Resource Allocation for IRS-Enabled Secure Multiuser Multi-Carrier Downlink URLLC Systems

Mohammad NaseriTehrani
University of Oulu,
Center for Wireless Communication (CWC),
Oulu, Finland.
email: *Mohammad.Naseritehrani@oulu.fi*

Shahrokh Farahmand
Iran University of Science and Technology (IUST),
Tehran, Iran.
email: *shahrokhf@iust.ac.ir*

Abstract—Secure ultra-reliable low-latency communication (URLLC) has been recently investigated with the fundamental limits of finite block length (FBL) regime in mind. Analysis has revealed that when eavesdroppers outnumber BS antennas or enjoy a more favorable channel condition compared to the legitimate users, base station (BS) transmit power should increase exorbitantly to meet quality of service (QoS) constraints. Channel-induced impairments such as shadowing and/or blockage pose a similar challenge. These practical considerations can drastically limit secure URLLC performance in FBL regime. Deployment of an intelligent reflecting surface (IRS) can endow such systems with much-needed *resiliency* and *robustness* to satisfy stringent latency, availability, and reliability requirements. We address this problem and propose to minimize the total BS transmit power by simultaneously designing the beamformers and artificial noise at the BS and phase-shifts at the IRS, while guaranteeing the required number of securely transmitted bits with the desired packet error probability, information leakage, and maximum affordable delay. The proposed optimization problem is non-convex and we apply block coordinate descent and successive convex approximation to iteratively solve a series of convex sub-problems instead. The proposed algorithm converges to a sub-optimal solution in a few iterations and attains substantial power saving and robustness compared to baseline schemes.

Index Terms—URLLC, Physical layer security, Intelligent reflecting surface, Successive convex approximation

I. Introduction

Ultra-reliable low-latency communication (URLLC) is founded on two conflicting features of high reliability, e.g., bit error rates (BERs) of 10^{-6}, and low latency, e.g., delays of at most 1ms. In a similar fashion, physical layer security (PLS) stands out as a promising approach to enhance both secrecy and service availability by exploiting the physical characteristics of wireless channel. PLS-based resource allocation has relied on secrecy capacity formula that is valid in the infinite block length regime and under additive white Gaussian noise (AWGN) channel assumption. These resource allocation schemes were developed without considering the crucial low latency requirement of URLLC users, which is realized by short packet transmissions (SPT). To fill this gap, [1] investigated a secure URLLC multiuser downlink setup with a single carrier with multiple eavesdroppers. Still, unfavorable channel conditions, such as multipath fading, blockage, and spatial correlation between BS-users and BS-eavesdroppers channels, would severely affect QoS, energy efficiency, and security [1]. Subsequently, the required secure number of bits can not be guaranteed at the intended receiver.

In this regard, IRS-assisted communication has enhanced the performance of different communication techniques such as multi-carrier transmissions [2], multi-antenna communications [3], and PLS [4]. Most of previous works in IRS resource allocation mainly focused on the single-carrier communications [5]. However, multi-carrier communications provides a host of desirable features such as simplified equalization, multi-user diversity and flexible resource allocation of power and bandwidth. As a challenge for multi-carrier techniques, IRS reflection coefficients need to be designed to serve all sub-carriers efficiently and simultaneously [2]. Only recently, URLLC resource allocation has begun to benefit from the advantages IRSs offer [6]. However, a joint investigation of resource allocation for secure multi-carrier URLLC when IRS is deployed is missing from the literature.

Targeting this research gap, our work's main contribution is to study the problem of minimizing the total BS transmit power by jointly designing the beamformers and artificial noise (AN) at the BS and phase shifts at the IRS, subject to a required minimum number of securely transmitted bits to URLLC users. Our approach is different from [1] as it is both multi-carrier and employs an IRS. On the other hand, [7] is different as it is both single carrier and single antenna and solves the loosely speaking dual problem of maximizing sum-secure-rate subject to latency and power constraints without IRS. We apply block coordinate descent (BCD) and successive convex approximation (SCA) to solve the ensuing non-convex problem. Instead of dropping rank constraints which may render the obtained solution infeasible, we utilize an iterative penalty-based SCA method that transforms the rank constraint into linear matrix inequalities (LMIs) per iteration [8].

II. System Model

We consider a single cell, where a BS equipped with N_T antennas is trying to transmit data to K single-antenna URLLC users indexed by $k = \{1, \ldots, K\}$. There exist J single-antenna eavesdroppers indexed by $j = \{1, \ldots, J\}$. An IRS with N_I elements is deployed to help the BS communicate securely with the intended URLLC users, cf. Fig. 1. We use frames of duration of T_f seconds, where each frame is divided into N time slots indexed by $n = \{1, \ldots, N\}$. $\bar{n}$ symbols are transmitted during each time slot. Total bandwidth F is divided into M sub-carriers with $B_s := F/M$ Hz of bandwidth each. The value of $\bar{n}$ depends on the sub-carrier bandwidth B_s and
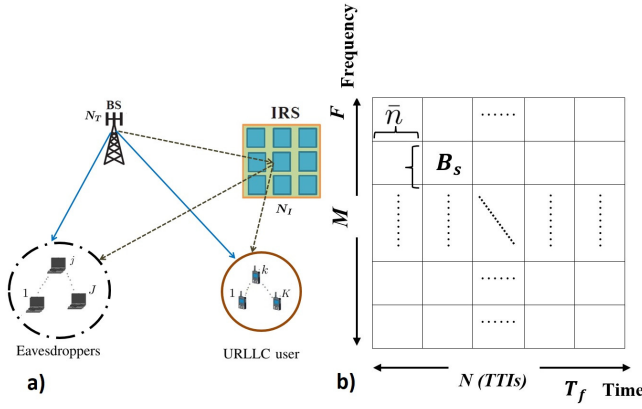
Fig. 1. System setup and model parameters

the total frame duration T_f, i.e., $\bar{n} = \frac{B_s T_f}{N}$, which is assumed to be an integer value. We further assume that only those users whose maximum tolerable delay can be satisfied in the current frame are admitted.

Upon applying linear beamforming at the BS, signal vector transmitted by BS on sub-carrier m in time slot n becomes

$$\mathbf{x}[m,n] = \sum_{k=1}^{K} \mathbf{w}_k[m,n] s_k[m,n] + \mathbf{v}[m,n], \quad (1)$$

where $\mathbf{w}_k[m,n] \in \mathbb{C}^{N_T \times 1}$ denotes the beamforming vector for user k on sub-carrier m in time slot n, and $s_k[m,n]$ represents IID complex zero-mean, unit variance symbol transmitted to user k on sub-carrier m in time slot n. Moreover, $\mathbf{v}[m,n]$ describes the AN component and is modeled as a zero-mean complex circularly-symmetric Gaussian random vector with Hermitian symmetric covariance matrix $\mathbf{V}[m,n]$. We assume a block fading channel model whose coherence time exceeds T_f. Furthermore, each sub-carrier channel is flat. We further assume that perfect channel state information (CSI) is available at the BS. As a result, our proposed algorithm will provide a performance benchmark on any method derived under partial or no CSI availability. Received signal at k-th user is given by

$$y_k[m,n] = \bar{\mathbf{h}}_k^H[m]\mathbf{x}[m,n] + z_k[m,n], \quad (2)$$

where we have defined $\bar{\mathbf{h}}_k^H[m] := \mathbf{h}_k^H[m]\mathbf{\Phi}[n]\mathbf{H}[m] + \mathbf{g}_k^H[m]$ and $\mathbf{h}_k^H[m] \in \mathbb{C}^{1 \times N_I}$, $\mathbf{g}_k^H[m] \in \mathbb{C}^{1 \times N_T}$, and $\mathbf{H}[m] \in \mathbb{C}^{N_I \times N_T}$ denote the channels between IRS-user k, BS-user k, and BS-IRS, respectively. Also, $\mathbf{\Phi}[n] = \text{diag}(\phi[n]) \in \mathbb{C}^{N_I \times N_I}$ represents the phase shift matrix of the IRS with N_I elements, and $z_k[m,n] \sim \mathcal{CN}(0, \sigma^2)$ indicates the noise at receiver k. Substituting (1) into (2), we obtain

$$y_k[m,n] = \bar{\mathbf{h}}_k^H[m,n]\mathbf{w}_k[m,n]s_k[m,n] + z_k[m,n] \quad (3)$$
$$+ \sum_{l \neq k}^{K} \bar{\mathbf{h}}_k^H[m,n]\mathbf{w}_l[m,n]s_l[m,n] + \bar{\mathbf{h}}_k^H[m,n]\mathbf{v}[m,n],$$

where the first term in the second line denotes interference at user k. In a similar fashion, the signal received at eavesdropper j is given by $y_j[m,n] = \bar{\mathbf{h}}_j^H[m]\mathbf{x}[m,n] + z_j[m,n]$, where we have defined $\bar{\mathbf{h}}_j^H[m] := \mathbf{h}_j^H[m]\mathbf{\Phi}[n]\mathbf{H}[m] + \mathbf{g}_j^H[m]$. The

received signal at eavesdropper j is derived similar to (3) with channel/noise indices k changed to j to denote eavesdropper channels. The corresponding channel vectors are $\mathbf{h}_j^H[m] \in \mathbb{C}^{1 \times N_I}$ and $\mathbf{g}_j^H[m] \in \mathbb{C}^{1 \times N_T}$ for the IRS-eavesdropper j and BS-eavesdropper j and $z_j[m,n] \sim \mathcal{CN}(0, \sigma^2)$ is the noise at eavesdropper j. We use $\gamma_k[m,n]$ and $\gamma_{jk}[m,n]$ to represent the SINR for user k at the intended receiver and eavesdropper j respectively.

III. PROBLEM FORMULATION

By considering asymptotically long codewords, both error probability and information leakage can be made arbitrarily small as long as transmission rate is kept below the secrecy capacity [9]. Unfortunately, the long codeword assumption is not practical in URLLC applications. A closed-form achievable secrecy rate for short packet transmission (SPT) was derived for AWGN channel in [10], and later extended to the multi-carrier scenario [11]. If one desires a maximum packet error probability of ϵ_k at the intended user, and a maximum information leakage of $\delta_{j,k}$ from user k to eavesdropper j, the total number of securely transmitted bits to user k is derived by [1]. Its multi-carrier extension is given by

$$\bar{B}_k = \bar{n} \sum_{m=1}^{M} \sum_{n=1}^{N} \log_2(1 + \gamma_k[m,n]) - aQ^{-1}(\epsilon_k) \left(\sum_{m=1}^{M} \sum_{n=1}^{N} \bar{n} \ Z_k[m,n] \right)^{\frac{1}{2}}$$
$$\quad (4)$$

$$- \max_{j \in \{1,2,...,J\}} \left(\bar{n} \sum_{m=1}^{M} \sum_{n=1}^{N} \log_2(1 + \gamma_{j,k}[m,n]) \right. \quad (5)$$

$$\left. + aQ^{-1}(\delta_{j,k}) \left(\sum_{m=1}^{M} \sum_{n=1}^{N} \bar{n} Z_{j,k}[m,n] \right)^{\frac{1}{2}} \right),$$

Channel dispersion is defined as $Z_k[m,n] = \left(1 - (1 + \gamma_k[m,n])^{-2}\right), \forall k$ and $Z_{j,k}[m,n] = \left(1 - (1 + \gamma_{j,k}[m,n])^{-2}\right), \forall j,k$ [12]. In practice, we would like to guarantee a minimum QoS of B_k^{req} to user k, which represents the minimum number of securely communicated bits that user k demands.

Let us define $\mathbf{w}, \mathbf{V}, \mathbf{\Phi}$ as the collection of $\mathbf{w}_k[m,n]$, $\mathbf{V}[m,n]$, and $\mathbf{\Phi}[n]$, respectively. Next, we aim to minimize the total transmit power at the BS while guaranteeing a minimum quality of service for each URLLC user. To this end, the main optimization problem is given by

$$\min_{\mathbf{w}, \mathbf{V}, \mathbf{\Phi}} \sum_{n=1}^{N} \sum_{m=1}^{M} \left(\sum_{k=1}^{K} \|\mathbf{w}_k[m,n]\|^2 + \text{Tr}\left(\mathbf{V}[m,n]\right) \right)$$

s.t. $\bar{B}_k\left(\mathbf{w}, \mathbf{V}, \mathbf{\Phi}\right) \geq B_k^{\text{req}}, \quad \mathbf{w}_k[m,n] = 0, \ \forall n > D_k, \ \forall k,$

$$\mathbf{V}[m,n] \succeq 0, \forall m, n, \quad |\mathbf{\Phi}_{i,i}(n)| = 1, \forall i, n, \quad (6)$$

where $\mathbf{\Phi}_{i,i}[n]$ is the i-'th diagonal element of matrix $\mathbf{\Phi}[n]$ for $i = \{1, 2, ..., N_I\}$, and D_k represents the maximum tolerable delay for user k. We set beamformer weights for user k equal to zero after time D_k as decoding later than D_k will be of no use to the device as it violates maximum tolerable delay. Problem (6) is non-convex with coupling between optimization variables $\mathbf{w}, \mathbf{V}$, and $\mathbf{\Phi}$ through the QoS constraint. To tackle these issues, we apply BCD and utilize SCA to iteratively solve each non-convex sub-problem.

$$\gamma_k[m,n] = \frac{\text{Tr}\left(\tilde{\boldsymbol{\Phi}}[n]\mathbf{G}_k[m]\mathbf{W}_k[m,n]\mathbf{G}_k^H[m]\right)}{\sum_{l\neq k}^K \text{Tr}\left(\tilde{\boldsymbol{\Phi}}[n]\mathbf{G}_k[m]\mathbf{W}_l[m,n]\mathbf{G}_k^H[m]\right) + \text{Tr}\left(\tilde{\boldsymbol{\Phi}}[n]\mathbf{G}_k[m]\mathbf{V}[m,n]\mathbf{G}_k^H[m]\right) + \sigma^2}, \quad (7)$$

IV. Our Proposed BCD Approach

To facilitate solving (6) via semi-definite program (SDP), we define positive semi-definite matrices $\mathbf{W}_k[m,n] := \mathbf{w}_k[m,n]\mathbf{w}_k[m,n]^H$, and we introduce $\mathbf{W}_k$ as collections of these $\mathbf{W}_k[m,n]$. Furthermore, we define $\tilde{\boldsymbol{\Phi}}[n] := \tilde{\phi}[n]\tilde{\phi}^H[n]$, $\forall n$ where $\tilde{\phi}[n] := [\phi^H[n], 1]^H$. The SINR definitions can be compactly written as traces. For instance, $\gamma_k[m,n]$ can be written compactly as in (7) on top of this page where $\mathbf{G}_k[m] = \left[\left(\text{diag}(\mathbf{h}_k^H[m])\mathbf{H}[m]\right)^T \mathbf{g}_k^*[m]\right]^T$. In the same vein, SINR of user k at eavesdropper j denoted by $\gamma_{kj}[m,n]$ is given by (7) with $\mathbf{G}_k$ replaced by $\mathbf{G}_j$. Next, we reformulate the QoS expression as $\bar{B}_k = R_k(\boldsymbol{\gamma}_k) - C_k(\boldsymbol{\gamma}_k) - \max_{j\in\{1,2,\dots,J\}} C_{j,k}(\boldsymbol{\gamma}_{j,k})$ where R_k, C_k, and $C_{j,k}$ are given by first and second terms in (4), and (5), respectively. By defining slack variables $\tau_k := \max_{j\in\{1,2,\dots,J\}} C_{j,k}$ and auxiliary variable $\alpha_k[m,n]$, and $\zeta_{j,k}[m,n]$ to decouple the constraints, an equivalent optimization problem to (6) is formulated as

$$\min_{\mathbf{W},\mathbf{V},\tilde{\boldsymbol{\Phi}},\boldsymbol{\tau},\boldsymbol{\alpha},\boldsymbol{\zeta}} \sum_{n=1}^N \sum_{m=1}^M \left(\sum_{k=1}^K \text{Tr}(\mathbf{W}_k[m,n]) + \text{Tr}\left(\mathbf{V}[m,n]\right)\right)$$

s.t. C1a : $R_k(\boldsymbol{\alpha}_k) - C_k(\boldsymbol{\alpha}_k) - \tau_k \geq B_k^{\text{req}}, \forall k,$

C1b : $\tau_k \geq C_{j,k}(\boldsymbol{\zeta}_{j,k})$, $\forall j, k,$

C2 : $\text{Tr}(\mathbf{W}_k[m,n]) = 0, \forall n > D_k, \forall k,$

C3 : $\mathbf{V}[m,n] \succeq 0, \forall m, n,$ C4 : $\mathbf{W}_k[m,n] \succeq 0, \forall k, m, n,$

C5 : $\text{Rank}(\mathbf{W}_k[m,n]) \leq 1, \forall k, m, n,$

C6 : $\text{diag}(\tilde{\boldsymbol{\Phi}}[n]) = I_{N_I+1}, \forall n,$ C7 : $\tilde{\boldsymbol{\Phi}}[n] \succeq 0, \forall n,$

C8 : $\text{Rank}(\tilde{\boldsymbol{\Phi}}[n]) = 1, \forall n,$

C9 : $\alpha_k[m,n] \leq \gamma_k[m,n], \forall k, m, n,$

C10 : $\zeta_{j,k}[m,n] \geq \gamma_{j,k}[m,n], \forall j, k, m, n,$ (8)

where $\boldsymbol{\tau} := \{\tau_k\}$, $\boldsymbol{\alpha} := \{\boldsymbol{\alpha}_k\}$, and $\boldsymbol{\zeta} := \{\boldsymbol{\zeta}_{j,k}\}$. For a single carrier system, i.e. $M = 1$, [1] has proven that the constraints C9 and C10 hold with equality at the optimum. For the multi-carrier setup, our numerical results indicate that they are tight at the achieved sub-optimal solution as well.

Finally, we apply BCD to problem (8) and decompose it into two sub-problems $\tilde{\text{P}}1$ and $\tilde{\text{P}}2$. They are given by

$$\tilde{\text{P}}1 : \min_{\mathbf{W},\mathbf{V},\boldsymbol{\tau},\boldsymbol{\alpha},\boldsymbol{\zeta}} \sum_{n=1}^N \sum_{m=1}^M \left(\sum_{k=1}^K \text{Tr}(\mathbf{W}_k[m,n]) + \text{Tr}\left(\mathbf{V}[m,n]\right)\right)$$

s.t. C1a, C1b, C2, C3, C4, C5, C9, C10. (9)

$$\tilde{\text{P}}2 : \min_{\check{\boldsymbol{\Phi}},p} p$$

s.t. $\tilde{\text{C}}6 : \text{diag}(\check{\boldsymbol{\Phi}}[n]) = pI_{N_I+1}, \forall n,$ C7, C8, C9, C10. (10)

We have defined $\check{\boldsymbol{\Phi}}[n] := p\tilde{\boldsymbol{\Phi}}[n]$. Specific formulation of the second sub-problem is attributed to [13], where it is revealed that solving $\tilde{\text{P}}1$ and $\tilde{\text{P}}2$ iteratively yields a sequence of decreasing objective values in (8). The constraints C1a, C1b, C5, C9, and C10 are non-convex in $\tilde{\text{P}}1$, while constraint C8 is non-convex in $\tilde{\text{P}}2$.

V. SCA for BCD Sub-Problems

An SCA algorithm for the single-carrier version of problem $\tilde{\text{P}}1$ has been proposed by [1]. We solve $\tilde{\text{P}}1$ by a straightforward multi-carrier extension of [1, Algorithm 1] whose details are omitted due to space limitations.

Next, we focus on $\tilde{\text{P}}2$ in (10) and optimize $\check{\boldsymbol{\Phi}}$, while fixing the variables $\hat{\mathbf{w}}_k$, $\hat{\mathbf{V}}$, $\hat{\boldsymbol{\tau}}, \hat{\boldsymbol{\alpha}}$, and $\hat{\boldsymbol{\zeta}}$ to their optimum obtained from the previous BCD step of solving $\tilde{\text{P}}1$. It should be mentioned that C9 and C10 are non-convex with respect to optimization variables in $\tilde{\text{P}}1$, while they are convex with respect to optimization variables in $\tilde{\text{P}}2$. Utilizing (7), C9 is reformulated into a linear inequality with respect to $\check{\boldsymbol{\Phi}}$ as

C9 : $\hat{\alpha}_k(m,n)\left(\sum_{l\neq k}^K \text{Tr}\left(\mathbf{G}_k[m]\check{\mathbf{W}}_l[m,n]\mathbf{G}_k^H[m]\check{\boldsymbol{\Phi}}[n]\right)\right.$

$$\left. + \text{Tr}\left(\mathbf{G}_k[m]\check{\mathbf{V}}[m,n]\mathbf{G}_k^H[m]\check{\boldsymbol{\Phi}}[n]\right) + \sigma^2\right)$$

$$\leq \text{Tr}\left(\mathbf{G}_k[m]\check{\mathbf{W}}_k[m,n]\mathbf{G}_k^H[m]\check{\boldsymbol{\Phi}}[n]\right), \quad \forall k, m, n \quad (11)$$

where $\check{\mathbf{W}}_k[m,n] := \hat{\mathbf{W}}_k[m,n]/\hat{p}$, $\check{\mathbf{V}}[m,n] := \hat{\mathbf{V}}[m,n]/\hat{p}$. Furthermore, we have $\hat{p} := \sum_{n=1}^N \sum_{m=1}^M \left(\sum_{k=1}^K \text{Tr}(\hat{\mathbf{W}}_k[m,n]) + \text{Tr}(\hat{\mathbf{V}}[m,n])\right)$. Similarly, C10 can be reformulated as in (11) with $\hat{\alpha}_k(m,n), \mathbf{G}_k[m]$ replaced by $\hat{\zeta}_{j,k}(m,n), \mathbf{G}_j[m]$ respectively and the inequality direction reversed. The next task is to address the non-convex rank one constraint C8. A novel method to deal with these types of constraints is provided by [8]. Their approach replaces the rank constraint with a semi-definite constraint

$$\tilde{\text{C}}8 : \quad r_n\mathbf{I}_{N_I} - \check{\mathbf{U}}_{N_I}^{(i)}[n]^H\check{\boldsymbol{\Phi}}[n]\check{\mathbf{U}}_{N_I}^{(i)}[n] \succeq 0. \quad (12)$$

Here, $\check{\mathbf{U}}_{N_I}[n]$ represents the $(N_I + 1) \times N_I$ matrix whose columns are the smallest N_I eigenvectors of $\check{\boldsymbol{\Phi}}[n]$. In order for $\check{\boldsymbol{\Phi}}[n]$ to be rank one, $\tilde{\text{C}}8$ should hold with $r_n = 0$. Since $\check{\mathbf{U}}_{N_I}[n]$ is not available, we use SCA and utilize the smallest N_I eigenvectors of $\check{\boldsymbol{\Phi}}^{(i)}[n]$, which is the optimum solution of previous SCA iteration and denote them by $\check{\mathbf{U}}_{N_I}^{(i)}[n]$ in (12). Furthermore, to ensure that ultimately $r_n = 0$ while obtaining an initial feasible point easily, we penalize r_n in the objective. At SCA iteration i, the following convex problem is solved

$$\min_{\check{\boldsymbol{\Phi}},p,\mathbf{r}} \Upsilon := p + \lambda^{(i)} \sum_{n=1}^N r_n, \quad \text{s.t } \tilde{\text{C}}6, \text{C}7, \tilde{\text{C}}8, \text{C}9, \text{C}10, (13)$$

where $\lambda^{(i)}$ represents a sequence of increasing weights. The proposed algorithm for the phase shift optimization is summarized in Algorithm 1. In the end, the overall BCD algorithm is summarized in Algorithm 2.

Algorithm 1 SCA for $\tilde{P}2$ in (10)

1) **Initialize** $\check{\Phi}^{(1)}$, $\lambda^{(1)}$, $\lambda_{\max} \gg 1$, $\eta > 1$, and $0 \le Er_{\text{SCA}} \ll 1$.
2) **Repeat**
3) Solve (13) for given $\check{\Phi}^{(i)}$ to obtain $\check{\Phi}^{(i+1)}$
4) Set $i \longrightarrow i + 1$, update $\lambda^{(i+1)} = \min(\eta\lambda^{(i)}, \lambda_{\max})$
5) **Untill** $\dfrac{\left|\Upsilon(\check{\Phi}^{(i+1)}) - \Upsilon(\check{\Phi}^{(i)})\right|}{\left|\Upsilon(\check{\Phi}^{(i)})\right|} \le Er_{\text{SCA}}$
6) **Output** $\Phi^* = \dfrac{\check{\Phi}^{(i)}}{p^{(i)}}$

Algorithm 2 BCD Algorithm for Solving (8)

1) **Initialize** $\{\mathbf{w}^{(1)}, \mathbf{V}^{(1)}, \mathbf{\Phi}^{(1)}\}$, and $0 \le Er_{\text{BCD}} \ll 1$.
2) **Repeat**
3) For given $\mathbf{\Phi} = \mathbf{\Phi}^{(\mu)}$, solve (9) via the multi-carrier extension of [1, Algorithm 1] to obtain $\mathbf{w}^{(\mu+1)}, \mathbf{V}^{(\mu+1)}$
4) Given $\mathbf{w}^{(\mu+1)}, \mathbf{V}^{(\mu+1)}$, solve (13) via **Algorithm 1** to obtain $\mathbf{\Phi}^{(\mu+1)}$. Set $\mu \longrightarrow \mu + 1$
5) **Till** ratio of improvement in objective $\le Er_{\text{BCD}}$
6) **Return** $\mathbf{w}^* = \mathbf{w}^{(\mu)}, \mathbf{V}^* = \mathbf{V}^{(\mu)}, \mathbf{\Phi}^* = \mathbf{\Phi}^{(\mu)}$

VI. NUMERICAL RESULTS

All channels, i.e., BS-IRS, IRS-user, BS-user, BS-eavesdropper, and IRS-eavesdropper which we denote by x are modeled as $g_x \times PL_{d_x}$, where g_x represents the small scale fading, and $PL_{d_x} = \left(\frac{c}{4\pi f_c d_{\text{ref}}}\right)\left(\frac{d_x}{d_{\text{ref}}}\right)^{-\Gamma_x} b_x$ describes the combined path-loss dependent large-scale fading and shadowing / blockage effects. Table I summarizes the selected parameters. Besides being uniformly located in disks of different radius as in Table I, authentic URLLC users and eavesdroppers maintain the same channel Rician factor and path loss exponent. Our simulation geometry is according to Fig. 1, where users and eavesdropper are located in separate disks with radii specified in Table I. Furthermore, we consider the network center, BS position, and IRS location to be at $(0, 0)$ meters (m), $(0, -100)$ m, and $(50, 0)$ m, respectively. The distance between URLLC users/eavesdroppers disk centers from IRS are given by $d_{\text{Iu}} = 4$ m and $d_{\text{Ie}} = 200$ m, respectively. The distance of users and eavesdroppers disk centers from BS are given by $d_{\text{Bu}} = 500$ m and $d_{\text{Be}} = 505$ m, respectively. The parameters of first BCD sub-problem, i.e., [1, Algorithm 1], are set to $\{t = 10, t_{\max} = 10^6, \eta = 6, I_{\max} = 16\}$, while parameters of second BCD sub-problem, i.e., **Algorithm 1** in this work, are set to $\{\lambda^{(1)} = 0.1, \lambda_{\max} = 10^5, \eta = 1.2, E_{r_{\text{SCA}}} = 10^{-5}\}$. We have defined $I_{\max}$ as the maximum number of iterations that can be afforded. A second, more practical scenario is also investigated where the channel of legitimate users and eavesdroppers are spatially correlated and eavesdroppers are closer to the BS with $d_{\text{Be}} = 250$. To model correlations, we exploit a spatial correlation matrix $\mathbf{R}$ to generate $\mathbf{g}_k, \forall k$ and $\mathbf{g}_j, \forall j$, while the other channels remain independent and unchanged. It is assumed that $[\mathbf{R}]_{i,j} = \rho^{|i-j|}$ with $\rho = 0.95$ [4].

A. Benchmark Schemes

- **SC**: Secrecy capacity for infinite block length where all channel dispersions are omitted from constraints C1a and C1b in (8). This amounts to letting $\bar{n}$ go to infinity. The

Table I: System parameters.

|	
Cell radius: Eavesdroppers, users	$r_{Ie} = 50$ m, $r_{Iu} = 5$ m
Number and bandwidth of subcarriers, and time slots	$M = 32$, Bw = 240 kHz and $N = 4$
Carrier frequency and Noise power density	$f_c = 6$ GHz and N_0 = -174 dBm/Hz
Number of bits per packet and system delay	$B_k^{\text{req}} = 160$ bits and $T_f = 0.21667$ ms
Maximum base station transmit power $P_{\max}$, d_{ref}	45 dBm, 1 m
Max error probability and information leakage	$\epsilon_k = 10^{-6}$, $\delta_{j,k} = 10^{-6}, \forall j, k$
Rician factor	$K_{\text{BI}} = 10$, $K_{\text{Bu}} = 0$, and $K_{\text{Iu}} = 0$
Path loss exponent	$\Gamma_{\text{BI}} = 2.1$, $\Gamma_{\text{Bu}} = 3.5$, and $\Gamma_{\text{Iu}} = 2.1$
shadowing/blockage	$b_{\text{Bu}} = -10$ dB and $b_{\text{Be}} = -10$ dB,
K, J, N_T, N_I, D_1, D_k for $k > 1$	2, 2, 2, 50, 2, 4
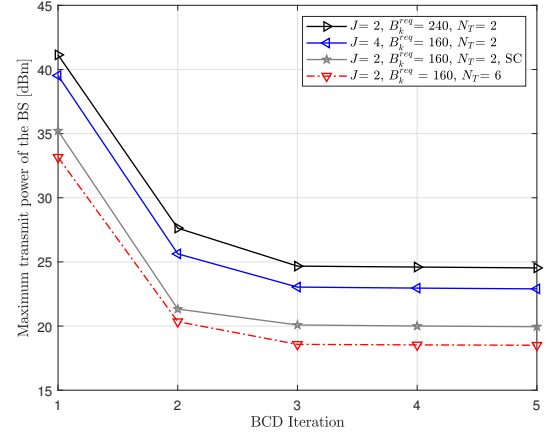
Fig. 2. Convergence speed of the proposed algorithm

same BCD Algorithm 2 is utilized to find a sub-optimal solution for this scheme. It provides a lower bound on the total transmit power at the BS for FBL [1].

- **Baseline 1**: We adopt random phase shifts at the IRS. Given a random phase shift matrix, we jointly optimize the beamformers and AN at the BS via [1, Algorithm 1].
- **Baseline 2**: We consider conventional secure-URLLC with No IRS and optimize the beamforming vector and AN at the BS [6].

B. Simulation Results

Fig. 2 corroborates the fast convergence rate of the BCD algorithm in approximately 5 iterations. This convergence occurs regardless of the number of eavesdroppers, BS antennas, and required QoS, which is suitable for URLLC use cases.

In Fig. 3, we study the impact of required number of secure communication bits $B_k^{\text{req}}, \forall k$, on the average transmit power at the BS for $N_T = 2, 6$. It is evident that without IRS, BS could only guarantee the required number of securely transmitted bits at an exorbitant increase in its total transmit power. Interestingly, Baseline 1 outperforms Baseline 2 even though it exploits the IRS in a naive way. Our proposed BCD enjoys substantial power savings versus both baselines. As expected, SC lower bound achieves the highest power saving. However, SC is designed for infinite block length and not applicable to URLLC scenarios. Finally, IRS ensures that even with small number of active antennas, i.e., $N_T = 2$ or $N_T = 6$ one can still obtain significant power savings at the BS side.
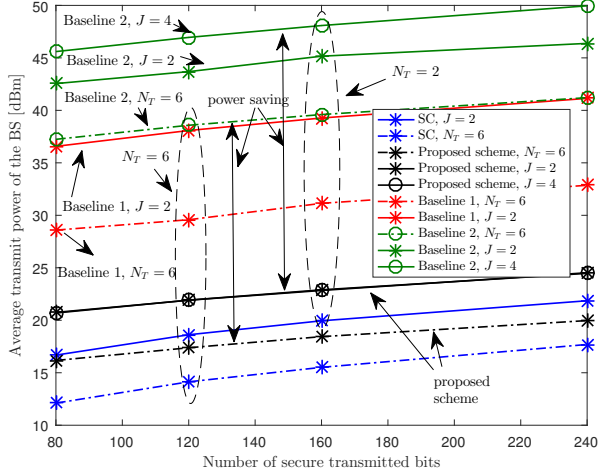
Fig. 3. Avg. transmit power vs. number of secure bits / packet

Fig. 4. Avg. transmit power vs. number of IRS elements

From another aspect, Fig. 3 also illustrates the impact of number of eavesdroppers on performance. When eavesdroppers outnumber the BS antennas, i.e., $N_T = 2 < J = 4$, transmit beamforming at the BS would suffer from insufficient spatial DoF for signal suppression in the direction of eavesdroppers. This drawback is illustrated by Baseline 2 which yields an excessive increase in BS transmit power. The presence of an IRS prevents such a power increase at the BS and enables the system to achieve the required secrecy rate. Even when secrecy rate decreases by the presence of more eavesdroppers, our proposed method can re-establish the needed QoS without any noticeable increase in power, while this is not the case for no IRS.

In Fig. 4, we investigate the impact of spatially correlated channels on average transmit power at the BS versus number of IRS elements. One observes that Baseline 2 suffers a significant increase of BS transmit power in spatially correlated channels in comparison to its uncorrelated counterpart. This indicates that conventional techniques such as BS beamforming and/or AN introduction at BS could not achieve the required secrecy rate with a practically feasible BS power. In contrast, the proposed scheme is robust to spatially correlated BS-users/BS-eavesdroppers channels as well as stronger BS-eavesdropper channel gains and the increase in BS transmit power is hardly noticeable. This advantage comes from the extra DoFs appearing due to IRS deployment which manages to realize constructive and destructive combinations of the desired signal at legitimate users and eavesdroppers, respectively. In addition, we observe that transmit power of the proposed scheme decreases monotonically as the number of IRS elements increases even in unfavorable channel conditions. While Baseline 1 avoids the significant power increase of Baseline 2, it still demands significantly more power compared to the proposed scheme. Interestingly, our proposed approach that considers finite block length limitations comes surprisingly close to the unachievable SC benchmark.
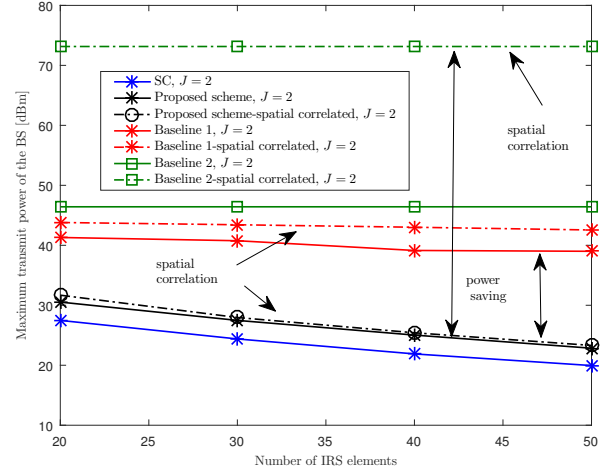
VII. CONCLUSION

Minimizing the total BS transmit power for secure multiuser downlink IRS-enabled MISO-URLLC systems was investigated subject to a minimum required number of securely transmitted bits. Simulation results corroborated the improved performance and robustness compared to no IRS schemes.

REFERENCES

[1] W. R. Ghanem, V. Jamali, and R. Schober, "Resource allocation for secure multi-user downlink MISO-URLLC systems," in *IEEE International Conference on Communications (ICC)*, 2020, pp. 1–7.

[2] Y. Yang, B. Zheng, S. Zhang, and R. Zhang, "Intelligent reflecting surface meets OFDM: Protocol design and rate maximization," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4522–4535, July 2020.

[3] S. Zhang and R. Zhang, "Capacity characterization for intelligent reflecting surface aided MIMO communication," *IEEE J. Select. Areas Commun.*, vol. 38, no. 8, pp. 1823–1838, Jun 2020.

[4] 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, May 2019.

[5] A. Kammoun, A. Chaaban, M. Debbah, M.-S. Alouini *et al.*, "Asymptotic max-min SINR analysis of reconfigurable intelligent surface assisted MISO systems," *IEEE Trans. Wirel. Commun.*, vol. 19, no. 12, pp. 7748–7764, Apr 2020.

[6] W. R. Ghanem, V. Jamali, and R. Schober, "Joint beamforming and phase shift optimization for multicell IRS-aided OFDMA-URLLC systems," *arXiv preprint arXiv:2010.07698*, Oct 2020.

[7] H. Ren, C. Pan, Y. Deng, M. Elkashlan, and A. Nallanathan, "Resource allocation for secure URLLC in mission-critical IoT scenarios," *IEEE Trans. Commun,*, vol. 68, no. 9, pp. 5793–5807, Jun 2020.

[8] C. Sun and R. Dai, "An iterative rank penalty method for nonconvex quadratically constrained quadratic programs," *SIAM Journal on Control and Optimization*, vol. 57, no. 6, pp. 3749–3766, 2019.

[9] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[10] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069–4093, July 2019.

[11] W. R. Ghanem, V. Jamali, Y. Sun, and R. Schober, "Resource allocation for multi-user downlink MISO OFDMA-URLLC systems," *IEEE Trans. Commun*, vol. 68, no. 11, pp. 7184–7200, Aug 2020.

[12] Y. Polyanskiy, "Channel coding: Non-asymptotic fundamental limits," Ph.D. dissertation, Princeton University.

[13] X. Yu, D. Xu, D. W. K. Ng, and R. Schober, "IRS-assisted green communication systems: Provable convergence and robust optimization," *arXiv preprint arXiv:2011.06484*, Nov 2020.