Time Allocation Methods for Secure Wireless Powered Communication Networks

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

***Abstract*—In this work, we investigate a wireless powered communication network (WPCN) where multiple eavesdroppers attempt to intercept the information between a hybrid access-point (H-AP) and an energy harvesting (EH) user. During the first energy transfer (ET) phase, the EH user and an EH cooperative jammer harvest energy from the transmitted signals of the H-AP. Then, in the next information transfer (IT) phase, the user sends confidential information to the H-AP while the jammer broadcasts artificial noises to the eavesdroppers by utilizing their previously harvested energy. We particularly consider optimization of the time allocation between the ET and the IT phases by which the secrecy rate is maximized. To cut down a computational burden, a low-complexity closed-form solution of the time allocation factor with some interesting behaviors will be proposed by a worst-case approximation. Through simulation results, we evaluate the performance of our proposed scheme and show that a performance gain compared to conventional schemes becomes clearer with the increased number of eavesdroppers.**

***Index Terms*—Physical-layer security, cooperative jammer, artificial noise (AN), energy harvesting (EH), wireless powered communication networks (WPCN).**

I. Introduction

In recent years, energy harvesting (EH) utilizing wireless radio frequency signals has been regarded as a promising alternative to providing energy sources in communication networks [1]. Specifically, simultaneous wireless information and power transfer (SWIPT) and wireless powered communication networks (WPCN) are two main branches of EH systems that have drawn a lot of attentions [2]. In the SWIPT, transmitted signals convey both information and energy to simultaneously achieve information delivery and wireless energy recharging [3]–[8]. In contrast, for the WPCN, a hybrid access-point (H-AP) first broadcasts energy-carrying signals to recharge EH nodes in an energy transfer (ET) phase, and then the EH nodes transmit information signals in a subsequent information transfer (IT) phase by utilizing the energy harvested in the previous ET phase [9]–[11].

Meanwhile, physical-layer security issues in communications have also been brought up for the last decades [12]. One of the technologies for enhancing the secrecy performance is to transmit artificial noises (AN) on top of the transmitted signals to interfere eavesdroppers [13]. The authors in [14] and [15] recently considered the physical-layer security in SWIPT with the AN employed at the transmitter side by treating EH receivers as potential eavesdroppers. For WPCN, the authors of [16] introduced two-phase secure EH communications with an EH jammer and an eavesdropper, and obtained the maximum throughput based on a secrecy outage probability constraint. In all the aforementioned works, however, the trade-off between the ET and the IT durations for a wiretap WPCN was not explicitly studied.

Motivated by this need, a recent work in [17] discovered some effective resource allocation methods in wiretap WPCNs. However, the approach in [17] to finding ET and IT durations to maximize the secrecy rate requires a number of iterative subgradient methods, which significantly increases computational complexity. In this paper, we consider a WPCN with an EH jammer and multiple eavesdroppers which attempt to intercept the information between an EH user and an H-AP. During the first ET phase, the EH user and an EH cooperative jammer harvest energy from the transmitted signals of the H-AP. Then, in the next IT phase, the user sends secret information to the H-AP while the jammer broadcasts AN to the eavesdroppers by utilizing their previously harvested energy. Under this system, we first review the optimization of the time allocation between the ET and the IT phases that maximizes secrecy rate. It will be shown that the secrecy rate with respect to each eavesdropper is strongly quasi-concave in the time allocation factor, and thus a globally optimal solution is obtained by applying a subgradient method. To further reduce a computational burden, we will propose a low-complexity closed-form solution with some interesting behaviors by a worst-case approximation. Finally, simulation results evaluate the secrecy performance of our proposed scheme by comparing with conventional ones.

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

Fig. 1 depicts our system model for the WPCN where an H-AP (S), a dedicated EH user (U), an EH jammer (J), and multiple eavesdroppers (E_m for $m = 1, ..., M$) 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] [9], where

This work was supported by the National Research Foundation through the Ministry of Science, ICT, and Future Planning (MSIP), Korean Government under Grant 2017R1A2B3012316.

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

H. Lee is with Information Systems Technology and Design (ISTD) pillar, Singapore University of Technology and Design (SUTD), Singapore (e-mail: hoon_lee@sutd.edu.sg).

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).

978-1-5386-6358-5/18/$31.00 ©2018 IEEE

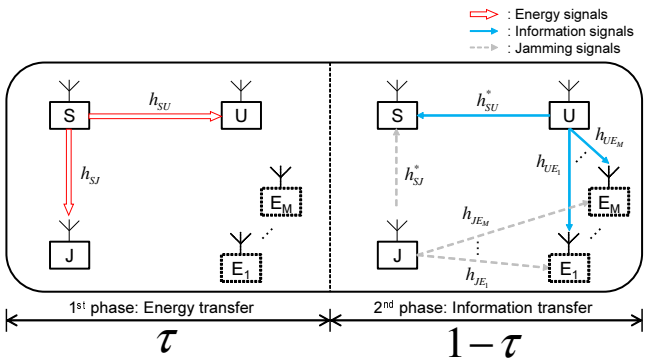

Fig. 1. Schematic diagram for the two-phase WPCN

the H-AP first broadcasts an energy signal during 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 information signal and AN, respectively, in the subsequent 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 channel coefficient from node X to Y by $h_{\mathsf{XY}} \in \mathbb{C}$ where $\mathsf{X},\mathsf{Y} \in \{S, U, J, E_m \forall m\}$. Assuming quasi-static flat-fading, all channel gains stay constant during each time block. Also, each eavesdropper is temporarily regarded as an inactive user that may participate in communications in the future [16]. Then, we assume that the channel state information of h_{JE_m} and h_{UE_m}, $\forall m$, as well as the legitimate channel h_{SU} and h_{SJ} are all available to the network.[1]

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

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

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]

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

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 the eavesdroppers. To combat this security issue, the jammer simultaneously generates AN $x_J \sim \mathcal{CN}(0,1)$ to reduce the eavesdroppers' decoding capacity.[2] Then, the received signal at the information receiving node $\mathsf{X}_I \in \{S, E_m \forall m\}$ is given by

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

[1]The channel state information of eavesdroppers can be estimated by detecting the inevitably leaked local oscillator power from eavesdroppers' receiver RF front-ends and deploying additional nodes called *torches* [18] [19].

[2]The worst case AN is known to be Gaussian [13].

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 AN 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 [15]. Then, the signal-to-noise ratio (SNR) at the H-AP and the signal-to-interference-plus-noise ratio (SINR) at the m-th eavesdropper E_m result in

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

$$\text{SINR}_{E_m} = \frac{|h_{UE_m}|^2 P_U}{|h_{JE_m}|^2 P_J + \sigma^2_{E_m}} = \frac{\tau B_m}{\tau(C_m - 1) + 1}, \quad (3)$$

where $A \triangleq \zeta_U \eta_U |h_{SU}|^4 P_S / \sigma^2_S$, $B_m \triangleq \zeta_U \eta_U |h_{SU}|^2 |h_{UE_m}|^2 P_S / \sigma^2_{E_m}$ and $C_m = \zeta_J \eta_J |h_{SJ}|^2 |h_{JE_m}|^2 P_S / \sigma^2_{E_m}$.

By examining (2) and (3), one can show that the secrecy rate equals [14]

$$r_s = \min_m \quad r_{s,m}, \quad (4)$$

where $r_{s,m} \triangleq W(1-\tau)[\log_2(1+\text{SNR}_S) - \log_2(1+\text{SINR}_{E_m})]^+$ denotes the secrecy rate against the m-th eavesdropper with W being the system bandwidth. This leads to a secrecy rate maximization problem as

$$(\text{P1}): \max_{\tau} \; r_s$$
$$\text{s.t.} \;\; 0 < \tau < 1.$$

In what follows, we first study a globally optimal time allocation factor τ_{opt} by exploiting some functional characteristics of r_s. We then present a closed-form solution τ_{cl} by applying a worst-case approximation to further reduce the computational complexity and provide useful insights. For a benchmark scheme, the conventional WPCN without a jammer will be briefly discussed as well.

III. Optimal Solution for Secrecy Rate Maximization

In this section, we review the optimal solution τ_{opt} of (P1) as in [17]. To this end, we first state the following lemma which identifies a feasible region of τ to ensure a positive secrecy rate.

Lemma 1: $r_{s,m}$ is positive for $\tau_{0,m} < \tau < 1$, where $\tau_{0,m} \triangleq \left[\frac{B_m - A}{AC_m + B_m - A}\right]^+$.

Proof: From (4), we have $r_{s,m} > 0$ when $\text{SNR}_S > \text{SINR}_{E_m}$, which reduces to $\tau((AC_m + B_m - A)\tau - (B_m - A)) > 0$. First, when $AC_m + B_m - A \le 0$, it is obvious that $B_m - A < 0$ since $AC_m > 0$. Therefore, $r_{s,m}$ is positive for $\tau > 0$ and $AC_m + B_m - A = 0$, or for $0 < \tau < 1 < \frac{B_m - A}{AC_m + B_m - A}$ and $AC_m + B_m - A < 0$.

On the other hand, when $AC_m + B_m - A > 0$, $r_{s,m}$ is positive for $\tau > 0$ and $B_m - A < 0$, or for $\frac{B_m - A}{AC_m + B_m - A} < \tau < 1$ and $B_m - A \ge 0$. Combining these results completes the proof. ■

Based on Lemma 1, let us reformulate (P1) into an equivalent form by introducing a new variable $z > 0$ as

$$(\text{P1.1}): \max_{z,\tau} \; z \tag{5a}$$

$$\text{s.t.} \;\; r_{s,m} \geq z, \; \forall m, \tag{5b}$$

$$\tau_{0,m} < \tau < 1, \; \forall m. \tag{5c}$$

To solve (P1.1), we first consider the feasibility of the problem by fixing z and define $\mathcal{Q}_m \triangleq \{\tau \in \mathbb{R} | r_{s,m} \geq z, \; \tau_{0,m} < \tau < 1\}$ such that the feasible set of (P1.1) is denoted as $\mathcal{Q} = \cap_{m=1}^{M} \mathcal{Q}_m$. Then, we obtain each $\mathcal{Q}_m$ with the aid of the following theorem.

Theorem 1: The secrecy rate $r_{s,m}$ for the m-th eavesdropper is a strongly quasi-concave function with respect to τ for $\tau_{0,m} < \tau < 1$.

Proof: See Appendix B in [17]. ∎

With Theorem 1, any stationary point of $r_{s,m}$ represents the global maximum. Hence, we can easily determine the convex sets $\mathcal{Q}_m$ by utilizing sub-gradient methods such as the bisection method [20] with a given z. After that, the optimal z for (P1.1) is computed by investigating the convex intersection $\mathcal{Q}$, which can be rewritten as $\mathcal{Q} = \{\tau \in \mathbb{R} | \tau_{\mathcal{Q},\min} \leq \tau \leq \tau_{\mathcal{Q},\max}\}$, where $\tau_{\mathcal{Q},\min} \triangleq \min_{\tau \in \mathcal{Q}} \tau$ and $\tau_{\mathcal{Q},\max} \triangleq \max_{\tau \in \mathcal{Q}} \tau$. In case of $\mathcal{Q} = \emptyset$, z should be decreased to have a non-empty feasible region. Otherwise, if $\mathcal{Q} \neq \emptyset$, we can infer that a higher secrecy rate is still achievable and increase z. This iteration can be done by the bisection method as well. A detailed updating procedure of z is summarized in Algorithm 1.

Algorithm 1. Optimal time allocation method for secrecy rate maximization

Initialize $z_{\max}$ and $z_{\min}$.
Repeat
  Set $z = \frac{z_{\max}+z_{\min}}{2}$.
  Determine the sets $\mathcal{Q}_m, \forall m$ and $\mathcal{Q} = \bigcap_{m=1}^{M} \mathcal{Q}_m$.
  If $\mathcal{Q} = \emptyset$, $z_{\max} = z$; otherwise, $z_{\min} = z$.
Until $|z_{\max} - z_{\min}|$ converges.
Set $\tau_{\text{opt}} = \frac{\tau_{\mathcal{Q},\min}+\tau_{\mathcal{Q},\max}}{2}$.

IV. Closed-form Solution for Secrecy Rate Maximization

We now provide a closed-form solution for (P1) in order to reduce the computational complexity of the optimal algorithm in [17] and provide some insightful results. Consider the worst-case scenario where the noise is absent at eavesdroppers as in [13] and [16], i.e., $\sigma_{E_m}^2 = 0, \forall m$ in (3). This assumption leads to a lower bound of the secrecy rate $r_s \geq r_{s,\text{LB}}$, where

$$r_{s,\text{LB}} \triangleq \min_m W(1-\tau)\left[\log_2\left(1+A\frac{\tau}{1-\tau}\right)-\log_2\left(1+\frac{\tilde{B}_m}{\tilde{C}_m}\right)\right]^+$$
$$= W(1-\tau)\left[\log_2\left(1+A\frac{\tau}{1-\tau}\right)-\log_2\left(1+\frac{\tilde{B}_{\bar{m}}}{\tilde{C}_{\bar{m}}}\right)\right]^+,$$

with $\tilde{B}_m \triangleq \zeta_U \eta_U |h_{SU}|^2 |h_{UE_m}|^2 P_S$, $\tilde{C}_m \triangleq \zeta_J \eta_J |h_{SJ}|^2 |h_{JE_m}|^2 P_S$ and $\bar{m} \triangleq \arg\max_m \frac{\tilde{B}_m}{\tilde{C}_m}$.

Similar to Lemma 1, a positive $r_{s,\text{LB}}$ in this case is achieved for $\frac{\tilde{B}_{\bar{m}}}{A\tilde{C}_{\bar{m}}+\tilde{B}_{\bar{m}}} < \tau < 1$, and it can be easily shown that $r_{s,\text{LB}}$ is a concave function on this region, since its second derivative is always negative. Thus, letting the first derivative equal to zero and applying some mathematical manipulations, we obtain the following closed-form solution as

$$\tau_{\text{cl}} = \frac{1 - \frac{\mathcal{W}_{L,0}\left(\frac{\tilde{C}_{\bar{m}}}{\tilde{B}_{\bar{m}}+\tilde{C}_{\bar{m}}}(A-1)e^{-1}\right)}{(A-1)}}{\mathcal{W}_{L,0}\left(\frac{\tilde{C}_{\bar{m}}}{\tilde{B}_{\bar{m}}+\tilde{C}_{\bar{m}}}(A-1)e^{-1}\right)+1}, \tag{6}$$

where $\mathcal{W}_{L,k}(\cdot)$ stands for the Lambert W function with a specific branch k [21].

Let us investigate this solution in different SNR regimes. First, for the case of low $\text{SINR}_{E_{\bar{m}}}$, i.e., $\tilde{B}_{\bar{m}} \ll \tilde{C}_{\bar{m}}$, the closed-form solution (6) is approximated as

$$\tau_{\text{cl}} \simeq \frac{1 - \frac{\mathcal{W}_{L,0}((A-1)e^{-1})}{(A-1)}}{\mathcal{W}_{L,0}((A-1)e^{-1})+1}, \tag{7}$$

which corresponds to a solution of the conventional information rate maximization WPCN without an eavesdropper [9]. Note that $\mathcal{W}_{L,0}(x)$ is a monotonically increasing function for $x > 0$, and we have $\lim_{x\to\infty} \frac{\mathcal{W}_{L,0}(x)}{x} = 0$ by L'Hôpital's rule. Therefore, in this case, the allocated time for the ET phase reduces as a user gets closer to the H-AP or, equivalently, as A increases.

However, if there exist non-negligible eavesdroppers, i.e., $\tilde{B}_{\bar{m}} \gg \tilde{C}_{\bar{m}}$, (6) approaches

$$\tau_{\text{cl}} \simeq \frac{1 - \frac{\mathcal{W}_{L,0}((A-1)(\frac{\tilde{C}_{\bar{m}}}{\tilde{B}_{\bar{m}}})e^{-1})}{(A-1)}}{\mathcal{W}_{L,0}((A-1)(\frac{\tilde{C}_{\bar{m}}}{\tilde{B}_{\bar{m}}})e^{-1})+1},$$

and it implies that the time duration for the ET increases as $\text{SINR}_{E_{\bar{m}}}$ or, equivalently, as $\frac{\tilde{B}_{\bar{m}}}{\tilde{C}_{\bar{m}}}$ grows. In other words, more time resource is allocated for the ET so that the jammer can satisfactorily interrupt the eavesdroppers with sufficient harvested energy.

V. A Case without an EH Jammer

So far, we have assumed that the EH jammer always operates in the network. As a benchmark scheme, we now consider the conventional WPCN without a jammer, which corresponds to $\zeta_J = 0$. In this case, $r_{s,m}$ in (4) reduces to

$$\hat{r}_{s,m}$$
$$= W(1-\tau)\left[\log_2\left(1+A\frac{\tau}{1-\tau}\right)-\log_2\left(1+B_m\frac{\tau}{1-\tau}\right)\right]^+.$$

Different from Lemma 1 where there always exists a certain positive secrecy rate region, $\hat{r}_{s,m}$ attains a positive value for $0 < \tau < 1$ only when $A > B_m$. Otherwise, $r_{s,m}$ is zero for the whole time block. We can easily interpret this condition as that the effective eavesdropping channel gain B_m must be a degraded form of the legitimate channel gain A from the first place. Moreover, for $A > B_m$, $\hat{r}_{s,m}$ is concave with respect to τ, since its second derivative can be shown to be always negative. Thus, as long as $A > B_m, \forall m$, we can apply Algorithm 1 in a similar fashion to determine the optimal time allocation for a system without a jammer.

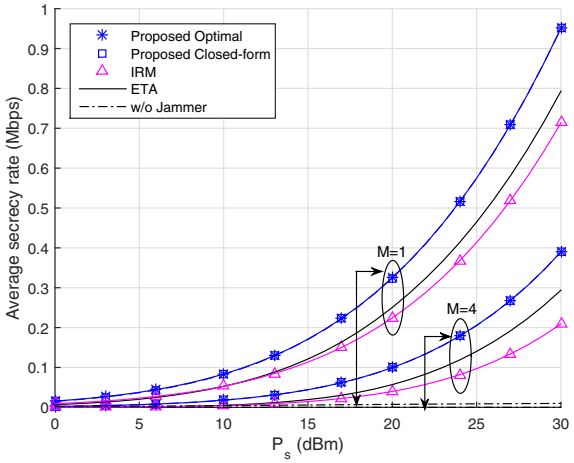

Fig. 2. Average secrecy rate comparison as a function of P_S where $d_{SU} = 5$ m, $d_{SJ} = 4$ m and $d_{UE_m} = 1$ m

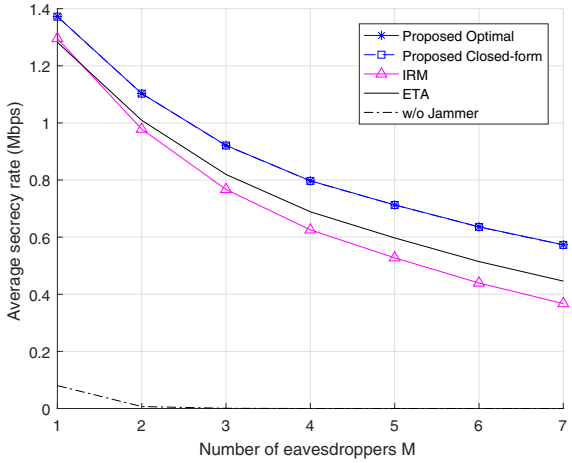

Fig. 3. Average secrecy rate comparison as a function of the number of eavesdroppers M with $P_S = 500$ mW, $d_{SU} = 7$ m and $d_{SJ} = 2$ m, while d_{UE_m} is randomly selected from 1 m to 5 m

VI. Simulation Results

In this section, we provide numerical examples of the secrecy performance in the WPCN with an EH jammer. We adopt the distance-dependent path loss model such that $|h_{\mathsf{XY}}|^2 = 10^{-3} d_{\mathsf{XY}}^{-3} |\mathsf{h}_{\mathsf{XY}}|^2$, $\forall \mathsf{X},\mathsf{Y} \in \{S, U, J, E_m \forall m\}$, where d_{XY} and h_{XY} are the distance and the small-scale channel coefficient between node X and Y, respectively as in [9] and [15]. From the H-AP, the user and the jammer have a fixed position with distance d_{SU} and d_{SJ}, respectively. Also, the eavesdroppers are randomly placed with distance d_{UE_m} from the user for $m = 1, ..., M$.

The bandwidth, the EH efficiency and the portion of the harvested energy for transmission of users are fixed as $W = 1$ 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, $\forall \mathsf{X}$. Throughout this section, the secrecy performance is averaged over both channel realizations and the locations of the nodes, and our proposed solutions are compared with the following schemes.

- *Information rate maximization scheme (IRM)*: The throughput at the H-AP is maximized without consideration of the eavesdroppers [9].
- *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 illustrates the secrecy rate as a function of the transmit power P_S at the H-AP with $d_{SU} = 5$ m, $d_{SJ} = 4$ m and $d_{UE_m} = 1$ m, $\forall m$. We assume all the small-scale channel coefficients follow Rayleigh distributions. In the plot, we see that the IRM is even worse than the ETA from the perspective of secrecy performance. Specifically, with $P_S = 30$ dBm, we observe that the proposed schemes outperform the IRM by 33 % when $M = 1$ and it almost doubles when $M = 4$. One interesting observation is that a system without the EH jammer hardly achieves any secrecy rate, which verifies the importance of the jammer in the wiretap WPCN. We also confirm that the closed-form solution provides almost optimal performance for all cases with much reduced complexity.

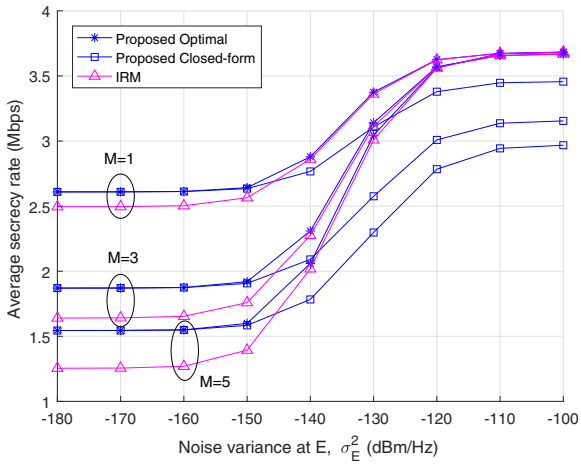

Fig. 4. Average secrecy rate comparison as a function of $\sigma_{E_m}^2$ with $P_S = 500$ mW, $d_{SU} = 5$ m, $d_{SJ} = 2$ m and d_{UE_m}=2 m

Fig. 3 exhibits the average secrecy rate with different numbers of eavesdroppers. We set $P_S = 500$ mW, $d_{SU} = 7$ m and $d_{SJ} = 2$ m, while d_{UE_m} is randomly selected from 1 m to 5 m. In addition, we assume the legitimate channel coefficients h_{SJ} and h_{SU} follow Rician distributions with K factor of 5, while others follow Rayleigh distribution as usual. The figure demonstrates that as the number of eavesdroppers increases, a performance gain of the proposed schemes becomes higher compared to the conventional methods which do not properly consider the presence of eavesdroppers. For instance, we have a 55 % gain over the IRM with 7 eavesdroppers, although the gain is small with just one eavesdropper. Also, the closed-form solution performs almost the same as the optimum. When there is no EH jammer, however, secure communication is nearly impossible.

In Fig. 4, we examine the effect of the noise power $\sigma_{E_m}^2$ at the eavesdroppers on the secrecy rate performance with $P_S = 500$ mW, $d_{SU} = 5$ m, $d_{SJ} = 2$ m and d_{UE_m}=2 m. Ob-

viously, the closed-form solution attains nearly global optimal performance when the noise power is relatively low. On the other hand, as the magnitude of $\sigma_{E_m}^2$ increases, the proposed closed-form solution shows some degradation in its secrecy rate compared to the global optimal and IRM. However, since high $\sigma_{E_m}^2$ means that the eavesdroppers are not capable of satisfactorily decoding eavesdropped signals anyhow, the low $\sigma_{E_m}^2$ range is much more important place to consider when designing a secure WPCN. Hence, our proposed closed-form scheme is practically worth. We also emphasize from Fig. 4 that by simply switching between the closed-form solution and the IRM solution depending on $\sigma_{E_m}^2$, we can design a uniformly low-complexity secure WPCN in all $\sigma_{E_m}^2$ ranges since the solution for IRM scheme is also obtained closed-form as in (7).

From the figures, we can thus conclude that the proposed schemes significantly improve the secrecy rate, and the performance gain becomes more pronounced with the increased number of eavesdroppers compared to other schemes. Also, note that the closed-form solution achieves nearly optimal secrecy rate in most cases.

VII. Conclusion

In this work, we have investigated time allocation methods for a secure WPCN with the aid of an EH jammer in the presence of eavesdroppers. We have particularly obtained both optimal and closed-form time allocations for the ET and the IT phases which maximize the secrecy rate. The numerical examples have evaluated these proposed methods and confirmed the remarkable effect of the EH jammer on the secrecy performance. We have also 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] 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.

[6] 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.

[7] 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.

[8] Z. Zhu, Z. Wang, K.-J. Lee, Z. Chu, and I. Lee, "Robust transceiver designs in multiuser MISO broadcasting with simultaneous wireless information and power transmission," *Journal of Communications and Networks*, vol. 18, pp. 173–181, April 2016.

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

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

[16] 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.

[17] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy performance optimization for wireless powered communication networks with an energy harvesting jammer," *IEEE Transactions on Communications*, vol. 65, pp. 764–774, February 2017.

[18] A. Mukherjee and A. L. Swindlehurst, "Detecting Passive Eavesdroppers in the MIMO Wiretap Channel," *in Proc. IEEE ICASSP*, pp. 2809–2812, March 2012.

[19] Y. Choi and D. Kim, "Performance Analysis with and without Torch Node in Secure Communications," *in Proc. IEEE International Conference on Advanced Technologies for Communications (ATC)*, pp. 84–87, October 2015.

[20] S. Boyd and L. Vanderberghe, *Convex Optimization*. Cambridge University Press, 2004.

[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.