Safeguarding MIMO Communications with Reconfigurable Metasurfaces and Artificial Noise

George C. Alexandropoulos\textsuperscript{1}, Konstantinos Katsanos\textsuperscript{1}, Miaowen Wen\textsuperscript{2}, and Daniel B. da Costa\textsuperscript{3}

\textsuperscript{1}Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, Greece
\textsuperscript{2}School of Electronic and Information Engineering, South China University of Technology, China
\textsuperscript{3}Department of Computer Engineering, Federal University of Ceará, Brazil

E-mails: \{alexandg, kkatsan\}@di.uoa.gr, eemwwen@sccet.edu.cn, danielbcosta@ieee.org

Abstract—Wireless communications empowered by Reconfigurable Intelligent (meta)Surfaces (RISs) are recently gaining remarkable research attention due to the increased system design flexibility offered by RISs for diverse functionalities. In this paper, we consider a Multiple Input Multiple Output (MIMO) physical layer security system including one legitimate passive and one eavesdropping passive RIS with the former being transparent to the eavesdropper and the latter’s presence being unknown at the legitimate link. We first focus on the eavesdropping subsystem and present a joint design of the eavesdropper’s combining vector and the reflection coefficients of the eavesdropping RIS. Then, focusing on secrecy rate maximization, we propose a transmission scheme that jointly designs the legitimate precoding vector and Artificial Noise (AN) covariance matrix, as well as the reflection coefficients of the legitimate RIS. Our simulation results reveal that, in the absence of a legitimate RIS, AN and precoding are incapable of offering nonzero secrecy rates even for eavesdropping RISs with small numbers of unit elements. However, when a large-element legitimate RIS is deployed, confidential communication can be safeguarded against cases with even more than a 3L-element eavesdropping RIS.

Index Terms—Artificial noise, metasurfaces, MIMO, optimization, physical layer security, reconfigurable intelligent surfaces.

I. INTRODUCTION

Reconfigurable Intelligent (meta)Surfaces (RISs) have been recently envisioned as a revolutionary means to transform any passive wireless communication environment into an active reconfigurable one \cite{1, 2, 3}, offering increased environmental intelligence for diverse communication objectives. A RIS is an artificial planar structure with integrated electronic circuits \cite{4} that can be programmed to manipulate an incoming electromagnetic field in a wide variety of functionalities \cite{5, 6}. Among the various RIS-enabled objectives belongs the Physical Layer Security (PLS) \cite{7}, which is considered as a companion technology to conventional cryptography, targeting at significantly enhancing the quality of secure communication in beyond 5-th generation (5G) wireless networks.

One of the very first recent studies on RIS-enabled PLS systems is \cite{8}, which considered a legitimate Multiple Input Single Output (MISO) broadcast system, multiple eavesdroppers, and one RIS for various configurations for the reflections coefficients of its discrete unit elements. In that work, aiming at safeguarding legitimate communication, an alternating optimization approach for designing the RIS phase matrix and the legitimate precoder was presented together with a suboptimal scheme based on Zero Forcing (ZF) precoding that nulls information leakage to the eavesdroppers. In \cite{9}, the secrecy rate maximization problem was investigated for a RIS-empowered legitimate system comprising of a multi-antenna transmitter and a single-antenna receiver in the vicinity of an eavesdropper with multiple antenna elements. Efficient resource allocation algorithms for the case of multiple legitimate receivers and one eavesdropper were presented in \cite{10, 11, 12}. The MISO secrecy channel with the help of a single legitimate RIS was also considered in \cite{13} with the goal to minimize the transmit power subject to a constraint which keeps the secrecy rate above a target value. It was shown by means of computer simulations that RIS deployment leads to transmit power reservation. On the other hand, a new type of attack, termed as RIS jamming attack, was investigated in \cite{14}, according to which a passive RIS reflects jamming signals harming legitimate communication. The presented experimental results exhibited that the legitimate received signal can be downgraded up to 98%, witnessing that a RIS can be effectively used by the eavesdropping side for zero-power jamming.

All above recent studies indicate that RIS-empowered PLS systems are able to offer increased flexibility for both the legitimate and eavesdropping sides, enabling increased secrecy or jamming or cooperative jamming \cite{15} in efficient ways. In this paper, we study Multiple Input Multiple Output (MIMO) PLS systems with both legitimate and eavesdropping passive RISs. Focusing first on the eavesdropping subsystem, we present a joint design of the eavesdropper’s combining vector and the reflection coefficients of the eavesdropping RIS. Then, by formulating and solving a novel joint design problem for the legitimate subsystem, we propose a PLS transmission scheme incorporating legitimate precoding and Artificial Noise (AN), and passive beamforming from the legitimate RIS. Our simulation results demonstrate that AN and legitimate RIS can secure confidential communication over eavesdropping RISs with large numbers of unit elements.

Notation: Vectors and matrices are denoted by boldface lowercase and boldface capital letters, respectively. The transpose, conjugate, Hermitian transpose, and inverse of \(\mathbf{A}\) are denoted by \(\mathbf{A}^T\), \(\mathbf{A}^*\), \(\mathbf{A}^H\), and \(\mathbf{A}^{-1}\), respectively, and \(|\mathbf{A}|\) is the determinant of \(\mathbf{A}\), while \(\mathbf{I}_n\) \((n \geq 2)\) is the \(n \times n\) identity matrix and \(\mathbf{0}_{n \times m}\) \((n, m \geq 2)\) is a \(n \times m\) matrix with zeros. \(\text{Tr}(\mathbf{A})\) and
Eavesdropping RIS

\[
\begin{array}{c}
\text{A Unit Cells} \\
\text{G}_1 \\
\text{G}_2 \\
\text{E} \\
\text{K Antennas} \\
\text{H}_1 \\
\text{H}_2 \\
\text{RX} \\
\text{M Antennas} \\
\text{Legitimate RIS} \\
\text{L Unit Cells} \\
\text{BS} \\
\text{N Antennas} \\
\end{array}
\]

Fig. 1. The considered PLS system comprising of three multi-antenna nodes and two multi-element RISs, one serving the eavesdropper E and the other the legitimate BS-RX link. BS is assumed unaware of the existence of the eavesdropping RIS, the same is assumed for E regarding the legitimate RIS.

\[\mathbf{u}_{\text{max}}(\mathbf{A})\] represent A’s trace and eigenvector corresponding to its maximum eigenvalue, with notation \(\mathbf{A} \succ 0\) (\(A \succeq 0\)) means that the square matrix A is Hermitian positive definite (semi-definite). \([\mathbf{A}]_{i,j}\) is the \((i,j)\)-th element of \(\mathbf{A}\), \([\mathbf{a}]_i\) is \(a\)'s \(i\)-th element of \(\mathbf{a}\), \(\text{diag}[\mathbf{a}]\) denotes a square diagonal matrix with \(a\)'s elements in its main diagonal, and \(\nabla_{\mathbf{a}} f\) denotes the gradient vector of a scalar function \(f\) along the direction indicated by \(\mathbf{a}\). \(\mathbb{C}\) represents the complex number set, \(|a|\) denotes the amplitude of the complex scalar \(a\) and \(\arg(a)\) its phase, and \(\mathbb{E}\{\cdot\}\) is the expectation operator. \(\mathbf{x} \sim \mathcal{CN}(\mathbf{a}, \mathbf{A})\) indicates a complex Gaussian random vector with mean \(\mathbf{a}\) and covariance matrix \(\mathbf{A}\).

II. SYSTEM AND SIGNAL MODELS

The considered system model, as illustrated in Fig. 1, consists of a Base Station (BS) equipped with \(N\) antenna elements wishing to communicate in the downlink direction with a legitimate Receiver (RX) having \(M\) antennas. This downlink transmission is assumed to be further empowered by a legitimate RIS with \(L\) unit cells, which is placed close to RX. In the vicinity of the legitimate BS-RX link exists a \(K\)-antenna Eavesdropper (E) with an eavesdropping RIS of \(\Lambda\) unit elements close to it, that is intended for enabling legitimate information decoding at E’s side. We assume that the legitimate RIS is connected to the legitimate node via dedicated hardware and control signaling for online reconfigurability; the same holds for E and the eavesdropping RIS. The BS knows about the existence of E and focuses on securing its confidential link with RX; however, it is unaware of the presence of the eavesdropping RIS. It is also assumed that the deployment of the legitimate RIS is transparent to E.

We assume throughout this paper that perfect channel information is available at the BS and E sides via pilot-assisted channel estimation. Specifically, BS possesses the channels \(\mathbf{H} \in \mathbb{C}^{M \times N}\), \(\mathbf{H}_1 \in \mathbb{C}^{L \times N}\), and \(\mathbf{H}_2 \in \mathbb{C}^{M \times L}\) referring to the BS-RX, BS to legitimate RIS, and RX to legitimate RIS links, respectively. It is also assumed that BS and E cooperate in order to both estimate the BS-E channel \(\mathbf{H}_E \in \mathbb{C}^{K \times N}\) as follows: BS transmits pilot signals to E that estimates \(\mathbf{H}_E\) and then feeds this estimation back to BS. This cooperation may apply to the case where E plays the dual role of a legitimate receiver and of an eavesdropper. Recall that BS is unaware of the existence of the eavesdropping RIS, hence, it has no knowledge of the BS to eavesdropping RIS channel \(\mathbf{G}_1 \in \mathbb{C}^{L \times N}\) and the eavesdropping RIS to E channel \(\mathbf{G}_2 \in \mathbb{C}^{K \times L}\). However, the latter two channels are assumed available at the E side. We also assume that due to obstacles there are no actual channels between the legitimate RIS and E, and the eavesdropping RIS and RX. It is noted that channels where a RIS is involved can be estimated either at the RIS side with a single active hardware element [16] or via cascaded channel estimation with pilot reflection patterns at RIS [17]. In the case of an eavesdropping RIS as in [16], the BS pilots can be available to the RIS side for channel estimation from E that possesses them.

A. Received Signal Models and Secrecy Rate

To secure the confidentiality of the legitimate link, BS applies AN [13] that is jointly designed with the BS precoding vector \(\mathbf{v} \in \mathbb{C}^{N \times 1}\) and the legitimate RIS reflection (passive beamforming) vector \(\mathbf{\Phi}_L \triangleq [e^{j\theta_1}, e^{j\theta_2}, \ldots, e^{j\theta_L}]^T \in \mathbb{C}^{L \times 1}\), where \(\theta_l\) with \(l = 1, 2, \ldots, L\) denotes the phase shifting value at the \(l\)-th RIS unit element. We represent by \(\mathbf{x} \in \mathbb{C}^{N \times 1}\) the transmitted signal from the BS antenna elements, which is composed as \(\mathbf{x} \triangleq \mathbf{v}s + \mathbf{z}\), where \(s\) is the unit-amplitude complex-valued legitimate information symbol that is assumed independent from the AN vector \(\mathbf{z} \in \mathbb{C}^{N \times 1}\) having the covariance matrix \(\mathbf{Z} \triangleq \mathbb{E}\{\mathbf{zz}^H\}\). The baseband received signal vectors \(\mathbf{y}_{\text{RX}} \in \mathbb{C}^{M \times 1}\) and \(\mathbf{y}_E \in \mathbb{C}^{K \times 1}\) at the RX and E antenna elements can be mathematically expressed as

\[
\mathbf{y}_{\text{RX}} = (\mathbf{H} + \mathbf{H}_2\mathbf{\Phi}_L) (\mathbf{v}s + \mathbf{z}) + \mathbf{n}_{\text{RX}},
\]

\[
\mathbf{y}_E = (\mathbf{H}_E + \mathbf{G}_1\mathbf{\Psi}_1) (\mathbf{v}s + \mathbf{z}) + \mathbf{n}_E,
\]

where \(\mathbf{\Phi}_L \triangleq \text{diag}[\mathbf{\phi}] \in \mathbb{C}^{L \times L}\) and \(\mathbf{\Psi}_1 \triangleq \text{diag}[\mathbf{\psi}] \in \mathbb{C}^{L \times L}\) with \(\mathbf{\psi} \triangleq [e^{j\beta_1}, e^{j\beta_2}, \ldots, e^{j\beta_L}]^T \in \mathbb{C}^{L \times 1}\) being the eavesdropping RIS reflection vector in which \(\beta_k\) with \(k = 1, 2, \ldots, L\) represents the phase shifting value at the \(k\)-th RIS unit element. In the latter two expressions, \(\mathbf{n}_{\text{RX}} \sim \mathcal{CN}(0, \sigma_1^2\mathbf{I}_M)\) and \(\mathbf{n}_E \sim \mathcal{CN}(0, \sigma_2^2\mathbf{I}_K)\) stand for the Additive White Gaussian Noise (AWGN) vectors.

By assuming ideal capacity-achieving combining at RX and that E deploys the combining vector \(\mathbf{w} \in \mathbb{C}^{K \times 1}\) (to be explicitly designed later on), the achievable rates at the legitimate and eavesdropping links are given, respectively, by

\[
\mathcal{R}_{\text{RX}} \triangleq \log_2 \left| \mathbf{I}_M + \mathbf{H}_E\mathbf{v}\mathbf{v}^H\mathbf{H}_E^H \left( \sigma_2^2\mathbf{I}_M + \mathbf{H}_E\mathbf{Z}\mathbf{H}_E^H \right)^{-1} \right|,
\]

\[
\mathcal{R}_E \triangleq \log_2 \left( 1 + \frac{\mathbf{w}^H\mathbf{H}_E\mathbf{v}\mathbf{v}^H\mathbf{H}_E^H \mathbf{w}}{\mathbf{w}^H\mathbf{w} \left( \sigma_1^2\mathbf{I}_K + \mathbf{H}_E\mathbf{Z}\mathbf{H}_E^H \right)^{-1} \mathbf{w}} \right),
\]

where \(\mathbf{H}_E \triangleq \mathbf{H} + \mathbf{H}_2\mathbf{\Phi}_L\) and \(\mathbf{H}_E \triangleq \mathbf{H}_E + \mathbf{G}_1\mathbf{\Psi}_1\). The secrecy rate is then obtained as \(\mathcal{R}_s \triangleq \max(\mathcal{R}_{\text{RX}} - \mathcal{R}_E, 0)\).
Algorithm 1 Eavesdropping Design Solving $\mathcal{O}_{PE}$

1. **Input:** $n = 0$, $\epsilon > 0$, $\hat{\mathbf{H}}_E$, ZF precoder $\mathbf{v}$, feasible $\mathbf{w}^{(0)}$ and $\psi^{(0)}$, and $\mathcal{R}_E$ as defined in $\mathcal{O}_{PE}$.

2. for $n = 1, 2, \ldots$

3. Compute $\mathbf{H} = G_2 \text{diag}(\psi^{(n-1)}) \mathbf{G}_1$.

4. Given $\psi^{(n-1)}$, obtain $\mathbf{w}^{(n)} = \sigma^{-2} \mathbf{u}_{\text{max}}(\mathbf{H}_E \mathbf{vv}^H \mathbf{H}_E^H)$.

5. Using $\mathbf{w}^{(n)}$, obtain $[\psi^{(n)}]_k = [\mathbf{v}]_k/|[\mathbf{v}]_k| \forall k$.

6. if $\mathcal{R}^{(n)}_E - \mathcal{R}^{(n-1)}_E < \epsilon$, break; end if.

7. end for

8. **Output:** $\mathbf{w}^{(n)}$ and $\psi^{(n)}$.

B. Design of the Eavesdropping Parameters $\mathbf{w}$ and $\psi$

We assume that E is unaware of the fact that BS transmits the AN vector $\mathbf{z}$ and jointly designs $\mathbf{w}$ and $\psi$ profiting from the availability of the channels $\mathbf{H}_E$, $\mathbf{G}_1$, and $\mathbf{G}_2$. To this end, E considers that BS performs ZF precoding to null $\mathbf{H}_E$, as such, it assumes that its baseband received signal is given by $\mathbf{y}_E \triangleq \mathbf{G}_2 \mathbf{\Psi} \mathbf{G}_1 \mathbf{v}_E + \mathbf{n}_E$ (and not as in (2) including AN). It then formulates the following joint design optimization problem:

$$\mathcal{O}_{PE}: \max_{\mathbf{w}, \psi} \mathcal{R}_E \triangleq \log_2 \left(1 + \sigma^{-2} \mathbf{w}^H \mathbf{H}_E \mathbf{vv}^H \mathbf{H}_E^H \mathbf{w}\right)$$

s.t. $\mathbf{w}^H \mathbf{w} = 1$, $|\psi| = 1$ $\forall k = 1, 2, \ldots, \Lambda$,

where $\mathbf{H}_E \triangleq \mathbf{G}_2 \mathbf{\Psi} \mathbf{G}_1$. This problem focusing on maximizing E’s achievable rate (in the way E conceives this metric) is non-convex due to the coupled optimization variables in $\mathcal{R}_E$ and the unit-modulus constraints. To solve it, we adopt the following Alternating Optimization (AO) approach: $\mathbf{w}$ is obtained for fixed $\psi$, and then keeping the derived $\mathbf{w}$ fixed, the new $\psi$ is calculated; this approach is followed till the convergence of $\mathcal{O}_{PE}$’s objective. Keeping $\psi$ fixed in $\mathcal{O}_{PE}$ and removing the constraint for it, leads to an optimization problem over $\mathbf{w}$, which is solved as $\mathbf{w}_{\text{opt}} = \sigma^{-2} \mathbf{u}_{\text{max}}(\mathbf{H}_E \mathbf{vv}^H \mathbf{H}_E^H)$. Then, for fixed $\mathbf{w}$, the resulting optimization problem over $\psi$ can be shown to be solved with $[\psi_{\text{opt}}]_k = |[\mathbf{v}]_k/|[\mathbf{v}]_k| \forall k = 1, 2, \ldots, \Lambda$, where $\epsilon \triangleq \text{diag}(\mathbf{G}_1 \mathbf{v}^H \mathbf{G}_2^H \mathbf{w})$ [19]. The AO algorithm solving $\mathcal{O}_{PE}$ is summarized in Algorithm 1.

III. PROPOSED RIS-EMPPOWERED SECRECY DESIGN

According to the considered system model, BS lacks knowledge about the existence of an eavesdropping RIS. Hence, its believed baseband received signal at E given the availability of $\mathbf{H}_E$ at its side is $\mathbf{y}_E \triangleq \mathbf{H}_E (\mathbf{v}_E + \mathbf{z}) + \mathbf{n}_E$, instead of the actual signal in (2). Using the latter expression and assuming capacity-achieving combining at E, the BS formulates E’s achievable rate as the following function of $\mathbf{v}$ and $\mathbf{Z}$:

$$\mathcal{R}_E \triangleq \log_2 \left|\mathbf{I}_K + \mathbf{H}_E \mathbf{vv}^H \mathbf{H}_E^H \left(\sigma^2 \mathbf{I}_K + \mathbf{H}_E \mathbf{Z} \mathbf{H}_E^H\right)^{-1}\right|.$$  (5)

In this paper, we consider the following secrecy rate maximization problem for the joint design of the legitimate BS precoding vector $\mathbf{v}$ and AN covariance matrix $\mathbf{Z}$, and the reflection vector $\mathbf{\phi}$ of the legitimate RIS:

$$\mathcal{O}_{PL}: \max_{\mathbf{v}, \mathbf{v}^H \mathbf{Z} \mathbf{Z}^H} \mathcal{R}_E \triangleq \mathcal{R}_{RX} - \mathcal{R}_E$$

s.t. $\text{Tr}(\mathbf{vv}^H) + \text{Tr}(\mathbf{Z}) \leq P$, $|\mathbf{\phi}_{\ell}| = 1 \forall \ell = 1, 2, \ldots, L$,

where $P$ denotes the total transmit power budget. The latter joint design problem is solved via the following AO approach.

1) $\mathcal{O}_{PL}$’s optimization with respect to $\mathbf{v}$: By holding $\mathbf{\phi}$ and $\mathbf{Z}$ fixed in $\mathcal{O}_{PL}$ and applying the Sylvester’s determinant identity, the following design problem arises:

$$\mathcal{O}_{PL,\mathbf{v}}: \max_{\mathbf{v}} \left\{ \frac{1 + \mathbf{v}^H \tilde{\mathbf{H}} \mathbf{H} \left(\sigma^2 \mathbf{I}_M + \tilde{\mathbf{H}} \mathbf{Z} \mathbf{H}^H\right)^{-1} \mathbf{H} \mathbf{v}}{1 + \mathbf{v}^H \mathbf{H} \left(\sigma^2 \mathbf{I}_K + \mathbf{H} \mathbf{Z} \mathbf{H}^H\right)^{-1} \mathbf{H} \mathbf{v}} \right\},$$

where matrices $\mathbf{Y}_1, \mathbf{Y}_2 \in \mathbb{C}^{N \times N}$ are obtained as

$$\mathbf{Y}_1 \triangleq \frac{1}{P - \text{Tr}(\mathbf{Z})} \mathbf{I}_N + \mathbf{H} \mathbf{H}^H \left(\sigma^2 \mathbf{I}_M + \tilde{\mathbf{H}} \mathbf{Z} \mathbf{H}^H\right)^{-1} \mathbf{H},$$

$$\mathbf{Y}_2 \triangleq \frac{1}{P - \text{Tr}(\mathbf{Z})} \mathbf{I}_N + \mathbf{H} \mathbf{H}^H \left(\sigma^2 \mathbf{I}_K + \mathbf{H} \mathbf{Z} \mathbf{H}^H\right)^{-1} \mathbf{H}.$$  (7)

The optimal solution for the generalized Rayleigh quotient in $\mathcal{O}_{PL,\mathbf{v}}$ is given by

$$\mathbf{v}_{\text{opt}} = \sqrt{P - \text{Tr}(\mathbf{Z})} \mathbf{u}_{\text{max}} \left(\mathbf{Y}_2^{-1} \mathbf{Y}_1\right).$$  (8)

2) $\mathcal{O}_{PL}$’s optimization with respect to $\mathbf{Z}$: We define $\mathbf{Z} \in \mathbb{C}^{N \times N}$ such that $\mathbf{Z} = \mathbf{Z}^H$ and consider the following Lemma resulting from [20] for expressing $\mathcal{R}_E$ in an equivalent form.

**Lemma 1.** Suppose that $\mathbf{M} \in \mathbb{C}^{N \times N}$ with $\mathbf{M} \succeq 0$ is expressed as $\mathbf{M} = (\mathbf{ABC} - \mathbf{I}_N) (\mathbf{ABC} - \mathbf{I}_N)^H + \mathbf{ARA}^H$, where $\mathbf{A} \in \mathbb{C}^{N \times M}$, $\mathbf{B} \in \mathbb{C}^{M \times N}$, $\mathbf{C} \in \mathbb{C}^{N \times N}$, and $\mathbf{R} \in \mathbb{C}^{M \times M}$ with $\mathbf{R} \succ 0$. Let also the scalar function $f(\mathbf{S}, \mathbf{A}) \triangleq \log_2 |\mathbf{S} - \text{Tr}(\mathbf{S})| + N$ with $\mathbf{S} \in \mathbb{C}^{N \times N}$. The following maximum values for $f(\mathbf{S}, \mathbf{A})$ hold:

$$\log_2 |\mathbf{M}|^{\mathbf{1}} = \max_{\mathbf{S} \succ 0} f(\mathbf{S}, \mathbf{A}),$$

$$\log_2 |\mathbf{I}_N + (\mathbf{BC})^H \mathbf{R}^{-1} \mathbf{BC}| = \max_{\mathbf{S} \succ 0, \mathbf{A}} f(\mathbf{S}, \mathbf{A}),$$

where (9)’s value is obtained with the solution $\mathbf{S}_{\text{opt}} = \mathbf{M}^{-1}$.

We first make use of Sylvester’s determinant identity and Lemma 1 for $N = 1$ to re-express $\mathcal{R}_{RX}$ in $\mathcal{O}_{PL}$’s objective in the following form:

$$\mathcal{R}_{RX} = \max_{\mathbf{S} \succ 0, \mathbf{q}} (\log_2 (\mathbf{s} - \mathbf{s} \cdot 1)), \quad \text{for} \quad \mathbf{S} \succ 0, \mathbf{q},$$

$$\text{subject to} \quad \mathbf{S} = \mathbf{S}_{\text{opt}} = \mathbf{M}^{-1}.$$
where the unknown \( q \in \mathbb{C}^{M \times 1} \) denotes RX’s combining vector and \( m \triangleq \mathbb{E} \{ |q^H y_{RX} - s|^2 \} \) represents the symbol’s Mean Squared Error (MSE), which can be computed as

\[
m = |q^H \hat{H} v - 1|^2 + q^H (\sigma^2 I_M + \tilde{H} Z Z^H \tilde{H}) q.
\] (12)

In the sequel, we consider the following two formulas:

\[
\hat{R}_{E,1} = \log_2 |I_K + \sigma^{-2} H E \tilde{Z} Z^H H_E^H|,
\] (13)

\[
\hat{R}_{E,2} = \log_2 |I_K + \sigma^{-2} H E (v v^H + \tilde{Z} Z^H) H_E^H|.
\] (14)

After some straightforward manipulations, \( \hat{R}_E \) in OP_L’s objective can be re-expressed as \( \hat{R}_E = -\hat{R}_{E,1} + \hat{R}_{E,2} \). Based on Lemma 1, \( \hat{R}_{E,1} \) and \( \hat{R}_{E,2} \) can be re-written as:

\[
\hat{R}_{E,1} = \max_{s_1 > 0} (\log_2 |s_1| - \text{Tr}(s_1 M) + N),
\] (15)

\[
-\hat{R}_{E,2} = \max_{s_2 > 0} (\log_2 |s_2| - \text{Tr}(s_2 (I_K + \sigma^{-2} H E (v v^H + \tilde{Z} Z^H) H_E^H) + K)),
\] (16)

where \( M = (A^H H_E \tilde{Z} - I_N) (A^H H_E \tilde{Z} - I_N)^H + \sigma^2 A^H A \), \( s_1 \in \mathbb{C}^{N \times N} \) and \( s_2 \in \mathbb{R}^{K \times K} \). By using (11), (15), and (16), the desired optimization with respect to \( Z \) and the introduced auxiliary variables is expressed as follows:

\[
\text{OP}_{L,X} : \begin{array}{c}
\max_{Z} \quad \hat{R}_X \triangleq \hat{R}_{RX} + \hat{R}_{E,1} - \hat{R}_{E,2} \\
\text{s.t.} \quad \text{Tr}(\tilde{Z} Z^H) \leq P - \text{Tr}(v v^H),
\end{array}
\]

where set \( \mathcal{X} \triangleq \{\tilde{Z}, q, A, s > 0, s_1 > 0, s_2 > 0\} \). It can be shown that \( \text{OP}_{L,X} \) is not jointly convex, but it is convex with respect to the block of variables \( \{q, A\}, \{s, s_1, s_2\}, \) and \( Z \).

We next solve this problem with an AO-based approach.

**Optimizing \( \text{OP}_{L,X} \) with respect to \( \{q, A\} \):** For fixed \( \{s, s_1, s_2\}, \) \( A \), and \( Z \), the following problem is deduced

\[
\begin{aligned}
\text{OP}_{L,q} : \quad & \max_{q} \quad (q^H H v v^H H q - q^H \hat{H} v - v^H \hat{H} q) \\
& \quad + q^H \tilde{H} Z Z^H \tilde{H}^H q + \sigma^2 q^H q,
\end{aligned}
\]

which is solved by equating to zero its first-order partial derivative with respect to \( q^* \), yielding

\[
q_{opt} = (\sigma^2 I_M + \tilde{H} v v^H \tilde{H} + \tilde{H} Z Z^H \tilde{H}^H)^{-1} H v.
\] (17)

Following a similar procedure for the optimization with respect to \( A \)’s, results in the following optimal solution:

\[
A_{opt} = (\sigma^2 I_K + H E \tilde{Z} Z^H H_E^H)^{-1} H E \tilde{Z}.
\] (18)

**Optimizing \( \text{OP}_{L,X} \) with respect to \( \{s, s_1, s_2\} \):** By substituting (17) into (12), the MSE for \( s \) at RX is given by

\[
m = 1 - v^H \hat{H} \left( \sigma^2 I_M + \tilde{H} (v v^H + \tilde{Z} Z^H) \hat{H}^H \right)^{-1} H v.
\] (19)

which, after applying the matrix inversion lemma, it yields

\[
s_{opt} = 1 + \sigma^{-2} v^H \hat{H} \left( I_M + \sigma^{-2} \tilde{H} Z Z^H \hat{H} \right)^{-1} H v.
\] (20)

In a similar manner, we set \( s_1 = M^{-1} \) in (15). Then by substituting \( A_{opt} \) given in (13), we have that:

\[
S_{1,opt} = I_N + \sigma^{-2} \tilde{H} H_E^H H E \tilde{Z}.
\] (21)

The optimum \( S_2 \) is obtained in an analogous way as

\[
S_{2,opt} = \left( I_K + \sigma^{-2} (H E (v v^H + \tilde{Z} Z^H) H_E^H) \right)^{-1}.
\] (22)

**Optimizing \( \text{OP}_{L,X} \) with respect to \( \tilde{Z} \):** The objective of this problem can be re-expressed as the following function of \( \tilde{Z} \):

\[
\hat{R}_{\tilde{Z}} = -\text{Tr}(H E A S_1 A^H H E \tilde{Z} Z^H) \\
+ \lambda \text{Tr}(H E A S_1 Z^H) \\
+ \lambda \text{Tr}(S_1 A^H H E \tilde{Z} Z^H) - \sigma^2 \text{Tr}(H E S_1 S_2 H E \tilde{Z} Z^H),
\]

which leads to the following maximization problem:

\[
\text{OP}_{L,Z} : \quad \max_{Z} \hat{R}_{\tilde{Z}} \quad \text{s.t.} \quad \text{Tr}(\tilde{Z} Z^H) \leq P - \text{Tr}(v v^H).
\]

The Lagrangian function for the latter problem is derived as

\[
\mathcal{L}(\tilde{Z}, \lambda) = \hat{R}_{\tilde{Z}} - \lambda \left( \text{Tr}(\tilde{Z} Z^H) - P + \text{Tr}(v v^H) \right),
\]

with \( \lambda \geq 0 \) being the Lagrange multiplier. By setting to zero its first-order derivative with respect to \( \tilde{Z} \), results in

\[
\hat{Z}_{opt} = (\lambda I_N + D^{-1}) H E A S_1,
\] (25)

where \( D \triangleq s \tilde{H} H q q^H H + H E A S_1 A^H H E + \sigma^2 H E S_2 H E \).

To finally guarantee convergence of \( \text{OP}_{L,Z} \)’s solution to a Karush-Kuhn-Tucker point and satisfy the complementary slackness condition, we solve the following dual problem:

\[
\text{OP}'_{L,Z} : \quad \min_{\lambda \geq 0} \left( \max_{\tilde{Z}} \mathcal{L}(\tilde{Z}, \lambda) \right),
\] (26)

where the inner problem is solved by (25). The outer problem can be efficiently solved via the bisection method.

**3) \( \text{OP}_L \)’s optimization with respect to \( \phi \):** The optimization variable \( \phi \) in \( \text{OP}_L \) appears only in the legitimate rate \( \hat{R}_X \).

By omitting the logarithm from the \( \hat{R}_X \) expression, we define the following function of \( \phi \):

\[
C_{RX} \triangleq v^H (H + H_F H_1) H (H + H_F H_1) v,
\]

where \( P \triangleq (\sigma^2 I_M + (H + H_F H_1) Z (H + H_F H_1)^H)^{-1} \).

Then, by applying basic algebraic manipulations, the \( \text{OP}_L \) with respect to \( \phi \) becomes equivalent to

\[
\text{OP}_{L,\phi} : \quad \max_{\phi} C_{RX}, \quad \text{s.t.} \quad |\phi| = 1 \forall \ell = 1, 2, \ldots, L,
\]

where the objective \( C_{RX} \) is defined as

\[
C_{RX} = \text{Tr}(H v v^H H^H P) + \text{Tr}(H_1 v v^H H^H PH_2) \\
+ \text{Tr}(H v v^H H^H P H_2^H P) + \text{Tr}(H_2 H_1 v v^H H^H \Phi^H H^H P).
\] (28)

The \( \text{OP}_{L,\phi} \) is non-convex with unit-modulus constraints, which solve via a Projected Gradient Ascent (PGA)
Algorithm 2 Proposed Secrecy Design Solving $\mathcal{OP}_L$.

1: **Input:** $n = 0$, $\epsilon, \mu > 0$, $H$, $H_L$, feasible $\mathbf{v}^{(0)}$, $Z^{(0)}$, $\phi^{(0)}$ and $R_s^{(0)}$ as defined in $\mathcal{OP}_L$.
2: **for** $n = 1, 2, \ldots$
3: 3: Update $\mathbf{v}^{(n)}$ according to (8).
4: 4: Given $\mathbf{v}^{(n)}$, compute $q$, $A$, $s_i$, $S_1$, and $S_2$ using (17), (18), (20), (21), and (22), respectively.
5: 5: Solve $\mathcal{OP}_L^{(n)}$ in (26) and set $Z^{(n)} = Z^{(0)}(Z^{(n)})_H$.
6: 6: Solve $\mathcal{OP}_L^{(n)}, \varphi$ using the PGA algorithm to obtain $\phi^{(n)}$.
7: 7: **if** $R_s^{(n)} - R_s^{(n-1)} < \epsilon$, **break**; **end if**.
8: **end for**
9: **Output:** $\mathbf{v}^{(n)}$, $Z^{(n)}$, and $\phi^{(n)}$.

algorithm similar to [21]. To this end, we first compute the gradient vector $\forall \ell = 1, 2, \ldots, L$ as $\nabla \phi_{\mathbf{c}_L} = \sum_{j=1}^L [F_j]_{\ell} \epsilon$ with

$$F_1 = -H_j^H P \mathbf{H} \mathbf{v}^H \mathbf{H}^H P \mathbf{H} \mathbf{\varphi},$$

$$F_2 = -H_j^H P \phi H_j \mathbf{v}^H \mathbf{H}^H P \mathbf{\varphi},$$

$$F_3 = H_j^H P \mathbf{v}^{H} \mathbf{H}^H \phi_1^H - H_j^H P \mathbf{H} \mathbf{v}^{H} \mathbf{H}^H \phi_2^H \mathbf{\varphi},$$

$$F_4 = H_j^H P \phi_1 \mathbf{H} \mathbf{v}^{H} \mathbf{H}^H \phi_1^H - H_j^H P \phi_2 \mathbf{H} \mathbf{v}^{H} \mathbf{H}^H \phi_2^H \mathbf{\varphi},$$

where $\mathbf{\varphi} \triangleq \mathbf{H} \mathbf{Z}^H \mathbf{H} + \mathbf{H}_L \mathbf{\Phi}_L \mathbf{Z} \mathbf{H}^H \mathbf{L}$. For the latter derivations, we have used the rule $\partial (\mathbf{M}^{-1}) = -\mathbf{M}^{-1} (\partial \mathbf{M}) \mathbf{M}^{-1}$. It is noted that each $F_j$ corresponds to (28)’s $j$-th summand. Then, $\phi$ is computed via the following iterative procedure: by using a random feasible initialization $\phi^{(1)}$, the $\phi^{(i+1)}$ at the $(i+1)$-th iteration of the PGA algorithm is obtained from the $\phi^{(i)}$ of the $i$-th iteration as

$$\phi^{(i+1)} = \phi^{(i)} + \mu \nabla \phi^{(i)} \mathbf{c}_L^T,$$

$$\phi^{(i+1)} = \exp \left( j \arg \left( \phi^{(i+1)} \right) \right),$$

where $\mu > 0$ denotes the algorithmic step size.

All previously presented algorithmic steps solving $\mathcal{OP}_L$ for the proposed RIS-empowered joint secrecy design of $\phi$, $\mathbf{v}$, and $Z$ are summarized in Algorithm 2.

IV. NUMERICAL RESULTS AND DISCUSSION

In this section, we investigate the secrecy rate performance of the proposed PLS scheme over frequency flat Rayleigh fading channels with zero mean and unit variance, and for distance-dependent pathloss with exponent equal to 2 for all involved links. We have particularly evaluated the achievable rates of the legitimate and eavesdropping links using expressions (3) for $R_{\text{RX}}$ and (4) for $R_{\text{E}}$, respectively, and $R_s$ providing the achievable secrecy rate. In the results that follow, we have considered that $E$ adopts the proposed RIS-empowered design presented in Section III-E including receive combining. For the legitimate system, we have used the proposed PLS scheme in Section III encompassing BS precoding, AN, and legitimate RIS passive beamforming, as well as a special version of it for the case where a legitimate RIS is not available. For this special version, we have solved a similar problem to $\mathcal{OP}_L$, via Lemma 1 and AO, by removing the links involving the legitimate RIS and the optimization over its relevant variable $\phi$. In our simulations, the BS was located in the origin of the $xy$ plane, whereas RX and E lied on a circle of radius $10m$ in the angles $45^\circ$ and $85^\circ$, respectively, from BS. The first unit element of the eavesdropping RIS was placed in the middle of the line connecting RX and E, and the other elements expand along the positive directions of the $x$ and $y$ axes. In a similar manner, the legitimate RIS is placed in the same circle as RX and E in the angle $20^\circ$ from BS. In addition, we have used the following parameter setting: $N = \{8, 32\}$, $K = 4$, $L = 50$, $\sigma^2 = 1$, and 1000 independent Monte Carlo realizations.

We commence in Fig. 2 with the achievable rate performance in bps/Hz for the legitimate and eavesdropping links as functions of the BS transmit SNR, defined as $P/\sigma^2$. For these results, we have considered that the legitimate system does not include a RIS, and targets at securing confidential transmissions with only BS precoding and AN. It can be seen from both subfigures that the rates increase with increasing SNR for both the legitimate and eavesdropping links. In the left subfigure for $N = 8$ BS antennas, it is depicted that RX’s rate is larger than E’s rate for $\Lambda = 20$, however, when the larger simulated values for $\Lambda$ are considered, E’s rate is similar or larger than that of RX. This reveals that, with the proposed schemes for RX and E, the secrecy rate equals to 0 for cases of existence of an eavesdropping RIS with $\Lambda > 60$ unit elements. For such cases, BS precoding and AN are incapable of safeguarding the legitimate link. In the right subfigure of Fig. 2 we have set the BS antennas as $N = 32$. Interestingly, the increase in $N$ results in improvement of both the legitimate and the eavesdropping rates, implying that the eavesdropping RIS can even in this case enable information stealth. This is
Fig. 3. Achievable secrecy rates in bps/Hz versus the transmit SNR in dB for \( N = 8 \) antenna elements at the legitimate BS, \( L = 50 \) unit elements at the legitimate RIS, and different numbers \( \Lambda \) for the unit elements of the eavesdropping RIS. In contrast to Fig. 2, the legitimate system safeguards communication with BS precoding, AN, and RIS passive beamforming.

particularly true for \( \Lambda = 100 \) resulting in secrecy rate equal to 0. The latter behavior happens due to the fact that BS is unaware of the eavesdropping RIS’s presence possessing only \( \mathbf{H}_E \) for its joint design. Increasing \( N \) can improve the secrecy rate, but only for eavesdropping RISs with small number of elements. Note that \( \Lambda \) can be much higher than \( N \).

In Fig. 3, we consider that the legitimate system deploys a RIS with \( L = 50 \) unit elements and applies the joint design of Section III. We have plotted the achievable secrecy rates in bps/Hz versus the transmit SNR in dB for the case where the BS antennas are set to \( N = 8 \), and for different numbers \( \Lambda \) for the unit elements of the eavesdropping RIS. It is obvious that for all considered \( \Lambda \) values, the resulting secrecy rates are positive implying the feasibility of secure communication. Clearly, the closer to the value \( L = 50 \) the value of \( \Lambda \) is, the larger is the secrecy rate, which for all cases increases with increasing transmit SNR. This reveals that the adoption of even a small-sized legitimate RIS provides security guarantees over RIS-empowered eavesdropping systems. As an example from Fig. 3 a legitimate RIS with \( L = 50 \) yields positive secrecy rates even when \( \Lambda = 180 \), i.e., for an eavesdropping RIS with \( 3 \times \) more unit elements.

V. CONCLUSION

In this paper, we studied RIS-empowered PLS systems, where RISs are deployed from both the legitimate and the eavesdropping subsystems. We focused on the case where the RISs are placed close to the receivers and their existence is unknown to the competing system. A joint design of legitimate precoding, AN, and legitimate RIS passive beamforming was presented that was shown to be capable of safeguarding MIMO communication over RIS-empowered eavesdropping systems.

REFERENCES

[1] C. Liaskos, S. Nie, A. I. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. F. Akyildiz, “A new wireless communication paradigm through software-controlled metasurfaces,” IEEE Commun. Mag., vol. 56, no. 9, pp. 162–169, Sep. 2018.
[2] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, “Reconfigurable intelligent surfaces for energy efficiency in wireless communication,” IEEE Trans. Wireless Commun., vol. 18, no. 8, pp. 4157–4170, Aug. 2019.
[3] 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.
[4] N. Kaina, M. Dupre, G. Lerosey, and M. Fink, “Shaping complex microwave fields in reverberating media with binary tunable metasurfaces,” Sci. Rep. 4, pp. 1–7, Article No 076401, 2014.
[5] M. D. Renzo, M. Debbah, D.-T. Phan-Huy, A. Zappone, M.-S. Alouini, C. Yuen, V. Sciancalepore, G. C. Alexandropoulos, J. Hoiydis, H. Gacanin, J. de Rosny, A. Bounceu, G. Lerosey, and M. Fink, “Smart radio environments empowered by AI reconfigurable meta-surfaces: An idea whose time has come,” EURASIP J. Wireless Commun. Netw., vol. 129, pp. 1–20, May 2019.
[6] C. Huang, S. Hu, G. C. Alexandropoulos, A. Zappone, C. Yuen, R. Zhang, M. D. Renzo, and M. Debbah, “Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends,” IEEE Wireless Commun., to appear, 2020.
[7] 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.
[8] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, “Intelligent reflecting surface: A programmable wireless environment for physical layer security,” IEEE Access, vol. 7, pp. 82599–82612, Jul. 2019.
[9] 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.
[10] 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.
[11] 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 GLOBECOM, Waikoloa, USA, Dec. 2019, pp. 1–6.
[12] X. Yu, D. Xu, and R. Schober, “Enabling secure wireless communications via intelligent reflecting surfaces,” in Proc. IEEE GLOBECOM, Waikoloa, USA, Dec. 2019, pp. 1–6.
[13] Z. Chu, W. Hao, F. Xiao, and J. Shi, “Intelligent reflecting surface aided multi-antenna secure transmission,” IEEE Wireless Commun. Lett., vol. 9, no. 1, pp. 108–112, Jan. 2020.
[14] B. Lyu, D. T. Hoang, S. Gong, D. Niyato, and D. I. Kim, “IRS-based wireless jamming attacks: When jammers can attack without power,” [online] https://arxiv.org/abs/2001.08963, 2020.
[15] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, “Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis,” IEEE Trans. Veh. Technol., vol. 66, no. 8, pp. 7495–7505, Aug. 2017.
[16] G. C. Alexandropoulos and E. Vlachos, “A hardware architecture for reconfigurable intelligent surfaces with minimal active elements for explicit channel estimation,” in Proc. IEEE ICASSP, Barcelona, Spain, May 2020, pp. 9175–9179.
[17] D. Mishra and H. Johansson, “Channel estimation and low-complexity beamforming design for passive intelligent surface assisted MISO wireless energy transfer,” in Proc. IEEE ICASSP, Brighton, UK, May 2019, pp. 4659–4663.
[18] Y. Liu, L. Li, G. C. Alexandropoulos, and M. Pesavento, “Securing relay networks with artificial noise: An error performance based approach,” MDPI Entropy 19, no. 8: 384, pp. 7495–7505, Jul. 2017.
[19] M. Soltanian and P. Stoica, “Designing unimodular codes via quadratic optimization,” IEEE Trans. Sig. Proc., vol. 62, no. 5, pp. 1221–1234, Mar. 2014.
[20] O. Shi, M. Razaviyayn, Z.-Q. Luo, and C. He, “An iteratively weighted MMSE approach to distributed sum-utility maximization for a MIMO interfering broadcast channel,” IEEE Trans. Signal Process., vol. 59, no. 9, pp. 4331–4340, Sep. 2011.
[21] Q. Nadeem, A. Kammoun, A. Chaaban, M. Debbah, and M. Alouini, “Asymptotic Max-Min SINR analysis of reconfigurable intelligent surface assisted MISO systems,” IEEE Trans. Wireless Commun., to appear, 2020.