Secrecy Outage Minimization for Wireless Powered Communication Networks with an Energy Harvesting Jammer

Jihwan Moon, Hoon Lee, Changick Song, *Member*, *IEEE*, and Inkyu Lee, *Fellow*, *IEEE*

***Abstract*—In this work, we consider a wireless powered communication network (WPCN) with an energy harvesting (EH) jammer where an eavesdropper tries to wiretap the communication between a user and a hybrid access-point (H-AP). In our system, the H-AP first transmits an energy signal to recharge the batteries of the EH user and the EH jammer in the energy transfer (ET) phase. Then, in the subsequent information transfer (IT) phase, the user sends its information signal to the H-AP, while the jammer generates the jamming signal to interfere the eavesdropper utilizing the harvested energy in the ET phase. Assuming only the channel distribution information (CDI) of the eavesdropper is available at the legitimate nodes, we analyze and minimize the secrecy outage probability by optimizing the time allocation between the two phases. To reduce the complexity, we also provide a simple closed-form solution, and the simulation results verify that its performance approaches the optimum.**

I. Introduction

Recently, energy harvesting (EH) utilizing wireless radio frequency (RF) signal has been regarded as a promising alternative to providing energy sources in communication networks. The EH is considered to be useful in many situations such as disasters, extreme environments or sensor networks embedded in human bodies for a biomedical purpose [1].

The two mainstreams of communication systems based on the EH are simultaneous wireless information and power transfer (SWIPT) and wireless powered communication networks (WPCN) [2]. In SWIPT, the transmitted signals contain both information and energy to concurrently achieve information delivery and wireless energy recharging [3]–[9]. On the other hand, for WPCN, a hybrid access-point (H-AP) first broadcasts energy-carrying signals to recharge EH nodes in the energy transfer (ET) phase, and then the EH nodes transmit information-carrying signals in the information transfer (IT) phase by utilizing the harvested energy in the previous ET phase [10]–[12].

In the meantime, physical layer security issues in communications have also been brought up for the last decades [13]. One of the technologies for enhancing the secrecy performance is to transmit artificial noise (AN) on top of the transmitted signals to interfere eavesdroppers [14] [15]. For EH communication systems, the authors in [16]–[18] considered the physical layer security with the AN employed at the transmitter side by treating the EH receivers as potential eavesdroppers. A three-node fading wiretap channel composed of a transmitter, an information receiver and an energy receiver was studied in [18], and the optimal transmit power allocation between the AN and the information signals was proposed. The work in [19] introduced two-phase secure RF EH communications with an EH jammer and an eavesdropper and obtained the maximum throughput based on secrecy outage probability constraint. All these works, however, have not explicitly analyzed the time allocation between ET and IT in the wiretap WPCN, which is regarded as a major challenge for WPCN.

In this paper, we consider a WPCN with an EH jammer and an eavesdropper which tries to wiretap the communication between an EH user and an H-AP. The H-AP recharges both the user and the jammer in the first ET phase. Then, by using the harvested energy, the user transmits its information signal to the H-AP in the subsequent IT phase, while the jammer generates the jamming signal to interfere the eavesdropper. Since the exact channel state information is practically difficult to obtain, we investigate a case where only the channel distribution information (CDI) of the eavesdropper is known to the legitimate nodes. Particularly, we derive an analytic expression of the secrecy outage probability and propose the outage probability minimization problem to find an optimal time allocation between ET and PT phases. It will be shown that the outage probability is non-convex with respect to the time allocation factor. To circumvent the high computational complexity of an inevitable exhaustive search, we effectively reduce the one-dimensional search size by examining the analytic expression. Moreover, in order to further lower the heavy computation, we also provide a closed-form solution by worst-case approximation. Simulation results demonstrate that the near-optimal performance is achieved by the proposed closed-form solution with significant performance gain compared to other schemes, and validate our analysis on the secrecy outage probability.

The remainder of the paper is organized as follows: Section II describes the system model, and Section III discusses the optimal time allocation for the secrecy outage probability minimization problem. Then, we propose a closed-form solution in Section IV and consider the conventional WPCN without a jammer as a benchmark scheme in Section V. Finally, in Section VI, we evaluate the secrecy performance of our system through numerical examples, and Section VII concludes the paper.

Notations: We use $\mathbb{R}$, $\mathbb{C}$ as sets of real and complex numbers, respectively, and $\Pr(\nu)$ stands for the probability of an event ν. Moreover, $|\cdot|$, $(\cdot)^*$ and $\mathbb{E}[\cdot]$ are the absolute value,

This work was supported by the National Research Foundation of Korea (NRF) funded by the Korea Government (MSIP) under Grant 2014R1A2A1A10049769.

J. Moon, H. Lee, and I. Lee are with the School of Electrical Engineering, Korea University, Seoul, Korea (e-mail: {anschino, ihun1, inkyu}@korea.ac.kr).

C. Song is with the Dept. of Information and Communications Eng., Korea National University of Transportation, Chungju, Korea (e-mail: c.song@ut.ac.kr).

978-1-5090-1328-9/16/$31.00 ©2016 IEEE

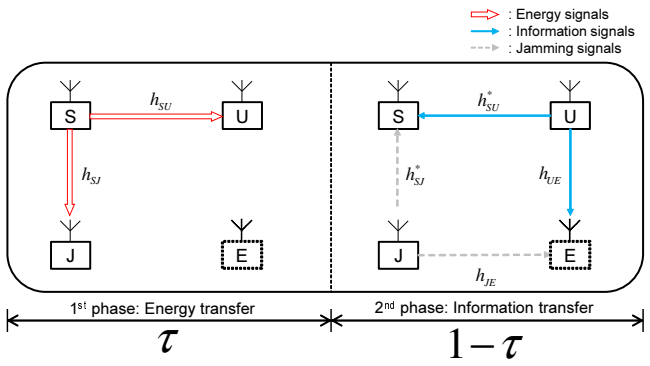

Fig. 1. Schematic diagram for the two-phase WPCN

complex conjugate and the expectation operation, respectively. We define $[x]^+ \triangleq \max(0, x)$, and $\mathcal{CN}(m, \sigma^2)$ denotes a circularly symmetric complex Gaussian distribution with mean m and variance σ^2.

II. System Model

In Fig. 1, we describe the system model for the WPCN where a H-AP S, a dedicated EH user U, an EH jammer J, and an eavesdropper E are equipped with a single antenna. It is assumed that the H-AP operates with a constant power supply, while the user and the jammer harvest energy from the RF signals transmitted from the H-AP. We employ the two-phase WPCN protocol [2] [10], where the H-AP first broadcasts the energy-carrying RF signal in the ET phase for τ amount of the total time block. Then, based on the energy harvested in the previous phase, the user and the jammer transmit their information signal and jamming signal, respectively, during the IT phase for the remaining $1-\tau$ portion of the time block. Without loss of generality, we assume that the time block length equals one.

Throughout the paper, we denote the path-loss effect and the channel coefficient from node X to Y by $L_{\mathsf{XY}} \in \mathbb{R}$ and $h_{\mathsf{XY}} \in \mathbb{C}$, respectively, where $\mathsf{X},\mathsf{Y} \in \{S, U, J, E\}$. Assuming quasi-static flat-fading, all channel gains stay constant during each time block and follow a Rayleigh distribution. It is also assumed that both h_{SU} and h_{SJ} are perfectly known at the H-AP and the user, since channel reciprocity holds for both the ET and the IT phases. During these phases, an eavesdropper is temporarily regarded as an inactive user that may participate in communications in the future [19]. Then, we assume that the location information of the eavesdropper and the CDI of h_{JE} and h_{UE} are available to the network.

During the ET phase, the received signal at energy receiving node $\mathsf{X}_e \in \{U, J\}$ is expressed as

$$y_{\mathsf{X}_e} = \sqrt{P_S L_{S\mathsf{X}_e}} h_{S\mathsf{X}_e} x_S + n_{\mathsf{X}_e},$$

where P_S is the transmit power at the H-AP, $x_S \sim \mathcal{CN}(0,1)$ equals the transmitted symbol from the H-AP, and $n_{\mathsf{X}_e} \sim \mathcal{CN}(0, \sigma^2_{\mathsf{X}_e})$ indicates the complex Gaussian noise at node X_e. Then, the harvested energy at node X_e can be written by [4]

$$\mathcal{E}_{\mathsf{X}_e} = \eta_{\mathsf{X}_e} \mathbb{E}[|y_{\mathsf{X}_e}|^2]\tau = \eta_{\mathsf{X}_e} P_S L_{S\mathsf{X}_e} |h_{S\mathsf{X}_e}|^2 \tau,$$

where $\eta_{\mathsf{X}_e} \in (0, 1]$ represents the EH efficiency at node X_e.

In the IT phase, the user transmits its information signal $x_U \sim \mathcal{CN}(0,1)$ to the H-AP by utilizing the harvested energy $\mathcal{E}_U$. In our system, a security problem arises due to the presence of an eavesdropper. To combat this security issue, the jammer simultaneously generates the jamming signal $x_J \sim \mathcal{CN}(0,1)$ to reduce the eavesdropper's decoding capacity.[1] Then, the received signal at the information receiving node $\mathsf{X}_I \in \{S, E\}$ is given by

$$y_{\mathsf{X}_I} = \sqrt{P_U L_{\mathsf{X}_I U}} h^*_{\mathsf{X}_I U} x_U + \sqrt{P_J L_{\mathsf{X}_I J}} h^*_{\mathsf{X}_I J} x_J + n_{\mathsf{X}_I}, \quad (1)$$

where $P_{\mathsf{X}_e} \triangleq \frac{\zeta_{\mathsf{X}_e} \mathcal{E}_{\mathsf{X}_e}}{1-\tau}$ represents the transmit power with $\zeta_{\mathsf{X}_e} \in (0, 1]$ being a portion of the harvested energy used for signal transmission at node X_e.

We assume that the jamming signal x_J is known at the H-AP, which means that the jamming interference $\sqrt{P_J} h^*_{SJ} x_J$ in (1) can be removed at the H-AP [18]. Then, the signal-to-noise ratio (SNR) at the H-AP and the signal-to-interference-plus-noise ratio (SINR) at the eavesdropper E result in

$$\mathrm{SNR}_S = \frac{|h_{SU}|^2 P_U L_{SU}}{\sigma^2_S} = \frac{\tau}{1-\tau} A', \quad (2)$$

$$\mathrm{SINR}_E = \frac{|h_{UE}|^2 P_U L_{UE}}{|h_{JE}|^2 P_J L_{JE} + \sigma^2_E} = \frac{\tau B' |h_{UE}|^2}{\tau(C'|h_{JE}|^2 - 1) + 1}, \quad (3)$$

where $A' \triangleq \zeta_S \eta_S |h_{SU}|^4 P_S L^2_{SU} / \sigma^2_S$, $B' \triangleq \zeta_U \eta_U |h_{SU}|^2 P_S L_{SU} L_{UE} / \sigma^2_E$ and $C' \triangleq \zeta_J \eta_J |h_{SJ}|^2 P_S L_{SJ} L_{JE} / \sigma^2_E$. By examining (2) and (3), one can show that the secrecy rate equals [16]

$$r_s = W(1-\tau)[\log_2(1 + \mathrm{SNR}_S) - \log_2(1 + \mathrm{SINR}_E)]^+, \quad (4)$$

where W denotes the system bandwidth.

In this paper, we consider the case where only the location and CDI of the eavesdropper is available to the H-AP and the user, and design the system such that the outage probability is minimized. The secrecy outage probability is defined by the probability that the secrecy rate r_s falls below a certain positive threshold r_{th} as [20]

$$P_{out} = \Pr(r_s \le r_{th}). \quad (5)$$

Thus, we have a problem of minimizing the secrecy outage probability as

$$(\mathrm{P}): \min_{\tau} \; P_{out} \quad \text{s.t.} \; 0 < \tau < 1.$$

In the following sections, we provide both the optimal and closed-form solutions for (P).

III. Optimal Solution for Secrecy Outage Probability Minimization

In this section, we derive an analytic expression for the secrecy outage probability and obtain an optimal solution to (P). For convenience, we make use of a monotonic transformation

[1] The worst case AN is known to be Gaussian [14]. Also, we focus on the physical layer security and do not consider any possible encryption techniques.

$s = \frac{\tau}{1-\tau}$ throughout this section. Noting that the operator $[\cdot]^+$ in (4) can be dropped for $r_{th} > 0$, (5) is rewritten by

$$P_{out} = \Pr\Bigg(\log_2(1 + A's) - \log_2\left(1 + \frac{B'|h_{UE}|^2 s}{C'|h_{JE}|^2 s + 1}\right) \leq \frac{r_{th}}{W}(1+s)\Bigg), \tag{6}$$

In the following theorem, we derive an analytic expression of the outage probability (6).

Theorem 1: For a given r_{th}, the secrecy outage probability P_{out} is

$$P_{out} = \begin{cases} \frac{G(s)}{1+G(s)} e^{-\frac{V(s)}{G(s)}} & , \quad \text{if } 1 + A's - 2^{\frac{r_{th}}{W}(1+s)} > 0 \\ 1 & , \quad \text{otherwise} \end{cases} \tag{7}$$

where $G(s) \triangleq D 2^{\frac{r_{th}}{W}(1+s)}/(1 + A's - 2^{\frac{r_{th}}{W}(1+s)})$, $D \triangleq \frac{\zeta_U \eta_U |h_{SU}|^2 P_S L_{SU} L_{UE}}{\zeta_J \eta_J |h_{SJ}|^2 P_S L_{SJ} L_{JE}}$ and $V(s) \triangleq \frac{1}{C's}$.

Proof: From (5), the secrecy outage occurs when the channel capacity from the user to the H-AP is smaller than the threshold r_{th}. In other words, if $W(1-\tau)\log_2\left(1 + A'\frac{\tau}{1-\tau}\right) \leq r_{th}$, or equivalently $1 + A's - 2^{\frac{r_{th}}{W}(1+s)} \leq 0$, we have $P_{out} = 1$.

Now, we consider the case $1 + A's - 2^{\frac{r_{th}}{W}(1+s)} > 0$. Denoting X' and Y' as $X' = |h_{UE}|^2$ and $Y' = |h_{JE}|^2$, X' and Y' independently follow a Chi-square distribution with two degrees of freedom. Thus, we have

$$\begin{aligned} P_{out} &= \Pr(Y' \leq G(s)X' - V(s)) \\ &= \int_{\frac{V(s)}{G(s)}}^{\infty} \int_0^{G(s)x - V(s)} e^{-x} e^{-y} dy dx = \frac{G(s)}{1+G(s)} e^{-\frac{V(s)}{G(s)}}. \end{aligned}$$

Finally, substituting it into (6) yields Theorem 1. ∎

Based on Theorem 1, we reformulate (P) as

$$(\text{P.1}): \min_s \quad \frac{G(s)}{1+G(s)} e^{-\frac{V(s)}{G(s)}}, \tag{8}$$

$$\text{s.t.} \quad 1 + A's - 2^{\frac{r_{th}}{W}(1+s)} > 0, \tag{9}$$

$$s > 0.$$

We will now assume that (P.1) is feasible.[2] It is worth noting that (P.1) is non-convex in general due to (8), and it is not easy to determine an optimal solution. One may solve (P.1) by an exhaustive search method for all $s > 0$. However, the complexity is prohibitive since the optimization variable s is unbounded. Hence, we now decrease the search size of s and obtain the optimal solution in the reduced and bounded search region.

Since the function $1 + A's - 2^{\frac{r_{th}}{W}(1+s)}$ in (9) is concave on s, the feasible domain of (P.1) is a convex set. Thus, we can rewrite (9) as $\tilde{s}_L < s < \tilde{s}_U$, where $\tilde{s}_L > 0$ and $\tilde{s}_U > 0$ are determined by solving the equation $1 + A's - 2^{\frac{r_{th}}{W}(1+s)} = 0$ as

$$\tilde{s}_L = -\frac{W}{r_{th}\ln 2}\mathcal{W}_{L,0}(\theta) - \frac{1}{A'}, \tag{10}$$

$$\tilde{s}_U = -\frac{W}{r_{th}\ln 2}\mathcal{W}_{L,-1}(\theta) - \frac{1}{A'}, \tag{11}$$

[2]Since $P_{out} = 1$ for $1 + A's - 2^{\frac{r_{th}}{W}(1+s)} \leq 0$, we do not consider such a case in (P.1).

with $\theta \triangleq -r_{th}\ln 2 \cdot 2^{\frac{r_{th}}{W}(1-\frac{1}{A'})}/(WA')$ which is always smaller than 0, and $\mathcal{W}_{L,k}(\cdot)$ stands for the Lambert W function with a specific branch k [21].

Now, let us examine the gradient of P_{out} with respect to $G(s)$ and $V(s)$ as

$$\nabla_{G(s),V(s)} P_{out} = \begin{bmatrix} \frac{\partial P_{out}}{\partial G(s)} \\ \frac{\partial P_{out}}{\partial V(s)} \end{bmatrix} = \begin{bmatrix} \frac{(G(s)V(s)+G(s)+V(s))\exp\left(-\frac{V(s)}{G(s)}\right)}{G(s)(G(s)+1)^2} \\ -\frac{\exp\left(-\frac{V(s)}{G(s)}\right)}{G(s)+1} \end{bmatrix}.$$

Since $\frac{\partial P_{out}}{\partial G(s)} > 0$ and $\frac{\partial P_{out}}{\partial V(s)} < 0$ for $G(s) > 0$ and $V(s) > 0$, the outage probability P_{out} decreases as $G(s)$ and $V(s)$ become smaller and larger, respectively. Meanwhile, the gradients of $G(s)$ and $V(s)$ with respect to s are given by

$$\frac{\partial G(s)}{\partial s} = \frac{D(A'(\ln 2 \cdot r_{th} s - W) + \ln 2 \cdot r_{th}) 2^{\frac{r_{th}}{W}(1+s)}}{W\left(1 + A's - 2^{\frac{r_{th}}{W}(1+s)}\right)^2},$$

$$\frac{\partial V(s)}{\partial s} = -\frac{1}{C's^2}.$$

Note that $G(s)$ has the unique minimum stationary point at $\bar{s} = \frac{W}{r_{th}\ln 2} - \frac{1}{A'}$, which lies in $(\tilde{s}_L, \tilde{s}_U)$ since $0 < -\mathcal{W}_{L,0}(\theta) < 1$ and $1 < -\mathcal{W}_{L,-1}(\theta)$ in (10) and (11) for $\theta < 0$.

In contrast, $V(s)$ monotonically decreases with $s > 0$. As a result, the secrecy outage probability P_{out} monotonically increases over $(\bar{s}, \tilde{s}_U)$, and thus the minimum outage occurs in $(\tilde{s}_L, \bar{s}]$. Therefore, we can employ a one-dimensional exhaustive search method over the reduced search size $(\tilde{s}_L, \bar{s}]$ for the optimal solution s_{SO} for the secrecy outage problem (P.1), and the optimal time allocation factor is computed as $\tau_{\text{SO}} = \frac{s_{\text{SO}}}{s_{\text{SO}}+1}$.

IV. Closed-form Solution for Secrecy Outage Probability Minimization

To circumvent the high complexity of one-dimensional search, we now derive a closed-form solution $\hat{s}_{\text{SO}}$ of (P.1). To this end, we assume that the noise power is negligibly small at the eavesdropper, which leads to an upper bound of P_{out} in (7) as

$$P_{out,\text{UB}} = \begin{cases} \frac{G(s)}{1+G(s)} & , \quad \text{if } 1 + A's - 2^{\frac{r_{th}}{W}(1+s)} > 0 \\ 1 & , \quad \text{otherwise.} \end{cases}$$

As $P_{out,\text{UB}}$ monotonically increases with $G(s)$ and $V(s) = 0$, the solution $\hat{s}_{\text{SO}}$ which minimizes $P_{out,\text{UB}}$ becomes the minimizer of $G(s)$, i.e., $\hat{s}_{\text{SO}} = \bar{s}$ as defined in Section III. Hence, we obtain the closed-form time allocation factor $\hat{\tau}_{\text{SO}}$ as

$$\hat{\tau}_{\text{SO}} = \frac{\bar{s}}{\bar{s}+1} = \frac{WA' - r_{th}\ln 2}{WA' - (1-A')r_{th}\ln 2}.$$

V. A Case without an EH Jammer

In this subsection, we investigate the conventional WPCN without a jammer, i.e., $\zeta_J = 0$. Since (7) is undefined for $\zeta_J = 0$, we first let $C' = 0$ in (6) as

$$P_{out} = \Pr\Bigg(\log_2(1 + A's) - \log_2(1 + B'|h_{UE}|^2 s) \leq \frac{r_{th}}{W}(1+s) \Bigg).$$

Following the similar approach in Theorem 1, it can be shown that

$$P_{out} = \begin{cases} \exp\left(-\frac{\tilde{G}(s)}{B'}\right) & , \quad \text{if } 1 + A's - 2^{\frac{r_{th}}{W}(1+s)} > 0 \\ 1 & , \quad \text{otherwise} \end{cases} \tag{12}$$

where $\tilde{G}(s) \triangleq (1 + A's - 2^{\frac{r_{th}}{W}(1+s)})/(s \cdot 2^{\frac{r_{th}}{W}(1+s)})$. Noting that $1 + A's - 2^{\frac{r_{th}}{W}(1+s)}$ and $s \cdot 2^{\frac{r_{th}}{W}(1+s)}$ are concave and convex, respectively, $\tilde{G}(s)$ is therefore a quasi-concave function of s with a unique stationary point that minimizes (12). Hence, employing a sub-gradient method such as the bisection method yields the optimal time allocation for a system without a jammer.

VI. Simulation Results

In this section, we provide numerical examples of the secrecy performance in the WPCN with an EH jammer and an eavesdropper. We adopt the distance-dependent path loss model such that $L_{\mathsf{XY}} = 10^{-3} d_{\mathsf{XY}}^{-3}$, $\forall \mathsf{X},\mathsf{Y} \in \{S, U, J, E\}$, where d_{XY} is the distance between node X and Y as in [10] and [18]. From the H-AP, the user and the jammer have fixed positions with distance d_{SU} and d_{SJ}, respectively. Also, the eavesdropper is randomly placed with distance d_{UE} from the user. The bandwidth W, the EH efficiency and the portion of the harvested energy for transmission are set to $W = 1$ MHz, $\eta_{\mathsf{X}} = 0.5, \forall \mathsf{X}$ and $\zeta_{\mathsf{X}} = 0.7, \forall \mathsf{X}$, respectively. Furthermore, we set the noise power $\sigma_{\mathsf{X}}^2 = -160$ dBm/Hz, $\forall \mathsf{X}$. The threshold secrecy rate is fixed as $r_{th} = 100$ kbps. Throughout this section, the secrecy performance is averaged over both channel realizations and the locations of the user and the eavesdropper.

We compare our proposed solutions with the following schemes.

- *Information rate maximization scheme (IRM)*: The throughput at the H-AP is maximized without consideration of the eavesdroppers [10].
- *Equal time allocation (ETA)*: The ET and the IT phases are equally divided as $\tau = 0.5$.
- *Without jammer*: The WPCN with no EH jammer is employed as $\zeta_J = 0$.

Fig. 2 shows the secrecy outage probability as a function of τ with $P_s = 100$ mW, $d_{SU} = 5$ m, $d_{SJ} = 5$ m and $d_{UE} = 5$ m. It is observed that our analysis in (7) and (12) well predict the numerical secrecy outage performance. Interestingly, we note that the minimum outage point is quite different between the cases with and without the EH jammer. One possible explanation for this difference is that the "w/o Jammer" can be considered as the system with an EH jammer that is located extremely far away from all the other nodes. In this case, it might be inefficient to spend a large amount of time for ET because the jammer barely harvests any energy regardless of τ. Thus, a better choice is likely to allocate most of the time resource for IT and just an enough portion for the ET phase so that the user can transmit with sufficient power.

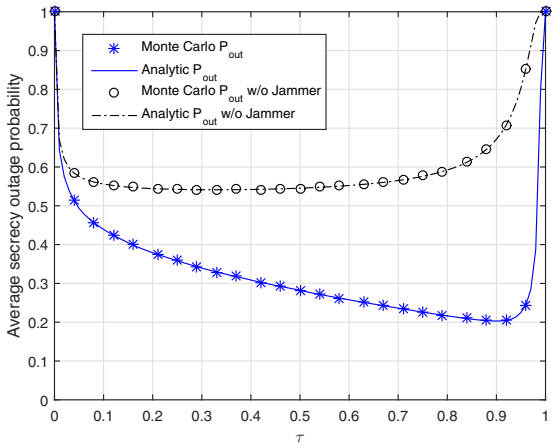

Fig. 2. Average secrecy outage probability as a function of τ where where $P_S = 100$ mW $d_{SU} = 5$ m, $d_{SJ} = 5$ m and $d_{UE} = 5$ m

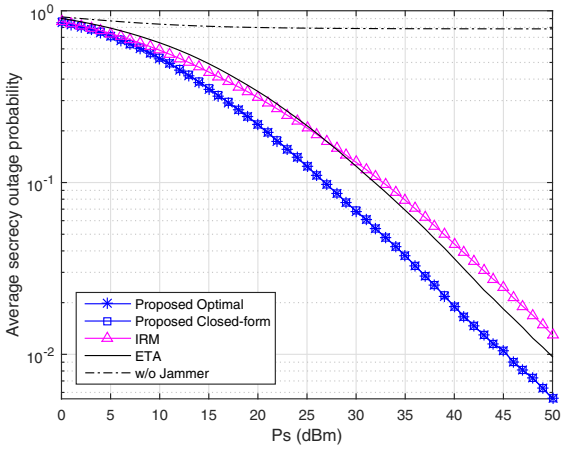

Fig. 3. Average secrecy outage probability as a function of P_S where $d_{SU} = 6$ m, $d_{SJ} = 3$ m and $d_{UE} = 4$ m

Fig. 3 illustrates the average secrecy outage probability performance as a function of P_S with $d_{SU} = 6$ m, $d_{SJ} = 3$ m and $d_{UE} = 4$ m. It is confirmed that the closed-form solution approaches the optimum in all P_S ranges. We also see that the proposed schemes outperform the IRM and the ETA. In particular, there is about 6 dB gain compared to the IRM at the outage probability of 0.1, and the gain increases with P_S.

In Fig. 4, we compare the secrecy outage probability by increasing the threshold secrecy rate r_{th} when $P_S = 100$ mW, $d_{SU} = 6$ m, $d_{SJ} = 3$ m, and $d_{UE} = 4$ m. Interestingly, when there is no specific threshold secrecy outage imposed, i.e., $r_{th} = 10^{-6}$ bps/Hz $\simeq 0$ bps/Hz, the outage probability approaches zero with the proposed schemes while it is lower bounded when the other compared schemes are employed. We can interpret each bound as the percentage of instances

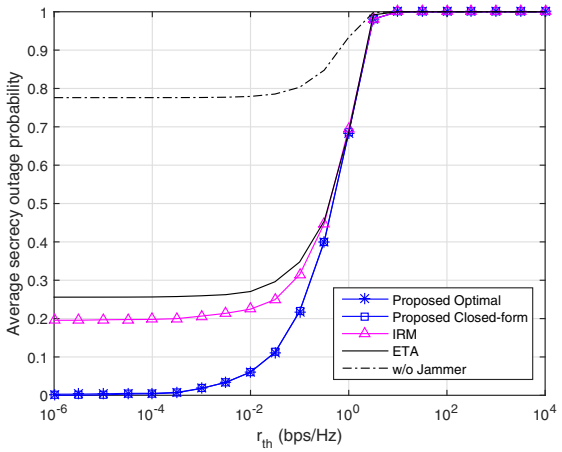

Fig. 4. Average secrecy outage probability as a function of r_{th} where $P_S = 100$ mW, $d_{SU} = 6$ m, $d_{SJ} = 3$ m and $d_{UE_m} = 4$ m

that perfect security is not guaranteed even with appropriate time allocation. For example, without a jammer, although we optimally adjust the duration of ET and IT, secrecy outage occurs with probability of 0.75, which is undesirably high. From the figures, we can thus conclude that the proposed scheme significantly improves the secrecy outage probability compared to other schemes.

VII. Conclusion

In this paper, we have investigated the optimal time allocation method for a secure WPCN with the aid of an EH jammer in the presence of an eavesdropper when only CDI of the eavesdropper is known. We have derived an analytic expression for the secrecy outage probability and found the optimal solution and a closed-form time allocation that minimize the secrecy outage probability. The numerical examples have validated the proposed methods and confirmed the effect of the EH jammer on the secrecy performance. We also have demonstrated that the proposed closed-form solution achieves almost the same performance of the optimal scheme with much reduced complexity.

References

[1] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless Networks with RF Energy Harvesting: A Contemporary Survey," *IEEE Communications and Surveys & and Tutorials*, vol. 17, pp. 757–789, Second quarter 2015.

[2] H. Ju and R. Zhang, "Optimal Resource Allocation in Full-Duplex Wireless-Powered Communication Network," *IEEE Transactions on Communications*, vol. 62, pp. 3528–3540, October 2014.

[3] L. R. Varshney, "Transporting Information and Energy Simultaneously," *in Proc. IEEE International Symposium on Inofrmation Theory*, pp. 1612–1616, July 2008.

[4] R. Zhang and C. K. Ho, "MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer," *IEEE Transactions on Wirless Communications*, vol. 12, pp. 1989–2001, May 2013.

[5] J. Xu, L. Liu, and R. Zhang, "Multiuser MISO Beamforming for Simultaneous Wireless Information and Power Transfer," *IEEE Transactions on Signal Processing*, vol. 62, pp. 4798–4810, September 2014.

[6] J. Park and B. Clerckx, "Joint Wireless Information and Energy Transfer in a K-user MIMO Interference Channel," *IEEE Transactions on Wireless Communications*, vol. 13, pp. 5781–5796, October 2014.

[7] H. Lee, S.-R. Lee, K.-J. Lee, H.-B. Kong, and I. Lee, "Optimal Beamforming Designs for Wireless Information and Power Transfer in MISO Interference Channels," *IEEE Transactions on Wirless Communications*, vol. 14, pp. 4810–4821, September 2015.

[8] X. Gui, Z. Zhu, and I. Lee, "Sum Rate Maximizing in a Multi-user MIMO System with SWIPT," *in Proc. IEEE Vehicular Technology Conference (VTC)*, pp. 1–5, May 2015.

[9] Z. Zhu, K.-J. Lee, Z. Wang, and I. Lee, "Robust Beamforming and Power Splitting Design in Distributed Antenna System with SWIPT under Bounded Channel Uncertainty," *in Proc. IEEE Vehicular Technology Conference (VTC)*, pp. 1–5, May 2015.

[10] H. Ju and R. Zhang, "Throughput Maximization in Wireless Powered Communication Networks," *IEEE Transactions on Wirless Communications*, vol. 13, pp. 418–428, January 2014.

[11] H. Lee, K.-J. Lee, H. Kim, B. Clerckx, and I. Lee, "Resource Allocation Techniques for Wireless Powered Communication Networks with Energy Storage Constraint," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 2619–2628, April 2016.

[12] H. Kim, H. Lee, M. Ahn, H.-B. Kong, and I. Lee, "Joint Subcarrier and Power Allocation Method in Wireless Powered Communication Networks for OFDM Systems," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 1–9, July 2016.

[13] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, pp. 1550–1573, Third quarter 2014.

[14] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 2180–2189, June 2008.

[15] X. Zhou and M. R. McKay, "Secure Transmission with Artificial Noise over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 3831–3842, October 2010.

[16] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy Wireless Information and Power Transfer with MISO Beamforming," *IEEE Transactions on Signal Processing*, vol. 64, pp. 1850–1863, April 2014.

[17] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 13, pp. 4599–4615, August 2014.

[18] H. Xing, L. Liu, and R. Zhang, "Secrecy Wireless Information and Power Transfer in Fading Wiretap Channel," *IEEE Transactions on Vehicular Technology*, vol. 65, pp. 180–190, January 2016.

[19] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure Communication with a Wireless-Powered Friendly Jammer," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 401–415, January 2016.

[20] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-Scale MIMO Relaying Techniques for Physical Layer Security: AF or DF?," *IEEE Transacations on Wireless Communications*, vol. 14, pp. 5135–5146, September 2015.

[21] R. Corless, G. Gonnet, D. Hare, D. Jeffery, and D. Knuth, "On the Lambert W Function," *Advances in Computational Mathematics*, vol. 5, pp. 329–359, 1996.