

HKUST SPD - INSTITUTIONAL REPOSITORY

Title	Robust and Secure Wireless Communications via Intelligent Reflecting Surfaces
Authors	Yu, Xianghao; Xu, Dongfang; Sun, Ying; Ng, Derrick Wing Kwan; Schober, Robert
Source	IEEE Journal on Selected Areas in Communications, v. 38, (11), November 2020, article number 9133130, p. 2637-2652
Version	Accepted Version
DOI	10.1109/JSAC.2020.3007043
Publisher	IEEE
Copyright	© 2020 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

This version is available at HKUST SPD - Institutional Repository (<https://repository.ust.hk>)

If it is the author's pre-published version, changes introduced as a result of publishing processes such as copy-editing and formatting may not be reflected in this document. For a definitive version of this work, please refer to the published version.

Robust and Secure Wireless Communications via Intelligent Reflecting Surfaces

Xianghao Yu, *Member, IEEE*, Dongfang Xu, *Student Member, IEEE*, Ying Sun, *Member, IEEE*,
Derrick Wing Kwan Ng, *Senior Member, IEEE*, and Robert Schober, *Fellow, IEEE*

Abstract—In this paper, intelligent reflecting surfaces (IRSs) are employed to enhance the physical layer security in a challenging radio environment. In particular, a multi-antenna access point (AP) has to serve multiple single-antenna legitimate users, which do not have line-of-sight communication links, in the presence of multiple multi-antenna potential eavesdroppers whose channel state information (CSI) is not perfectly known. Artificial noise (AN) is transmitted from the AP to deliberately impair the eavesdropping channels for security provisioning. We investigate the joint design of the beamformers and AN covariance matrix at the AP and the phase shifters at the IRSs for maximization of the system sum-rate while limiting the maximum information leakage to the potential eavesdroppers. To this end, we formulate a robust non-convex optimization problem taking into account the impact of the imperfect CSI of the eavesdropping channels. To address the non-convexity of the optimization problem, an efficient algorithm is developed by capitalizing on alternating optimization, a penalty-based approach, successive convex approximation, and semidefinite relaxation. Simulation results show that IRSs can significantly improve the system secrecy performance compared to conventional architectures without IRS. Furthermore, our results unveil that, for physical layer security, uniformly distributing the reflecting elements among multiple IRSs is preferable over deploying them at a single IRS.

Index Terms—Alternating optimization, imperfect channel state information, intelligent reflecting surface, physical layer security.

I. INTRODUCTION

TWO fundamental properties of the wireless medium, namely broadcast and superposition, make wireless transmissions inherently vulnerable to security breaches, which has been a pivotal issue in modern wireless communication systems [2]–[4]. Besides conventional cryptographic encryption methods employed in the application layer, advanced signal processing techniques developed for facilitating security in

the physical layer have emerged as indispensable means to guarantee secure wireless communication in recent years [4]. The essential premise of these techniques is to exploit the intrinsic randomness of the noise and fading characteristics of wireless communication channels to limit the amount of information that can be extracted by potential eavesdroppers. Various approaches for enhancing physical layer security of wireless networks have been proposed in the literature including cooperative relaying [5], artificial noise (AN)-aided beamforming [6], and cooperative jamming [7]. However, these existing approaches have two main demerits. First, deploying active relays and other helpers for security provisioning incurs high hardware cost and consumes additional energy. Second, in unfavorable wireless propagation environments, it is difficult to guarantee satisfactory secrecy performance even if AN or jamming signals are exploited. However, the propagation properties of wireless channels cannot be adaptively controlled with traditional communication technologies as would be desirable for ensuring secure communication. To overcome these two shortcomings of existing systems, a new cost-effective and energy-efficient paradigm is needed which is capable of shaping the radio propagation environment.

Benefiting from the rapid evolution of radio frequency (RF) micro-electro-mechanical systems (MEMS), programmable and reconfigurable metasurfaces have found abundant applications in different domains in recent years [8]–[11]. Among various types of metasurfaces, intelligent reflecting surfaces (IRSs), a kind of passive metasurface, are particularly appealing and have been recently exploited for wireless communication system design [12], [12]–[18]. Specifically, IRSs are able to change the end-to-end signal propagation direction with low-cost *passive* components, e.g., printed dipoles and phase shifters, which is a revolutionary new characteristic that has not been leveraged in any of the contemporary wireless systems. Furthermore, metasurfaces in the form of artificial thin films can be easily coated on existing infrastructures such as walls of buildings, which reduces the operational expenditure and complexity of deploying IRSs. Hence, IRSs hold great promise for many applications as they provide a cost-effective approach to control the radio propagation environment while avoiding the deployment of additional power-hungry and expensive communication devices, e.g., amplify-and-forward relays [19]. In particular, these characteristics position IRSs as a key enabler for improving the physical layer security of wireless communication systems in an economical and energy-efficient manner [20]. However, to fully unleash the potential of IRSs for security provisioning, joint optimization of the

Manuscript received December 3, 2019; revised April 20, 2020; accepted May 8, 2020. X. Yu is supported by the Alexander von Humboldt Foundation. D. Xu is supported by the Chinese Scholarship Council (CSC). D. W. K. Ng is supported by funding from the UNSW Digital Grid Futures Institute, UNSW, Sydney, under a cross-disciplinary fund scheme and by the Australian Research Council’s Discovery Project (DP190101363). This work has been presented in part at the IEEE Global Communications Conference, Waikoloa, HI, USA, Dec. 2019 [1]. (*Corresponding author: Dongfang Xu.*)

X. Yu, D. Xu, and R. Schober are with the Institute for Digital Communications, Friedrich-Alexander-University Erlangen-Nürnberg (FAU), 91054 Erlangen, Germany (e-mail: {xianghao.yu, dongfang.xu, robert.schober}@fau.de).

Y. Sun is with the School of Industrial Engineering, Purdue University, West Lafayette, IN 47907, USA (e-mail: sun578@purdue.edu).

D. W. K. Ng is with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia (e-mail: w.k.ng@unsw.edu.au).

IRSs and conventional approaches to enhance physical layer security, such as transmit beamforming and AN injection at the access point (AP), is required.

Recently, the amalgamation of IRSs and physical layer security has received significant attention in the literature. Initial results on IRS-assisted secure wireless systems were provided in [1], [21], [22], starting from a simple network model with only one legitimate user and one eavesdropper. As a matter of fact, one of the difficulties for algorithm design for IRS-assisted systems are the highly non-convex unit modulus constraints induced by the phase shifter implementation of IRSs. Based on semidefinite relaxation (SDR) and Gaussian randomization methods, suboptimal solutions for both the beamformer at the AP and the phase shifts at the IRS were developed in [22]. Majorization minimization techniques were leveraged in [1], [21] to tackle the non-convex unit modulus constraints, which led to a better performance compared to the classical SDR method. Secure wireless systems comprising multiple legitimate users and multiple eavesdroppers were investigated in [23] and [24], respectively, where manifold optimization and SDR were applied to handle the non-convexity of the formulated problems. To guarantee secure communication, joint optimization of transmit beamforming and AN injection at the AP were considered in both [23] and [24]. The authors of [25] studied the maximization of the minimum secrecy rate among several legitimate users in the presence of multiple eavesdroppers, where the unit modulus constraints of the phase shifters were approximated by a set of convex constraints. Although this approach considerably simplifies the algorithm design, it may lead to a significant performance loss. All these existing works [1], [21]–[25] assumed that the potential eavesdroppers were equipped with a single antenna and perfect channel state information (CSI) of the eavesdropping channels was available at the AP. However, in practice, a worst-case assumption is needed for successful security provisioning, i.e., the eavesdroppers are expected to possess more hardware resources and computational capabilities than the legitimate users, e.g., antenna elements and interference mitigation capabilities. Furthermore, acquiring perfect CSI of the eavesdropping channels at the AP is challenging since potential eavesdroppers are not continuously interacting with the AP and the corresponding CSI at the AP may be outdated even if the channel is only slowly time-varying. Therefore, the assumptions of single-antenna eavesdroppers and perfect eavesdropper CSI at the AP are generally overly optimistic which weakens the generality and practicality of the system models considered in [1], [21]–[25] and the associated resource allocation algorithm designs. To the best of the authors' knowledge, the design of robust and secure IRS-assisted wireless communication systems with multi-antenna eavesdroppers has not been studied in the literature, yet.

To address the aforementioned issues, this paper investigates physical layer security provisioning for IRS-assisted wireless systems, where a multi-antenna AP transmits confidential data to multiple single-antenna legitimate users in the presence of several multi-antenna potential eavesdroppers. To help establish a favorable propagation environment for secure communication, IRSs implemented by programmable phase

shifters are deployed. The system sum-rate is maximized by taking into account the imperfect knowledge of the CSI of the eavesdropping channels, while the maximum information leakage to the potential eavesdroppers is constrained. To this end, the design of the considered robust and secure IRS-assisted multiuser multiple-input single-output (MISO) system is formulated as a non-convex optimization problem. The highly non-convex unit modulus constraints induced by the phase shifter implementation and the infinitely many inequality constraints introduced by the imperfect CSI are the main challenges for solving the problem. First, an efficient alternating optimization (AO) based approach is developed to tackle the non-convexity of the problem, and subsequently, the design of the transmit beamformers, AN covariance matrix, and IRS phase shifts is handled by successive convex approximation (SCA) and SDR-based methods. In particular, the non-convex IRS phase shift design problem with unit modulus constraints is reformulated as an equivalent rank-constrained problem, for which an effective difference of convex (d.c.) function representation is adopted to handle the rank-one constraint. Simulation results confirm the effectiveness of the AO based algorithm compared to various baseline methods. Furthermore, our results reveal that by deploying IRSs, favorable channel conditions are created for the legitimate users, and therefore, the physical layer security of wireless systems can be significantly improved. Moreover, we show that uniformly distributing the reflecting elements across multiple IRSs is beneficial for enhancing the secrecy performance.

Notations: In this paper, the imaginary unit of a complex number is denoted by $j = \sqrt{-1}$. Matrices and vectors are denoted by boldface capital and lower-case letters, respectively. The set of nonnegative integers is denoted as $\mathbb{N} = \{0, 1, \dots\}$. $\mathbb{C}^{m \times n}$ denotes the set of all $m \times n$ complex-valued matrices; \mathbb{H}^m denotes the set of all $m \times m$ Hermitian matrices; \mathbf{I}_m is the m -dimensional identity matrix; $\mathbf{1}_m$ represents the $m \times 1$ all-ones vector; $\mathbf{0}$ represents the all-zeros matrix. \mathbf{X}^* , \mathbf{X}^T , and \mathbf{X}^H stand for the conjugate, transpose, and conjugate transpose of matrix \mathbf{X} , respectively. The ℓ_2 -norm of vector \mathbf{x} is denoted as $\|\mathbf{x}\|$. The determinant, Frobenius norm, nuclear norm, and spectral norm of matrix \mathbf{X} are represented as $\det(\mathbf{X})$, $\|\mathbf{X}\|_F$, $\|\mathbf{X}\|_*$, and $\|\mathbf{X}\|_2$, respectively. $\text{diag}(\mathbf{x})$ denotes a diagonal matrix whose diagonal elements are extracted from vector \mathbf{x} , and $\text{blkdiag}(\mathbf{X}_1, \dots, \mathbf{X}_n)$ denotes a block diagonal matrix whose diagonal components are $\mathbf{X}_1, \dots, \mathbf{X}_n$; $\text{Diag}(\mathbf{X})$ represents a vector whose elements are extracted from the diagonal elements of matrix \mathbf{X} . The largest eigenvalue of matrix \mathbf{X} and the corresponding eigenvector are denoted by $\lambda_{\max}(\mathbf{X})$ and $\boldsymbol{\lambda}_{\max}(\mathbf{X})$, respectively. \triangleq and \sim mean “defined as” and “distributed as”, respectively. $\text{Tr}(\mathbf{X})$ and $\text{Rank}(\mathbf{X})$ denote the trace and rank of matrix \mathbf{X} ; $\mathbf{X} \succeq \mathbf{0}$ indicates that \mathbf{X} is a positive semidefinite (PSD) matrix. The distribution of a circularly symmetric complex Gaussian (CSCG) vector with mean vector \mathbf{x} and covariance matrix $\boldsymbol{\Sigma}$ is denoted by $\mathcal{CN}(\mathbf{x}, \boldsymbol{\Sigma})$. For a real-valued continuous function $f(\mathbf{X})$, $\nabla_{\mathbf{X}} f$ represents the gradient of f with respect to matrix \mathbf{X} . $\mathbb{E}[\cdot]$ represents statistical expectation and $[x]^+ = \max\{0, x\}$. The optimal value of an optimization variable \mathbf{X} is denoted by \mathbf{X}^* .

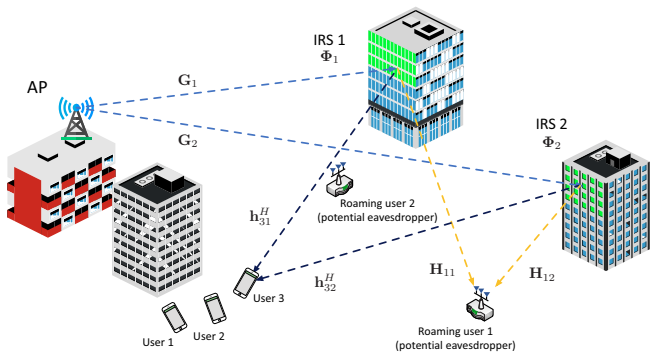


Fig. 1. An IRS-assisted multiuser MISO secure communication system comprising $K = 3$ legitimate users, $J = 2$ roaming users, and $L = 2$ IRSs coated on two buildings. The reflecting elements are represented by green rectangles. For the ease of illustration, only the parameters of the channels from the IRSs to potential eavesdropper 1 and legitimate user 3 are shown.

II. SYSTEM MODEL

In this section, we first present the system model for secure IRS-assisted multiuser MISO downlink wireless communication. Then, we discuss our assumptions regarding CSI knowledge for system design.

A. IRS-Assisted System Model

We consider the downlink of an IRS-assisted secure communication system that comprises one AP, K single-antenna legitimate users, J roaming users, and L IRSs, as shown in Fig. 1. The AP is equipped with $N_t > 1$ transmit antennas. Different from the local legitimate users, the J roaming users are traveling wireless devices belonging to other communication systems and are equipped with $N_r > 1$ antennas. The roaming users may attempt to deliberately eavesdrop the signals transmitted to the legitimate users. Therefore, we treat the J roaming users as potential eavesdroppers. In addition, L passive IRSs are deployed in the network to improve the physical layer security, where IRS l is equipped with M_l programmable phase shifters. The direct links from the AP to the legitimate users are assumed to be blocked by obstacles (e.g., buildings). As a result, the AP communicates with the legitimate users via the IRSs and focuses its transmit beams on the IRSs. We assume that both the AP and the IRSs are deployed at sufficiently high altitudes such that the potential eavesdroppers cannot intercept the links between the AP and the IRSs. Furthermore, as the beams reflected by the IRSs to the legitimate users and potential eavesdroppers are typically tilting down to the ground to serve the legitimate users, reflections between IRSs are negligible. Therefore, the downlink received baseband signals at legitimate user k and potential eavesdropper j can be expressed as¹

$$y_k = \sum_{l \in \mathcal{L}} \mathbf{h}_{kl}^H \Phi_l \mathbf{G}_l \left(\sum_{i \in \mathcal{K}} \mathbf{w}_i s_i + \mathbf{z} \right) + n_k$$

¹For multiple IRSs, the delays between the propagation paths reflected by different IRSs are typically much shorter than the symbol duration. For example, in a small cell network with 200 m cell radius, the maximum delay is 1.3 μs while the symbol duration in the Long-Term Evolution (LTE) standard is 70 μs [26]. Thus, intersymbol interference is not considered in (1) and (2).

$$= \mathbf{h}_k^H \Phi \mathbf{G} \left(\sum_{i \in \mathcal{K}} \mathbf{w}_i s_i + \mathbf{z} \right) + n_k, \quad \forall k \in \mathcal{K}, \quad (1)$$

$$y_j = \sum_{l \in \mathcal{L}} \mathbf{H}_{jl} \Phi_l \mathbf{G}_l \left(\sum_{i \in \mathcal{K}} \mathbf{w}_i s_i + \mathbf{z} \right) + \mathbf{n}_j$$

$$= \mathbf{H}_j \Phi \mathbf{G} \left(\sum_{i \in \mathcal{K}} \mathbf{w}_i s_i + \mathbf{z} \right) + \mathbf{n}_j, \quad \forall j \in \mathcal{J}, \quad (2)$$

respectively, where $\mathcal{L} = \{1, \dots, L\}$, $\mathcal{K} = \{1, \dots, K\}$, $\mathcal{J} = \{1, \dots, J\}$, $\mathbf{h}_k^H = [\mathbf{h}_{k1}^H, \dots, \mathbf{h}_{kL}^H]$, $\mathbf{H}_j = [\mathbf{H}_{j1}, \dots, \mathbf{H}_{jL}]$, $\Phi = \text{blkdiag}(\Phi_1, \dots, \Phi_L)$, and $\mathbf{G} = [\mathbf{G}_1, \dots, \mathbf{G}_L]^T$. Here, the information-bearing signal transmitted by the AP to legitimate user i and the corresponding beamforming vector are denoted as $s_i \in \mathbb{C}$ and $\mathbf{w}_i \in \mathbb{C}^{N_t \times 1}$, respectively, where $\mathbb{E}[|s_i|^2] = 1$, $\forall i$, without loss of generality. The channel matrix from the AP to IRS l is denoted as $\mathbf{G}_l \in \mathbb{C}^{M_l \times N_t}$, while the channel vector between legitimate user k and IRS l is represented by $\mathbf{h}_{kl}^H \in \mathbb{C}^{1 \times M_l}$. $\mathbf{H}_{jl} \in \mathbb{C}^{N_r \times M_l}$ is the channel matrix between eavesdropper j and IRS l . The phase shift matrix Φ_l at IRS l is given by $\Phi_l = \text{diag}(\mathbf{v}_l)$, where $\mathbf{v}_l = [e^{j\theta_{l1}}, e^{j\theta_{l2}}, \dots, e^{j\theta_{lM_l}}]^T$ and θ_{li} is the controllable phase shift introduced by the i -th reflecting element of IRS l [27]. In addition, $n_k \sim \mathcal{CN}(0, \sigma_{1,k}^2)$ and $\mathbf{n}_j \sim \mathcal{CN}(\mathbf{0}, \sigma_{e,j}^2 \mathbf{I}_{N_r})$ represent the additive white Gaussian noise (AWGN) at legitimate user k and potential eavesdropper j , with $\sigma_{1,k}^2$ and $\sigma_{e,j}^2$ being the corresponding noise variances, respectively. $\mathbf{z} \in \mathbb{C}^{N_t \times 1}$ is the AN vector generated by the AP to deliberately combat the eavesdroppers. Specifically, \mathbf{z} is modeled as a CSCG vector with $\mathbf{z} \sim \mathcal{CN}(\mathbf{0}, \mathbf{Z})$, where $\mathbf{Z} \in \mathbb{H}^{N_t}$, $\mathbf{Z} \succeq \mathbf{0}$, is the covariance matrix of the AN vector. The AN is assumed to be unknown to both the legitimate users and the potential eavesdroppers. For notational convenience, in the rest of this paper, we drop index l in the elements of the phase shift matrices of all IRSs and use $\Phi = \text{diag}(\mathbf{v})$, where $\mathbf{v} = [\mathbf{v}_1^T, \mathbf{v}_2^T, \dots, \mathbf{v}_L^T]^T \triangleq [e^{j\theta_1}, e^{j\theta_2}, \dots, e^{j\theta_M}]^T$ and $M = \sum_{l \in \mathcal{L}} M_l$.

Remark 1: The legitimate users are expected to have limited capabilities compared to the potential eavesdroppers. In order to ensure secure communication under such unfavorable conditions, we consider the worst case where all legitimate users are equipped with a single antenna while all potential eavesdroppers have multiple antennas.

Remark 2: We assume that resource allocation is performed separately for blocked and non-blocked legitimate users, respectively, via user scheduling. In particular, the AP can directly serve the non-blocked legitimate users using the direct channels without the help of IRSs. In this paper, we focus on the resource allocation for the blocked legitimate users which are supported by multiple IRSs. In IRS-assisted systems, the multi-antenna AP focuses its transmit beams on the IRSs to take full advantage of the reflecting elements. Moreover, we assume that the AP and IRSs are installed well above ground on top of high buildings. Thus, the legitimate users and potential eavesdroppers, which are located on the ground, cannot intercept the AP-IRS link. Therefore, the signal leakage from the AP to the legitimate users and potential eavesdroppers

$$R_k = \log_2 \left(1 + \frac{|\mathbf{h}_k^H \Phi \mathbf{G} \mathbf{w}_k|^2}{\text{Tr}(\mathbf{G}^H \Phi \mathbf{h}_k \mathbf{h}_k^H \Phi \mathbf{G} \mathbf{Z}) + \sigma_{1,k}^2 + \sum_{i \in \mathcal{K} \setminus \{k\}} |\mathbf{h}_k^H \Phi \mathbf{G} \mathbf{w}_i|^2} \right) \quad (4)$$

via the respective direct links is negligible in the considered IRS-assisted system.

B. Channel State Information (CSI)

The legitimate users transmit pilot signals to the AP via the IRSs to facilitate channel estimation. As a result, the AP is able to periodically acquire the CSI of the legitimate users. Several channel estimation techniques for IRS-assisted systems have been proposed recently, e.g., [28], [29]. Hence, we assume the availability of perfect CSI for the AP-IRS-legitimate user links, \mathbf{G} and $\{\mathbf{h}_k\}_{k=1}^K$, during the whole transmission period. On the other hand, for the potential eavesdroppers (roaming users), they send signals to their dedicated wireless systems rather than the AP. Furthermore, as the potential eavesdroppers usually try to hide their existence from the AP, they are not expected to cooperate with the AP for CSI acquisition. Therefore, although the signal leakage from the potential eavesdroppers to the AP can still be utilized for channel estimation [30], the acquired CSI is expected to be coarse and outdated. To account for this effect, we adopt a deterministic model [31]–[34] to characterize the CSI uncertainty. Specifically, the CSI of the links between the IRSs and eavesdropper j is modeled as follows

$$\begin{aligned} \mathbf{H}_j &= \bar{\mathbf{H}}_j + \Delta \mathbf{H}_j, \\ \Omega_j &\triangleq \{\Delta \mathbf{H}_j \in \mathbb{C}^{N_r \times M} : \|\Delta \mathbf{H}_j\|_F \leq \epsilon_j\}, \quad j \in \mathcal{J}, \end{aligned} \quad (3)$$

where $\bar{\mathbf{H}}_j \in \mathbb{C}^{N_r \times M}$ is the estimate of the channel of potential eavesdropper j at the AP at the beginning of the scheduling slot. The CSI estimation error for eavesdropper j is modeled by the term $\Delta \mathbf{H}_j$. Continuous set Ω_j contains all possible CSI estimation errors with their norms bounded by $\epsilon_j > 0$. The adopted deterministic model in (3) is a flexible and general CSI uncertainty model, which is able to account for the bounded CSI uncertainty caused by different elements of the CSI acquisition process in IRS-assisted systems, e.g., quantization errors of the phase shifts at the IRSs [35], noisy estimation [36], and outdated feedback. The uncertainty radius ϵ_j represents the level of uncertainty and can be chosen smaller for more accurate quantization and channel estimation algorithms, and longer coherence times.

III. RESOURCE ALLOCATION PROBLEM FORMULATION

In this section, we define the adopted performance metrics and formulate the resource allocation design as an optimization problem.

A. Achievable Rate and Secrecy Rate

According to the signal model in (1), the achievable rate (bits/s/Hz) of legitimate user k is given by (4), as shown on the top of this page [37]. Then, for security provisioning, we make a worst-case assumption regarding the capabilities of the

potential eavesdroppers. In particular, we assume that the potential eavesdroppers have unlimited computational resources and therefore are able to cancel all multiuser interference before decoding the information transmitted to a given legitimate user. Therefore, the channel capacity (bits/s/Hz) between the AP and potential eavesdropper j for decoding the signal of legitimate user k is given by

$$C_{j,k} = \log_2 \det(\mathbf{I}_{N_r} + \mathbf{Q}_j^{-1} \mathbf{H}_j \Phi \mathbf{G} \mathbf{w}_k \mathbf{w}_k^H \mathbf{G}^H \Phi^H \mathbf{H}_j^H), \quad (5)$$

where $\mathbf{Q}_j = \mathbf{H}_j \Phi \mathbf{G} \mathbf{Z} \mathbf{G}^H \Phi^H \mathbf{H}_j^H + \sigma_{e,j}^2 \mathbf{I}_{N_r}$ is the noise covariance matrix at potential eavesdropper j . Hence, the maximum achievable secrecy rate between the AP and legitimate user k is given by

$$R_{s,k} = \left[R_k - \max_{j \in \mathcal{J}} \{C_{j,k}\} \right]^+, \quad (6)$$

and the system sum secrecy rate is given by $R_s = \sum_{k \in \mathcal{K}} R_{s,k}$.

B. Optimization Problem Formulation

In this paper, we adopt a worst-case robust sum-rate maximization (WCR-SRM) problem formulation for norm-bounded CSI uncertainties [38]. In particular, our goal is to maximize the system sum-rate while keeping the maximum information leakage to the eavesdroppers below a desired level². The joint design of the transmit beamformers and AN at the AP and the phase shifts at the IRSs can be formulated as follows

$$\begin{aligned} &\underset{\mathbf{w}_k, \Phi, \mathbf{Z} \in \mathbb{H}^{N_t}}{\text{maximize}} && \sum_{k \in \mathcal{K}} R_k \\ &\text{subject to} && \text{C1: } \sum_{k \in \mathcal{K}} \|\mathbf{w}_k\|^2 + \text{Tr}(\mathbf{Z}) \leq P, \\ &&& \text{C2: } \mathbf{Z} \succeq \mathbf{0}, \quad \text{C3: } \Phi = \text{diag}(\mathbf{v}), \\ &&& \text{C4: } \max_{\Delta \mathbf{H}_j \in \Omega_j} C_{j,k} \leq \tau_{k,j}, \quad \forall k, j. \end{aligned} \quad (7)$$

In constraint C1, P is a nonnegative parameter denoting the maximum transmit power of the AP. Constraint C2 and $\mathbf{Z} \in \mathbb{H}^{N_t}$ are imposed as the covariance matrix of the AN is a Hermitian PSD matrix. Since the IRSs are assumed to be implemented by a total of M passive phase shifters, the equivalent phase shift matrix Φ is constrained to be a diagonal matrix with M unit modulus elements, as specified by constraint C3. The physical layer security of the system is guaranteed by constraint C4 such that the system secrecy rate is bounded from below by $R_s \geq \sum_{k \in \mathcal{K}} \left[R_k - \max_{j \in \mathcal{J}} \{\tau_{k,j}\} \right]^+$.

²Note that the considered WCR-SRM formulation with information leakage constraints offers a higher flexibility for resource allocation than the direct maximization of the secrecy rate with respect to the heterogeneous secrecy requirement of different applications, e.g., video streaming, emails, Internet-of-Things (IoT), etc. In particular, the secrecy performance of each potential eavesdropper can be controlled via the information leakage parameter $\tau_{k,j}$, which allows the system operator to strike a balance between the system sum-rate and the system secrecy rate.

Here, $\tau_{k,j}$ is a predefined parameter which limits the maximum tolerable information leakage to potential eavesdropper j for wiretapping the signal transmitted to legitimate user k .

Remark 3: Unlike existing works on IRS-assisted secure communication focusing on more favorable scenarios, e.g., [1], [21]–[25], in this paper, we consider the case where the potential eavesdroppers are equipped with multiple antennas but the legitimate users have only one antenna. This corresponds to a worst-case assumption where the potential eavesdroppers possess more capabilities than the legitimate users. As a result, the formulated problem (7) is a generalization of the optimization problems considered in existing works. The objective function is not jointly concave with respect to \mathbf{w}_k , Φ , and \mathbf{Z} because Φ is coupled with \mathbf{w}_k and \mathbf{Z} . Constraint C3 is highly non-convex as the phase of each phase shifter is constrained to have unit magnitude. Furthermore, the CSI estimation error is taken into consideration, which leads to infinitely many non-convex constraints in C4, which forms another challenge for solving problem (7). To the best of the authors' knowledge, this is the first work that takes into account CSI uncertainty for the design of IRS-assisted wireless systems. Although there is no general approach to solving problem (7) optimally, in the next section, we shall propose an effective algorithm to find a locally optimal solution for problem (7).

IV. ALGORITHM DESIGN FOR SECURE IRS-ASSISTED WIRELESS COMMUNICATION

In this section, we focus on solving the formulated optimization problem. First, we tackle the coupling of the optimization variables via AO. In fact, AO is a widely applicable and empirically efficient approach for handling optimization problems involving coupled optimization variables. It has been successfully applied to several wireless communication design problems such as hybrid precoding [39], resource allocation [40], and IRS-enabled wireless communication [1]. For the problem at hand, based on the principle of AO, we alternately solve for $\{\mathbf{w}_k, \mathbf{Z}\}$ and Φ while fixing the other variables. This yields a stationary point solution of problem (7) as will be detailed in the following two subsections.

A. Optimization of Transmit Beamforming and AN

We first present the optimization of the beamforming vectors \mathbf{w}_k and AN covariance matrix \mathbf{Z} for a given phase shift matrix Φ . In particular, we first convert the infinitely many constraints in constraint C4 to a finite number of equivalent constraints. To develop efficient algorithms for optimizing \mathbf{w}_k and \mathbf{Z} , SDR and SCA techniques are then leveraged to tackle the non-convexity of both the objective function and constraint C4 of problem (7). Now, for a given phase shift matrix Φ , the optimization problem for the design of \mathbf{w}_k and \mathbf{Z} is given by

$$\begin{aligned} & \underset{\mathbf{w}_k, \mathbf{Z} \in \mathbb{H}^{N_t}}{\text{maximize}} && \sum_{k \in \mathcal{K}} R_k \\ & \text{subject to} && \text{C1: } \sum_{k \in \mathcal{K}} \|\mathbf{w}_k\|^2 + \text{Tr}(\mathbf{Z}) \leq P, \\ & && \text{C2: } \mathbf{Z} \succeq \mathbf{0}, \\ & && \text{C4: } \max_{\Delta \mathbf{H}_j \in \Omega_j} C_{j,k} \leq \tau_{k,j}, \quad \forall k, j. \end{aligned} \quad (8)$$

Constraint C4 is a non-convex constraint involving infinitely many inequality constraints due to the continuity of the CSI uncertainty sets Ω_j . To overcome this difficulty, we first convert the infinite number of constraints in C4 to an equivalent form with only a finite number of constraints by leveraging the following proposition and lemma.

Proposition 1. *Constraint C4 has the following equivalent representation*

$$\begin{aligned} \text{C4} \Leftrightarrow & \max_{\Delta \mathbf{H}_j \in \Omega_j} \mathbf{H}_j \Phi \mathbf{G} [(2^{\tau_{k,j}} - 1) \mathbf{Z} - \mathbf{w}_k \mathbf{w}_k^H] \mathbf{G}^H \Phi^H \mathbf{H}_j^H \\ & + \sigma_{e,j}^2 (2^{\tau_{k,j}} - 1) \mathbf{I}_{N_r} \succeq \mathbf{0}. \end{aligned} \quad (9)$$

Proof: See Appendix A. \blacksquare

While constraint C4 is transformed in Proposition 1 into a more tractable form in terms of linear matrix inequalities (LMIs), there are still an infinite number of such LMIs. To tackle this challenge, we resort to the following lemma to convert constraint C4 into an equivalent form involving a finite number of LMIs.

Lemma 1. *(Generalized S-Procedure [41, Prop. 3.4]) Consider the quadratic matrix inequality (QMI)*

$$\begin{aligned} h(\mathbf{X}) &= \mathbf{X}^H \mathbf{A} \mathbf{X} + \mathbf{X}^H \mathbf{B} + \mathbf{B}^H \mathbf{X} + \mathbf{C} \succeq \mathbf{0}, \\ \forall \mathbf{X} \in \left\{ \mathbf{Y} \mid \text{Tr}(\mathbf{D} \mathbf{Y} \mathbf{Y}^H) \leq 1, \mathbf{D} \succeq \mathbf{0} \right\}, \end{aligned} \quad (10)$$

where $\mathbf{A}, \mathbf{D} \in \mathbb{H}^m$, $\mathbf{X}, \mathbf{B} \in \mathbb{C}^{m \times n}$, and $\mathbf{C} \in \mathbb{H}^n$. This QMI holds if and only if there exist $p \geq 0$ such that

$$\begin{bmatrix} \mathbf{C} & \mathbf{B}^H \\ \mathbf{B} & \mathbf{A} \end{bmatrix} - p \begin{bmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{0} & -\mathbf{D} \end{bmatrix} \succeq \mathbf{0}, \quad (11)$$

provided that there exists a point $\hat{\mathbf{X}}$ such that $h(\hat{\mathbf{X}}) \succeq \mathbf{0}$.

Substituting (3) into (9), we can recast constraint C4 as follows

$$\begin{aligned} & \Delta \mathbf{H}_j \Phi \mathbf{R}_k \Phi^H \Delta \mathbf{H}_j^H + \bar{\mathbf{H}}_j \Phi \mathbf{R}_k \Phi^H \Delta \mathbf{H}_j^H \\ & + \Delta \mathbf{H}_j \Phi \mathbf{R}_k \Phi^H \bar{\mathbf{H}}_j^H + \bar{\mathbf{H}}_j \Phi \mathbf{R}_k \Phi^H \bar{\mathbf{H}}_j^H \\ & + \sigma_{e,j}^2 (2^{\tau_{k,j}} - 1) \mathbf{I}_{N_r} \succeq \mathbf{0}, \\ & \forall \Delta \mathbf{H}_j \in \left\{ \mathbf{Y} \mid \text{Tr}(\epsilon_j^{-2} \mathbf{Y} \mathbf{Y}^H) \leq 1 \right\}, \end{aligned} \quad (12)$$

where $\mathbf{R}_k \triangleq \mathbf{G} [(2^{\tau_{k,j}} - 1) \mathbf{Z} - \mathbf{w}_k \mathbf{w}_k^H] \mathbf{G}^H$. Then, by applying Lemma 1, constraint C4 is further expressed as

$$\text{C4} \Leftrightarrow \bar{\text{C4}}: \mathbf{P}_{k,j} + \mathbf{S}_j \Phi \mathbf{R}_k \Phi^H \mathbf{S}_j^H \succeq \mathbf{0}, \quad \forall k, j, \quad (13)$$

where $\mathbf{S}_j = [\bar{\mathbf{H}}_j^T \quad \mathbf{I}_M]^T$,

$$\mathbf{P}_{k,j} = \begin{bmatrix} [\sigma_{e,j}^2 (2^{\tau_{k,j}} - 1) - p_{k,j}] \mathbf{I}_{N_r} & \mathbf{0} \\ \mathbf{0} & p_{k,j} \epsilon_j^{-2} \mathbf{I}_M \end{bmatrix}, \quad (14)$$

and $p_{k,j} \geq 0, \forall k, j$. The transformed constraint $\bar{\text{C4}}$ involves only KJ LMI constraints, which is more amenable for algorithm design compared to the infinitely many constraints in the original constraint C4. However, the resulting optimization problem is still not jointly convex with respect to $p_{k,j}$, \mathbf{w}_k , and

$$\tilde{R}_k = \log_2 \left(1 + \frac{\text{Tr}(\mathbf{M}_k \mathbf{W}_k)}{\text{Tr}(\mathbf{M}_k \mathbf{Z}) + \sigma_{1,k}^2 + \sum_{i \in \mathcal{K} \setminus \{k\}} \text{Tr}(\mathbf{M}_k \mathbf{W}_i)} \right) \quad (16)$$

$$\begin{aligned} \nabla_{\mathbf{Z}} D_1(\mathbf{W}, \mathbf{Z}) &= -\frac{1}{\ln 2} \sum_{j \in \mathcal{K}} \frac{\mathbf{M}_j}{\text{Tr}(\mathbf{Z} \mathbf{M}_j) + \sigma_{1,j}^2 + \sum_{i \in \mathcal{K} \setminus \{j\}} \text{Tr}(\mathbf{W}_i \mathbf{M}_j)}, \\ \nabla_{\mathbf{W}_k} D_1(\mathbf{W}, \mathbf{Z}) &= -\frac{1}{\ln 2} \sum_{j \neq k} \frac{\mathbf{M}_j}{\text{Tr}(\mathbf{Z} \mathbf{M}_j) + \sigma_{1,j}^2 + \sum_{i \in \mathcal{K} \setminus \{j\}} \text{Tr}(\mathbf{W}_i \mathbf{M}_j)} \end{aligned} \quad (19)$$

\mathbf{Z} . To proceed, we recast the optimization problem as a rank-constrained semidefinite programming (SDP) problem. With $\mathbf{W}_k \triangleq \mathbf{w}_k \mathbf{w}_k^H$ problem (8) can be rewritten as

$$\begin{aligned} &\underset{p_{k,j} \geq 0, \mathbf{W}_k, \mathbf{Z} \in \mathbb{H}^{N_t}}{\text{minimize}} && - \sum_{k \in \mathcal{K}} \tilde{R}_k \\ &\text{subject to} && \text{C1: } \sum_{k \in \mathcal{K}} \text{Tr}(\mathbf{W}_k) + \text{Tr}(\mathbf{Z}) \leq P, \\ & && \text{C2: } \mathbf{Z} \succeq \mathbf{0}, \quad \text{C5: } \mathbf{W}_k \succeq \mathbf{0}, \quad (15) \\ & && \overline{\text{C4:}} \mathbf{S}_j \Phi \mathbf{R}_k \Phi^H \mathbf{S}_j^H + \mathbf{P}_{k,j} \succeq \mathbf{0}, \quad \forall k, j, \\ & && \text{C6: Rank}(\mathbf{W}_k) \leq 1, \quad \forall k, \end{aligned}$$

where \tilde{R}_k is shown in (16) on the top of this page and $\mathbf{M}_k = \mathbf{G}^H \Phi^H \mathbf{h}_k \mathbf{h}_k^H \Phi \mathbf{G}$. The constraints $\mathbf{W}_k \succeq \mathbf{0}$, $\mathbf{W}_k \in \mathbb{H}^{N_t}$, and $\text{Rank}(\mathbf{W}_k) \leq 1$ are imposed to guarantee that $\mathbf{W}_k = \mathbf{w}_k \mathbf{w}_k^H$ still holds after optimizing \mathbf{W}_k . All constraints of problem (15) are convex except for constraint C6. Next, we tackle the non-convexity of the objective function in problem (15). To enable efficient algorithm design, we first rewrite the objective function in form of d.c. functions, i.e., $-\sum_{k \in \mathcal{K}} \tilde{R}_k = N_1 - D_1$, where

$$\begin{aligned} N_1 &= - \sum_{k \in \mathcal{K}} \log_2 \left(\text{Tr}(\mathbf{Z} \mathbf{M}_k) + \sigma_{1,k}^2 + \sum_{i \in \mathcal{K}} \text{Tr}(\mathbf{W}_i \mathbf{M}_k) \right), \\ D_1 &= - \sum_{k \in \mathcal{K}} \log_2 \left(\text{Tr}(\mathbf{Z} \mathbf{M}_k) + \sigma_{1,k}^2 + \sum_{i \in \mathcal{K} \setminus \{k\}} \text{Tr}(\mathbf{W}_i \mathbf{M}_k) \right) \end{aligned} \quad (17)$$

are two functions that are both jointly convex in terms of $p_{k,j}$, \mathbf{W}_k , and \mathbf{Z} . Now, we adopt the SCA method to obtain a convex upper bound for the objective function in an iterative manner. To facilitate SCA, we construct a global underestimator for function D_1 , where we use superscript (t) to denote the iteration index of the optimization variables. In particular, for any feasible point $\mathbf{W}^{(t)} \triangleq \{\mathbf{W}_k^{(t)}\}_{k=1}^K$ and $\mathbf{Z}^{(t)}$, a lower bound of function D_1 is given by its first-order Taylor approximation, which can be expressed as

$$\begin{aligned} &D_1(\mathbf{W}, \mathbf{Z}) \\ &\geq D_1(\mathbf{W}^{(t)}, \mathbf{Z}^{(t)}) + \text{Tr} \left(\nabla_{\mathbf{Z}}^H D_1(\mathbf{W}^{(t)}, \mathbf{Z}^{(t)}) (\mathbf{Z} - \mathbf{Z}^{(t)}) \right) \\ &+ \sum_{k \in \mathcal{K}} \text{Tr} \left(\nabla_{\mathbf{W}_k}^H D_1(\mathbf{W}^{(t)}, \mathbf{Z}^{(t)}) (\mathbf{W}_k - \mathbf{W}_k^{(t)}) \right), \end{aligned} \quad (18)$$

where the gradients of function D_1 with respect to \mathbf{Z} and \mathbf{W}_k are given in (19) on the top of this page. By employing this upper bound on the objective function, the only remaining

non-convexity of problem (15) is due to rank constraint C6. Generally, solving such a rank-constrained problem is known to be NP-hard [42]. To overcome this issue, we adopt the SDR technique and drop the rank constraint C6. Therefore, the resulting problem that needs to be solved at feasible point $\mathbf{W}^{(t)}$ and $\mathbf{Z}^{(t)}$ is given by

$$\begin{aligned} &\underset{p_{k,j} \geq 0, \mathbf{W}_k, \mathbf{Z} \in \mathbb{H}^{N_t}}{\text{minimize}} && N_1 - \text{Tr} \left(\nabla_{\mathbf{Z}}^H D_1(\mathbf{W}^{(t)}, \mathbf{Z}^{(t)}) \mathbf{Z} \right) \\ & && - \sum_{k \in \mathcal{K}} \text{Tr} \left(\nabla_{\mathbf{W}_k}^H D_1(\mathbf{W}^{(t)}, \mathbf{Z}^{(t)}) \mathbf{W}_k \right) \\ &\text{subject to} && \text{C1: } \sum_{k \in \mathcal{K}} \text{Tr}(\mathbf{W}_k) + \text{Tr}(\mathbf{Z}) \leq P, \quad (20) \\ & && \text{C2: } \mathbf{Z} \succeq \mathbf{0}, \quad \text{C5: } \mathbf{W}_k \succeq \mathbf{0}, \quad \forall k, \\ & && \overline{\text{C4:}} \mathbf{P}_{k,j} + \mathbf{S}_j \Phi \mathbf{R}_k \Phi^H \mathbf{S}_j^H \succeq \mathbf{0}, \quad \forall k, j. \end{aligned}$$

This relaxed problem is jointly convex with respect to $p_{k,j}$, \mathbf{W}_k , and \mathbf{Z} , and hence can be efficiently solved by standard convex program solvers such as CVX [43]. However, in general, there is no guarantee that the solution obtained by SDR satisfies the rank constraint. Nevertheless, we prove the tightness of the SDR method for problem (20) in the following theorem.

Theorem 1. *Suppose the optimal solution of problem (20) is denoted as $\{\mathbf{W}_k^*, \mathbf{Z}^*, p_{k,j}^*\}$, where $\text{Rank}(\mathbf{W}_k^*) > 1$. Then, there always exists another optimal solution of problem (20), denoted as $\{\tilde{\mathbf{W}}_k^*, \tilde{\mathbf{Z}}^*, \tilde{p}_{k,j}^*\}$, which not only achieves the same objective value as $\{\mathbf{W}_k^*, \mathbf{Z}^*, p_{k,j}^*\}$, but also meets the rank constraint, i.e., $\text{Rank}(\tilde{\mathbf{W}}_k^*) \leq 1$.*

Proof: See Appendix B for the proof of Theorem 1. The construction of the optimal rank-one solution is given in (44). ■

Theorem 1 indicates that we can always obtain or construct a rank-constrained optimal solution for problem (20). In addition, according to Theorem 1, the optimal beamforming vector \mathbf{w}_k^* can always be recovered from $\tilde{\mathbf{W}}_k^*$ given in (44) by performing Cholesky decomposition, i.e., $\tilde{\mathbf{W}}_k^* = \mathbf{w}_k^* (\mathbf{w}_k^*)^H$.

B. Optimization of Phase Shifts at IRSs

Next, we present the optimization of phase shift matrix Φ for given transmit beamforming vectors \mathbf{w}_k and AN co-

$$\hat{R}_k = \log_2 \left(1 + \frac{\text{Tr}(\mathbf{L}_k \mathbf{W}_k \mathbf{L}_k^H \mathbf{V}^T)}{\text{Tr}(\mathbf{L}_k \mathbf{Z} \mathbf{L}_k^H \mathbf{V}^T) + \sigma_{1,k}^2 + \sum_{i \in \mathcal{K} \setminus \{k\}} \text{Tr}(\mathbf{L}_k \mathbf{W}_i \mathbf{L}_k^H \mathbf{V}^T)} \right) \quad (24)$$

variance matrix \mathbf{Z} . By applying Lemma 1, the optimization problem for the IRSs is given by

$$\begin{aligned} & \underset{p_{k,j} \geq 0, \Phi}{\text{minimize}} && - \sum_{k \in \mathcal{K}} R_k \\ & \text{subject to} && \text{C3: } \Phi = \text{diag}(\mathbf{v}), \\ & && \overline{\text{C4:}} \mathbf{P}_{k,j} + \mathbf{S}_j \Phi \mathbf{R}_k \Phi^H \mathbf{S}_j^H \succeq \mathbf{0}, \quad \forall k, j. \end{aligned} \quad (21)$$

The main difficulty in solving problem (21) is the unit modulus constraint C3 on the main diagonal elements of Φ . To the best of the authors' knowledge, there is no general approach to solve unit modulus constrained non-convex optimization problems optimally. In this paper, we propose to rewrite problem (21) by adopting $\mathbf{v} = \text{Diag}(\Phi)$ as the optimization variable instead of Φ itself, which paves the way for leveraging SDP and SCA methods to facilitate the design of an efficient algorithm for secure IRS-assisted systems. To start with, we first take constraint $\overline{\text{C4}}$ as an example to illustrate the proposed reformulation. By performing the singular value decomposition (SVD) of $\mathbf{R}_k = \sum_i \mathbf{p}_{k,i} \mathbf{q}_{k,i}^H$, we have

$$\begin{aligned} \mathbf{S}_j \Phi \mathbf{R}_k \Phi^H \mathbf{S}_j^H &= \sum_i \mathbf{S}_j \Phi \mathbf{p}_{k,i} \mathbf{q}_{k,i}^H \Phi^H \mathbf{S}_j^H \\ &= \sum_i \mathbf{S}_j \text{diag}(\mathbf{p}_{k,i}) \mathbf{v} \mathbf{v}^H \text{diag}(\mathbf{q}_{k,i}^H) \mathbf{S}_j^H. \end{aligned} \quad (22)$$

Then, the objective function can be rewritten as a function of \mathbf{v} in a similar manner as (22). To facilitate SDP, we define $\mathbf{V} \triangleq \mathbf{v} \mathbf{v}^H$, and therefore problem (21) can be recast as

$$\begin{aligned} & \underset{p_{k,j} \geq 0, \mathbf{V} \in \mathbb{H}^M}{\text{minimize}} && - \sum_{k \in \mathcal{K}} \hat{R}_k \\ & \text{subject to} && \overline{\text{C4:}} \mathbf{P}_{k,j} + \sum_i \mathbf{S}_j \text{diag}(\mathbf{p}_{k,i}) \mathbf{V} \\ & && \quad \times \text{diag}(\mathbf{q}_{k,i}^H) \mathbf{S}_j^H \succeq \mathbf{0}, \quad \forall k, j, \\ & && \text{C7: } \text{Diag}(\mathbf{V}) = \mathbf{1}_M, \quad \text{C8: } \mathbf{V} \succeq \mathbf{0}, \\ & && \text{C9: } \text{Rank}(\mathbf{V}) = 1, \end{aligned} \quad (23)$$

where \hat{R}_k is given in (24) on the top of this page and $\mathbf{L}_k = \text{diag}(\mathbf{h}_k^H) \mathbf{G}$. Constraints $\mathbf{V} \in \mathbb{H}^M$, C8, and C9 are imposed to guarantee that $\mathbf{V} = \mathbf{v} \mathbf{v}^H$ holds after optimization. More importantly, constraint C7 is introduced to guarantee the unit modulus constraint when recovering \mathbf{v} from \mathbf{V} .

Recall that for the optimization of \mathbf{W}_k and \mathbf{Z} , we have temporarily removed the rank constraint on \mathbf{W}_k and proved the tightness of the SDR method. However, due to the presence of constraint C7 induced by the unit modulus constraint, the rank of the solution obtained from problem (23) is generally larger than one [42]. As a result, instead of applying the SDR method adopted in Section IV-A, we handle the rank-one constraint via a different approach. In particular, we first rewrite the rank-one constraint C9 in an equivalent form:

$$\text{C9} \Leftrightarrow \overline{\text{C9:}} \|\mathbf{V}\|_* - \|\mathbf{V}\|_2 \leq 0. \quad (25)$$

Note that for any $\mathbf{X} \in \mathbb{H}^m$, the inequality $\|\mathbf{X}\|_* = \sum_i \sigma_i \geq \|\mathbf{X}\|_2 = \max_i \{\sigma_i\}$ holds, where σ_i is the i -th singular value of \mathbf{X} . Equality holds if and only if \mathbf{X} has unit rank. Constraint $\overline{\text{C9}}$ ensures this equality, which is equivalent to enforcing constraint C9.

Constraint $\overline{\text{C9}}$ is in a d.c. form and therefore still non-convex with respect to \mathbf{V} . To overcome the non-convexity, we apply a penalty-based method as in [44, Ch. 17], [45] by moving constraint $\overline{\text{C9}}$ into the objective function, which results in the following optimization problem

$$\begin{aligned} & \underset{p_{k,j} \geq 0, \mathbf{V} \in \mathbb{H}^M}{\text{minimize}} && N_2 - D_2 + \frac{1}{2\rho} (\|\mathbf{V}\|_* - \|\mathbf{V}\|_2) \\ & \text{subject to} && \overline{\text{C4:}} \mathbf{P}_{k,j} + \sum_i \mathbf{S}_j \text{diag}(\mathbf{p}_{k,i}) \mathbf{V} \\ & && \quad \times \text{diag}(\mathbf{q}_{k,i}^H) \mathbf{S}_j^H \succeq \mathbf{0}, \quad \forall k, j, \\ & && \text{C7: } \text{Diag}(\mathbf{V}) = \mathbf{1}_M, \quad \text{C8: } \mathbf{V} \succeq \mathbf{0}, \end{aligned} \quad (26)$$

where

$$\begin{aligned} N_2 &= - \sum_{k \in \mathcal{K}} \log_2 \left(\text{Tr}(\mathbf{L}_k \mathbf{Z} \mathbf{L}_k^H \mathbf{V}^T) + \sigma_{1,k}^2 \right. \\ & \quad \left. + \sum_{i \in \mathcal{K}} \text{Tr}(\mathbf{L}_k \mathbf{W}_i \mathbf{L}_k^H \mathbf{V}^T) \right), \\ D_2 &= - \sum_{k \in \mathcal{K}} \log_2 \left(\text{Tr}(\mathbf{L}_k \mathbf{Z} \mathbf{L}_k^H \mathbf{V}^T) + \sigma_{1,k}^2 \right. \\ & \quad \left. + \sum_{i \in \mathcal{K} \setminus \{k\}} \text{Tr}(\mathbf{L}_k \mathbf{W}_i \mathbf{L}_k^H \mathbf{V}^T) \right), \end{aligned} \quad (27)$$

and $\rho > 0$ is a penalty factor penalizing the violation of constraint $\overline{\text{C9}}$, and the following proposition states the equivalence of problems (23) and (26).

Proposition 2. *Let \mathbf{V}_s be the optimal solution of problem (26) for penalty factor ρ_s . When ρ_s is sufficiently small, i.e., for $\rho_s \rightarrow 0$, then any limit point $\bar{\mathbf{V}}$ of the sequence $\{\mathbf{V}_s\}$ is an optimal solution of problem (23).*

Proof: See Appendix C. ■

Proposition 2 implies that we can obtain a rank-one solution $\bar{\mathbf{V}}$ by solving problem (26) for a sufficiently small value of penalty factor ρ . In other words, the diagonal elements of the phase shift matrix Φ , i.e., \mathbf{v} , can always be recovered from the rank-one solution $\bar{\mathbf{V}}$ by performing Cholesky decomposition of $\bar{\mathbf{V}} = \mathbf{v} \mathbf{v}^H$. Since after the proposed series of transformations, the constraints in problem (26) form a convex set, we may adopt a similar approach as in Section IV-A to tackle the d.c. objective function and employ SCA. In particular, for any feasible point $\mathbf{V}^{(t)}$, a lower bound for $\tilde{D}_2 = D_2 + \frac{1}{2\rho} \|\mathbf{V}\|_2$ is obtained as

$$\tilde{D}_2(\mathbf{V}) \geq \tilde{D}_2(\mathbf{V}^{(t)}) + \text{Tr} \left(\nabla_{\mathbf{V}}^H \tilde{D}_2(\mathbf{V}^{(t)}) (\mathbf{V} - \mathbf{V}^{(t)}) \right), \quad (28)$$

$$\nabla_{\mathbf{V}} \tilde{D}_2 = \frac{1}{2\rho} \lambda_{\max}(\mathbf{V}) \lambda_{\max}^H(\mathbf{V}) - \frac{1}{\ln 2} \sum_{k \in \mathcal{K}} \frac{\mathbf{L}_k^* \left(\mathbf{Z}^T + \sum_{i \in \mathcal{K} \setminus \{k\}} \mathbf{W}_i^T \right) \mathbf{L}_k^T}{\text{Tr}(\mathbf{L}_k \mathbf{Z} \mathbf{L}_k^H \mathbf{V}^T) + \sigma_{1,k}^2 + \sum_{i \in \mathcal{K} \setminus \{k\}} \text{Tr}(\mathbf{L}_k \mathbf{W}_i \mathbf{L}_k^H \mathbf{V}^T)} \quad (29)$$

Algorithm 1 Alternating Optimization Algorithm

- 1: Randomly construct the initial points $\mathbf{w}_k^{(0)}$ and $\mathbf{Z}^{(0)}$. Initialize $\Phi^{(0)}$ with random phases. Set convergence tolerance ε and iteration index $t = 0$;
 - 2: **repeat**
 - 3: Find $\mathbf{W}_k^{(t+1)}$ and $\mathbf{Z}^{(t+1)}$ by solving problem (20) for the given $\Phi = \Phi^{(t)}$;
 - 4: Set $\mathbf{V}^{(t)} = \text{Diag}(\Phi^{(t)}) \text{Diag}(\Phi^{(t)})^H$;
 - 5: Solve problem (30) for given $\mathbf{W}_k = \mathbf{W}_k^{(t+1)}$ and $\mathbf{Z} = \mathbf{Z}^{(t+1)}$, and update $\mathbf{V}^{(t+1)}$;
 - 6: Decompose $\mathbf{V}^{(t+1)} = \mathbf{v}^{(t+1)} (\mathbf{v}^{(t+1)})^H$ and update $\Phi^{(t+1)} = \text{diag}(\mathbf{v}^{(t+1)})$;
 - 7: $t \leftarrow t + 1$;
 - 8: **until** $\frac{\sum_{k \in \mathcal{K}} (R_k^{(t)} - R_k^{(t-1)})}{\sum_{k \in \mathcal{K}} R_k^{(t-1)}} \leq \varepsilon$
-

where $\nabla_{\mathbf{V}} \tilde{D}_2$ is given in (29) on the top of this page. Therefore, the optimization problem to be solved for a given feasible point $\mathbf{V}^{(t)}$ becomes

$$\begin{aligned} & \underset{p_{k,j} \geq 0, \mathbf{V} \in \mathbb{H}^M}{\text{minimize}} && \frac{1}{2\rho} \|\mathbf{V}\|_* + N_2 - \text{Tr} \left(\nabla_{\mathbf{V}}^H \tilde{D}_2 \left(\mathbf{V}^{(t)} \right) \mathbf{V} \right) \\ & \text{subject to} && \text{C4: } \mathbf{P}_{k,j} + \sum_i \mathbf{S}_j \text{diag}(\mathbf{p}_{k,i}) \mathbf{V} \\ & && \quad \times \text{diag}(\mathbf{q}_{k,i}^H) \mathbf{S}_j^H \succeq \mathbf{0}, \quad \forall k, j, \quad (30) \\ & && \text{C7: } \text{Diag}(\mathbf{V}) = \mathbf{1}_M, \quad \text{C8: } \mathbf{V} \succeq \mathbf{0}. \end{aligned}$$

This optimization problem is jointly convex with respect to $p_{k,j}$ and \mathbf{V} , and hence it can be efficiently solved by standard convex program solvers such as CVX [43].

The overall AO algorithm proposed in this section is summarized in **Algorithm 1**. Note that the minimum values of problems (20) and (30) serve as upper bounds for the optimal values of problems (15) and (26), respectively. By iteratively solving problems (20) and (30) optimally in Steps 3 and 5 in **Algorithm 1**, we can monotonically tighten these upper bounds. In this way, the objective values achieved by the sequence $\{\mathbf{w}^{(t)}, \mathbf{Z}^{(t)}, \Phi^{(t)}\}_{t \in \mathbb{N}}$ form a non-increasing sequence that converges to a stationary value in polynomial time, and any limit point of the sequence $\{\mathbf{w}^{(t)}, \mathbf{Z}^{(t)}, \Phi^{(t)}\}_{t \in \mathbb{N}}$ is a stationary point of problem (7) [46]. Furthermore, the computational complexity of each iteration of the proposed AO algorithm is given by $\mathcal{O} \left(\log \frac{1}{\varepsilon} \left((\sqrt{N_t} + \sqrt{M}) K^3 J^3 + (N_t^{\frac{3}{2}} + M^{\frac{3}{2}}) K^2 J^2 \right) \right)$, where $\mathcal{O}(\cdot)$ is the big-O notation³.

³According to [47, Th. 3.12], the computational complexity of an SDP problem with m SDP constraints, where each constraint involves an $n \times n$ PSD matrix, is given by $\mathcal{O}(\sqrt{n} \log \frac{1}{\varepsilon} (mn^3 + m^2n^2 + m^3))$. For problems (20) and (30), we have $m = KJ + 1$, $n = N_t$ and $m = KJ + 1$, $n = M$, respectively.

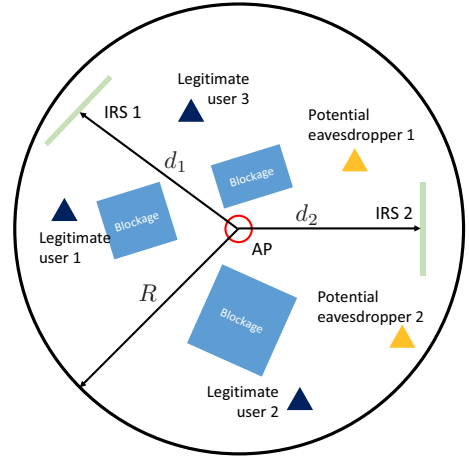


Fig. 2. Simulation setup for an IRS-assisted multiuser MISO secure communication system, which consists of $K = 3$ legitimate users, $J = 2$ potential eavesdroppers, and $L = 2$ IRSs.

TABLE I
SYSTEM PARAMETERS

Carrier center frequency	2.4 GHz
Path loss exponents for channels with and without LoS components, α_l	2 and 4
Ricean factors for channels with and without LoS components, β_l	5 and 0
Noise power at the legitimate users and potential eavesdroppers, $\sigma_{1,k}^2$ and $\sigma_{e,j}^2$	-90 dBm
Cell radius, R	200 m
Penalty factor, ρ	5×10^{-4}
Convergence tolerance, ε	10^{-3}

V. SIMULATION RESULTS

A. Simulation Setup

The schematic system model for the simulated single-cell network is shown in Fig. 2. The AP is located at the center of the cell with radius R . The legitimate users and potential eavesdroppers are randomly and uniformly distributed in the cell. Since our motivation for deploying IRSs in secure wireless systems is to establish favorable communication links for legitimate users that would otherwise be blocked, we consider a scenario where L IRSs are deployed to improve the secrecy performance of K legitimate users whose direct links to the AP are blocked by obstacles. Each potential eavesdropper is equipped with $N_r = 2$ antennas unless specified otherwise. The channel matrix \mathbf{G}_l between the AP and IRS l is modeled as follows

$$\mathbf{G}_l = \sqrt{L_0 d_l^{-\alpha_l}} \left(\sqrt{\frac{\beta_l}{1 + \beta_l}} \mathbf{G}_l^L + \sqrt{\frac{1}{1 + \beta_l}} \mathbf{G}_l^N \right), \quad (31)$$

where $L_0 = \left(\frac{\lambda_c}{4\pi}\right)^2$ is a constant with λ_c being the wavelength of the center frequency of the information carrier. The distance

between the AP and IRS l is denoted by d_l while α_l is the corresponding path loss exponent. The small-scale fading is assumed to be Ricean fading with Ricean factor β_l . The line-of-sight (LoS) and non-LoS components are represented by \mathbf{G}_l^L and \mathbf{G}_l^N , which are modeled as the product of the array response vectors of the transceivers and Rayleigh fading, respectively. The other channels in the system are generated in a similar manner as we expect that legitimate users with LoS links to the IRSs are served and the potential eavesdroppers may also position themselves in the LoS of the IRSs. To facilitate the presentation, we define the maximum normalized estimation error of the eavesdropping channels as $\kappa_j = \epsilon_j / \|\tilde{\mathbf{H}}_j\|_F, \forall j$. The system parameters used for our simulations are listed in Table I.

B. Baseline Schemes

We adopt two baseline schemes for comparison. For baseline 1, we adopt simple design choices without performing iterative optimization. In particular, we adopt maximum ratio transmission (MRT) for transmit beamforming, apply an isotropic radiation pattern for AN injection, and implement the IRSs with random phases. As for MRT, we set $\mathbf{w}_k = \sqrt{\varrho_k} \frac{\mathbf{G}^H \Phi^H \mathbf{h}_k}{\|\mathbf{G}^H \Phi^H \mathbf{h}_k\|}$, where ϱ_k is the power allocated to legitimate user k , which is optimized together with the power allocated to the AN to satisfy the total transmit power and secrecy constraints as stated in (7). For baseline 2, we evaluate the system performance when IRSs are not deployed⁴. In this case, the legitimate users are blocked by infrastructures, and therefore the channels between the AP and the legitimate users are assumed to be non-LoS. As the potential eavesdroppers can move freely in the network, the channels between the AP and the eavesdroppers are assumed to be still LoS-dominated, which is an unfavorable scenario for secure communication. In baseline 2, we optimize the beamforming vectors and AN covariance matrix at the AP by setting $\Phi = \mathbf{I}_{N_t}$ and solving problem (8).

In the following, we investigate the impact of the different system parameters by focusing on the case of one IRS in Sections V-C to V-H while multi-IRS systems are studied in Section V-I.

C. Convergence of the Proposed Algorithm

In Fig. 3, we investigate the convergence of the proposed algorithm for different numbers of antenna elements, N_t , IRS reflecting elements, M , and legitimate users, K . As can be observed from Fig. 3, the proposed algorithm monotonically converges for all considered values of N_t , M , and K . In particular, for $N_t = M = 5$, $N_r = 2$, $K = 3$, $J = 2$, the proposed algorithm converges after around 15 iterations on average. For the case with more antennas and IRS reflecting elements, i.e., $N_t = M = 10$, $N_r = 3$, $K = 3$, $J = 2$, the

⁴If IRSs are not used, the information carrying beams emitted by the AP are typically down tilted and energy is beamformed towards the ground to reach the legitimate users, and therefore, different from the scenario described in Remark 2, the signals received at the legitimate users and eavesdroppers via the direct links are not negligible. Therefore, the direct links have to be taken into consideration for baseline 2.

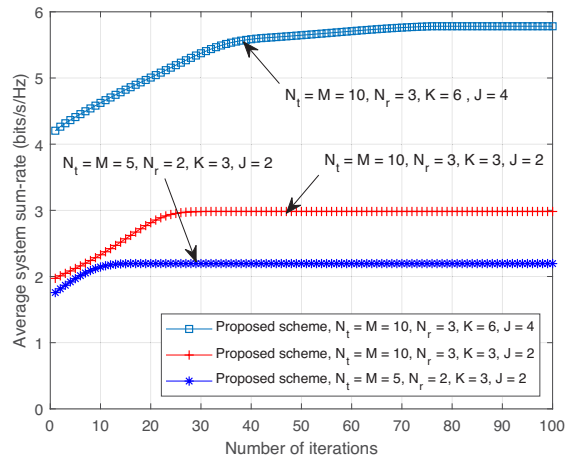


Fig. 3. Convergence of the proposed algorithm for different values of N_t , N_r , M , K , and J . The system parameters are set as $P = 30$ dBm, $d_1 = 60$ m, $\kappa_j^2 = 0.1$, and $\tau_{k,j} = 1$ bit/s/Hz.

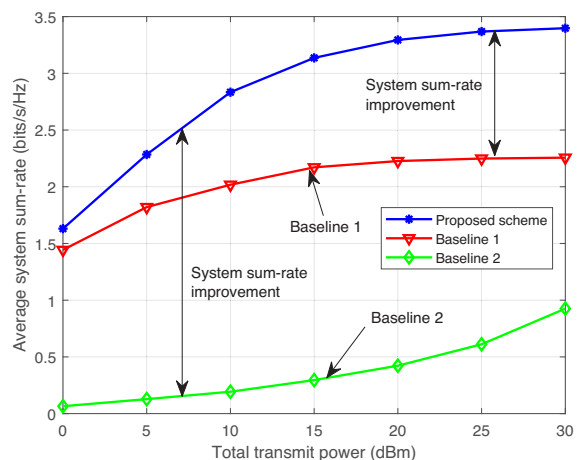


Fig. 4. Average system sum-rate (bits/s/Hz) versus the total transmit power of the AP (dBm) for $N_t = M = 6$, $N_r = 3$, $K = 4$, $J = 2$, $d_1 = 115$ m, $\kappa_j^2 = 0.1$, and $\tau_{k,j} = 1$ bit/s/Hz. The double sided arrows indicate the performance gain achieved by the proposed scheme over the baseline schemes.

proposed algorithm needs additional 15 iterations on average to converge since the dimensions of the solution space of problems (20) and (30) scale with N_t , N_r , and M . For the case with more legitimate users and potential eavesdroppers, i.e., $N_t = M = 10$, $N_r = 3$, $K = 6$, $J = 4$, the proposed algorithm needs considerably more iterations to converge since the numbers of optimization variables and constraints in problems (20) and (30) both increase with the numbers of legitimate users K and potential eavesdroppers J . In summary, the number of iterations required for the proposed algorithm to converge is less sensitive to the numbers of antennas and IRS reflecting elements than to the numbers of legitimate users and potential eavesdroppers.

D. Average System Sum Rate Versus the Maximum Transmit Power

In Fig. 4, we show the average system sum-rate versus the maximum total transmit power at the AP, P , while limiting the information leakage to the potential eavesdroppers to $\tau_{k,j} = 1$

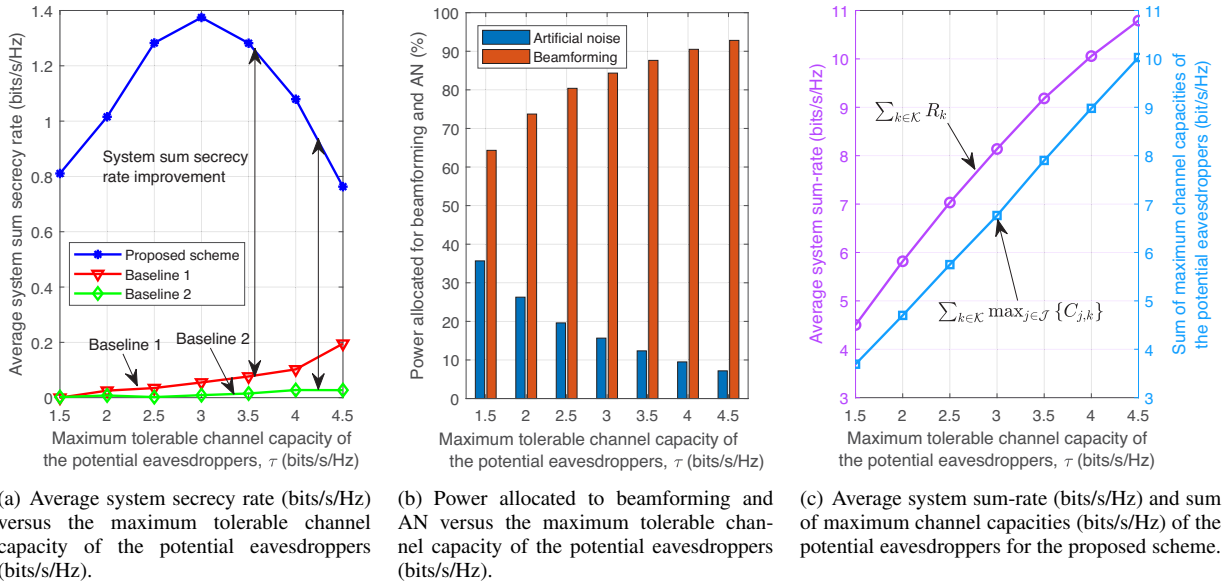


Fig. 5. The system parameters are set as $N_t = M = 6$, $K = 3$, $J = 2$, $d_1 = 50$ m, $\kappa_j^2 = 0.1$, and $P = 10$ dBm.

bit/s/Hz, $\forall k, j$. As can be observed from Fig. 4, the system sum-rate increases monotonically with the maximum transmit power budget. This is because by applying the proposed optimization framework, the signal-to-interference-plus-noise ratios (SINRs) of the legitimate users can be improved by providing them with additional transmit power, which leads to an improvement of the system sum-rate. Fig. 4 also shows that the average system sum-rate of the proposed scheme exceeds that of both considered baseline schemes by a considerable margin. In particular, for baseline 1, the fixed MRT beamforming is unable to fully exploit the extra degrees of freedom (DoFs) introduced by the additional transmit power. In fact, the MRT strategy in baseline 1 is unable to mitigate multiuser interference resulting in performance saturation in the high transmit power regime. For baseline 2, the performance loss compared to the proposed scheme is mainly due to the huge path loss of the AP-legitimate user links as the legitimate users are assumed to be heavily attenuated. Fig. 4 reveals the huge performance gains enabled by deploying an IRS to establish an LoS propagation environment for the legitimate users.

E. Secrecy Rate Versus the Maximum Tolerable Channel Capacity of the Eavesdroppers

Fig. 5(a) depicts the average secrecy rate defined in (6) versus the maximum tolerable channel capacity of the potential eavesdroppers, $\tau_{k,j}$. We assume that the maximum tolerable capacity of all eavesdroppers are identical, i.e., $\tau_{k,j} = \tau$, $\forall k, j$. As can be observed, the system secrecy rate is almost zero if the IRS is not available (baseline 2), which is mainly due to the poor channel conditions between the AP and the legitimate users. In other words, for blocked legitimate users, secure wireless communication cannot be guaranteed without the favorable propagation environment created by the IRS. Furthermore, the average secrecy rate achieved by the proposed scheme is significantly higher than that of baseline 1, which confirms the effectiveness of the proposed algorithm.

As shown in Fig. 5(b), when τ is small, a large portion of the transmit power is allocated to transmitting AN to deteriorate the achievable rates of the potential eavesdroppers, and therefore, there is less power left for information beamforming to maximize the system sum-rate. As τ increases, the constraints on the performance of the eavesdroppers are relaxed, and hence, more transmit power is allocated to beamforming and to improving the system sum-rate, as can be observed in Figs. 5(b) and 5(c). Recall that the secrecy rate is given by $R_s = \sum_{k \in \mathcal{K}} \left[R_k - \max_{j \in \mathcal{J}} \{C_{j,k}\} \right]^+$. For large τ , the maximum channel capacity of the potential eavesdroppers $\sum_{k \in \mathcal{K}} \max_{j \in \mathcal{J}} \{C_{j,k}\}$ grows faster than the system sum-rate $\sum_{k \in \mathcal{K}} R_k$, as can be observed in Fig. 5(c). Therefore, the secrecy rate decreases for large τ , see also Fig. 5(a). Hence, if system sum secrecy rate maximization is desired, τ has to be carefully chosen. We note that the maximum secrecy rate can be found by solving the considered problem for different values of τ .

F. Energy Efficiency Evaluation

IRSs are advocated as energy-efficient devices for assisting wireless communication. In Fig. 6, we investigate the energy efficiency versus the number of antenna elements at the AP and the number of reflecting elements at the IRS. We adopt a linear power consumption model, and the energy efficiency (bits/J/Hz) is defined as the ratio of the system sum-rate to the total power consumption of the system [48]

$$\eta_{EE} = \frac{\sum_{k \in \mathcal{K}} R_k}{\frac{1}{\mu} P + N_t P_t + P_o + P_l}, \quad (32)$$

where μ is the power amplifier efficiency, and P_t accounts for the circuit power consumption introduced by deploying one antenna element, which is mainly caused by the power consumed by the corresponding RF chain. P_o is the static

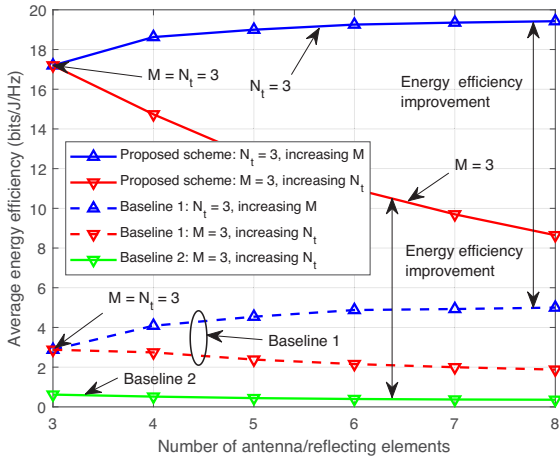


Fig. 6. Average system energy efficiency (bits/J/Hz) versus the number of antennas, N_t , or reflecting elements, M , for $K = 3$, $J = 2$, $d_1 = 50$ m, $\kappa_j^2 = 0.1$, $\tau_{k,j} = 1$ bit/s/Hz, and $P = 5$ dBm.

circuit power of the AP, consumed by the cooling system, power supply, etc., and P_1 is the power consumption of the IRS controller. Following [48], we set $\mu = 0.32$, $P_t = 35$ mW, $P_1 = 20$ mW, and $P_o = 34$ mW. In Fig. 6, we show the average energy efficiency as a function of the number of reflecting elements at the IRS for $N_t = 3$ antennas (black curves) and as a function of the number of transmit antennas for $M = 3$ IRS reflecting elements (red curves). As can be observed from Fig. 6, increasing the number of IRS elements leads to an improvement of the energy efficiency. The reason behind this is twofold. On the one hand, as they are passive devices, enlarging the IRS size causes little additional power consumption. On the other hand, additional phase shifters can reflect more of the power received from the AP, which leads to a power gain, and provide more flexibility for resource allocation, which improves the beamforming gain for the links from the IRS to the legitimate users. In contrast, the energy efficiency is a monotone decreasing function with respect to the number of antennas at the AP. This is mainly because more power-hungry RF chains are required as the number of antennas increases, which outweighs the system sum-rate gain introduced by deploying more antennas. Fig. 6 clearly demonstrates the superiority of IRS-assisted secure communication systems compared to conventional multi-antenna secure wireless systems in terms of energy efficiency.

G. Average System Sum-Rate Versus the Number of Legitimate Users

Fig. 7 shows the average system sum-rate versus the number of legitimate users, K . As can be observed, the system sum-rates achieved by the proposed scheme and both baseline schemes monotonically increase with the number of legitimate users. This is due to the fact that both the proposed scheme and the two baseline schemes are able to exploit multiuser diversity. However, the system sum-rate and its growth rate are substantially lower for the baseline schemes compared to the proposed scheme. In particular, the MRT strategy adopted in baseline 1 fails to mitigate multiuser interference, which

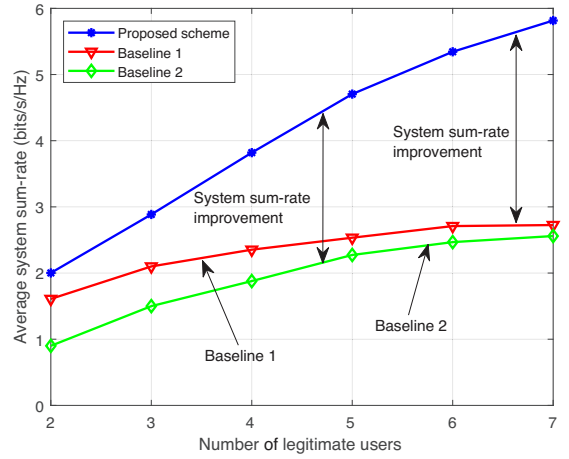
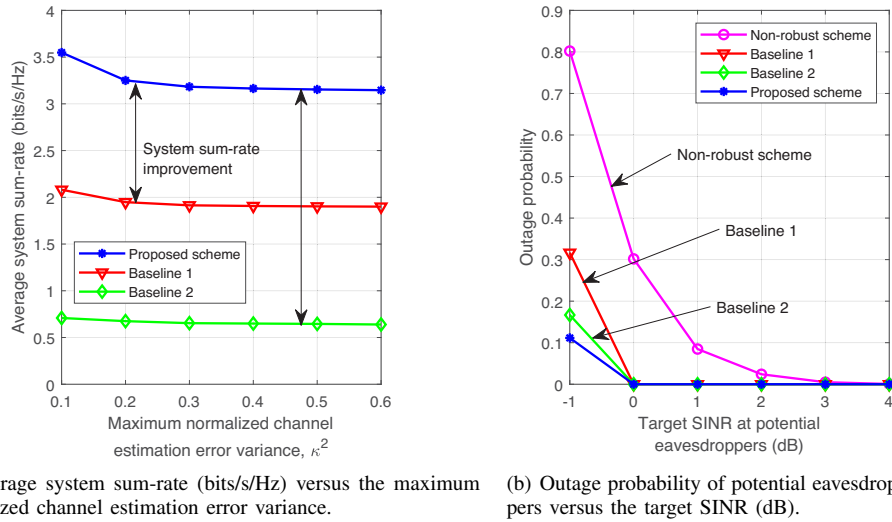


Fig. 7. Average system sum-rate (bits/s/Hz) versus the number of legitimate users, K , for $N_t = M = 10$, $J = 2$, $d_1 = 50$ m, $P = 25$ dBm, $\kappa_j^2 = 0.1$, and $\tau_{k,j} = 1$ bit/s/Hz.

quickly leads to a saturation of the performance. On the other hand, without the LoS links created by the IRS for the legitimate users, baseline 2 achieves the lowest system sum-rate among the three considered schemes. These observations underline the superiority of IRS-assisted secure multiuser systems and the proposed algorithm.

H. CSI Uncertainty

Fig. 8(a) shows the average system sum-rate versus the normalized maximum channel estimation error variance. We assume that all eavesdropping channels have the same maximum normalized estimation error variance, i.e., $\kappa_j = \kappa$, $\forall j$. As can be observed, for the proposed scheme and both baseline schemes, the average system sum-rates decrease as the quality of the CSI degrades. In particular, the worse the quality of the estimated CSI is, the more difficult it is for the AP to perform accurate beamforming and efficient AN jamming, which results in a lower achievable system sum-rate. In addition, the proposed scheme significantly outperforms both baseline schemes over the entire range of considered estimation error variances, which indicates that the proposed scheme can exploit the spatial DoFs available for security provisioning more efficiently than the two baseline schemes even in the presence of CSI uncertainty. In Fig. 8(b), the outage probability of the potential eavesdroppers versus the target SINR is investigated for $\kappa^2 = 0.1$. The outage probability is defined as the probability that the received SINR values at the eavesdroppers are higher than a predefined target SINR. For comparison, we also investigate the outage probability of a non-robust scheme. The considered non-robust scheme treats the estimated CSI of the eavesdropping channels, i.e., $\bar{\mathbf{H}}_j$, as perfect CSI. As can be observed, a significant outage probability reduction can be achieved via robust optimization with the proposed scheme and even with the baseline schemes compared to the non-robust scheme, especially in the low target SINR regime. Specifically, the outage probability of the proposed scheme is 10% at -1 dB whereas the outage probability of the non-robust scheme is as high as 80%.



(a) Average system sum-rate (bits/s/Hz) versus the maximum normalized channel estimation error variance. (b) Outage probability of potential eavesdroppers versus the target SINR (dB).

Fig. 8. The system parameters are set as $N_t = M = 6$, $K = 3$, $J = 2$, $d_1 = 20$ m, $P = 10$ dBm, and $\tau_{k,j} = 1$ bit/s/Hz.

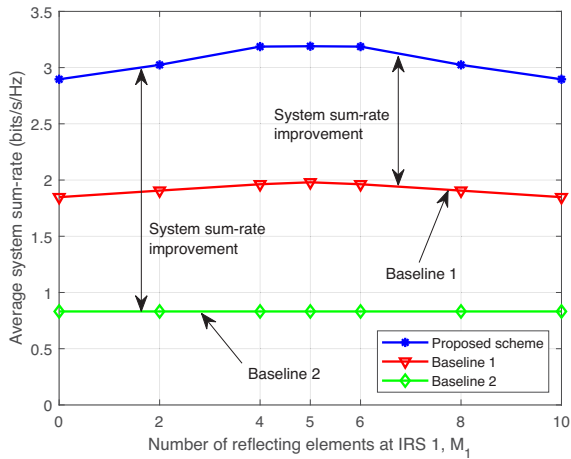


Fig. 9. Average system sum-rate (bits/s/Hz) versus the number of reflecting elements at IRS 1, for $M = 10$, $N_t = 6$, $K = 3$, $J = 2$, $d_1 = d_2 = 20$ m, $P = 25$ dBm, $\kappa_j^2 = 0.1$, and $\tau_{k,j} = 1$ bit/s/Hz.

Furthermore, as we set the maximum tolerable channel capacity of the potential eavesdroppers to $\tau_{k,j} = 1$ bit/s/Hz, the outage probabilities of the proposed scheme and both baseline schemes are zero when the target SINRs are no less than 0 dB (as $\log_2(1+1) = 1$ bit/s/Hz). In contrast, the outage probability for the non-robust scheme at 0 dB is still higher than 30%. These results confirm the robustness of the proposed scheme.

I. Single IRS or Multiple IRSs?

In this subsection, we compare the average system sum-rates achieved by deploying a single IRS and two IRSs in the secure wireless network shown in Fig. 2. For the scenario when two IRSs are deployed, they are symmetrically located to the East and West of the AP. We assume that there are in total $M = 10$ reflecting elements available for deployment of the two IRSs. In particular, M_1 reflecting elements are allocated to IRS 1, and $M_2 = M - M_1$ elements are assigned to IRS 2. As can be observed in Fig. 9, the proposed scheme considerably

outperforms both baseline schemes for all IRS settings. In addition, it is beneficial to deploy two IRSs compared to only one. This is because multiple IRSs create multiple independent propagation paths which introduces macro diversity, and thus, facilitates the establishment of strong end-to-end LoS channels from the AP to the legitimate users. Specifically, when multiple IRSs are deployed in the network, the distance between each legitimate user and its nearest IRS is reduced, which improves the system sum-rate. On the other hand, although the distance between each potential eavesdropper and its nearest IRS is also shortened, our proposed algorithm can effectively degrade the channel quality of the eavesdroppers such that the secrecy performance is improved. In fact, the peak system sum-rate is achieved by uniformly distributing the reflecting elements among the deployed IRSs, i.e., 5 reflecting elements for each IRS. As indicated by Fig. 6, the performance gain diminishes as the number of reflecting elements at one IRS grows large compared to the number of users. Therefore, a biased allocation with exceedingly many reflecting elements at one of the IRSs is not favorable.

VI. CONCLUSIONS

In this paper, we incorporated IRSs in multiuser MISO systems to achieve secure communication in the presence of multiple multi-antenna potential eavesdroppers for the challenging case where the legitimate users do not have a LoS link to the AP. The transmit beamformers, AN covariance matrix, and IRS phase shifts were jointly optimized to maximize the system sum-rate while satisfying secrecy constraints for the potential eavesdroppers. We focused on the robust design of such IRS-assisted secure wireless systems taking into account the imperfection of the CSI of the eavesdropping channels. An efficient AO algorithm that yields a stationary solution of the formulated non-convex optimization problem was proposed. In particular, the resulting challenging unit modulus constrained optimization problem was transformed to a rank constrained problem, for which an effective d.c. function representation was employed to facilitate the application of SDR and SCA

techniques. Simulation results have verified the tremendous potential of IRSs to improve the physical layer security of future wireless communication systems in an energy-efficient manner. Our results also confirmed the robustness of the proposed scheme with respect to imperfect CSI and its ability to exploit multiuser diversity. Furthermore, design guidelines for multi-IRS systems were provided. In particular, the uniform distribution of the reflecting elements among multiple IRSs was shown to be favorable for improving physical layer security and exploiting macro diversity gains.

APPENDIX

A. Proof of Proposition 1

According to Sylvester's determinant identity $\det(\mathbf{I} + \mathbf{A}\mathbf{B}) = \det(\mathbf{I} + \mathbf{B}\mathbf{A})$, we have

$$\begin{aligned}
& \max_{\Delta \mathbf{H}_j \in \Omega_j} \log_2 \det(\mathbf{I}_{N_r} + \mathbf{Q}_j^{-1} \mathbf{H}_j \Phi \mathbf{G} \mathbf{w}_k \\
& \quad \times \mathbf{w}_k^H \mathbf{G}^H \Phi^H \mathbf{H}_j^H) \leq \tau_{k,j} \\
\Leftrightarrow & \max_{\Delta \mathbf{H}_j \in \Omega_j} \log_2 (1 + \mathbf{w}_k^H \mathbf{G}^H \Phi^H \mathbf{H}_j^H \mathbf{Q}_j^{-1} \mathbf{H}_j \Phi \mathbf{G} \mathbf{w}_k) \leq \tau_{k,j} \\
\Leftrightarrow & \max_{\Delta \mathbf{H}_j \in \Omega_j} \text{Tr}(\mathbf{Q}_j^{-1} \mathbf{H}_j \Phi \mathbf{G} \mathbf{w}_k \mathbf{w}_k^H \mathbf{G}^H \Phi^H \mathbf{H}_j^H) \leq 2^{\tau_{k,j}} - 1 \\
\stackrel{(a)}{\Leftrightarrow} & \max_{\Delta \mathbf{H}_j \in \Omega_j} \lambda_{\max}(\mathbf{Q}_j^{-1/2} \mathbf{H}_j \Phi \mathbf{G} \mathbf{w}_k \\
& \quad \times \mathbf{w}_k^H \mathbf{G}^H \Phi^H \mathbf{H}_j^H \mathbf{Q}_j^{-1/2}) \leq 2^{\tau_{k,j}} - 1 \\
\Leftrightarrow & \max_{\Delta \mathbf{H}_j \in \Omega_j} (2^{\tau_{k,j}} - 1) \mathbf{Q}_j - \mathbf{H}_j \Phi \mathbf{G} \mathbf{w}_k \mathbf{w}_k^H \mathbf{G}^H \Phi^H \mathbf{H}_j^H \succeq \mathbf{0},
\end{aligned} \tag{33}$$

where (a) holds since matrix $\mathbf{Q}_j^{-1} \mathbf{H}_j \Phi \mathbf{G} \mathbf{w}_k \mathbf{w}_k^H \mathbf{G}^H \Phi^H \mathbf{H}_j^H$ has rank one, and therefore its maximum eigenvalue is the only non-zero eigenvalue. By substituting the expression of \mathbf{Q}_j defined after (5) into the last LMI, we obtain the result in Proposition 1.

B. Proof of Theorem 1

We first express problem (20) in its epigraph form as follows⁵

$$\begin{aligned}
& \underset{\eta_k, p_{k,j} \geq 0, \mathbf{W}_k, \mathbf{Z} \in \mathbb{H}^{N_t}}{\text{minimize}} & - \sum_{k \in \mathcal{K}} \text{Tr}(\mathbf{W}_k \nabla_{\mathbf{W}_k}^H D_1) \\
& & - \text{Tr}(\mathbf{Z} \nabla_{\mathbf{Z}}^H D_1) - \sum_{k \in \mathcal{K}} \log_2(\eta_k + \sigma_{1,k}^2) \\
& \text{subject to} & \text{C1, C2, } \overline{\text{C4}}, \text{C5,} \\
& & \text{C10: } \sum_{i \in \mathcal{K}} \text{Tr}(\mathbf{W}_i \mathbf{M}_k) \\
& & + \text{Tr}(\mathbf{Z} \mathbf{M}_k) \geq \eta_k, \quad \forall k.
\end{aligned} \tag{34}$$

This problem is jointly convex with respect to the optimization variables and satisfies Slater's constraint qualification [49, Ch.

⁵To keep the presentation concise, in this proof, we simplify the notations $\nabla_{\mathbf{Z}} D_1(\mathbf{W}^{(t)}, \mathbf{Z}^{(t)})$ and $\nabla_{\mathbf{W}_k} D_1(\mathbf{W}^{(t)}, \mathbf{Z}^{(t)})$ to $\nabla_{\mathbf{Z}} D_1$ and $\nabla_{\mathbf{W}_k} D_1$, respectively.

5.2.3]. Therefore, strong duality holds and the Lagrangian function in terms of \mathbf{W}_k is given by

$$\begin{aligned}
\mathcal{L} = & - \sum_{k \in \mathcal{K}} \text{Tr}(\mathbf{W}_k \nabla_{\mathbf{W}_k}^H D_1) + \gamma \sum_{k \in \mathcal{K}} \text{Tr}(\mathbf{W}_k) \\
& - \sum_{k \in \mathcal{K}} \delta_k \sum_{i \in \mathcal{K}} \text{Tr}(\mathbf{W}_i \mathbf{M}_k) - \sum_{k \in \mathcal{K}} \text{Tr}(\Upsilon_k \mathbf{W}_k) \\
& + \sum_{k \in \mathcal{K}} \sum_{j \in \mathcal{J}} \text{Tr}(\Omega_{k,j} \mathbf{S}_j \Phi \mathbf{G} \mathbf{W}_k \mathbf{G}^H \Phi^H \mathbf{S}_j^H) + \xi,
\end{aligned} \tag{35}$$

where ξ includes all terms that do not involve \mathbf{W}_k . The Lagrange multipliers associated with constraints C1, C4, C5, and C10 in problem (34) are denoted by $\gamma \geq 0$, $\Omega_{k,j} \in \mathbb{H}^{M+N_r}$, $\Upsilon_k \in \mathbb{H}^{N_t}$, and $\delta_k \geq 0$, respectively. Then, we investigate the structure of \mathbf{W}_k by checking the Karush-Kuhn-Tucker (KKT) conditions for problem (34), which are given by

$$\begin{aligned}
\text{K1: } & \Upsilon_k^* \mathbf{W}_k^* = \mathbf{0}, \quad \text{K2: } \gamma^* \geq 0, \delta_k^* \geq 0, \Omega_{k,j}^* \succeq \mathbf{0}, \Upsilon_k^* \succeq \mathbf{0}, \\
\text{K3: } & \nabla_{\mathbf{W}_k} \mathcal{L}(\mathbf{W}_k^*) = \mathbf{0},
\end{aligned} \tag{36}$$

where γ^* , $\Omega_{k,j}^*$, Υ_k^* , and δ_k^* are the optimal Lagrangian multipliers for the dual problem of (34). Since constraint C10 is active at the optimal solution, we have $\delta_k > 0$. KKT condition K3 can be further expressed as $\Upsilon_k^* = \mathbf{B}_k^* - \delta_k^* \mathbf{M}_k$, where

$$\begin{aligned}
\mathbf{B}_k^* = & \gamma^* \mathbf{I}_{N_t} - \nabla_{\mathbf{W}_k} D_1(\mathbf{W}^{(t)}) - \sum_{i \in \mathcal{K} \setminus \{k\}} \delta_i^* \mathbf{M}_i \\
& + \sum_{j \in \mathcal{J}} \mathbf{G}^H \Phi^H \mathbf{S}_j^H \Omega_{k,j}^* \mathbf{S}_j \Phi \mathbf{G}.
\end{aligned} \tag{37}$$

First, we discuss the case when matrix \mathbf{B}_k^* is full rank, i.e., $\text{Rank}(\mathbf{B}_k^*) = N_t$. Recall that $\mathbf{M}_k = \mathbf{G}^H \Phi^H \mathbf{h}_k \mathbf{h}_k^H \Phi \mathbf{G}$ is a rank-one matrix. Then, we obtain for the rank of matrix Υ_k^* ,

$$\text{Rank}(\Upsilon_k^*) = \text{Rank}(\mathbf{B}_k^* - \delta_k^* \mathbf{M}_k) \geq N_t - 1. \tag{38}$$

The last inequality holds because $\text{Rank}(\mathbf{A} - \mathbf{B}) \geq \text{Rank}(\mathbf{A}) - \text{Rank}(\mathbf{B})$ for any \mathbf{A} and \mathbf{B} of the same dimension. Suppose $\text{Rank}(\Upsilon_k^*) = N_t$, then K1 implies that $\mathbf{W}_k^* = \mathbf{0}$, i.e., $\text{Rank}(\mathbf{W}_k^*) = 0$. Suppose $\text{Rank}(\Upsilon_k^*) = N_t - 1$, then K1 implies that the null space of Υ_k^* is spanned by a vector, and \mathbf{W}_k^* can be expressed as

$$\mathbf{W}_k^* = \mathbf{a}_k^* (\mathbf{a}_k^*)^H. \tag{39}$$

Hence, the optimal solution \mathbf{W}_k^* of problem (20) satisfies C6 if $\text{Rank}(\mathbf{B}_k^*) = N_t$.

Next, we exploit [50, Prop. 4.1] and study the case when matrix \mathbf{B}_k^* is not full rank, i.e., $r = \text{Rank}(\mathbf{B}_k^*) < N_t$. Let $\Pi_k^* \in \mathbb{C}^{N_t \times (N_t - r)}$ be the orthonormal basis of \mathbf{B}_k^* 's null space, whose columns are $\{\pi_{k,i}^*\}_{i=1}^{N_t - r}$. Since Υ_k^* is the Lagrangian multiplier associated with the PSD constraint C5, we have

$$\begin{aligned}
& \Upsilon_k^* \succeq \mathbf{0} \\
\Rightarrow & (\pi_{k,i}^*)^H \Upsilon_k^* \pi_{k,i}^* = (\pi_{k,i}^*)^H (\mathbf{B}_k^* - \delta_k^* \mathbf{M}_k) \pi_{k,i}^* \geq 0 \\
\Rightarrow & \delta_k^* \left| (\pi_{k,i}^*)^H \mathbf{G}^H \Phi^H \mathbf{h}_k \right|^2 \leq 0.
\end{aligned} \tag{40}$$

Since constraint C10 is active at the optimal solution, we have $\delta_k > 0$. Therefore,

$$\begin{aligned} \left| (\boldsymbol{\pi}_{k,i}^*)^H \mathbf{G}^H \boldsymbol{\Phi}^H \mathbf{h}_k \right|^2 = 0 &\Rightarrow \mathbf{M}_k \boldsymbol{\Pi}_k^* = \mathbf{0} \\ \Rightarrow \mathbf{B}_k^* \boldsymbol{\Pi}_k^* - \delta_k^* \mathbf{M}_k \boldsymbol{\Pi}_k^* = \boldsymbol{\Upsilon}_k^* \boldsymbol{\Pi}_k^* = \mathbf{0}, \end{aligned} \quad (41)$$

which means that $\boldsymbol{\Pi}_k$ spans $N_t - r$ orthogonal dimensions of $\boldsymbol{\Upsilon}_k^*$'s null space. Therefore, let \mathbf{N}_k^* be the orthonormal basis of $\boldsymbol{\Upsilon}_k^*$'s null space, where $\text{Rank}(\mathbf{N}_k^*) \geq N_t - r$. In addition, we have

$$\begin{aligned} \text{Rank}(\boldsymbol{\Upsilon}_k^*) &\stackrel{(b)}{\geq} r - 1 \\ \Rightarrow \text{Rank}(\mathbf{N}_k^*) &= N_t - \text{Rank}(\boldsymbol{\Upsilon}_k^*) \leq N_t - r + 1, \end{aligned} \quad (42)$$

where (b) follows from the same inequality as (38). As a result, the rank of \mathbf{N}_k^* is either $N_t - r$ or $N_t - r + 1$. Suppose $\text{Rank}(\mathbf{N}_k^*) = N_t - r$, according to (41), we have $\mathbf{N}_k^* = \boldsymbol{\Pi}_k^*$. According to K1 and (41), \mathbf{W}_k^* can be expressed as $\mathbf{W}_k^* = \sum_{i=1}^{N_t-r} c_{k,i}^* \boldsymbol{\pi}_{k,i}^* (\boldsymbol{\pi}_{k,i}^*)^H$, where $c_{k,i}^* \in \mathbb{R}$ is a scaling factor for $\boldsymbol{\pi}_{k,i}^*$. However, in this case, we have $\mathbf{W}_k^* \mathbf{M}_k = \mathbf{0}$ since we have proved that $\mathbf{M}_k \boldsymbol{\Pi}_k^* = \mathbf{0}$ in (41). This means that there is no information received by legitimate user k even if we allocate power to the beamformer for legitimate user k . Hence, this cannot correspond to the optimal solution of problem (20). Suppose $\text{Rank}(\mathbf{N}_k^*) = N_t - r + 1$, then we can express \mathbf{N}_k^* as $\mathbf{N}_k^* = [\boldsymbol{\Pi}_k^* \quad \mathbf{a}_k^*]$ and therefore the optimal solution \mathbf{W}_k^* can be written in the form of

$$\mathbf{W}_k^* = a_k^* \mathbf{a}_k^* (\mathbf{a}_k^*)^H + \sum_{i=1}^{N_t-r} c_{k,i}^* \boldsymbol{\pi}_{k,i}^* (\boldsymbol{\pi}_{k,i}^*)^H, \quad (43)$$

where $c_{k,i}^* > 0$, $a_k^* \in \mathbb{R}$ is a scaling factor for \mathbf{a}_k^* , $(\boldsymbol{\Pi}_k^*)^H \mathbf{a}_k^* = \mathbf{0}$ since \mathbf{N}_k^* is the orthonormal basis of $\boldsymbol{\Upsilon}_k^*$'s null space, and we have $\boldsymbol{\Upsilon}_k^* \mathbf{a}_k^* = \mathbf{0}$ according to (41). Therefore, we propose to construct an optimal rank-one $\tilde{\mathbf{W}}_k^*$ when matrix \mathbf{B}_k^* is not full rank as follows:

$$\begin{aligned} \tilde{\mathbf{W}}_k^* &= \mathbf{W}_k^* - \sum_{i=1}^{N_t-r} c_{k,i}^* \boldsymbol{\pi}_{k,i}^* (\boldsymbol{\pi}_{k,i}^*)^H = a_k^* \mathbf{a}_k^* (\mathbf{a}_k^*)^H, \\ \tilde{\mathbf{Z}}^* &= \mathbf{Z}^* + \sum_{i=1}^{N_t-r} c_{k,i}^* \boldsymbol{\pi}_{k,i}^* (\boldsymbol{\pi}_{k,i}^*)^H, \quad \tilde{p}_{k,j}^* = p_{k,j}^*. \end{aligned} \quad (44)$$

Note that with the construction in (44), we obtain a rank-one solution $\tilde{\mathbf{W}}_k^*$ and a PSD matrix $\tilde{\mathbf{Z}}^*$. Hence, the remaining tasks for proving the tightness of SDR are to check the feasibility of $\tilde{\mathbf{W}}_k^*$ and $\tilde{\mathbf{Z}}^*$, and to show that this construction yields the same optimal objective value as \mathbf{W}_k^* and \mathbf{Z}^* . It is easy to see that the construction in (44) does not affect the value of N and constraint C1 in (17) due to the fact that $\mathbf{Z}^* + \sum_{k \in \mathcal{K}} \mathbf{W}_k^* = \tilde{\mathbf{Z}}^* + \sum_{k \in \mathcal{K}} \tilde{\mathbf{W}}_k^*$. For constraint C4 in problem (20), we have

$$\begin{aligned} &\mathbf{P}_{k,j} + \mathbf{S}_j \boldsymbol{\Phi} \mathbf{G} \left[(2^{\tau_{k,j}} - 1) \tilde{\mathbf{Z}}^* - \tilde{\mathbf{W}}_k^* \right] \mathbf{G}^H \boldsymbol{\Phi}^H \mathbf{S}_j^H \\ &= \mathbf{P}_{k,j} + \mathbf{S}_j \boldsymbol{\Phi} \mathbf{G} \left[(2^{\tau_{k,j}} - 1) \mathbf{Z}^* - \mathbf{W}_k^* \right] \mathbf{G}^H \boldsymbol{\Phi}^H \mathbf{S}_j^H \\ &\quad + \mathbf{S}_j \boldsymbol{\Phi} \mathbf{G} \mathbf{D}_k^* \mathbf{G}^H \boldsymbol{\Phi}^H \mathbf{S}_j^H, \end{aligned} \quad (45)$$

where

$$\begin{aligned} \mathbf{D}_k^* &= (2^{\tau_{k,j}} - 1) \sum_{j \neq k} \sum_{i=1}^{N_t-r} c_{j,i}^* \boldsymbol{\pi}_{j,i}^* (\boldsymbol{\pi}_{j,i}^*)^H \\ &\quad + 2^{\tau_{k,j}} \sum_{i=1}^{N_t-r} c_{k,i}^* \boldsymbol{\pi}_{k,i}^* (\boldsymbol{\pi}_{k,i}^*)^H \succeq \mathbf{0}. \end{aligned} \quad (46)$$

Therefore, the LMIs in C4 still hold for $\tilde{\mathbf{W}}_k^*$ and $\tilde{\mathbf{Z}}^*$. Finally, we show that the construction in (44) does not change the value of the last two terms in the objective function of problem (20). According to (19), we have

$$\begin{aligned} &-\text{Tr}(\mathbf{Z}^* \nabla_{\mathbf{Z}}^H D_1) - \sum_{k \in \mathcal{K}} \text{Tr}(\mathbf{W}_k^* \nabla_{\mathbf{W}_k}^H D_1) \\ &= \frac{1}{\ln 2} \sum_{j \in \mathcal{K}} \frac{\text{Tr} \left[\left(\mathbf{Z}^* + \sum_{k \neq j} \mathbf{W}_k^* \right) \mathbf{M}_j \right]}{\text{Tr} \left[\left(\mathbf{Z}^{(t)} + \sum_{i \neq j} \mathbf{W}_i^{(t)} \right) \mathbf{M}_j \right] + \sigma_{1,j}^2}, \end{aligned} \quad (47)$$

where

$$\begin{aligned} &\left(\tilde{\mathbf{Z}}^* + \sum_{k \neq j} \tilde{\mathbf{W}}_k^* \right) \mathbf{M}_j \\ &= \left(\mathbf{Z}^* + \sum_{k \neq j} \mathbf{W}_k^* \right) \mathbf{M}_j + \left(\sum_{i=1}^{N_t-r} c_{j,i}^* \boldsymbol{\pi}_{j,i}^* (\boldsymbol{\pi}_{j,i}^*)^H \right) \mathbf{M}_j \\ &= \left(\mathbf{Z}^* + \sum_{k \neq j} \mathbf{W}_k^* \right) \mathbf{M}_j. \end{aligned} \quad (48)$$

The last equality holds since we have proved that $\mathbf{M}_k \boldsymbol{\Pi}_k^* = \mathbf{0}$ in (41), which completes the proof of Theorem 1.

C. Proof of Proposition 2

Denote the objective function of problem (23) as $f(\mathbf{V})$, and let \mathbf{V}^* be its optimal solution, that is, $f(\mathbf{V}^*) \leq f(\mathbf{V})$, for all \mathbf{V} that satisfy⁶ $\|\mathbf{V}\|_* - \|\mathbf{V}\|_2 = 0$. Denote the objective function of problem (26) as $g(\mathbf{V}; \rho)$. Since \mathbf{V}_s is the optimal solution of problem (26) for penalty factor ρ_s , we have $g(\mathbf{V}_s; \rho_s) \leq g(\mathbf{V}^*; \rho_s)$, which leads to the inequality

$$\begin{aligned} &f(\mathbf{V}_s) + \frac{1}{2\rho_s} (\|\mathbf{V}_s\|_* - \|\mathbf{V}_s\|_2) \\ &\leq f(\mathbf{V}^*) + \frac{1}{2\rho_s} (\|\mathbf{V}^*\|_* - \|\mathbf{V}^*\|_2) = f(\mathbf{V}^*), \end{aligned} \quad (49)$$

where the last equality holds as \mathbf{V}^* is the optimal solution of problem (23) and therefore the rank-one constraint must be satisfied. By rewriting (49), we obtain

$$\|\mathbf{V}_s\|_* - \|\mathbf{V}_s\|_2 \leq 2\rho_s [f(\mathbf{V}^*) - f(\mathbf{V}_s)]. \quad (50)$$

Suppose $\bar{\mathbf{V}}$ is a limit point of sequence $\{\mathbf{V}_s\}$ and there is an infinite subsequence \mathcal{S} such that $\lim_{s \in \mathcal{S}} \mathbf{V}_s = \bar{\mathbf{V}}$. By taking the limit as $s \rightarrow \infty$, $s \in \mathcal{S}$, on both sides of (50), we have

$$\begin{aligned} &\|\bar{\mathbf{V}}\|_* - \|\bar{\mathbf{V}}\|_2 = \lim_{s \in \mathcal{S}} (\|\mathbf{V}_s\|_* - \|\mathbf{V}_s\|_2) \\ &\leq \lim_{s \in \mathcal{S}} 2\rho_s [f(\mathbf{V}^*) - f(\mathbf{V}_s)] \stackrel{\rho_s \rightarrow 0}{=} 0, \end{aligned} \quad (51)$$

⁶In this proof, we investigate the effect of moving constraint C9 into the objective function of problem (23). Therefore, we do not consider constraints C4, C7, and C8 as they are common constraints shared by both problems (23) and (26).

where the first equality holds due to the continuity of the function $\|\mathbf{X}\|_* - \|\mathbf{X}\|_2$. Hence, we have $\|\bar{\mathbf{V}}\|_* - \|\bar{\mathbf{V}}\|_2 = 0$, so $\bar{\mathbf{V}}$ is feasible for problem (23). Furthermore, by taking the limit as $s \rightarrow \infty$ for $s \in \mathcal{S}$ in (49), we have by the non-negativity of ρ_s and of the term $\|\mathbf{V}_s\|_* - \|\mathbf{V}_s\|_2$ that

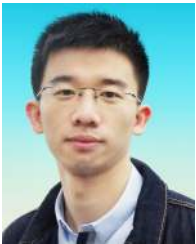
$$f(\bar{\mathbf{V}}) \leq f(\bar{\mathbf{V}}) + \lim_{s \in \mathcal{S}} \frac{1}{2\rho_s} (\|\mathbf{V}_s\|_* - \|\mathbf{V}_s\|_2) \leq f(\mathbf{V}^*). \quad (52)$$

As $\bar{\mathbf{V}}$ is a feasible point whose objective value is no larger than that of the optimal solution \mathbf{V}^* , we conclude that $\bar{\mathbf{V}}$, too, is an optimal solution for (23), which completes the proof.

REFERENCES

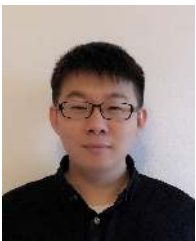
- [1] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, Dec. 2019, pp. 1–6.
- [2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
- [3] X. Du and H. Chen, "Security in wireless sensor networks," *IEEE Wireless Commun.*, vol. 15, no. 4, pp. 60–66, Aug. 2008.
- [4] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2017.
- [5] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.
- [6] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Robust and secure resource allocation for full-duplex MISO multicarrier NOMA systems," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 4119–4137, Sep. 2018.
- [7] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
- [8] T. J. Cui, M. Q. Qi, X. Wan, J. Zhao, and Q. Cheng, "Coding metamaterials, digital metamaterials and programmable metamaterials," *Light: Science & Applications*, vol. 3, no. 10, p. e218, 2014.
- [9] D. Xu, X. Yu, and R. Schober, "Resource allocation for intelligent reflecting surface-assisted cognitive radio networks," in *Proc. IEEE Int. Wkshp. Signal Process. Adv. Wireless Commun. (SPAWC)*, Atlanta, GA, USA, May 2020.
- [10] M. Najafi, V. Jamali, R. Schober, and H. Vincent Poor, "Physics-based modeling and scalable optimization of large intelligent reflecting surfaces," *arXiv:2004.12957*, Apr. 2020.
- [11] S. Asaad, R. F. Schaefer, and H. Vincent Poor, "Hybrid precoding for secure transmission in reflect-array-assisted massive MIMO systems," in *Proc. IEEE Int. Conf. Acoustics, Speech Signal Process. (ICASSP)*, Barcelona, Spain, 2020, pp. 8693–8697.
- [12] X. Yu, D. Xu, and R. Schober, "Optimal beamforming for MISO communications via intelligent reflecting surfaces," *arXiv:2001.11429*, Jan. 2020.
- [13] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, 2020.
- [14] S. Zhang and R. Zhang, "Capacity characterization for intelligent reflecting surface aided MIMO communication," *arXiv:1910.01573*, Oct. 2019.
- [15] C. Pan, H. Ren, K. Wang, W. Xu, M. Elkashlan, A. Nallanathan, and L. Hanzo, "Intelligent reflecting surface for multicell MIMO communications," *arXiv:1907.10864*, Aug. 2019.
- [16] J. Zhang, E. Björnson, M. Matthaiou, D. W. K. Ng, H. Yang, and D. J. Love, "Prospective multiple antenna technologies for beyond 5G," *arXiv:1910.00092*, Mar. 2020.
- [17] C. Pan, H. Ren, K. Wang, M. Elkashlan, A. Nallanathan, J. Wang, and L. Hanzo, "Intelligent reflecting surface enhanced MIMO broadcasting for simultaneous wireless information and power transfer," *arXiv:1908.04863*, Feb. 2020.
- [18] X. Yu, D. Xu, and R. Schober, "MISO wireless communication systems via intelligent reflecting surfaces," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Changchun, China, Aug. 2019, pp. 735–740.
- [19] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 162–169, Sep. 2018.
- [20] M. Di Renzo *et al.*, "Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come," *EURASIP J. Wireless Commun. Netw.*, vol. 129, no. 1, pp. 1–20, May 2019.
- [21] 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.
- [22] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, Oct. 2019.
- [23] D. Xu, X. Yu, Y. Sun, D. W. K. Ng, and R. Schober, "Resource allocation for secure IRS-assisted multiuser MISO systems," in *Proc. IEEE Global Commun. Conf. Wkshps. (GLOBECOM Wkshps)*, Waikoloa, HI, USA, Dec. 2019, pp. 1–6.
- [24] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Communications Letters*, to appear.
- [25] J. Chen, Y. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82 599–82 612, Jun. 2019.
- [26] G. Arunabha, J. Zhang, J. G. Andrews, and R. Muhamed, *Fundamentals of LTE*. The Prentice Hall, 2010.
- [27] 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.
- [28] G. T. de Araújo and A. L. de Almeida, "PARAFAC-based channel estimation for intelligent reflective surface assisted MIMO system," *arXiv:2001.06554*, Jan. 2020.
- [29] J. Chen, Y.-C. Liang, H. V. Cheng, and W. Yu, "Channel estimation for reconfigurable intelligent surface aided multi-user MIMO systems," *arXiv:1912.03619*, Dec. 2019.
- [30] J. Chen, X. Chen, W. H. Gerstacker, and D. W. K. Ng, "Resource allocation for a massive MIMO relay aided secure communication," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1700–1711, Aug. 2016.
- [31] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.
- [32] G. Zheng, K.-K. Wong, and T.-S. Ng, "Robust linear MIMO in the downlink: A worst-case optimization with ellipsoidal uncertainty regions," *EURASIP J. Adv. Signal Process.*, vol. 2008, no. 1, pp. 1–15, 2008.
- [33] J. Wang and D. P. Palomar, "Worst-case robust MIMO transmission with imperfect channel knowledge," *IEEE Trans. Signal Process.*, vol. 57, no. 8, pp. 3086–3100, Aug. 2009.
- [34] D. Xu, X. Yu, Y. Sun, D. W. K. Ng, and R. Schober, "Resource allocation for IRS-assisted full-duplex cognitive radio systems," *arXiv:2003.07467*, Mar. 2020.
- [35] C. You, B. Zheng, and R. Zhang, "Intelligent reflecting surface with discrete phase shifts: Channel estimation and passive beamforming," *arXiv:1911.03916*, Dec. 2019.
- [36] Z. Wang, L. Liu, and S. Cui, "Channel estimation for intelligent reflecting surface assisted multiuser communications: Framework, algorithms, and analysis," *arXiv:1912.11783*, Dec. 2019.
- [37] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE 62nd Veh. Technol. Conf.*, Dallas, TX, USA, Sep. 2005, pp. 1906–1910.
- [38] Q. Li and W. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.
- [39] X. Yu, J.-C. Shen, J. Zhang, and K. B. Letaief, "Alternating minimization algorithms for hybrid precoding in millimeter wave MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 485–500, Apr. 2016.
- [40] W. Zhao and S. Wang, "Resource allocation for device-to-device communication underlying cellular networks: An alternating optimization method," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1398–1401, Aug. 2015.
- [41] Z.-Q. Luo, J. F. Sturm, and S. Zhang, "Multivariate nonnegative quadratic mappings," *SIAM J. Optim.*, vol. 14, no. 4, pp. 1140–1162, Jul. 2004.

- [42] Z.-Q. Luo, W. Ma, A. M. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.
- [43] M. Grant, S. Boyd, and Y. Ye, "CVX: Matlab software for disciplined convex programming," 2008.
- [44] J. Nocedal and S. Wright, *Numerical Optimization*. Springer Science & Business Media, 2006.
- [45] T. Jiang and Y. Shi, "Over-the-air computation via intelligent reflecting surfaces," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, Dec. 2019, pp. 1–6.
- [46] Y. Sun, P. Babu, and D. P. Palomar, "Majorization-minimization algorithms in signal processing, communications, and machine learning," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 794–816, Feb. 2017.
- [47] I. Pólik and T. Terlaky, *Interior Point Methods for Nonlinear Optimization*. Springer, 2010.
- [48] D. Nguyen, L. Tran, P. Pirinen, and M. Latva-aho, "Precoding for full duplex multiuser MIMO systems: Spectral and energy efficiency maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 16, pp. 4038–4050, Aug. 2013.
- [49] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.
- [50] L. Liu, R. Zhang, and K. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850–1863, Apr. 2014.



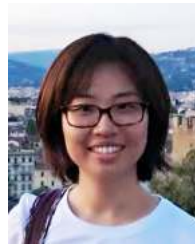
Xianghao Yu (S'15–M'19) received his B.Eng. degree in information engineering from Southeast University, Nanjing, China, in 2014, and his Ph.D. degree in electronic and computer engineering from the Hong Kong University of Science and Technology (HKUST), Hong Kong, China, in 2018. He is currently a Humboldt Post-Doctoral Research Fellow at the Institute for Digital Communications, Friedrich-Alexander-University Erlangen-Nuremberg (FAU), Erlangen, Germany. His research interests include millimeter wave communications, intelligent reflecting surface-assisted communications, MIMO systems, mathematical optimization, and stochastic geometry.

Dr. Yu co-authored the book entitled *Stochastic Geometry Analysis of Multi-Antenna Wireless Networks* (Springer, 2019). He received the IEEE Global Communications Conference (GLOBECOM) 2017 Best Paper Award, the 2018 IEEE Signal Processing Society Young Author Best Paper Award, and the IEEE GLOBECOM 2019 Best Paper Award.



Dongfang Xu (S'19) received the B.S. degree in communication engineering from Shandong University, Jinan, China, in 2014, and the M.S. degree in communication and multimedia engineering from Friedrich-Alexander-Universität Erlangen-Nürnberg, Erlangen, Germany, in 2017, where he is currently pursuing the Ph.D. degree in electrical engineering. His research interests include convex and nonconvex optimization, unmanned aerial vehicle communications, and physical layer security. He is also a co-recipient of the IEEE Global

Communications Conference (GLOBECOM) 2019 Best Paper Award.



Ying Sun (S'14) received the B.Sc. degree in electronic information from the Huazhong University of Science and Technology, Wuhan, China, in 2011, and the Ph.D. degree from the Department of Electronic and Computer Engineering at the Hong Kong University of Science and Technology. She is currently a postdoctoral researcher with the School of Industrial Engineering, Purdue University.

Her research interests include optimization algorithms, statistical signal processing, and machine learning.



Derrick Wing Kwan Ng (S'06–M'12–SM'17) received the bachelor degree with first-class honors and the Master of Philosophy (M.Phil.) degree in electronic engineering from the Hong Kong University of Science and Technology (HKUST) in 2006 and 2008, respectively. He received his Ph.D. degree from the University of British Columbia (UBC) in 2012. He was a senior postdoctoral fellow at the Institute for Digital Communications, Friedrich-Alexander-University Erlangen-Nürnberg (FAU), Germany. He is now working as a Senior

Lecturer and a Scientia Fellow at the University of New South Wales, Sydney, Australia. His research interests include convex and non-convex optimization, physical layer security, IRS-assisted communication, UAV-assisted communication, wireless information and power transfer, and green (energy-efficient) wireless communications.

Dr. Ng received the Best Paper Awards at the IEEE TCGCC Best Journal Paper Award 2018, INISCOM 2018, IEEE International Conference on Communications (ICC) 2018, IEEE International Conference on Computing, Networking and Communications (ICNC) 2016, IEEE Wireless Communications and Networking Conference (WCNC) 2012, the IEEE Global Telecommunication Conference (Globecom) 2011, and the IEEE Third International Conference on Communications and Networking in China 2008. He has been serving as an editorial assistant to the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS from Jan. 2012 to Dec. 2019. He is now serving as an editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and an area editor for the IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY. Also, he is listed as a Highly Cited Researcher by Clarivate Analytics in 2018 and 2019.



Robert Schober (S'98–M'01–SM'08–F'10) received the Diplom (Univ.) and the Ph.D. degrees in electrical engineering from Friedrich-Alexander University of Erlangen-Nuremberg (FAU), Germany, in 1997 and 2000, respectively. From 2002 to 2011, he was a Professor and Canada Research Chair at the University of British Columbia (UBC), Vancouver, Canada. Since January 2012 he is an Alexander von Humboldt Professor and the Chair for Digital Communication at FAU. His research interests fall into the broad areas of Communication Theory,

Wireless Communications, and Statistical Signal Processing.

Dr. Schober received several awards for his work including the 2002 Heinz Maier Leibnitz Award of the German Science Foundation (DFG), the 2004 Innovations Award of the Vodafone Foundation for Research in Mobile Communications, a 2006 UBC Killam Research Prize, a 2007 Wilhelm Friedrich Bessel Research Award of the Alexander von Humboldt Foundation, the 2008 Charles McDowell Award for Excellence in Research from UBC, a 2011 Alexander von Humboldt Professorship, a 2012 NSERC E.W.R. Stacie Fellowship, and a 2017 Wireless Communications Recognition Award by the IEEE Wireless Communications Technical Committee. Since 2017, he has been listed as a Highly Cited Researcher by the Web of Science. He is a Fellow of the Canadian Academy of Engineering and a Fellow of the Engineering Institute of Canada. From 2012 to 2015, he served as Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS. Currently, he serves as Member of the Editorial Board of the PROCEEDINGS OF THE IEEE and as VP Publications for the IEEE Communication Society (ComSoc).