropper $E_k$, respectively. $n_{E,k}$ is white complex Gaussian noise, $n_{E,k} \sim \mathcal{CN}(0, N_0)$.

The instantaneous received SNR at the destination $D$ and the eavesdropper $E_k$ are, respectively, presented as

$$\gamma_{SD} = \frac{\eta\alpha P_0\|\mathbf{h}_{PS}\|^2|h_{SD}|^2}{(1-\alpha)N_0 d_S^{\theta_S} d_D^{\theta_D}} = a\gamma_S\gamma_D, \tag{5}$$

$$\gamma_{SE,k} = \frac{\eta\alpha P_0\|\mathbf{h}_{PS}\|^2|h_{SE,k}|^2}{(1-\alpha)N_0 d_S^{\theta_S} d_{E,k}^{\theta_{E,k}}} = a\gamma_S\gamma_{E,k}, \tag{6}$$

where, $a = \frac{\eta\alpha\gamma_0}{1-\alpha}$, $\gamma_S = \frac{\|\mathbf{h}_{PS}\|^2}{d_S^{\theta_S}}$, $\gamma_D = \frac{|h_{SD}|^2}{d_D^{\theta_D}}$, $\gamma_{E,k} = \frac{|h_{SE,k}|^2}{d_{E,k}^{\theta_{E,k}}}$, $\gamma_0 = \frac{P_0}{N_0}$ is the average transmit SNR. The cummulative density function (CDF) of $\gamma_D$ and $\gamma_{E,k}$ are, respectively, given by

$$\begin{aligned} F_{\gamma_D}(x) &= \left(1 - e^{-\frac{x}{\lambda_D}}\right)^{N_S} \\ &\overset{(o)}{=} 1 + \sum_{p=1}^{N_S} \binom{N_S}{p} (-1)^p e^{-\frac{px}{\lambda_D}}, \end{aligned} \tag{7}$$

and

$$F_{\gamma_{E,k}}(x) = 1 - e^{-\frac{x}{\lambda_{E,k}}}, \tag{8}$$

where $(o)$ is obtained by applying ([16], Eq. (1.111)) for binomial expansion, $\lambda_D = \frac{(|h_{SD}|^2)}{d_D^{\theta_D}}$ and $\lambda_{E,k} = \frac{(|h_{SE,k}|^2)}{d_{E,k}^{\theta_{E,k}}}$.

## 3 Secrecy Performance Analysis

### 3.1 Preliminaries

In this subsection, secrecy capacity and joint CDF of $\gamma_{SD}$ and $\gamma_{SE,k}$ $(1 \le k \le K)$ are presented.

The instantaneous secrecy capacity corresponding to the $k$-th eavesdropper is defined as [5]

$$\begin{aligned} C_{S,k} &= \max\{0, C_{SD} - C_{SE,k}\} \\ &= \begin{cases} 0, & \gamma_{SD} \le \gamma_{SE,k} \\ \log_2\left(\frac{1+\gamma_{SD}}{1+\gamma_{SE,k}}\right), & \gamma_{SD} > \gamma_{SE,k} \end{cases}, \end{aligned} \tag{9}$$

where, $C_{SD} = \log_2(1+\gamma_{SD})$ and $C_{SE,k} = \log_2(1+\gamma_{SE,k})$ are the instantaneous channel capacities of the legal and $k$-th eavesdropper channels, respectively.

**Lemma 1.** *Let $X$ and $Y$ be $\gamma_{SD}$ and $\gamma_{SE,k}$ $(1 \le k \le K)$, respectively. Under Rayleigh fading, the joint CDF of $X$ and $Y$ is derived as*

$$\begin{aligned} F_{X,Y}^{(k)}(x,y) = 1 - \frac{t^{N_S}\mathcal{K}_{N_S}(t)}{\Gamma(N_S)2^{N_S-1}} + \sum_{p=1}^{N_S} \binom{N_S}{p} \frac{(-1)^p}{\Gamma(N_S)2^{N_S-1}} \\ \times \left[u^{N_S}\mathcal{K}_{N_S}(u) - v^{N_S}\mathcal{K}_{N_S}(v)\right], \end{aligned} \tag{10}$$

*where,* $\binom{N_S}{p} = \frac{N_S!}{(N_S-p)!p!}$ *is the binomial coefficient,* $X = \gamma_{SD}$, $Y = \gamma_{SE,k}$, $t = 2\sqrt{\frac{y}{a\lambda_S\lambda_{E,k}}}$, $u = 2\sqrt{\frac{px}{a\lambda_S\lambda_D}}$, $v = 2\sqrt{\frac{p\lambda_{E,k}x+\lambda_D y}{a\lambda_S\lambda_D\lambda_{E,k}}}$.

*Proof.* See Appendix A.

### 3.2 Existence Probability of Secrecy Capacity

At this point, we investigate the existence probability of secrecy capacity ($P_{CS}$), which is one of the important measures to evaluate the secrecy performance of a wireless network. For the $k$-th eavesdropper, it is computed as

$$\begin{aligned} P_{CS,k} &= \Pr(C_{S,k} > 0) \\ &= \int_0^{\infty} \int_0^{x} f_{\gamma_{SD},\gamma_{SE,k}}(x,y)dydx \\ &= \int_0^{\infty} \left[ \frac{\partial F_{\gamma_{SD},\gamma_{SE,k}}(x,y)}{\partial x} \right]_{y=x} dx. \end{aligned} \tag{11}$$

**Proposition 1.** *In the presence of $K$ eavesdroppers, the existence probability of secrecy capacity of the considered system over Rayleigh fading channels can be derived as*

$$P_{CS} = \prod_{k=1}^{K} \sum_{p=1}^{N_S} \binom{N_S}{p} \frac{(-1)^{p+1}\lambda_D}{p\lambda_{E,k} + \lambda_D}. \tag{12}$$

*Proof.* See Appendix B.

### 3.3 Secrecy Outage Probability

Another prominent measure which is used to evaluate the secrecy performance is secrecy outage probability ($P_{Out}$). It is defined as the probability that the instantaneous secrecy capacity less than a given secrecy transmission rate, $R > 0$. Given the definition, $P_{Out}$ is formulated by (for the $k$-th eavesdropper)

$$\begin{aligned} P_{Out,k} &= \Pr(C_{S,k} < R) \\ &= \int_0^{\infty} \int_0^{2^R(1+y)-1} f_{\gamma_{SD},\gamma_{SE,k}}(x,y)dxdy \\ &= \int_0^{\infty} \left[ \frac{\partial F_{\gamma_{SD},\gamma_{SE,k}}(x,y)}{\partial y} \right]_{x=2^R(1+y)-1} dx. \end{aligned} \tag{13}$$

**Proposition 2.** *In the presence of $K$ eavesdroppers, the secrecy outage probability of the considered system over Rayleigh fading channels can be derived as*

$$\begin{aligned} P_{Out} = 1 - \prod_{k=1}^{K} \sum_{p=1}^{N_S} \binom{N_S}{p} \frac{(-1)^{p+1}\lambda_D}{\Gamma(N_S)\, 2^{N_S-1}\, (p2^R\lambda_{E,k} + \lambda_D)} \\ \times \left[ 2\sqrt{\frac{p\,(2^R-1)}{a\lambda_S\lambda_D}} \right]^{N_S} \mathcal{K}_{N_S} \left[ 2\sqrt{\frac{p\,(2^R-1)}{a\lambda_S\lambda_D}} \right]. \end{aligned} \tag{14}$$

*Proof.* See Appendix C.

## 4 Numerical Results and Discussion

In this section, numerical results in terms of the existence probability of secrecy capacity ($P_{CS}$) and the secrecy outage probability ($P_{Out}$) are presented to clarify the physical layer secrecy performance of the considered system.

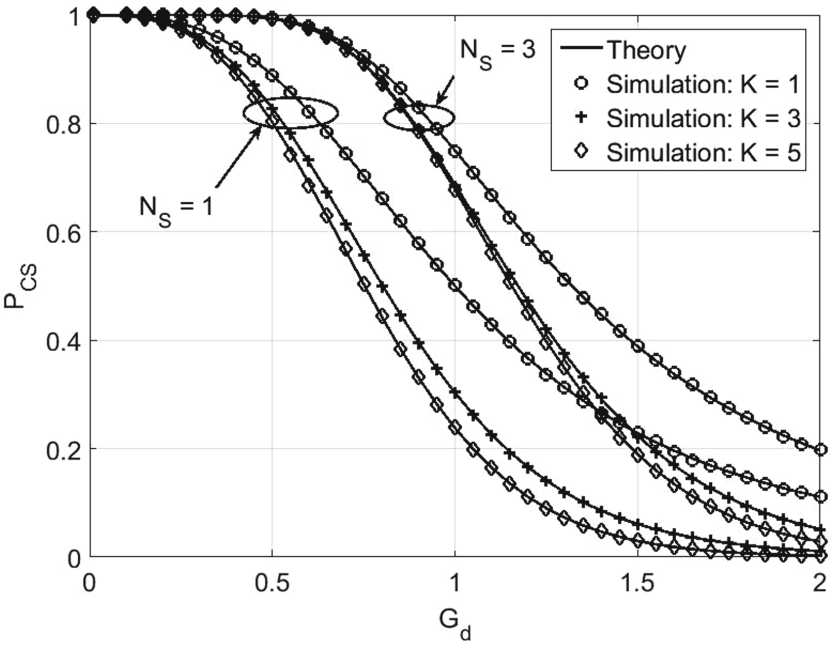


**Fig. 2.** $P_{CS}$ vs. $G_d$ with $\alpha = 0.5$, $\eta = 1$, $d_S = 2$ (m), $\theta_S = \theta_D = \theta_E = 3$, $\gamma_0 = 10$ (dB).

Accounting for the path-loss exponent of the wiretap links, we set $\theta_{E,1} = \theta_{E,2} = ... = \theta_{E,K} = \theta_E$. Furthermore, $K$ eavesdroppers are randomly located (following uniform distribution) in a circle of radius 5 (m) from the source. To evaluate the impact of the distances $d_D$ and $d_{E,k}$ $(1 \leq k \leq K)$ on the secrecy performance parameters ($P_{CS}$ and $P_{Out}$), we define a factor $G_d = \frac{d_D}{d_E}$, with $d_E = \min\limits_{1 \leq k \leq K} \{d_{E,k}\}$. It can be seen that when $G_d < 1$, the position of the destination is closer to the source than that of all the $K$ eavesdroppers. Additionally, as $G_d > 1$, some of eavesdroppers or all of them are placed closer to the source than the destination.

Figures 2 and 3 plots $P_{CS}$ and $P_{Out}$ versus $G_d$, respectively. Moreover, different values of $N_S$ and $K$ are considered in these figures. It can be seen that while the larger number of antennas at the source ($N_S$) leads to the growth of the secrecy performance ($P_{CS}$ increases and $P_{Out}$ decreases), it decreases ($P_{CS}$ decreases and $P_{Out}$ increases) with respect to the upward trend in the number of eavesdroppers ($K$). Moreover, we can see that the increase in $G_d$ makes $P_{CS}$

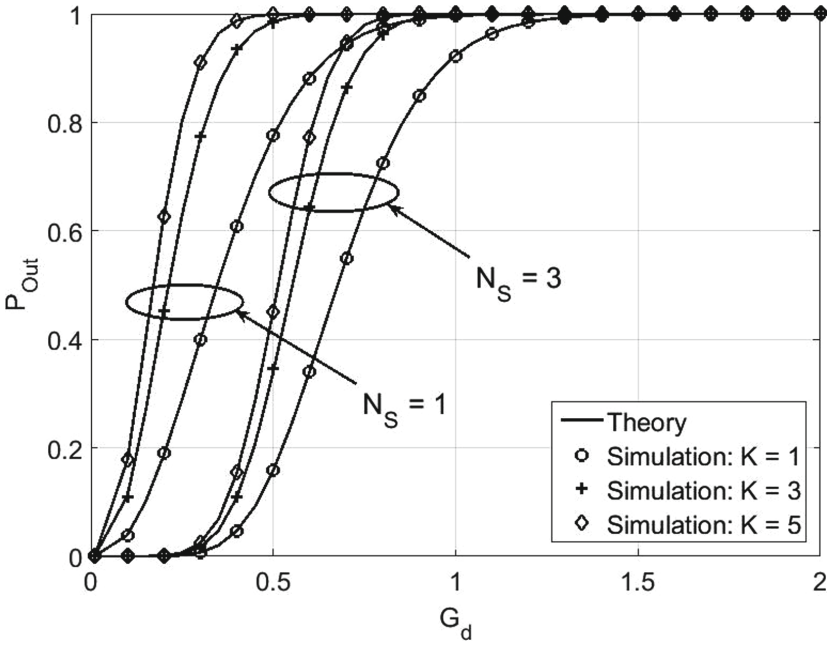


**Fig. 3.** $P_{Out}$ vs. $G_d$ with $\alpha = 0.5$, $\eta = 1$, $d_S = 2$ (m), $R = 1$ (bit/s/Hz), $\theta_S = \theta_D = \theta_E = 3$, $\gamma_0 = 10$ (dB).

degrade and $P_{Out}$ upgrade. This can be explained that the greater $G_d$ is, the larger $S \to D$ distance is, hence the capacity of legal channel is much smaller than that of illegal channels. When $G_d \to 0$ then $P_{CS} \to 1$ and $P_{Out} \to 0$, and when $G_d > 1$ then $P_{CS} \to 0$ and $P_{Out} \to 1$.

As can be seen from (12) and (14) that $P_{CS}$ does not depend on $\alpha$, $\eta$ and $\gamma_0$ (i.e., it is not influenced by the amount of harvested energy at the source) but $P_{Out}$ is observed as a function of these system parameters as shown in Figs. 4 and 5, respectively. Specifically, it is apparent from Fig. 4 that when $\alpha$ and $\eta$ scale up (i.e., the amount of harvested energy increases) then $P_{Out}$ scales down, hence the secrecy performance of the considered system is improved. The similar conclusions is also obtained when $\gamma_0$ increases as illustrated in Fig. 5.

Generally, from the aforementioned results (in Figs. 2, 3, 4, and 5), one can conclude that the secrecy performance of the considered system is better with the increase in the number of antennas as well as the amount of harvested energy at the source. Furthermore, the presence of multiple eavesdroppers makes the secrecy performance get worse. Finally, our analysis is confirmed by the excelent match between the analytical and simulation results.

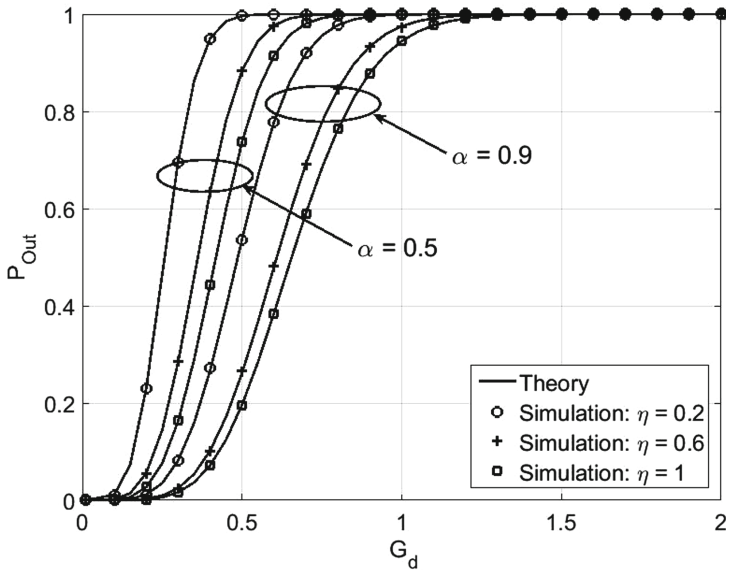


**Fig. 4.** $P_{Out}$ vs. $G_d$ with $N_S = 2$, $K = 3$, $d_S = 2$ (m), $R = 1$ (bits/s/Hz), $\theta_S = \theta_D = \theta_E = 3$, $\gamma_0 = 10$ (dB).

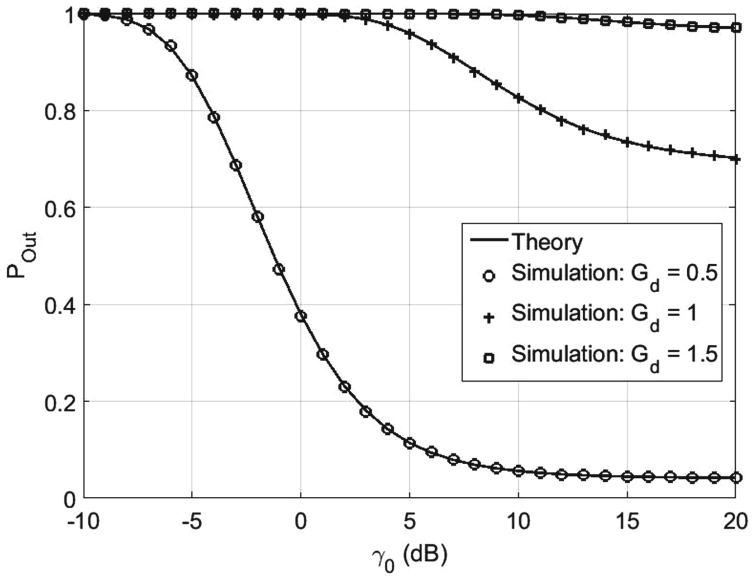


**Fig. 5.** $P_{Out}$ vs. $\gamma_0$ with $\alpha = 0.5$, $\eta = 1$, $N_S = 2$, $K = 3$, $d_S = 2$ (m), $R = 1$ (bit/s/Hz), $\theta_S = \theta_D = \theta_E = 3$.

## 5 Conclusion and Future Scope

In this paper, we have investigated a RF-EH network under the secure communication over Rayleigh fading channels, in which the energy-constrained source is equipped with multiple antennas. Furthermore, the MRC and TAS schemes have been employed at the source to exploit the benefits of multiple antennas. To analyze the secrecy performance of the considered system, we have derived the exact close-form expressions of existence probability of secrecy capacity and secrecy outage probability. Also, by means of these analytical results, the impact of various system parameters, such as energy harvesting time, energy conversion efficiency, source location, and average transmit SNR, on the secrecy performance have been evaluated. Furthermore, our results have showed that by applying multiple antennas at the source and using MRC as well as TAS techniques, both secrecy performance of the considered system and EH capability of the source are improved.

In the future work, we will extend this system model to multiuser schedule scheme with hybrid energy harvesting architecture, i.e., the combination of time switching and power splitting, to improve the secrecy performance of wireless networks.

**Acknowledgement.** This work was supported by Newton Prize 2017 and by a Research Environment Links grant, ID 339568416, under the Newton Programme Vietnam partnership. The grant is funded by the UK Department of Business, Energy and Industrial Strategy (BEIS) and delivered by the British Council. For further information, please visit www.newtonfund.ac.uk/.

## Appendix A: Proof of Lemma 1

According to the probability definition, the joint CDF of $X$ and $Y$ is given by

$$\begin{aligned} F_{X,Y}^{(k)}(x,y) &= \Pr\left(X < x, Y < y\right) \\ &= \Pr\left(\gamma_D < \frac{x}{a\gamma_S}, \gamma_{E,k} < \frac{y}{a\gamma_S}\right) \\ &= \int_0^\infty F_{\gamma_D}\left(\frac{x}{az}\right) F_{\gamma_{E,k}}\left(\frac{y}{az}\right) f_{\gamma_S}(z)dz. \end{aligned} \tag{A.1}$$

Substituting (2), (7), and (8) into (A.1) and then using ([16], Eq. (3.471.9)), the final result is obtained as shown in (10).

## Appendix B: Proof of Proposition 1

By employing ([16], Eq. (6.561.16)) and ([16], Eq. (8.486.14)), (11) is expanded as

$$\begin{aligned} P_{CS,k} &= \sum_{p=1}^{\infty} \binom{N_S}{p} \frac{(-1)^p 2p}{\Gamma(N_S)\, 2^{N_S-1} a \lambda_S \lambda_D} \left\{ \int_0^{\infty} v_x^{N_S-1} \mathcal{K}_{N_S-1}[v_x]\, dx \right. \\ &\qquad \left. - \int_0^{\infty} (u)^{N_S-1} \mathcal{K}_{N_S-1}(u)\, dx \right\} \\ &= \sum_{p=1}^{\infty} \binom{N_S}{p} \frac{(-1)^p}{\Gamma(N_S)\, 2^{N_S-1}} \left\{ \frac{p\lambda_{E,k}}{p\lambda_{E,k} + \lambda_D} \int_0^{\infty} t^{N_S} \mathcal{K}_{N_S-1}(t)\, dx \right. \\ &\qquad \left. - \int_0^{\infty} t^{N_S} \mathcal{K}_{N_S-1}(t)\, dx \right\} \\ &= \sum_{p=1}^{\infty} \binom{N_S}{p} \frac{(-1)^{p+1} \lambda_D}{p\lambda_{E,k} + \lambda_D}, \end{aligned} \tag{B.1}$$

where, $v_x = 2\sqrt{\frac{(p\lambda_{E,k}+\lambda_D)x}{a\lambda_S\lambda_D\lambda_{E,k}}}$ and $u = 2\sqrt{\frac{px}{a\lambda_S\lambda_D}}$.

In the presence of $K$ eavesdroppers, the existence probability of secrecy capacity is given by

$$\begin{aligned} P_{CS} &= \Pr(C_{S,1} > 0, ..., C_{S,K} > 0) \\ &= \prod_{k=1}^{K} \Pr(C_{S,k} > 0). \end{aligned} \tag{B.2}$$

The final result of $P_{CS}$ in (12) is obtained by substituting (B.1) into (B.2).

## Appendix C: Proof of Proposition 2

Similar to the process of calculating (11) in Appendix B, the integral in (13) is solved by the help of ([16], Eq. (6.561.16)) and ([16], Eq. (8.486.14)) and the result is indicated in (C.1) as follows:

$$
\begin{aligned}
P_{Out,k} &= \frac{2}{\Gamma(N_S)\, 2^{N_S-1} a\lambda_S \lambda_{SE,k}} \left\{ \int_0^{\infty} (t)^{N_S-1} \mathcal{K}_{N_S-1}(t)\, dy + \sum_{p=1}^{N_S} \binom{N_S}{p} (-1)^p \right. \\
&\qquad \left. \times \int_0^{\infty} [w]^{N_S-1} \mathcal{K}_{N_S-1}[w]\, dy \right\} \\
&= \frac{1}{\Gamma(N_S)\, 2^{N_S-1}} \left\{ \int_0^{\infty} t^{N_S} \mathcal{K}_{N_S-1}(t)\, dt \right. \\
&\qquad \left. + \sum_{p=1}^{N_S} \binom{N_S}{p} \frac{(-1)^p \lambda_D}{p2^R \lambda_{E,k} + \lambda_D} \int_u^{\infty} t^{N_S} \mathcal{K}_{N_S-1}(t)\, dt \right\} \\
&= 1 - \sum_{p=1}^{N_S} \binom{N_S}{p} \frac{(-1)^{p+1} \lambda_D}{\Gamma(N_S)\, 2^{N_S-1} (p2^R \lambda_{E,k} + \lambda_D)} \\
&\qquad \times \left[ 2\sqrt{\frac{p(2^R-1)}{a\lambda_S \lambda_D}} \right]^{N_S} \mathcal{K}_{N_S} \left[ 2\sqrt{\frac{p(2^R-1)}{a\lambda_S \lambda_D}} \right],
\end{aligned}
\tag{C.1}
$$

where, $t = 2\sqrt{\frac{y}{a\lambda_S \lambda_{E,k}}}$ and $w = 2\sqrt{\frac{(p2^R\lambda_{E,k}+\lambda_D)y + p\lambda_{E,k}(2^R-1)}{a\lambda_S \lambda_D \lambda_{E,k}}}$.

For K eavesdroppers, the secrecy outage probability is computed as

$$
\begin{aligned}
P_{Out} &= 1 - \Pr(C_{S,1} \geq R, ..., C_{S,K} \geq R) \\
&= 1 - \prod_{k=1}^{K} \Pr(C_{S,k} \geq R) \\
&= 1 - \prod_{k=1}^{K} [1 - \Pr(C_{S,k} < R)].
\end{aligned}
\tag{C.2}
$$

Substituting (C.1) into (C.2), the final result of $P_{Out}$ in (14) is derived.

## References


1. Lu, X., Wang, P., Niyato, D., Kim, D.I., Han, Z.: Wireless networks with RF energy harvesting: a contemporary survey. IEEE Commun. Surv. Tutor. **17**(2), 757–789 (2015)
2. Krikidis, I., Timotheou, S., Nikolaou, S., Zheng, G., Ng, D.W.K., Schober, R.: Simultaneous wireless information and power transfer in modern communication systems. IEEE Commun. Mag. **52**(11), 104–110 (2014)
3. Ha, D.B., Tran, D.D., Tran, H.V., Hong, E.K.: Performance of amplify-and-forward relaying with wireless power transfer over dissimilar channels. Elektronika ir Elektrotechnika J. **21**(5), 90–95 (2015)

4. Bloch, M., Barros, J., Rodrigues, M.R., McLaughlin, S.W.: Wireless information-theoretic security. IEEE Trans. Inform. Theory **54**(6), 2515–2534 (2008)
5. Tran, D.D., Ha, D.-B., Tran-Ha, V., Hong, E.K.: Secrecy analysis with MRC/SC-based eavesdropper over heterogeneous channels. IETE J. Res. **61**(4), 363–371 (2015)
6. Liu, Y., Wang, L., Duy, T.T., Elkashlan, M., Duong, T.Q.: Relay selection for security enhancement in cognitive relay networks. IEEE Wirel. Commun. Lett. **4**, 46–49 (2015)
7. Yang, N., Yeoh, P.L., Elkashlan, M.: Transmit antenna selection for security enhancement in MIMO wiretap channels. IEEE Trans. Comm. **61**(1), 144–154 (2013)
8. Li, Q., Zhang, Q., Qin, J.: Secure relay beamforming for simultaneous wireless information and power transfer in nonregenerative relay networks. IEEE Trans. Veh. Technol. **63**(5), 2462–2467 (2014)
9. Kalamkar, S.S., Banerjee, A.: Secure communication via a wireless energy harvesting untrusted relay. IEEE Trans. Veh. Technol. **66**(3), 2199–2213 (2017)
10. Chen, X., Chen, J., Liu, T.: Secure wireless information and power transfer in large-scale MIMO relaying systems with imperfect CSI. In: IEEE GLOBECOM, pp. 4131–4136 (2014)
11. He, B., Zhou, X.: On the placement of RF energy harvesting node in wireless networks with secrecy considerations. In: IEEE Globecom Workshops, pp. 1355–1360 (2014)
12. Xing, H., Liu, L., Zhang, R.: Secrecy wireless information and power transfer in fading wiretap channel. IEEE Trans. Veh. Technol. **65**(1), 180–190 (2016)
13. Shi, Q., Xu, W., Wu, J., Song, E., Wang, Y.: Secure beamforming for MIMO broadcasting with wireless information and power transfer. IEEE Trans. Wirel. Commun. **14**(5), 2841–2853 (2015)
14. Ng, D.W.K., Lo, E.S., Schober, R.: Robust beamforming for secure communication in systems with wireless information and power transfer. IEEE Trans. Wirel. Commun. **13**(8), 4599–4615 (2014)
15. Nasir, A.A., Zhou, X., Durrani, S., Kennedy, R.A.: Relaying protocols for wireless energy harvesting and information processing. IEEE Trans. Wirel. Commun. **12**(7), 3622–3636 (2013)
16. Gradshteyn, I., Ryzhik, I.: Table of Integrals, Series, and Products, 7th edn. Academic Press, Cambridge (2007)