Poster: Multi-Receiver Physical Layer Security Using Reconfigurable Intelligent Surfaces

Simone Marrocco*, Paolo Casari*†, Michele Segata*†
*Department of Information Engineering and Computer Science – University of Trento, Italy †CNIT, Italy

***Abstract*— Physical layer security (PLS) aims at introducing security and privacy mechanisms directly at the signal level, as an additional measure on top of what is provided by higher layers. One recent approach proposes to exploit reconfigurable intelligent surfaces (RISs) to enhance signal quality towards an intended receiver while generating disrupting interference towards a potential eavesdropper. Existing approaches consider single receiver/single RIS scenarios in a simplified setting, making it difficult to evaluate the actual applicability of the approach. In this work we extend the existing model to work with multiple receivers and multiple RISs discussing secrecy characteristics in the spatial domain, rather than for a single eavesdropper. Our results show the applicability of our extended approach together with the limitations of using passive RISs compared to active ones, as well as highlighting the challenges related to mobility.**

I. Using RIS for Physical Layer Security

As the number of devices interacting with each other wirelessly is continuously growing, cybersecurity attacks pose more and more threats. Considering future connected autonomous vehicles (CAVs), the concerns are even higher, as security issues can directly affect passenger safety. For this reason, modern crypto and privacy technique try to secure communication starting from the lowest possible layer of the stack, i.e., protecting the signal through physical layer security (PLS) techniques. In this section, we introduce this concept and the background necessary to understand our approach.

In particular, our proposal is based on the work in [1], where the authors study different communication schemes that would allow for secure non line of sight (NLOS) communication using reconfigurable intelligent surfaces (RISs), that would also act as artificial noise against eavesdroppers.

We will focus here on the Space Shift Keying (SSK) modulation scheme [2], where we use the antenna index as the only mean to relay information. In particular, [1] considers a transmitter Alice, a legitimate receiver Bob, and an eavesdropper Eve each with K antennas, and a RIS with N reflecting elements creating a virtual line of sight (LOS) between Alice and Bob. Eve receives both the LOS signal together with the one reflected from the RIS. By modeling with $\boldsymbol{H}$, $\boldsymbol{G}$, $\boldsymbol{B}$, and $\boldsymbol{F}$, the channels between Alice and the RIS, the RIS and Bob, Alice and Eve, and the RIS and Eve, respectively, the received signals at Bob and Eve are

$$\boldsymbol{y}_{\text{Bob}} = \boldsymbol{GPHx} \in \mathbb{C}^K, \quad \boldsymbol{y}_{\text{Eve}} = \boldsymbol{Bx} + \boldsymbol{FPHx} \in \mathbb{C}^K, \tag{1}$$

where $\boldsymbol{x} \in \mathbb{C}^K$ is the transmitted signal, a vector where only one element is non zero, $\boldsymbol{p} \in \mathbb{C}^N$ is the configuration of the RIS, and $\boldsymbol{P} = \text{diag}(\boldsymbol{p})$ is the reflection matrix. The objective is finding a RIS configuration $\boldsymbol{p}$ that allows the communication channel gain matrix $\boldsymbol{GPH}$ to be diagonal by solving

$$||\boldsymbol{GPH} - [\boldsymbol{GPH}]_{\text{diag}}||^2 = 0, \tag{2}$$

where $||\cdot||$ denotes the Frobenius norm and $[\cdot]_{\text{diag}}$ the operator that sets the elements that are not located on the diagonal to 0. The solution is obtained by solving $\boldsymbol{p}^\dagger \boldsymbol{W} \boldsymbol{p} = 0$, where

$$\boldsymbol{W} = \sum_{i=1}^{K} \sum_{k=1, i \neq k}^{K} (\boldsymbol{g}_{k,*} \odot \boldsymbol{h}_{*,i}^\intercal)^\dagger (\boldsymbol{g}_{k,*} \odot \boldsymbol{h}_{*,i}^\intercal) \in \mathbb{C}^{N \times N} \tag{3}$$

with $\boldsymbol{g}_{k,*}, \boldsymbol{h}_{*,i}^\intercal \in \mathbb{C}^N$ being the k-th row and the i-th column of $\boldsymbol{G}$ and $\boldsymbol{H}$, respectively, $\odot$ the element-wise product, and $(\cdot)^\intercal$ and $(\cdot)^\dagger$ being the classic and the Hermitian transpose, respectively. The solutions to $\boldsymbol{p}^\dagger \boldsymbol{W} \boldsymbol{p} = 0$ can be obtained by finding the null-space of $\boldsymbol{W}$, in particular by exploiting the singular value decomposition $\boldsymbol{W} = \boldsymbol{R\Sigma V}^\intercal$ and taking the submatrix $\boldsymbol{U} \in \mathbb{C}^{N \times N - K^2 + K}$ made by the last $N - K^2 + K$ columns of $\boldsymbol{R} \in \mathbb{C}^{N \times N}$.

Finally, we can choose any non-zero linear combination of the columns of $\boldsymbol{U}$ as configuration $\boldsymbol{p}$, in particular by choosing any random vector $\boldsymbol{q} \neq \boldsymbol{0} \in \mathbb{C}^{N-K^2+K}$ and computing

$$\boldsymbol{p} = \frac{\eta}{||\boldsymbol{Uq}||_\infty} \boldsymbol{Uq} \tag{4}$$

where $\eta \in (0, 1]$ denotes the the reflection efficiency, and $||\cdot||_\infty$ is the infinity norm, used to normalize the vector $\boldsymbol{p}$.

II. Multi-RIS and Multi-receiver Security

The approach we describe in Sect. I is limited to a single receiver and a single RIS. Yet, in a typical CAV scenario a vehicle might be willing to communicate with multiple receivers and exploiting multiple RISs. In this section, we expand the existing work to consider such scenario.

In particular, assuming J receivers and a single RIS, we now have J channel matrices $\boldsymbol{G}_j$ from the RIS to each receiver. The system we want to solve now is

$$||\boldsymbol{G}_j \boldsymbol{PH} - [\boldsymbol{G}_j \boldsymbol{PH}]_{diag}||^2 = 0, \quad \forall j \in \{1, \ldots, J\} \tag{5}$$

As before, we want to solve $\boldsymbol{p}^\dagger \boldsymbol{W} \boldsymbol{p} = 0$, this time with

$$\left[\boldsymbol{W}_1^\intercal, \ldots, \boldsymbol{W}_J^\intercal\right]^\intercal = \boldsymbol{W} = \boldsymbol{R\Sigma V}^\dagger \in \mathbb{C}^{JN \times N} \tag{6}$$

$$\boldsymbol{W}_j = \sum_{i=1}^{K} \sum_{k=1, i \neq k}^{K} (\boldsymbol{g}_{jk,*} \odot \boldsymbol{h}_{*,i}^\intercal)^\dagger (\boldsymbol{g}_{jk,*} \odot \boldsymbol{h}_{*,i}^\intercal) \in \mathbb{C}^{N \times N}, \tag{7}$$

where $\boldsymbol{g}_{jk,*}$ is the k-th row of $\boldsymbol{G}_j$.

The problem is that now $\boldsymbol{R} \in \mathbb{C}^{JN \times JN}$ and, using the same methodology as in Sect. I, would result in a configuration $\boldsymbol{p} \in \mathbb{C}^{JN}$. We can instead take a different approach using $\boldsymbol{U}_1 \in \mathbb{C}^{N - J(K^2-K) \times N}$, i.e., the last $N - J(K^2 - K)$ rows of $\boldsymbol{V}^\dagger \in \mathbb{C}^{N\times N}$ and taking $\boldsymbol{U} = \boldsymbol{U}_1^\dagger \in \mathbb{C}^{N\times N-J(K^2-K)}$, applying again Eq. (4).

To consider M RISs chained together in series, we also need to take into account the channel gains $\boldsymbol{C}_m \in \mathbb{C}^{N\times N}$ between RIS m and $m+1$. Our system becomes

$$||\boldsymbol{G}\boldsymbol{P}_1\boldsymbol{C}_1...\boldsymbol{P}_M\boldsymbol{H} - [\boldsymbol{G}\boldsymbol{P}_1\boldsymbol{C}_1...\boldsymbol{P}_M\boldsymbol{H}]_{diag}||^2 = 0. \quad (8)$$

We can configure the first $M-1$ RISs by randomly choosing their configuration vectors $\boldsymbol{p}_1, ..., \boldsymbol{p}_{M-1}$, and then compute $\boldsymbol{p}_M$ as in the multiple receivers case. More formally define

$$\boldsymbol{G}' = \boldsymbol{G}\boldsymbol{P}_1\boldsymbol{C}_1...\boldsymbol{P}_{M-1}\boldsymbol{C}_{M-1} \in \mathbb{C}^{K\times N} \quad (9)$$

and then solve

$$||\boldsymbol{G}'\boldsymbol{P}_M\boldsymbol{H} - [\boldsymbol{G}'\boldsymbol{P}_M\boldsymbol{H}]_{diag}||^2 = 0. \quad (10)$$

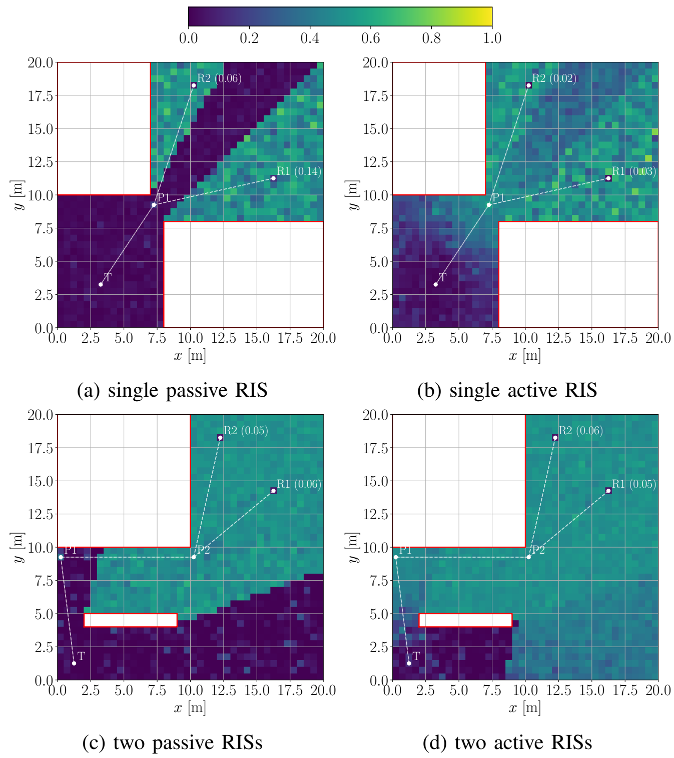
III. Performance evaluation

We evaluate the performance of our proposed method using spatial bit error rate (BER) heatmaps. In particular we consider two scenarios with different geometries, creating LOS and NLOS zones. In both of them we consider two receivers. In the first one, we use a single RIS, while in the second one we use two to create a double reflection. To compute the heatmap, we consider an area of $20\,\mathrm{m}^2$, computing the BER inside such area with a resolution of $50\,\mathrm{cm}$. For the LOS, we consider a free space path loss model with a path loss exponent $\alpha = 2$. For NLOS conditions, we consider for active RISs only the free space path loss from the last RIS to the receiver, and for passive RISs both the free space path loss from RIS to receiver, from RIS to RIS and from transmitter to RIS. On top of the path loss, we consider a Rayleigh fading with Scale parameter $\xi = 1.0$ and Shape parameter $\tau = 0.6$ between each pair of communicating actors antennas. Finally, we consider a fixed signal to noise ratio (SNR) of $10\,\mathrm{dB}$, evaluating the BER for passive and active RISs. In the former case, the RIS simply reflects the signal resulting in a double path loss [3], while in the latter we assume the RIS to be retransmitting the signal with the same power as the original transmitter.

Fig. 1 shows the BER heatmaps for the different scenarios considered. Starting from Fig. 1a (single passive RIS) we can draw several conclusions. First, our proposed approach works very well towards the intended receivers. Indeed they lie within a dark blue square, indicating that the BER for them is very close to zero. Moreover, we can observe the secrecy introduced around them, as the nearby area has a BER around 0.5, which corresponds to random guessing. Second, we can see the limitations of using passive RIS, as the reflection is not strong enough to disturb the signal in area where there is direct LOS with the transmitter. Noise from multiple passive RISs is still not enough, as shown in (Fig. 1c).

Considering the same scenario but with active RIS (Fig. 1b), we see an improvement in secrecy. Eavesdroppers with direct LOS to the transmitter still get BER close to 0.5, depending on the distance from both the transmitter and the RISs.

Considering the scenario with multiple RISs (Figs. 1c and 1d) the conclusions are similar. The approach works very well also with multiple RISs, but with a better secrecy when considering active surfaces as we are able to cover a much bigger area.



(a) single passive RIS

(b) single active RIS

(c) two passive RISs

(d) two active RISs

Figure 1. Spatial heatmap of the BER for SNR$=10\,\mathrm{dB}$ and $K=4$ for single RIS, $K=2$ for two RISs.

IV. Conclusions and future work

This work has shown the feasibility of RIS-based PLS for multiple receivers and RISs, together with showing the spatial secrecy properties. In all results we observed that the area with low BER around the receivers is very small. On one hand, this is very good for secrecy but, on the other, it means that ensuring secrecy under mobility might be challenging. While our contribution is effective for stationary antennas, further research is needed to expand our work for mobile actors. One solution might be using such an approach when vehicles are stationary, e.g., when stopped at an intersection, to securely set up a protected channel and then use standard cryptographic techniques, or finding ways to predict channel gains of moving objects. Finally, we plan to extend our approach to consider multiple RIS reflections in parallel.

Acknowledgments

This work was financed by the European Union - NextGenerationEU - National Recovery and Resilience Plan (NRRP) - Mission 4 Component 2 Investment 1.3 - Cascade Call by "SERICS - Security and Rights in CyberSpace", "PRECODE project - Privacy Enhanced Communications for Cooperative Driving Environments" (PE00000014 - CUP C69J24000330008).

References

[1] J. Luo et al., "Reconfigurable Intelligent Surface: Reflection Design Against Passive Eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 20, no. 5, May 2021.

[2] J. Jeganathan et al., "Space shift keying modulation for MIMO channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, Jul. 2009.

[3] M. Segata et al., "CoopeRIS: A framework for the simulation of reconfigurable intelligent surfaces in cooperative driving environments," *Elsevier Computer Networks*, vol. 248, Jun. 2024.