Eavesdropping with Intelligent Reflective Surfaces: Threats and Defense Strategies

Eavesdropping with Intelligent Reflective Surfaces: Threats and Defense Strategies

Francesco Malandrino
CNR-IEIIT
Torino, Italy

Alessandro Nordio
CNR-IEIIT
Torino, Italy

Carla Fabiana Chiasserini
Politecnico di Torino and CNR-IEIIT
Torino, Italy

***Abstract*—Intelligent reflecting surfaces (IRSs) have several prominent advantages, including improving the level of wireless communications security and privacy. In this work, we focus on this aspect and design a solution to counteract the presence of passive eavesdroppers overhearing transmissions from a base station towards legitimate users. Unlike most of the existing works addressing passive eavesdroppring, the proposed solution has low complexity, is suitable for scenarios where nodes are equipped with a limited number of antennas, and effectively trades off the legitimate users' data rate for secrecy rate.**

***Index Terms*—Intelligent reflecting surfaces, smart radio environment, secrecy rate**

I. Introduction

It is expected that future generation of mobile communications (6G) will exploit THz frequencies (e.g., 0.1–10 THz [1], [2]) for indoor as well as outdoor applications. THz communications can indeed offer very high data rates, although over short distances, due to harsh propagation conditions and severe path loss. To circumvent these problems, massive MIMO (M-MIMO) communication and beamforming techniques can be exploited to concentrate the transmitted power towards the intended receiver. Further, the use of intelligent reflecting surfaces (IRSs) [3] has emerged as a way to enable smart radio environments (SRE) [4], i.e., to control and adapt the radio environment to the communication between a transmitter and a receiver, aiming at optimizing the performance.

IRSs are passive beamforming devices, composed of a large number of low-cost antennas, that receive signals from sources, customize them by basic operations, and then forward it toward desired directions [5]–[7]. As discussed in [8], IRSs can be efficiently used to improve the security and privacy of wireless communications, as they can make the channel better for legitimate users, and worse for malicious ones.

As an example, the authors of [9] target the case of *aligned* eavesdroppers, lying between the transmitter and the legitimate receiver: in this case, the authors envision avoiding direct transmissions, and using IRSs to maximize the secrecy rate. Jamming is an effective, even if harsh, method to improve privacy by making the eavesdropper's channel worse: as an example, [10] envisions using IRSs to both serve legitimate users and jam the malicious one, maximizing the secrecy rate subject to power constraints. In MIMO scenarios, passive eavesdroppers can be blinded through standard beamforming techniques, thanks to the so-called secrecy-for-free property of MIMO systems with large antenna arrays. Several recent works, including [11], aim at achieving the same security level against active attackers, by leveraging filtering techniques and the fact that legitimate and malicious node are statistically distinguishable from each other. In a similar scenario, [12] presents an alternating optimization that jointly optimizes both transmitter and IRS parameters in order to maximize the secrecy rate.

In this work, we investigate the secrecy performance of IRS-based communications, considering the presence of a malicious receiver passively overhearing the downlink transmission intended for a legitimate user. Unlike previous works, we seek to reduce the complexity of the decisions to make by leveraging the key observation that, in virtually all real-world scenarios, IRSs point *towards a UE*. It follows that we can study the way IRSs are *used* to steer the signal, as opposed to the standard approach of optimizing the complex coefficients of the *matrices* describing the behavior of terminals and IRSs. The result is a very significant reduction of the solution space to explore, hence, of the complexity of the decision-making process as a whole.

The rest of the paper is organized as follows. Sec. II introduces the model of the system under study and behavior of the malicious node. Sec. III presents the problem formulation and our solution, while Sec. IV shows some results and tradeoffs. Finally, Sec. V concludes the paper.

II. System Model

We consider a wireless network operating in the THz bands, composed of:

- a base station (BS) whose ULA has M_{BS} isotropic elements and transmitting K streams, one for each legitimate user;
- K legitimate users (UE), each equipped with an ULA composed of M_{UE} isotropic elements;
- N IRSs ($N \geq K$); the n-th IRS includes L_n^2 elements (or meta-atoms), arranged in a $L_n \times L_n$ square grid or uniform planar array (UPA). The IRSs contribute to the BS-UEs communication by appropriately forwarding the BS signal toward the users;
- a passive eavesdropper (or malicious node, MN), whose ULA is composed of M_{MN} isotropic elements. The MN eavesdrops one of the K data streams by intercepting the signals reflected by the IRSs.

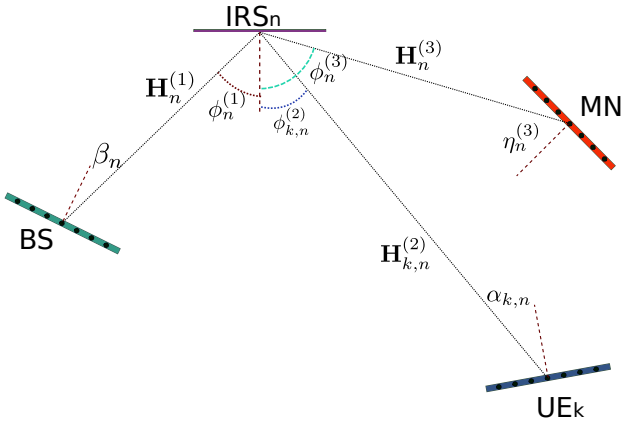


Fig. 1. Communication model: a base station (BS) is transmitting toward a user equipment (UE$_k$), thanks to the help of the IRSs. UE$_k$ is the victim of the malicious node (MN), which intercepts the signals reflected by the IRSs.

In the remainder of this section, we characterize the main elements of the system we consider, namely, the channel and IRSs (Sec. II-A), the nodes and their behavior (Sec. II-B), the metrics we consider (Sec. II-C), and the time dimension (Sec. II-D).

A. Channel and IRS

The elements of the ULAs and of the IRSs are assumed to be separated by $\lambda/2$ where λ is the wavelength of the signal carrier. We assume that no line-of-sight (LoS) path exists between the BS and the UEs. However, communication is made possible by the ability of the IRSs to reflect the BS signal towards the users [13]. All IRSs and user nodes, including the MN, are assumed to have the same height above ground, as depicted in Figure 1. This assumption allows simplifying the discussion and the notation while capturing the key aspects of the system. In the following, we detail the communication chain as well as the channel model.

Communication channel. While in many works dealing with GHz communications, the channel matrix connecting two multi-antenna devices is often modeled according to Rayleigh or Rice distributions, in the THz bands the channel statistic is not yet completely characterized. Moreover, at such high frequencies the signal suffers from strong free-space attenuation, and is blocked even by small solid obstacles. In practice, the receiver needs to be in line-of-sight (LoS) with the transmitter to be able to communicate. Also, recent studies [14] highlight that already at sub-THz frequencies all scattered components and multipath effects can be neglected. This conclusion is also supported by the fact that, typically, both the transmitter and the receiver employ massive beamforming techniques in order to concentrate the signal energy along a specific direction and compensate for high path losses. In such conditions, the channel matrix between any two devices can thus be modeled as:

$$\mathbf{H}^{\mathrm{LOS}} = ac\mathbf{p}\mathbf{q}^{\mathsf{H}} \tag{1}$$

where the scalar a takes into account large scale fading effects due to, e.g., obstacles temporarily crossing the LoS path between transmitter and receiver. The coefficient c instead accounts for the attenuation and phase rotation due to propagation. More specifically, let d be the distance between the transmitting and the receiving device and G be the array gain of one of them. Then the expression for c is given by:

$$c = \sqrt{\frac{GA}{4\pi d^2}} \mathrm{e}^{\mathrm{j}\frac{2\pi}{\lambda}d} \tag{2}$$

where A is the effective area of the other device. Finally, $\mathbf{p}$ and $\mathbf{q}$ are norm-1 vectors representing, respectively, the spatial signatures of the receive and transmit antenna arrays. The spatial signature of a ULA composed of M_{z} (z =BS,UE,MN) isotropic elements spaced by $\lambda/2$ and observed from an angle β (measured with respect to a direction orthogonal to the ULA), is given by the size-M_z vector $\mathbf{s}(\beta, M_z)$, whose m-th element is given by

$$[\mathbf{s}(\beta, M_z)]_m = \frac{1}{\sqrt{M_z}} \mathrm{e}^{-\mathrm{j}\frac{\pi}{2}(M_z-1)\sin\beta} \mathrm{e}^{-\mathrm{j}\pi(m-1)\sin\beta}. \tag{3}$$

This relation applies to devices equipped with ULAs such as the BS, the UEs and the MN. However, it can also be applied to IRSs since their planar configuration can be viewed as a superposition of several ULAs.

IRS characterization. IRSs are made of meta-atoms (modeled as elementary spherical scatterer) whose scattered electromagnetic field holds in the far-field regime [15], [16]. The n-th IRS, $n = 1, \ldots, N$, is composed of L_n^2 meta-atoms arranged in an $L_n \times L_n$ square grid. The area of the n-th IRS is, thus, given by $A_n = L_n^2\lambda^2/4$. The meta-atom at position (ℓ, ℓ') in the n-th IRS applies a (controlled) continuous phase shift, $\theta_{n,\ell,\ell'}$ to the signal impinging on it. In many works that assume rich scattering communication channels, such phase-shifts are independently optimized in order to maximize some performance figures. However, under the channel model in (1), phase-shifts are related to each other [17], [18] according to the linear equation:

$$\theta_{n,\ell,\ell'} = \pi q_n \left(\ell - 1 - \frac{L_n - 1}{2}\right) + \psi_n \tag{4}$$

where q_n and ψ_n control, respectively, the direction and the phase of the reflected signal. For simplicity, we arrange the phase shifts $\theta_{n,\ell,\ell'}$ in the diagonal matrix

$$\bar{\mathbf{\Theta}}_n = \mathbf{I}_{L_n} \otimes \mathbf{\Theta}_n$$

where $\mathbf{\Theta}_n = \mathrm{diag}(\theta_{n,1,\ell'}, \ldots, \theta_{n,L_n,\ell'})$, $\otimes$ denotes the Kronecker product, and $\mathbf{I}_{L_n}$ is the identity matrix of size L_n. As an example, let $\phi_n^{(1)}$ be the angle of arrival (AoA) of the BS signals on the n-th IRS and let $\phi_{n,k}^{(2)}$ be the direction of the k-th IRS as observed from the n-th IRS (see Figure 1). Then, in order to let the n-IRS reflect the BS signal towards the k-th UE, we set [13]

$$q_n = \sin\phi_n^{(1)} - \sin\phi_{n,k}^{(2)}. \tag{5}$$

In a practical case, a given IRS serves a single UE; thus, we define as *permutation* a mapping between the set of UEs and the set of IRSs:

$$\nu_p : \{1, \ldots, K\} \to \{1, \ldots, N\}.$$

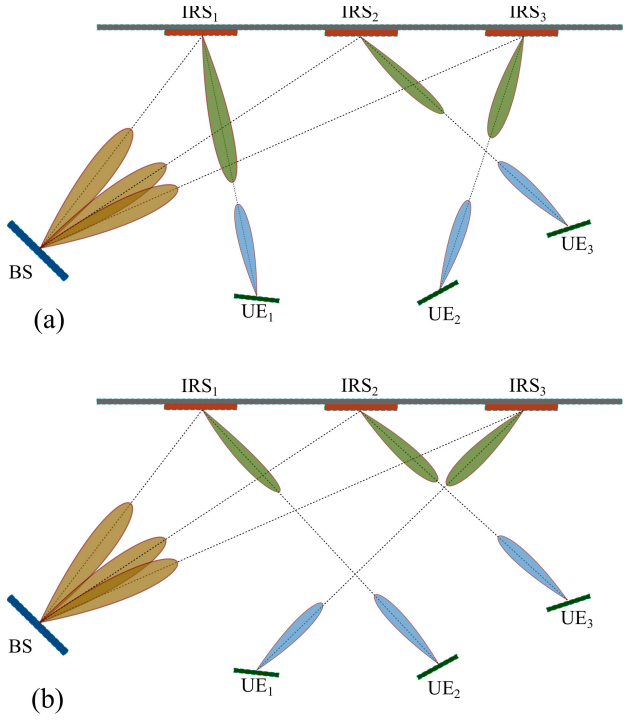


Fig. 2. Two possible permutations for a network with $N = K = 3$. The configuration in (a) corresponds to the map $\nu_a(1) = 1$, $\nu_a(2) = 3$, and $\nu_a(3) = 2$, while the configuration in (b) corresponds to the map $\nu_b(1) = 3$, $\nu_b(2) = 1$, and $\nu_b(3) = 2$.

Under this map, IRS $\nu_p(k)$ forwards the BS signal towards the k-th UE and, by symmetry, the k-th UE points its beam towards the $\nu_p(k)$-th IRS. The number of possible permutations (or maps) is then $P = N!/(N-K)!$ and its set is denoted by $\mathcal{P}$. Moreover, we also denote by $\bar{\Theta}_{n,p}$ the matrix of the n-IRS phase-shifts under the permutation $p = 1, \ldots, P$. An example of possible permutations for a network composed of $N = 3$ IRSs and $K = 3$ UEs is depicted in Figure 2.

B. Network nodes

Base station. The BS transmit a signal with bandwidth B and wavelength λ. Such signal contains K data streams, one for each UE. Let x_k be the zero-mean unit variance Gaussian complex i.i.d. random symbol generated for the k-th stream at a given time. Also, let $\boldsymbol{\gamma}_k$, be the beamforming vector employed for transmitting x_k. Then, the signal transmitted by the BS is given by:

$$\mathbf{t} = \boldsymbol{\Gamma}\mathbf{x} \tag{6}$$

where $\boldsymbol{\Gamma} = [\boldsymbol{\gamma}_1, \ldots, \boldsymbol{\gamma}_K]$, $\mathbf{x} = [x_1, \ldots, x_K]^{\mathsf{T}}$. We assume that the total transmit power is limited by $\mathbb{E}[|\mathbf{t}|^2] = \|\boldsymbol{\Gamma}\|_{\mathrm{F}}^2 \leq P_t$, where $\|\cdot\|_{\mathrm{F}}$ denotes the Frobenius norm.

Legitimate receivers (UEs). The signal received by the k-th UE under the p-th map is given by

$$r_{k,p} = \underbrace{\mathbf{f}_{k,p}^{\mathsf{H}} \sum_{n=1}^{N} \mathbf{H}_{k,n}^{(2)} \bar{\boldsymbol{\Theta}}_{n,p} \mathbf{H}_{n}^{(1)}}_{\widetilde{\mathbf{h}}_{n,p}^{\mathsf{H}}} \mathbf{t} + n_k \tag{7}$$

where $n_k \sim \mathcal{N}_{\mathbb{C}}(0, N_0 B)$ is additive Gaussian complex noise, whose power spectral density is N_0. B is the signal bandwidth and $\mathbf{f}_{k,p}$ is the beamforming vector at the k-th UE. According to the channel model in (1), $\mathbf{H}_n^{(1)} = a_n^{(1)} c_n^{(1)} \mathbf{p}_n^{(1)} \mathbf{q}_n^{(1)\mathsf{H}}$ is the channel connecting the BS to the n-th IRS and $\mathbf{H}_{k,n}^{(2)} = a_{k,n}^{(2)} c_{k,n}^{(2)} \mathbf{p}_{n,k}^{(2)} \mathbf{q}_{n,k}^{(2)\mathsf{H}}$ is the channel matrix connecting the n-th IRS to the k-th UE. In particular, we have $\mathbf{q}_n^{(1)} = \mathbf{s}(\beta_n, M_{\mathrm{BS}})$, $\mathbf{p}_n^{(1)} = \frac{1}{\sqrt{L_n}} \mathbf{1}_{L_n} \otimes \bar{\mathbf{p}}_n^{(1)}$, $\bar{\mathbf{p}}_n^{(1)} = \mathbf{s}(\phi_n^{(1)}, L_n)$, $\mathbf{p}_{k,n} = \mathbf{s}(\alpha_{k,n}, M_{\mathrm{UE}})$, $\mathbf{q}_{n,k}^{(2)} = \frac{1}{\sqrt{L_n}} \mathbf{1}_{L_n} \otimes \bar{\mathbf{q}}_{k,n}^{(2)}$ and $\bar{\mathbf{q}}_{k,n}^{(2)} = \mathbf{s}(\phi_{k,n}^{(2)}, L_n)$. The angles β_n, $\phi_n^{(1)}$, $\phi_{k,n}^{(2)}$, and $\alpha_{k,n}$ are specified in Figure 1. Furthermore, $c_n^{(1)} = \frac{\sqrt{M_{\mathrm{BS}} A_n}}{\sqrt{4\pi} d_n^{(1)}} \mathrm{e}^{\mathrm{j}\frac{2\pi}{\lambda} d_n^{(1)}}$ and $c_{k,n}^{(2)} = \frac{\sqrt{M_{\mathrm{UE}} A_n}}{\sqrt{4\pi} d_{n,k}^{(2)}} \mathrm{e}^{\mathrm{j}\frac{2\pi}{\lambda} d_{n,k}^{(2)}}$ where $d_n^{(1)}$ and $d_{n,k}^{(2)}$ are, respectively, the distance between the BS and the n-th IRS, and the distance between the n-th IRS and the k-th UE.

We assume that the UE ULA is only capable of analog beamforming. Thus, the norm-1 vector $\mathbf{f}_{k,p}$ is defined as $\mathbf{f}_{k,p} = \mathbf{s}(\alpha_{k,n}, M_{\mathrm{UE}})$ where $n = \nu_p(k)$, i.e., the beam generated by the k-th UE ULA points to the $\nu_p(k)$-th IRS. By collecting in the vector $\mathbf{r}_p$ the signals received by the K UEs and by recalling (6), we can write

$$\begin{aligned} \mathbf{r}_p &= \widetilde{\mathbf{H}}_p^{\mathsf{H}} \mathbf{t} + \mathbf{n} \\ &= \widetilde{\mathbf{H}}_p^{\mathsf{H}} \boldsymbol{\Gamma} \mathbf{x} + \mathbf{n} \end{aligned} \tag{8}$$

where $\widetilde{\mathbf{H}}_p = [\widetilde{\mathbf{h}}_{1,p}, \ldots, \widetilde{\mathbf{h}}_{K,p}]$ and $\mathbf{n} = [n_1, \ldots, n_K]^{\mathsf{T}}$.

Malicious node. By eavesdropping the communication, the MN acts as an additional receiver. When the p-th map is applied and the MN ULA points to the n-th IRS, the received signal can be written similarly to (7), as

$$\begin{aligned} o_{n,p} &= \mathbf{b}_n^{\mathsf{H}} \sum_{m=1}^{N} \mathbf{H}_m^{(3)} \bar{\boldsymbol{\Theta}}_{m,p} \mathbf{H}_m^{(1)} \mathbf{t} + \zeta \\ &= \widetilde{\mathbf{b}}_{n,p}^{\mathsf{H}} \mathbf{t} + \zeta \end{aligned} \tag{9}$$

where $\mathbf{H}_n^{(3)} = a_n^{(3)} c_n^{(3)} \mathbf{p}_n^{(3)} \mathbf{q}_n^{(3)\mathsf{H}}$ is the channel matrix connecting the n-th IRS to the MN, $\mathbf{p}_n^{(3)} = \mathbf{s}(\eta_n, M_{\mathrm{MN}})$, $\mathbf{q}_n^{(3)} = \frac{1}{\sqrt{L_n}} \mathbf{1}_{L_n} \otimes \bar{\mathbf{q}}_n^{(3)}$, $\bar{\mathbf{q}}_n^{(3)} = \mathbf{s}(\phi_n^{(3)}, L_n)$ (see Figure 1). Also, $c_n^{(3)} = \frac{\sqrt{M_{\mathrm{MN}} A_n}}{\sqrt{4\pi} d} \mathrm{e}^{\mathrm{j}\frac{2\pi}{\lambda} d_n^{(3)}}$ where $d_n^{(3)}$ is the distance between the MN and the n-th IRS. Finally, $\zeta \sim \mathcal{N}_{\mathbb{C}}(0, N_0 B)$ represents the additive noise at the receiver and $\mathbf{b}_n = \mathbf{s}(\eta_n, M_{\mathrm{MN}})$ is the norm-1 beamforming vector.

C. Metrics of interest

For each combination of IRS-to-UE assignment, we are interested in deriving two main metrics, namely, the SINR (hence, the data rate) and the secrecy rate.

The SINR achieved at each UE depends on the precoding strategy employed at the BS, i.e., on the choice of the precoder $\boldsymbol{\Gamma}$. For example, the zero-forcing (ZF) precoder permits to remove the inter-user interference while providing good (although not optimal) performance. Under the p-th map, ν_p, the ZF precoder is obtained by solving for $\boldsymbol{\Gamma}_p$ the equation $\widetilde{\mathbf{H}}_p^{\mathsf{H}} \boldsymbol{\Gamma}_p = \mu \mathbf{Q}$ where $\mathbf{Q} = \mathrm{diag}(q_1, \ldots, q_K)$ is an arbitrary

positive diagonal matrix and the scalar μ should be set so as to satisfy the power constraint $\|\mathbf{\Gamma}_p\|_{\mathrm{F}}^2 = P_t$. Its expression is given by:

$$\mathbf{\Gamma}_p \triangleq \frac{\sqrt{P_t}\widetilde{\mathbf{H}}_p^{+}\mathbf{Q}^{1/2}}{\|\widetilde{\mathbf{H}}_p\mathbf{Q}^{1/2}\|_{\mathrm{F}}}\,. \tag{10}$$

where $\widetilde{\mathbf{H}}_p^{+} = \widetilde{\mathbf{H}}_p^{\mathsf{H}}(\widetilde{\mathbf{H}}_p\widetilde{\mathbf{H}}_p^{\mathsf{H}})^{-1}$ is the Moore-Penrose pseudo-inverse of $\widetilde{\mathbf{H}}_p$. Then, the SINR at the k-th UE is given by,

$$\mathrm{SINR}_{k,p}^{\mathrm{UE}} = \frac{P_t q_k}{N_0 B\|\widetilde{\mathbf{H}}_p\mathbf{Q}^{1/2}\|_{\mathrm{F}}^2} \tag{11}$$

Similarly, we can write the SINR at the MN when the latter points its ULA to the n-th IRS while eavesdropping the k-th data stream, as

$$\mathrm{SINR}_{n,k,p}^{\mathrm{MN}} = \frac{q_k|\widetilde{\mathbf{b}}_{n,p}^{\mathsf{H}}\boldsymbol{\gamma}_{k,p}|^2}{\sum_{h\neq k} q_h|\widetilde{\mathbf{b}}_{n,p}^{\mathsf{H}}\boldsymbol{\gamma}_{h,p}|^2 + N_0 B}\,. \tag{12}$$

where $\boldsymbol{\gamma}_{k,p}$ is the k-th column of $\mathbf{\Gamma}_p$ whose expression is given by (10). The data rate for UE k under the p-map can be computed as

$$R(k,p) = B\log_2\left(1+\mathrm{SINR}_{k,p}^{\mathrm{UE}}\right). \tag{13}$$

Finally, the secrecy rate (SR) obtained when the MN eavesdrops the k-th stream by pointing its antenna to the n-th IRS, under the p-map, is given by

$$\mathrm{SR}(n,k,p) = \max\left\{0, R(k,p) - B\log_2(1+\mathrm{SINR}_{n,k,p}^{\mathrm{MN}})\right\} \tag{14}$$

The $\max$ operator in (14) is required since, under certain circumstances, $\mathrm{SINR}_{n,k,p}^{\mathrm{MN}}$ might be larger than $\mathrm{SINR}_{k,p}^{\mathrm{UE}}$.

D. Permutations and time

We define a set of IRS-to-UE assignments as a *permutation*; intuitively, each permutation corresponds to one way to serve the users. Given the set $\mathcal{P}$ of *all* possible permutations, the BS chooses a set $\bar{\mathcal{P}}$ of permutations to activate, as well as a criterion that legitimate nodes shall follow to determine the next permutation to move to. In other words, legitimate nodes will always know the next permutation to use (e.g., because they follow the same hash chain [19]), while the eavesdropper can not. We further assume that all chosen permutations are used with equal probability, and that they are notified to legitimate users in a secure manner, while the eavesdropper has no way of knowing the next permutation in advance. As noted earlier, hash chains allow to attain both goals.

Concerning time, we normalize everything to the time it takes to receivers (legitimate or not) to switch from one configuration to another, and call that one *time unit*. The BS also sets the number of time units the legitimate users should stay with each permutation. As for the eavesdropper, we consider the most unfavorable scenario for the legitimate users and assume that MN has already estimated the probability with which its victim is served by each IRS, and that it can leverage such information.

III. Problem Formulation and Solution Concept

In this section, we formulate the problem of optimizing the decisions made by the BS, i.e., the choice of the permutations to use and the time to wait before switching to the next permutation, in order to obtain the best possible secrecy rate *and* the required data rate.

Given the set $\mathcal{P}$ of permutations, we can indicate with $\nu_p(k) \in [1\dots N]$ the IRS used to serve user k under permutation p. We also know the rate $R(k,p)$, i.e., the rate experienced by user k under combination p, as well as $\mathrm{SR}(n,k,p)$, i.e., the secrecy rate obtained under permutation p when the victim is user k and the eavesdropper is listening to IRS n. Further, let $k^\star$ identify the eavesdropping victim.

Given $\mathcal{P}$, we have to decide which permutations to use, by setting binary variables $y(p) \in \{0,1\}$; also, let $\bar{\mathcal{P}} \subseteq \mathcal{P}$ be the set of used permutations. From the decisions $y(p)$, we can write the probability $\omega(k,n)$ that user k is served through IRS n under *any* of the chosen permutation, i.e.,

$$\omega(k,n) = \frac{\sum_{p\in\bar{\mathcal{P}}}\mathbb{1}_{[\nu_p(k)=n]}}{|\bar{\mathcal{P}}|}. \tag{15}$$

The second decision to make is the time $\tau \geq 1$ for which each permutation is applied before switching to a new one. If the time needed for switching permutation is equal to one time unit and the communication is paused during such switching time, (i.e., every $\tau+1$), the *average* rate for each legitimate user k is given by:

$$R_{\mathrm{avg}}(k) = \frac{\tau}{\tau+1}\frac{\sum_{p\in\bar{\mathcal{P}}}R(k,p)}{|\bar{\mathcal{P}}|}\,. \tag{16}$$

As expected, (16) tells us that having a small τ, i.e., switching between permutations too frequently, hurts the performance.

Moving to the eavesdropper, its objective is to have the smallest possible secrecy rate (SR) for its victim $k^\star$. There are two strategies it can follow towards this end:

- *static*: always pointing to the IRS that is most frequently used to serve the victim $k^\star$, i.e., $n^\star = \arg\max_n \omega(k^\star,n)$, or
- *dynamic*: "invest" δ time units to try all IRSs, identify the one serving the victim $k^\star$, and then point towards it.

In the first case, the resulting SR is given by:

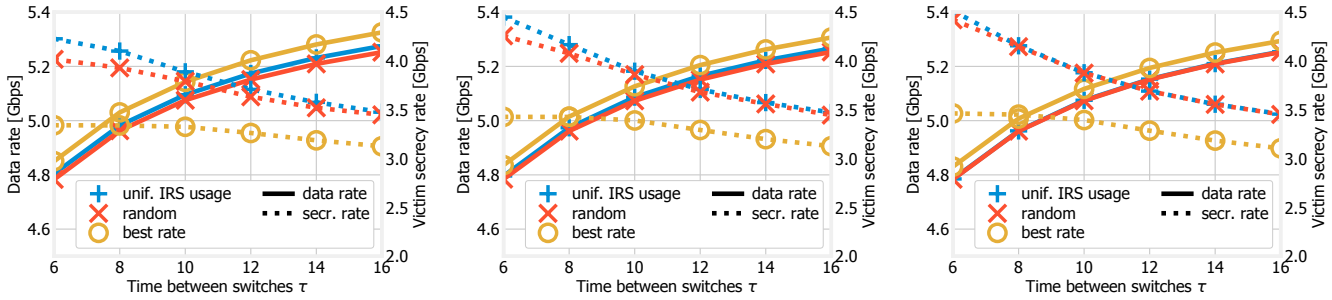
$$\mathrm{SR}_{\mathrm{avg}}^{\mathrm{static}}(k^\star) = \frac{1}{|\bar{\mathcal{P}}|}\sum_{p\in\bar{\mathcal{P}}}\mathrm{SR}(n^\star,k^\star,p)\,, \tag{17}$$

while in the latter case, the SR is:

$$\mathrm{SR}_{\mathrm{avg}}^{\mathrm{dynamic}}(k^\star) = \frac{1}{|\bar{\mathcal{P}}|}\sum_{p\in\bar{\mathcal{P}}}\left[\frac{\tau-\delta}{\tau}\min_n \mathrm{SR}(n,k^\star,p) + \frac{\delta R(k^\star,p)}{\tau}\right] \tag{18}$$

if $\delta \leq \tau$, and $\mathrm{SR}_{\mathrm{avg}}^{\mathrm{dynamic}}(k^\star) = \frac{1}{|\bar{\mathcal{P}}|}R(k^\star,p)$ otherwise.

The quantity within square brackets in (18) comes from the fact that, for each permutation (i.e., each τ time units), the eavesdropper spends δ units trying all IRSs (during which the secrecy rate will be $R(k^\star,p)$, i.e., complete secrecy), and $\tau-\delta$ units experiencing the minimum secrecy rate across all IRSs.



(a) (b) (c)

Fig. 3. Data rate (solid lines) and secrecy rate (dotted lines) as a function of the interval τ between permutation changes, under different strategies for choosing $\bar{\mathcal{P}}$, when the number of active permutations is $|\bar{\mathcal{P}}| = 5$ (a), $|\bar{\mathcal{P}}| = 10$ (b), and $|\bar{\mathcal{P}}| = 20$ (c).

In both cases, SR values are *subordinate to the fact that the BS is transmitting* – clearly, if there is no transmission, there can be no secrecy rate. Also notice how we must write SR values as dependent upon the eavesdropping victim $k^\star$: indeed, the eavesdropper knows who its victim is, while legitimate users do not.

The eavesdropper will choose the strategy that best suits it, i.e., results in the lowest secrecy rate. It follows that the resulting secrecy rate is:

$$\mathrm{SR}_{\mathrm{avg}}(k^\star) = \min\left\{\mathrm{SR}_{\mathrm{avg}}^{\mathrm{static}}(k^\star), \mathrm{SR}_{\mathrm{avg}}^{\mathrm{dynamic}}(k^\star)\right\}.$$

Our high-level goal is to maximize the secrecy rate, so long as all legitimate users get at least an average rate $R_{\min}$:

$$\max_{\bar{\mathcal{P}},\tau} \min_{k} \mathrm{SR}_{\mathrm{avg}}(k), \tag{19}$$

$$\text{s.t.} \quad R_{\mathrm{avg}}(k) \geq R_{\min}, \quad \forall k. \tag{20}$$

It is interesting to remark how objective (19) must be stated in a max-min form: indeed, since we do not know who the eavesdropping victim is, we want to optimize for the worst-case scenario in which the node with the lowest SR is indeed the victim.

IV. Performance Evaluation

In this section, we seek to characterize and understand the possible trade-offs between the data rate and secrecy rate, and how the decisions we make, i.e., the choice of $\bar{\mathcal{P}}$ and τ, influence both.

In order to obtain clear, easy-to-interpret results, we focus on a small scale scenario including:

- one BS, placed at coordinates $(0, 0)$, equipped with $M_{\mathrm{BS}} = 32$ antennas; in our setting the transmit power is $P_t = 30\,\mathrm{dBm}$, the signal wavelength $\lambda = 3\,\mathrm{mm}$, (corresponding to the carrier frequency $f_c = 100\,\mathrm{GHz}$), the signal bandwidth is $B = 1\,\mathrm{GHz}$, and $N_0 = -174\,\mathrm{dBm/Hz}$. Moreover, in (10) we set $\mathbf{Q} = \mathbf{I}_K$ so that all UEs experience the same SNR.
- $K = 4$ UEs, randomly distributed over a 10×10 m^2 surface, and equipped with $M_{\mathrm{UE}} = 4$ antennas;
- $N = 4$ IRSs of size 64×64 meta-atoms, randomly placed over the northern wall;
- an eavesdropper, randomly placed within 1 m from its intended victim, which is always UE 1 (i.e., $k^\star = 1$). The eavesdropper is also equipped with $M_{\mathrm{MN}} = 4$ antenna elements.

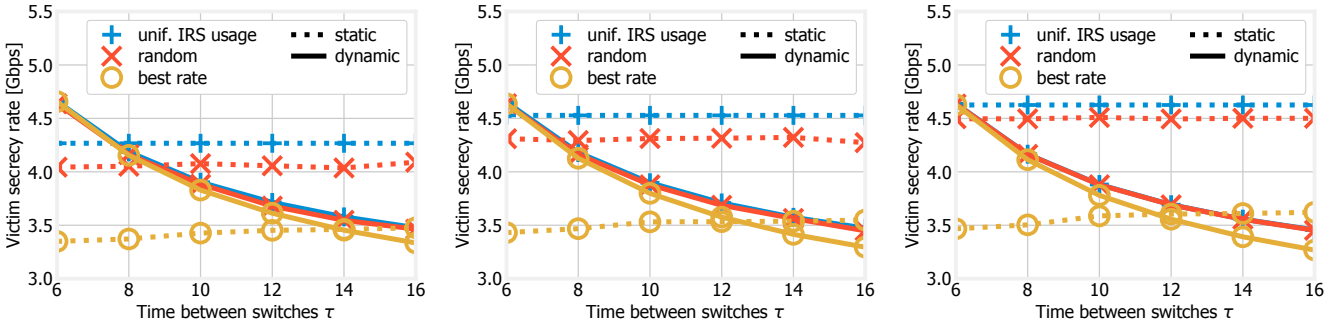
As $N = K = 4$, there are $|\mathcal{P}| = 4! = 24$ possible permutations. Since we assume that no direct LoS communication is possible between the BS and the UEs, each UE is always associated with an IRS that forwards to the UE the signal from the BS. Finally we conside $R_{\min} = 0$ and, for simplicity, ignore fading effects.

Throughout our performance evaluation, we compare the following approaches to choose the set $\bar{\mathcal{P}}$:

- **best rate**: the $|\bar{\mathcal{P}}|$ permutations with the highest data rate are selected;
- **uniform IRS usage**: the permutations are chosen so that each UE is served by each IRS with (approximately) the same probability, with ties broken by selecting the highest-rate permutation;
- **random**: permutations are chosen at random, with uniform probability.

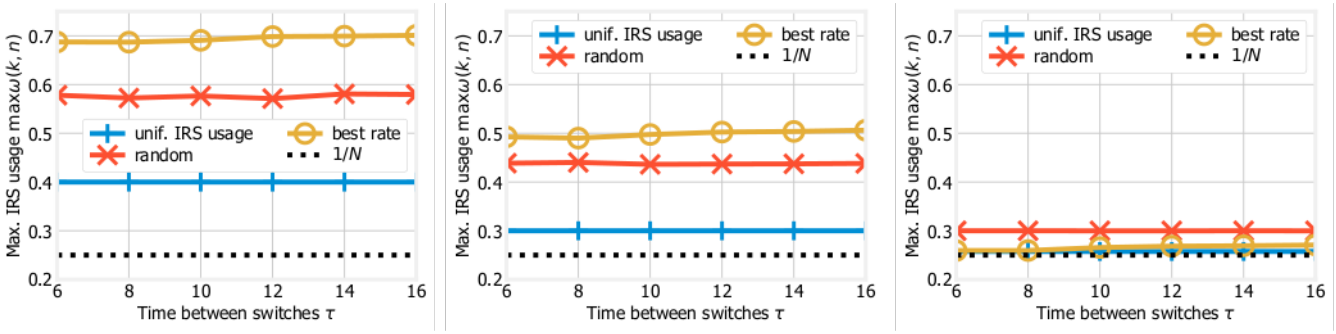
Figure 3 shows the data rate and secrecy rate, represented by solid and dotted lines respectively, as a function of the interval τ between configuration changes, and for different numbers of active permutations, i.e., different values of $|\bar{\mathcal{P}}|$. A first aspect we observe is that moving towards larger values of $|\bar{\mathcal{P}}|$, i.e., a higher number of active permutations, decreases the data rate while increasing the secrecy rate. The reason for the former effect can be seen from the expression of the average rate expression (16), which is maximum when only one permutation is active, namely, the one with the highest rate. Conversely, having more active permutations makes the work of the malicious node harder, hence, it results in a higher secrecy rate.

Furthermore, it is possible to see how the average rate (solid lines in the plots) increases for higher values of τ, i.e., when permutations are kept for a longer time. This is consistent with (16); intuitively, if the same network configuration is kept for a longer time, the effect of configuration switches is less significant. For similar reasons, the secrecy rate (dotted lines in the plots) decreases as τ increases: once the eavesdropper has identified the best IRS to point to, a higher value of τ



(a) (b) (c)

Fig. 4. Secrecy rate under the static (dotted lines) and dynamic (solid lines) strategies, as a function of the interval τ between permutation changes, under different approaches to choose $\bar{\mathcal{P}}$, when the number of active permutations is $|\bar{\mathcal{P}}| = 5$ (a), $|\bar{\mathcal{P}}| = 10$ (b), and $|\bar{\mathcal{P}}| = 20$ (c).



(a) (b) (c)

Fig. 5. Maximum IRS usage, i.e., $\max_{k,n} \omega(k,n)$ as a function of the interval τ between permutation changes, under different approaches to choose $\bar{\mathcal{P}}$, when the number of active permutations is $|\bar{\mathcal{P}}| = 5$ (a), $|\bar{\mathcal{P}}| = 10$ (b), and $|\bar{\mathcal{P}}| = 20$ (c).

means that it has more time to successfully intercept the communication.

Comparing the different approaches to choose $\bar{\mathcal{P}}$, it is possible to once more observe the intrinsic conflict between data rate and secrecy rate. The *best rate* approach results, predictably, in the highest data rate, but also in a very low secrecy rate. On the other hand, the *uniform IRS usage* approach yields a very good secrecy rate, at the cost of a data rate which barely exceeds that of *random*.

We now focus on the eavesdropper and its behavior. To this end, Figure 4 portrays the secrecy rate resulting from the two eavesdropping strategies discussed in Sec. III, namely, static (dotted lines) and dynamic (solid lines). It is clear that the dynamic strategy results in a very high secrecy rate when τ is small, i.e., permutations are changed frequently, and becomes more advantageous (for the eavesdropper) as τ increases. Such a behavior makes intuitive sense: the dynamic strategy is predicated on investing N time units to find out the best IRS to point to, and doing so is pointless if the configuration will change soon afterwards. As for the static strategy, the resulting secrecy rate does not depend, as per (17), upon τ, hence, its performance is relatively constant.

Interestingly, the value of τ for which the curves in Figure 4 overlap, i.e., the eavesdropper will move from the static to the dynamic strategy, depends upon the number $|\bar{\mathcal{P}}|$ of active permutation, as well as upon the approach followed to choose them. This further highlights the nontrivial way in which the decisions of the legitimate and malicious nodes interact, even in comparatively simple scenarios like the one we consider.

Last, Figure 5 depicts the maximum IRS usage, i.e., the quantity $\max_{k,n} \omega(k,n)$; such a quantity appears in (17), hence, it is linked to how strong the static strategy is. Intuitively, keeping $\max_{k,n} \omega(k,n)$ as low as possible makes the static strategy less beneficial for the eavesdropper; since, as per Figure 4, the static strategy is often the most effective, doing so has the potential to increase the overall secrecy rate, especially for low values of τ. Indeed, we can see from Figure 5 that the *uniform IRS usage* strategy results in the smallest maximum IRS usage, which correspond to the highest secrecy rates in Figure 3 and Figure 4.

This further confirms the notion emerging from our whole performance evaluation, namely, that selecting multiple active permutations and frequently switching between them is necessary to thwart the eavesdropper, however, both actions come at a price in terms of network performance, i.e., data rate. This, in turn, highlights the need for a deeper understanding of the effects of the decisions made by both the BS and the malicious nodes, and for algorithms able to leverage such insight.

V. Conclusions

We considered a base station transmitting towards users through the help of intelligent reflecting surfaces, and the presence of a passive eavesdropper overhearing the data stream destined to a legitimate user. To maximize the secrecy rate in the system, we proposed a solution that leverage the different possible IRS configurations and let IRS and legitimate users switch from one configuration to another with a given periodicity. Importantly, our scheme (i) exhibits low-complexity, (ii) is suitable for scenarios where the nodes have a limited number of antenna elements, and (iii) provides high secrecy rate at a small cost in terms of data rate degradation for legitimate users. Such results are attained thanks to our approach of studying the way IRSs are *used*, i.e., the users they will point to, as opposed to simply optimizing their coefficient disregarding their real-world meaning.

References

[1] J. Qiao and M.-S. Alouini, "Secure transmission for intelligent reflecting surface-assisted mmwave and terahertz systems," *IEEE Wireless Communications Letters*, vol. 9, pp. 16–32, 2020.

[2] I. F. Akyildiz, J. M. Jornet, and C. Han, "Terahertz band: next frontier for wireless communications," *Physical Communication*, vol. 12, pp. 16–32, 2014.

[3] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Communications Magazine*, pp. 106–112, January 2020.

[4] M. Di Renzo, M. Debbah, D.-T. Phan-Huy, A. Zappone, M.-S. Alouini, C. Yuen, V. Sciancalepore, G. C. Alexandropoulos, J. Hoydis, H. Gacanin *et al.*, "Smart radio environments empowered by reconfigurable ai meta-surfaces: An idea whose time has come," *EURASIP Journal on Wireless Communications and Networking*, 2019.

[5] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Communications Magazine*, 2018.

[6] C. Liaskos, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "Using any surface to realize a new paradigm for wireless communications," *Communications of the ACM*, 2018.

[7] M. Alsharif, A. K. amd M.A. Albreem, S. Chaudhry, M. Zia, and S. Kim, "Sixth generation (6g) wireless networks: Vision, research activities, challenges and potential solutions," *Symmetry*, vol. 12, no. 4:676, 2020.

[8] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," *arXiv preprint arXiv:1904.09573v3*, 2020.

[9] G. Zhou, C. Pan, H. Ren, K. Wang, A. Nallanathan, and K.-K. Wong, "User cooperation for irs-aided secure swipt mimo: Active attacks and passive eavesdropping," *arXiv preprint arXiv:2006.05347*, 2020.

[10] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Communications Letters*, 2020.

[11] A. Bereyhi, S. Asaad, R. R. Müller, R. F. Schaefer, and H. V. Poor, "Secure transmission in irs-assisted mimo systems with active eavesdroppers," *arXiv preprint arXiv:2010.07989*, 2020.

[12] L. Dong and H.-M. Wang, "Secure mimo transmission via intelligent reflecting surface," *IEEE Wireless Communications Letters*, 2020.

[13] A. Tarable, F. Malandrino, L. Dossi, R. Nebuloni, G. Virone, and A. Nordio, "Meta-Surface Optimization in 6G Sub-THz Communications," in *IEEE ICC Workshop on Terahertz Communications*, 2020.

[14] Y. Xing, O. Kanhere, S. Ju, and T. S. Rappaport, "Indoor wireless channel properties at millimeter wave and sub-terahertz frequencies," *IEEE Global Communications Conference*, 2019.

[15] M. Di Renzo, F. Habibi Danufane, X. Xi, J. de Rosny, and S. Tretyakov, "Analytical modeling of the path-loss for reconfigurable intelligent surfaces – anomalous mirror or scatterer ?" in *2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2020, pp. 1–5.

[16] Ö. Özdogan, E. Björnson, and E. G. Larsson, "Intelligent reflecting surfaces: Physics, propagation, pathloss modeling," *IEEE Wireless Communications Letters*, vol. 9, no. 5, 2020.

[17] M. Dunna, C. Zhang, D. Sievenpiper, and D. Bharadia, "Scattermimo: Enabling virtual mimo with smart surfaces," *MobiCom '20: Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, 2020.

[18] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network: Joint active and passive beamforming design," *IEEE Globecom*, pp. 1–6, 2018.

[19] S. Hussain, M. S. Rahman, and L. T. Yang, "Key predistribution scheme using keyed-hash chain and multipath key reinforcement for wireless sensor networks," in *IEEE PerCom*, 2009.