# Exploiting Reconfigurable Intelligent Surfaces to Achieve Multi-Receiver Physical Layer Security

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

***Abstract*— Secure and private communications can be made possible by operating at different levels of the communication stack. One possibility is to work directly at the physical layer, with physical layer security (PLS) techniques. In this work, we propose a PLS-based approach towards secure and private communications, in particular by exploiting reconfigurable intelligent surfaces (RISs). By properly tuning the configuration of the RISs it is possible to enable communication with a set of intended receivers while making the signal unintelligible in nearby areas. This work shows the effectiveness of the approach, while also highlighting its limitations and the challenges that need to be tackled for realizing it in practice.**

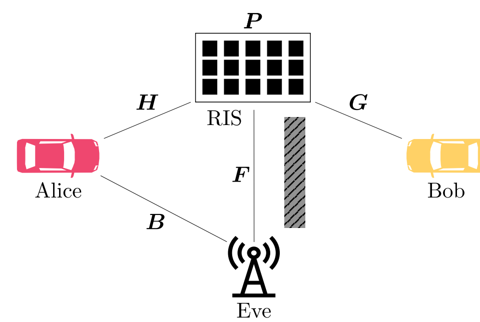



Figure 1. Communication scenario.

## I. Introduction and Related Work

As the number of wireless devices continues to rise, the risk of cybersecurity attacks becomes increasingly worrying. This concern is especially critical for future connected autonomous vehicles (CAVs), where security breaches could directly compromise the safety of passengers and road users. To address this, modern cryptographic and privacy methods aim to secure communications already at teh lowest levels of the protocol stack, i.e., working directly at the signal level through an approach known as physical layer security (PLS).

PLS can support different security functions, such as authentication, secret key generation, and integrity checks by relying on pseudo-random signal features that are observable by legitimate parties while being partly secret to attackers. For example, an attacker could impersonate a legitimate network node by compromising a cryptographic key that was assumed to be sufficiently strong. However, the received signal power or other features of the wireless communication channel can tell a receiver that a transmission the data is coming from a different device [1].

Signal-level characteristics are tightly related to communication devices, and can be exploited to intrude the users' privacy by localizing or tracking the movement of network devices. It has been suggested to alter the signal prior to transmitting it, in order to make localization ineffective and defend from such attacks. For example, one approach is to artificially change the power of orthogonal frequency-division multiplexing (OFDM) subcarriers so that an attacker cannot localize a transmitter through channel state information (CSI) [2]. This approach relies on the fact that the receiver would in any case equalize subcarriers to correct for the channel's frequency selectivity, hence limited artificial changes to subcarrier power do not prevent the receiver from decoding the signal.

In this work, we try to enforce both privacy and security by making the signal "spatially understandable," meaning that the signal should be correctly decoded within an area of limited size around the intended receiver, while being perceived as random noise elsewhere. For this, we exploit reconfigurable intelligent surfaces (RISs). which can reflect wireless signals towards an intended direction [3] or even towards multiple receivers [4], enabling communication behind obstacles such as buildings. The working principle is the same as in beamforming, i.e., using multiple antennas with different phase-amplitude configurations to point beams towards certain directions. The only difference is that RISs reflect impinging signals, either passively or actively (i.e., by amplifying the outgoing signal).

In this work, we exploit RISs for a different purpose than mere coverage extension. RISs, by design, modify the characteristics of a signal to improve reception but, in the same way, it can be used to disrupt it for eavesdroppers. In the same vein, we can improve the received signal quality at an intended device, while making the signal look like random noise to a malicious listener [5]. In particular, the work in [5] provides a very important first analysis of the above use of RISs, albeit limited to a single-RIS, single-receiver scenario. In this work we extend the approach to consider multiple RISs and, most importantly, multiple receivers. In particular, Sect. II introduces the necessary background, Sect. III describes our contribution considering multiple RISs and receivers, while Sect. IV presents the performance evaluation of our approach.

## II. RIS-enabled Physical Layer Security

In this section we review the work in [5] to provide the necessary background, and then extend the approach to consider multiple receivers and multiple RISs. Tab. I summarizes the notation and the operators used throughout the paper.

Wit reference to the scenario in Fig. 1, we consider a transmitter Alice, a legitimate receiver Bob, and a malicious eavesdropper Eve. We assume all of them to have the same

Table I
MATHEMATICAL NOTATION AND OPERATORS.

| Symbol | Meaning |
|---|---|
| $\boldsymbol{x}, \boldsymbol{y}$ | Transmitted and received signals |
| $\boldsymbol{B}, \boldsymbol{F}, \boldsymbol{G}, \boldsymbol{H}$ | Channel matrices (see Eq. (1)) |
| $\boldsymbol{p}, \boldsymbol{P}$ | RIS configuration vector and matrix, $\boldsymbol{P} = \text{diag}(\boldsymbol{p})$ |
| $K$ | Number of antennas |
| $N$ | Number of RIS reflecting elements |
| $\|\|\cdot\|\|$ | Frobenius norm: $\|\|A_{N\times M}\|\|= \sqrt{\sum_{i=1}^{N}\sum_{j=1}^{M}\|a_{i,j}\|^2}$ |
| $\|\|\cdot\|\|_\infty$ | Infinity norm: $\|\|\boldsymbol{x}\|\|_\infty = \max_i \|\boldsymbol{x}_i\|$ |
| $[\cdot]_{\text{diag}}$ | Diagonalization operator: $([A]_{\text{diag}})_{i,j} = a_{i,j}$ if $i = j, 0$ otherwise |
| $\odot$ | element-by-element product |
| $(\cdot)^\intercal, (\cdot)^\dagger$ | Classic and Hermitian (conjugate) transpose |
| $\boldsymbol{g}_{i,*},\ \boldsymbol{g}_{*,j}$ | $i$-th row and $j$-th column of matrix $\boldsymbol{G}$ |

number of antennas $K$. We also assume that Alice and Bob are not connected by a line of sight (LoS) link, whereas Eve can be located anywhere. A RIS with $N$ reflecting elements is available to create a virtual LoS path between Alice and Bob.

The modulation used for communications is Space Shift Keying (SSK) [6], which uses the index of one of the $K$ antennas as the mean to encode information. The receiver decodes the data by looking at which of its antennas receives a signal and which ones do not. $K$ antennas can thus encode $\log_2(K)$ bits.

Continuing the description of Fig. 1, each pair of communicating actors is characterized by a channel gain matrix, which describes the channel gain between each pair of antennas between the two actors. As shown in the picture, we model channel gain matrices with letters $\boldsymbol{H}$, $\boldsymbol{G}$, $\boldsymbol{B}$, $\boldsymbol{F}$, as summarized below:

$$\begin{aligned} &\text{Alice} \xrightarrow{\boldsymbol{H}} \text{RIS}, \quad \text{Alice} \xrightarrow{\boldsymbol{B}} \text{Eve}, \\ &\text{RIS} \xrightarrow{\boldsymbol{G}} \text{Bob}, \quad \text{RIS} \xrightarrow{\boldsymbol{F}} \text{Eve}. \end{aligned} \tag{1}$$

Define with $\boldsymbol{x} \in \mathbb{C}^K$ the signal transmitted by Alice. As we are using SSK, $\boldsymbol{x}$ is a vector with a single non-zero element. Moreover, call $\boldsymbol{p} \in \mathbb{C}^N$ and let $\boldsymbol{P} = \text{diag}(\boldsymbol{p})$ be the reflection matrix modeling the action of the RIS. Under this configuration, the signals received by Bob and Eve are

$$\boldsymbol{y}_{\text{Bob}} = \boldsymbol{GPHx} \in \mathbb{C}^K, \quad \boldsymbol{y}_{\text{Eve}} = \boldsymbol{Bx} + \boldsymbol{FPHx} \in \mathbb{C}^K, \tag{2}$$

where we remark that Bob only receives the signal reflected by the RIS, while Eve could receive both the direct LoS signal, if it exists, and the reflected one.

Assuming the channel matrices $\boldsymbol{H}$ and $\boldsymbol{G}$ are known, the objective is to find a configuration $\boldsymbol{p}$ for the RIS that makes $\boldsymbol{GPH}$ a diagonal matrix, with no element on the diagonal equal to 0. To understand why, recall that using the SSK modulation scheme means that only one element of the transmit vector $\boldsymbol{x}$ is not 0. More formally,

$$\exists!\, i \in \{1, \dots, K\} : \boldsymbol{x}_i \neq 0. \tag{3}$$

If $\boldsymbol{GPH}$ is diagonal, Eq. (3) holds for $\boldsymbol{y}_{\text{Bob}}$ as well, and the index of the non-zero element will be the same as in $\boldsymbol{x}$, enabling Bob to decode the data.

To diagonalize $\boldsymbol{GPH}$ we can solve

$$\|\boldsymbol{GPH} - [\boldsymbol{GPH}]_{\text{diag}}\|^2 = 0, \tag{4}$$

whose solution can be obtained by solving $\boldsymbol{p}^\dagger \boldsymbol{W} \boldsymbol{p} = 0$, where

$$\boldsymbol{W} = \sum_{i=1}^{K} \sum_{k=1, i\neq k}^{K} (\boldsymbol{g}_{k,*} \odot \boldsymbol{h}_{*,i}^\intercal)^\dagger (\boldsymbol{g}_{k,*} \odot \boldsymbol{h}_{*,i}^\intercal) \in \mathbb{C}^{N\times N}. \tag{5}$$

In Eq. (5), the inner part is a dyadic matrix, where column vector $(\boldsymbol{g}_{k,*} \odot \boldsymbol{h}_{*,i}^\intercal)$ is pre-multiplied by its own conjugate-transpose version.

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 $\boldsymbol{W} = \boldsymbol{R\Sigma V}^\dagger$ and taking the sub- matrix $\boldsymbol{U} \in \mathbb{C}^{N\times N-K^2+K}$ 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

$$\boldsymbol{p} = \frac{\eta}{\|\boldsymbol{Uq}\|_\infty} \boldsymbol{Uq} \tag{6}$$

where $\eta \in (0, 1]$ denotes the the reflection efficiency. The division by $\|\boldsymbol{Uq}\|_\infty$ normalizes the vector $\boldsymbol{p}$.

## III. CONSIDERING MULTIPLE RECEIVERS AND RISS

The approach we describe in Sect. II considers a single receiver and a single RIS but there might be scenarios, especially considering CAVs, where a single transmission might be addressed to multiple receivers. In the following we extend the work in [5] to account for such possibility.

### A. Multiple Receivers, Single RIS

We start by considering a single RIS and $J$ receivers. Call $\boldsymbol{G}_j$ the channel matrix from the RIS to receiver $j$. The system in Eq. (4) can now be rewritten as

$$\|\boldsymbol{G}_j\boldsymbol{PH} - [\boldsymbol{G}_j\boldsymbol{PH}]_{\text{diag}}\|^2 = 0, \quad \forall j \in \{1, \dots, J\} \tag{7}$$

We again find a solution by solving $\boldsymbol{p}^\dagger \boldsymbol{W} \boldsymbol{p} = 0$, but now $\boldsymbol{W}$ is defined as

$$\begin{bmatrix} \boldsymbol{W}_1 \\ \vdots \\ \boldsymbol{W}_J \end{bmatrix} = \boldsymbol{W} = \boldsymbol{R\Sigma V}^\dagger \in \mathbb{C}^{JN\times N} \tag{8}$$

with

$$\boldsymbol{W}_j = \sum_{i=1}^{K} \sum_{k=1, i\neq k}^{K} (\boldsymbol{g}_{jk,*} \odot \boldsymbol{h}_{*,i}^\intercal)^\dagger (\boldsymbol{g}_{jk,*} \odot \boldsymbol{h}_{*,i}^\intercal) \in \mathbb{C}^{N\times N}. \tag{9}$$

The slightly different notation from Tab. I for $\boldsymbol{g}_{jk,*}$ simply indicates the $k$-th row of $\boldsymbol{G}_j$.

To find the configuration $\boldsymbol{p} \in \mathbb{C}^N$, however, we have to take a different approach than the one in Sect. II, because $\boldsymbol{R} \in \mathbb{C}^{JN\times JN}$. Therefore, we cannot take the last columns as the dimensions do not match, and would result in a configuration $\boldsymbol{p} \in \mathbb{C}^{JN}$. We solve the issue by taking the last $N - J(K^2 - K)$ rows of $\boldsymbol{V}^\dagger \in \mathbb{C}^{N\times N}$ and define

$$\boldsymbol{U}_1 \in \mathbb{C}^{N-J(K^2-K)\times N} \tag{10}$$

Then simply consider $\boldsymbol{U} = \boldsymbol{U}_1^\dagger \in \mathbb{C}^{N\times N-J(K^2-K)}$ and apply again Eq. (6) to obtain $\boldsymbol{p}$.

### B. Multiple Receivers, Multiple RISs

We now extend the previous case by considering $M$ RISs, assuming them to be chained together in series. For this we need to define the channel gains between each pair of consecutive RISs. In particular $\boldsymbol{C}_m \in \mathbb{C}^{N\times N}$ denotes the channel gain between RIS $m$ and $m+1$, so for a specific receiver $j$, the communication chain would look as follows:

$$\text{Alice} \xrightarrow{\boldsymbol{H}} \text{RIS}_1 \xrightarrow{\boldsymbol{C}_1} \dots \xrightarrow{\boldsymbol{C}_{M-1}} \text{RIS}_M \xrightarrow{\boldsymbol{G}_j} \text{Bob}_j. \quad (11)$$

We start by considering the case in Eq. (11), i.e., where all receivers receive the signal from the last RIS in the chain only. We then extend the approach to get rid of this simplifying assumption.

In particular, for receiver $j$ we can rewrite Eq. (7) as

$$||\boldsymbol{G}_j\boldsymbol{P}_M\boldsymbol{C}_{M-1}...\boldsymbol{P}_1\boldsymbol{H} - [\boldsymbol{G}_j\boldsymbol{P}_M\boldsymbol{C}_{M-1}...\boldsymbol{P}_1\boldsymbol{H}]_{\text{diag}}||^2 = 0, \quad \forall j \in \{1,\dots,J\} \quad (12)$$

If the receivers are only hearing the last RIS, we can simply 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. In this way, the intermediate RISs will contribute in creating artificial noise. We can thus define

$$\boldsymbol{H}' = \boldsymbol{C}_{M-1}\boldsymbol{P}_{M-1}\dots\boldsymbol{C}_1\boldsymbol{P}_1\boldsymbol{H}, \quad (13)$$

as a channel gain matrix considering the random configurations and then solving as before

$$||\boldsymbol{G}_j\boldsymbol{P}_M\boldsymbol{H}' - [\boldsymbol{G}_j\boldsymbol{P}_M\boldsymbol{H}']_{\text{diag}}||^2 = 0, \forall j \in \{1,\dots,J\}. \quad (14)$$

In general we can also have situations where receivers are not all necessarily connected to the last RIS in che chain. In this case, instead of randomly configuring $\boldsymbol{p}_1,...,\boldsymbol{p}_{M-1}$, we can iteratively calculate the RISs configurations for those connected to a receiver, and then use such vectors instead of the random configurations to compute the next ones in the line.

More formally, define $r(j)$ as the index of the RIS in the chain that serves receiver $j$, and order the receivers so that $j=0$ corresponds to the first served receiver in the chain of RISs. As in Eq. (13), we define

$$\boldsymbol{H}_0 = \boldsymbol{C}_{r(0)-1}\boldsymbol{P}_{r(0)-1}\dots\boldsymbol{C}_1\boldsymbol{P}_1\boldsymbol{H}, \quad (15)$$

which can be solved similarly to Eq. (14), i.e.,:

$$||\boldsymbol{G}_0\boldsymbol{P}_{r(0)}\boldsymbol{H}_0 - [\boldsymbol{G}_0\boldsymbol{P}_{r(0)}\boldsymbol{H}_0]_{\text{diag}}||^2 = 0. \quad (16)$$

**Note:** The only difference with respect to Eqs. (7), (8) and (10) is that the number of receivers $J$ does not refer to the total, but to the number of receivers served by the RIS we are specifically solving Eq. (16) for.

We then continue with the next RIS, i.e., considering the first receiver $i > j$ such that $r(i) \neq r(j)$. We can then generalize the approach defining

$$\boldsymbol{H}_i = \boldsymbol{C}_{r(i)-1}\boldsymbol{P}_{r(i)-1}\dots\boldsymbol{C}_1\boldsymbol{P}_1\boldsymbol{H}, \quad (17)$$

and solving

$$||\boldsymbol{G}_i\boldsymbol{P}_{r(i)}\boldsymbol{H}_i - [\boldsymbol{G}_i\boldsymbol{P}_{r(i)}\boldsymbol{H}_i]_{\text{diag}}||^2 = 0 \quad (18)$$

for all receivers $i$ served by RIS $r(i)$. For all intermediate RISs not serving any receiver, the configuration can be picked at random as before.

Table II
SIMULATION PARAMETERS.

| Parameter | Value |
|---|---|
| $K$ | 4 (number of antennas) |
| $N$ | 36 (number of RIS elements) |
| $\alpha$ | 2 (LoS path loss exponent) |
| $\xi$ | 1 (Rice scale parameter) |
| $\tau$ | 0.6 (Rice shape parameter) |
| $K$ | Number of antennas |
| $N$ | Number of RIS reflecting elements |
| SNR | $10\,\text{dB}$ |
| Scenario size | $20\,\text{m} \times 20\,\text{m}$ |
| Scenario resolution | $50\,\text{cm} \times 50\,\text{cm}$ |
| BER trials | 1000 per spatial point |

## IV. PERFORMANCE EVALUATION

We evaluate our approach by means of spatial bit error rate (BER) heatmaps. We consider three scenarios with different geometries leading to LoS and non line of sight (NLoS) areas. In the three scenarios we consider different configurations:

**Scenario I:** Single RIS with two receivers;

**Scenario II:** Two RISs with two receivers, both receivers served by the second RIS;

**Scenario III:** Three RISs with five receivers, one served by the first RIS, two served by the second RIS, and two served by the third one.

We consider an area of $20\,\text{m}^2$ and overlay a grid of square elements having $50\,\text{cm}$ of side length. For each grid element, we compute the BER enabled by RIS-aided communications. To compute the received signal strength, we model LoS conditions via a free space path loss model with an exponent $\alpha = 2$. To model reflections we consider both passive and active RISs. For passive RISs, the signal is simply reflected as-is by the surface, and we compute the total path loss as the product of all linear-scale losses from the transmitter up to the final receiver. This method is referred to as "product of distances" in [4]. For active RISs, we assume that the signal is re-amplified by the surface, hence we compute the path loss only between the each receiver and the RIS that serves it. In areas where we receive multiple signals (e.g., both by the transmitter and a RIS), we simply sum them, as per Eq. (2).

On top of path loss, between each antenna and each reflecting element on the RIS we consider a Rice fading with scale $\xi = 1.0$ and shape $\tau = 0.6$. To obtain the heatmap, we compute the BER by repeating a simulation 1000 times per grid element. In each repetition, for a specific point, we observe the received signal $\boldsymbol{y}$ and we chose as active antenna the one with the highest received power. The BER is then computed depending on the bits that have been correctly decoded. For example, assume that with $K = 4$ antennas we encode:

Antenna 0 $\rightarrow$ 00 Antenna 1$\rightarrow$ 01
Antenna 2 $\rightarrow$ 10 Antenna 3$\rightarrow$ 11

If we transmit $\boldsymbol{x} = [1,0,0,0]^\intercal$ and receive $\boldsymbol{y} = [0.39, 0.92, 0, 0]^\intercal$, we wrongly choose Antenna 1. Thus, the second bit is wrong, and the BER is 0.5.

Finally, on top of each received vector $\boldsymbol{y}$, we consider a fixed signal to noise ratio (SNR) of $10\,\mathrm{dB}$ using additive white gaussian noise (AWGN). Tab. II summarizes the simulation parameters. The code used for the performance evaluation is available online as open source softwar e.[1]

Fig. 2 shows the BER heatmaps for all the three scenarios, for passive (left panels) and active RISs (right panels). Starting from Scenario I with passive RIS (Fig. 2a), we can observe that the approach works as intended, as receivers lie within dark blue squares, indicating a low BER. We remark that the BER values (e.g., $8\,\%$ for the intended receiver) are in line with the ones of the original work in [5]. Moreover, we emphasize that we are altering channel characteristics for security reasons, and the final goal is being capable of defending against eavesdroppers, not low BER or high spectral efficiency. In fact, the yellow areas around the two unintended receivers correspond to a high BER, about 0.5. Fig. 2a also shows the limitation of passive RISs. In areas where both the transmitter and the RIS signals are received, the direct LoS from the transmitter is too strong for the RIS to create any significant interference.

If we look at active RISs instead (Fig. 2b), secrecy improves on a much larger area. Eavesdroppers with direct LoS to the transmitter still experience high BER, while the BER for intended receivers remains unaltered.

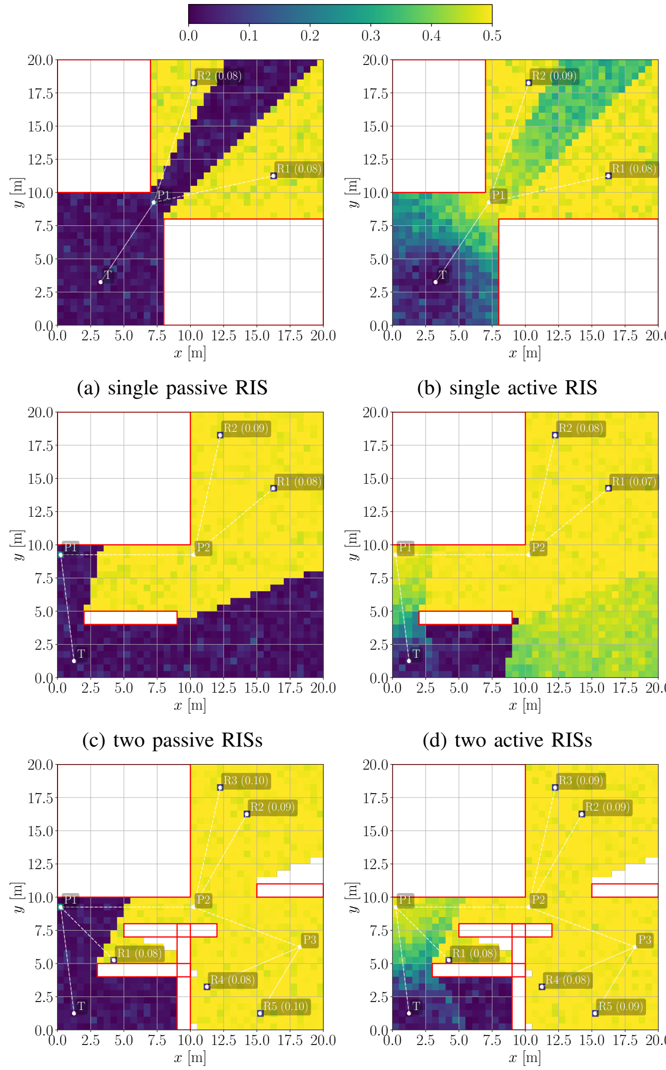
With respect to Scenario II, i.e., two RISs and two receivers (Figs. 2c and 2d) we can draw similar conclusions. The BER experienced by intended receivers in line with the previous results, and the same holds for eavesdropping areas, with a clear advantage when using active RISs. Finally, for Scenario III (Figs. 2e and 2f), the conclusions are again similar, proving how our proposed approach generalizes to different configurations.

## V. Conclusions and Future Work

We demonstrated that reconfigurable intelligent surfaces (RISs) can be used for physical layer security (PLS) in scenarios with multiple receivers and RISs by evaluating the capability to induce high bit error rate (BER) on malicious eavesdroppers. While the small area of low BER around receivers guarantees high security and privacy, it poses a challenge when considering mobile users. Our current method works well for stationary antennas, but future research should focus on mobile scenarios. Possible solutions include establishing secure channels when vehicles are stationary (e.g., at intersections) and then switching to standard cryptographic methods, or predicting channel gains for moving objects. Moreover, we also plan to extend our approach to consider multiple RISs in a parallel configuration.


## 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).


(a) single passive RIS

(b) single active RIS

(c) two passive RISs

(d) two active RISs

(e) multiple passive RISs

(f) multiple active RISs

Figure 2. Spatial heatmaps of the BER for SNR $= 10\,\mathrm{dB}$, $K = 4$, and $N = 36$.

## References


[1] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," *IEEE Communications Magazine*, vol. 54, no. 6, Jun. 2016.

[2] L. Ghiro, M. Cominelli, F. Gringoli, and R. Lo Cigno, "Wi-Fi Localization Obfuscation: An implementation in openwifi," *Elsevier Computer Communications*, vol. 205, May 2023.

[3] W. Tang, M. Z. Chen, X. Chen, J. Y. Dai, Y. Han, M. Di Renzo, Y. Zeng, S. Jin, Q. Cheng, and T. J. Cui, "Wireless Communications With Reconfigurable Intelligent Surface: Path Loss Modeling and Experimental Measurement," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, Jan. 2021.

[4] M. Segata, P. Casari, M. Lestas, A. Papadopoulos, D. Tyrovolas, T. Saeed, G. K. Karagiannidis, and C. Liaskos, "CoopeRIS: A framework for the simulation of reconfigurable intelligent surfaces in cooperative driving environments," *Elsevier Computer Networks*, vol. 248, Jun. 2024.

[5] J. Luo, F. Wang, S. Wang, H. Wang, and D. Wang, "Reconfigurable Intelligent Surface: Reflection Design Against Passive Eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 20, no. 5, May 2021.

[6] J. Jeganathan, A. Ghrayeb, L. Szczecinski, and A. Ceron, "Space shift keying modulation for MIMO channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, Jul. 2009.


1. https://github.com/Marrocco-Simone/pls-ris