IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received January 28, 2021, accepted February 2, 2021, date of publication February 10, 2021, date of current version February 22, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3058504

On the Secrecy for Relay-Aided SWIPT Internet of Things System With Cooperative Eavesdroppers

KANG SONG[1,2,3], (Member, IEEE), MENGYUN NIE[1], JING JIANG[3], (Member, IEEE), CHUNGUO LI[2], (Senior Member, IEEE), AND YONGFENG YIN[4], (Member, IEEE)

[1]College of Electronic and Information Engineering, Qingdao University, Qingdao 266071, China
[2]School of Information Science and Engineering, Southeast University, Nanjing 210096, China
[3]Shaanxi Key Laboratory of Information Communication Network and Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
[4]School of Reliability and Systems Engineering, Beihang University, Beijing 100191, China

Corresponding author: Yongfeng Yin (yyf@buaa.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61901241, Grant 61941115, Grant 61671144, Grant 61871321, and Grant 61801257; in part by the Shandong Provincial Natural Science Foundation, China, under Grant ZR2017BF028 and Grant ZR2019BF001; in part by the Key Laboratory Foundation of Science and Technology on Reliability and Environmental Engineering Laboratory under Grant 6142004190401; in part by the Aviation Science Foundation of China under Grant 20170751006; and in part by the Open Research Funds of Shaanxi Key Laboratory of Information Communication Network and Security under Grant ICNS201903.

ABSTRACT In this paper, the secrecy performance in internet of things (IoTs) networks with cooperative eavesdroppers has been investigated, where simultaneous wireless information and power transfer (SWIPT) nodes perform as relay nodes. The secrecy energy efficiency (SEE) maximization problem for single relay node has been introduced to extend the life-time for IoT nodes without power supply. The optimization problem is firstly transformed into two sub-problems, and then each sub-problem is solved by bisection method. Furthermore, the model has been extended into multiple relay nodes and a novel relay selection algorithm for SEE maximization has been proposed. Finally, the advantage of the proposed algorithm has been verified from simulations.

INDEX TERMS IoT, multiple eavesdroppers, secrecy energy efficiency, SWIPT, relay.

I. INTRODUCTION

With the rapid development of sensor, communication and network technologies, the number of IoT nodes increases exponentially. Especially, more and more wearable, implantable and intracorporal IoT nodes has been widely deployed to collect physiological and psychological data for health care and monitoring. In order to achieve these goals, these specific IoT nodes are usually very small and battery powered, which brings great challenges to the energy efficiency (EE) [1]–[3]. Therefore, it has been attracting the attention of many researchers in recent years. And many studies have been dedicated to EE optimization problem in IoT networks [4]–[6]. In [4], a novel power allocation algorithm aiming at maximizing EE with low-complexity was proposed. A power allocation method for a distributed antenna system (DAS) to maximize EE was studied in [5]. The energy efficiency and the spectral efficiency for orthogonal frequency division multiplexing (OFDM)-based visible light communication schemes were investigated in [6].

Moreover, for some kinds of IoT nodes, e.g. implantable nodes, it is impractical to powered by battery or even impossible to change its battery components [7]. Nevertheless, the battery life is far from meeting people's needs. Consequently, chargeable nodes with wireless energy harvesting has been considered as the potential candidate for IoT nodes in smart health and emotion care networks [8]. In [9], data transmission in a DF energy harvesting (EH) relay-assisted network was considered, where BS's energy efficiency maximization problem has been investigated. The resource allocation for energy harvesting-based direct communication system has been studied in [10], where the weighted energy efficiency maximization problem has been solved by leveraging a game-theoretic learning approach.

Cooperative communication has been proven to be an efficient method to enhance the performance of the communication system [11]–[14], which could also be employed to improve the energy efficiency of IoT networks. However,

The associate editor coordinating the review of this manuscript and approving it for publication was Arturo Conde.

in the view of the broadcast characteristics of wireless signals, there are also great security problems in IoT networks, especially in cooperative IoT networks [15]–[18]. Many people have studied the security rate problem based on eavesdropping channel, especially in physical layer [19], [20]. The security rate formula was first introduced in [21]. In [22], secrecy capacity for amplify-and-forward relay networks with EH-based relay has been analyzed, where legitimate destination works as artificial noise source. In [23], the authors investigated the antenna selection problem without the channel state information (CSI) of eavesdropping channel. The secrecy outage probability for cooperative eavesdroppers for DF relay networks is analyzed in [24]. With the development of the green communication, some researchers combined energy efficiency and secrecy capacity, which is much more practical. In [25], a beamforming design algorithm to achieve energy efficiency optimization in MIMO multi-user systems has been proposed, where secrecy capacity constraints has been considered. In [26], distributed beamforming scheme for both transmission nodes and artificial noise generator has been proposed for heterogeneous networks with SWIPT. A power splitting (PS) relaying strategy with distributed beamforming has been investigated for multiple relay networks in [27]. In [28] and [29], the secrecy energy efficiency (SEE) for save-then-transmit energy harvesting system with single eavesdropper has been studied, where optimal energy absorption rate for the system has been obtained.

As far as we know, there is few literature on the secrecy energy efficiency for relay-aided SWIPT IoT system with cooperative eavesdroppers. In this paper, firstly, we study the secrecy energy efficiency in SWIPT IoT-based networks with multiple eavesdroppers where those eavesdroppers cooperate to eavesdrop the signal from the source, which is much more general than single eavesdropper scenario. And the optimal transmit power P_S and power splitting coefficient ρ are derived to maximize the instantaneous secrecy energy efficiency. Then we further proposed the optimal relay selection scheme through joint optimization. Finally, the numerical simulation is performed, and our derivations have been verified by simulation.

The rest of this paper is organized as follows: Section 2 provides an overview of the system model and introduces relevant variables. The secrecy energy efficiency maximization problem is presented in Section 3. And in Section 4, we transform the original problem into two sub-problems, and introduce the concrete steps of solving the optimization problem. Furthermore, we extend the model into multiple relays and investigate the relay selection scheme in Section 5. In Section 6, numerical results are presented to demonstrate the effectiveness of the proposed algorithm.

II. SYSTEM MODEL

In this paper, we consider a relay-assisted IoT system including a source S, a battery-enabled relay R, a destination D and n eavesdroppers $\{E_1, E_1, \ldots, E_n\}$, as depicted in Fig. 1. Each device within the network is equipped with single antenna.

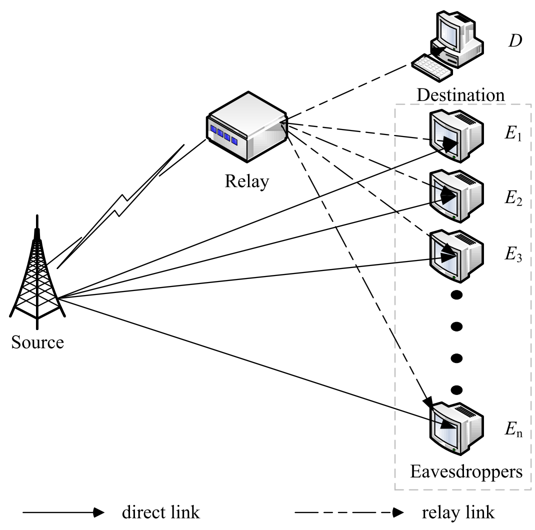


FIGURE 1. System model for single relay.

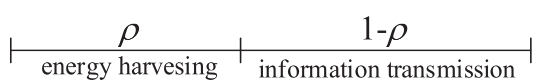


FIGURE 2. PS protocol model.

And the system based on PS protocol of SWIPT. Considering the actual communication environment, there exist direct links between the source S and eavesdroppers while S to the destination without direct links. The relay contains an energy harvester, an information decoder and operates in a DF mode, where the total receive power of relay node is divided into two different parts, as depicted in Fig. 2.

We assume that the channel model is Rayleigh fading channel, in which the channel coefficients have independent and same distribution, and remain unchanged in a transmission process. It is assumed that there is a perfect CSI for all transmissions known at the destination node. The whole system works as follows: in the first phase, S transmits energy which is used for energy harvesting and signal transmission to R. In the second phase, R uses the harvested energy to retransmit the received signal to D. In addition, we consider the energy collection and decoding time of the relay to be negligible.

We define the normalized information signal transmitted by the source and relay as s and x which satisfy $E\left\{|s|^2\right\} = 1$ and $E\left\{|x|^2\right\} = 1$. What's more, P_S and P_R denote the transmit power at the source and relay respectively. Due to the power limitation, the transmit power at the source is limited, and the maximum of P_S is denoted as P_{Smax}.

The energy is transmitted from S to R and then the received power at R is divided into two parts which is used for the energy absorption and signal transmission respectively. The received signal at the relay node and i-th eavesdropper can be given by

$$y_R = \sqrt{P_S}hs + n_{SR} \tag{1}$$

$$y_{SEi} = \sqrt{P_S} h_{Ei} s + n_{SEi} \tag{2}$$

where h and h_{Ei} denote the channel coefficients in the S-relay link and S-eavesdropper link, respectively. n_{SR} and n_{SEi} are the additive white Gaussian noise (AWGN) at the relaying and eavesdropping end respectively, which is an independent and identically distributed (i.i.d.) complex Gaussian random variable with zero mean and variance σ_R^2, σ_E^2 respectively. When the desired signal is received from the source, the relay decodes it to obtain an estimate of the original signal. The signal received at the legitimate destination and the eavesdropping end can be expressed as

$$y_D = \sqrt{P_R} g_D x + n_{RD} \tag{3}$$
$$y_{REi} = \sqrt{P_R} g_{Ei} x + n_{REi} \tag{4}$$

where g_D and g_{Ei} denote the channel coefficients in the relay-destination link and relay-eavesdropper link, respectively. n_{RD} and n_{REi} are the AWGN at the destination and eavesdropping end respectively.

According to the PS protocol, in this model, part of the total energy is treated as harvested energy, and the rest is used for data transmission. The energy absorbed by the relay can be gained by

$$Q = P_S \rho |h|^2 T \tag{5}$$

The average power of the relay during the data transmission satisfies

$$P_R = \frac{E[Q]}{T} = P_S \rho |h|^2 T \tag{6}$$

The total power consumption for the system can be given by

$$P_{total} = P_C + P_S \tag{7}$$

where P_C is the total circuits consumptions. From equation (1) and (2), we can derive the SNR at the relay node and eavesdropper in the direct link for the transmission as

$$\gamma_{SR} = \frac{P_S(1-\rho)|h|^2}{\sigma_R^2} \tag{8}$$
$$\gamma_{SEi} = \frac{P_S|h_{Ei}|^2}{\sigma_{SE_i}^2} \tag{9}$$

The effective SNR of the relay-destination and relay-eavesdropper links are given as

$$\gamma_{RD} = \frac{P_R|g_D|^2\rho}{\sigma_D^2} \tag{10}$$
$$\gamma_{REi} = \frac{P_R|g_{Ei}|^2\rho}{\sigma_{Ei}^2} \tag{11}$$

from equations (8), (9), (10) and (11) and by using (6), we have

$$\gamma_{SR} = \frac{P_S(1-\rho)|h|^2}{\sigma_R^2} \tag{12}$$
$$\gamma_{SEi} = \frac{P_S|h_{Ei}|^2}{\sigma_{SE_i}^2} \tag{13}$$
$$\gamma_{RD} = \frac{P_S|g_D|^2|h|^2}{\sigma_D^2} \tag{14}$$
$$\gamma_{REi} = \frac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2} \tag{15}$$

The maximal ratio combiner (MRC) has been considered to estimate the worst case of the information leakage. The total received SNR for all eavesdroppers after combining the received signals by the usage of the MRC can be given by

$$\gamma_E = \sum_{i=1}^{n} (\gamma_{REi} + \gamma_{SEi}) = \sum_{i=1}^{n} \left(\frac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2} + \frac{P_S|h_{Ei}|^2}{\sigma_{SE_i}^2} \right) \tag{16}$$

Therefore, the capacity between different links can be expressed as

$$R_{SR} = \log_2(1+\gamma_{SR}) = \log_2\left(1 + \frac{P_S(1-\rho)|h|^2}{\sigma_R^2}\right) \tag{17}$$

for S-R and

$$R_{RD} = \log_2(1+\gamma_{RD}) = \log_2\left(1 + \frac{P_S|g_D|^2|h|^2\rho}{\sigma_D^2}\right) \tag{18}$$

for $R-D$ and

$$\begin{aligned} R_E &= \log_2(1+\gamma_E) \\ &= \log_2\left(1 + \sum_{i=1}^{n}\left(\frac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2} + \frac{P_S|h_{Ei}|^2}{\sigma_{SE_i}^2}\right)\right) \end{aligned} \tag{19}$$

for the link including E.

let $\gamma = \min\{\gamma_{SR}, \gamma_{RD}\}$, $R = \min\{R_{SR}, R_{RD}\}$ then secrecy capacity of the system is

$$R_S = R - R_E = \log_2\left(\frac{1+\gamma}{1+\gamma_E}\right) \tag{20}$$

The secrecy energy efficiency of the model is defined as

$$U = \frac{R_S}{P_S + P_C} \tag{21}$$

which is a function of P_S and ρ. Therefore, The SEE could also be written as $U(P_S, \rho)$.

III. MAXIMIZATION OF THE SECURE ENERGY EFFICIENCY

In this section, we investigate the maximization of the secrecy energy efficiency related to the source's power P_S and power splitting coefficient ρ. In general, the resource allocation under secrecy energy efficiency optimization could be expressed as

$$\begin{aligned} &\max U(P_S, \rho) \\ &s.t.\ 0 < \rho < 1 \\ &\quad 0 < P_S < P_{\max} \end{aligned} \tag{22}$$

where $P_{\max}$ is the base station's power limitation. Obviously, it's a piecewise function, we can get the expression for segment point $\rho^* = \frac{\sigma_D^2}{\sigma_R^2 |g_D|^2}$ from $\gamma_{SR} = \gamma_{RD}$. It's impossible for the power splitting coefficient ρ to get the value of 0 or 1, which means that there is no energy absorption before transmission or no signal transfer in the system, respectively. We optimize P_S and ρ successively in each segment.

IV. MODEL SOLUTION

The maximization of SEE should be discussed in two segments by comparing sizes γ_{SR} and γ_{RD}. We could get that segment point $\rho^* = \frac{\sigma_D^2}{\sigma_R^2 |g_D|^2}$. Consequently, the objective function (22) can be rewrite as follows.

(i). When $\rho \in (0, \rho^*)$, $\gamma_{SR} > \gamma_{RD}$, so $\gamma = \gamma_{RD}$. Eq. (22) could be rewritten as

$$\max \frac{\log_2\left(\frac{1+\gamma_{RD}}{1+\gamma_E}\right)}{P_S + P_C}$$
$$s.t.\ 0 < \rho < \rho^*$$
$$0 < P_S < P_{\max} \tag{23}$$

(ii). When $\rho \in (\rho^*, 1)$, $\gamma_{SR} < \gamma_{RD}$, so $\gamma = \gamma_{SR}$. Eq. (22) could be rewritten as

$$\max \frac{\log_2\left(\frac{1+\gamma_{SR}}{1+\gamma_E}\right)}{P_S + P_C}$$
$$s.t.\ \rho^* < \rho < 1$$
$$0 < P_S < P_{\max} \tag{24}$$

Problem (22) has the following lemmas based on iteration algorithm in each case. We could receive that there exists the optimal values as for two variables ρ and P_S through lemmas.

A. CASE 1 $\rho \in (0, \rho^*)$

Lemma 1: When $\rho \in (0, \rho^*)$, there exists $P_S^* \in (0, P_{S\max})$, $\rho_1^* \in (0, \rho^*)$ make U reach the maximum, especially $\rho_1^* = \rho^*$.

Proof: In this segment, the solution process is as follows.

With the fixed P_S, we analyzed the first partial derivative of ρ as Eq. (25) on the bottom of the next page. From (25), we could find $\frac{\partial U}{\partial \rho} > 0$ which means that U monotonously increases for ρ, so $\rho_1^* = \rho^*$ is the optimal value. Then with the fixed ρ, we analyzed U first partial derivative to P_S as Eq. (26) on the bottom of the next page.

It's obviously that $(P_S + P_C)^2 > 0$, so we can tell what is the sign of the fraction just by the sign of the numerator Y, let the derivation of Y relative to PS is as Eq. (28) on the bottom of the next page. Due to the fact that $\lim_{P_S \to 0} Y > 0$ and $\lim_{P_S \to \infty} Y < 0$, U is monotonously decreasing.

We could draw a conclusion that there is a unique P_S^*, which satisfies U is monotonously increases when $P_S < P^*$ and U is monotonously decreases when $P_S > P^*$, we could get P^* via making $Y = 0$. ■

Algorithm 1 Transmit power optimization algorithm for SEE maximization

1: Initialize $P_0 = 0$, $P_1 = P_{S\max}$, $P_S^* = 0, f = \frac{\partial U}{\partial P_S}$
2: **while** $f(P_S^*)$ is larger than the threshold **do**
3: $\quad P_S^* = \frac{P_0+P_1}{2}$
4: $\quad$**if** $f(P_0)f(P_S) > 0$ **then**
5: $\quad\quad P_0 = P_S$
6: $\quad$**else**
7: $\quad\quad P_1 = P_S$
8: $\quad$**end if**
9: **end while**
10: **return** P_S^*

B. CASE 2 $\rho \in (\rho^*, 1)$

Lemma 2: When $\rho^* \in (\rho^*, 1)$, there exists $P_S^* \in (0, P_{S\max})$, $\rho_2^* \in (\rho^*, 1)$ to make the U reach the maximum, especially $\rho_2^* = \rho^*$.

Proof: When $(\rho^*, 1)$, the objective function is described as (24).

Similar to case 1, with the fixed P_S and ρ, We analyze the partial derivatives of U with respect to ρ and P_S as Eq. (29) and Eq. (30) on the bottom of the next page, respectively. It could be obtain that U monotonously decreases for ρ, so ρ^* is the only optimal value, which is correspondent to segment 1. Secondly, let we could find $\frac{\partial Y}{\partial P_S}$ as Eq. (32) on the bottom of the next page and

$$\begin{cases} \lim_{P_S \to 0} Y > 0 \\ \lim_{P_S \to \infty} Y < 0 \end{cases} \tag{33}$$

Consequently, in function $U(P_S, \rho)$, U increases monotonically with the growth of P_S at first, and then decreases monotonically with the growth of P_S, there exists only one value of P_S (i.e. P_S^*) to maximize the value of U. ■

By synthesizing the above two cases, regardless of the value range of subsection point ρ^*, SEE can always reach a maximum value. Hence, we can derive the following theorem.

Theorem 1: There exists $\rho \in (0, 1)$ and $P_S \in (0, P_{S\max})$ to get the optimal SEE.

Based on theorem above, The extreme value of ρ is independent of P_S. For SEE, there is an unique point P_S^* between 0 and $P_{S\max}$ to achieve the maximum. And the optimal secrecy energy efficiency could be derived by Algorithm 1.

V. RELAY SELECTION

In this section, the source communicates with the destination and with the assistance of relays $\{R_1, R_2 \ldots R_k\}$ as shown in Fig. 3. All nodes of the relays equip with the single antenna. Using DF relaying protocol, k relay nodes are introduced for assisting the transmission from S to D. Meanwhile, several eavesdroppers attempt to intercept legitimate transmission from both the S and R. Accordingly, the selection problem can be formulated as

$$\begin{aligned} &\max U_k\left(\rho_k, P_{sk}\right) \\ &s.t.\ 0<\rho_k<1 \\ &\qquad 0<P_{sk}<P_{\max} \end{aligned} \tag{34}$$

Note that U_k, P_{sk} and ρ_{sk} are the SEE of the system, the transmit power and power splitting factor of kth relay when kth relay has been selection.

To find the solution in the relay selection, we first calculate the secrecy energy efficiency for each relay. Then the relay with the highest SEE is selected as the optimal relay. The specific summary of the relay selection algorithm is shown in

$$\frac{\partial U}{\partial \rho}=\frac{\sigma_D^2\left[\frac{P_S|g_D|^2|h|^2}{\sigma_D^2}+\sum_{i=1}^{n}\frac{P_S^2|h_{Ei}|^2|g_D|^2|h|^2}{\sigma_{SEi}^2\sigma_D^2}-\sum_{i=1}^{n}\frac{P_S|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}\right]}{\ln 2\left(P_S+P_C\right)\left(\sigma_D^2+P_S\rho|g_D|^2|h|^2\right)\left(1+\sum_{i=1}^{n}\left(\frac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\frac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)}>0 \tag{25}$$

$$\frac{\partial U}{\partial P_S}=\frac{\dfrac{\sigma_D^2\left[\frac{|g_D|^2|h|^2\rho}{\sigma_D^2}-\sum_{i=1}^{n}\left(\frac{\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\frac{|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right](P_S+P_C)}{\ln 2\left(\sigma_D^2+P_S\rho|g_D|^2h^2\right)\left(1+\sum_{i=1}^{n}\left(\frac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\frac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)}-\log_2\left(\dfrac{\sigma_D^2+P_S\rho|g_D|^2|h|^2}{\sigma_D^2\left(1+\sum_{i=1}^{n}\left(\frac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\frac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)}\right)}{(P_S+P_C)^2} \tag{26}$$

$$\begin{aligned} Y=&\frac{\sigma_D^2\left[\frac{|g_D|^2|h|^2\rho}{\sigma_D^2}-\sum_{i=1}^{n}\left(\frac{\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\frac{|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right](P_S+P_C)}{\ln 2\left(\sigma_D^2+P_S\rho|g_D|^2|h|^2\right)\left(1+\sum_{i=1}^{n}\left(\frac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\frac{P_S|h_{Ei}|2}{\sigma_{SEi}^2}\right)\right)} \\ &-\log_2\left(\frac{\sigma_D^2+P_S\rho|g_D|^2|h|^2}{\sigma_D^2\left(1+\sum_{i=1}^{n}\left(\frac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\frac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)}\right) \end{aligned} \tag{27}$$

$$\begin{aligned} \frac{\partial Y}{\partial P_S}=&-\frac{-\sigma_D^2\left[\frac{|g_D|^2|h|^2\rho}{\sigma_D^2}-\sum_{i=1}^{n}\left(\frac{\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\frac{|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right](P_S+P_C)\left(\rho|g_D|^2|h|^2+\sigma_D^2\sum_{i=1}^{n}\left(\frac{\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\frac{|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)}{\ln 2\left(\sigma_D^2+P_S\rho|g_D|^2|h|^2\right)^2\left(1+\sum_{i=1}^{n}\left(\frac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\frac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)^2} \\ &\frac{+2\sum_{i=1}^{n}\left(\frac{P_S\rho^2|g_D|^2|g_{Ei}|^2|h|^4}{\sigma_{Ei}^2}+\frac{P_S\rho|g_D|^2|h|^2|h_{Ei}|^2}{\sigma_{SEi}^2}\right)}{\ln 2\left(\sigma_D^2+P_S\rho|g_D|^2|h|^2\right)^2\left(1+\sum_{i=1}^{n}\left(\frac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\frac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)^2}<0 \end{aligned} \tag{28}$$

$$\frac{\partial U}{\partial \rho}=\frac{\sigma_R^2\left[-\frac{P_S|h|^2}{\sigma_R^2}\left(1+\sum_{i=1}^{n}\left(\frac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\frac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)-\left(\sum_{i=1}^{n}\frac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}\right)\frac{P_S|h|^2(1-\rho)}{\sigma_R^2}\right]}{\ln 2\left(P_S+P_C\right)\left(\sigma_R^2+P_Sh^2(1-\rho)\right)\left(1+\sum_{i=1}^{n}\left(\frac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\frac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)}<0 \tag{29}$$

Algorithm 2 Relay Selection Algorithm

```
Initialize k, U_0 = 0, j
for i = 1 : k do
    solve the problem(34) in piecewise function
    obtain the SEE as U_i
    if U_i > U_0 then
        U_0 = U_i
        j = i
    end if
end for
return SEE = U_0 and j
```

Algorithm 2, where k of the algorithm stands for the number of relays, and $j-th$ relay is the optimal one.

VI. SIMULATION

In this section, numerical results are provided to evaluate performance of the proposed SEE optimization model in multiple eavesdroppers with SWIPT. Unless otherwise stated

TABLE 1. Table of simulation parameters.

	$\lvert h_E\rvert$	$\lvert g_E\rvert$	σ_E	σ_{SE}
E_1	0.2	0.2	0.2	0.3
E_2	0.3	0.3	0.2	0.4
E_3	0.3	0.3	0.3	0.5

we set system parameter as follows the circuit power consumption $P_C = 1.2$. we assume the channel coefficients of $|h| = 0.8$, and the noise of destination and relay is $\sigma_D = 0.2$, $\sigma_R = 0.2$ respectively. Owing to multiple eavesdroppers, there exists multiple values in each parameter and they are depicted as table 1. As for part of relay selection, we take a random number for g_E. In the first segment we take g_D for $g_D > g_E$, for the other segment, we assign h while $h > g_E$.

In Fig. 4 and Fig. 5, we discussed the relationship between the average SEE and power splitting coefficient when the source's power is changing. Obviously, the function is increasing monotonically when $0 < \rho < \rho^*$ while it is

$$\frac{\partial U}{\partial P_S}=\frac{\dfrac{\sigma_R^2\left[\dfrac{|h|^2}{\sigma_R^2}(1-\rho)-\sum\limits_{i=1}^{n}\left(\dfrac{\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\dfrac{|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right](P_S+P_C)}{\ln 2\left(\sigma_R^2+P_S|h|^2(1-\rho)\right)\left(1+\sum\limits_{i=1}^{n}\left(\dfrac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\dfrac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)}-\log_2\left(\dfrac{\sigma_R^2+P_S h^2(1-\rho)}{\sigma_R^2\left(1+\sum\limits_{i=1}^{n}\left(\dfrac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\dfrac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)}\right)}{(P_S+P_C)^2} \tag{30}$$

$$\begin{aligned}Y=&\frac{\sigma_R^2\left[\dfrac{|h|^2}{\sigma_R^2}(1-\rho)-\sum\limits_{i=1}^{n}\left(\dfrac{\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\dfrac{|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right](P_S+P_C)}{\ln 2\left(\sigma_R^2+P_S|h|^2(1-\rho)\right)\left(1+\sum\limits_{i=1}^{n}\left(\dfrac{P_S\rho g_{Ei}^2|h|^2}{\sigma_{Ei}^2}+\dfrac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)}\\&-\log_2\left(\frac{\sigma_R^2+P_S|h|^2(1-\rho)}{\sigma_R^2\left(1+\sum\limits_{i=1}^{n}\left(\dfrac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\dfrac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)}\right)\end{aligned} \tag{31}$$

$$\begin{aligned}\frac{\partial Y}{\partial P_S}=&-\frac{\sigma_R^2\left[\dfrac{|h|^2}{\sigma_R^2}(1-\rho)-\sum\limits_{i=1}^{n}\left(\dfrac{\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\dfrac{|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right](P_S+P_C)\left(|h|^2(1-\rho)+\sigma_R^2\sum\limits_{i=1}^{n}\left(\dfrac{P_S\rho|g_{Ei}|^2h^2}{\sigma_{Ei}^2}+\dfrac{P_Sn|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)}{\ln 2\left(\sigma_R^2+P_S|h|^2(1-\rho)\right)^2\left(1+\sum\limits_{i=1}^{n}\left(\dfrac{P_S\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\dfrac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)^2}\\&+\frac{2\sum\limits_{i=1}^{n}\left(\dfrac{P_S\rho|g_{Ei}|^2(1-\rho)|h|^4}{\sigma_{Ei}^2}+\dfrac{P_S|h|^2(1-\rho)|h_{Ei}|^2}{\sigma_{SEi}^2}\right)}{\ln 2\left(\sigma_R^2+P_S|h|^2(1-\rho)\right)^2\left(1+\sum\limits_{i=1}^{n}\left(\dfrac{P_Sn\rho|g_{Ei}|^2|h|^2}{\sigma_{Ei}^2}+\dfrac{P_S|h_{Ei}|^2}{\sigma_{SEi}^2}\right)\right)^2}<0\end{aligned} \tag{32}$$

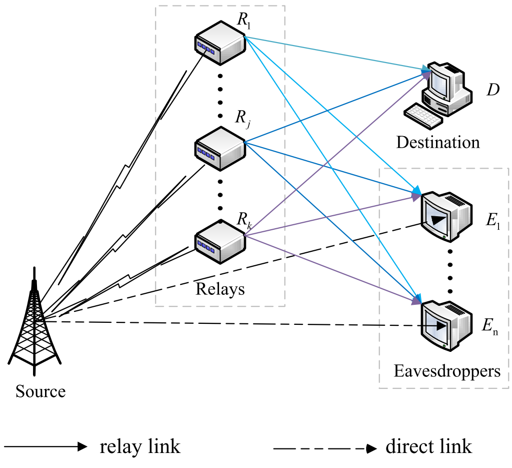


FIGURE 3. System model for multiple relays with relay selection.

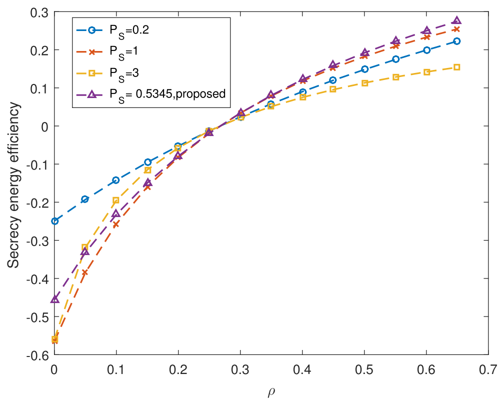


FIGURE 4. The changing trend of the SEE with the change of P_S in different ρ while $0 < \rho < \rho^*$.

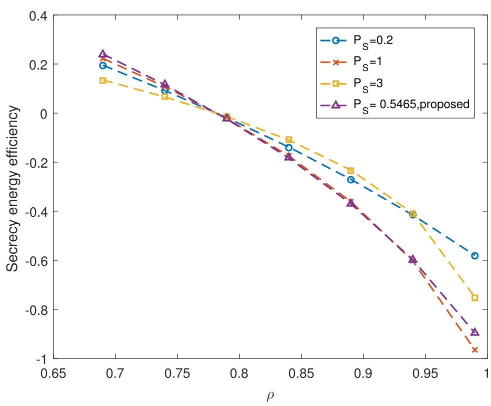


FIGURE 5. The changing trend of the SEE with the change of P_S in different ρ while $\rho^* < \rho < 1$.

decreasing monotonically, so we can get the maximum value when $\rho = 0.69$, which is the optimal point of the function.

Fig. 6 and Fig. 7 show the relationship between the average SEE and source's power when we give different power splitting coefficients. The SEE function is convex within the scope of the definition domain. We can obtain the optimal $P_S = 0.5435$ when U is the optimal by comparing two cases.

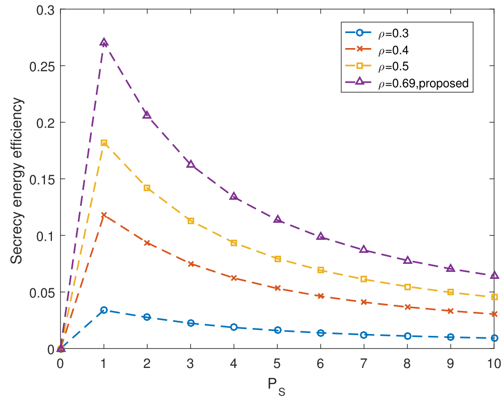


FIGURE 6. The changing trend of the SEE with the change of ρ in different P_S when $0 < \rho < \rho^*$.

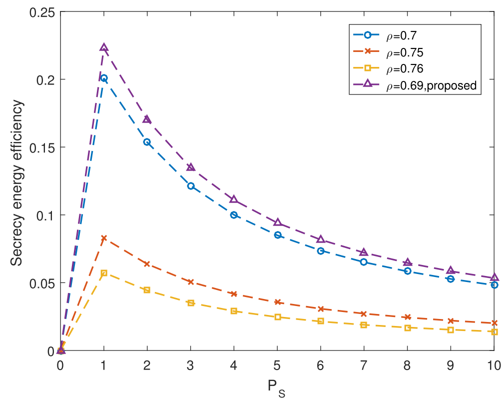


FIGURE 7. The changing trend of the SEE with the change of ρ in different P_S when $\rho^* < \rho < 1$.

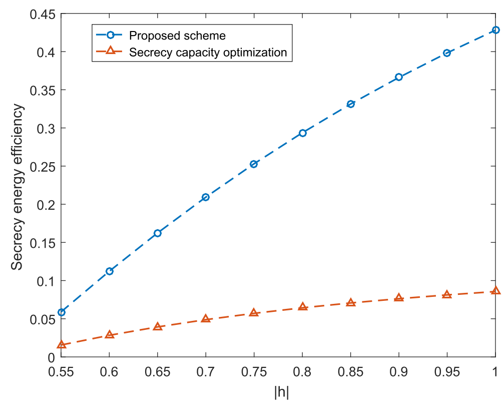


FIGURE 8. The contrast between secrecy capacity and secrecy energy efficiency when $0 < \rho < \rho^*$.

As shown in Fig. 8 and Fig. 9, under the above optimal parameter values, we compare the performance of SEE and SE algorithm with the change of channel parameters. Obviously, SEE is more efficient.

Fig. 10 and Fig. 11 show the impact of the number of relays on SEE of the optimal relaying selection schemes. It can be seen that the average SEE efficiency is improved significantly when the number of relays are increasing, which confirms the fact that the potential relay nodes could provide

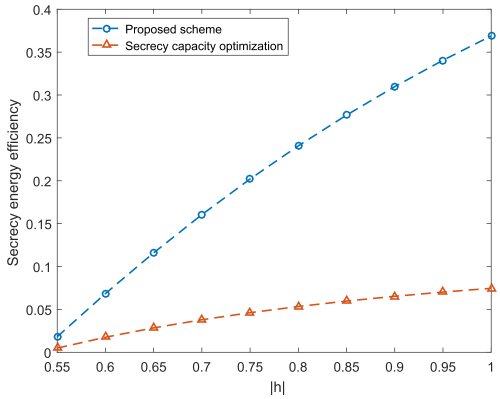


FIGURE 9. The contrast between secrecy capacity and secrecy energy efficiency when $\rho^* < \rho < 1$.

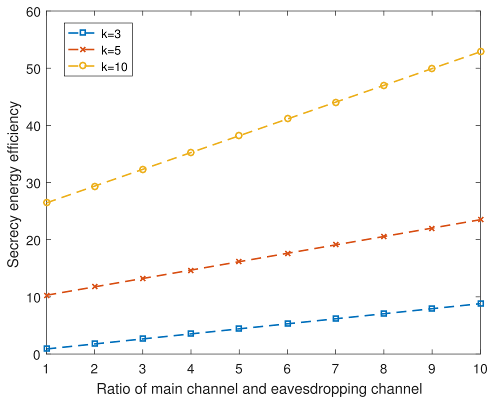


FIGURE 10. The relationship between the optimal SEE and the numbers of the relays when $0 < \rho < \rho^*$.

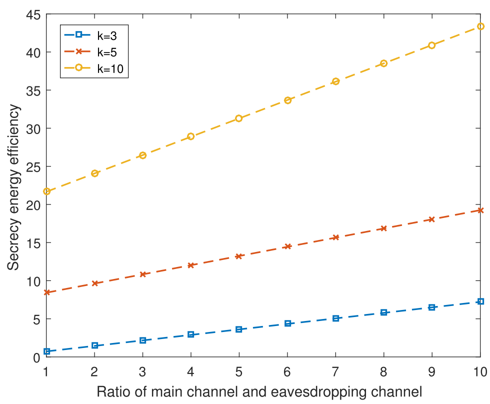


FIGURE 11. The relationship between the optimal SEE and the numbers of the relays when $\rho^* < \rho < 1$.

diversity SEE gains. The diversity gains increases as the number of relays grows.

VII. CONCLUSION

In this paper, we have investigated the SEE of a DF relaying system with SWIPT, where multiple eavesdroppers have been considered. We analyze the optimal transmit power and power splitting coefficient of the system. Since the maximum energy efficiency problem is a non-linear function with respect to each variable when one of which is considered as a constant, we solve it by taking the alternative optimization. To further improve the SEE performance, we introduce multiple relays proposed relay selection scheme for SEE maximization. The simulation results show that our model and solving process are effective and verify the secrecy performance superiority of the proposed scheme over the equal power allocation scheme and secrecy rate maximization method.

REFERENCES

[1] Z. Chang, Z. Wang, X. Guo, C. Yang, Z. Han, and T. Ristaniemi, "Distributed resource allocation for energy efficiency in OFDMA multicell networks with wireless power transfer," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 2, pp. 345–356, Feb. 2019.

[2] Z. Chang, L. Lei, H. Zhang, T. Ristaniemi, S. Chatzinotas, B. Ottersten, and Z. Han, "Energy-efficient and secure resource allocation for multiple-antenna NOMA with wireless power transfer," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 4, pp. 1059–1071, Dec. 2018.

[3] X. Yu, X. Dang, B. Wen, S.-H. Leung, and F. Xu, "Energy-efficient power allocation for millimeter-wave system with non-orthogonal multiple access and beamforming," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 7877–7889, Aug. 2019.

[4] J. Wu, J. Liu, W. Li, and X. You, "Low-complexity power allocation for energy efficiency maximization in DAS," *IEEE Commun. Lett.*, vol. 19, no. 6, pp. 925–928, Jun. 2015.

[5] H. Kim, S.-R. Lee, C. Song, K.-J. Lee, and I. Lee, "Optimal power allocation scheme for energy efficiency maximization in distributed antenna systems," *IEEE Trans. Commun.*, vol. 63, no. 2, pp. 431–440, Feb. 2015.

[6] Y. Sun, F. Yang, and L. Cheng, "An overview of OFDM-based visible light communication systems from the perspective of energy efficiency versus spectral efficiency," *IEEE Access*, vol. 6, pp. 60824–60833, 2018.

[7] B. Ji, Y. Li, B. Zhou, C. Li, K. Song, and H. Wen, "Performance analysis of UAV relay assisted IoT communication network enhanced with energy harvesting," *IEEE Access*, vol. 7, pp. 38738–38747, 2019.

[8] T. M. Hoang, V. V. Son, N. C. Dinh, and P. T. Hiep, "Optimizing duration of energy harvesting for downlink NOMA full-duplex over Nakagami-M fading channel," *AEU-Int. J. Electron. Commun.*, vol. 95, pp. 199–206, Oct. 2018.

[9] M. Zhao, J. Zhao, W. Zhou, J. Zhu, and S. Zhang, "Energy efficiency optimization in relay-assisted networks with energy harvesting relay constraints," *China Commun.*, vol. 12, no. 2, pp. 84–94, Feb. 2015.

[10] H. Dai, Y. Huang, Y. Xu, C. Li, B. Wang, and L. Yang, "Energy-efficient resource allocation for energy harvesting-based device-to-device communication," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 509–524, Jan. 2019.

[11] W. Zhou, X. Li, J. Xia, W. Jiao, and M. Hua, "Optimal pilot design for MIMO broadcasting systems based on the positive definite matrix manifold," *IEEE Access*, vol. 7, pp. 99589–99601, 2019.

[12] W. Zhou, X. Li, H. Wu, Y. Xu, Q. Zhou, and Y. Rao, "Predictive precoding based on the Grassmannian manifold for UAV-enabled cache-assisted B5G communication systems," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, pp. 1–18, Dec. 2020.

[13] K. Song and C. Li, "Blockchain-enabled relay-aided wireless networks for sustainable e-agriculture," *J. Cleaner Prod.*, vol. 281, Jan. 2021, Art. no. 124496.

[14] C. Li, P. Liu, C. Zou, F. Sun, J. M. Cioffi, and L. Yang, "Spectral-efficient cellular communications with coexistent one- and two-hop transmissions," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6765–6772, Aug. 2016.

[15] Z. Chang, X. Hou, X. Guo, T. Ristaniemi, and Z. Han, "Secure and energy-efficient resource allocation for wireless power enabled full-/half-duplex multiple-antenna relay systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11208–11219, Dec. 2017.

[16] X. Yu, Y. Hu, Q. Pan, X. Dang, N. Li, and M. H. Shan, "Secrecy performance analysis of artificial-noise-aided spatial modulation in the presence of imperfect CSI," *IEEE Access*, vol. 6, pp. 41060–41067, 2018.

[17] C. Li, H. J. Yang, F. Sun, J. M. Cioffi, and L. Yang, "Multiuser overhearing for cooperative two-way multiantenna relays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3796–3802, May 2016.

[18] C. Li, S. Zhang, P. Liu, F. Sun, J. M. Cioffi, and L. Yang, "Overhearing protocol design exploiting intercell interference in cooperative green networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 441–446, Jan. 2016.

[19] H. Zhang, P. Sun, C. Li, Y. Huang, and L. Yang, "Cooperative precoding for wireless energy transfer and secure cognitive radio coexistence systems," *IEEE Signal Process. Lett.*, vol. 24, no. 5, pp. 540–544, May 2017.

[20] R. Zhao, H. Lin, Y.-C. He, D.-H. Chen, Y. Huang, and L. Yang, "Secrecy performance of transmit antenna selection for MIMO relay systems with outdated CSI," *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 546–559, Feb. 2018.

[21] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[22] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in AF multi-antenna relaying networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025–3038, Jul. 2016.

[23] H. Chen, W. Zhu, L. Zeng, and X. Cai, "Secrecy capacity based on suboptimal multi-antennas selection and power allocation," in *Proc. IEEE Inf. Technol., Netw., Electron. Autom. Control Conf.*, May 2016, pp. 83–86.

[24] P. L. Yeoh, N. Yang, and K. J. Kim, "Secrecy outage probability of selective relaying wiretap channels with collaborative eavesdropping," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.

[25] A. Zappone, P.-H. Lin, and E. A. Jorswieck, "Secrecy energy efficiency for MIMO single- and multi-cell downlink transmission with confidential messages," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 2059–2073, Aug. 2019.

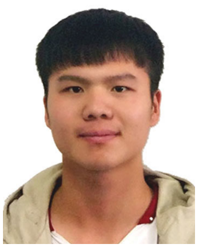
[26] X. Hu, B. Li, K. Huang, Z. Fei, and K.-K. Wong, "Secrecy energy efficiency in wireless powered heterogeneous networks: A distributed ADMM approach," *IEEE Access*, vol. 6, pp. 20609–20624, 2018.

[27] Z. Zhou, M. Peng, Z. Zhao, W. Wang, and R. S. Blum, "Wireless-powered cooperative communications: Power-splitting relaying with energy accumulation," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 969–982, Apr. 2016.

[28] Z. Ji, M. Nie, L. Meng, Q. Wang, C. Li, and K. Song, "On secrecy energy efficiency of RF energy harvesting system," in *Proc. IEEE Int. Workshop Signal Process. Syst. (SiPS)*, Oct. 2019, pp. 278–283.

[29] K. Song, Q. Wang, L. Peng, C. Li, and X. Wu, "Secrecy energy efficiency optimization for DF relaying IoT systems with passive eavesdropping terminal," *Phys. Commun.*, vol. 44, Feb. 2021, Art. no. 101254.

KANG SONG (Member, IEEE) received the B.S. degree from Anhui University, China, in 2009, and the Ph.D. degree in information and communication engineering from Southeast University, China, in 2016. Since August 2016, he has been a Faculty with the School of Electronic and Information Engineering, Qingdao University. His current research interests include cooperative communications and heterogeneous networks.



MENGYUN NIE is currently pursuing the B.S. degree with Qingdao University. His current research interests include the Internet of Things (IoTs) networks and signal processing.

JING JIANG (Member, IEEE) received the M.Sc. degree from Xidian University, in 2005, and the Ph.D. degree in information and communication engineering from Northwestern Polytechnical University, China, in 2009. She was the Leader of the 3GPP LTE MIMO Project, ZTE Corporation, China, from 2006 to 2013. She is currently a Professor with the Shaanxi Key Laboratory of Information Communication Network and Security, Xi'an University of Posts and Telecommunications, Xi'an, China. Her research interests include massive multiple-input multiple-output systems and millimeter-wave communications. She has been a member of the 3GPP.

CHUNGUO LI (Senior Member, IEEE) received the bachelor's degree in wireless communications from Shandong University, in 2005, and the Ph.D. degree in wireless communications from Southeast University, in 2010.

In July 2010, he joined the Faculty of Southeast University, Nanjing, China, where he is currently an Advisor of Ph.D. candidates and a Full Professor. From June 2012 to June 2013, he was the Postdoctoral Researcher with Concordia University, Montreal, Canada. From July 2013 to August 2014, he was with the DSL Laboratory, Stanford University, as a Visiting Associate Professor. From August 2017 to July 2019, he was an Adjunct Professor with Xizang Minzu University under the supporting Tibet Program organized by the China National Human Resources Ministry. His research interests include wireless communications and cyberspace security and machine learning-based image/video signal processing. He is a Fellow of IET and the Chair of the IEEE CIS Nanjing Chapter.

YONGFENG YIN (Member, IEEE) received the M.S. and Ph.D. degrees from the School of Reliability and Systems Engineering, Beihang University, Beijing, China, in 2003 and 2010, respectively. He was a Visiting Scholar with Colorado State University, USA, from 2015 to 2016. He is currently an Associate Professor with the School of Reliability and Systems Engineering, Beihang University. His research interests include software engineering, software testing and verification techniques, and software reliability engineering. He is also a member of ACM and CCF.