


Research Article

Secrecy Wireless-Powered Sensor Networks for Internet of Things

Junxia Li,¹ Hui Zhao ,¹ Xueyan Chen,² Zheng Chu,^{3,4} Li Zhen,⁴ Jing Jiang,⁴ and Haris Pervaiz⁵

¹College of Information Science and Engineering, Xinjiang University, Urumqi 830046, China

²Zhengzhou University of Light Industry, Zhengzhou 450002, China

³University of Surrey, Guildford GU2 7XH, UK

⁴College of Communication and Information Engineering, Xi'an University of Post and Telecommunications, Xi'an, Shanxi 710061, China

⁵School of Computing and Communications, Lancaster University, Lancaster LA1 4WA, UK

Correspondence should be addressed to Hui Zhao; zherry@126.com

Received 30 April 2020; Revised 27 June 2020; Accepted 12 August 2020; Published 22 September 2020

Academic Editor: Di Zhang

Copyright © 2020 Junxia Li et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper investigates a secure wireless-powered sensor network (WPSN) with the aid of a cooperative jammer (CJ). A power station (PS) wirelessly charges for a user equipment (UE) and the CJ to securely transmit information to an access point (AP) in the presence of multiple eavesdroppers. Also, the CJ are deployed, which can introduce more interference to degrade the performance of the malicious eavesdroppers. In order to improve the secure performance, we formulate an optimization problem for maximizing the secrecy rate at the AP to jointly design the secure beamformer and the energy time allocation. Since the formulated problem is not convex, we first propose a global optimal solution which employs the semidefinite programming (SDP) relaxation. Also, the tightness of the SDP relaxed solution is evaluated. In addition, we investigate a worst-case scenario, where the energy time allocation is achieved in a closed form. Finally, numerical results are presented to confirm effectiveness of the proposed scheme in comparison to the benchmark scheme.

1. Introduction

Internet of things (IoT) has been considered one of the appealing paradigms for future wireless network which significantly improves massive connectivity for the sensor devices [1]. However, the IoT devices suffer from energy-constrained issues. In this case, the devices in an IoT network will disconnect the IoT server due to limited battery size in this low-energy consumption nature. In a variety of IoT applications, e.g., those enabling the smart manufactures, due to the life cycle of the IoT devices which is approximately 10 to 20 years or more, it has led to severely demanding battery life constraints. Therefore, energy efficiency has been one of the main challenges in IoT networks [2].

On the other hand, reliable data transmission for IoT networks has become increasingly important, especially in vari-

ous civilian and military applications. For secured IoT networks, the IoT devices guarantee a reliable connection with the access point to safeguard the private information, such as credit card transaction, online personal data, and military intelligent transmissions [3]. As a matter of fact, information security has become an essential part of the IoT system. Conventionally, a reliable wireless network is guaranteed via conventional cryptographic techniques which are implemented in the network layer. Nevertheless, due to the inherent quality of wireless transmission, it will incur large overhead as well as various issues in the key distribution and management to build a reliable link [4, 5]. As an alternative approach, physical layer security has been developed to provide the secrecy capacity metric by exploiting information-theoretical fundamentals [3]. In recent years, a variety of resource allocation algorithms have been developed in physical layer security scenarios to improve

the secrecy performance of the wireless networks. Additionally, physical layer security has also been studied in the scenario of multiantenna [5–7]. In secure communications, the transmit power efficiency plays a key role to enhance the secrecy capacity. Ideally, the transmit power at the base station (BS) is minimized to satisfy the transmission requirement on achievable secrecy rate [8, 9]. Recently, the reliability and security of wireless system have been considered in [10, 11], which can be applied in IoT applications. In [10], cooperative dual-hop nonorthogonal multiple access (NOMA) was investigated, where the transceivers consider a detrimental factor of in-phase and quadrature-phase imbalance (IQI). A decode-and-forward (DF) relay was employed to assist the secure communication between the source and destination. To characterize the performance of this system, exact and asymptotic analytical expressions for the outage probability (OP) and intercept probability (IP) are derived in terms of the closed-form expression. Integrating ambient backscatter (AmBC) into the NOMA system has been investigated in [11], where the source is aimed at communicating with two NOMA users in the presence of an eavesdropper. A more practical case is that nodes and backscatter device (BD) suffer from IQI.

Wireless-powered communication networks (WPCNs), as an enabler of energy harvesting, have been considered one of the promising techniques to deal with the energy-constrained issue in the IoT system. In WPCNs, large amounts of IoT devices are deployed to collect the energy from dedicated energy sources to supply wireless charging services for the IoT sensor nodes via radio frequency (RF) wireless energy transfer (WET) [2]. In recent years, there has been a variety of existing literature focused on how to effectively use the harvested energy to improve system performance [12–16]. In [12], a generic transmission WPCN was proposed, where a “harvest-then-transmit” was investigated. In this WPCN, the devices first harvest energy via the RF signals broadcast by an AP in the downlink and then implement wireless information transfer (WIT) in the uplink. In response to the doubly near-far effect in [12], the proportional fairness is explored by jointly designing power and time allocation in [13]. In [14], the WPCN application in AmBC was investigated, where wireless-powered IoT devices can collect energy and transmit their own information using the primary signal. By exploiting the energy supply among devices, a new wireless-powered chain model was proposed in IoT networks, where the IoT devices not only transmit information to the AP but also extract the energy from the RF signal of others [15]. In addition, a nonlinear energy harvesting model was proposed to maximize sum throughput and the minimum individual throughput for all wireless-powered users [16]. Moreover, a group of power stations (PSs) are composed of a dedicated WET network which is deployed to coordinate WIT networks in the vicinity [17, 18]. Specifically, these IoT devices can achieve more energy benefits from these PSs to prolong their own battery life via wireless charging, which outperform the traditional battery-powered counterparts. The WPCN highlights its advantage to reduce the operational cost and improves the robustness of wireless communication net-

works, which is more suitable for the low energy use cases, named wireless-powered sensor networks (WPSNs) [1]. Recently, a worst-case secure WPCN has been considered, where the eavesdroppers intercept the legitimate information between a H-AP and the user, and the jammer node acts as an artificial noise to interfere eavesdroppers by utilizing its harvested energy [19]. Moreover, multiple-input single-output (MISO) simultaneous wireless information and power transfer (SWIPT) has been investigated to integrate the energy harvesting user with security requirement [20–22]. In [20], secrecy energy efficiency maximization was exploited with an energy harvesting receiver, where the formulated problem is fractional programming and can be reformulated into difference of concave (DC) functions. Thus, the successive convex approximation and Dinkelbach’s algorithm are employed to iteratively solve this optimization problem. An artificial noise- (AN-) aided secure SWIPT was investigated to improve the secure performance and energy harvesting efficiency under channel certainty of the eavesdroppers [21]. In [22], the outage-constrained robust secure design was studied, where the energy receivers can overhear the desired information which can be treated as potential eavesdroppers. Although the abovementioned works have investigated the WPCN integrated with some promising techniques, the reliable information transfer supported by WPCN still remains a performance bottleneck. Thus, integration of WPCN with the secure communications is a promising solution to address the energy-constraint and reliable issues simultaneously. Also, it is noted that the secure transmission of the IoT devices can be guaranteed by the wireless charging service. To the best of our knowledge, there have been no published works that model and investigate this secure WPCN in IoT system, which motivates this work.

In this paper, we investigate a cooperative jamming- (CJ-) aided secure WPSN. In particular, a multiantenna PS employs an energy beamforming to offer wireless charging services for a user equipment (UE) (i.e., IoT device) as well as a CJ node, and then, the UE utilizes the harvested energy to build a secure communication link with the AP when there existed multiple eavesdroppers. Meanwhile, the CJ uses the harvested energy to introduce interference, so that the reception of the eavesdroppers can be degraded. For this communication model, the main contributions of this paper are summarized as follows:

- (1) First, it is aimed at maximizing the achievable secrecy rate to jointly design the energy beamforming and time allocation. Due to the nonconvex property of the formulated problem, it cannot be solved directly. In order to circumvent this nonconvexity, we first analyze the feasibility of the optimal time allocation for the given energy beamforming. Next, we propose a global optimal scheme where the energy beamforming is optimally designed for a given time allocation. This reformulated problem is further divided into a two-level optimization problem via introducing an auxiliary variable. Specifically, this formulated optimization problem can be solved via a semidefinite

programming (SDP) relaxation and one-dimensional line search. In addition, the optimal time allocation can be achieved via numerical search

- (2) Second, a novel low-complexity scheme is exploited, which is based on a worst-case scenario, i.e., eavesdroppers' noise-free signal. The time allocation can be derived in terms of closed-form expression via Lambert W function, while the energy beamforming can be achieved via similar relaxation with a global optimal scheme. Numerical results are demonstrated to validate the proposed scheme

The remainder of this paper is organized as follows. In Section 2, we introduce the system model and formulate the problem. In Section 3, we present the global optimal solution for the original problem. We propose the low-complexity scheme for the formulated problem in Section 4. In Section 5, we provide numerical results to evaluate the proposed scheme. Finally, the conclusions of this paper are presented in Section 6.

2. System Model

In this section, we investigate a CJ-aided secure WPSN as shown in Figure 1. Specifically, a power station (PS), powered by a stable energy supply (i.e., microgrid), wirelessly charges for a user equipment (UE), which utilizes its harvested energy to establish a secure transmission link with an access point (AP) overheard by multiple eavesdroppers (this system model practically fits within the civilian and military applications). Specifically, the UE is regarded as a smart sensor node embedded into the smart wearable devices, which harvests the energy to support monitor personal private information transmitted to the access point. Also, this UE acts as a low-power sensor node deployed in the battlefield which needs to collect the energy service from the PS to transmit the intelligence information monitored by the UE to the AP). In this paper, we assume that the UE employs the linear energy harvesting. This is due to the fact that this assumption practically holds when the harvested energy at the UE is relatively lower than its battery capacity. Meanwhile, a dedicated CJ is deployed to collect the energy from the PS to introduce addition interference to degrade the reception of the eavesdroppers. We consider the case that the PS is equipped with N_{PS} transmit antennas, while all the other nodes use a single antenna. In this paper, we consider quasistatic flat-fading channel model, where all channel gains remain constant during each time block. We assume that \mathbf{h} , \mathbf{g}_j , h_s , $h_{e,k}$, l_j , and $f_{j,k}$ are denoted as the channel coefficients between the PS and the UE, the PS and the jammer, the UE and the AP, the UE and the k th eavesdropper, the jammer and the AP, and the jammer and the k th eavesdropper, respectively. A well-known "harvesting-then-transmit" protocol is considered in downlink WPT phase and uplink WIT phase. We also assume that the whole transmission time block is T . In the WET phase, i.e., $\theta \in (0, 1)$, the PS wirelessly charges for the UE and the jammer; thus, the harvested energy at the UE

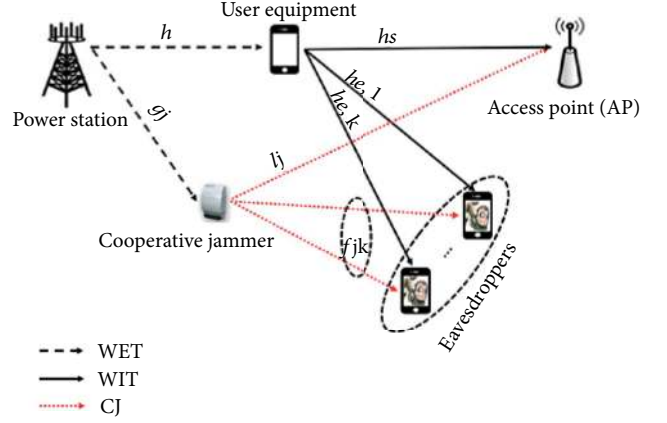


FIGURE 1: System model.

and the jammer can be written, respectively, as

$$\begin{aligned} E_{IT} &= \eta P_s |\mathbf{h}^H \mathbf{w}|^2 \theta, \\ E_J &= \eta P_s |\mathbf{g}_j \mathbf{w}|^2 \theta, \end{aligned} \quad (1)$$

where $\eta \in (0, 1]$ accounts for the energy efficiency at the UE and the jammer, \mathbf{w} denotes the normalized energy beamforming at the PS, and P_s is the transmit power at the PS. Accordingly, the transmit power at the UE and the j th jammer is given by, respectively,

$$\begin{aligned} P_{IT} &= \frac{\eta P_s |\mathbf{h}^H \mathbf{w}|^2 \theta}{T - \theta}, \\ P_J &= \frac{\eta P_s |\mathbf{g}_j \mathbf{w}|^2 \theta}{T - \theta}. \end{aligned} \quad (2)$$

During the WIT phase, i.e., $T - \theta$, the UE and the jammer utilize the harvested energy to perform the information transfer. Specifically, the UE transmits the confidential information to the AP when there existed multiple eavesdroppers during the WIT phase; meanwhile, the CJ introduces the interference, so that the reception of the eavesdroppers is degraded. Noting that, the jammer guarantees that there is no interference leakage to the AP, i.e., the jammer is dedicated to help the UE to interfere with the eavesdropper, where there is a cooperation between the AP and the jammer such that the AP can decode the interference signal from the jammer. Thus, we write the mutual information at the AP and the k th eavesdropper, respectively, as follows:

$$\begin{aligned} R_u(\mathbf{w}, \theta) &= \log_2 \left(1 + \frac{\eta \theta P_s |\mathbf{h}^H \mathbf{w}|^2 |h_s|^2}{(T - \theta) \sigma_s^2} \right) \\ &= \log_2 \left(1 + \frac{\theta}{T - \theta} X_s(\mathbf{w}) \right), \end{aligned} \quad (3)$$

$$\begin{aligned}
R_{e,k}(\mathbf{w}, \theta) &= \log_2 \left(1 + \frac{(\eta\theta P_s |\mathbf{h}^H \mathbf{w}|^2 / T - \theta) |h_{e,k}|^2}{(\eta\theta P_s |\mathbf{g}_J^H \mathbf{w}|^2 / T - \theta) |f_{J,k}|^2 + \sigma_e^2} \right) \\
&= \log_2 \left(1 + \frac{\eta\theta P_s |\mathbf{h}^H \mathbf{w}|^2 |h_{e,k}|^2}{\theta (P_s \eta |\mathbf{g}_J^H \mathbf{w}|^2 |f_{J,k}|^2 - \sigma_{e,k}^2) + T\sigma_e^2} \right) \\
&= \log_2 \left(1 + \frac{\theta X_{e,k}(\mathbf{w})}{\theta (X_{J,k}(\mathbf{w}) - 1) + T} \right),
\end{aligned} \tag{4}$$

where

$$\begin{aligned}
X_s(\mathbf{w}) &= \frac{\eta P_s |h_s|^2 |\mathbf{h}^H \mathbf{w}|^2}{\sigma_s^2}, \\
X_{e,k}(\mathbf{w}) &= \frac{\eta P_s |h_{e,k}|^2 |\mathbf{h}^H \mathbf{w}|^2}{\sigma_e^2}, \\
X_{J,k}(\mathbf{w}) &= \frac{\eta P_s |f_{J,k}|^2 |\mathbf{g}_J^H \mathbf{w}|^2}{\sigma_e^2}.
\end{aligned} \tag{5}$$

From (3), the achievable secrecy rate at the AP can be expressed as

$$R_s(\mathbf{w}, \theta) = \left[R_u - \max_{k \in [1, K]} R_{e,k} \right]^+. \tag{6}$$

Thus, we formulate the secrecy throughput maximization subject to the energy beamformer and time allocation constraints, which is given by

$$\max_{\theta, \mathbf{w}} (T - \theta) R_s(\mathbf{w}, \theta) \tag{7}$$

$$\text{s.t.} \quad \|\mathbf{w}\|^2 \leq 1, \quad 0 < \theta < 1. \tag{8}$$

Problem (7) is nonconvex due to its objective function; thus, it cannot be solved directly. In order to address this problem, we employ a two-layer approach to globally obtain the optimal time allocation θ and energy beamformer \mathbf{w} . We further provide a worst-case scenario and obtain the closed-form expression of the optimal time allocation.

3. Global Optimal Solution to (7)

In this section, we propose a global optimal scheme to solve problem (7). Specifically, the energy beamforming can be optimally designed for given time allocation, which is reformulated into two level subproblems. The inner level problem can be solved by using an SDP, and the outer level problem is a single-variable optimization problem, which employs a one-dimensional line search to achieve the optimal energy beamforming. In addition, the time allocation can be optimally designed via numerical search.

3.1. Feasibility Analysis. In this subsection, we characterize the feasibility of time allocation of problem for the given

energy beamforming \mathbf{w} . Thus, the following lemma is required to exploit the feasibility of problem (7).

Lemma 1. For a given \mathbf{w} , problem (7) is feasible for $\theta_{\min} < \theta < 1$, where

$$\theta_{\min} = \arg \max_{k \in [1, K]} \frac{X_{e,k}(\mathbf{w}) - X_s(\mathbf{w})}{X_s(\mathbf{w})X_{J,k}(\mathbf{w}) - X_s(\mathbf{w}) + X_{e,k}(\mathbf{w})}. \tag{9}$$

Proof. In order to show the feasibility of (7), it is achieved from (6) that $R_s > 0$ such that we have

$$R_u - R_{e,k} > 0, \quad \forall k. \text{ Thus,}$$

$$\frac{\theta}{T - \theta} X_s(\mathbf{w}) > \frac{\theta X_{e,k}(\mathbf{w})}{\theta (X_{J,k}(\mathbf{w}) - 1) + T}, \tag{10}$$

$$\theta [(X_s(\mathbf{w})X_{J,k}(\mathbf{w}) - X_s(\mathbf{w}) + X_{e,k}(\mathbf{w}))\theta - T(X_{e,k}(\mathbf{w}) - X_s(\mathbf{w}))] > 0. \tag{11}$$

From (11), we have two cases, i.e., $X_s(\mathbf{w})X_{J,k}(\mathbf{w}) - X_s(\mathbf{w}) + X_{e,k}(\mathbf{w}) \leq 0$ and $X_s(\mathbf{w})X_{J,k}(\mathbf{w}) - X_s(\mathbf{w}) + X_{e,k}(\mathbf{w}) > 0$. First, we discuss the case $X_s(\mathbf{w})X_{J,k}(\mathbf{w}) - X_s(\mathbf{w}) + X_{e,k}(\mathbf{w}) \leq 0$, which results in $X_{e,k}(\mathbf{w}) - X_s(\mathbf{w}) < 0$ due to $X_s(\mathbf{w})X_{J,k}(\mathbf{w}) > 0$. In order to guarantee $R_u - R_{e,k} > 0$, one of the following inequalities should be satisfied:

$$\begin{cases} \theta > 0, \\ X_s(\mathbf{w})X_{J,k}(\mathbf{w}) - X_s(\mathbf{w}) + X_{e,k}(\mathbf{w}) = 0, \\ 0 < \theta < 1 < \frac{X_{e,k}(\mathbf{w}) - X_s(\mathbf{w})}{X_s(\mathbf{w})X_{J,k}(\mathbf{w}) - X_s(\mathbf{w}) + X_{e,k}(\mathbf{w})}, \\ X_s(\mathbf{w})X_{J,k}(\mathbf{w}) - X_s(\mathbf{w}) + X_{e,k}(\mathbf{w}) < 0. \end{cases} \tag{12}$$

Then, we discuss the second case $X_s(\mathbf{w})X_{J,k}(\mathbf{w}) - X_s(\mathbf{w}) + X_{e,k}(\mathbf{w}) > 0$. In order to guarantee $R_u - R_{e,k} > 0$, one of the following inequalities should hold:

$$\forall k, \begin{cases} \theta > 0, \\ X_{e,k}(\mathbf{w}) - X_s(\mathbf{w}) < 0, \\ \frac{X_{e,k}(\mathbf{w}) - X_s(\mathbf{w})}{X_s(\mathbf{w})X_{J,k}(\mathbf{w}) - X_s(\mathbf{w}) + X_{e,k}(\mathbf{w})} \leq \theta < 1, \\ X_{e,k}(\mathbf{w}) - X_s(\mathbf{w}) \geq 0. \end{cases} \tag{13}$$

From the abovementioned results, we obtain

$$\theta_{\min} \leq \theta < 1, \tag{14}$$

where

$$\theta_{\min} = \arg \max_{k \in [1, K]} \frac{X_{e,k}(\mathbf{w}) - X_s(\mathbf{w})}{X_s(\mathbf{w})X_{J,k}(\mathbf{w}) - X_s(\mathbf{w}) + X_{e,k}(\mathbf{w})}. \tag{15}$$

By exploiting Lemma 1, we can derive the optimal time allocation through one-dimensional line search over $\theta \in (\theta_{\min}, 1)$.

3.2. Global Optimal Scheme. In the previous subsection, we characterize the feasibility condition for the formulated problem (7) to obtain optimal time allocation. To proceed, we optimize the energy beamformer \mathbf{w} in (7) for a given time allocation θ , which is written as

$$\max_{\mathbf{w}} R_s \quad (16)$$

$$\text{s.t.} \quad \|\mathbf{w}\|^2 \leq 1. \quad (17)$$

Problem (16) is nonconvex in terms of \mathbf{w} such that it cannot be solved directly. To tackle it, we propose a global optimal scheme via employing two-dimensional line search and SDP relaxation. First, we fix the time allocation θ and introduce an auxiliary variable t such that problem (16) can then be rewritten as

$$\begin{aligned} R_s^* &= \max_{\mathbf{w}, t} \log_2 \left(1 + \frac{\theta}{T-\theta} X_s(\mathbf{w}) \right) + \log_2(t) \\ \text{s.t.} \quad \max_{k \in [1, K]} \log_2 \left(1 + \frac{\theta X_{e,k}(\mathbf{w})}{\theta(X_{J,k}(\mathbf{w}) - 1) + T} \right) &\leq \log_2 \left(\frac{1}{t} \right), \\ \|\mathbf{w}\|^2 &\leq 1. \end{aligned} \quad (18)$$

Although we have introduced an auxiliary variable t to reformulate problem (16), it is still nonconvex and intractable. In order to circumvent this issue, problem (16) can be divided into two-level subproblems, which can be given by the following:

(1) Outer level: the outer level subproblem is given by

$$R_s^* = \max_t \log_2(1 + \Gamma(t)) + \log_2(t) \quad (19)$$

$$\text{s.t.} \quad t_{\min} \leq t \leq 1, \quad (20)$$

where $\Gamma(t) = (\theta/(T-\theta))X_s(\mathbf{w})$ and t_{\min} denote the lower bound of variable t . Note that this lower bound can be easily derived as $t_{\min} = (1 + (\eta\theta P_s |h_s|^2 \|\mathbf{h}\|^2) / ((T-\theta)\sigma_s^2))^{-1}$ [23].

(2) Inner level: for a given t , the inner level subproblem is written as

$$\Gamma(t) = \max_{\mathbf{w}} \frac{\eta\theta P_s |h_s|^2 |\mathbf{h}^H \mathbf{w}|^2}{(T-\theta)\sigma_s^2} \quad (21)$$

$$\text{s.t.} \quad \max_{k \in [1, K]} \log_2 \left(1 + \frac{\eta\theta P_s |\mathbf{h}^H \mathbf{w}|^2 |h_{e,k}|^2}{\theta(P_s \eta |\mathbf{g}_J^H \mathbf{w}|^2 |f_{J,k}|^2 - \sigma_e^2) + T\sigma_e^2} \right) \leq \log_2 \left(\frac{1}{t} \right), \quad (22)$$

$$\|\mathbf{w}\|^2 \leq 1. \quad (23)$$

From (19), the outer level subproblem is a single-variable optimization problem in terms of t with interval $t \in [t_{\min}, 1]$, which is tackled via one-dimensional line search, while the inner level subproblem (21) is still nonconvex due to its constraint with any feasible t . In the following, we will tackle the inner stage problem (21) to optimally design the energy beamforming \mathbf{w} .

3.3. Optimal Solution to (21). In this subsection, we consider a SDP relaxation to optimally solve the inner stage problem (21). First, let us denote $\mathbf{W} = \mathbf{w}\mathbf{w}^H$; problem (21) can be relaxed as

$$\begin{aligned} \Gamma(t) &= \max_{\mathbf{W} \succeq 0} \frac{\eta\theta P_s |h_s|^2 \text{Tr}(\mathbf{h}\mathbf{h}^H \mathbf{W})}{(T-\theta)\sigma_s^2} \\ \text{s.t.} \quad \log_2 \left(1 + \frac{\eta\theta P_s |h_{e,k}|^2 \text{Tr}(\mathbf{h}\mathbf{h}^H \mathbf{W})}{\theta(P_s \eta |f_{J,k}|^2 \text{Tr}(\mathbf{g}_J \mathbf{g}_J^H \mathbf{W}) - \sigma_e^2) + T\sigma_e^2} \right) &\leq \log_2 \left(\frac{1}{t} \right), \end{aligned} \quad (24a)$$

$$\text{Tr}(\mathbf{W}) \leq 1, \quad (24b)$$

$$\text{rank}(\mathbf{W}) \leq 1. \quad (24c)$$

Problem (24) is intractable due to (24a) and (24c). To proceed, by exploiting a few of the mathematical manipulations to tackle (24a), (24) can be equivalently modified as

$$\tilde{\Gamma}(t) = \max_{\mathbf{W} \succeq 0} \text{Tr}(\mathbf{h}\mathbf{h}^H \mathbf{W}) \quad (25)$$

$$\begin{aligned} \text{s.t.} \quad \eta\theta P_s |h_{e,k}|^2 \text{Tr}(\mathbf{h}\mathbf{h}^H \mathbf{W}) \\ - \theta \left(\frac{1}{t} - 1 \right) \left(P_s \eta |f_{J,k}|^2 \text{Tr}(\mathbf{g}_J \mathbf{g}_J^H \mathbf{W}) - \sigma_e^2 \right) \end{aligned} \quad (26)$$

$$- \left(\frac{1}{t} - 1 \right) T\sigma_e^2 \leq 0, \quad \forall k,$$

$$(17b), (17c). \quad (27)$$

Note that $\Gamma^* = (\eta\theta P_s |h_s|^2 / (T-\theta)\sigma_s^2) \tilde{\Gamma}^*$. Problem (25) is an SDP; by ignoring the nonconvex rank-one constraint, we adopt an interior-point approach to solve it [24]. To proceed, the condition of the optimality to the problem is characterized by showing that problem (24) yields a rank-one solution [25]. By exploiting the two-level-based SDP approach, we solve problem (16) for a given time allocation θ . Then, we consider the optimal solution of the time allocation θ , where problem (7) is equivalently formulated as

$$\max_{\theta} (T-\theta) \left[\log_2 \left(1 + \frac{\theta}{T-\theta} X_s \right) - \log_2 \left(1 + \frac{\theta X_e}{\theta(X_J - 1) + T} \right) \right], \quad (28)$$

$$\text{s.t.} \quad \theta_{\min} < \theta < 1, \quad (29)$$

where $X_e = \arg\max_{k \in [1, K]} X_{e,k}$ and $X_J = \arg\min_{k \in [1, K]} X_{J,k}$. For

convenience and without loss of generality, we substitute X_l into $X_l(\mathbf{w})$, $l \in \{s, e, j\}$.

4. Low-Complexity Scheme

In the previous section, we exploited a global optimal scheme to solve problem (7) via the SDP approach and two-dimensional search. However, this scheme involves two-dimensional search for the slack variable t and time allocation θ , respectively, which introduces a higher computational complexity and is time-consuming. In order to tackle this issue, in this section, we propose a novel low-complexity approach to obtain the optimal time allocation θ in terms of a closed-form expression. This approach can effectively reduce the complexity, since it only involves one-dimensional line search for the slack variable t .

4.1. Optimal Solution to Low-Complexity Scheme. In this subsection, we propose a novel low-complexity scheme to solve problem ((7)), which assumes that the noise-free signal is available at the eavesdroppers, i.e., $\sigma_{e,k}^2 = 0$, $\forall k$. In order to implement the low-complexity scheme, we first rewrite the worst-case secrecy rate as

$$R_{\text{wc}} = \left[\log_2 \left(1 + \frac{\theta}{T-\theta} X_s(\mathbf{w}) \right) - \max_{k \in [1, K]} \log_2 \left(1 + \frac{\bar{X}_{e,k}(\mathbf{w})}{\bar{X}_{j,k}(\mathbf{w})} \right) \right]^+, \quad (30)$$

where $\bar{X}_{e,k} = \eta P_s |h_{e,k}|^2 |\mathbf{h}^H \mathbf{w}|^2$ and $\bar{X}_{j,k} = \eta P_s |f_{j,k}|^2 |\mathbf{g}^H \mathbf{w}|^2$. Thus, the worst-case secrecy rate maximization problem can be formulated as

$$\max_{\mathbf{w}, \theta} (T - \theta) R_{\text{wc}} \quad (31)$$

$$\text{s.t.} \quad \|\mathbf{w}\|^2 \leq 1, 0 < \theta < 1. \quad (32)$$

Problem (31) is not jointly convex for the coupled variables \mathbf{w} and θ . Similar to Section 3, we first fix the time allocation to optimally design the energy beamforming \mathbf{w} , which is omitted here to conserve space. To proceed, we propose the optimal time allocation in a closed form for problem (31) with a given \mathbf{w} . Note that (30) provides a lower bound of the achievable secrecy rate R_s , i.e., $R_s \geq R_{\text{wc}}$. By exploiting the SDP relaxation to design energy beamforming \mathbf{w} , the worst-case secrecy rate can be modified as

$$R_{\text{wc}} = \left[\log_2 \left(1 + \frac{\theta}{T-\theta} X_s \right) - \log_2 \left(1 + \frac{\bar{X}_e}{\bar{X}_j} \right) \right], \quad (33)$$

where $\bar{X}_e = \arg \max_{k \in [1, K]} \bar{X}_{e,k}(\mathbf{w})$ and $\bar{X}_j = \arg \min_{k \in [1, K]} \bar{X}_{j,k}$

(\mathbf{w}). And problem (31) can be rewritten for a given \mathbf{w} as

$$\max_{\theta} \bar{R}_{\text{wc}}(\theta) = (T - \theta) \left[\log_2 \left(1 + \frac{\theta}{T-\theta} X_s \right) - \log_2 \left(1 + \frac{\bar{X}_e}{\bar{X}_j} \right) \right] \quad (34)$$

$$\text{s.t.} \quad \bar{\theta}_{\min} < \theta < 1, \quad (35)$$

where $\bar{\theta}_{\min} = \bar{X}_e / (X_s \bar{X}_j + X_e)$. It is worth noting that problem ((34)) is a special case of ((28)) with the eavesdroppers' noise-free signal, which incurs an upper bound of the eavesdroppers' achievable rate. It is verified that problem (28) is convex in terms of time allocation θ . We first consider that the first-order derivative of the objective function in (28) equals to zero, which is given by

$$\frac{\partial \bar{R}_{\text{wc}}}{\partial \theta} = - \left[\log_2 \left(1 + \frac{\theta}{T-\theta} X_s \right) - \log_2 \left(1 + \frac{\bar{X}_e}{\bar{X}_j} \right) \right] - \frac{1}{\ln 2} \frac{TX_s}{(1 + (\theta/T - \theta)X_s)(T - \theta)} = 0, \quad (36)$$

$$\left(1 + \frac{\theta}{T-\theta} X_s \right) \ln \left(1 + \frac{\theta}{T-\theta} X_s \right) - \left(1 + \frac{\theta}{T-\theta} X_s \right) \cdot \left[1 + \ln \left(1 + \frac{\bar{X}_e}{\bar{X}_j} \right) \right] = X_s - 1. \quad (37)$$

To proceed reformulation, let $z = 1 + (\theta/(T - \theta))X_s$; (37) is equivalently modified as

$$z \ln z - z \left[1 + \ln \left(1 + \frac{\bar{X}_e}{\bar{X}_j} \right) \right] = X_s - 1. \quad (38)$$

The following equations can be derived via a few of the exponential transformations:

$$\begin{aligned} e^{z[\ln z - \ln(e^{1+(\bar{X}_e/\bar{X}_j)})]} &= e^{X_s - 1} \Rightarrow e^{z \ln(z/(e^{1+(\bar{X}_e/\bar{X}_j)}))} = e^{X_s - 1} \\ &\Rightarrow e^{(z/(e^{1+(\bar{X}_e/\bar{X}_j)})) \ln(z/(e^{1+(\bar{X}_e/\bar{X}_j)}))} \\ &= e^{(X_s - 1)/e^{1+(\bar{X}_e/\bar{X}_j)}} \\ &\Rightarrow e^{\ln(z/(e^{1+(\bar{X}_e/\bar{X}_j)}))} \ln \left(\frac{z}{e^{1+(\bar{X}_e/\bar{X}_j)}} \right) \\ &= \frac{X_s - 1}{e^{1+(\bar{X}_e/\bar{X}_j)}}. \end{aligned} \quad (39)$$

By exploiting Lambert W function, (39) is equivalent

to the following equality:

$$\ln \left(\frac{z}{e(1 + (\bar{X}_e/\bar{X}_j))} \right) = W \left(\frac{X_s - 1}{e(1 + (\bar{X}_e/\bar{X}_j))} \right), \quad (40)$$

where $W(\cdot)$ represents the Lambert W function. Thus, the optimal time allocation can be derived as

$$\theta^* = \frac{\left[e^{W((X_s-1)/(e(1+(\bar{X}_e/\bar{X}_j))))+1} (1 + (\bar{X}_e/\bar{X}_j)) - 1 \right] T}{X_s - 1 + e^{W((X_s-1)/(e(1+(\bar{X}_e/\bar{X}_j))))+1} (1 + (\bar{X}_e/\bar{X}_j))}. \quad (41)$$

By exploiting the property of the Lambert W function $e^{W(x)} = x/W(x)$, (41) can be further equivalently simplified as

$$\theta^* = \frac{[1 - W[(X_s - 1)(\bar{X}_j / ((\bar{X}_e + \bar{X}_j)e))] / (X_s - 1)] T}{W[(X_s - 1)(\bar{X}_j / ((\bar{X}_e + \bar{X}_j)e)) + 1]}. \quad (42)$$

By exploiting (42), we derived the optimal time allocation in terms of a closed-form expression for given energy beamforming \mathbf{w} . Thus, in order to optimally obtain the worst-case achievable secrecy rate, we present an alternating optimization algorithm to iteratively design energy beamforming \mathbf{w} and time allocation θ , respectively, which is guaranteed to converge to satisfy the Karush-Kuhn-Tucker (KKT) conditions of problem (31).

4.2. Special Case. In the previous subsection, we have optimally designed the time allocation in terms of a closed-form expression to propose the low-complexity schemes. This optimal time allocation fits within generic worst cases of the achievable secrecy rate. In this subsection, we characterize the optimal time allocation for two special cases in terms of signal-to-interference-plus-noise ratio (SINR) regions of the eavesdroppers. First, we derive the optimal time allocation in low-SINR region, e.g., $\bar{X}_e < \bar{X}_j$. Thus, according to (42), the optimal time allocation can be further approximated as

$$\theta_{\text{low}}^* = \frac{[1 - (W((X_s - 1)/e) / (X_s - 1))] T}{W((X_s - 1)/e) + 1}. \quad (43)$$

The optimal solution (43) releases a fact that secure WPSN system is degraded into the conventional WPSN-based rate maximization, where the jamming node introduces extra interference which has a prominent role to design the time allocation similar to the case that the reception of the eavesdroppers is too small to be ignored. In addition, the scenario of higher-SINR region at the eavesdroppers is characterized, where $\bar{X}_e \gg \bar{X}_j$ holds. Thus, for the higher SINR

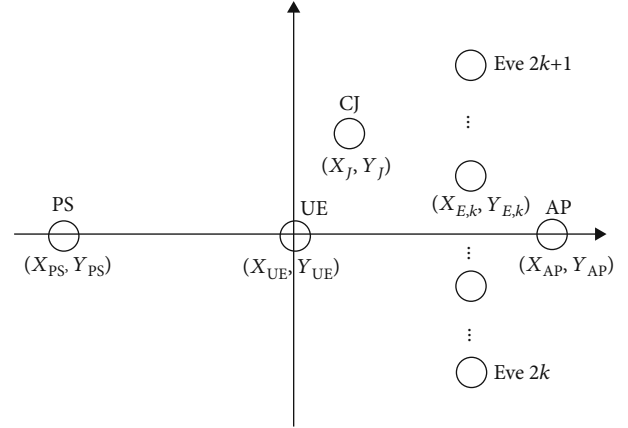


FIGURE 2: System deployment.

case, (42) can be further simplified as

$$\theta_{\text{high}}^* = \frac{[1 - W[(X_s - 1)(\bar{X}_j / e\bar{X}_e)] / (X_s - 1)] T}{W[(X_s - 1)\bar{X}_j / e\bar{X}_e + 1]}. \quad (44)$$

This scenario unveils the fact that more energy time is allocated to the WPT phase for the UE while the jamming node also needs more sufficient energy collected from the PS to introduce extra interference to degrade the reception of the eavesdroppers.

5. Numerical Results

In this section, we present the numerical results to evaluate the performance of the proposed scheme in the secure WPSN system. In simulation, we take into consideration the system deployment as shown in Figure 2 to describe the system model, where the PS, the UE, the CJ, and the AP are located $(X_{PS}, Y_{PS}) = (-50, 0)$, $(X_{UE}, Y_{UE}) = (0, 0)$, and $(X_J, Y_J) = (20, 8)$, and $(X_{AP}, Y_{AP}) = (50, 0)$, respectively. Also, all of eavesdroppers are located at $(X_{E,k}, Y_{E,k}) = (30, n * l/2)$ when $n = 1, \dots, 2 * k + 1$, or $(X_{E,k}, Y_{E,k}) = (30, -(n - 1) * k/2)$ when $n = 2, \dots, 2 * k$, where l denotes the interval between two neighbouring eavesdroppers. The channel coefficient is composed of distance-dependent path loss model and small-scale fading, where the path loss model is set to $PL = Ad^{-\kappa}$, where $A = 10^{-3}$, κ is the path loss exponent, and d represents the distance between any two devices, i.e., the PS and UE, the PS and the CJ, the UE and the AP, the UE and the eavesdroppers, and the CJ and the eavesdroppers. All small-scale channel coefficients are generated to follow Rayleigh fading. Also, we set $P_s = 20$ dBm, $\eta = 0.8$, and $\sigma^2 = -150$ dBm unless otherwise stated. In order to highlight the proposed scheme, we evaluate the performance of the benchmark schemes in comparison to the proposed scheme. Specifically, we take into consideration two benchmark schemes: (1) maximum ratio transmission (MRT) scheme, in this way, the direction of the energy beamformer is consistent with channel \mathbf{h} ; (2) equal time allocation (ET) scheme, where the transmission time is equally allocated for both WET and WIT durations.

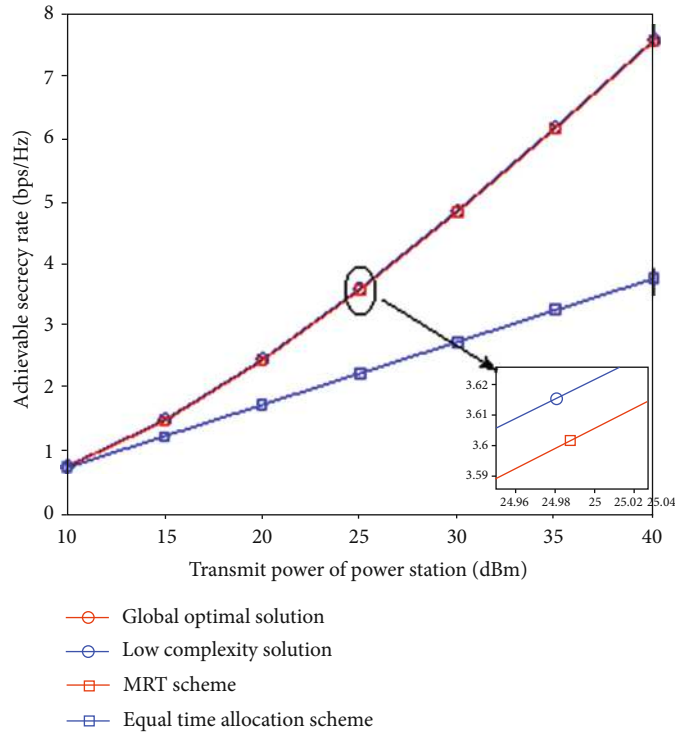


FIGURE 3: Achievable secrecy rate versus transmit power at PS.

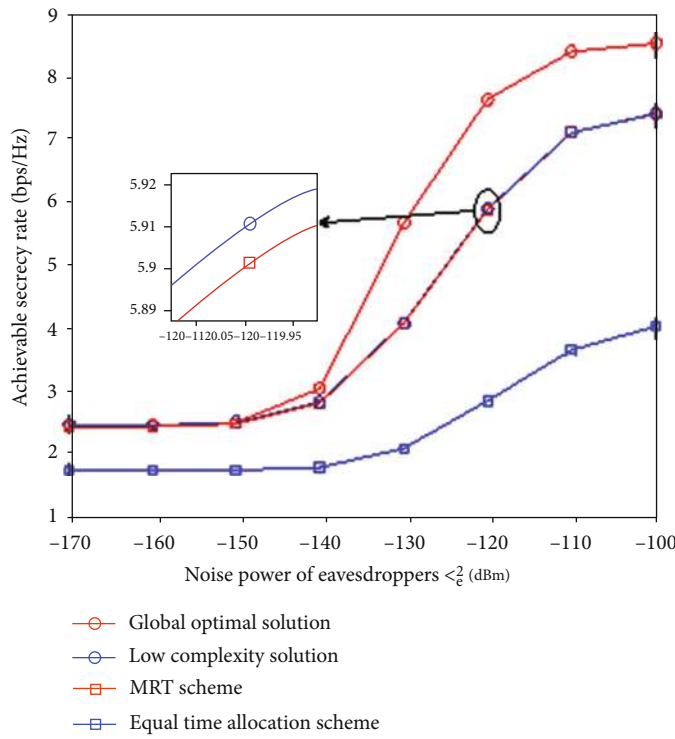


FIGURE 4: Achievable secrecy rate versus noise power.

First, Figure 3 presents the achievable secrecy rate versus transmit power at the PS P_s . From this figure, it can be seen that the achievable secrecy rate increases with P_s in terms

of each scheme. This releases that larger transmit power at the PS can guarantee the reliability of the WIT. Also, the proposed low-complexity scheme can achieve the same

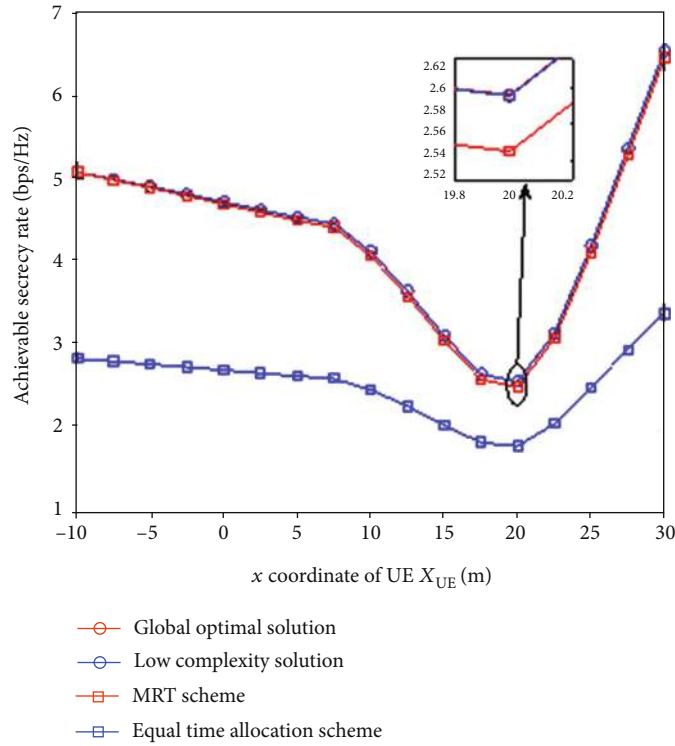


FIGURE 5: Achievable secrecy rate versus UE x -coordinate.

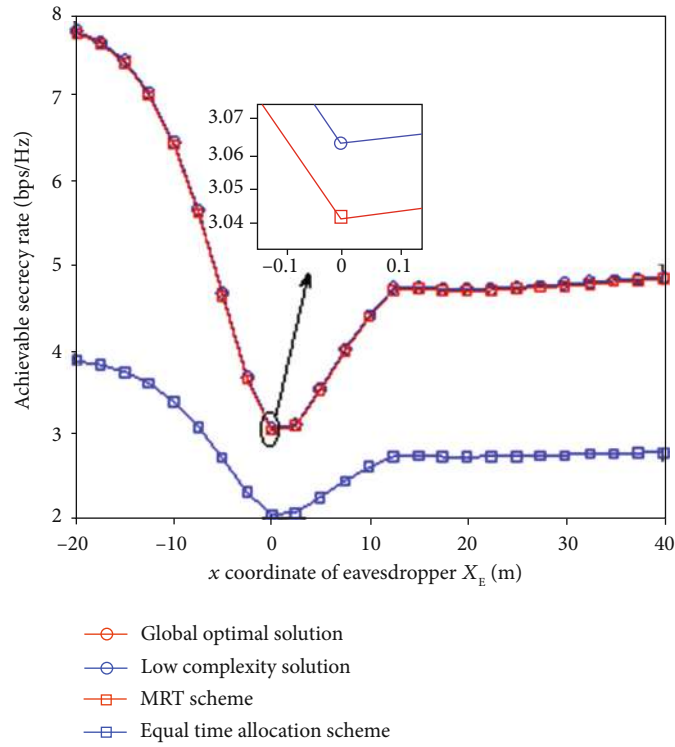


FIGURE 6: Achievable secrecy rate versus eavesdropper x -coordinate.

achievable secrecy rate as the global optimal scheme, which validates the correctness and effectiveness of the derivations in Section 4. In addition, we evaluate the performance of the proposed scheme against the benchmark schemes, it is

shown that the proposed scheme is superior to the MRT scheme and outperforms the ET scheme in terms of the achievable secrecy rate. This effectively highlights the importance of the optimal time allocation in our proposed scheme.

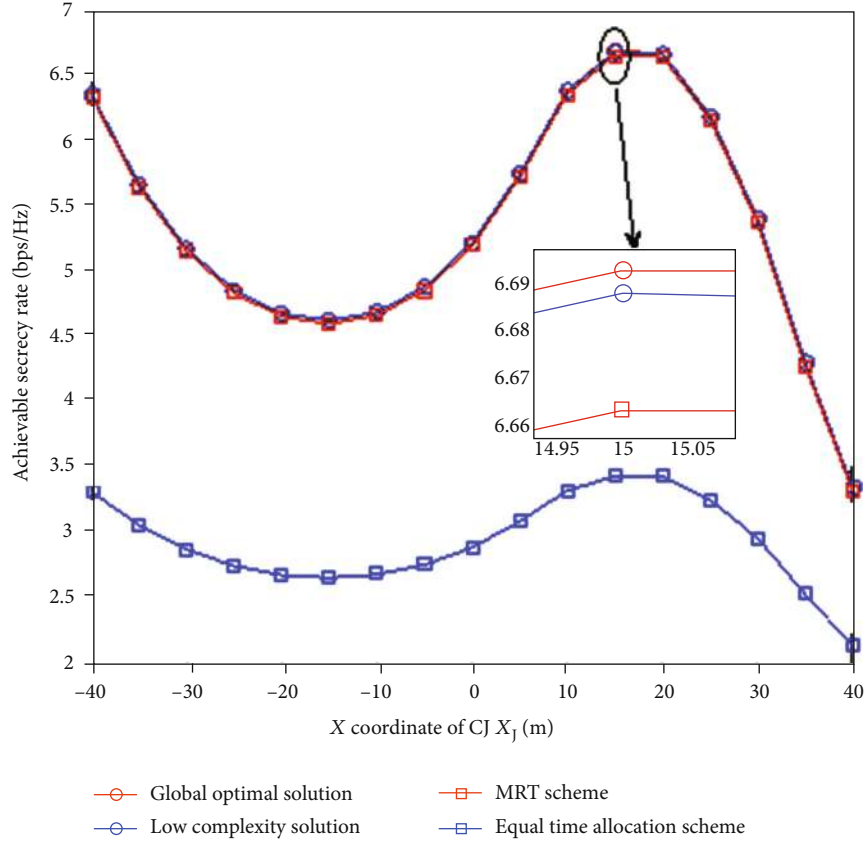


FIGURE 7: Achievable secrecy rate versus CJ x -coordinate.

Next, we evaluate the impact of the noise power of eavesdroppers σ_e^2 on the achievable secrecy rate in Figure 4. These results clearly show that, if the noise power σ_e^2 is relatively low, the proposed low-complexity scheme has the same performance with the global optimal scheme in terms of achievable secrecy rate. As σ_e^2 increases, the proposed low-complexity scheme shows a degradation in terms of the achievable secrecy rate in comparison to the global optimal scheme. This is due to the fact that the eavesdroppers are not able to decode the overheard signal in the high-noise power region σ_e^2 , such that the low-complexity scheme can be considered in a low-noise power region to design a secure WPSN. Also, the low-complexity scheme slightly outperforms the MRT scheme and obtains higher achievable secrecy rate than the ET scheme.

Then, the impact of the deployment of the UE, the eavesdroppers, and the CJ on the achievable secrecy rate is evaluated. In Figure 5, the achievable secrecy rate versus the x -coordinate of the UE X_{UE} is presented, where the achievable secrecy rate first decreases and then has an increasing trend after $X_{UE} = 20$ m for each scheme. This confirms the optimal deployment of the UE, where the UE is deployed nearer to the AP or PS to gain a higher achievable secrecy rate. In Figure 6, we present that the achievable secrecy rate versus the x -coordinate of the eavesdroppers X_E , where the achievable secrecy rate has an obviously decreasing trend and then increases after $X_E = 0$ m for each scheme; also,

the achievable secrecy rate gradually achieves a stable trend after approximately $X_E = 12$ m. Similar arguments in Figures 5 and 6 can be justified with Figure 3, where the proposed low-complexity scheme achieves the same performance with the global optimal scheme and outperforms the MRT and ET schemes in terms of the achievable secrecy rate.

Finally, the impact of the deployment of the CJ has been evaluated. Specifically, Figure 7 shows that the achievable secrecy rate has a decreasing trend when the x -coordinate of the CJ X_j is small and increases as X_j is located from -15 m to 15 m and then will decline again after that. This confirms the optimal deployment of the CJ, where it is deployed nearer to the PS or in the vicinity of the UE to achieve a higher achievable secrecy rate. This is because this deployment enables the CJ to obtain a higher energy harvesting efficiency to introduce a higher interference to degrade the reception of the eavesdroppers. In addition, the proposed low-complexity scheme is matched with the global optimal scheme, as well as outperforms the MRT and the ET schemes in terms of the achievable secrecy rate.

6. Conclusion

This paper investigated a secure WPSN with the assistance of a CJ. The PS provides wireless energy for a UE and the CJ to secure information transfer to the AP and introduce

extra interference to the eavesdroppers, respectively. Our aim is to jointly design the secure beamformer and the energy time allocation via maximizing the secrecy throughput at the AP. Due to nonconvexity of the formulated problem, we first propose a global optimal solution which employs the semidefinite programming (SDP) relaxation. In addition, we investigate a worst-case scenario, where the closed-form expression of energy time allocation is derived. Finally, our proposed schemes have been validated through the numerical results, which highlight that the jammer plays an improving role in the secure WPSN.

Data Availability

The (Matlab) data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the Xinjiang Uygur Autonomous Region Natural Science Foundation Project (2019D01C033), National Natural Science Foundation Project (61771416 and U1903213), the Basic and Frontier Technology Research Project of Henan Province, and 2020 Science and Technology Research Project of Henan Province (202102210122); in part by the Natural Science Foundation of China (NSFC) under Grant 61901370; in part by the Special Research Project of Education Department of Shanxi Province under Grant 19JK0794; and in part by the Open Fund of the Shanxi Key Laboratory of Information Communication Network and Security under Grant ICNS201801.

References

- [1] Z. Chu, F. Zhou, Z. Zhu, R. Q. Hu, and P. Xiao, "Wireless powered sensor networks for internet of things: maximum throughput and optimal power allocation," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 310–321, 2018.
- [2] S. Bi, C. K. Ho, and R. Zhang, "Wireless powered communication: opportunities and challenges," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 117–125, 2015.
- [3] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.
- [4] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 4, pp. 1678–1690, 2014.
- [5] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, pp. 1833–1847, 2015.
- [6] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Transactions on Signal Processing*, vol. 59, no. 8, pp. 3799–3812, 2011.
- [7] F. Zhou, Z. Li, J. Cheng, Q. Li, and J. Si, "Robust AN-aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT," *IEEE Transactions on Wireless Communications*, vol. 16, no. 4, pp. 2450–2464, 2017.
- [8] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4599–4615, 2014.
- [9] D. W. K. Ng and R. Schober, "Secure and green SWIPT in distributed antenna networks with limited backhaul capacity," *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 5082–5097, 2015.
- [10] X. Li, M. Zhao, X.-C. Gao et al., "Physical layer security of cooperative NOMA for IoT networks under I/Q imbalance," *IEEE Access*, vol. 8, pp. 51189–51199, 2020.
- [11] X. Li, M. Zhao, Y. Liu, L. Li, Z. Ding, and A. Nallanathan, "Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance," *IEEE Transactions on Vehicular Technology*, p. 1, 2020.
- [12] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 1, pp. 418–428, 2014.
- [13] Y. Cheng, P. Fu, Y. Chang, B. Li, and X. Yuan, "Joint power and time allocation in full-duplex wireless powered communication networks," *Mobile Information Systems*, vol. 2016, Article ID 4845865, 15 pages, 2016.
- [14] X. Kang, Y.-C. Liang, and J. Yang, "Riding on the primary: a new spectrum sharing paradigm for wireless-powered IoT devices," *IEEE Transactions on Communications*, vol. 17, no. 9, pp. 6335–6347, 2018.
- [15] J. Wang, X. Kang, Y. Liang, and S. Sun, "An energy harvesting chain model for wireless-powered IoT networks," in *2018 10th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–6, Hangzhou, China, 2018.
- [16] E. Boshkovska, D. W. K. Ng, N. Zlatanov, A. Koelpin, and R. Schober, "Robust resource allocation for MIMO wireless powered communication networks based on a non-linear EH model," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 1984–1999, 2017.
- [17] K. Huang and X. Zhou, "Cutting the last wires for mobile communications by microwave power transfer," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 86–93, 2015.
- [18] K. Huang and V. K. N. Lau, "Enabling wireless power transfer in cellular networks: architecture, modeling and deployment," *IEEE Transactions on Wireless Communications*, vol. 13, no. 2, pp. 902–912, 2014.
- [19] J. Moon, H. Lee, C. Song, and I. Lee, "Time allocation methods for secure wireless powered communication networks," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, Chicago, IL, USA, USA, 2018.
- [20] M. Zhang, K. Cumanan, J. Thiyagalingam et al., "Energy efficiency optimization for secure transmission in MISO cognitive radio network with energy harvesting," *IEEE Access*, vol. 7, pp. 126234–126252, 2019.
- [21] M. Zhang, K. Cumanan, L. Ni, H. Hu, A. G. Burr, and Z. Ding, "Robust beamforming for AN aided MISO SWIPT system with unknown eavesdroppers and non-linear eh model," in

- 2018 *IEEE Globecom Workshops (GC Wkshps)*, pp. 1–7, Abu Dhabi, United Arab Emirates, United Arab Emirates, 2018.
- [22] L. Ni, X. Da, H. Hu, M. Zhang, and K. Cumanan, “Outage constrained robust secrecy energy efficiency maximization for EH cognitive radio networks,” *IEEE Wireless Communications Letters*, vol. 9, no. 3, pp. 363–366, 2020.
- [23] Q. Li and W.-K. Ma, “Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization,” *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2704–2717, 2013.
- [24] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, Cambridge, UK, 2004.
- [25] Z. Chu, Z. Zhu, M. Johnston, and S. Y. Le Goff, “Simultaneous wireless information power transfer for MISO secrecy channel,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 6913–6925, 2016.
- [26] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, “Transmit solutions for MIMO wiretap channels using alternating optimization,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1714–1727, 2013.