

# IRS-Assistance with Outdated CSI: Element subset selection for secrecy performance enhancement

Chu Li, Aydin Sezgin  
Ruhr-Universität Bochum, Germany  
Email: {chu.li, aydin.sezgin}@rub.de

**Abstract**—In this work, we investigate the secrecy performance in an intelligent reflecting surface (IRS)-assisted downlink system. In particular, we consider a base station (BS)-side IRS and as such, the BS-IRS channel is assumed to be known perfectly. Of more importance, we consider the case, in which only outdated channel state information (CSI) of the IRS-user channel is available. We study the impact of outdated CSI on the secrecy performance numerically and analytically. Furthermore, we propose an element subset selection (ESS) method in order to improve the secrecy performance. A key observation is that minimal secrecy outage probability (SOP) can be achieved using a subset of the IRS, and the optimal number of selected reflecting elements can be effectively found by closed-form expressions.

## I. INTRODUCTION

Due to the broadcast nature of the wireless medium, transmission over a wireless network is prone to eavesdropping on information intended to be exchanged between legitimate terminals. To securely transmit the data, physical security layer (PLS) techniques can be applied [1], [2]. In recent years, intelligent reflecting surfaces (IRS) have been applied in the field of PLS, which shows great potential to improve the security of wireless communication. IRS is a surface consisting of a large number of reflecting elements whose phase can be adaptively controlled by a microcontroller. The basic idea of an IRS-assisted system is to configure the IRS to reflect the signal in the direction of the desired legitimate receiver. Compared to conventional systems, IRS-assisted systems can achieve higher reliability and security at a lower cost [3]–[5].

The secrecy performance of IRS-assisted systems has been studied in many recent works. In [6], [7], the secrecy performance is analyzed in terms of secrecy outage probability (SOP) and secrecy rate in single-input single-output (SISO) systems considering the quantized phase error at IRS. The authors in [8] jointly designed the secure beamforming and artificial noise (AN) to maximize the secrecy rate in IRS-assisted multiple-input single-output (MISO) systems using the alternating direction method of multiplier (ADMM). This work is later extended to multiple-input multiple-output (MIMO) systems in [9], where majorization-minimization (MM) is used. The aforementioned works all assume perfect CSI, which is usually not the case in practice. In [10], the authors proposed a robust design of the beamformer at the base station (BS) and the phase shifters at IRS to maximize the system

sum rate considering CSI with estimation errors. Besides the estimation error, outdated CSI is also a major contributor to CSI imperfections [11]. In practice, the channel often changes with time. In addition, the channel estimation process and configuration of the beamformer at the BS and the phase shifters at the IRS may take time, especially if the number of reflecting elements is large. Consequently, the CSI observed by the BS may be outdated for subsequent data transmission. Configuring the beamformer at the BS and IRS phase shifters using outdated CSI will result in a loss of signal-to-noise ratio (SNR) and may degrade the secrecy performance.

In this work, we study the secrecy performance in IRS-assisted downlink systems considering outdated CSI of IRS-user channel. Since the phase shift at IRS cannot be configured precisely in practice, we further assume that each reflecting element suffers from an independent and uniformly distributed random phase error. We present the statistical characterization of SNR at Bob and Eve and derive the closed-form expressions of the SOP taking into account the outdated CSI. In addition, we propose a novel element subset selection (ESS) method that has low complexity and can be used to improve secrecy performance. More specifically,  $K$  of the total  $N$  reflecting elements are selected and turned on during transmission, while the other elements are turned off. The correctness of the closed-form expressions is verified by Monte-Carlo simulations. Additionally, we observe that the minimum SOP is achieved by using a subset of the reflecting elements.

## II. SYSTEM MODEL

In this work, we consider a BS with  $M$  antennas communicating with a legitimate user Bob in the presence of an eavesdropper Eve. Both Bob and Eve are equipped with single antennas. The transmission is facilitated by IRS, which consists of  $N = N_H N_V$  reflecting elements. The size of each element is  $d_H \times d_V$ , where  $d_H$  and  $d_V$  are the horizontal width and vertical height, respectively. Herein, we consider the IRS at the BS side, i.e., both BS and IRS are on the top of some high-rise buildings and close to each other [12]. Meanwhile, the IRS can be adaptively configured by the BS. Considering BS-side IRS, the channel between BS and IRS is modeled as

$$\mathbf{H} = \sqrt{\beta_H} \mathbf{a}(\varphi_1, \theta_1) \mathbf{b}^H(\varphi_2, \theta_2), \quad (1)$$

where  $\beta_H$  is the distance-dependent path loss factor,  $\mathbf{a}(\varphi_1, \theta_1) \in \mathbb{C}^M$  and  $\mathbf{b}(\varphi_2, \theta_2) \in \mathbb{C}^N$  are the steering vectors at BS and IRS, respectively. In this context,  $\varphi_1$  and  $\theta_1$

This work was funded by the Federal Ministry of Education and Research (BMBF) of the Federal Republic of Germany (Förderkenzeichen 16KISK095, 6G ANNA).

represent the azimuth and elevation angle of departure (AoD) at BS, while  $\varphi_2$  and  $\theta_2$  denote the azimuth and elevation angle of arrival (AoA) at IRS. Furthermore, the  $m$ -th element of  $\mathbf{a}$  is given by

$$\mathbf{a}_m = e^{j2\pi \frac{d_{BS}}{\lambda} (m-1) \sin \varphi_1 \sin \theta_1}, \quad (2)$$

where  $d_{BS}$  and  $\lambda$  are the inter-antenna separation at the BS and the carrier wavelength, respectively. Also, the  $n$ -th element of  $\mathbf{b}$  is

$$\mathbf{b}_n = e^{j\frac{2\pi}{\lambda} (k(n)d_H \cos \theta_2 \sin \varphi_2 + l(n)d_V \sin \theta_2)}, \quad (3)$$

where  $k(n) = \text{mod}(n-1, N_H)$  and  $l(n) = \lfloor (n-1)/N_H \rfloor$  are the horizontal and vertical indices of  $n$ -th element, respectively [13]. In this work, it is assumed that  $d_{BS} = d_H = d_V = 0.5\lambda$ , such that there is no correlation between the individual transmit antennas and the reflecting elements<sup>1</sup>. In practice, the distance-dependent path loss factor  $\beta_H$  in (1) remains unchanged for a long time. Also,  $\mathbf{a}(\theta_{\varphi_1, \theta_1})$  and  $\mathbf{b}(\theta_{\varphi_2, \theta_2})$  can be calculated accurately if the location and construction of the IRS are known. For this reason, we assume that perfect information of  $\mathbf{H}$  is available at BS, Bob and Eve. Furthermore, we use a  $N \times N$  diagonal matrix to represent the IRS

$$\tilde{\Phi} = \text{diag}(e^{j\tilde{\phi}_1}, e^{j\tilde{\phi}_2}, \dots, e^{j\tilde{\phi}_N}), \quad (4)$$

where  $\tilde{\phi}_n = \phi_n + \Delta\phi_n$  is the phase shift at the  $n$ -th reflecting element,  $\phi_n$  and  $\Delta\phi_n$  are the precise phase shift and random phase error at each element, respectively. More specifically, here we consider the discrete phase shift in IRS such that  $\Delta\phi_n$  is uniformly distributed in  $[-\frac{\pi}{L}, \frac{\pi}{L}]$ , where  $L$  is the number of quantization levels [14]. Moreover, the characteristic function of  $\Delta\phi_n$  can be computed by

$$\mu_p = \mathbb{E}[e^{jp\Delta\phi_n}] = \text{sinc}\left(-p\frac{\pi}{L}\right), \quad p \in \mathbb{Z}, \quad (5)$$

where  $\text{sinc}(x) = \frac{\sin(x)}{x}$ . The IRS-Bob channel and IRS-Eve channel are modeled as

$$\mathbf{h}_B \sim \mathcal{CN}(0, \beta_B \mathbf{I}_N), \quad \mathbf{h}_E \sim \mathcal{CN}(0, \beta_E \mathbf{I}_N), \quad (6)$$

where  $\beta_B$  and  $\beta_E$  are the path-loss factors. Furthermore, the direct link is assumed to be blocked by obstacles. Hence, the received signal at Bob and Eve are, respectively, given by

$$y_B = \sqrt{P}(\mathbf{H}\tilde{\Phi}\mathbf{h}_B)^H \mathbf{w}x + n_B, \quad (7)$$

$$y_E = \sqrt{P}(\mathbf{H}\tilde{\Phi}\mathbf{h}_E)^H \mathbf{w}x + n_E, \quad (8)$$

where  $P$  is the transmit power,  $\mathbf{w}$  denotes the beamformer at BS,  $x$  is the transmit data symbol with  $\mathbb{E}[|x|^2] = 1$ ,  $n_B \sim \mathcal{CN}(0, \sigma_B^2)$  and  $n_E \sim \mathcal{CN}(0, \sigma_E^2)$  are the receiver noise at Bob and Eve, respectively.

In this work, we consider a practical passive eavesdropper where the instantaneous CSI of  $\mathbf{h}_E$  is not available at the

<sup>1</sup>Although we set  $d_H = d_V = 0.5\lambda$ , there is still a weak correlation between the reflecting elements. However, the effect of such a weak correlation is negligible, which can be easily demonstrated by simulations. Therefore, in this work, it is assumed that there is no correlation between the individual reflecting elements

BS. Note that, unlike the BS-IRS channel, we assume that the instantaneous CSI of  $\mathbf{h}_B$  observed by the BS is outdated. This is because the channels between the IRS and the users usually changes over time, caused by the movements of the users and other objects around them. Let  $\hat{\mathbf{h}}_B$  denote the outdated version of  $\mathbf{h}_B$ , the relation between  $\hat{\mathbf{h}}_B$  and  $\mathbf{h}_B$  can be expressed as

$$\mathbf{h}_B = \rho \hat{\mathbf{h}}_B + \mathbf{e}_B, \quad (9)$$

where  $\rho = J_0(2\pi f_d T_d)$  is the correlation coefficient, and  $J_0$  is the zero-order Bessel function,  $f_d$  and  $T_d$  are the Doppler frequency and the time distance between  $\mathbf{h}_B$  and  $\hat{\mathbf{h}}_B$ , respectively. Moreover,  $\mathbf{e}_B$  is the complex Gaussian distributed error with covariance matrix  $(1 - \rho^2)\beta_g \mathbf{I}_N$ . The beamformer  $\mathbf{w}$  and IRS will be designed based on  $\mathbf{H}$  and  $\hat{\mathbf{h}}_B$ . More specifically, we apply maximum ratio transmission (MRT) to design the beamformer at BS expressed as

$$\mathbf{w} = \frac{\mathbf{H}\tilde{\Phi}\hat{\mathbf{h}}_B}{\|\mathbf{H}\tilde{\Phi}\hat{\mathbf{h}}_B\|}. \quad (10)$$

Now, similar to (9), we use  $\hat{\mathbf{h}}_E$  to represent the outdated version of  $\mathbf{h}_E$  modeled as

$$\mathbf{h}_E = \rho \hat{\mathbf{h}}_E + \mathbf{e}_E, \quad (11)$$

where  $\mathbf{e}_E \sim \mathcal{CN}(0, (1 - \rho^2)\beta_E \mathbf{I}_N)$ . Based on the system model introduced in this section, we analyze the secrecy performance in the following sections.

### III. SECRECY ANALYSIS

Let  $\gamma_B$  and  $\gamma_E$  denote the instantaneous SNR at Bob and Eve, respectively. According to [1], the instantaneous secrecy capacity is defined as

$$C_s(\gamma_B, \gamma_E) = [\log_2(1 + \gamma_B) - \log_2(1 + \gamma_E)]^+, \quad (12)$$

where  $[x]^+ = \max(0, x)$ . Unlike most state-of-the-art works, where Bob and Eve have their own perfect CSI, we investigate the secrecy performance in different scenarios, 1) Bob (and Eve) know their individual outdated CSI  $\hat{\mathbf{h}}_B$  (and  $\hat{\mathbf{h}}_E$ ), 2) Bob (and Eve) know their individual perfect CSI  $\mathbf{h}_B$  (and  $\mathbf{h}_E$ ), 3) Bob knows his outdated CSI  $\hat{\mathbf{h}}_B$  while Eve knows her perfect CSI  $\mathbf{h}_E$ . In the following, we characterize the received SNR at Bob and Eve in III-A and III-B. The secrecy outage probability is investigated in III-C.

#### A. SNR at Bob

In this subsection, we analyze the SNR at Bob assuming outdated and perfect CSI, respectively. If Bob knows his outdated CSI, i.e.,  $\hat{\mathbf{h}}_B$ , and coherent detection is performed, the received signal at Bob in (7) can be recast as

$$\begin{aligned} y_B &= \sqrt{P}(\mathbf{H}\tilde{\Phi}\mathbf{h}_B)^H \mathbf{w}x + n_B \\ &= \sqrt{P}(\mathbf{H}\tilde{\Phi}(\rho \hat{\mathbf{h}}_B + \mathbf{e}_B))^H \mathbf{w}x + n_B \\ &= \sqrt{P}\rho(\mathbf{H}\tilde{\Phi}\hat{\mathbf{h}}_B)^H \mathbf{w}x + \underbrace{\sqrt{P}(\mathbf{H}\tilde{\Phi}\mathbf{e}_B)^H \mathbf{w}x + n_B}_{\hat{n}_B}. \end{aligned} \quad (13)$$

Here, we treat the term containing the random error  $\mathbf{e}_B$  as the additional noise, and we use  $\hat{n}_B$  to denote the overall effective noise. The variance of  $\hat{n}_B$  is calculated as

$$\begin{aligned}\hat{\sigma}_B^2 &= \mathbb{E}[\hat{n}_B \hat{n}_B^H] = \sigma_B^2 + P \mathbb{E} \left[ \left| (\mathbf{H} \tilde{\Phi} \mathbf{e}_t)^H \frac{\mathbf{H} \Phi \hat{\mathbf{h}}_B}{\|\mathbf{H} \Phi \hat{\mathbf{h}}_B\|} \right|^2 \right] \\ &= \sigma_B^2 + PMN\beta_H(1 - \rho^2)\beta_B,\end{aligned}\quad (14)$$

where the last equality is obtained by substituting (1) and (10). Thus, the instantaneous SNR at Bob under the assumption of outdated CSI is given by

$$\begin{aligned}\hat{\gamma}_B &= \frac{P}{\mathbb{E}[\hat{\mathbf{n}}_B \hat{\mathbf{n}}_B^H]} \left| \rho (\mathbf{H} \tilde{\Phi} \hat{\mathbf{h}}_B)^H \mathbf{w} \right|^2 \\ &= \frac{P}{\hat{\sigma}_B^2} M \beta_H \rho^2 \left| \sum_{n=1}^N \hat{\mathbf{h}}_{B,n}^H e^{-j\tilde{\phi}_n} \mathbf{b}_n \right|^2,\end{aligned}\quad (15)$$

where  $\mathbf{b}_n$  and  $\hat{\mathbf{h}}_{B,n}$  are the  $n$ -th element of  $\mathbf{b}$  and  $\hat{\mathbf{h}}_B$ , respectively. If Bob has his perfect channel information, i.e.,  $\mathbf{h}_B$ , the instantaneous SNR at Bob is given by

$$\tilde{\gamma}_B = \frac{P}{\sigma_B^2} M \beta_H \left| \sum_{n=1}^N \mathbf{h}_{B,n}^H e^{-j\tilde{\phi}_n} \mathbf{b}_n \right|^2. \quad (16)$$

Next, we design the IRS to maximize the secrecy capacity in (12). To this end, the optimal IRS should be designed to maximize the SNR at Bob and minimize the SNR at Eve. However, since we assume that BS is unaware of Eve's instantaneous CSI, we find the optimal IRS by maximizing the SNR at Bob. In this context, the optimal IRS is obtained as

$$\phi_n^{opt} = \angle \left( \hat{\mathbf{h}}_{B,n}^H \mathbf{b}_n \right). \quad (17)$$

It is noticed that the optimal IRS maximizing  $\hat{\gamma}_B$  in (15) and  $\tilde{\gamma}_B$  in (16) are the same since only  $\mathbf{H}$  and  $\mathbf{h}_B$  are known to the BS and the IRS is being controlled by the BS. By plugging (17) in (15) and (16), we observe the distributions of  $\hat{\gamma}_B$  and  $\tilde{\gamma}_B$  in the following lemma.

*Lemma 1.*  $\hat{\gamma}_B$  and  $\tilde{\gamma}_B$  follow the Gamma distributions,

$$\hat{\gamma}_B \sim \text{Gamma}(\hat{\kappa}_B, \hat{\omega}_B), \quad (18)$$

$$\tilde{\gamma}_B \sim \text{Gamma}(\tilde{\kappa}_B, \tilde{\omega}_B), \quad (19)$$

where the scale parameters  $\hat{\kappa}_B$ ,  $\tilde{\kappa}_B$ , and the shape parameters  $\hat{\omega}_B$ ,  $\tilde{\omega}_B$  are introduced in Appendix A. The corresponding average SNRs at Bob are given by

$$\mathbb{E}[\hat{\gamma}_B] = \frac{P}{\hat{\sigma}_B^2} M \beta_H (\rho^2 N \beta_B + \rho^2 N(N-1) \frac{\pi}{4} \beta_B \mu_1^2), \quad (20)$$

$$\mathbb{E}[\tilde{\gamma}_B] = \frac{P}{\sigma_B^2} M \beta_H (N \beta_B + \rho^2 N(N-1) \frac{\pi}{4} \beta_B \mu_1^2). \quad (21)$$

*Proof.* See Appendix A.  $\square$

### B. SNR at Eve

Now, we investigate the SNR at Eve. Similar to (15) and (16), the instantaneous SNR at Eve assuming outdated and perfect CSI are, respectively, given by

$$\hat{\gamma}_E = \frac{P}{\hat{\sigma}_E^2} M \beta_H \rho^2 \left| \sum_{n=1}^N \hat{\mathbf{h}}_{E,n}^H e^{-j\tilde{\phi}_n} \mathbf{b}_n \right|^2, \quad (22)$$

$$\tilde{\gamma}_E = \frac{P}{\sigma_E^2} M \beta_H \left| \sum_{n=1}^N \mathbf{h}_{E,n}^H e^{-j\tilde{\phi}_n} \mathbf{b}_n \right|^2, \quad (23)$$

where

$$\hat{\sigma}_E^2 = \sigma_E^2 + PMN\beta_H(1 - \rho^2)\beta_E. \quad (24)$$

Next, we obtain the distribution of Eve's SNR as follows.

*Lemma 2.*  $\hat{\gamma}_E$  and  $\tilde{\gamma}_E$  follow the exponential distributions,

$$\hat{\gamma}_E \sim \text{Exp}(\hat{\lambda}_E), \quad \tilde{\gamma}_E \sim \text{Exp}(\tilde{\lambda}_E), \quad (25)$$

where  $\hat{\lambda}_E = \mathbb{E}[\hat{\gamma}_E] = \frac{PM\beta_H\rho^2 N\beta_E}{\hat{\sigma}_E^2 + PMN\beta_H(1-\rho^2)\beta_E}$  and  $\tilde{\lambda}_E = \mathbb{E}[\tilde{\gamma}_E] = \frac{P}{\sigma_E^2} M\beta_H N\beta_E$ .

*Proof.* The IRS is designed according to IRS-Bob channel, thereby  $\phi_n^{opt}$  can be considered as a randomly distributed variable by Eve. Thus, the SNRs at Eve can be approximated to exponential distributed variables [7].  $\square$

### C. Secrecy outage probability (SOP)

In this subsection, we analyze the secrecy performance in terms of the SOP, which is a crucial metric for measuring the security of a wireless channel. The SOP is defined as the probability that the secrecy capacity falls below a certain secrecy rate  $R_s$ ,

$$\begin{aligned}P_{so} &= \Pr(C_s \leq R_s) = \Pr \left[ \log_2 \left( \frac{1 + \gamma_B}{1 + \gamma_E} \right) \leq R_s \right] \\ &= \Pr [\gamma_B \leq 2^{R_s} (1 + \gamma_E) - 1] \\ &= \int_0^\infty F_{\gamma_B}(2^{R_s} (1 + \gamma_E) - 1) f_{\gamma_E}(\gamma_E) d\gamma_E,\end{aligned}\quad (26)$$

where  $\gamma_B \in [\hat{\gamma}_B, \tilde{\gamma}_B]$ , and  $\gamma_E \in [\hat{\gamma}_E, \tilde{\gamma}_E]$ .  $F_{\gamma_B}(\cdot)$  and  $f_{\gamma_E}(\cdot)$  are the corresponding probability density function (pdf) and cumulative density function (cdf) of the SNR at Bob and Eve.

*Theorem 1.* The exact SOP is given by

$$\begin{aligned}P_{so} &= \frac{1}{\Gamma(\kappa_B)} \sum_{p=0}^\infty \frac{\left( -\frac{1}{\omega_B} (2^{R_s} - 1) \right)^p}{p!} \\ &\quad \times G_{3,3}^{2,2} \left[ \frac{\omega_B}{\lambda_E 2^{R_s}} \mid \begin{matrix} 1, 1 + p - \kappa_B, 1 + p \\ 1, p, 1 + p \end{matrix} \right],\end{aligned}\quad (27)$$

where  $\kappa_B \in [\hat{\kappa}_B, \tilde{\kappa}_B]$ ,  $\omega_B \in [\hat{\omega}_B, \tilde{\omega}_B]$ ,  $\lambda_E \in [\hat{\lambda}_E, \tilde{\lambda}_E]$  and  $G_{\cdot,\cdot}^{\cdot,\cdot}$  denotes the Meijer's G-function [15]. Note that even though (27) contains infinite series, it converges quickly and can be approximated by a few terms.

*Proof.* The proof idea is analogous to [16, Corollary 9], hence omitted due to space constraints.  $\square$

To obtain further insights on the SOP, the following corollary is provided.

*Corollary 1.* The lower bound of the SOP is obtained as

$$P_{so} \geq \left( \frac{\lambda_E}{2^{-R_s} \omega_B + \lambda_E} \right)^{\kappa_B}, \quad (28)$$

where  $\kappa_B \in [\hat{\kappa}_B, \tilde{\kappa}_B]$ ,  $\omega_B \in [\hat{\omega}_B, \tilde{\omega}_B]$  and  $\lambda_E \in [\hat{\lambda}_E, \tilde{\lambda}_E]$ .

*Proof.* See Appendix B.  $\square$

#### IV. ELEMENT SUBSET SELECTION

In this section, we introduce ESS that can be used to improve the secrecy performance. ESS is inspired by transmit antenna selection, which is a technique used to enhance the wireless transmission [11], [17]. The key idea of ESS is to select the reflecting elements based on IRS-Bob's channel. During data transmission, only the selected elements are turned on, while the other elements are turned off. More specifically, the outdated CSI  $\hat{\mathbf{h}}_B$  is used to perform ESS in this work. The selection is considered random from Eve's point of view, which does not help to improve Eve's SNR but is beneficial to improve Bob's SNR. As a result, the secrecy performance can be effectively enhanced.

As the outdated CSI  $\hat{\mathbf{h}}_B$  is known to the BS, the ESS is performed based on its magnitude  $|\hat{\mathbf{h}}_B|$ . We arrange  $|\hat{\mathbf{h}}_B|$  in descending order as

$$|\hat{\mathbf{h}}_{B,s_1}| > |\hat{\mathbf{h}}_{B,s_2}| > \dots > |\hat{\mathbf{h}}_{B,s_N}|. \quad (29)$$

Here,  $K$  elements are selected from the total of  $N$  reflecting elements, and the set of selected indices is represented by  $\mathbf{S} = [s_1, s_2, \dots, s_K]$ . Therefore, the instantaneous SNR at Bob with ESS under outdated and perfect CSI are, respectively, given by

$$\hat{\gamma}_B^* = \frac{PM\beta_H\rho^2K^2}{\sigma_B^2 + PMK\beta_H(1-\rho^2)\beta_B} \left| \frac{1}{K} \sum_{n \in \mathbf{S}} |\hat{\mathbf{h}}_{B,n}| e^{j\tilde{\phi}_n} \right|^2, \quad (30)$$

$$\tilde{\gamma}_B^* = \frac{P}{\sigma_B^2} K^2 M \beta_H \left| \frac{1}{K} \left( \rho \sum_{n \in \mathbf{S}} |\hat{\mathbf{h}}_{B,n}| e^{j\Delta\phi_n} + \sum_{n \in \mathbf{S}} \mathbf{e}_{B,n} e^{j\tilde{\phi}_n} \right) \right|^2. \quad (31)$$

Let us define

$$\bar{h}_B = \frac{1}{K} \sum_{n \in \mathbf{S}} |\hat{\mathbf{h}}_{B,n}| = \mathbb{E} \left[ |\hat{\mathbf{h}}_{B,s_1}|, |\hat{\mathbf{h}}_{B,s_2}|, \dots, |\hat{\mathbf{h}}_{B,s_K}| \right]. \quad (32)$$

For large number  $N$ , we obtain  $\Pr(x \leq |\hat{\mathbf{h}}_{B,s_K}|) = \frac{N-K}{N}$ . It follows that  $|\hat{\mathbf{h}}_{B,s_K}| = \sqrt{-\beta_B \ln(1 - \frac{N-K}{N})}$ , since  $|\hat{\mathbf{h}}_{B,n}|$  obeys a Rayleigh distribution whose quantile can be computed by  $Q(q) = \sqrt{-\beta_B \ln(1-q)}$ . Additionally, the pdf and cdf of  $|\hat{\mathbf{h}}_{B,n}|$  are, respectively, given by

$$f(x) = \frac{2x}{\beta_B} e^{-\frac{x^2}{\beta_B}}, \quad F(x) = 1 - e^{-\frac{x^2}{\beta_B}}. \quad (33)$$

Thus, the mean value of (32) can be calculated by

$$\begin{aligned} \bar{\mu}_B &= \mathbb{E}[\bar{h}_B] = \frac{1}{1 - F(|\hat{\mathbf{h}}_{B,s_K}|)} \int_{|\hat{\mathbf{h}}_{B,s_K}|}^{\infty} x f(x) dx \\ &= \frac{1}{1 - F(|\hat{\mathbf{h}}_{B,s_K}|)} \int_{|\hat{\mathbf{h}}_{B,s_K}|}^{\infty} \frac{2x^2}{\beta_B} e^{-\frac{x^2}{\beta_B}} dx \\ &= \frac{\sqrt{2\beta_B}}{1 - F(|\hat{\mathbf{h}}_{B,s_K}|)} \int_{\frac{|\hat{\mathbf{h}}_{B,s_K}|^2}{\beta_B}}^{\infty} \sqrt{r} e^{-r} dr \\ &= \frac{\sqrt{2\beta_B}}{1 - F(|\hat{\mathbf{h}}_{B,s_K}|)} \Gamma \left( \frac{3}{2}, \frac{|\hat{\mathbf{h}}_{B,s_K}|^2}{\beta_B} \right), \end{aligned} \quad (34)$$

where  $\Gamma(\alpha, x)$  is the upper incomplete gamma function defined as  $\Gamma(\alpha, x) = \int_x^{\infty} t^{\alpha-1} e^{-t} dt$ , which is available in most software tools. According to [18], when  $N$  is large,  $\bar{h}_B$  is asymptotically normally distributed as

$$\bar{h}_B \sim \mathcal{N}(\bar{\mu}_B, \bar{\beta}_B), \quad (35)$$

where  $\bar{\mu}_B$  is given by (34),  $\bar{\beta}_B = \frac{p(1-p)}{N[f(F^{-1}(p))]^2}$  and  $p = 1 - e^{-\bar{\mu}_B^2/\beta_B}$ . Taking advantage of the fact that the random phase error at each element is independent of Bob's channel, we obtain the distribution of  $\hat{\gamma}_B^*$  and  $\tilde{\gamma}_B^*$  in the following lemma.

*Lemma 3.* The distributions of Bob's SNR with ESS assuming outdated and perfect CSI at Bob are, respectively, given by

$$\hat{\gamma}_B^* \sim \text{Gamma}(\hat{\kappa}_B^*, \hat{\omega}_B^*), \quad (36)$$

$$\tilde{\gamma}_B^* \sim \text{Gamma}(\tilde{\kappa}_B^*, \tilde{\omega}_B^*), \quad (37)$$

where  $\hat{\kappa}_B^* = \frac{K\mu_1^2\bar{\mu}_B^2}{2(\bar{\mu}_B^2 + \bar{\beta}_B)(1+\mu_2-2\mu_1^2)+4K\bar{\beta}_B\mu_1^2}$ ,  $\tilde{\kappa}_B^* = \frac{\rho^2 K \mu_1^2 \bar{\mu}_B^2}{2\rho^2(\bar{\mu}_B^2 + \bar{\beta}_B)(1+\mu_2-2\mu_1^2)+4\rho^2 K \bar{\beta}_B \mu_1^2 + 2(1-\rho^2)\beta_B}$ ,  $\hat{\omega}_B^* = \frac{\mathbb{E}[\hat{\gamma}_B^*]}{\hat{\kappa}_B^*}$  and  $\tilde{\omega}_B^* = \frac{\mathbb{E}[\tilde{\gamma}_B^*]}{\tilde{\kappa}_B^*}$ , in which

$$\mathbb{E}[\hat{\gamma}_B^*] = \frac{PM\beta_H\rho^2K(\bar{\mu}_B^2 + \bar{\beta}_B)(1 - \mu_1^2 + K\mu_1^2)}{\sigma_B^2 + PMK\beta_H(1 - \rho^2)\beta_B}, \quad (38)$$

$$\mathbb{E}[\tilde{\gamma}_B^*] = \frac{PM\beta_H\rho^2K}{\sigma_B^2} \left( (\bar{\mu}_B^2 + \bar{\beta}_B)(1 - \mu_1^2 + K\mu_1^2) + K(1 - \rho^2)\beta_B \right), \quad (39)$$

*Proof.* By using (35) and following the same steps as used in Lemma 1, we obtain the distribution of  $\hat{\gamma}_B^*$  and  $\tilde{\gamma}_B^*$ . Details are omitted due to space constraints.  $\square$

*Remark 1.* Note that the ESS for Eve is considered random, so the distribution of Eve's SNR with ESS can be easily obtained by Lemma 2, replacing  $N$  with  $K$ . We use  $\hat{\gamma}_E^*$  and  $\tilde{\gamma}_E^*$  to denote the instantaneous SNR at Eve with ESS assuming outdated and perfect CSI, and we obtain

$$\hat{\lambda}_E^* = \mathbb{E}[\hat{\gamma}_E^*] = \frac{PM\beta_H\rho^2K\beta_E}{\sigma_E^2 + PMK\beta_H(1-\rho^2)\beta_E}, \quad (40)$$

$$\tilde{\lambda}_E^* = \mathbb{E}[\tilde{\gamma}_E^*] = \frac{P}{\sigma_E^2} M\beta_H K\beta_E. \quad (41)$$

*Remark 2.* The SNR distribution at Bob and Eve remain unchanged with ESS. Therefore, the closed-form expression of the SOP with ESS and the corresponding lower bound can be obtained from Theorem 1 and Corollary 1 by setting  $\kappa_B \in [\hat{\kappa}_B^*, \tilde{\kappa}_B^*]$ ,  $\omega_B \in [\hat{\omega}_B^*, \tilde{\omega}_B^*]$  and  $\lambda_E \in [\hat{\lambda}_E^*, \tilde{\lambda}_E^*]$ .

Finally, the optimal number of selected reflecting elements can be obtained by

$$K_{opt} = \text{argmin} P_{so}^*(K), \quad (42)$$

where  $P_{so}^*(K)$  is the SOP as a function of  $K$ . Therefore, the SOP with optimal ESS can be calculated by  $P_{so}^*(K_{opt})$ .

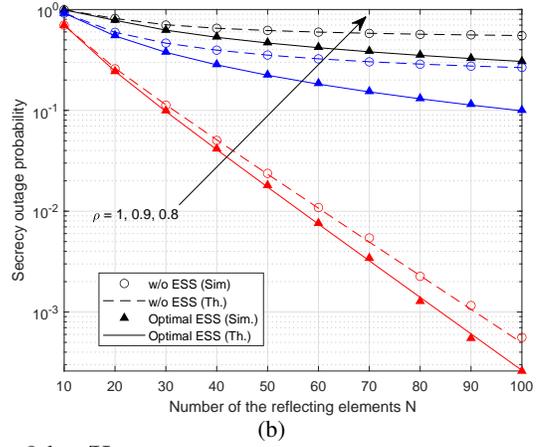
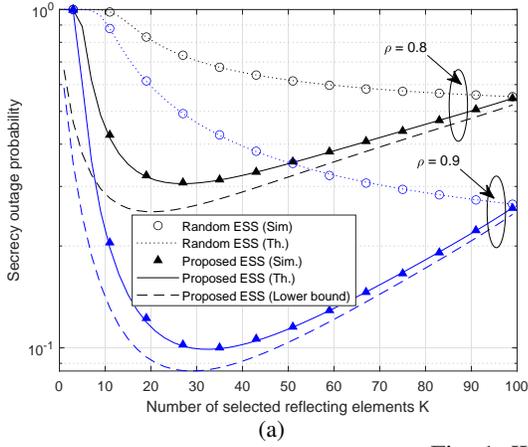


FIG. 1: Worst-case SOP,  $R_s = 2 \text{ bps/Hz}$

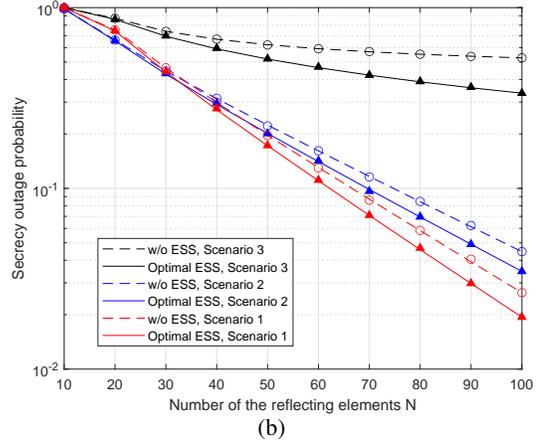
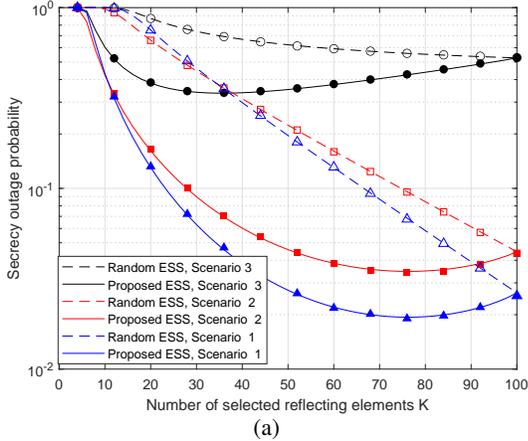


Fig. 2: Comparison of the SOP in different scenarios,  $\rho = 0.9$ ,  $R_s = 4 \text{ bps/Hz}$

## V. NUMERICAL RESULTS

In this section, we present the numerical results to evaluate the secrecy performance using the proposed ESS method. We obtain the numerical results by averaging over  $10^5$  Monte-Carlo simulations. Throughout the simulations, we set  $M = 4$ ,  $P = 5 \text{ dBm}$ ,  $\sigma_B^2 = \sigma_E^2 = -120 \text{ dBm}$ , and  $N = 100$  (if not specified otherwise). We assume that the distance between BS and IRS is  $d_1 = 10 \text{ m}$ , and the distance between IRS and Bob/Eve is  $d_2 = 80 \text{ m}$ . The pass-loss factors  $\beta_H$  and  $\beta_{B/E}$  are obtained by  $\beta_H = C_1 d_1^{-\alpha_1}$  and  $\beta_{B/E} = C_2 d_2^{-\alpha_2}$ , where  $C_1 = -26 \text{ dB}$ ,  $C_2 = -28 \text{ dB}$ ,  $\alpha_1 = 2.2$ , and  $\alpha_2 = 3.67$ . Also, it is assumed that the IRS phase error is uniformly distributed in  $[-\frac{\pi}{4}, \frac{\pi}{4}]$ .

We first evaluate the SOP in the scenario where Bob knows his outdated CSI  $\hat{\mathbf{h}}_B$  and Eve knows her perfect CSI  $\mathbf{h}_E$  in Fig. 1. This is the worst case because outdated CSI available at the receiver degrades the SNR at Bob. As a result, the secrecy performance is more critical than in other scenarios. Fig. 1a shows the SOP as a function of the number of selected reflecting elements  $K$ . Moreover, we compare the performance of the random ESS with that of the proposed ESS. It can be seen that the proposed ESS performs better than the random ESS. Meanwhile, the performance of both selections is the same when  $K = 100$ , since all elements available are selected. An interesting observation is that the

minimum SOP is achieved when only a small number of the reflecting elements are selected. We also compare the theoretical results with the simulation results. As can be seen, the theoretical results agree very well with the simulation results, which validates Theorem 1. Besides, the lower bound of the proposed ESS behaves similarly to the exact results and therefore can be used to find the optimal number of the selected reflecting elements. Fig. 1b shows the secrecy outage probability as a function of the number of reflecting elements  $N$ , where we compare the SOP using all elements (w/o ESS) and using the optimal ESS. It can be seen that the SOP becomes smaller as the number of reflecting elements increases. Also, the SOP is getting higher as the correlation parameter  $\rho$  decreases, which means that the outdated CSI degrades the secrecy performance. Besides, we find that the secrecy performance with optimal ESS is better than without ESS, especially for large  $N$ . Moreover, a perfect agreement between the theoretical and simulation results is observed, indicating the correctness of closed-form expressions.

In Fig. 2, we compare the SOP in different scenarios, where we use curves and markers to represent the theoretical and simulation results, respectively. The scenarios are defined in section III. Fig. 2a illustrates the SOP with the random ESS and the proposed ESS versus the number of selected reflecting elements  $K$ . It can be seen that the minimum SOP

with the proposed ESS for all scenarios is achieved by using only a subset of the IRS. Thus, it is necessary to find the optimal number of selected elements to achieve the minimum SOP. The secrecy performance without ESS and with the optimal ESS is compared in Fig. 2b, where we can see that the secrecy performance with the optimal ESS is better than that without ESS, implying that our proposed method can effectively enhance the secrecy performance in all scenarios.

## VI. CONCLUSION

In this work, we have studied the secrecy performance in an IRS-assisted multi-antenna BS system. In particular, we assumed that the BS is aware of the outdated CSI and the beamformers at the BS and IRS are designed by the outdated CSI. We characterized the SNR at Bob and Eve, which was used to analyze the SOP. In addition, we proposed an ESS method to improve the secrecy performance. Both the simulation and analytical results show that the proposed method can effectively improve the secrecy performance. An interesting observation is that the minimum secrecy outage probability can be achieved with a subset of the IRS.

## APPENDIX

### A. Proof of Lemma 1

Substituting (17) into (15), we obtain  $\hat{\gamma}_B = \frac{P}{\sigma_B^2} M \beta_H \rho^2 \left| \sum_{n=1}^N e^{j\Delta\phi_n} \hat{\mathbf{h}}_{B,n} \right|^2$ . Let  $\hat{X} = \sum_{n=1}^N e^{j\Delta\phi_n} \hat{\mathbf{h}}_{B,n}$ , assuming large number  $N$ , we have  $\text{Re}[\hat{X}] \sim \mathcal{N}(\hat{m}_u, \hat{\delta}_u^2)$  and  $\text{Im}[\hat{X}] \sim \mathcal{N}(0, \hat{\delta}_v^2)$ , where  $\hat{m}_u = \frac{N}{2} \sqrt{\pi} \beta_B \mu_1$ ,  $\hat{\delta}_u^2 = \frac{N}{2} \beta_B (1 + \mu_2 - \frac{\pi}{2} \mu_1^2)$ , and  $\hat{\delta}_v^2 = \frac{N}{2} \beta_B (1 - \mu_2)$  [14]. Thus, we obtain  $|\hat{X}|^2 = (\text{Re}[\hat{X}])^2 + (\text{Im}[\hat{X}])^2$  follow a Gamma distribution. It follows that  $\hat{\gamma}_B$  obeys a Gamma distribution with the mean value  $\mathbb{E}[\hat{\gamma}_B] = \frac{P}{\sigma_B^2} M \beta_H \rho^2 (|\text{Im}[\hat{X}]|^2 + |\text{Re}[\hat{X}]|^2) = \frac{P}{\sigma_B^2} M \beta_H \rho^2 (\hat{m}_u^2 + \hat{\delta}_u^2 + \hat{\delta}_v^2) = \frac{P}{\sigma_B^2} M \beta_H N \beta_B \rho^2 (1 + \frac{\pi}{4} \mu_1^2 (N - 1))$ , and the variance is given by  $\mathbb{V}[\hat{\gamma}_B] = \left( \frac{P}{\sigma_B^2} M \beta_H \rho^2 \right)^2 2 (2\hat{m}_u^2 \hat{\delta}_u^2 + \hat{\delta}_u^4 + \hat{\delta}_v^4)$ . Therefore, the shape and scale parameter can be computed by  $\hat{\kappa}_B = \frac{(\mathbb{E}[\hat{\gamma}_B])^2}{\mathbb{V}[\hat{\gamma}_B]} = \frac{(\hat{m}_u^2 + \hat{\delta}_u^2 + \hat{\delta}_v^2)^2}{2(2\hat{m}_u^2 \hat{\delta}_u^2 + \hat{\delta}_u^4 + \hat{\delta}_v^4)}$  and  $\hat{\omega}_B = \frac{\mathbb{V}[\hat{\gamma}_B]}{\mathbb{E}[\hat{\gamma}_B]} = \frac{P}{\sigma_B^2} M \beta_H \rho^2 \frac{2(2\hat{m}_u^2 \hat{\delta}_u^2 + \hat{\delta}_u^4 + \hat{\delta}_v^4)}{(\hat{m}_u^2 + \hat{\delta}_u^2 + \hat{\delta}_v^2)}$ , respectively. In the case where the perfect CSI is available, Bob's SNR is given by  $\tilde{\gamma}_B = \frac{P}{\sigma_B^2} M \beta_H |\rho \sum_{n=1}^N e^{j\Delta\phi_n} \hat{\mathbf{h}}_{B,n} + \sum_{n=1}^N \mathbf{e}_{B,n}|^2$ . Let  $\tilde{X} = \sum_{n=1}^N e^{j\Delta\phi_n} \hat{\mathbf{h}}_{B,n} + \sum_{n=1}^N \mathbf{e}_{B,n}$ , we have  $\text{Re}[\tilde{X}] \sim \mathcal{N}(\tilde{m}_u, \tilde{\delta}_u^2)$  and  $\text{Im}[\tilde{X}] \sim \mathcal{N}(0, \tilde{\delta}_v^2)$ , where  $\tilde{m}_u = \rho \frac{N}{2} \sqrt{\pi} \beta_B \mu_1$ ,  $\tilde{\delta}_u^2 = \rho^2 \frac{N}{2} \beta_B (1 + \mu_2 - \frac{\pi}{2} \mu_1^2) + \frac{N}{2} (1 - \rho^2) \beta_B$ , and  $\tilde{\delta}_v^2 = \rho^2 \frac{N}{2} \beta_B (1 - \mu_2) + \frac{N}{2} (1 - \rho^2) \beta_B$ . Following the same steps as deriving the scale and shape parameters under the assumption of outdated CSI, we observe  $\tilde{\kappa}_B = \frac{(\tilde{m}_u^2 + \tilde{\delta}_u^2 + \tilde{\delta}_v^2)^2}{2(2\tilde{m}_u^2 \tilde{\delta}_u^2 + \tilde{\delta}_u^4 + \tilde{\delta}_v^4)}$  and  $\tilde{\omega}_B = \frac{P}{\sigma_B^2} M \beta_H \frac{2(2\tilde{m}_u^2 \tilde{\delta}_u^2 + \tilde{\delta}_u^4 + \tilde{\delta}_v^4)}{(\tilde{m}_u^2 + \tilde{\delta}_u^2 + \tilde{\delta}_v^2)}$ .

### B. Proof of Corollary 1

The SOP in (26) can be rewritten as  $P_{so} = \Pr[\gamma_B \leq 2^{R_s} (1 + \gamma_E) - 1] = \Pr[\gamma_B \leq 2^{R_s} \gamma_E + \text{constant}] \geq 1 -$

$\Pr[\gamma_E/\gamma_B \leq 2^{-R_s}]$ . Exploiting the fact that  $\gamma_B$  and  $\gamma_E$  follow the Gamma and exponential distribution, we have  $\frac{\mathbb{E}[\gamma_B]\gamma_E}{\mathbb{E}[\gamma_E]\gamma_B}$  follows an original Fisher-Snedecor distribution with the degrees of freedom  $d_1 = 2$ ,  $d_2 = 2\kappa_B$ , where  $\mathbb{E}[\gamma_B]$  and  $\mathbb{E}[\gamma_E]$  are given by Lemma 1 and Lemma 2, respectively. As a result, we obtain  $P_{so} \geq 1 - \Pr[\gamma_E/\gamma_B \leq 2^{-R_s}] = 1 - \Pr\left[\frac{\mathbb{E}[\gamma_B]\gamma_E}{\mathbb{E}[\gamma_E]\gamma_B} \leq 2^{-R_s} \frac{\mathbb{E}[\gamma_B]}{\mathbb{E}[\gamma_E]}\right] = 1 - \text{I}_{\frac{d_1 x}{d_1 x + d_2}}(1, \kappa_B) = \left(\frac{\lambda_E}{2^{-R_s} \omega_B + \lambda_E}\right)^{\kappa_B}$ , where I is the regularized incomplete beta function and  $x = 2^{-R_s} \frac{\mathbb{E}[\gamma_B]}{\mathbb{E}[\gamma_E]}$ .

## REFERENCES

- [1] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.
- [2] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin, and C. Paar, "The Passive Eavesdropper Affects My Channel: Secret-Key Rates under Real-World Conditions," in *2016 IEEE Globecom Workshops*, 2016, pp. 1–6.
- [3] E. Björnson, H. Wymeersch, B. Matthiesen, P. Popovski, L. Sanguinetti, and E. de Carvalho, "Reconfigurable intelligent surfaces: A signal processing perspective with wireless applications," *IEEE Sign. Proc. Mag.*, vol. 39, no. 2, pp. 135–158, 2022.
- [4] P. Staat, S. Mulzer, S. Roth, V. Moonsamy, M. Heinrichs, R. Kronberger, A. Sezgin, and C. Paar, "IRShield: A countermeasure against adversarial physical-layer wireless sensing," in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 1705–1721.
- [5] K. Weinberger, A. A. Ahmad, A. Sezgin, and A. Zappone, "Synergistic Benefits in IRS- and RS-Enabled C-RAN With Energy-Efficient Clustering," *IEEE Trans. Wirel. Commun.*, vol. 21, no. 10, pp. 8459–8475, 2022.
- [6] E. Illi, M. K. Qaraqe, F. El Bouanani, and S. M. Al-Kuwari, "On the Secrecy Analysis of a RIS-aided Wireless Communication System Subject to Phase Quantization Errors," in *2022 IEEE BalkanCom.*, 2022, pp. 152–156.
- [7] I. Trigui, W. Ajib, and W. Zhu, "Secrecy outage probability and average rate of RIS-aided communications using quantized phases," *IEEE Commun. Lett.*, vol. 25, no. 6, pp. 1820–1824, 2021.
- [8] H. Niu, Z. Chu, F. Zhou, Z. Zhu, M. Zhang, and K. K. Wong, "Weighted sum secrecy rate maximization using intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 69, no. 9, pp. 6170–6184, 2021.
- [9] Z. Chu, W. Hao, P. Xiao, D. Mi, Z. Liu, M. Khalily, J. R. Kelly, and A. P. Feresidis, "Secrecy rate optimization for intelligent reflecting surface assisted MIMO system," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1655–1669, 2020.
- [10] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE JSAC*, vol. 38, no. 11, pp. 2637–2652, 2020.
- [11] N. S. Ferdinand, D. B. da Costa, and M. Latva-aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 864–867, 2013.
- [12] C. You, B. Zheng, W. Mei, and R. Zhang, "How to deploy intelligent reflecting surfaces in wireless network: BS-side, user-side, or both sides?," *Journal of Commun. and Info. Networks*, vol. 7, no. 1, pp. 1–10, 2022.
- [13] E. Björnson and L. Sanguinetti, "Rayleigh fading modeling and channel hardening for reconfigurable intelligent surfaces," *IEEE Wireless Commun. Lett.*, vol. 10, no. 4, pp. 830–834, 2020.
- [14] M. A. Badiu and J. P. Coon, "Communication through a large reflecting surface with phase errors," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 184–188, 2019.
- [15] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, Academic press, 2014.
- [16] O. S. Badarneh, P. C. Sofotasios, S. Muhaidat, S. L. Cotton, K. M. Rabie, and N. Aldahir, "Achievable physical-layer security over composite fading channels," *IEEE Access*, vol. 8, pp. 195772–195787, 2020.
- [17] J. G. Klotz and A. Sezgin, "Antenna selection criteria for interference alignment," in *IEEE PIMRC*, 2010, pp. 527–531.
- [18] F. Mosteller, "On some useful "inefficient" statistics," in *Selected Papers of Frederick Mosteller*, pp. 69–100. Springer, 2006.