Secrecy Performance Optimization for Wireless Powered Communication Networks With an Energy Harvesting Jammer

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

***Abstract*— In this paper, we consider a wireless powered communication network with an energy harvesting (EH) jammer where eavesdroppers try to wiretap the communication between users 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 users and the EH jammer in the energy transfer (ET) phase. Then, in the subsequent information transfer (IT) phase, each user sends information to the H-AP in a time division multiple access manner, while the jammer generates jamming signals to interfere the eavesdroppers. We adopt two different secrecy performance measurements according to the level of channel state information (CSI) of the eavesdroppers. First, with a single user, we maximize the secrecy rate by optimizing the time allocation between the ET and the IT phase when perfect CSI of the eavesdroppers is available at all nodes. In contrast, when the instantaneous CSI of the eavesdroppers is not available at legitimate nodes, we analyze and minimize the secrecy outage probability. We also extend the single user analysis to a more general multi-user situation with an additional consideration of the transmit power allocation at the jammer. Finally, we evaluate the performance of our proposed solutions through simulations and demonstrate that a performance gain compared to conventional schemes becomes more pronounced with the increased number of eavesdroppers and users.**

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

I. Introduction

ENERGY harvesting (EH) utilizing wireless radio frequency (RF) signal has recently 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]. Also, a rapidly growing industry on internet-of-things (IoT) has been another good application area for such a convenient wireless energy recharging method (see [2] and the references therein).

Communication systems based on the EH are divided into two mainstreams: simultaneous wireless information and power transfer (SWIPT) and wireless powered communication networks (WPCN) [3]. In the SWIPT, transmitted signals carry both information and energy to concurrently achieve information delivery and wireless energy recharging [4]–[10]. In contrast, for the WPCN, hybrid access-points (H-AP) first broadcast energy-carrying signals to recharge EH nodes in the energy transfer (ET) phase, and then the EH nodes transmit information signals in the information transfer (IT) phase by utilizing the energy harvested in the previous ET phase. Note that unlike SWIPT with a time-switching mode, users in WPCN utilize their energy for transmission rather than decoding. Many researches have focused on resource allocation problems in WPCN in order to maximize the system performance such as sum throughput [11]–[13].

In the meantime, physical-layer security issues in communications have also been brought up for the last decades [14]. One of the technologies for enhancing the secrecy performance is to transmit artificial noise (AN) on top of the transmitted signals to interfere eavesdroppers [15], [16]. The authors in [17]–[19] recently considered the physical-layer security with the AN employed at the transmitter side by treating EH receivers as potential eavesdroppers. Specifically, in [17], jointly optimal information and energy beamformers were provided to maximize the secrecy rate of an information receiver with certain EH requirements on the energy receivers. In the presence of passive EH users who can become potential eavesdroppers, beamforming vectors for information, energy, and AN signals were jointly designed in [18] for minimizing the total transmit power subject to a secrecy rate constraint. Also, a three-node wiretap channel composed of a transmitter, an information receiver and an energy receiver was studied in [19], and the optimal transmit power allocation between AN and information signals was proposed. For an EH cognitive radio network, a recent work in [20] studied a throughput maximization problem for secondary users when malicious jammers exist.

Manuscript received March 8, 2016; revised July 14, 2016 and September 14, 2016; accepted October 22, 2016. Date of publication November 1, 2016; date of current version February 14, 2017. This work was supported by National Research Foundation (NRF) funded by the Ministry of Science, ICT & Future Planning (MSIP) of Korea Government under Grant 2014R1A2A1A10049769. The work of C. Song was supported by the NRF funded by the MISP of Korea Government under Grant NRF-2015R1C1A1A02036927. The associate editor coordinating the review of this paper and approving it for publication was D. Niyato.

J. Moon, H. Lee, and I. Lee are with the School of Electrical Engineering, Korea University, Seoul 02841, South Korea (e-mail: anschino@korea.ac.kr; ihun1@korea.ac.kr; inkyu@korea.ac.kr).

C. Song is with the Department of Information and Communications Engineering, Korea National University of Transportation, Chungju 27469, South Korea (e-mail: c.song@ut.ac.kr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2016.2623627

Although many studies have investigated the secrecy performance in SWIPT, relatively less work has been done on wiretap WPCN. In [21], the authors 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. Also, the authors in [22] evaluated the secrecy rate with the aid of a relay and EH jammers. In both systems, however, the user neither harvests energy nor transmits information in uplink, thereby the trade-off between ET and IT time duration for wiretap WPCN was not explicitly analyzed.

In this paper, we consider a multi-user WPCN with an EH jammer and multiple eavesdroppers who try to wiretap the communication between the EH users and an H-AP. The H-AP recharges both the users and the jammer in the first ET phase. Then, by using the harvested energy, each user transmits information to the H-AP one at a time in a time division multiple access (TDMA) manner during the subsequent IT phase, while the jammer generates jamming signals to interfere the eavesdroppers. We investigate two different secrecy performance measures, namely secrecy rate (SR) and secrecy outage probability (SOP) according to the level of channel state information (CSI) of the eavesdroppers. In both cases, we aim to jointly optimize the time durations for ET and each user's IT phase as well as the transmit power allocation at the jammer.

First, with a single user, we maximize the SR with an assumption that perfect CSI of the eavesdroppers is available at all legitimate nodes. It will be shown that the SR for each eavesdropper is strongly quasi-concave with respect to the time allocation factor between the ET and the IT phases, and thus a globally optimal solution can be obtained by applying a simple line search method. Also, we consider a case where only channel distribution information (CDI) and the location of the eavesdroppers are known to the legitimate nodes. In this case, the optimal time allocation factor which minimizes the SOP can be determined based on an analytical expression for the SOP derived in this paper. To further reduce the computational complexity, we also propose a closed-form time allocation factor by the worst case approximation.

Next, we extend our results to a general K-user wiretap WPCN where the IT phase is divided into K time slots, each of which is dedicated to individual information transmission. Unlike the single user case where only the time durations are optimized, the transmit power allocation at the jammer should also be carefully assigned in the general multi-user case. Hence, by jointly optimizing the time duration and power allocation, we maximize the minimum SR among the users when CSI of the eavesdroppers is available and minimize the maximum SOP in the absence of the eavesdroppers' CSI. These problems are, however, generally non-convex and difficult to solve. We thus propose alternating optimization methods to provide local optimal solutions. Simulation results evaluate the secrecy performance of our proposed schemes by comparing with conventional ones.

It is worth mentioning some differences of our system from the previous works in [11] and [21]. First, unlike [21], we examine the case where users also harvest energy from the H-AP to transmit information in uplink. Thus, in our paper, the time allocation between the ET and the IT phases arises as an important parameter to optimize the secrecy performance. In addition, while the results in [21] are only valid for a single user case, our work covers general multi-user scenarios. In [11], the authors considered a problem of maximizing the sum throughput for multi-user WPCN. However, the algorithms in [11] are not directly applicable to our system, since the problems for the wiretap WPCN are generally non-convex. One of our major contributions is thus to show quasi-concavity of the SR, which plays an important role for solving the SR maximization problem.

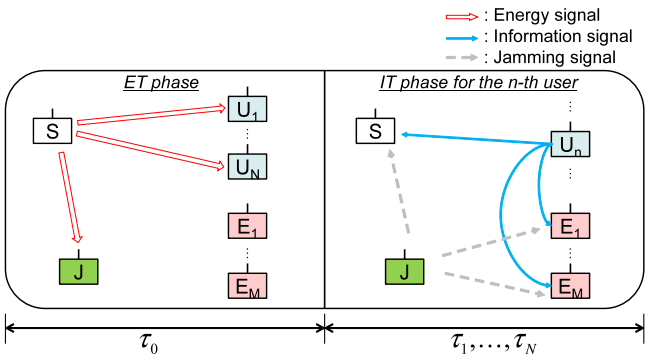

Fig. 1. Schematic diagram for the two-phase WPCN.

The remainder of the paper is organized as follows: Section II describes the system model, and Section III considers both SR maximization and SOP minimization problems for a single user WPCN. We then extend our results to a general multi-user configuration in Section IV and demonstrate the secrecy performance of our system through simulations in Section V. Lastly, Section VI 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, 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 an H-AP S, EH users U_n for $n = 1, \ldots, N$, an EH jammer J, and multiple eavesdroppers E_m for $m = 1, \ldots, M$ are equipped with a single antenna. It is assumed that the H-AP operates with a constant power supply, while the users and the jammer utilize the harvested energy from the RF signals transmitted from the H-AP. We employ the two-phase WPCN protocol [3], [11], where the H-AP first broadcasts the energy-carrying signals in the ET phase for a τ_0 proportion of the total time block, and then each user and the jammer transmit information and jamming signals, respectively, during the IT phase. To avoid co-channel interference, we assume that each user occupies the uplink channel one at a time in a TDMA manner, and thus the n-th user is assigned a τ_n 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 $\mathsf{X},\mathsf{Y} \in \{S, J, U_n \forall n, E_m \forall m\}$. Assuming quasi-static flat-fading, all channel gains stay constant during each time block. It is also assumed that both h_{SU} and h_{SJ} are perfectly known at the H-AP and the users, since channel reciprocity holds for both ET and IT phases. During these phases, each eavesdropper is temporarily regarded as an inactive user that may participate in communications in the future [21], in which the location information of the eavesdroppers and CDI of h_{JE_m} and h_{UE_m}, $\forall m$, are available to the network. In this work, we particularly consider Rayleigh distributions of $|h_{JE_m}|$ and $|h_{UE_m}|$, $\forall m$.

During the ET phase, the received signal at the energy receiving node $\mathsf{X}_e \in \{U_n \forall n, J\}$ is

$$y_{\mathsf{X}_e} = \sqrt{P_S L_{S\mathsf{X}_e}} h_{S\mathsf{X}_e} x_S + z_{\mathsf{X}_e}, \tag{1}$$

where P_S stands for the transmit power at the H-AP, $x_S \sim \mathcal{CN}(0,1)$ equals the transmitted symbol from the H-AP, and $z_{\mathsf{X}_e} \sim \mathcal{CN}(0, \sigma^2_{\mathsf{X}_e})$ indicates the complex Gaussian noise at node X_e. Then, the harvested energy at node X_e can be written by [5]

$$\mathcal{E}_{\mathsf{X}_e} = \eta_{\mathsf{X}_e} \mathbb{E}[|y_{\mathsf{X}_e}|^2]\tau_0 = \eta_{\mathsf{X}_e} P_S L_{S\mathsf{X}_e} |h_{S\mathsf{X}_e}|^2 \tau_0, \tag{2}$$

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

In the IT phase, the n-th user transmits its information signal $x_{U_n} \sim \mathcal{CN}(0,1)$ to the H-AP by utilizing the harvested energy $\mathcal{E}_{U_n}$. In our system, a security problem arises due to the presence of eavesdroppers. To combat this security issue, the jammer simultaneously generates a jamming signal $x_J[n] \sim \mathcal{CN}(0,1)$ at each time slot n of duration τ_n to reduce the eavesdroppers' decoding capacity.[1]

Then, the received signal at the information receiving node $\mathsf{X}_I \in \{S, E_m \forall m\}$ in the n-th time slot is given by[2]

$$\begin{aligned} y_{\mathsf{X}_I}[n] = &\sqrt{P_{U_n} L_{\mathsf{X}_I U_n}} h^*_{\mathsf{X}_I U_n} x_{U_n} \\ &+ \sqrt{P_J[n] L_{\mathsf{X}_I J}} h^*_{\mathsf{X}_I J} x_J[n] + z_{\mathsf{X}_I}, \end{aligned} \tag{3}$$

where $P_{U_n} \triangleq \frac{\zeta_{U_n} \mathcal{E}_{U_n}}{\tau_n}$ and $P_J[n] \triangleq \frac{\zeta_J[n] \mathcal{E}_J}{\tau_n}$ represent the transmit power with $\zeta_{U_n} \in (0,1]$ and $\zeta_J[n] \in (0,1]$ being a portion of the harvested energy used for signal transmission from node U_n and J, respectively, at the n-th time slot.

We assume that the jamming signal $x_J[n]$ is known at the H-AP, which means that the jamming interference $\sqrt{P_J[n] L_{SJ}} h^*_{SJ} x_J[n]$ in (3) can be removed at the H-AP.[3] Then, the throughput $R_S[n]$ and $R_{E_m}[n]$ at the H-AP and the m-th eavesdropper, respectively, are given by

$$R_S[n] = W\tau_n \log_2\left(1 + A[n]\frac{\tau_0}{\tau_n}\right), \tag{4}$$

$$R_{E_m}[n] = W\tau_n \log_2\left(1 + \frac{B_m[n]\tau_0}{C_m \zeta_J[n]\tau_0 + \tau_n}\right), \tag{5}$$

where W is the system bandwidth, $A[n] \triangleq \zeta_{U_n}\eta_{U_n} P_S L^2_{SU_n} |h_{SU_n}|^4/\sigma^2_S$, $B_m[n] \triangleq \zeta_{U_n}\eta_{U_n} P_S L_{SU_n} L_{U_n E_m} |h_{SU_n}|^2 |h_{U_n E_m}|^2/\sigma^2_{E_m}$, and $C_m \triangleq \eta_J P_S L_{SJ} L_{JE_m} |h_{SJ}|^2 |h_{JE_m}|^2/\sigma^2_{E_m}$. From (4) and (5), one can show that the SR during the n-th time slot equals [17]

$$r[n] = \min_m \; r_{E_m}[n], \tag{6}$$

where $r_{E_m}[n] \triangleq [R_S[n] - R_{E_m}[n]]^+$.

In this paper, we consider two different secrecy measures according to the level of the channel knowledge of eavesdroppers. First, when CSI of the eavesdroppers is perfectly known at the H-AP and the users, the problem of maximizing the minimum SR among the users can be formulated by[4]

$$\text{(P1)} \quad \max_{\{\tau_n\},\{\zeta_J[n]\}} \; \min_n \; r[n] \tag{7a}$$

$$\text{s.t.} \; \sum_{n=1}^{N} \zeta_J[n] \le \zeta_{J,\max}, \quad \sum_{n=0}^{N} \tau_n \le 1, \tag{7b}$$

where $\zeta_{J,\max} \in (0,1]$ indicates the maximum allowed proportion of the harvested energy for transmission in one time block. In (P1), we jointly optimize the jammer's power allocation $\{\zeta_J[n]\}$ and the time allocation $\{\tau_n\}$. The constraint (7b) ensures that the total jammer's transmit power does not exceed its previously harvested power.

On the other hand, if only CDI and the location information of the eavesdroppers are available at the legitimate nodes, we design the system such that the maximum SOP among the users is minimized. The SOP for each time slot duration τ_n is defined by the probability that the SR $r[n]$ falls below a certain positive threshold r_{th} as [27]

$$P_{out}[n] = \Pr(r[n] \le r_{th}), \tag{8}$$

which leads to a maximum SOP minimization problem as

$$\text{(P2)} \quad \min_{\{\tau_n\},\{\zeta_J[n]\}} \; \max_n \; P_{out}[n] \tag{9a}$$

$$\text{s.t.} \; \sum_{n=1}^{N} \zeta_J[n] \le \zeta_{J,\max}, \quad \sum_{n=0}^{N} \tau_n \le 1. \tag{9b}$$

In what follows, we first consider single user scenarios to present globally optimal solutions and provide useful insights on the system. We then extend the results to general multi-user cases.

[1]The Gaussian jamming signals are not only analytically tractable, but also practically effective for a Gaussian input and Gaussian channel [23], [24].

[2]We assume that the eavesdroppers know the predefined time allocation factors, which corresponds to the worst case scenario for the legitimate users.

[3]In order to share the jamming signal $x_J[n]$, the same set of Gaussian pseudo-random jamming signals are generated and indexed at both of the H-AP and the jammer. Then, the jammer randomly selects a seed and the corresponding index is transmitted to the H-AP in prior to jamming. Note that the indices can be securely transmitted by adopting a two-step phase-shift modulation method [19].

[4]The CSI 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* [25], [26].

III. Single User Wiretap WPCN

Throughout this section, we investigate a single user wiretap WPCN with $N = 1$. For simplicity, we drop the time slot index n, and let τ_0 be the ET phase duration while the remaining $1 - \tau_0$ is assigned for the IT phase. ζ_J is now set to $\zeta_J = \zeta_{J,\max}$. Then, the resulting single user SR then reduces to

$$\begin{aligned} r &= \min_m \; r_{E_m} \\ &= \min_m \; W(1-\tau_0)\Bigg[\log_2\left(1+\frac{\tau_0}{1-\tau_0}A\right) \\ &\qquad - \log_2\left(1+\frac{\tau_0 B_m}{\tau_0(C_m\zeta_J-1)+1}\right)\Bigg]^+. \end{aligned} \tag{10}$$

A. SR Maximization With Perfect CSI of Eavesdroppers

In this subsection, we find the optimal solution $\tau_{0,\mathrm{SR}}$ of (P1) assuming that CSI of the eavesdroppers is perfectly known at the legitimate nodes. First, the following lemma identifies a feasible region of τ_0 to ensure a positive SR.

Lemma 1: r_{E_m} is positive for $\check{\tau}_m < \tau_0 < 1$, where

$$\check{\tau}_m \triangleq \left[\frac{B_m - A}{AC_m\zeta_J + B_m - A}\right]^+.$$

Proof: See Appendix A. ∎

Based on Lemma 1, we can reformulate (P1) into an equivalent form by introducing a new variable $\nu > 0$ as

$$\begin{aligned} (\mathrm{P1.1}) \quad & \max_{\nu,\tau_0} \nu && \text{(11a)} \\ & \text{s.t. } r_{E_m} \geq \nu, \quad \forall m, && \text{(11b)} \\ & \qquad \check{\tau}_m < \tau_0 < 1, \quad \forall m. && \text{(11c)} \end{aligned}$$

To solve (P1.1), we first consider the feasibility of the problem by fixing ν and define $\mathcal{Q}_m \triangleq \{\tau_0 \in \mathbb{R} | r_{s,m} \geq \nu,\ \check{\tau}_m < \tau_0 < 1\}$ such that the feasible set of (P1.1) is denoted as $\mathcal{Q} = \bigcap_{m=1}^{M} \mathcal{Q}_m$. Then, we obtain each $\mathcal{Q}_m$ with the aid of the following theorem.

Theorem 1: The SR r_{E_m} for the m-th eavesdropper is strongly quasi-concave with respect to τ_0 for $\check{\tau}_m < \tau_0 < 1$.

Proof: See Appendix B. ∎

From Theorem 1, one can see that any stationary point of r_{E_m} represents a unique global maximum. Hence, after fixing ν, we can easily determine the convex set $\mathcal{Q}_m$ for $m = 1, \ldots, M$ by leveraging sub-gradient methods such as the bisection method [28]. Then, the optimal ν for (P1.1) is computed by investigating the convex intersection $\mathcal{Q}$, which can be rewritten as $\mathcal{Q} = \{\tau_0 \in \mathbb{R} | \tau_{0,\min} \leq \tau_0 \leq \tau_{0,\max}\}$, where $\tau_{0,\min} \triangleq \min_{\tau_0 \in \mathcal{Q}} \tau_0$ and $\tau_{0,\max} \triangleq \max_{\tau_0 \in \mathcal{Q}} \tau_0$. In case of $\mathcal{Q} = \emptyset$, ν should be decreased to have a non-empty feasible region. Otherwise, we can infer that a higher SR is still achievable, and thus we increase ν. This can be done by an outer bisection iteration. A detailed updating procedure of ν is summarized in Algorithm 1.

Algorithm 1 Optimal Time Allocation Method for SR Maximization

Initialize $\nu_{\max}$ and $\nu_{\min}$.
Repeat
  Set $\nu = \frac{\nu_{\max}+\nu_{\min}}{2}$.
  Determine the sets $\mathcal{Q}_m, \forall m$ and $\mathcal{Q} = \bigcap_{m=1}^{M} \mathcal{Q}_m$.
  If $\mathcal{Q} = \emptyset$, $\nu_{\max} = \nu$; otherwise, $\nu_{\min} = \nu$.
Until $|\nu_{\max} - \nu_{\min}|$ converges.
Set $\tau_{0,\mathrm{SR}} = \frac{\tau_{0,\min}+\tau_{0,\max}}{2}$.

B. SOP Minimization With CDI of Eavesdroppers

Now, we investigate (P2) for the case where only CDI and the location information of eavesdroppers are available at the legitimate nodes. For convenience, we make use of a monotonic transformation $s_0 = \frac{\tau_0}{1-\tau_0}$ throughout this section. First, the SOP in (8) can be rewritten as

$$\begin{aligned} P_{out} &= 1 - \Pr\left(\min_m r_{E_m} > r_{th}\right) \\ &= 1 - \prod_{m=1}^{M} \Pr(r_{E_m} > r_{th}) = 1 - \prod_{m=1}^{M}(1 - P_{out,m}), \end{aligned} \tag{12}$$

where

$$\begin{aligned} P_{out,m} &\triangleq \Pr(r_{E_m} \leq r_{th}) \\ &= \Pr\Bigg(\log_2(1+As_0) - \log_2\left(1+\frac{B_m s_0}{C_m\zeta_J s_0 + 1}\right) \\ &\qquad \leq \frac{r_{th}}{W}(1+s_0)\Bigg). \end{aligned} \tag{13}$$

Then, the following lemma shows an analytic expression of (13).

Lemma 2: For a given r_{th}, the single user SOP P_{out} is expressed as

$$P_{out} = \begin{cases} 1 - \prod_{m=1}^{M}\left(1 - \frac{G_m(s_0)}{1+G_m(s_0)} e^{-\frac{V_m(s_0)}{G_m(s_0)}}\right), & \text{if } s_0 \in \mathcal{S}, \\ 1, & \text{otherwise,} \end{cases} \tag{14}$$

where $G_m(s_0) \triangleq D_m 2^{\frac{r_{th}}{W}(1+s_0)}/(1 + As_0 - 2^{\frac{r_{th}}{W}(1+s_0)})$, $D_m \triangleq (\zeta_U\eta_U L_{SU}L_{UE_m}|h_{SU}|^2)/(\zeta_J\eta_J L_{SJ}L_{JE_m}|h_{SJ}|^2)$, $V_m(s_0) \triangleq \frac{1}{F_m s_0}$, $F_m \triangleq \zeta_J\eta_J P_S L_{SJ}L_{JE_m}|h_{SJ}|^2/\sigma^2_{E_m}$ and $\mathcal{S} \triangleq \{s_0 \in \mathbb{R} | 1 + As_0 - 2^{\frac{r_{th}}{W}(1+s_0)} > 0, s_0 > 0\}$

Proof: See Appendix C. ∎

In fact, the condition $1 + As_0 - 2^{\frac{r_{th}}{W}(1+s_0)} \leq 0$ in the previous lemma indicates instances where the channel capacity from the user to the H-AP is smaller than the threshold r_{th} such that a secrecy outage occurs for sure. Based on Lemma 2, we can rewrite (P2) as

$$\begin{aligned} (\mathrm{P2.1}) \quad & \min_{s_0} \; 1 - \prod_{m=1}^{M}\left(1 - \frac{G_m(s_0)}{1+G_m(s_0)} e^{-\frac{V_m(s_0)}{G_m(s_0)}}\right), && \text{(15a)} \\ & \text{s.t. } 1 + As_0 - 2^{\frac{r_{th}}{W}(1+s_0)} > 0 \text{ and } s_0 > 0. && \text{(15b)} \end{aligned}$$

Note that the SOP in (15a) is non-convex in general, and thus it is not easy to find the optimal solution. In the following,

we first obtain the optimal solution by decreasing the search size of s_0 for computational efficiency, and then further reduce the complexity by providing a simple closed-form solution.

1) Optimal Solution for SOP Minimization: In (15b), the function $1+As_0-2^{\frac{r_{th}}{W}(1+s_0)}$ is concave on s_0, and thus we can rewrite (15b) as $s_L < s_0 < s_U$, where $s_L > 0$ and $s_U > 0$ are determined by solving the equation $1+As_0-2^{\frac{r_{th}}{W}(1+s_0)}=0$ as

$$s_L = -\frac{W}{r_{th}\ln 2}\mathcal{W}_{L,0}(\xi) - \frac{1}{A}, \tag{16}$$

$$s_U = -\frac{W}{r_{th}\ln 2}\mathcal{W}_{L,-1}(\xi) - \frac{1}{A}. \tag{17}$$

Here, $\mathcal{W}_{L,k}(\cdot)$ stands for the Lambert W function with a specific branch k [29], and $\xi \triangleq -\frac{r_{th}}{WA}\ln 2 \cdot 2^{\frac{r_{th}}{W}(1-\frac{1}{A})}$ which is always smaller than 0.

Now, let us examine the gradient of $P_{out,m}$ with respect to $G_m(s_0)$ and $V_m(s_0)$ as

$$\nabla_{G_m(s_0),V_m(s_0)} P_{out,m} = \begin{bmatrix} \frac{\partial P_{out,m}}{\partial G_m(s_0)} \\ \frac{\partial P_{out,m}}{\partial V_m(s_0)} \end{bmatrix} = \begin{bmatrix} \frac{(G_m(s_0)V_m(s_0)+G_m(s_0)+V_m(s_0))\exp\left(-\frac{V_m(s_0)}{G_m(s_0)}\right)}{G_m(s_0)(G_m(s_0)+1)^2} \\ -\frac{\exp\left(-\frac{V_m(s_0)}{G_m(s_0)}\right)}{G_m(s_0)+1} \end{bmatrix}. \tag{18}$$

Since $\frac{\partial P_{out,m}}{\partial G_m(s_0)} > 0$ and $\frac{\partial P_{out,m}}{\partial V_m(s_0)} < 0$ for $G_m(s_0) > 0$ and $V_m(s_0) > 0$, respectively, the SOP for the m-th eavesdropper $P_{out,m}$ decreases as $G_m(s_0)$ and $V_m(s_0)$ become smaller and larger, respectively.

Meanwhile, the gradients of $G_m(s_0)$ and $V_m(s_0)$ with respect to s_0 are given by

$$\frac{\partial G_m(s_0)}{\partial s_0} = \frac{D_m(A(\ln 2 \cdot r_{th}s_0 - W) + \ln 2 \cdot r_{th})2^{\frac{r_{th}}{W}(1+s_0)}}{W\left(1+As_0-2^{\frac{r_{th}}{W}(1+s_0)}\right)^2}, \tag{19}$$

$$\frac{\partial V_m(s_0)}{\partial s_0} = -\frac{1}{F_m s_0^2}. \tag{20}$$

Note that $G_m(s_0), \forall m$ has a unique minimum stationary point at

$$s_C = \frac{W}{r_{th}\ln 2} - \frac{1}{A}, \tag{21}$$

which lies in (s_L, s_U) since $0 < -\mathcal{W}_{L,0}(\xi) < 1$ in (16) and $1 < -\mathcal{W}_{L,-1}(\xi)$ in (17) for $\xi < 0$. In contrast, $V_m(s_0)$ monotonically decreases with $s_0 > 0$ for all $m = 1, \ldots, M$. As a result, the SOP P_{out} monotonically increases over $[s_C, s_U)$, and the global minimum SOP occurs in $(s_L, s_C]$. We thus employ a one-dimensional exhaustive search method over the reduced region of $(s_L, s_C]$ for the optimal solution $s_{0,\text{SOP}}$, and the optimal time allocation factor is thereby $\tau_{0,\text{SOP}} = \frac{s_{0,\text{SOP}}}{s_{0,\text{SOP}}+1}$.

2) Closed-Form Solution for SOP Minimization: To further reduce the computational complexity for solving (P2.1), we now derive a closed-form solution $\hat{s}_{0,\text{SOP}}$. To this end, we assume that the noise power is negligible at the eavesdroppers, which leads to an upper bound of P_{out} in (14) as [15], [21]

$$P_{out,\text{UB}} = \begin{cases} 1 - \prod_{m=1}^{M}\left(1 - \frac{G_m(s_0)}{1+G_m(s_0)}\right), & \text{if } s_0 \in \mathcal{S}, \\ 1, & \text{otherwise.} \end{cases} \tag{22}$$

As $P_{out,\text{UB}}$ monotonically increases with $G_m(s_0)$, a solution $\hat{s}_{0,\text{SOP}}$ which minimizes $P_{out,\text{UB}}$ becomes the minimizer of $G_m(s_0)$, $\forall m$, i.e., $\hat{s}_{0,\text{SOP}} = s_C$ given in (21). Hence, we obtain the closed-form time allocation factor

$$\hat{\tau}_{0,\text{SOP}} = \frac{s_C}{s_C+1} = \frac{WA - r_{th}\ln 2}{WA - (1-A)r_{th}\ln 2}. \tag{23}$$

When the channel gain between the H-AP and the user is strong, i.e., large A, we can see that $\hat{\tau}_{0,\text{SOP}} \to \frac{W}{W+r_{th}\ln 2}$. In this case, a longer IT phase duration of $1-\hat{\tau}_{0,\text{SOP}}$ is allocated if higher threshold secrecy rate r_{th} is imposed on. On the contrary, when the channel gain is weak such that A is small, we have $\hat{\tau}_{0,\text{SOP}} \to 1$ regardless of r_{th}. This implies that most of the time block should be dedicated for ET so that the user can securely transmit with sufficient energy.

IV. Multi-User Wiretap WPCN

We now provide solutions for (P1) and (P2) in general multi-user cases with $N > 1$. Unlike the single user scenarios, we additionally optimize the transmit power portion $\zeta_J[n]$ at the jammer for each n-th time slot, which induces non-convexity issues in (P1) and (P2). Since it is not trivial to obtain globally optimal solutions, we resort to an alternating optimization approach between the time durations $\{\tau_n\}$ and the power allocation $\{\zeta_J[n]\}$. It will be shown that the proposed algorithms for both (P1) and (P2) guarantee at least local optimality.

A. SR Maximization With Perfect CSI of Eavesdroppers

In this subsection, we consider problem (P1) which maximizes the minimum secrecy rate among users.

1) Time Allocation: First, the time allocation factors $\{\tau_{n,\text{SR}}\}$ are obtained with given power allocation $\{\zeta_J[n]\}$. By introducing a new variable $\theta_T > 0$, we can reformulate (P1) as

$$\text{(P1.2)} \quad \max_{\{\tau_n\},\theta_T} \quad \theta_T \tag{24a}$$

$$\text{s.t. } r_{E_m}[n] \geq \theta_T, \quad \forall m, n, \tag{24b}$$

$$\sum_{n=0}^{N} \tau_n \leq 1. \tag{24c}$$

Analogous to Algorithm 1 in the single user case, the optimal θ_T can be identified by a line search method in the outer loop, while an inner problem is addressed to check the feasibility of each value of θ_T as

$$\text{(P1.2.1)} \quad \min_{\{\tau_n\}} \quad \sum_{n=0}^{N} \tau_n \tag{25a}$$

$$\text{s.t. } r_{E_m}[n] \geq \theta_T, \quad \forall m, n. \tag{25b}$$

Note that if θ_T is feasible, solutions satisfy $\sum_{n=0}^{N}\tau_n \leq 1$. Otherwise, we have $\sum_{n=0}^{N}\tau_n > 1$.

In order to solve (P1.2.1), we first fix τ_0. Then, similar to Lemma 1 in the single user case, we can prove that $r_{E_m}[n]$ is positive for $\tau_n < \min\{\left[\frac{A[n]C_m\zeta_J[n]\tau_0}{B_m[n]-A[n]}\right]^+, 1-\tau_0\}$. Also, following the proof of Theorem 1, it can be easily shown that $r_{E_m}[n]$ is a strongly quasi-concave function with respect to τ_n for $\tau_n < \min\{\left[\frac{A[n]C_m\zeta_J[n]\tau_0}{B_m[n]-A[n]}\right]^+, 1-\tau_0\}$. Therefore, the constraint (25b) for each m and n becomes a convex set defined by $\bar{Q}_m[n]$, which can be obtained by utilizing the bisection method due to strongly quasi-concavity [28].

Since the resulting feasible region $\bar{Q}_n$ of τ_n is given by the intersection of the convex sets $\bar{Q}_m[n], \forall m$ as $\bar{Q}_n = \bigcap_{m=1}^{M} \bar{Q}_m[n]$, the optimal solution $\tau_{n,\mathrm{SR}}$ of (P1.2.1) is simply $\tau_{n,\mathrm{SR}} = \min_{\tau_n \in \bar{Q}_n} \tau_n$ for $n = 1, \ldots, N$. Meanwhile, the optimal $\tau_{0,\mathrm{SR}}$ for (P1.2.1) can be computed by a one-dimensional search for $\tau_{0,\mathrm{SR}} \in (0, 1)$ such that $\sum_{n=0}^{N} \tau_{n,\mathrm{SR}}$ is minimized. Thus, by using the bisection method in the outer loop, we increase θ_T if the inner problem solutions satisfy $\sum_{n=0}^{N} \tau_{n,\mathrm{SR}} \le 1$ for the current θ_T is feasible. Otherwise, θ_T should be decreased.

2) Power Allocation: Next, we optimize the power allocation $\{\zeta_J[n]\}$ with the obtained $\{\tau_{n,\mathrm{SR}}\}$. Similar to the time allocation case, the original problem (P1) can be recast to

$$\text{(P1.3)} \quad \max_{\{\zeta_J[n]\},\theta_J} \ \theta_J \tag{26a}$$

$$\text{s.t. } r[n] \ge \theta_J, \quad \forall n, \tag{26b}$$

$$\sum_{n=1}^{N} \zeta_J[n] \le \zeta_{J,\max}, \tag{26c}$$

where $0 < \theta_J < \min_n R_S[n]$ is a new optimization variable.

We again tackle (P1.3) by finding the optimal θ_J through a line search method in the outer loop, and solve an inner feasibility problem. From (6) and some mathematical manipulations, the inner problem can be formulated as

$$\text{(P1.3.1)} \quad \min_{\{\zeta_J[n]\}} \ \sum_{n=1}^{N} \zeta_J[n] \tag{27a}$$

$$\text{s.t. } \zeta_J[n] \ge \frac{B_m[n]}{\left(2^{\frac{R_S[n]-\theta_J}{W\tau_n}}-1\right)C_m} - \frac{\tau_n}{C_m\tau_0} \triangleq \gamma_m[n], \ \forall m, n. \tag{27b}$$

Note that $\zeta_J[n]$ for the n-th time slot must simultaneously satisfy (27b) for all $m = 1, \ldots, M$. Therefore, the optimal solution $\zeta_{J,\mathrm{SR}}[n]$ of (P1.3.1) is given by $\zeta_{J,\mathrm{SR}}[n] = \max_m \gamma_m[n]$ for $n = 1, \ldots, N$. Once (P1.3.1) is solved, we increase θ_J in the outer loop if the solutions satisfy $\sum_{n=1}^{N} \zeta_{J,\mathrm{SR}}[n] \le \zeta_{J,\max}$. On the other hand, when $\sum_{n=1}^{N} \zeta_{J,\mathrm{SR}}[n] > \zeta_{J,\max}$ such that θ_J is infeasible, θ_J should be decreased. The overall procedure for the SR maximization is summarized in Algorithm 2.

In the following, let us briefly examine a convergence behavior of Algorithm 2. At each iteration, the minimum SR $\min_n r[n]$ monotonically increases, since solutions for (P1.2) and (P1.3) are the Karush-Kuhn-Tucker stationary point of (P1), provided that (P1.2) and (P1.3) are optimally solved. It is also obvious that $\min_n r[n]$ is upper bounded by some finite value. Hence, this guarantees Algorithm 2 converges to at least a local optimal point.

Algorithm 2 SR Maximization for Multi-User Wiretap WPCN

Initialize $\{\zeta_{J,\mathrm{SR}}[n]\}$ and $\theta_J = 0$.
Repeat
  Set $\theta_{T,\max}$ sufficiently large and $\theta_{T,\min} = \theta_J$.
  Repeat
    Set $\theta_T = \frac{\theta_{T,\max}+\theta_{T,\min}}{2}$.
    For $\tau_0 \in (0, 1)$, solve (P1.2.1) to obtain $\{\tau_n\}_{n=1}^{N}$.
    Set $\tau_{0,\mathrm{SR}}$ and $\{\tau_{n,\mathrm{SR}}\}_{n=1}^{N}$ such that $\sum_{n=0}^{N} \tau_{n,\mathrm{SR}}$ is minimum.
    If $\sum_{n=0}^{N} \tau_{n,\mathrm{SR}} \le 1$, $\theta_{T,\min} = \theta_T$; otherwise, $\theta_{T,\max} = \theta_T$.
  Until $|\theta_{T,\max} - \theta_{T,\min}|$ converges.
  Set $\theta_{J,\max} = \min_n R_S[n]$ and $\theta_{J,\min} = \theta_T$.
  Repeat
    Set $\theta_J = \frac{\theta_{J,\max}+\theta_{J,\min}}{2}$.
    Set $\zeta_{J,\mathrm{SR}}[n] = \max_m \gamma_m[n]$ for $n = 1, \ldots, N$.
    If $\sum_{n=1}^{N} \zeta_{J,\mathrm{SR}}[n] \le \zeta_{J,\max}$, $\theta_{J,\min} = \theta_J$; otherwise, $\theta_{J,\max} = \theta_J$.
  Until $|\theta_{J,\max} - \theta_{J,\min}|$ converges.
Until $\min_n r[n]$ converges.

B. SOP Minimization With CDI of Eavesdroppers

For this subsection, we provide a solution for (P2) which minimizes the maximum SOP among users. Following the approach in Lemma 2, the outage probability in the multi-user case can be expressed as

$$P_{out}[n] = \begin{cases} 1 - \prod_{m=1}^{M} \left(1 - \frac{\tilde{G}_m[n]}{1+\tilde{G}_m[n]} e^{-\frac{\tilde{V}_m[n]}{\tilde{G}_m[n]}}\right), & \text{if } \tau_n \in \mathcal{T}[n], \\ 1, & \text{otherwise,} \end{cases} \tag{28}$$

where $\tilde{G}_m[n] \triangleq \tilde{D}_m[n] 2^{\frac{r_{th}}{W\tau_n}}/(1 + A[n]\frac{\tau_0}{\tau_n} - 2^{\frac{r_{th}}{W\tau_n}})$, $\tilde{D}_m[n] \triangleq \frac{\zeta_{U_n}\eta_{U_n}L_{SU_n}L_{UE_m}|h_{SU_n}|^2}{\zeta_J[n]\eta_J L_{SJ}L_{JE_m}|h_{SJ}|^2}$, $\tilde{V}_m[n] \triangleq 1/(\tilde{F}_m\zeta_J[n]\frac{\tau_0}{\tau_n})$, $\tilde{F}_m \triangleq \eta_J P_S L_{SJ} L_{JE_m} |h_{SJ}|^2/\sigma_{E_m}^2$, and $\mathcal{T}[n] \triangleq \{\tau_n \in \mathbb{R} | 1 + A[n]\frac{\tau_0}{\tau_n} - 2^{\frac{r_{th}}{W\tau_n}}\} > 0$ for $n = 1, \ldots, N$.

Similar to the single user case in Section III-B, $P_{out}[n]$ in (28) is generally non-convex and thus difficult to handle. To make the problem more tractable, we apply the worst case approximation where the noise power at the eavesdroppers is negligible [15], [21]. Then, an upper bound of SOP for $n = 1, \ldots, N$ becomes

$$P_{out,\mathrm{UB}}[n] = \begin{cases} 1 - \prod_{m=1}^{M} \left(1 - \frac{\tilde{G}_m[n]}{1+\tilde{G}_m[n]}\right), & \text{if } \tau_n \in \mathcal{T}[n], \\ 1, & \text{otherwise.} \end{cases} \tag{29}$$

Finally, we can construct a problem for minimizing the maximum value of (29) as

$$\text{(P2.2)} \quad \min_{\{\tau_n\},\{\zeta_J[n]\}} \ \max_n \ P_{out,\mathrm{UB}}[n] \tag{30a}$$

$$\text{s.t. } 1 + A[n]\frac{\tau_0}{\tau_n} - 2^{\frac{r_{th}}{W\tau_n}} > 0, \quad \forall n, \tag{30b}$$

$$\sum_{n=1}^{N} \zeta_J[n] \le \zeta_{J,\max}, \quad \sum_{n=0}^{N} \tau_n \le 1. \tag{30c}$$

Still, (P2.2) is non-convex, and it is not trivial to find a globally optimal solution of (P2.2). In the following, we propose an alternating optimization procedure which yields a local optimal solution.

1) Time Allocation: For given power allocation $\{\zeta_J[n]\}$, we can reformulate (P2.2) into an equivalent form with a new variable $0 \leq \lambda_T < 1$ as

$$\text{(P2.3)} \quad \min_{\{\tau_n\},\lambda_T} \ \lambda_T \tag{31a}$$

$$\text{s.t. } P_{out,\mathrm{UB}}[n] \leq \lambda_T, \quad \forall n, \tag{31b}$$

$$1 + A[n]\frac{\tau_0}{\tau_n} - 2^{\frac{r_{th}}{W\tau_n}} > 0, \quad \forall n, \tag{31c}$$

$$\sum_{n=0}^{N} \tau_n \leq 1. \tag{31d}$$

As in the SR maximization problem in Section IV-A, the optimal λ_T can be found by a line search method in the outer loop, and for each λ_T, its feasibility is examined by solving the following problem:

$$\text{(P2.3.1)} \quad \min_{\{\tau_n\}} \ \sum_{n=0}^{N} \tau_n \tag{32a}$$

$$\text{s.t. } 1 + A[n]\frac{\tau_0}{\tau_n} - 2^{\frac{r_{th}}{W\tau_n}} > 0, \quad \forall n, \tag{32b}$$

$$P_{out,\mathrm{UB}}[n] \leq \lambda_T, \quad \forall n. \tag{32c}$$

In order to efficiently solve (P2.3.1), we first fix τ_0 and define $s_n \triangleq \frac{1}{\tau_n}$ for $n = 1, \ldots, N$. Then, it can be observed that the left-hand side of (32b) becomes concave in terms of s_n. Thus, the constraint in (32b) can be rewritten as $s_{n,L} < s_n < s_{n,U}$, where

$$s_{n,L} = -\frac{W}{r_{th}\ln 2}\mathcal{W}_{L,0}(\phi) - \frac{1}{A[n]\tau_0}, \tag{33}$$

$$s_{n,U} = -\frac{W}{r_{th}\ln 2}\mathcal{W}_{L,-1}(\phi) - \frac{1}{A[n]\tau_0}, \tag{34}$$

with $\phi = -\frac{r_{th}}{WA[n]\tau_0}\ln 2 \cdot 2^{-\frac{r_{th}}{WA[n]\tau_0}} < 0$.

For (32c), one can see that $\tilde{G}_m[n]$ in $P_{out,\mathrm{UB}}[n]$ is quasi-convex in terms of s_n since the numerator is convex while the denominator is concave [30]. Also, a unique minimizer of $\tilde{G}_m[n]$ is given by a stationary point $s_{n,C} = \frac{W}{r_{th}\ln 2} - \frac{1}{A[n]\tau_0}$ as in (21), which lies in $(s_{n,L}, s_{n,U})$ since $0 < -\mathcal{W}_{L,0}(\phi) < 1$ in (33) and $1 < -\mathcal{W}_{L,-1}(\phi)$ in (34) for $\phi < 0$. Therefore, $P_{out,\mathrm{UB}}[n]$ of (32c) increases for $s_n \in [s_{n,C}, s_{n,U})$ due to the fact that $P_{out,\mathrm{UB}}[n]$ is an increasing function of $\tilde{G}_m[n]$.

If $P_{out,\mathrm{UB}}[n]$ equals λ_T at $s_n = s_{n,C}$, it is obvious that the optimal solution is $\tau_{n,\mathrm{SOP}} = \frac{1}{s_{n,C}}$ for $n = 1, \ldots, N$. On the other hand, when $P_{out,\mathrm{UB}}[n] < \lambda_T$ at $s_n = s_{n,C}$, the objective function in (32a) can be further minimized by finding $s_n > s_{n,C}$ (hence smaller τ_n), since $P_{out,\mathrm{UB}}$ is an increasing function for $s_n \in (s_{n,C}, s_{n,U})$. In this case, the optimal solution $\tau_{n,\mathrm{SOP}}$ for $n = 1, \ldots, N$ is expressed as

$$\tau_{n,\mathrm{SOP}} = \frac{1}{s_{n,\lambda_T}}, \tag{35}$$

where s_{n,λ_T} is chosen to satisfy $P_{out,\mathrm{UB}}[n] = \lambda_T$, which can be easily determined by the bisection method.

To summarize, the optimal ET phase duration $\tau_{0,\mathrm{SOP}}$ can be found by a simple one-dimensional search in a bounded region $(0, 1)$, while $\{\tau_{n,\mathrm{SOP}}\}_{n=1}^{N}$ for (P2.3.1) are calculated by (35). Therefore, if (P2.3.1) is feasible and $\sum_{n=0}^{N}\tau_{n,\mathrm{SOP}} \leq 1$, we increase λ_T and decrease otherwise in the outer loop.

2) Power Allocation: With the given $\{\tau_{n,\mathrm{SOP}}\}$, we formulate the power allocation problem by introducing a new variable $0 \leq \lambda_J < 1$ as

$$\text{(P2.4)} \quad \min_{\{\zeta_J[n]\},\lambda_J} \ \lambda_J \tag{36a}$$

$$\text{s.t. } P_{out,\mathrm{UB}}[n] \leq \lambda_J, \quad \forall n, \tag{36b}$$

$$\sum_{n=1}^{N} \zeta_J[n] \leq \zeta_{J,\max}. \tag{36c}$$

Then, the following problem is considered to check the feasibility for each value of λ_J as

$$\text{(P2.4.1)} \quad \min_{\{\zeta_J[n]\}} \ \sum_{n=1}^{N} \zeta_J[n] \tag{37a}$$

$$\text{s.t.} \quad P_{out,\mathrm{UB}}[n] \leq \lambda_J, \quad \forall n. \tag{37b}$$

One can show from (29) that $P_{out,\mathrm{UB}}[n]$ in (37b) is a decreasing function of $\zeta_J[n]$. Therefore, we can rewrite (37b) as

$$\zeta_J[n] \geq \delta_J[n], \tag{38}$$

where the constant $\delta_J[n]$ satisfies $P_{out,\mathrm{UB}}[n] = \lambda_J$ at $\zeta_J[n] = \delta_J[n]$. Note that the constant $\delta_J[n]$ in (38) can be readily determined by the bisection method due to monotonicity of $P_{out,\mathrm{UB}}[n]$.

It is obvious from (38) that a solution $\zeta_{J,\mathrm{SOP}}[n]$ of (P2.4.1) is given by $\zeta_{J,\mathrm{SOP}} = \delta_J[n]$ for $n = 1, \ldots, N$. Finally, we increase λ_J in the outer loop if solutions of the inner problem (P2.4.1) satisfy $\sum_{n=1}^{N}\zeta_{J,\mathrm{SOP}}[n] \leq \zeta_{J,\max}$ and decrease otherwise. The overall alternating optimization process and the convergence behavior for the SOP minimization are analogous to Algorithm 2, and thus omitted for brevity.

V. Simulation Results

In this section, we provide numerical examples of the secrecy performance in the WPCN with an EH jammer and multiple eavesdroppers. We adopt the distance-dependent path loss model such that $L_{\mathsf{XY}} = 10^{-3}d_{\mathsf{XY}}^{-3}$, $\forall \mathsf{X},\mathsf{Y} \in \{S, J, U_n\forall n, E_m\forall m\}$, where d_{XY} is the distance between node X and Y as in [11] and [19]. Noting that many EH communication systems have a small coverage in practice, we particularly consider the Nakagami fading channels h_{SJ} and h_{SU_n}, $\forall n$ for the legitimate nodes with the Nakagami factor of 3. 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 $\zeta_{U_n} = 0.7, \forall n$, respectively. Furthermore, we set the noise power $\sigma_{\mathsf{X}}^2 = -160$ dBm/Hz, $\forall \mathsf{X}$ unless stated otherwise. Throughout this section, the secrecy performance is averaged over both channel realizations and the locations of the nodes. We compare our proposed solution with the following schemes.

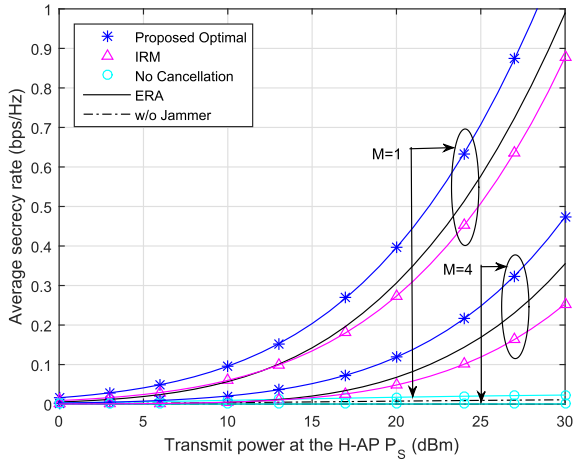

Fig. 2. Average secrecy rate comparison as a function of P_S where $d_{SU} = 5$ m, $d_{SJ} = 4$ m and $d_{UE_m} = 1$ m.

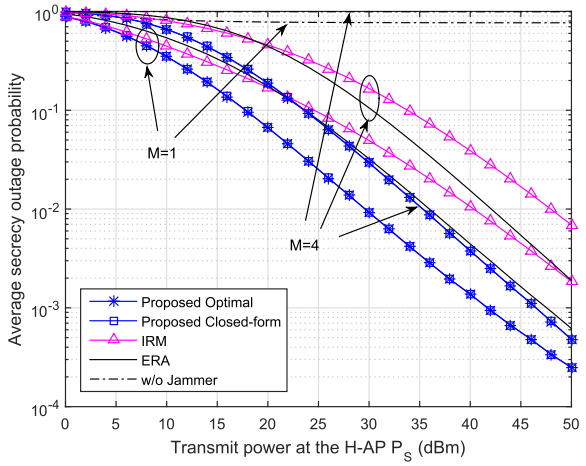

Fig. 3. Average secrecy outage probability as a function of P_S where $d_{SU} = 6$ m, $d_{SJ} = 3$ m and $d_{UE_m} = 4$ m.

- *Information rate maximization scheme (IRM)*: The sum throughput at the H-AP is maximized without consideration of the eavesdroppers [11].
- *Equal resource allocation (ERA)*: Both power and time resources are equally allocated.
- *Without jammer*: The WPCN with no EH jammer is employed as $\eta_J = 0$.

A. Single User Wiretap WPCN

We first investigate the secrecy performance in single user systems. We let the user and the jammer have a fixed distance d_{SU} and d_{SJ} from the H-AP, respectively. Also, the eavesdroppers are randomly placed with distance d_{UE_m} from the user for $m = 1, \ldots, M$. Fig. 2 illustrates the secrecy rate as a function of the transmit power P_S at the H-AP with $\zeta_J = 0.7$, $d_{SU} = 5$ m, $d_{SJ} = 4$ m and $d_{UE_m} = 1$ m, $\forall m$. In the plot, we see that the IRM is even worse than the ERA from the perspective of secrecy performance, which implies that a proper time allocation considering the eavesdroppers is indeed necessary. Moreover, with $P_S = 30$ dBm, we observe that the proposed optimal solution outperforms the IRM by 35 % when $M = 1$ and almost doubles when $M = 4$. This also demonstrates that as the number of eavesdroppers increases, a performance gain of the proposed scheme over the conventional methods becomes higher. One interesting observation is that the SR without the jamming signal cancellation at the H-AP, i.e., "*No Cancellation*", is similar to the case of no jammer which hardly achieves any secrecy. This verifies the importance of the cooperation between the H-AP and the jammer for the jamming signal cancellation in wiretap WPCN.

In Fig. 3 and 4, we provide simulation results when only CDI and the location information of the eavesdroppers are available to the legitimate nodes. Here, the threshold secrecy rate is fixed as $r_{th} = 100$ kbps. Fig. 3 presents the average SOP performance as a function of P_S with $\zeta_J = 0.7$, $d_{SU} = 6$ m, $d_{SJ} = 3$ m and $d_{UE_m} = 4$ m, $\forall m$. First, we confirm from the figure that the closed-form solution approaches the optimum in all P_S ranges. It is also shown that for both cases of $M = 1$ and 4, the proposed schemes outperform the IRM and the ERA. In particular, with one eavesdropper, there is about 10 dB gain compared to the IRM at the SOP of 0.01. Note that the performance gain becomes more pronounced as the number of eavesdroppers increases.

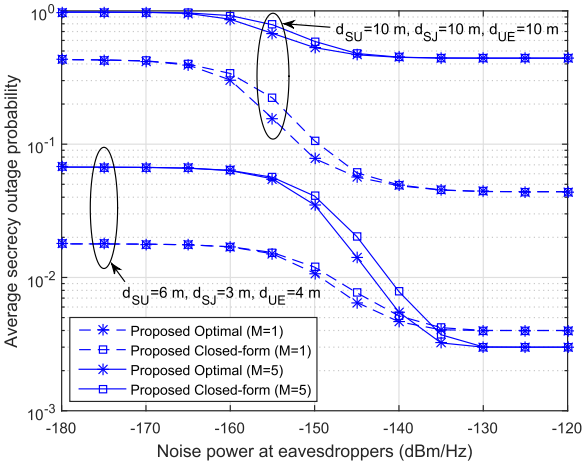

Fig. 4. Average secrecy outage probability as a function of $\sigma^2_{E_m}$ where $P_S = 500$ mW.

Fig. 4 illustrates the effect of the noise power spectral density at the eavesdropper on the proposed closed-form solution with $P_S = 500$ mW and $M = 1$ and 5. We observe that the performance gap between the proposed optimal algorithm and the closed-form solution is marginal for all noise power $\sigma^2_{E_m}$ and distances, which confirms the usefulness of our closed-form solution.

B. Multi-User Wiretap WPCN

In Fig. 5 and 6, we evaluate the proposed algorithms in the presence of multiple users as a function of P_S. For both figures, we set $M = 2$ and $N = 2$ and 4. Also, the jammer, users and eavesdroppers are randomly placed from the H-AP with the same distance of 5 m. We set $\zeta_{J,\max} = 1$. First, Fig. 5 demonstrates the average minimum SR among users where the proposed solution yields the best performance compared

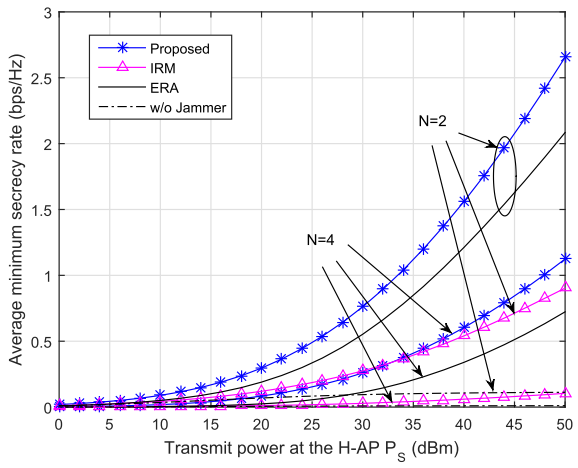

Fig. 5. Average minimum secrecy rate comparison as a function of P_S where $M = 2$, $d_{SU} = 5$ m, $d_{SJ} = 5$ m and $d_{SE_m} = 5$ m.

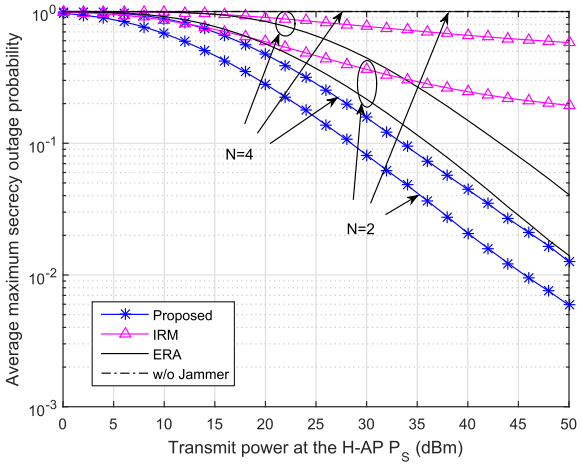

Fig. 6. Average maximum secrecy outage probability where $M = 2$, $d_{SU} = 5$ m, $d_{SJ} = 5$ m and $d_{SE_m} = 5$ m.

to other schemes. For example, at $P_S = 50$ dBm, the proposed scheme outperforms the ERA by 28% with 2 users. Similarly, in Fig. 6 where the average maximum SOP among users is evaluated, our proposed scheme is indeed superior to others for all P_S ranges. Specifically, there is approximately 8 dB gain at the SOP of 0.1 with 2 users when compared with the ERA. Note that the performance gain grows as the number of users increases in both figures, whereas the secrecy performance of IRM dramatically drops when multiple users are considered. From the figures, we can thus conclude that the proposed scheme significantly improves both the SR and SOP, and the gain becomes more pronounced with the increased number of eavesdroppers and users compared to other schemes.

VI. Conclusion and Future Works

In this paper, we have investigated the secrecy performance of wiretap WPCN with the aid of an EH jammer. We have considered two meaningful scenarios according to the level of CSI of the eavesdroppers. First, when perfect CSI is available to the legitimate nodes, we have optimized the time durations for ET and IT as well as the jammer's power allocation to maximize the minimum SR among users. Also, when only the location information and CDI of the eavesdroppers are known, we have derived an analytic expression for SOP and minimized the maximum SOP among users. The numerical examples have validated the proposed methods and confirmed the effect of the EH jammer on the secrecy performance. A system with a relay node or multiple jammers may be an interesting future topic.

Appendix A
Proof of Lemma 1

From (10), we have $r_{E_m} > 0$ when $\tau_0((AC_m\zeta_J + B_m - A)\tau_0 - (B_m - A)) > 0$. First, when $AC_m\zeta_J + B_m - A \leq 0$, it is obvious that $B_m - A < 0$ since $AC_m\zeta_J > 0$. Therefore, r_{E_m} is positive for $\tau_0 > 0$ and $AC_m\zeta_J + B_m - A = 0$, or $0 < \tau_0 < 1 < \frac{B_m - A}{AC_m\zeta_J + B_m - A}$ and $AC_m\zeta_J + B_m - A < 0$. On the other hand, when $AC_m\zeta_J + B_m - A > 0$, r_{E_m} is positive for $\tau_0 > 0$ and $B_m - A < 0$, or $\frac{B_m - A}{AC_m\zeta_J + B_m - A} < \tau_0 < 1$ and $B_m - A \geq 0$. Combining these results completes the proof.

Appendix B
Proof of Theorem 1

Let us define an upper contour set $\mathcal{K}_\alpha$ of r_{E_m} for any real α as

$$\mathcal{K}_\alpha = \{\tau_0 \in \mathbb{R} | r_{E_m} \geq \alpha, \check{\tau}_m < \tau_0 < 1\}.$$

By definition, r_{E_m} is a quasi-concave function if and only if $\mathcal{K}_\alpha$ is a convex set for all α [30]. When $\alpha \leq 0$, $\mathcal{K}_\alpha$ is convex since it reduces to $\{\tau_0 \in \mathbb{R} | 0 < \tau_0 < 1\}$. Thus, from now on, we focus on the convexity of $\mathcal{K}_\alpha$ for $\alpha > 0$.

For convenience, we use a monotonic transformation of $s = \frac{\tau_0}{1-\tau_0}$ for the rest of the proof. It can be easily verified that the convexity of a set is preserved in the transformation between τ_0 and s [28]. Therefore, $\mathcal{K}_\alpha$ is convex if and only if a set $\mathcal{F}_\alpha$ is convex, which is given by (39) at the bottom of this page, where $f(s) \triangleq (1+As)(C_m\zeta_J s+1) - ((B_m+C_m\zeta_J)s+1)2^{\frac{\alpha}{W}(s+1)}$ and $\bar{s}_m \triangleq [(B_m - A)/(AC_m\zeta_J)]^+$.

Now, we check the convexity of $\mathcal{F}_\alpha$ by examining $f(s)$. First, we notice that $\lim_{s\to 0} f(s) = 1 - 2^{\frac{\alpha}{W}} < 0$. Also, the second derivative of $f(s)$ in (40) which is shown at the bottom of this page monotonically decreases with s. Hence, one can see that $\frac{df(s)}{ds}$ either monotonically decreases, or monotonically increases and then decreases, which leads to a

$$\mathcal{F}_\alpha = \left\{ s \in \mathbb{R} \,\middle|\, W\frac{1}{s+1}\left[\left(\log_2(1+As) - \log_2\left(1 + \frac{B_m s}{C_m\zeta_J s + 1}\right)\right)\right]^+ \geq \alpha, s > \bar{s}_m \right\} = \{s \in \mathbb{R} | f(s) \geq 0\}, \quad (39)$$

$$\frac{d^2 f(s)}{ds^2} = 2AC_m\zeta_J - \left(2(B_m + C_m\zeta_J) + \frac{\alpha((B_m + C_m\zeta_J)s + 1)\ln 2}{W}\right)\frac{\alpha \ln 2}{W} 2^{\frac{\alpha}{W}(s+1)}, \quad (40)$$

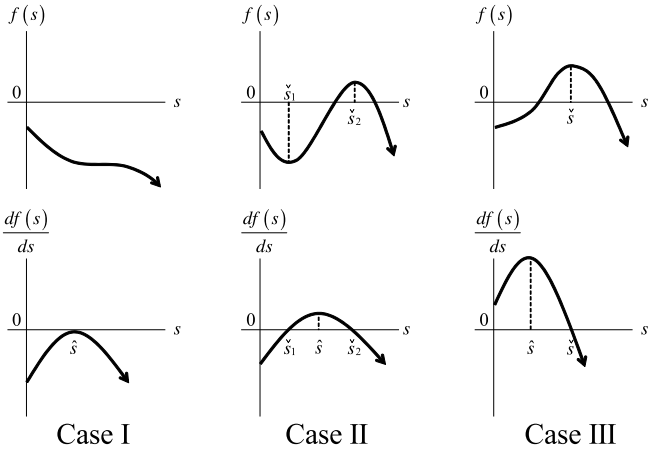

Fig. 7. Three possible cases of $f(s)$ and $\frac{df(s)}{ds}$.

unique maximum point $\hat{s}$ of $\frac{df(s)}{ds}$ for $s > 0$. If $\lim_{s\to 0} \frac{d^2 f(s)}{ds^2} \leq 0$, it is obvious that the set $\mathcal{F}_\alpha$ is convex since $f(s)$ is a concave function for all $s > 0$. On the other hand, if $\lim_{s\to 0} \frac{d^2 f(s)}{ds^2} > 0$, $f(s)$ is non-convex in general.

However, we can show that $\mathcal{F}_\alpha$ is still convex by classifying the functional forms of $f(s)$ into three cases as in Fig. 7.

- Case I: $\lim_{s\to 0} \frac{df(s)}{ds} < 0$ and $\left.\frac{df(s)}{ds}\right|_{s=\hat{s}} \leq 0$
  In this case, $f(s)$ is non-increasing for $s > 0$. Thus, $\mathcal{F}_\alpha = \emptyset$ is convex.
- Case II: $\lim_{s\to 0} \frac{df(s)}{ds} < 0$ and $\left.\frac{df(s)}{ds}\right|_{s=\hat{s}} > 0$
  Let two roots of $\frac{df(s)}{ds} = 0$ be $\check{s}_1$ and $\check{s}_2$ with $\check{s}_1 < \check{s}_2$. Then, $f(s)$ monotonically decreases for $0 < s < \check{s}_1$, which implies that $f(s) < 0$ for $0 < s < \check{s}_1$ due to the fact that $\lim_{s\to 0} f(s) < 0$. Therefore, we can rewrite $\mathcal{F}_\alpha$ as $\mathcal{F}_\alpha = \{s \in \mathbb{R} | f(s) \geq 0, s \geq \check{s}_1\}$. It is worth noting that for $s \geq \check{s}_1$, $f(s)$ is quasi-concave since it increases for $\check{s}_1 \leq s \leq \check{s}_2$ and decreases for $s > \check{s}_2$. As a result, $\mathcal{F}_\alpha$ is convex.
- Case III: $\lim_{s\to 0} \frac{df(s)}{ds} \geq 0$
  $f(s)$ is quasi-concave since $f(s)$ increases for $0 < s \leq \check{s}$ and decreases for $s > \check{s}$, where $\check{s}$ denotes the unique positive root of $\frac{df(s)}{ds} = 0$. Therefore, $\mathcal{F}_\alpha$ is also convex in this case.

To summarize, the upper contour set $\mathcal{K}_\alpha$ has been shown to be convex for all cases. It is also easy to see that a level set $\{s \in \mathbb{R} | r_{E_m} = \alpha, s > \bar{s}_m\}$ for every real α is a subset of the boundary of $\mathcal{K}_\alpha$ since $f(s)$ has at most two distinct stationary points. Moreover, because this convex set is a one-dimensional line segment, it is also strictly convex. Combining these, r_{E_m} is not only quasi-concave, but also strongly quasi-concave for $\check{\tau}_m < \tau_0 < 1$ [31]. This completes the proof.

APPENDIX C
PROOF OF LEMMA 2

First, note that the secrecy outage occurs for sure when the channel capacity from the user to the H-AP is smaller than the threshold r_{th}. In other words, if $W(1-\tau_0)\log_2\left(1 + A\frac{\tau_0}{1-\tau_0}\right) \leq r_{th}$, or equivalently $1 + As_0 - 2^{\frac{r_{th}}{W}(1+s_0)} \leq 0$, we have $P_{out} = 1$. Now, we consider the case $1 + As_0 - 2^{\frac{r_{th}}{W}(1+s_0)} > 0$. Denoting X' and Y' as $X' = \left|h_{UE_m}\right|^2$ and $Y' = \left|h_{JE_m}\right|^2$, X' and Y' independently follow a Chi-square distribution with two degrees of freedom. Thus, we have

$$\begin{aligned} P_{out,m} &= \Pr(Y' \leq G_m(s_0)X' - V_m(s_0)) \\ &= \int_{\frac{V_m(s_0)}{G_m(s_0)}}^{\infty} \int_0^{G_m(s_0)x - V_m(s_0)} e^{-x}e^{-y} dy dx \\ &= \frac{G_m(s_0)}{1 + G_m(s_0)} e^{-\frac{V_m(s_0)}{G_m(s_0)}}. \end{aligned} \tag{41}$$

Finally, substituting this result into (12) yields Lemma 2.

REFERENCES

[1] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tut.*, vol. 17, no. 2, pp. 757–789, 2nd Quart., 2015.

[2] M.-L. Ku, W. Li, Y. Chen, and K. J. R. Liu, "Advances in energy harvesting communications: Past, present, and future challenges," *IEEE Commun. Surveys Tut.*, vol. 18, no. 2, pp. 1384–1412, 2nd Quart. 2016.

[3] H. Ju and R. Zhang, "Optimal resource allocation in full-duplex wireless-powered communication network," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3528–3540, Oct. 2014.

[4] L. R. Varshney, "Transporting information and energy simultaneously," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 1612–1616.

[5] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.

[6] J. Xu, L. Liu, and R. Zhang, "Multiuser MISO beamforming for simultaneous wireless information and power transfer," *IEEE Trans. Signal Process.*, vol. 62, no. 18, pp. 4798–4810, Sep. 2014.

[7] J. Park and B. Clerckx, "Joint wireless information and energy transfer in a K-user MIMO interference channel," *IEEE Trans. Wireless Commun.*, vol. 13, no. 10, pp. 5781–5796, Oct. 2014.

[8] 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 Trans. Wirless Commun.*, vol. 14, no. 9, pp. 4810–4821, Sep. 2015.

[9] X. Gui, Z. Zhu, and I. Lee, "Sum rate maximizing in a multi-user MIMO system with SWIPT," in *Proc. IEEE Veh. Technol. Conf. (VTC)*, May 2015, pp. 1–5.

[10] 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 Veh. Technol. Conf. (VTC)*, May 2015, pp. 1–5.

[11] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 418–428, Jan. 2014.

[12] 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 Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2619–2628, Apr. 2016.

[13] 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 Trans. Wireless Commun.*, vol. 15, no. 7, pp. 1–9, Jul. 2016.

[14] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tut.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[15] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[16] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[17] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 64, no. 7, pp. 1850–1863, Apr. 2014.

[18] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.
[19] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 180–190, Jan. 2016.
[20] D. T. Hoang, D. Niyato, P. Wang, and D. I. Kim, "Performance analysis of wireless energy harvesting cognitive radio networks under smart jamming attacks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 1, no. 2, pp. 200–216, Jun. 2015.
[21] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401–415, Jan. 2016.
[22] H. Xing, K.-K. Wong, Z. Chu, and A. Nullanathan, "To harvest and jam: A paradigm of self-sustaining friendly jammers for secure AF relaying," *IEEE Trans. Signal Process.*, vol. 63, no. 24, pp. 6616–6631, Dec. 2015.
[23] J. Gao, S. A. Vorobyov, H. Jiang, and H. V. Poor, "Worst-case jamming on MIMO Gaussian channels," *IEEE Trans. Signal Process.*, vol. 63, no. 21, pp. 5821–5836, Nov. 2015.
[24] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3072–3081, Nov. 2001.
[25] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar. 2012, pp. 2809–2812.
[26] Y. Choi and D. Kim, "Performance analysis with and without torch node in secure communications," in *Proc. IEEE Int. Conf. Adv. Technol. Commun. (ATC)*, Oct. 2015, pp. 84–87.
[27] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135–5146, Sep. 2015.
[28] S. Boyd and L. Vanderberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[29] R. Corless, G. Gonnet, D. Hare, D. Jeffery, and D. Knuth, "On the lambert$W$ function," *Adv. Comput. Math.*, vol. 5, no. 1, pp. 329–359, 1996.
[30] M. S. Bazaraa, H. D. Sherali, and C. M. Shetty, *Nonlinear Programming: Theory and Algorithms*. Hoboken, NJ, USA: Wiley, 2006.
[31] R. A. Danao, "Strict convexity of the upper level sets of strictly quasiconcave functions," *Philippine Rev. Econ. Bus.*, vol. 27, no. 1, pp. 1–7, Jun. 1990.

Jihwan Moon (S'16) received the B.S. and M.S. degrees in electrical engineering from Korea University, Seoul, South Korea, in 2014 and 2016, respectively, where he is currently pursuing the Ph.D. degree with the School of Electrical Engineering. His research interests include information theory and wireless communications such as signal processing for physical-layer security and energy harvesting communications.

Hoon Lee (S'14) received the B.S. and M.S. degrees in electrical engineering from Korea University, Seoul, South Korea, in 2012 and 2014, respectively, where he is currently pursuing the Ph.D. degree with the School of Electrical Engineering. During the winter of 2014, he visited Imperial College London, London, U.K. as a visiting student. His research interests include information theory and signal processing for wireless communications such as MIMO wireless network and energy harvesting communication systems.

Changick Song (S'09–M'13) received the B.S., M.S., and Ph.D. degrees in electrical engineering from Korea University, Seoul, South Korea, in 2007, 2009, and 2012, respectively. He was a Visiting Researcher with the University of Southern California, Los Angeles, CA, USA, in 2009, and with Queen's University, Kingston, ON, Canada, in 2011. From 2012 to 2013, he was a Research Professor with Korea University and from 2013 to 2014, he was with the Communications and Signal Processing Group, Imperial College London, London, U.K., as a Post-Doctoral Research Associate. In 2014, he joined the Faculty of the Korea National University of Transportation, Chungju, South Korea, where he is currently an Assistant Professor with the Department of Information and Communications Engineering. His research interest includes information theory and signal processing for wireless communications and security.

Inkyu Lee (S'92–M'95–SM'01–F'16) received the B.S. degree (Hons.) in control and instrumentation engineering from Seoul National University, Seoul, South Korea, in 1990, and the M.S. and Ph.D. degrees in electrical engineering from Stanford University, Stanford, CA, USA, in 1992 and 1995, respectively. From 1995 to 2001, he was a Technical Staff Member with Bell Laboratories, Lucent Technologies, Murray Hill, NJ, USA, where he studied high-speed wireless system designs. From 2001 to 2002, he was with Agere Systems, Murray Hill, as a Distinguished Member of the Technical Staff. In 2009, he visited the University of Southern California, Los Angeles, CA, USA, as a Visiting Professor. Since 2002, he has been with Korea University, Seoul, South Korea, where he is currently a Professor of Electrical Engineering. He has authored over 130 journal papers in the IEEE and holds 30 U.S. patents granted or pending. His research interests include digital communications, signal processing, and coding techniques applied for next-generation wireless systems. He has served as an Associate Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS from 2001 to 2011, and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2007 to 2011. He has been a Chief Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (Special Issue on 4G Wireless Systems) in 2006. He currently serves as an Editor of the IEEE ACCESS. Also he is an IEEE Distinguished Lecturer for the vehicular technology society (VTS). He was a recipient of the IT Young Engineer Award at the IEEE/IEEK Joint Award in 2006, and of the Best Paper Award at APCC in 2006, the IEEE VTC in 2009, and ISPACS in 2013. He was also a recipient of the Best Research Award from the Korea Information and Communications Society in 2011, and the Best Young Engineer Award from the National Academy of Engineering in Korea (NAEK) in 2013. He has been elected as a member of NAEK in 2015. He is an IEEE fellow.