IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 19, 2020, accepted June 5, 2020, date of publication June 15, 2020, date of current version June 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3002382

Secrecy Performance Analysis and Optimization of Intelligent Reflecting Surface-Aided Indoor Wireless Communications

VAN PHU TUAN AND IC PYO HONG, (Member, IEEE)
Department of Information and Communication Engineering, Kongju National University, Cheonan 31080, South Korea
Corresponding author: Ic Pyo Hong (iphong@kongju.ac.kr)

This work was supported in part by the Basic Science Research Program under Grant 2018R1A2B6001680, and in part by the Priority Research Centers Program through the National Research Foundation of Korea under Grant 2019R1A6A1A03032988.

ABSTRACT This paper studies the secrecy performance of an intelligent reflecting surface (IRS)-aided indoor wireless communication where the IRS is capable of adjusting the direction and phase shift of reflected signal on its surface and assists a source to communicate with an authenticated user in the presence of several unauthenticated users, which can be potential eavesdroppers. The goal of this paper is to design a tile-allocation-and-phase-shift-adjustment (TAaPSA) strategy for the IRS to optimize the average secrecy rate (ASR); moreover, the respective secrecy outage probability (SOP) for this TAaPSA is evaluated. To achieve this goal, the ray model and the Rice distribution are adopted to describe the propagation of the IRS's reflected signals and the fading process, respectively. Closed-form analytical expressions for the ASR and the SOP are derived. Using these analytical results, a genetic algorithm (GA) is utilized to find an optimal TAaPSA strategy for the IRS. The accuracy of the analytical results and the improvement in ASR using GA-based TAaPSA strategy are verified by simulation results.

INDEX TERMS Physical layer security, intelligent reflecting surface, average secrecy rate, secrecy outage probability, genetic algorithm.

I. INTRODUCTION

The broadcast nature of wireless signals makes it easy to be attacked by eavesdroppers; especially with the fast-growing number of wireless devices, security in wireless communication has become a critical issue. Over the past decade, the physical layer security (PLS) approach which defines the perfect secrecy rate as the difference in capacities between legitimate and illegitimate users [1] has commonly adopted to evaluate the secrecy performance in recent studies. To enlarge the perfect secrecy rate, current techniques focus on improving the quality of authenticated links and/or to degrade potential wiretap links. In particular, the works of [2] and [3] employed jamming signal to prevent untrusted nodes of overhearing the confidential information. The work of [4] combined both the jamming signal and a relay-selection method to rise the security advantage from both user's and eavesdropper's sides where a relay that assists the communication at the highest perfect secrecy rate was selected to forward the confidential information. The works of [5] and [6] applied the maximal ratio combining (MRT) technique at multiple-antenna systems to exploit the spatial diversity at desired users, thus achieving a higher security capacity. In [7], the effectiveness of different diversity combining techniques, e.g., maximal ratio transmission (MRC) and selection combining (SC), on enhancing the secure communication for multiple-antenna relaying systems was investigated. Generally, the conventional approaches in PLS assumed that the wireless environment is uncontrollable and the enhancement in secrecy performance is achieved using more complex device's hardware and protocols.

To further improve the performance of wireless network, intelligent reflecting surfaces (IRSs) which open a concept of the programmable wireless environment have gained much intention from the research community. The IRS consists of a large number of low-cost reflecting tiles (RTs), each is made up of two main components, a meta-atom array which is periodically-repeated conductive structures with engineered electromagnetic (EM) properties and tunable switches which can change the structures of the meta-atom array [8].

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

By programming the states of these tunable switches, the IRS can adjust the EM behavior on its surface tailored to the demand of wireless network. The IRS shows its remarkable ability of mitigating the effect of the multi-path fading, which is an inherent attribute of conventional wireless systems, hence archiving a significant improvement in received power and latency [9], [10]. Furthermore, the IRS can realize some signal-processing techniques at the EM level which requires simpler manipulations and less complex hardware than the digital domain, such as, IRS-based modulation, IRS-based encoding, and multi-stream transmission [11]. The IRS is also considered as a potential technique to boost the performance of various wireless network. For example, the IRS can be employed in a wireless power transfer (WPT) network to focus the ambient redundant EM energy to harvesters [12] instead of absorbing it for co-interference elimination. In cooperative networks, the IRS can act as a relay to forward information without transmit RF chains and additional thermal noise added during reflections [13]. Moreover, it is possible to use the IRSs as large scale antennas to enable virtual massive multiple-input-multiple-output (MIMO) communications [14]. These impressive capabilities make the IRS become a promising technology to enhance performance as well as to achieve the high spectrum and energy efficiency for future networks.

Since the IRS has the ability to control the wireless environment, it has become an extremely effective supplement for the PLS technology. Recently, there are some works investigating the secure capability of IRS-aided wireless systems. The work of [15] studied the problem of secure communication via an IRS where the beamformer of a multi-antenna transmitter and phase shift coefficient of the IRS were jointly optimized using alternating optimization (AO) algorithms for the purpose of maximizing the secrecy rate of a single-antenna network including a legitimate receiver and an eavesdropper. The results of [15] pointed out that enlarging the size of the IRS is more efficient than increasing the number of transmit antennas in enhancing secrecy rate and energy efficiency. The extension of [15] to the case of existing the direct links between the transmitter and the receivers was studied in [16]. The work of [17] considered a similar model of [15] but for the MIMO scenario where transceivers are multi-antenna devices. To maximize the secrecy rate, an approximated AO algorithm consisting a numerical algorithm and a minorization-maximization algorithm was designed to jointly optimize the transmit covariance of the transmit signal block and the phase shifts of the IRS. This proposed algorithm was compared with and showed superiority in achieving a higher secrecy rate over other benchmark schemes, i.e., zero phase shift and random phase shift. The work of [18] investigated a more general IRS-assisted secure communication model where a multi-antenna transmitter with the help of an IRS severed the communication of a single-antenna network consisting of multiple legitimate receivers and eavesdroppers. Moreover, this work proposed two AO algorithms for solving the secrecy rate maximization problem of both continuous- and discrete-reflecting coefficients, respectively. The works of [19] studied the advantage of using jamming signals to boost the secrecy performance of an IRS-aided secure communication in the presence of multiple eavesdroppers. The superior results obtained with the help of the jamming signals indicated the effectiveness of the jamming signals when dealing with a multiple-eavesdropper scenario. The work of [20] examined indoor communication and proposed using the IRSs coated on walls to set up private secure physical links between a transmitter and legitimate users or jamming links to eavesdroppers, hence, efficiently preventing the eavesdroppers from receiving the wireless signal or degrading the received power at the eavesdroppers. To optimize the operation of the IRSs, such as steering and absorbing parameters, a genetic algorithm (GA) was utilized.

In this paper, we study the secrecy performance of an IRS-aided indoor wireless communication via two important secrecy metrics, i.e., secrecy outage probability (SOP) and average secrecy rate (ASR). This system consists of a source, an authenticated user and several unauthenticated users that can be potential eavesdroppers (PEs); in addition, wireless channels between them include both line-of-sight (LoS) and non-LOS links. The IRS is attached to a wall and assists the secure communication between the source and the authenticated user. Specifically, the IRS provides reflected links that are utilized for enhancing or degrading the channel quality of each receiver by altering the reflecting coefficient of each RT. This process is managed by a programmable controller. The contributions of this paper are summarized as follows.

- We propose a tile-allocation-and-phase-shift-adjustment (TAaPSA) strategy for the IRS which aims to boost the average secrecy performance of an IRS-aided indoor wireless communication system. By evaluating the average secrecy performance, our proposed TAaPSA significantly reduces computation for the IRS's configuration caused by channel variation thus reducing the energy consumption at the IRS.
- We use the ray model to describe the signal propagation on the IRS, then the channel between the source and each receiver is modeled as a combination of LoS link, reflected links and NLoS link, hence, its amplitude obeys the Rice distribution. We use the multinomial theorem to formulate the cumulative distribution function (CDF) of the strongest overhearing channel gain; then, we derive the closed-form analytical expressions for the SOP and the ASR.
- Using the analytical results, we find the optimal solution for the IRS's TAaPSA strategy, which indicates the reasonable number of RTs serving for each receiver in constraint of the total RTs and the best phase shift for each RT. This optimal strategy involves manipulating the complex mathematical equations over a large variable space, a mixed discrete-continuous domain, and non-independent relationships of variables; hence, a GA is applied to efficiently solve this problem. Moreover, we extend our investigation to practical IRS cases,

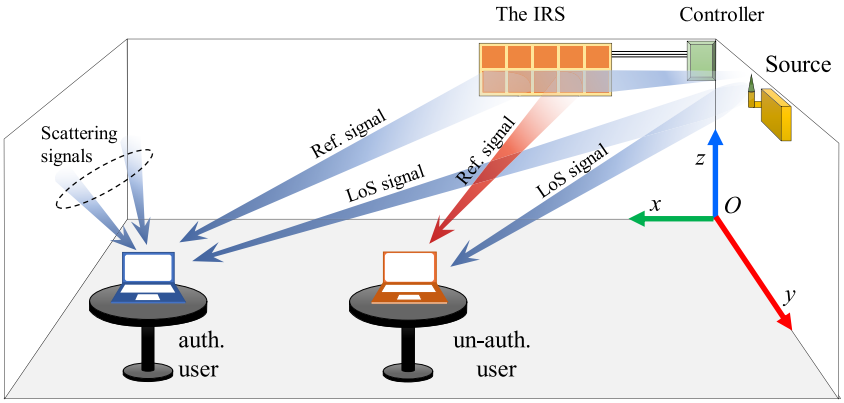


FIGURE 1. The system model.

i.e., discrete-phase-shift (DPS) and phase-dependent-amplitude-variation, to evaluate the secrecy performance loss.

- The accuracy of analytical results and the effectiveness of GA are verified by simulation results. These results provide insights into the system designs. Specifically, the phase shifts of RTs assisting the authenticated user's communication tend to enhance the channel quality while that of remaining RTs tend to degrade the PE's channel quality. When the number of the PEs is sufficiently large as compared to the number of RTs, the IRS prioritizes enhancing the authenticated user's channel quality; in contrast, it uses several RTs to degrade the PE's channel quality and uses the rest RTs supports the authenticated user's communication.

The rest of this paper is organized as follows. The system model and channel model are described in Section II. The analytical results for the SOP and ASR, and the GA-based TAaPSA strategy are presented in Section III. Simulation results and discussions are presented in Section IV. Finally, the conclusion is presented in Section V. Appendices A, V and V present the proofs of the Propositions.

Notation: $Ei(\cdot)$ is the exponential integral function [21, Eq (8.211.1)]; $\gamma(\alpha, x)$ and $\Gamma(\alpha, x)$ are the lower and upper incomplete gamma functions [21, Eq (8.350.1) and (8.350.2)], respectively; $|\cdot|$ is the modulus of a complex number; $\mathcal{CN}(0, \sigma_0^2)$ is a complex Gaussian distribution with zero mean and variance σ_0^2; $I_0(\cdot)$ is s the 0-*th* order modified Bessel function of the first kind [21, Eq (8.431.1)]; $\mathbb{E}\{X\}$ is the expectation of a random variable (RV) X; and $[X]^+ = \max\{X, 0\}$.

II. SYSTEM MODEL AND CHANNEL MODEL

We study the secure communication of an indoor communication system as illustrated in Fig. 1 where a transmitter S wants to send information to an authenticated user U in the presence of M unauthenticated users (we use E to denote the unauthenticated network) that can be PEs. An IRS including L RTs $R_l, l = 1, \ldots, L$, is employed to assist the secure communication of U. We use the ray model to describe the signal propagation on the IRS [10], [20], and assume that the IRS can adjust both direction and phase shift of the reflected wave. Let consider the communication between S and an user D. D can be U or one of PEs, $E_m, m = 1, \ldots, M$. The IRS uses a set of N RTs $\mathcal{N}_\mathrm{D} = \{\hat{R}_1, \ldots, \hat{R}_N\}, N \leqslant L$, to reflect the signal of S to D. When S broadcasts a signal $x(t)$ with power $\mathbb{E}\{|x(t)|^2\} = P_\mathrm{S}$, the received signal at D consists of the signals that propagate through the LoS link denoted by $h_\mathrm{SD}^\mathrm{LoS}$, fading channel denote by $h_\mathrm{D}^\mathrm{Fad}$ and reflecting links[1] of $\mathcal{N}_\mathrm{D}$ denoted by $h_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}^\mathrm{Ref}$. Using the free-space path loss (FSPL) model, $h_\mathrm{SD}^\mathrm{LoS}$ and $h_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}^\mathrm{Ref}$ are respectively expressed as

$$h_\mathrm{SD}^\mathrm{LoS} = \frac{\lambda_0}{4\pi d_\mathrm{SD}} e^{-j\varphi_\mathrm{SD}^\mathrm{pd}}, \tag{1}$$

$$h_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}^\mathrm{Ref} = \frac{\lambda_0}{4\pi d_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}} \phi_{\hat{\mathrm{R}}_n} e^{-j\varphi_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}^\mathrm{pd}}, \tag{2}$$

where $d_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}} = d_{\mathrm{S}\hat{\mathrm{R}}_n} + d_{\hat{\mathrm{R}}_n\mathrm{D}}$ is the propagation distance of $h_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}^\mathrm{Ref}$; $d_\mathrm{SD}, d_{\mathrm{S}\hat{\mathrm{R}}_n}$ and $d_{\hat{\mathrm{R}}_n\mathrm{S}}$ are the distances of $S \to D$, $S \to \hat{R}_n$ and $\hat{R}_n \to D$ links, respectively; $\varphi_\mathrm{SD}^\mathrm{pd} = \frac{2\pi f_0 d_\mathrm{SD}}{c}$ and $\varphi_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}^\mathrm{pd} = \frac{2\pi f_0 d_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}}{c}$ are the phase shifts caused by propagation distances d_SD and $d_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}$, respectively; f_0 is the center frequency of the transmitted signal; $\lambda_0 = \frac{c}{f_0}$ is the wavelength; c is the speed of light; $\phi_{\hat{\mathrm{R}}_n} = \alpha_{\hat{\mathrm{R}}_n} e^{j\varphi_{\hat{\mathrm{R}}_n}}$ is the reflecting coefficient of $\hat{R}_n$ with the reflection amplitude $\alpha_{\hat{\mathrm{R}}_n} \leqslant 1$ and phase shift $\varphi_{\hat{\mathrm{R}}_n}$. Let $\varphi_{\hat{\mathrm{R}}_n}^\mathrm{sc} = \varphi_{\hat{\mathrm{R}}_n} + \varphi_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}^\mathrm{pd} - \varphi_\mathrm{SD}^\mathrm{pd}$ denote the signal-combining phase shift (SCPS) which represents the difference in phase between the reflected signal from $\hat{R}_n$ and the LoS signal. The use of $\varphi_{\hat{\mathrm{R}}_n}^\mathrm{sc}$ makes analytical and simulation results become simpler. Additionally, the fading channel is modeled as $h_\mathrm{SD}^\mathrm{Fad} \sim \mathcal{CN}\left(0, 2\sigma_\mathrm{Fad}^2\right)$. The total effect

[1] We consider the reflected signal of R_l as the first signal traveling on the $S \to R_l \to D$ path [24]. The influence of the multiple-reflection signals reflected by the IRS and walls, which causes differences in attenuation, delay and phase shift at the receivers, can be counted in the fading channel.

of the channel between S and D is expressed as

$$h_{\mathrm{SD}} = \underbrace{h_{\mathrm{SD}}^{\mathrm{Fad}}}_{\text{scattered component}} + \underbrace{h_{\mathrm{SD}}^{\mathrm{LoS}} + \sum_{\hat{\mathrm{R}}_n \in \mathcal{N}_D} h_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}^{\mathrm{Ref}}}_{\text{dominant components}}. \quad (3)$$

From (1) and (2), it is seen that the dominant components in (3) is a deterministic process; hence, h_{SD} is a Rice distributed random variable $h_{\mathrm{SD}} \sim \mathcal{R}(\Omega_{\mathrm{SD}}, K_{\mathrm{SD}})$ with a scale parameter Ω_{SD} and a shape parameter K_{SD} [22]. To determine the values of Ω_{SD} and K_{SD}, we need to calculate the strength of the dominant components $\omega^2_{\mathrm{SD,dom}}$ in (3). Using (1) and (2), $\omega^2_{\mathrm{SD,dom}}$ is calculated as

$$\omega^2_{\mathrm{SD,dom}} = \left(\frac{\lambda_0}{4\pi}\right)^2 \left(\left(\frac{1}{d_{\mathrm{SD}}} + \mu_{\mathrm{proj}}\right)^2 + \left(\mu_{\mathrm{rej}}\right)^2\right), \quad (4)$$

where $\mu_{\mathrm{proj}} = \sum_{n\in\mathcal{N}_{\mathrm{D}}} \frac{\alpha_{\hat{\mathrm{R}}_n} \cos\left(\varphi^{\mathrm{sc}}_{\hat{\mathrm{R}}_n}\right)}{d^{\mathrm{Ref}}_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}}$ and $\mu_{\mathrm{rej}} \sum_{n\in\mathcal{N}_{\mathcal{D}}} \frac{\alpha_{\hat{R}_n} \sin\left(\varphi^{\mathrm{sc}}_{\hat{R}_n}\right)}{d^{\mathrm{Ref}}_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}}$ are obtained by considering the vector projection and vector rejection of each reflected signal vector onto and from the LoS signal vector, respectively. Then Ω_{SD} and K_{SD} are calculated as follows [23].

$$\Omega_{\mathrm{SD}} = \omega^2_{\mathrm{SD,dom}} + 2\sigma^2_{\mathrm{Fad}}, \quad (5)$$

$$K_{\mathrm{SD}} = \frac{\omega^2_{\mathrm{SD,dom}}}{2\sigma^2_{\mathrm{Fad}}}, \quad (6)$$

The equation (4) shows that Ω_{SD} can be adjusted by altering the reflecting coefficients of the RTs and the signal strength at D is maximized when the SCPS of $\hat{R}_n$ is set to $\varphi^{\mathrm{sc}}_{\hat{\mathrm{R}}_n} = 0$, thus the real phase shift of $\hat{R}_n$ is $\varphi_{\hat{\mathrm{R}}_n} = \varphi^{\mathrm{pd}}_{\mathrm{SD}} - \varphi^{\mathrm{pd}}_{\mathrm{S}\hat{\mathrm{R}}_n\mathrm{D}}$. On the other hand, the signal strength at D is minimized when the sum vector of all reflected signal vectors at D becomes the opposite vector of the LoS signal vector. For our considered system, it is impossible to simultaneously achieve both goals of maximizing the signal strength at U and minimizing the signal strengths at PEs. In the next sections, we study the SOP and ASR of the considered system. Then, a GA-based TAaPSA strategy is designed to optimize the number of RTs allocated to each receiver and the phase shift of each RT.

III. SECRECY PERFORMANCE ANALYSIS

A. SIGNAL TRANSMISSION AND DISTRIBUTION FUNCTIONS

In this section, we investigate the secrecy performance of the considered system via two important secrecy metrics, i.e., the SOP and ASR, using the channel model presented in Section II. According to [23], the probability density function (PDF) of $|h_{\mathrm{SD}}|^2$ and its series representation (using the relationship in [21, Eq (8.445)]) are respectively given by

$$f_{|h_{\mathrm{SD}}|^2}(x) = \mu_{\mathrm{SD}} e^{-K_{\mathrm{SD}}} e^{-\mu_{\mathrm{SD}}x} I_0\left(2\sqrt{K_{\mathrm{SD}}\mu_{\mathrm{SD}}x}\right), \quad (7)$$

$$= \mu_{\mathrm{SD}} e^{-K_{\mathrm{SD}}} e^{-\mu_{\mathrm{SD}}x} \sum_{k=0}^{\infty} \frac{(K_{\mathrm{SD}}\mu_{\mathrm{SD}})^k}{(k!)^2} x^k, \quad (8)$$

Since we consider a multiple-PE scenario, the instantaneous secrecy rate for each communication time slot depends on the instantaneous achievable rates of U and the best PE. In addition, the signals undergo Rice channels. This leads the complexity of the calculations of the SOP and the ASC. To simplify the calculation steps for the SOP and the ASC, the CDF of $|h_{\mathrm{SD}}|^2$ is presented in two different forms, i.e., $F^{(\mathrm{a})}_{|h_{\mathrm{SD}}|^2}(x)$ and $F^{(\mathrm{b})}_{|h_{\mathrm{SD}}|^2}(x)$, and each formula is appropriately used to derive a necessary mathematical expression.

Proposition 1: The CDF of a RV $|h_{\mathrm{SD}}|^2$ can be expressed as one of the follows

$$F^{(\mathrm{a})}_{|h_{\mathrm{SD}}|^2}(x) = e^{-(K_{\mathrm{SD}}+\mu_{\mathrm{SD}}x)} \sum_{p_n=1}^{\infty} \mathcal{A}^{\mathrm{SD}}_{p_n} x^{p_n}, \quad (9)$$

$$F^{(\mathrm{b})}_{|h_{\mathrm{SD}}|^2}(x) = 1 - e^{-(K_{\mathrm{SD}}+\mu_{\mathrm{SD}}x)} \sum_{p_n=1}^{\infty} \mathcal{B}^{\mathrm{SD}}_{p_n} x^{p_n}, \quad (10)$$

where $\mathcal{A}^{\mathrm{SD}}_{p_n}$ and $\mathcal{B}^{\mathrm{SD}}_{p_n}$ are given by

$$\mathcal{A}^{\mathrm{SD}}_{p_n} = \frac{\mu^{p_n}_{\mathrm{SD}}}{p_n!} \sum_{p_w=0}^{p_n-1} \frac{K^{p_w}_{\mathrm{SD}}}{p_w!}, \quad (11)$$

$$\mathcal{B}^{\mathrm{SD}}_{p_n} = \frac{\mu^{p_n}_{\mathrm{SD}}}{p_n!} \left(e^{K_{\mathrm{SD}}} - \sum_{p_w=0}^{p_n-1} \frac{K^{p_w}_{\mathrm{SD}}}{p_w!}\right). \quad (12)$$

Proof: See Appendix A. □

Next, we study the instantaneous secrecy rate of the considered system. Since S broadcasts $x(t)$, the received signal at D is $y_{\mathrm{D}}(t) = h_{\mathrm{SD}}x(t) + n_D(t)$ where $n_D(t) \sim \mathcal{CN}(0, N_0)$ is the additive white Gaussian noise (AWGN) at the antenna of D; hence the instantaneous achievable rate (AR) of D is expressed as

$$C_{\mathrm{D}} = \log_2\left(1 + \gamma_0 |h_{\mathrm{SD}}|^2\right), \quad (13)$$

where $\gamma_0 = \frac{P_S}{N_0}$.

In the presence of the multiple PEs, the instantaneous overhearing rate (OR) of E, C_{E}, is determined as the highest value among M instantaneous ORs measured at E_m, $m = 1, \ldots, M$. Therefore, C_{E} is calculated as

$$C_{\mathrm{E}} = \max_{1\le m\le M} \left\{C_{\mathrm{E}_m}\right\} = \log_2\left(1 + \gamma_0 \max_{1\le m\le M} \left\{|h_{\mathrm{SE}_m}|^2\right\}\right), \quad (14)$$

where h_{SE_m} is the channel coefficient between S and E_m.

To calculate C_{E}, the CDF of the largest order statistic of M independent non-identically distributed (i.n.i.d) RVs in (14) need to be studied. Similarly, we present it in two different forms as in Proposition 2.

Proposition 2: Let $Y \triangleq \max_{1\le m\le M} \left\{|h_{\mathrm{SE}_m}|^2\right\}$ be the largest order statistic of M i.n.i.d RVs $|h_{\mathrm{SE}_m}|^2$, $m = 1, \ldots, M$, the CDF of Y can be expressed as one of the follows

$$F^{(\mathrm{a})}_Y(x) = e^{-(K_{\mathrm{SE}}+\mu_{\mathrm{SE}}x)} \sum_{p_n=0}^{\infty} \mathcal{C}_{p_n} x^{p_n}, \quad (15)$$

$$F_Y^{(\mathrm{b})}(x) = 1 + \sum_{\mathcal{L}_1}^{\mathcal{L}_{(2^M-1)}} (-1)^{\hat{M}} e^{-(\hat{K}_{\mathrm{SE}} + \hat{\mu}_{\mathrm{SE}} x)} \sum_{p_n=0}^{\infty} \mathcal{D}_{p_n} x^{p_n}, \quad (16)$$

where $\mathcal{L}_v = \left[\delta_1^{[v]}, \ldots, \delta_M^{[v]}\right], 1 \le v \le (2^M - 1)$, *is a set of* M *bits* $\delta_m^{[v]} \in \{0, 1\}, 1 \le m \le M$, *satisfying the* M*-bit binary series* $\left[\delta_M^{[v]} \ldots \delta_1^{[v]}\right] = \mathrm{dec2bin}(v)$ *(where* $\mathrm{dec2bin}(\cdot)$ *is a decimal-to-binary conversion function).* $\mathcal{L}_v$ *is used to expand the product of a sums into sum of products as* $\prod_{m=1}^{M}(1 + g_m) = 1 + \sum_{\mathcal{L}=1}^{\mathcal{L}_{(2^M-1)}} \prod_{m=1}^{M} (g_m)^{\delta_m^{[v]}}$. $\mathcal{C}_{p_n}$ *and* $\mathcal{D}_{p_n}$ *are coefficients of* x^{p_n} *for equations (15) and (16), respectively, which are calculated as*

$$\mathcal{C}_{p_n} = \sum_{\left(\sum_{m=1}^{M} l_m = p_n\right)}^{\mathrm{All}} \prod_{m=1}^{M} \mathcal{A}_{l_m}^{\mathrm{SE}_m}, \quad (17)$$

$$\mathcal{D}_{p_n} = \sum_{\left(\sum_{m=1}^{M} \delta_m^{[v]} l_m = p_n\right)}^{\mathrm{All}} \prod_{m=1}^{M} \left(\mathcal{B}_{\delta_m^{[v]} l_m}^{\mathrm{SE}_m}\right)^{\delta_m^{[v]}}; \quad (18)$$

the notation $\sum_{\left(\sum_{m=1}^{M} \beta_m = p_n\right)}^{\mathrm{All}}$ *denotes for the sum of all possible non-overlapping sets* $\{\beta_1, \ldots, \beta_M\}$ *including* M *non-negative integers* β_m, $1 \le m \le M$, *and satisfying* $\sum_{m=1}^{M} \beta_m = p_n$; *and the other parameters are defined as follows:* $K_{\mathrm{SE}} = \sum_{m=1}^{M} K_{\mathrm{SE}_m}$, $\mu_{\mathrm{SE}} = \sum_{m=1}^{M} \mu_{\mathrm{SE}_m}$, $\hat{M} = \sum_{m=1}^{M} \delta_m^{[v]}$, $\hat{K}_{\mathrm{SE}} = \sum_{m=1}^{M} \delta_m^{[v]} K_{\mathrm{SE}_m}$ *and* $\hat{\mu}_{\mathrm{SE}} = \sum_{m=1}^{M} \delta_m^{[v]} \mu_{\mathrm{SE}_m}$.

Proof: See Appendix B. □

According to [25], the instantaneous achievable secrecy rate is expressed as

$$C_{\mathrm{sec}} = [C_{\mathrm{U}} - C_{\mathrm{E}}]^+, \quad (19)$$

where $C_U = \log_2(1 + \gamma_0 X)$, $C_E = \log_2(1 + \gamma_0 Y)$ and $X \triangleq |h_{\mathrm{SU}}|^2$ is the channel gain of the $S \to U$ link.

B. SECRECY OUTAGE PROBABILITY (SOP)

For a given target secrecy rate $R_{\mathrm{sec}}^{\mathrm{tar}}$, the SOP is the probability that C_{sec} is lower than this target rate. Using (19), the SOP of the considered system is calculated as

$$\begin{aligned}
\mathrm{SOP} &= \Pr\left(C_{\mathrm{sec}} < R_{\mathrm{sec}}^{\mathrm{tar}}\right) = \Pr\left(C_{\mathrm{U}} - C_{\mathrm{E}} < R_{\mathrm{sec}}^{\mathrm{tar}}\right) \\
&= \Pr\left(\frac{1 - 2^{R_{\mathrm{sec}}^{\mathrm{tar}}} + \gamma_0 X}{2^{R_{\mathrm{sec}}^{\mathrm{tar}}} \gamma_0} < Y\right) \\
&= 1 - \Pr\left(Y < \frac{1}{2^{R_{\mathrm{sec}}^{\mathrm{tar}}}}\left(\frac{1 - 2^{R_{\mathrm{sec}}^{\mathrm{tar}}}}{\gamma_0} + X\right), \frac{1 - 2^{R_{\mathrm{sec}}^{\mathrm{tar}}}}{\gamma_0} < X\right) \\
&= 1 - \int_0^{\infty} f_X\left(x + \frac{2^{R_{\mathrm{sec}}^{\mathrm{tar}}} - 1}{\gamma_0}\right) F_Y\left(\frac{x}{2^{R_{\mathrm{sec}}^{\mathrm{tar}}}}\right) dx. \quad (20)
\end{aligned}$$

Proposition 3: The SOP of the considered system is expressed as follows.

$$\begin{aligned}
\mathrm{SOP} = 1 - \mu_{\mathrm{SU}} e^{-K_{\mathrm{SU}} - \frac{\mu_{\mathrm{SU}}}{\gamma_0}\left(2^{R_{\mathrm{sec}}^{\mathrm{tar}}} - 1\right) - K_{\mathrm{SE}}} \sum_{k=0}^{\infty} \frac{\left(K_{\mathrm{SU}} \mu_{\mathrm{SU}}\right)^k}{(k!)^2} \\
\times \sum_{i=0}^{k} \binom{k}{i} \left(\frac{2^{R_{\mathrm{sec}}^{\mathrm{tar}}} - 1}{\gamma_0}\right)^{k-i} \sum_{p_n=0}^{\infty} \frac{\mathcal{C}_{p_n}}{2^{p_n R_{\mathrm{sec}}^{\mathrm{tar}}}} \\
\times (i + p_n)! \left(\mu_{\mathrm{AB}} + \frac{\mu_{\mathrm{SE}}}{2^{R_{\mathrm{sec}}^{\mathrm{tar}}}}\right)^{-i-p_n-1}. \quad (21)
\end{aligned}$$

Proof: See Appendix C-A. □

C. THE AVERAGE SECRECY RATE (ASR)

The ASR is the expected value of C_{sec} that refers to the average amount of data sent to U securely. Using (19) the ASR is calculated as

$$\begin{aligned}
\mathrm{ASR} &= \mathbb{E}\{C_{\mathrm{sec}}\} = \mathbb{E}\left\{[C_{\mathrm{U}} - C_{\mathrm{E}}]^+\right\} \quad (22a) \\
&\ge [\bar{C}_{\mathrm{U}} - \bar{C}_{\mathrm{E}}]^+, \quad (22b)
\end{aligned}$$

where $\bar{C}_{\mathrm{U}} = \mathbb{E}\{C_{\mathrm{U}}\}$ and $\bar{C}_{\mathrm{E}} = \mathbb{E}\{C_{\mathrm{E}}\}$. The inequality in (22b) is obtained using the fact $\mathbb{E}\{\max\{a, b\}\} \ge \max\{\mathbb{E}\{a\}, \mathbb{E}\{b\}\}$ [3]. The value of $\bar{C}_{\{\mathrm{U,E}\}}$ is calculated using the CDF of {X,Y}, respectively. Using the integration by parts, we have

$$\begin{aligned}
\bar{C}_{\{\mathrm{U,E}\}} &= \frac{1}{\ln(2)} \int_0^{\infty} \ln(1 + \gamma_0 x) f_{\{\mathrm{X,Y}\}}(x) dx \\
&= \frac{1}{\ln(2)} \int_0^{\infty} \frac{1}{1 + x}\left(1 - F_{\{\mathrm{X,Y}\}}\left(\frac{x}{\gamma_0}\right)\right) dx. \quad (23)
\end{aligned}$$

Proposition 4: The analytical expressions for $\bar{C}_U$ *and* $\bar{C}_E$ *are respectively given by*

$$\begin{aligned}
\bar{C}_{\mathrm{U}} = \frac{e^{\frac{\mu_{\mathrm{SU}}}{\gamma_0} - K_{\mathrm{SU}}}}{\ln(2)} \left(-\mathrm{Ei}\left(-\frac{\mu_{\mathrm{SU}}}{\gamma_0}\right) \sum_{p_n=0}^{\infty} \mathcal{B}_{p_n}^{\mathrm{SU}} (-\gamma_0)^{-p_n} \right. \\
\left. + \sum_{p_n=1}^{\infty} \mathcal{B}_{p_n}^{\mathrm{SU}} \sum_{k=1}^{p_n} \binom{p_n}{k} \frac{(k-1)!}{(-\gamma_0)^{p_n-k} \mu_{\mathrm{SU}}^k} \Gamma\left(k, \frac{\mu_{\mathrm{SU}}}{\gamma_0}\right)\right), \quad (24)
\end{aligned}$$

$$\begin{aligned}
\bar{C}_{\mathrm{E}} = \sum_{\mathcal{L}_1}^{\mathcal{L}_{(2^M-1)}} \frac{(-1)^{\hat{M}+1} e^{\frac{\hat{\mu}_{\mathrm{SE}}}{\gamma_0} - \hat{K}_{\mathrm{SE}}}}{\ln(2)} \sum_{p_n=0}^{\infty} \mathcal{D}_{p_n} \\
\times \left(\begin{array}{l} -\mathrm{Ei}\left(-\frac{\hat{\mu}_{SE}}{\gamma_0}\right)(-\gamma_0)^{-p_n} \\ + \sum_{k=0}^{p_n} \binom{p_n}{k} \frac{(k-1)!}{(-\gamma_0)^{p_n-k} \hat{\mu}_{\mathrm{SE}}^k} \Gamma\left(k, \frac{\hat{\mu}_{\mathrm{SE}}}{\gamma_0}\right) \end{array}\right). \quad (25)
\end{aligned}$$

Proof: See Appendix C-B and Appendix C-C. □

D. GENETIC ALGORITHM-BASED IRS TILE-ALLOCATION-AND-PHASE-SHIFT-ADJUSTMENT (TAaPSA) STRATEGY

The obtained analytical results for the SOP and the ASR allow us to access the secrecy performance for any given IRS's TAaPSA strategy. In this section, we study the optimal solution for the TAaPSA for achieving the optimal ASR (OASR).

This optimal TAaPSA includes the labels, which represent the tile-allocation strategy, and the phase shifts of all RTs. Due to the complexity of (24) and (25), it is difficult to obtain this optimal solution using a mathematical approach. In addition, our problem involves a large variable space, a mixed domain (a discrete domain for the labels and a continuous domain for the phase shifts) and a non-independent relationship between the label and the SCPS of each RT. For that reason, we design a GA, which can efficiently solve such problems, to find the optimal solution for the TAaPSA. Moreover, the GA can perform parallel computing [26]; hence, it is possible to reduce the computational time of calculating complex equations, such as (24) and (25), for all individuals in the population of our GA. Then, we evaluate the respective SOP for this optimal TAaPSA. Due to the hardware limitation, the continuous phase shifts at the RTs are practically difficult to implement [27]; hence, our GA is designed for both discrete and continuous phase-shift cases.

In our GA, the chromosomes obey the structure $\text{Chr} = [\varphi_1, \ldots, \varphi_L, I_1, \ldots, I_L]$ where φ_l and $I_l \in \{1, \ldots, M+1\}$ are the values of phase shifts and labels of the l-th RT of IRS, $l = 1, \ldots, L$. For continuous phase-shift case, $\varphi_l \in [\varphi_{\text{low}}, \varphi_{\text{up}})$ where φ_{low} and φ_{up} are the lower and upper limits for phase shift of the IRS; for discrete phase-shift (DPS) case, $\varphi \in \mathcal{F} \triangleq \{\theta_1, \ldots, \theta_Q\}$ where $\mathcal{F}$ is a set including Q possible phase shifts $\theta_q, q = 1, \ldots, Q$. If $I_l = m, m \in \{1, \ldots, M\}$, the l-th RT is allocated to E_m; and if $I_l = (M+1)$, the l-th RT is allocated to U. The values of φ_l and I_l are randomly selected within their ranges in the initialization step. Since we focus on maximizing the ASR, the fitness function for Chr is given by

$$f_{\text{Fitness}}(\text{Chr}) = \text{ASR}\big|_{\text{Chr}} = \left[\bar{C}_{\text{U}} - \bar{C}_{\text{E}}\right]^{+}\big|_{\text{Chr}}. \quad (26)$$

The procedure of the GA-based TAaPSA is described as follows:

- Step 1: Get the necessary parameters for evaluating (24) and (25) except for the parameters of the TAaPSS (i.e., labels and phase shifts); set the iteration counter $count = 0$ and the maximum number of iteration max_iter.
- Step 2: Randomly generate a population $\mathbb{P}_{count} = \{\text{Chr}_1, \ldots, \text{Chr}_{2K}\}$ consisting of $2K$ chromosomes within their ranges.
- Step 3: Evaluate the fitness value of each chromosome using (26); rank the chromosomes using on their fitness values; and save the best chromosome Chr_{best}.
- Step 4: Perform uniform crossover using Algorithm 1 with crossover probability p_c to produce the next population $\mathbb{P}_{count+1}$. Next, perform mutation for $\mathbb{P}_{count+1}$ using Algorithm 2 with mutation probability p_m. Then, replace a random chromosome in $\mathbb{P}_{count+1}$ by Chr_{best}.
- Step 5: Increase $count$ (i.e., $count{+}{+}$); repeat Steps 3 and 4 if $count$ does not exceed max_iter otherwise return the current population and its fitness values.

In the crossover operator, the extended intermediate recombination is used to produce the continuous phase-shift values of the offspring to enhance the accuracy of the GA [28]. The function rand() returns an uniform distributed random number in the interval (0,1) and the function randi($[m, n]$) returns an uniform distributed random integer in a range $[m, n]$. In Step 4, the best chromosome Chr_{best} is placed in the next population to ensure the improvement in ASR after each iteration. Moreover, the optimal ASR is finite; hence, our GA is guaranteed to converge.

Algorithm 1 Crossover

Input: Crossover probability (p_c), population ($\mathbb{P}$), population size ($2K$),
number of RTs (L), bounds of phase shift ($\varphi_{\text{low}}, \varphi_{\text{up}}$), discrete phase
shift flag (*disphase*), scale factor ($-0.25 \le \varepsilon \le 0.25$).
Ouput: $2K$ chromosomes after the crossover operation

```
randomly arrange 2K chromosomes in ℙ.
for k = 1 to K do
select (2k−1)th and 2kth chromosomes, i.e., x and y, in ℙ;
  for l = 1 to L do      % Perform crossover for each RT
    if rand() < p_c then
      swap x(L+l) and y(L+l);          % Swap labels
      if disphase == 1 then
        swap x(l) and y(l); % Swap discrete phase shifts
      else      % Extended intermediate recombination for continuous phase shifts
        κ ← (1+2ε)rand()−ε;      % κ ~ U(−ε, 1+ε)
        x̂ ← x(l);
        ŷ ← y(l);
        x(l) ← ŷ + κ(x̂ − ŷ);
        y(l) ← x̂ + κ(ŷ − x̂);
        check and reset out-of-bound values;
      end if
    end if
  end for
end for
return ℙ
```

IV. SIMULATION RESULTS AND DISCUSSIONS

In this section, we present numerical results to validate the analytical expressions and the effectiveness of GA presented in Section III. The infinite upper limits of summations in the expressions of the SOP and the ASR are approximated by $N_{\max}$. Unless otherwise specified, the simulation setup for the coordinates (in meters) is illustrated in Fig. 2 and the parameters for simulation results are presented in Table 1. In Fig. 2, a point C is the center point of the IRS and points E_1, E_2, E_3 and E_4 are four PEs. To study the effect of different number of PEs, i.e., $M = 1, \ldots, 4$, on the secrecy performance, let $\mathcal{E}_{\text{M}}$ be a set consisting of M PE's locations. $\mathcal{E}_{\text{M}}$ is set as: $\mathcal{E}_1 = \{\mathbf{E}_1\}$, $\mathcal{E}_2 = \{\mathbf{E}_1, \mathbf{E}_2\}$, $\mathcal{E}_3 = \{\mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3\}$ and $\mathcal{E}_4 = \{\mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3, \mathbf{E}_4\}$.

Algorithm 2 Mutation

Input: Mutation probability (p_m), population ($\mathbb{P}$), population size ($2K$),
number of RTs (L), bounds of phase shift ($\varphi_{\text{low}}, \varphi_{\text{up}}$), number of PEs
(M), discrete phase shift flag (*disphase*).
Ouput: $2K$ chromosomes after the mutation operation.

for $k = 1$ to $2K$ **do**
select k^{th} chromosome, i.e., x, in $\mathbb{P}$.
  for $l = 1$ to L **do** % Perform mutation for each RT
    if rand()<p_m **then**
      $x(L+l) \leftarrow$ randi([1, M+1]); % Change labels
      if *disphase* == 1 **then**
        randomly select a phase shift in $\mathcal{F}$ for $x(l)$;
      else
        randomly select a phase shift in $[\varphi_{\text{low}}, \varphi_{\text{up}})$ for $x(l)$;
      end if
    end if
  end for
end for
return $\mathbb{P}$

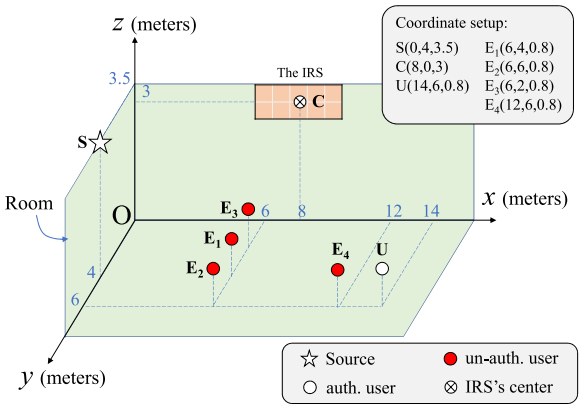
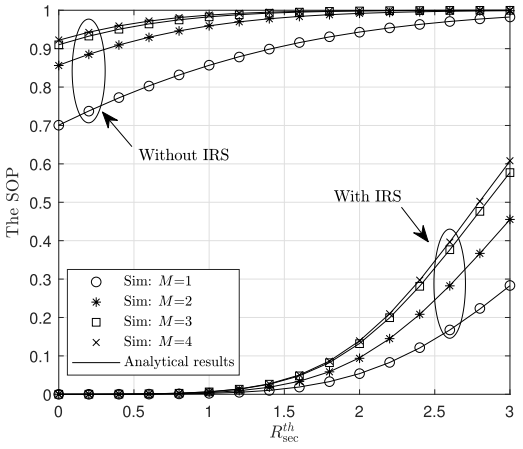


FIGURE 2. Simulation setup.

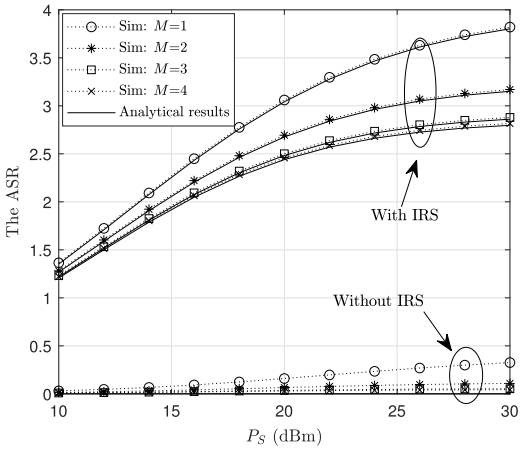
TABLE 1. Parameters for simulation results.

$\{f_0, \lambda_0, R_{\text{sec}}^{\text{tar}}\}$	{6 GHz, 0.05m, 1 bits/sec/Hz}
$\{P_{\text{S}}, \sigma_{\text{Fad}}^2, N_0\}$	{30, 19, -45}dBm
IRS's size ($l_{\text{IRS}} \times l_{\text{IRS}}$)	$10\lambda_0 \times 10\lambda_0 = 0.5{\times}0.5$ (meter^2)
Number of RTs	2(rows)×5(columns)
Room: width×length×height	$16 \times 8 \times 3.5$ (meter^3)
$\{N_{\max}, 2K, max\_iter, \varepsilon\}$	{80, 400, 300, 0.25}
$\{p_c, p_m\}$	{0.9, 0.1}
$\{\alpha_{\hat{R}_n}, \varphi_{\text{low}}, \varphi_{\text{up}}, \theta_q, Q\}$	$\{1, 0, 2\pi, 2\pi\frac{q-1}{Q}, 4\}$

Fig. 3 shows the SOP versus the target secrecy rate $R_{\text{sec}}^{\text{tar}}$ and the ASR versus the source transmit power P_{S}. Generally, it is seen that the SOP and the ASR are displayed as increasing



(a)

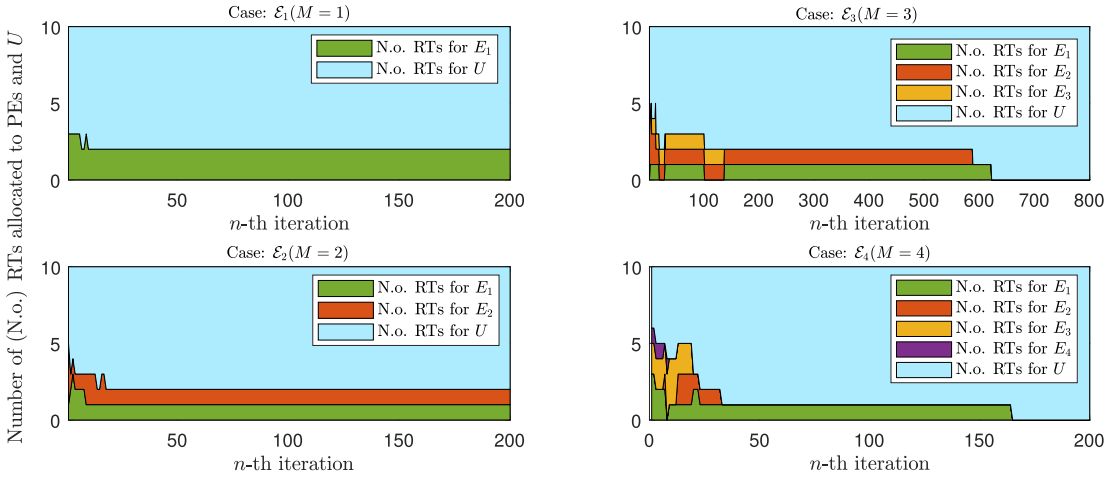


(b)

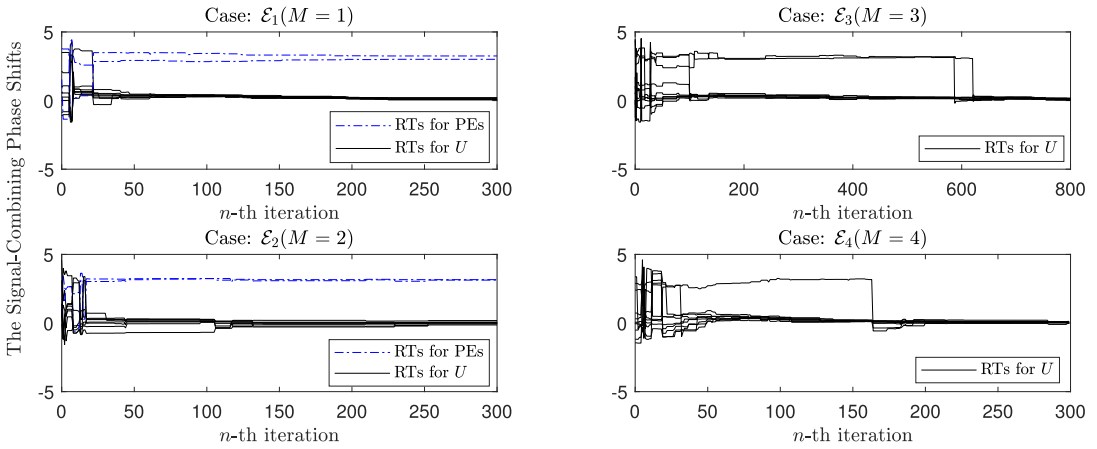
FIGURE 3. The effects of using IRS to improve (a) the SOP and (b) the ASR.

functions of $R_{\text{sec}}^{\text{tar}}$ and P_{S}, respectively, and the increase in the number of the PEs causes a higher security risk. Since we consider the worst case of secure communication where U is far from S and the PEs are close to S, the secrecy performance is very low in the non-IRS case. For instance, the SOP is around 0.7 when $R_{\text{sec}}^{\text{tar}} = 0$ bits/sec/Hz and grows rapidly when $R_{\text{sec}}^{\text{tar}}$ increases; and the ASR is around 0.1 bits/sec/Hz when $P_S = 30$ dBm. With the help of the IRS, the secrecy performance is significantly improved. As shown that the SOP is very small even $R_{\text{sec}}^{\text{tar}} = 1.5$ bits/sec/Hz whereas it approximates one for the non-IRS case. The simulation results of the SOP match well with the analytical results. For the ASR results, the approximation in (22b)) requires and sufficient high ASR to guarantee the equality. Therefore, for the non-IRS case, the analytical results seem inaccuracy due to very low ASR (around 0.2 bits/sec/Hz as shown in Fig. 3b); but for the contrary case, they agree well with the analytical results.

Fig. 4 shows the trends of the tile allocations and the SCPSs in range $[-0.5\pi, 1.5\pi)$, $\varphi_{\text{R}_l}^{\text{sc}}, l = 1 \ldots, L$, of the best chromosome Chr_{best} on each GA iteration. The IRS's phase shifts, φ_{R_l}, are obtained using the formula

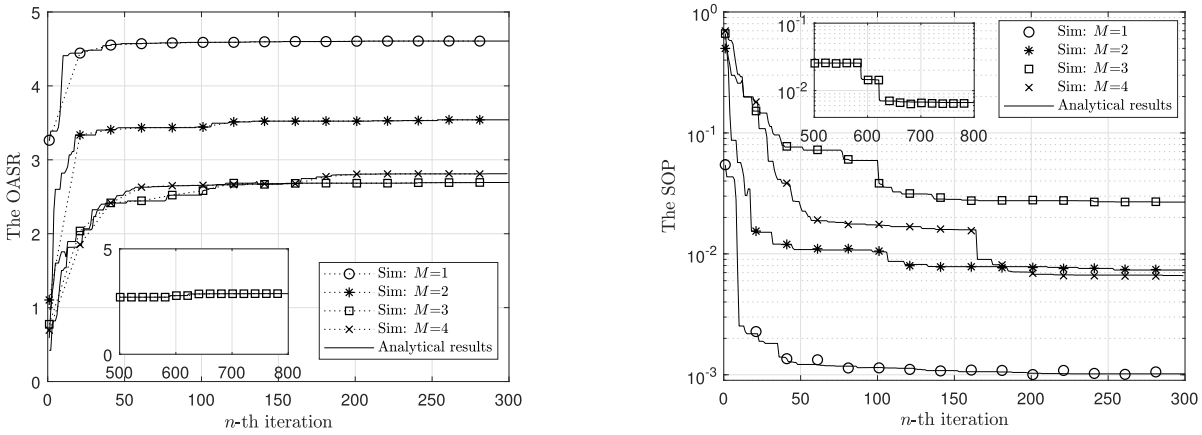


(a)



(b)

FIGURE 4. The optimal TAaPSA obtained using GA: (a) the numbers of the RTs allocated to PEs and user, and (b) the SCPS.



(a) (b)

FIGURE 5. The results of (a) The OASR and (b) the SOP over iterations.

$\varphi_{\mathrm{R}_l} = \varphi^{\mathrm{sc}}_{\mathrm{R}_l} - \varphi^{\mathrm{pd}}_{\mathrm{SR}_l\mathrm{D}} + \varphi^{\mathrm{pd}}_{\mathrm{SD}}$ where the phase shifts caused by the propagation distances $\varphi^{\mathrm{pd}}_{\mathrm{SR}_l\mathrm{D}}$ and $\varphi^{\mathrm{pd}}_{\mathrm{SD}}$ are constants. There are two optimal trends for the TAaPSA, i.e., Trend 1 and Trend 2, as described in Table 2. The SCPSs in Fig. 4b tend to zero and π for RTs serving U and PE, respectively. This means that the signal quality is improved

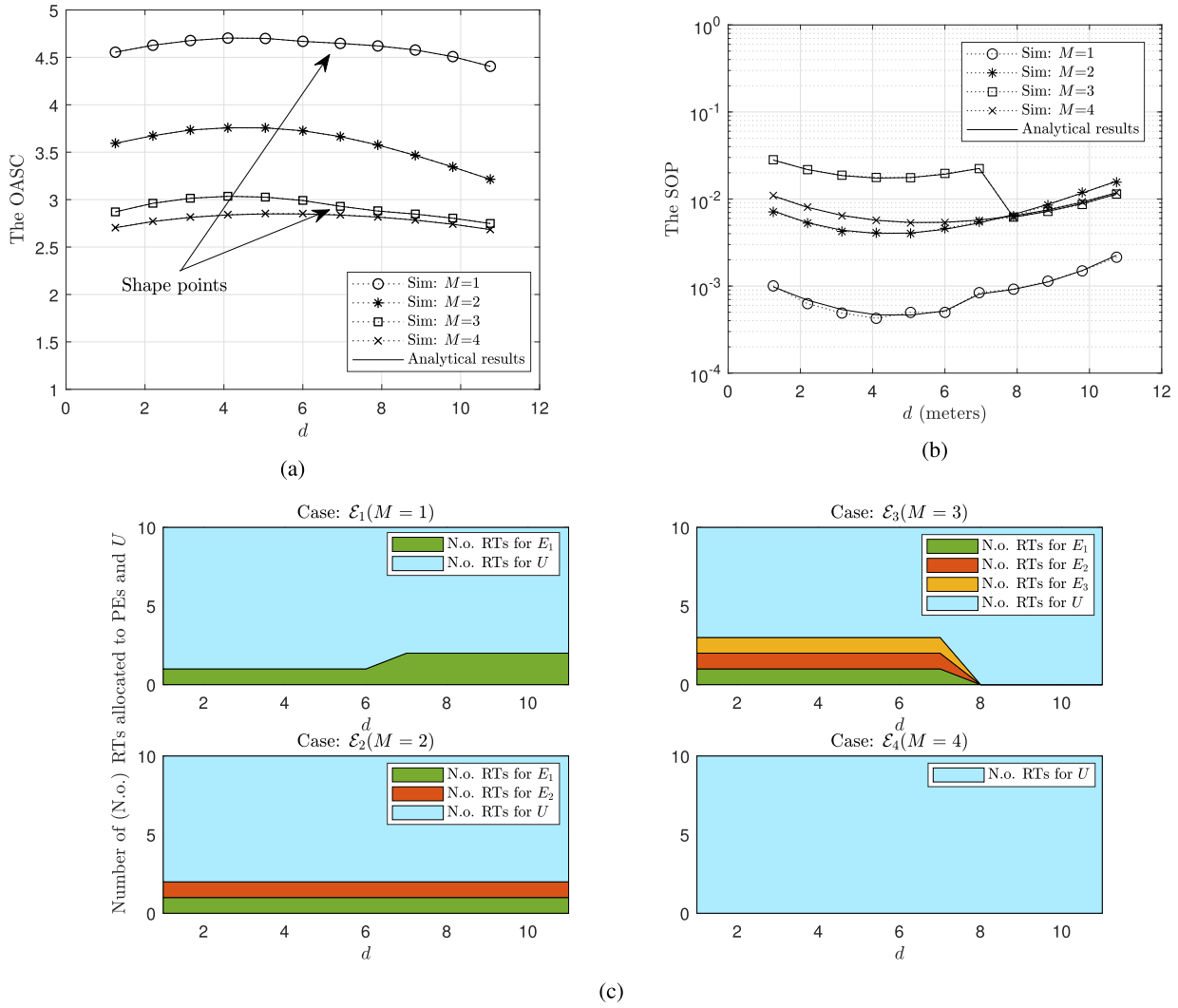


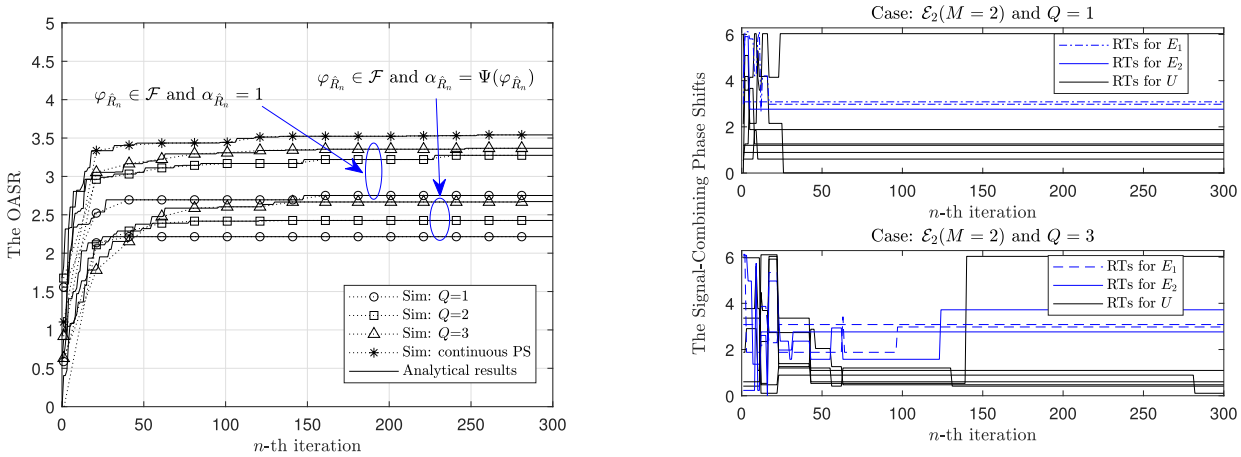
FIGURE 6. The effects of the IRS's location on (a) the OASR (b) the SOP and (c) the TAaPSS.

TABLE 2. Descriptions for Trend 1 and Trend 2.

	Trend 1	Trend 2
Methods	Improve the ASR by simultaneously enhancing the AR of U and degrading the OR at each PE.	Improve the ASR via enhancing the AR of U only.
PEs	Each PE is interfered by some RTs.	No RT is allocated to PEs.
User	The remain RTs assist the communication of U.	All RTs assist the communication of U.

at U and is degraded at the PE. The numbers of the RTs and PEs affect the optimal trend of the TAaPSA. Because of the logarithm function, the AR improves more slowly when more RTs are allocated to U; hence, the IRS does not need to use all RTs to assist the communication of U when M is small as compare to L. In particular, two RTs and one RT are allocated to each PE in the case of $M = 1$ and $M = 2$, respectively. When M is sufficient large as compare to L, the IRS must use a large number of RTs to disturb the overhearing of the PEs if it chooses Trend 1. This leads to the low AR of U and the system cannot reach the OASR. Therefore, the IRS chooses Trend 2 to achieve the OASR by boosting the AR of U only. For instance, it is seen in Fig. 4a that the IRS use Trend 1 and Trend 2 for the cases $M < 3$ and $M \geq 3$, respectively. The optimal chromosome converges after around 200 iterations; however, for the case $M = 3$, it takes a greater number of iterations to converge due to the difference in ASR between two optimal trends is very small (as shown in Fig. 5a).

Fig. 5 shows the OASR and the corresponding SOP obtained on each GA iteration. The OASR significantly increases during the first 150 iterations, then it improves slowly. Although the OASR seems to converge after the 250-th iteration, the TAaPSA needs more iterations to select the optimal trend, i.e., Trend 1 and Trend 2. This is clearly shown in the case of $M = 3$ that the OASR at the 250-th iteration is closed to the highest ASR, but the TAaPSA strategy switches to Trend 2 from the 620-th iteration. With a fixed target secrecy rate, the SOP generally improves as n



(a) (b)

FIGURE 7. (a) The OASRs of the DPSFA and DPDAV cases and (b) the SCPS of the DPDAV case over iterations.

increases due to the enhancement in OASR. On the other hand, the converged values for the SOPs are different. Since the SOP depends on both the mean and the deviation of the AR of U and ORs of PEs, the SOP can become better even the OASR receives lower values. For instance, the SOP for $M = 4$ seems better than the SOP for $M = 2$ while the OASR for $M = 4$ is smaller than the OASR for $M = 2$.

In Fig. 6, we set the coordinate of the center point of the IRS to $\mathbf{C}(d,0,3)$, $d \in [2.5l_{\text{IRS}}, 12]$ meters, and examine the effects of the IRS's location via varying d on the OASR, the corresponding SOP and the TAaPSA. The OASR improves when d increases from $2.5l_{\text{IRS}}$ to an optimal location d^*, and then it degrades with further increase in d. The value of d^* is in range [4, 6] meters. For $M = 1$ and $M = 2$, the TAaPSA obeys Trend 1 for all observed IRS's locations. Moreover, it is seen at Fig. 6c that one more RT is allocated to E_1 when $d > 8m$. For sufficient higher values of M (e.g., $M = 3$), there is a transition from Trend 1 to Trend 2 as seen at $d = 8$ meters. The reason of these changes is the travel distances of the reflected signals become too far to guarantee strong influence on the overhearing capacity at the PEs, hence, the IRS adjusts its parameters to use one more RT to degrade the OR at E_1 for the case $\mathcal{E}_1$ or to switch to Trend 2 for the case $\mathcal{E}_3$. The SOP's results for a given TAaPSA do not vary much when the IRS is shifted. The sharp points observed at the SOP's curves of the cases $\mathcal{E}_1$ and $\mathcal{E}_3$ are caused by the change in TAaPSA.

In Fig. 7, we extend our investigation to two cases of practical IRS and study the OASR for these cases. In one, the IRS supports several phase shifts $\theta_q, q = 1, \ldots, Q$, (presented in Table 1) with fixed reflection amplitude $\alpha_{\hat{\text{R}}_n} = 1$, discrete-phase-shift-fixed-amplitude (DPSFA) case. In the other, we study the joint effect of DPS and reflection amplitude variation caused by phase shift, discrete-phase-dependent-amplitude-variation (DPDAV) case. We use a phase shift model $\alpha_{\hat{\text{R}}_n} = \Psi(\varphi_{\hat{\text{R}}_n})$ proposed in [29] with parameters $\alpha_{\min} = 0.2$, $\zeta = 1.6$ and $\varphi_0 = 0.43\pi$ as follows.

$$\Psi(\varphi_{\hat{\text{R}}_n}) = (1-\alpha_{\min})\left(\frac{\sin(\varphi_{\hat{\text{R}}_n}-\varphi_0)+1}{2}\right)^{\zeta} + \alpha_{\min}. \quad (27)$$

The results of OASR in Fig. 7a show that the practical IRS causes a significant decrease in OASR; however, as compared to the non-IRS results shown in Fig. 3b, the practical IRS with two supported phase shift, i.e., $\mathcal{F} \triangleq \{0, \pi\}$, still produces a great advantage for secure communication. A higher number of the IRS's supported phase shifts allows the GA to achieve a higher resolution in phase shift, which leads to better solutions for the TAaPSA. In Fig. 7b, we plot the SCPC of the DPDAV case in range $[0, 2\pi)$. It is seen that the trend of SCPC is similar to that in Fig. 4b, i.e., the SCPS tends to zero and π for RTs allocated to U and PE, respectively. Due to the limits of possible values in $\mathcal{F}$, the SCPSs of RTs severing for PE are close to π and the SCPSs of the rest RTs are around zero or 2π. Moreover, the GA tends to use more RTs to degrade the ORs at PEs due to the degradation in reflection amplitude caused by the phase shift.

V. CONCLUSION

This paper studied the security capability of an IRS-aided indoor wireless communication system using an analytical approach that allows discovering the ASR and the SOP of the considered system. The closed-form analytical expressions for the SOP and ASR for a generalized TAaPSA strategy were derived. Then, the optimal TAaPSA strategy, which aims to maximize the ASR, was achieved using a GA. Moreover, the two practical IRS cases, i.e., DPSFA and DPDAV, were considered to investigate the performance loss caused by the IRS's limitations. The simulation results confirmed the accuracy of analytical results and enhancement of the ASR using GA. The obtained simulation results showed that the secrecy performance was remarkably improved with the help of the IRS and provided useful insight into the IRS's configuration

to archive the high security level. Specifically, the IRS adjusts the phase shifts of the RTs to achieve the SCPS of zero or π at the authenticated or unauthenticated users, respectively. The numbers of the RTs and the unauthenticated users have a significant effect on the optimal trend of the TAaPSA. For low numbers of the unauthenticated users, the ASR is maximized by simultaneously enhancing the AR of the authenticated user and degrading the ORs of the unauthenticated users; and for a contrary case, the IRS uses all RTs to boost the AR of the authenticated user. Moreover, the location of the IRS could be utilized as an additional effective solution to rise the secrecy performance. The paper studied the generalized model of the IRS; however, the secrecy performance results for particular IRS models can be obtained via modifying the parameters of the analytical results and the searching variable space of GA.

APPENDIX A

Using the definition of $\gamma(n,x)$ [21, Eq (8.350.1)], the CDF of $|h_{\rm SD}|^2$ is obtained after solving $f_{|h_{\rm SD}|^2}(x) = \int_0^{\infty} f_{|h_{\rm SD}|^2}(t)dt$ given as follows

$$F_{|h_{\rm SD}|^2}(x) = e^{-K_{\rm SD}} \sum_{k=0}^{\infty} \frac{K_{\rm SD}^k}{k!\Gamma(k+1)} \gamma(k+1, \mu_{\rm SD} x). \quad (28)$$

Due to the fact $\gamma(n,x) = \Gamma(n) - \Gamma(n,x)$, (28) can be rewritten as

$$F_{|h_{\rm SD}|^2}(x) = 1 - e^{-K_{\rm SD}} \sum_{k=0}^{\infty} \frac{K_{\rm SD}^k}{k!\Gamma(k+1)} \Gamma\left(k+1, \mu_{\rm SD} x\right). \quad (29)$$

Substituting the series representations $\gamma(n,x) = \Gamma(n) - \Gamma(n) e^{-x} \sum_{m=0}^{n-1} \frac{x^m}{m!}$ [21, Eq (8.352.1)] and $\Gamma(n,x) = \Gamma(n) e^{-x} \sum_{m=0}^{n-1} \frac{x^m}{m!}$ [21, Eq (8.352.2)] into (28) and (29), respectively, then using $\sum_{k=0}^{\infty} \alpha(k) \sum_{m=0}^{k+1} \beta(m) x^m = \sum_{m=0}^{\infty} x^m \beta(m) \sum_{k=m-1}^{\infty} \alpha(k)$ for combining like terms (note that $\alpha(-1) = 0$) and using the series representation $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$ [21, Eq (1.221.1)], we can obtain (9) and (10).

APPENDIX B

The CDF of Y is calculated as

$$F_Y(x) = \Pr(Y < x) = \prod_{m=1}^{M} F^{(\rm a)}_{|h_{{\rm SE}_m}|^2}(x), \quad (30a)$$

$$= \prod_{m=1}^{M} F^{(\rm b)}_{|h_{{\rm SE}_m}|^2}(x). \quad (30b)$$

Substituting (9) in to (30a), (30a) can be rewritten as

$$F_Y^{(\rm a)}(x) = e^{-K_{\rm SE}} e^{-\mu_{\rm SE} x} \prod_{m=1}^{M} \left(\sum_{p_n=1}^{\infty} \mathcal{A}_{p_n}^{{\rm SE}_m} x^{p_n} \right). \quad (31)$$

Using the fact

$$\prod_{m=1}^{M} \left(\sum_{n=0}^{\infty} \alpha(m,n) x^n \right) = \sum_{(\sum_{m=1}^{M} \beta_m = n)}^{\rm All} x^n \prod_{m=1}^{M} \alpha(m, \beta_m), \quad (32)$$

(31) can be rewritten as (15).

Substituting (10) in to (30b) yields

$$F_Y^{(\rm b)}(x) = \prod_{m=1}^{M} \left(1 - e^{-K_{{\rm SE}_m}} e^{-\mu_{{\rm SE}_m} x} \sum_{p_n=0}^{\infty} \mathcal{B}_{p_n}^{{\rm SE}_m} x^{p_n} \right). \quad (33)$$

The number 1 in the right-hand-side (RHS) of (33) causes the difficult in further calculations using $F_Y^{(\rm b)}(x)$. Hence, we consider each sum in RHS of (33) as the sum of 1 and the remain in the bracket and expand the product of these sums into the sum of products as mentioned in Proposition 2. By this way, (33) is rewritten as

$$\begin{aligned} F_Y^{(\rm b)}(x) &= 1 + \sum_{\mathcal{L}_1}^{\mathcal{L}_{(2^M-1)}} \prod_{m=1}^{M} \left(-e^{-(K_{{\rm SE}_m} + \mu_{{\rm SE}_m} x)} \right)^{\delta_m^{[v]}} \left(\sum_{p_n=0}^{\infty} \mathcal{B}_{p_n}^{{\rm SE}_m} x^{p_n} \right)^{\delta_m^{[v]}} \\ &= 1 + \sum_{\mathcal{L}_1}^{\mathcal{L}_{(2^M-1)}} (-1)^{\hat{M}} e^{-(\hat{K}_{\rm SE} + \hat{\mu}_{\rm SE} x)} \prod_{m=1}^{M} \left(\sum_{p_n=0}^{\infty} \mathcal{B}_{p_n}^{{\rm SE}_m} x^{p_n} \right)^{\delta_m^{[v]}}. \end{aligned} \quad (34)$$

Similarly, using (32), (34) can be rewritten as (16).

APPENDIX C

A. CALCULATION FOR THE SOP

Substituting (8) and (15) into (20) yields

$$\begin{aligned} {\rm SOP} &= 1 - \int_0^{\infty} \mu_{\rm SU} e^{-\left(K_{\rm SU} + \mu_{\rm SU}\left(x + \frac{2^{R_{\rm sec}^{\rm tar}} - 1}{\gamma_0}\right)\right)} \\ &\quad \times \sum_{k=0}^{\infty} \frac{(K_{\rm SU}\mu_{\rm SU})^k}{(k!)^2} \left(x + \frac{2^{R_{\rm sec}^{\rm tar}} - 1}{\gamma_0} \right)^k \\ &\quad \times e^{-\left(K_{\rm SE} + \frac{\mu_{\rm SE}}{2^{R_{\rm sec}^{\rm tar}}} x\right)} \sum_{p_n=0}^{\infty} \mathcal{C}_{p_n} \left(\frac{x}{2^{R_{\rm sec}^{\rm tar}}} \right)^{p_n} dx \\ &= 1 - \mu_{\rm SU} e^{-\left(K_{\rm SU} + K_{\rm SE} + \frac{\mu_{\rm SU}}{\gamma_0}\left(2^{R_{\rm sec}^{\rm tar}} - 1\right)\right)} \\ &\quad \times \sum_{k=0}^{\infty} \frac{(K_{\rm SU}\mu_{\rm SU})^k}{(k!)^2} \sum_{i=0}^{k} \binom{k}{i} \left(\frac{2^{R_{\rm sec}^{\rm tar}} - 1}{\gamma_0} \right)^{k-i} \\ &\quad \times \sum_{p_n=0}^{\infty} \frac{\mathcal{C}_{p_n}}{2^{p_n R_{\rm sec}^{\rm tar}}} \int_0^{\infty} x^{i+p_n} e^{-\left(\mu_{\rm SU} + \frac{\mu_{\rm SE}}{2^{R_{\rm sec}^{\rm tar}}}\right)x} dx. \end{aligned} \quad (35)$$

Using [21, Eq (3.351.3)], (35) can be rewritten as (21)

B. CALCULATION FOR $\bar{C}_U$

Substituting (10) into (23) yields

$$\bar{C}_{\rm U} = \frac{e^{-K_{\rm SU}}}{\ln(2)} \sum_{p_n=0}^{\infty} \frac{\mathcal{B}_{p_n}^{\rm SU}}{\gamma_0^{p_n}} \int_0^{\infty} \frac{x^{p_n}}{1+x} e^{-\frac{\mu_{\rm SU}}{\gamma_0} x} dx. \quad (36)$$

Letting $t = x+1$ and considering two cases of the exponent of t, one is t^{-1} and the other is t^n, $n = 0, 1, \ldots$, we have

$$\bar{C}_{\mathrm{U}} = \frac{e^{\frac{\mu_{\mathrm{SU}}}{\gamma_0} - K_{\mathrm{SU}}}}{\ln(2)} \left(\sum_{p_n=0}^{\infty} \frac{\mathcal{B}_{p_n}^{\mathrm{SU}}}{\gamma_0^{p_n}} (-1)^{p_n} \int_1^{\infty} t^{-1} e^{-\frac{\mu_{\mathrm{SU}}}{\gamma_0} t} dt + \sum_{p_n=1}^{\infty} \frac{\mathcal{B}_{p_n}^{\mathrm{SU}}}{\gamma_0^{p_n}} \sum_{k=1}^{p_n} \binom{p_n}{k} (-1)^{p_n-k} \int_1^{\infty} t^{k-1} e^{-\frac{\mu_{\mathrm{SU}}}{\gamma_0} t} dt \right). \tag{37}$$

Using [21, Eq (3.351.5) and (3.351.2)], (37) can be expressed as in (24).

C. CALCULATION FOR $\bar{C}_E$

Substituting (16) into (23) yields

$$\bar{C}_{\mathrm{E}} = \frac{-1}{\ln(2)} \sum_{\mathcal{L}_1}^{\mathcal{L}_{(2^M-1)}} (-1)^{\hat{M}} e^{-\hat{K}_{\mathrm{SE}}} \times \sum_{p_n=0}^{\infty} \frac{\mathcal{D}_{p_n}}{\gamma_0^{p_n}} \int_0^{\infty} \frac{x^{p_n}}{1+x} e^{-\frac{\hat{\mu}_{\mathrm{SE}}}{\gamma_0} x} dx. \tag{38}$$

Letting $t = x+1$ and considering two cases of the exponent of t, one is t^{-1} and the other is t^n, $n = 0, 1, \ldots$, we have

$$\bar{C}_E = \frac{-e^{\frac{\hat{\mu}_{SE}}{\gamma_0}}}{\ln(2)} \sum_{\mathcal{L}_1}^{\mathcal{L}_{(2^M-1)}} (-1)^{\hat{M}} e^{-\hat{K}_{SE}} \left(\sum_{p_n=0}^{\infty} \mathcal{D}_{p_n} (-\gamma_0)^{-p_n} \times \int_1^{\infty} t^{k-1} e^{-\frac{\hat{\mu}_{\mathrm{SE}}}{\gamma_0} t} dt + \sum_{p_n=0}^{\infty} \frac{\mathcal{D}_{p_n}}{\gamma_0^{p_n}} \sum_{k=0}^{p_n} \binom{p_n}{k} \times (-1)^{p_n-k} \int_1^{\infty} t^{k-1} e^{-\frac{\hat{\mu}_{\mathrm{SE}}}{\gamma_0} t} dt \right). \tag{39}$$

Using [21, Eq (3.351.5) and (3.351.2)], (39) can be expressed as in (25).

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan. 2015.

[2] K. Lee, J.-T. Lim, and H.-H. Choi, "Impact of outdated CSI on the secrecy performance of wireless-powered untrusted relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1423–1433, 2020.

[3] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2199–2213, Mar. 2017.

[4] A. Mabrouk, K. Tourki, M. O. Hasna, and N. Hamdi, "Performance analysis of secure AF relay networks using cooperative jamming under outdated CSI," *IET Commun.*, vol. 11, no. 14, pp. 2199–2205, Sep. 2017.

[5] Y. Ju, H.-M. Wang, T.-X. Zheng, and Q. Yin, "Secure transmissions in millimeter wave systems," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2114–2127, May 2017.

[6] J. Hu, S. Xu, W. Yang, and Y. Cai, "Secrecy performance of MRT/RAS system with outdated CSI in MIMO wiretap channels," in *Proc. Int. Conf. Cyberspace Technol. (CCT)*, 2013, pp. 422–427.

[7] Y. Huang, J. Wang, C. Zhong, T. Q. Duong, and G. K. Karagiannidis, "Secure transmission in cooperative relaying networks with multiple antennas," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6843–6856, Oct. 2016.

[8] L. Dai, B. Wang, M. Wang, X. Yang, J. Tan, S. Bi, S. Xu, F. Yang, Z. Chen, M. D. Renzo, C.-B. Chae, and L. Hanzo, "Reconfigurable intelligent surface-based wireless communications: Antenna design, prototyping, and experimental results," *IEEE Access*, vol. 8, pp. 45913–45923, 2020.

[9] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "Realizing wireless communication through software-defined HyperSurface environments," in *Proc. IEEE 19th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2018, pp. 14–15.

[10] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.

[11] M. Di Renzo, A. Zappone, M. Debbah, M.-S. Alouini, C. Yuen, J. de Rosny, and S. Tretyakov, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and road ahead," 2020, *arXiv:2004.09352*. [Online]. Available: http://arxiv.org/abs/2004.09352

[12] M. Song, P. Kapitanova, I. Iorsh, and P. Belov, *Metamaterials for Wireless Power Transfer*. St. Petersburg, Russia: Days Diffraction (DD), 2015, pp. 1–4.

[13] C. Huang, R. Mo, C. Yuen, and S. Member, "Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning," 2020, *arXiv:2002.10072*. [Online]. Available: http://arxiv.org/abs/2002.10072

[14] S. Hu, F. Rusek, and O. Edfors, "Beyond massive MIMO: The potential of data transmission with large intelligent surfaces," *IEEE Trans. Signal Process.*, vol. 66, no. 10, pp. 2746–2758, May 2018.

[15] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[16] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1488–1492, Sep. 2019.

[17] L. Dong and H.-M. Wang, "Secure MIMO transmission via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 787–790, Jun. 2020.

[18] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82599–82612, 2019.

[19] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, Jun. 2020.

[20] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A novel communication paradigm for high capacity and security via programmable indoor wireless environments in next generation wireless systems," *Ad Hoc Netw.*, vol. 87, pp. 1–16, May 2019.

[21] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, and D. Zwillinger, *Table of Integral, Series and Products*, 7th ed. Amsterdam, The Netherlands: Elsevier, 2007.

[22] V. Vikrant, *Wireless Communication*. New Delhi, India: Univ. Science Press, 2010.

[23] H. Suraweera, R. Louie, Y. Li, G. Karagiannidis, and B. Vucetic, "Two hop amplify-and-forward transmission in mixed Rayleigh and rician fading channels," *IEEE Commun. Lett.*, vol. 13, no. 4, pp. 227–229, Apr. 2009.

[24] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, Nov. 2019.

[25] Y. Huang, P. Zhang, Q. Wu, and J. Wang, "Secrecy performance of wireless powered communication networks with multiple eavesdroppers and outdated CSI," *IEEE Access*, vol. 6, pp. 33774–33788, 2018.

[26] J. Zhang, Y. Zhang, Z. Wang, J. Duan, and X. Huang, "An efficient optimization algorithm for extreme value of nonlinear function based on the SAGA and BP algorithm," *IEEE Access*, vol. 7, pp. 133058–133068, 2019.

[27] Q. Wu and R. Zhang, "Beamforming optimization for wireless network aided by intelligent reflecting surface with discrete phase shifts," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1838–1851, Mar. 2020.

[28] P. Kenneth, M. S. Rainer, and A. L. Jouni, *A. Differential Evolution A Practical Approach to Global Optimization*. Berlin Cham, Switzerland: Springer-Verlag, 2005.

[29] S. Abeywickrama, R. Zhang, Q. Wu, and C. Yuen, "Intelligent reflecting surface: Practical phase shift model and beamforming optimization," 2020, *arXiv:2002.10112*. [Online]. Available: http://arxiv.org/abs/2002.10112

VAN PHU TUAN received the B.E. and M.E. degrees in electronics and telecommunications engineering from the Ho Chi Minh City University of Technology, Vietnam, in 2010 and 2013, respectively, and the Ph.D. degree in electrical engineering from the University of Ulsan, South Korea, in 2018. From 2018 to 2019, he was a Postdoctoral Research Fellow with the University of Ulsan. He is currently a Postdoctoral Research Fellow with Kongju National University, South Korea. His major research interests include multiple-input-multiple-output communications systems, cooperative communications, physical layer security, non-orthogonal multiple access, energy harvesting, and optimization methods.

IC PYO HONG (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronics engineering from Yonsei University, Seoul, South Korea, in 1994, 1996, and 2000, respectively. From 2000 to 2003, he was with the Information and Communication Division, Samsung Electronics Company, Suwon, South Korea, where he was a Senior Engineer with the CDMA Mobile Research. Since 2003, he has been with the Department of Information and Communication Engineering, Kongju National University, Cheonan, South Korea. In 2006, he was a Visiting Scholar with Texas A&M University, College Station, TX, USA. In 2012, he was also a Visiting Scholar with Syracuse University, Syracuse, NY, USA. He is currently a Professor with Kongju National University. His research interests include numerical techniques in electromagnetics and periodic electromagnetic structures.