RIS-Based Physical Layer Security: Realistic Evaluation and Challenges Ahead

Simone Marrocco*, Paolo Casari*†, Michele Segata*†

*Department of Information Engineering and Computer Science – University of Trento, Italy   †CNIT, Italy

Abstract— **Physical layer security (PLS) deals with implementing security mechanisms directly at the physical layer, potentially at the signal level. The recent advances on reconfigurable intelligent surfaces (RISs) make it possible to exploit their manipulation capabilities to make a signal decodable at specific locations and unintelligible at other ones, adding additional security and privacy mechanisms on top of existing ones. In previous work, we devised a mathematical framework to achieve multi-receiver PLS in the presence of multiple RISs, showing its effectiveness by means of spatial bit error rate (BER) maps. Our analyses, however, modeled each reception point in the BER map as affected by an independent Rice fading realization on top of path loss, making it impossible to study the size of the secured area around intended receivers. In this work, we extend our analyses by exploiting the Sionna ray tracing (RT) software which, by considering 3D scenarios, can properly estimate the effects of fading by considering realistic reflections and multi-path propagation. The results confirm the applicability of the methodology, but raise several interesting points regarding spatial correlation and undesired signal attenuation effects.**

I. Introduction and related work

The pervasive nature of communication systems is causing security and privacy concerns to constantly grow. Security and privacy mechanisms are present in multiple layers of the TCP/IP stack, e.g., Transport Layer Security (TLS) in between transport and applications layers or WiFi Protected Access (WPA) at the data link layer.

Several security schemes work directly at the physical layer, adding extra security measures by working directly at the signal level. Such approaches fall under the umbrella of physical layer security (PLS). PLS can support all classic security features, including authentication or integrity checks that depend on particular characteristics of the signal which cannot be faked. Even if hard to retrieve, compromising a cryptographic key would enable an attacker to decrypt the content of a secured communication or even generate fake but valid messages. Instead, some features of the wireless signal such as its received power, or the Doppler shift and delay of multi-path channel components are extremely hard if not impossible to forge, due to the need to knowing the channel state information (CSI) between transmitter and receiver perfectly [1].

In a past work [2] we have investigated how to exploit reconfigurable intelligent surfaces (RISs) to achieve PLS from a transmitter towards multiple receivers. RISs are basically mirrors for wireless signals that, thanks to a matrix of reflective elements, can focus a signal coming from a certain direction towards a specific receiver. More details about their working principle are described in [3], but in simple terms they work
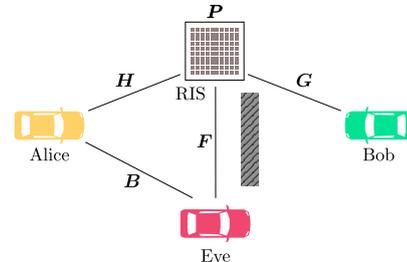

Figure 1. Communication scenario.

by changing the phase of the reflected signal on each of the reflecting elements, similar to beamforming. In our work we exploited this reconfiguration capability to alter the signal characteristics so as to make it decodable only by intended receivers, whereas the signal is seen as noise in other locations.

Different from what was done in past works, besides making the method effective for multiple receivers and in the presence of multiple RIS, we also considered a 2D spatial analysis, which enabled us to better appreciate how this approach would work in different scenarios rather than evaluating the bit error rate (BER) of a single link.

The problem in our analysis was the channel model. To generate a channel matrix at a specific point of the scenario, we computed the path loss and added independent Rice fading on top of it for each pair of transmitting and receiving antennas in direct line of sight (LoS). This approach makes every point independent of each other, making it impossible to study, for example, the spatial validity of the solution. To deal with this problem, gain more insights, and enable more realistic future studies on the subject we employ Sionna, a software which takes into account the geometrical description of the environment and, depending on the position of the communication nodes and their antenna configuration, calculates the channel matrix using ray tracing (RT), so considering the effect of multi-path reflections. This can provide us with very interesting and useful insights.

In the remainder of the paper we first recap how to enable RIS-based PLS (Sect. II), we introduce Sionna, its integration, and the scenarios we consider (Sect. III), and finally present the performance evaluation comparing stochastic channel conditions with RT ones (Sect. IV).

II. Physical Layer Security by means of RIS

In this section we briefly describe the mathematical framework we devise in [2]. We refer the reader to the original article for the details. Here we limit to the main idea for the sake of clarity throughout the rest of the paper. The scenario of interest is depicted in Fig. 1. We have a transmitter (Alice),
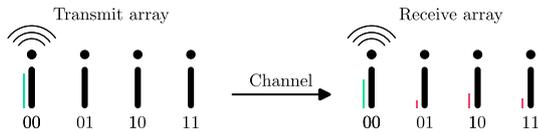
Figure 2. Simplified SSK communication principle. A single antenna transmits a data symbol; the receiver decodes by choosing the antenna receiving the highest power.

a legitimate receiver (Bob), an RIS which we can reconfigure to manipulate the signal, and an eavesdropper (Eve). Notice that this is a simplified view because, as anticipated in the introduction, our framework can handle multiple RISs and multiple legitimate receivers. Nodes are shown as vehicles just as an example: the type of communication node is irrelevant. In addition, eavesdroppers can be located anywhere, with the only limitation of not being very close to the transmitter or in the same location as legitimate receivers. When in LoS with the transmitter and in absence of RIS disturbance, we assume eavesdroppers to be able to estimate the channel and decode data. Each communication link is described by a complex channel matrix, where the size depends on the number of elements at the transmitter and at the receiver. We define

$$\text{Alice} \xrightarrow{H} \text{RIS} \xrightarrow{G} \text{Bob, Alice} \xrightarrow{B} \text{Eve, RIS} \xrightarrow{F} \text{Eve.} \quad (1)$$

We add subscripts to matrices when considering multiple RISs or receivers. In particular, in a chain of M consecutive RISs linking Alice to receiver Bob_j, C_i denotes the channel matrix between RIS i and $i+1$, i.e.,

$$\text{Alice} \xrightarrow{H} \text{RIS}_1 \xrightarrow{C_1} \dots \xrightarrow{C_{M-1}} \text{RIS}_M \xrightarrow{G_j} \text{Bob}_j. \quad (2)$$

For the transmitter, the receivers, and the eavesdroppers, we consider a linear antenna array made of K antennas, whereas RISs are made of N reflecting elements. Given this model, the received signal for a receiver Bob_j can be described with

$$y_{\text{Bob}_j} = G_j P_M C_{M-1} \dots P_1 H x, \quad (3)$$

where $x \in \mathbb{C}^K$ is the transmitted signal, which we modulate using Space Shift Keying (SSK) [4]. This means that information is encoded by the index of the antenna being used for transmission. In the case of 4 antennas, each antenna is associated with 2 bits of information, as shown in Fig. 2. In addition, $P_i \in \mathbb{C}^{N \times N}$ are diagonal matrices defining the configuration of RIS i. The values on the diagonal represent the attenuation and phase shift applied by the reflecting elements.

For brevity, we simplify Eq. (3) with $y_{\text{Bob}} = GPHx$ and similarly consider the signal received by Eve as $y_{\text{Eve}} = Bx + FPHx$, but as we show in [2], the approach can be generalized.

The goal is to find a configuration P so that the overall channel matrix GPH becomes a diagonal matrix only for legitimate receivers. To see why, recall that using SSK modulation means that only one element of x differs from zero, i.e., $\exists! \, i \in \{1, \dots, K\} : x_i \neq 0$. If GPH is diagonal, the same condition will hold for y_{Bob} enabling the receiver to decode the information. For other eavesdroppers, FPH will be a full and intractable matrix, which will also act as artificial noise in case of direct LoS with the transmitter.

Diagonalizing GPH requires us to solve

$$\|GPH - [GPH]_{\text{diag}}\|^2 = 0, \quad (4)$$

which can be achieved by exploiting singular value decomposition [2] and taking a portion of the right singular matrix, which we denote as $U \in \mathbb{C}^{N \times N - K^2 + K}$.

To obtain the RIS configuration P, we can choose any non-zero linear combination p of the columns of U and set $P = \text{diag}(p)$. To do so, we can choose any random vector $q \neq 0 \in \mathbb{C}^{N - K^2 + K}$ and compute

$$p = \frac{\eta}{\|Uq\|_\infty} Uq \quad (5)$$

where $\eta \in (0, 1]$ denotes the reflection efficiency. The division by $\|Uq\|_\infty$ normalizes the vector p. This method can be generalized to consider the case in Eq. (3) [2]. Frequent changes of P by choosing different values of q makes it harder for eavesdroppers to perform attacks based on statistical analyses.

III. Integration of the Sionna Ray Tracer

Sionna [5] is an open-source software developed by NVIDIA which enables the study of future communication systems considering modern RT techniques. RT can realistically compute the channel response by considering the reflections of the multi-path channel. RT is not a new technique, but it is now becoming common despite its computational complexity thanks to the recent evolution of GPUs.

Sionna enables users to consider a realistic 3D scenario, which can either be manually designed or generated starting from the map of a city, place communication nodes inside the map, define their characteristics, and finally compute the channel response for all receivers or even coverage maps. Communication nodes are described in terms of position, speed, orientation, and antenna configuration. In addition, it is possible to include RISs which, besides position and orientation, can be configured by setting the number of reflecting elements. The Sionna RIS model considers reflection efficiency due to orientation w.r.t. the receiver, but no other physical effects such as coupling among RIS elements.

After defining the scenario and the position of the communication nodes, it is necessary to define a "path solver," which is the object that actually performs ray tracing. This object can be parameterized to set the maximum number of bounces to consider for reflections, whether to consider the LoS path, specular reflections, diffuse reflections, and the like. Finally, Sionna will compute all the paths given the configuration and return all the channel matrices for every transmitter-receiver pair, and each matrix element represents the channel response for a specific pair of transmitter-receiver antennas (or reflecting element in case of the RIS).

A. Comparison between Stochastic and Ray Traced Channel

To compare the outcomes of our previous performance evaluation [2] and the ray tracing one, we implement the same scenarios within Sionna. In particular, we consider three scenarios in a simple square grid (20 m by 20 m) with a transmitter located in the bottom-left corner, different configurations in terms of obstructing buildings, RISs, and intended receivers. Scenario I includes one RIS and two intended receivers, scenario II two RISs in series and two

intended receivers served by the last RIS, while scenario III three RISs in series with five intended receivers served by one of the three RISs. For the RT evaluation, we simply extrude the 2D buildings into 3D objects.

The spatial resolution is $50\,\text{cm}$. For the stochastic channel, for each "pixel," we deterministically compute the path loss depending on the distance between the transmitter and the receiver using a free space path loss model with an exponent $\alpha = 2$. On top of it, we add a Rice fading with scale $\xi = 1$ and shape $\tau = 0.6$ computed independently for each pair of antennas or elements and obtain matrices $\boldsymbol{H}$ and $\boldsymbol{G}$. In the RT scenario, $\boldsymbol{H}$, $\boldsymbol{G}_j$, and $\boldsymbol{C}_i$ are retrieved from Sionna instead.

In our original work, we considered both passive and active RISs. However, we have shown that passive RISs can be ineffective due to the high path loss induced by the reflection. For this reason, we focus our analysis on active RISs, assuming that the signal is re-amplified during the reflection. To mimic this behavior, after computing the channel matrix $\boldsymbol{H}$ between the transmitter and the RIS, we rescale it by computing $\boldsymbol{H}' = \frac{\boldsymbol{H}}{||\boldsymbol{H}||_\infty}$, where $||\cdot||_\infty$ denotes the infinity norm. The rescaling preserves phase shifts while compensating for path loss effects. In case of cascaded RISs, we perform the same rescaling for the $\boldsymbol{C}_i$ matrices (obtaining $\boldsymbol{C}_i'$). Solving $\boldsymbol{P}$ to diagonalize $\boldsymbol{G}_j\boldsymbol{P}\boldsymbol{H}'$ is still done using the non-scaled matrices, but since our objective is only diagonalization, scalar multiplications do not influence the property.

Regardless of the channel model, the diagonalization process remains the same, as well as the performance evaluation. In particular, for each "pixel" in our two-dimensional scenario, we generate a set of $10\,000$ SSK-modulated data symbols, apply channel effects to it, add additive white gaussian noise (AWGN), and perform decoding measuring the BER. In the case of Sionna, this requires us to place a receiver at the center of each "pixel," obtain the channel matrix, and compute the BER. As outcome, we obtain a spatial BER map.

An important additional note is with respect to the orientation of nodes, which for RT can make a difference. In particular, transmitter and receiver arrays (both legitimate and not) are oriented perpendicular to the direction towards the RIS. This results in an implicit beamforming, both from transmitter to the RIS and from the RIS to every receiver. RISs, instead, are oriented to provide specular reflection from a transmitter (or a RIS) to one specific receiver. This is summarized, together with all other parameters, in Tab. I. Finally, we assume that Eve can estimate the channel between the transmitter and themselves, enabling them to decode SSK-modulated signals in the absence of the disturbance introduced by the RISs [4].

IV. Performance evaluation

We begin the analysis by looking at the BER maps in Fig. 3. The left image (Fig. 3a) shows the results for the stochastic channel, whereas the right one (Fig. 3b) shows the results for the RT channel obtained through Sionna. For the stochastic channel, the BER map shows a rather intuitive outcome. Close to the transmitter, the BER is low because the RIS reflection is not powerful enough to disturb potential unwanted receivers.

Table I
SIMULATION PARAMETERS.

Parameter	Value
K, N, α	4, 36, 2
Transmit frequency	$3.5\,\text{GHz}$
Transmit and noise power	$30\,\text{dBm}$ and $-90\,\text{dBm}$
Scenario size (resolution)	$20\,\text{m} \times 20\,\text{m}$ ($50\,\text{cm} \times 50\,\text{cm}$)
BER trials	$10\,000$ per spatial point
Stochastic channel parameters (Rice fading)	
Scale ξ and shape τ	1 and 6
Ray tracing parameters	
Buildings material	ITU-Marble [5]
Nodes and RIS configuration	1×4, 6×6
Antenna orientation (nodes)	Perpendicular w.r.t. direction to RIS
RIS orientation	Specular w.r.t. one specific tx-rx pair
Max ray bounces	3
Specular/diffuse reflections	Active/inactive
Refraction	Active
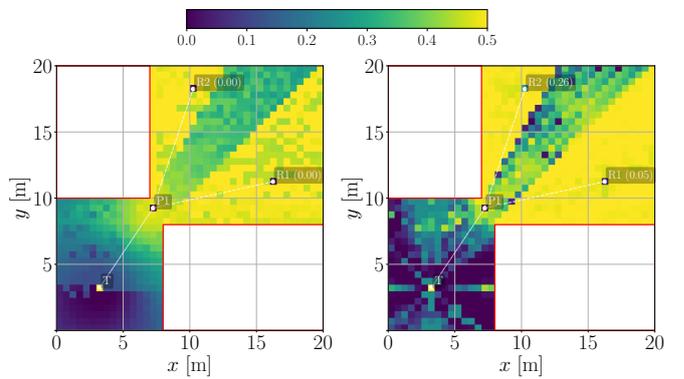
(a) single RIS, stochastic channel (b) single RIS, RT channel

Figure 3. Spatial heatmaps of the BER for scenario I.

Close to the RIS and in the upper-right part of the scenario, the impact of the disturbance is more relevant as the BER increases, with an area along the diagonal where the BER is lower than $50\,\%$ but still relevant. Where intended receivers are located, instead, the BER is basically zero, showing that the diagonalization effectively provides secrecy, enabling communication only with R_1 and R_2.

Comparing these results with the RT channel (Fig. 3b), we can observe several differences. The first is with respect to the BER for R_1 and R_2, which is not as low as for the stochastic channel. In particular it is around $5\,\%$ for R_1 and $26\,\%$ for R_2. The difference between the two values can be explained by the fact that in Sionna the RIS has an orientation which impacts the reflective efficiency. In the stochastic model the RIS is idealized, basically acting more as an omnidirectional relay. This effect can also be seen by looking at the edges of the cone along the diagonal of the scenario. In particular, on the left edge it is possible to spot more dark squares than on the right edge, indicating that the RIS orientation has an impact on secrecy in areas where the reflection is less efficient.

Coming back to the higher BER experienced by R_1 and R_2, we have to look at the spatial SNR, shown in Fig. 4. The left one (Fig. 4a) shows the SNR for the stochastic channel. The heatmap is smooth, as energy is isotropically radiated by the
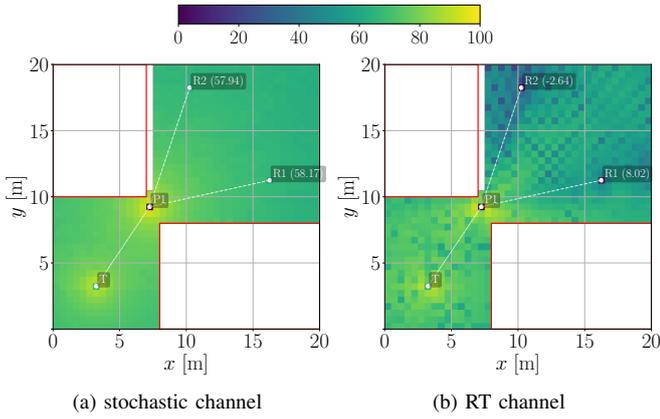
Figure 4. Spatial heatmaps of the SNR [dB] for scenario I.

Figure 5. Spatial heatmaps of the BER and SNR, RT channel.

transmitter and the RIS. The heatmap on the right (Fig. 4b) shows the SNR for the RT channel instead. Qualitatively the scenario is similar, as we can see the power emitted from the transmitter and the RIS and a similar attenuation pattern. Quantitatively, the behavior is quite different. First, the SNR in the top-right part of the scenario shows a chessboard pattern, which basically indicates that the quality of the signal highly depends on the position due to the constructive and destructive interference caused by reflections. This suggests that channel estimation and reconfiguration must be done quickly and frequently if we want to support mobility, as the configuration chosen for a specific receiver is valid only in that precise location, which is also clear from Fig. 3b.

The second and most important observation is that the SNR values for R_1 and R_2 are outliers compared to the chessboard pattern, as the values are $8\,\mathrm{dB}$ and $-2.6\,\mathrm{dB}$, respectively. We conjecture that the diagonalization introduces this effect, as this is not only seen in this scenario but in others as well.

Consider, for example, Fig. 5, which shows the BER and the SNR for scenarios II and III using RT. The results in terms of BER are qualitatively similar and they show that the approach provides reasonably low values with some exceptions where, due to the orientation of the RIS, the BER is above $33\,\%$. Concerning the SNR, we observe very low values for receivers experiencing high BER, but even for low-BER receivers the SNR is not very high compared to the stochastic scenario, where the SNR is always around $60\,\mathrm{dB}$ and the difference between the SNRs for the stochastic and the RT is always at least $30\,\mathrm{dB}$ (results omitted for space limitations). This phenomenon requires better understanding of the physical and mathematical framework used in this work. The causes may vary, from physical correlation of paths, to a stronger-than-anticipated power loss due to the RIS, as receivers positioned favorably get higher SNR, albeit lower than nearby eavesdroppers. Possible solutions include a particular choice of the random vector $\boldsymbol{q}$ in Eq. (5) that results in a RIS configuration $\boldsymbol{P}$ focusing the reflection towards the intended receivers, balanced with the need for randomness of $\boldsymbol{P}$ for better privacy. In addition, the scenarios considered might not yield a sufficiently rich multi-path environment, which is known to negatively affect MIMO performance.
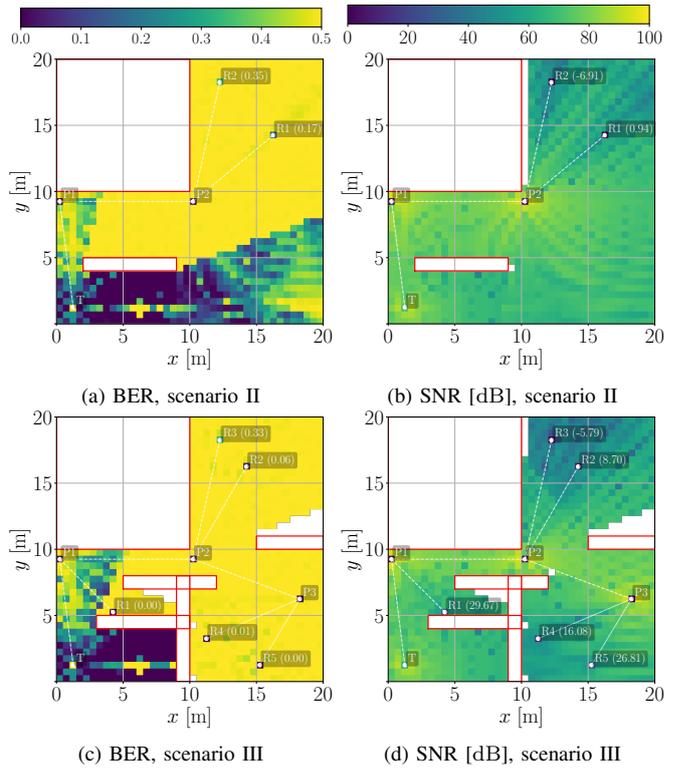
V. CONCLUSIONS AND FUTURE WORK

In this work, we evaluated the performance of a RIS-based PLS mechanism using a realistic, RT-based software to compare the results against an idealized stochastic channel. While the qualitatively comparable results confirm the effectiveness of the privacy-preserving method, the analysis has shown substantial differences with a realistic channel: the spatial correlation is small (requiring frequent channel estimation), and diagonalization induces unwanted signal attenuation at intended receivers. In our future work we plan to investigate this phenomenon, consider more complex communication scenarios with richer multi-path channels, counteract the effect by choosing optimized RIS configurations, and evaluate modulations other than SSK.

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] S. Marrocco, P. Casari, and M. Segata, "Exploiting Reconfigurable Intelligent Surfaces to Achieve Multi-Receiver Physical Layer Security," in *31st IEEE International Symposium on On-Line Testing and Robust System Design (IOLTS 2025)*, Ischia, Italy, Jun. 2025.

[3] 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.

[4] 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.

[5] J. Hoydis, F. A. Aoudia, S. Cammerer, M. Nimier-David, A. Binder, G. Marcus, and A. Keller, "Sionna RT: Differentiable Ray Tracing for Radio Propagation Modeling," in *2023 IEEE Globecom Workshops (GC Wkshps)*, Kuala Lumpur, Malaysia, Dec. 2023.