Università degli Studi di Padova

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

PHYSICAL-LAYER CHALLENGE-RESPONSE AUTHENTICATION WITH IRS AND MULTI-ANTENNA DEVICES

Relatore:	Correlatrice:
Prof. Stefano Tomasin	Prof. Anna Valeria Guglielmi

Laureanda:
Giulia Cassanego

ANNO ACCADEMICO: 2023/2024
Data di laurea: 25-09-2024

Contents

Sommario

This thesis investigates the use of Intelligent Reflecting Surfaces (IRS) in physical-layer authentication (PLA), with a specific focus on challenge-response (CR) mechanisms. IRS is a promising technology which enables to control and reconfigure wireless propagation channels. The IRS is under the control of the receiver (Bob), whose goal is to verify the identity of the transmitter. In fact, Bob randomly configures the IRS and then verifies that the resulting estimated channel is correspondingly modified. The CR-PLA scheme is evaluated in terms of the trade-off between communication and security performance, measured by the channel capacity and the probabilities of false alarms (FA) and missed detections (MD), respectively. In particular, we aim at designing the probability distribution of the random IRS configuration that maximizes the ergodic capacity under an upper bound constraint on the average misdetection and false alarm probabilities.

Introduction

In this thesis we investigate an alternative authentication mechanism that, instead of relying on traditional encryption methods, exploits the properties of the wireless transmission channel, i.e., Physical Layer Authentication (PLA). In particular, we focus on the Challenge-Response (CR) authentication, which is enhanced by the integration of Intelligent Reflecting Surfaces (IRSs), a promising technology that enables reconfigurable and adaptive wireless channels. In fact, IRS represents a solution to improve both the performance and security of communication systems while reducing costs and energy. This research aims to explore how IRS can be exploited to enhance PLA in wireless networks, where the receiver (Bob) dynamically controls the wireless propagation environment by setting the IRS configuration, and has the goal to detect if a message is sent from the legitimate source (Alice) or from an eavesdropper (Eve) who aims to impersonate Alice. We address the trade-off between communication and security performance, by properly choosing the IRS configuration.

In chapter 1 we introduce IRSs, presenting their benefits and the challenges that arise from their use.. Then, the authentication mechanisms, with a focus on PLA with IRSs, are discussed in chapter 2. In chapter 3, we evaluate the performance of CR authentication with IRSs, analyzing both communication and security performance. Lastly, conclusions are drawn in chapter 4.

Chapter 1

Intelligent Reflecting Surfaces

Recently, academia and industry have begun exploring technologies beyond 5G (B5G), such as the sixth-generation (6G) wireless networks, to achieve more demanding requirements than 5G. In fact, these requirements may not be fully achievable with the existing technology trends, due to their issues and limitations [1]. Hence, new and innovative technologies are required to ensure sustainable capacity growth in future wireless networks while maintaining low costs, complexity, and energy consumption.

1.1 Applications and Advantages

One such promising technology is the intelligent reflecting surface (IRS), which has emerged as a new paradigm for the development of smart and reconfigurable wireless channels or radio propagation environments for B5G/6G wireless communication systems. An IRS consists of a planar surface with a large number of passive reflecting elements, each capable of independently inducing a controllable amplitude and/or phase change to the incident signal. By deploying IRSs within a wireless network and smartly coordinating their reflections, the signal propagation or wireless channels between transmitters and receivers can be flexibly reconfigured to achieve desired propagation environments. This capability offers a new solution for overcoming challenges such as wireless channel fading and interference, potentially leading to significant improvements in communication capacity and reliability.

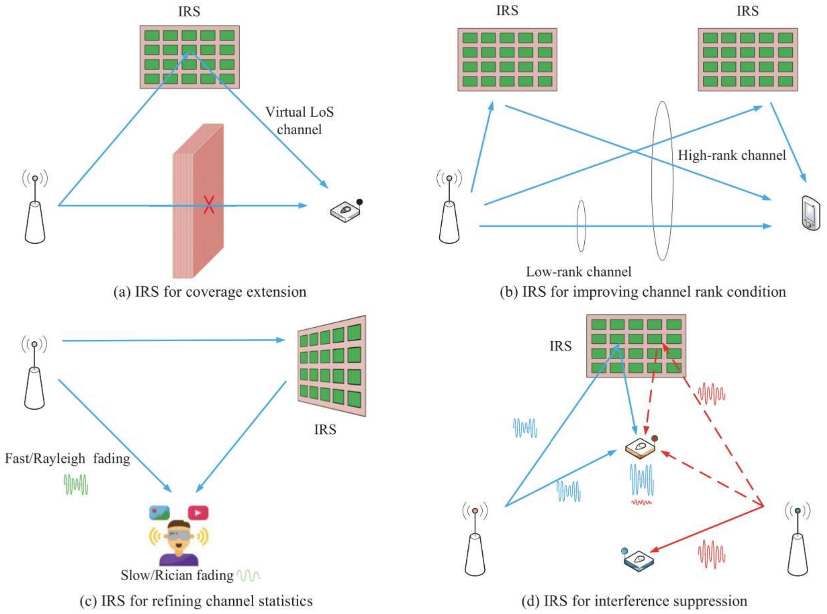

IRS
Virtual LoS channel
(a) IRS for coverage extension
IRS
IRS
High-rank channel
Low-rank channel
(b) IRS for improving channel rank condition
IRS
Fast/Rayleigh fading
Slow/Rician fading
(c) IRS for refining channel statistics
IRS
(d) IRS for interference suppression

Figure 1.1: Main use cases of IRS for wireless channel reconfiguration. [1]

As it can be seen from Figure 1.1, some of the most appealing IRS use cases include creating virtual line-of-sight (LoS) link to bypass obstacles between transceivers via smart reflection, adding signal paths toward desired direction to improve the channel rank condition, modifying the channel statistics or distribution (e.g. converting Rayleigh/fast fading into Rician/slow fading) in order to achieve ultra-high reliability, and suppressing or nullifying co-channel or inter-cell interference, among others.

These use cases yield a broad range of innovative applications in future IRS-assisted wireless networks, as illustrated in Figure 1.2. For instance, IRS is crucial for extending coverage in millimeter-wave (mmWave) and Terahertz (THz) communications, which are extremely vulnerable to blockage. Furthermore, deploying IRSs at the cell edge can help improve the desired signal power at cell-edge users and simplify the suppression of co-channel interference from neighboring cells. Additionally, the large aperture of IRS can be exploited to compensate for the significant power loss over long distance with reflect beamforming to nearby devices, enhancing the efficiency of simultaneous wireless information and power transfer (SWIPT) from the AP to wireless devices in settings such as smart offices or homes.

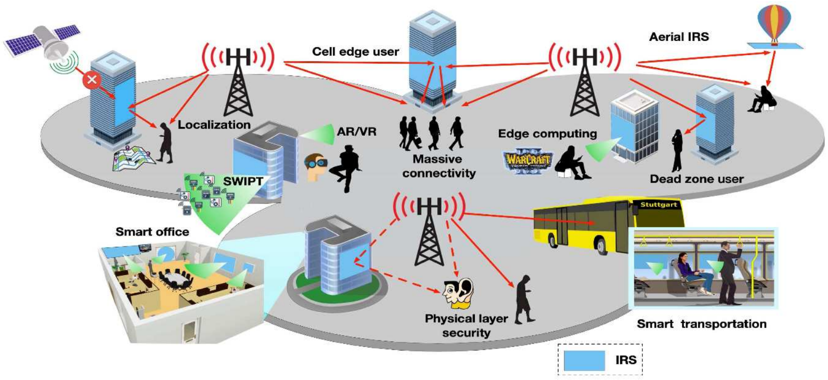


Figure 1.2: Illustration of IRS applications in future wireless network. [1]

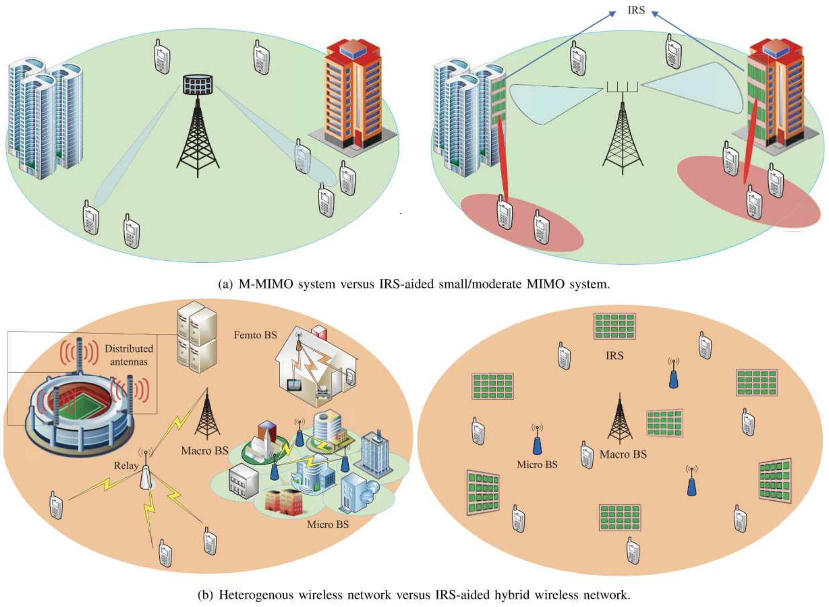
IRS also offers several practical advantages in terms of implementation. Firstly, if its elements only passively reflect the impinging signals, then the IRS does not require any transmit radio-frequency (RF) chains, making it significantly more cost-effective and energy-efficient to implement and operate compared to traditional active antenna arrays or the recently proposed active surfaces. Additionally, IRS operates in full-duplex (FD) mode and avoids issues like antenna noise amplification or self-interference, giving it competitive advantages over traditional active relays, such as half-duplex (HD) relay, which suffers form low spectral efficiency, and FD relay, that requires sophisticated self-interference cancellation techniques. Furthermore, since IRS is generally of low profile, light weight and conformal geometry, it can be easily mounted on or removed from environment objects for deployment or replacement. Lastly, IRS serves as an auxiliary device within wireless networks and can be integrated transparently, offering great flexibility and compatibility with existing wireless systems.

In indoor environments, IRS can be attached to the ceiling, walls, forniture, and even behind paintings or decorations, in order to help increase coverage and create high-capacity hot-spot. In particular, enhanced mobile broadband (eMBB) and massive machine-type communication (mMTC) applications are interested in this aspect. Indeed, for mMTC applications, due to the small fraction of devices active for communication at each time instant, IRS can be used to improve the device activity detection accuracy and efficiency by providing additional controllable paths.

In outdoor environments, IRS can be coated on the building facade, lamppost, advertising board, and even the surface of high-speed moving vehicles. In this way different applications can benefit of it, e.g., ultra-reliable and low latency communication (URLLC) for remote control and smart transportation thanks to the compensation of the Doppler and delay spread effects. For example, IRS can enhance communication reliability, by transforming typically random wireless channels into more deterministic ones, hence reducing packet retransmissions and minimizing the delay - an essential aspect for URLCC applications [1].

1.2 Paradigm Shifts and Challenges

Given these promising advantages, IRS is well-suited for widespread deployment in wireless networks to significantly enhance spectral and energy efficiency in a cost-effective way. Consequently, it is envisioned that IRS will lead to fundamental paradigm shifts of wireless system and network designs, moving form the current massive multiple-input-multiple-output (M-MIMO) system without IRS to the new IRS-aided small/moderate MIMO system, as well as from the existing heterogeneous wireless network to the new IRS-aided hybrid network in the future, as shown in Figure 1.3.



(a) M-MIMO system versus IRS-aided small/moderate MIMO system.

(b) Heterogenous wireless network versus IRS-aided hybrid wireless network.

Figure 1.3: Potential paradigm shifts of wireless system/network designs with IRS. [1]

On one hand, unlike M-MIMO systems that rely on tens and even hundreds of active antennas to generate sharp beams directly, an IRS-aided MIMO system enables the base station (BS) to be equipped with significantly fewer antennas without compromising the users' quality-of-service (QoS), by exploiting the large aperture of IRS to create fine-grained reflect beams through smart passive reflections (see Figure 1.3 (a)). As a result, the system hardware cost and energy consumption can be greatly reduced, especially as wireless systems transition to higher frequency bands in the future. On the other hand, while current wireless networks rely on a heterogenous multi-tier architecture consisting of macro and small BSs/Access Points (APs), relays, distributed antennas, etc., all of these are active nodes that generate new signals in the network, requiring complex coordination and interference management to enhance network spatial capacity as more active nodes are deployed. However, this strategy inevitably increases the network operation overhead, which could become unsustainable in terms of cost as the wireless network capacity demand continues to grow.

Furthermore, integrating IRSs into wireless network will shift the current active-only heterogeneous network to a new hybrid architecture comprising both active and passive components smartly working together (see Figure 1.3 (b)). By optimally balancing the deployment of active BSs and passive IRSs in the hybrid network a sustainable network capacity growth can be achieved in a more efficient and cheap way.

Although IRS can be seen as a promising technology, the design of IRS-aided wireless systems and networks presents new and unique challenges from a communication perspective, three of which are elaborated below.

The first challenge consists in carefully design the passive reflections of each reflecting element on an IRS , i.e., the IRS configuration, to properly achieve the desired propagation environments. Furthermore, it is worth noting that the optimization of the IRS configuration strictly depends on the channel to and from the IRS, whose knowledge is not so immediate. Moreover, to effectively serve all users in the network, regardless of whether they have a nearby IRS, the IRS passive reflections need to be jointly designed with the beamformers used at the BS and users sides to optimize the end-to-end communications.

Another challenge concerns the acquisition of the channel state information (CSI) between the IRS and its associated BSs/users, due to the passive nature of the IRS and then the lack of computation capabilities. An IRS typically consists of a large number of reflecting elements, each contributing to the channel coefficients that need to be estimated. This makes its optimization more difficult.

The last challenge regards the optimal deployment strategy for IRSs in wireless network, aimed at maximizing the network capacity. Indeed, this strategy is likely to differ significantly from those used in traditional wireless networks with only active BSs/APs and relays, due to the distinct characteristics of IRSs, i.e., passive reflection instead of active transmission or reception. Therefore, an exhaustive re-examination of deployment strategies is necessary.

In conclusion, IRS technology offers various promising applications across different fields, such as physical-layer security (further explored in the next chapter), wireless power transfer, unmanned aerial vehicle (UAV) communications, MmWave communications, mobile edge computing and so on [1]. However, the research on IRS-aided wireless communication is still in its early stages and it is crucial to explore new challenges and potential future research directions, such as theoretical IRS signal and channel modeling, practical IRS beamforming design, channel estimation and optimal deployment strategies.

Chapter 2

Physical-Layer Authentication

Authentication is the problem of establishing if a received message does really come from the legitimate source or has been forged by an impersonating attacker. This is indeed crucial for avoiding the risks involved in accepting unathenticated messages, such as denial of service, privacy leakage, and loss of control of devices [2]. Among all the authentication mechanisms, we focus on the Physical Layer Authentication (PLA), which exploits the propagation characteristics of the physical channel as signatures of the transmitting devices or the communication links. PLA has been studied in several contexts, such as orthogonal frequency division multiplexing (OFDM) and multiple-input multiple-output (MIMO) systems, underwater acoustic communications, and also from Neyman-Pearson tests to machine learning approaches [2].

2.1 Authentication Mechanisms

Message authentication mechanisms allow an agent (Bob) to verify that a received message was indeed sent by the legitimate agent (Alice), rather than by a malicious agent (Eve), who aims to impersonate Alice. There are two main classes of such mechanisms, i.e., tag-based (TB) and challenge-response (CR) authentication [3]. With the former mechanism, each message contains a tag or identifier that only Alice can generate and that Bob can recognize: e.g., Alice and Bob share a secret key, which Alice uses to encode information related to the message, Bob then decodes the tag using the same key to verify that the message is legitimate. With the latter mechanism, Alice and Bob share a secret that enables Bob to ask Alice random questions, with Alice being the only one able to provide the correct answer, so that Bob is allowed to confirm the authenticity.

Both TB and CR authentication mechanisms typically rely on encryption. In particular, in TB authentication the message is encrypted with the secret key of an asymmetric key encryption system. While, in CR authentication Alice applies a pre-determined function (known to Bob) to the challenge and encrypts it with a symmetric key (known only to Bob) before transmission.

However, alternative or complementary approaches to traditional encryption-based security methods have recently gained attention. This is particularly relevant for the current and future Internet of Things(IoT) networks, which involve numerous interconnected devices with diverse computational capabilities, data rates, and transmission burstiness [4]. These alternative approaches aim to provide lower energy consumption, run efficiently on devices with limited computational capabilities, and withstand new cyber-physical attacks. In particular, physical-layer security (PLS) stands out as a branch of information security that exploits the properties of the physical communication channel. In particular, the basic PHY-layer authentication approach consists of two phases: the identification acquisition phase and the identification verification phase [5]. In the first one, Bob (the verifier) estimates the channels using signals transmitted by Alice (the authentic source) which are authenticated at higher levels. In the second phase, whenever Bob receives a new message, he also estimates the channel over which the signal travelled and compares this estimate with that obtained in the first phase. If the two are consistent (considering they are both affected by noise), then the received message is stated authentic, otherwise it is considered fake.

In the literature, several authentication mechanisms have been explored, with particular attention to the TB authentication, in which, the CSI - the gain, impulse, or frequency response of the channel - is often used as tag [3]. In fact, PLA relies on two properties of wireless channels, i.e., their invariance over time and their high variation over space, that allow the receiver to verify if newly received messages have traveled through the same channel as authentic ones previously received. If this is the case, they are stated as authentic. Whereas, when an attacker sends a message from a different location than the legitimate sender, the signal will travel through significantly different channels and it can be detected as fake. [4].

In contrast, CR authentication within the context of PLA has received relatively little attention until now. In [3] a new mechanism for CR PLA is introduced, specifically for scenarios in which the channels can be (at least

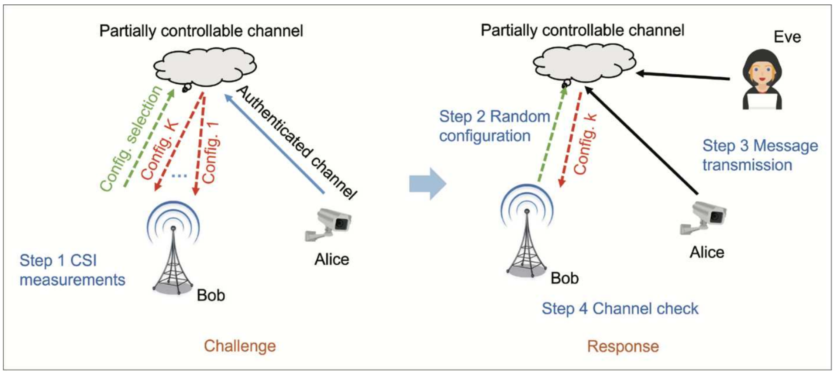


Figure 2.1: The CR PLS authentication scheme. [3]

partially) controlled by Bob, i.e., whose propagation characteristics can be in part determined by Bob (see Figure 2.1). In this case, Bob creates the challenge by setting some channel parameters (channel configurations) that, however, do not fully determine the channel. The response is the CSI that Bob estimates, which should be consistent with the selected configuration. The advantage of this procedure is that, by keeping the current channel configuration secret from Eve (the attacker), she cannot provide the correct response to Bob. The main advantage of CR PLA over the traditional TB PLA is that the random choice of the channel configuration prevents Eve from repeating a successful attack once it has been identified, i.e., she found the correct tag. Indeed, in CR PLA, multiple challenge-response couples are utilized, thus even if Eve discovers the correct response for a given challenge, she remains unaware of the others. Additionally, in the CR PLA scenario Eve is unaware of the current challenge (i.e., the current channel configuration), making the design of the attack strategy more complicated.

Note that, in CR PLA mechanism the security depends on the degree of control that Bob has on the channel, and, also, CR PLA mechanism modifies the channel itself, differently from other mechanism where a feature of an existing channel is selected for authentication [3]. Since IRS can be used to modify the propagation of wireless signals (and then the channel characteristics), CR-PLA mechanism can benefit of the IRS presence in RIS-assisted MIMO systems.

2.2 PLA with IRS

As an innovative approach to intelligently reconfigure wireless propagation, IRS holds great potential for significantly enhancing the security of traditional wireless networks, even in challenging scenarios where conventional PHY-layer security techniques prove ineffective [1]. In fact, IRS can increase the data transfer rate and cell coverage, and improve signal-to-noise ratio (SNR). Moreover, as previously mentioned, it can support PLS mechanisms [4].

In particular, when IRSs are optimized to focus on collecting signals from a specific area, the Alice-IRS-Bob communication channel is enhanced, thus, making it more distinctive and improving tag-based PLA. Furthermore, advanced IRS with sensing capabilities can offer deeper insights into the propagation channel, leading to more effective authentication, still in the context of TB authentication. For instance, in literature a tag-based PLA mechanism in IRS-assisted communication systems has been proposed: in an IRS communication system, the channel gain and background noise are extracted, and then applied to a random signal together with a private key, generating a cover tag signal [4]. Note that in this case previously known secret bits are used for authentication instead of PHY-layer characteristics.

IRSs are ideally suited for the CR PLA. Indeed, the IRS under the control of the receiver can be integrated in the CR-PLA mechanism. In particular, in this mechanism, Bob first randomly modifies the propagation environment, i.e., the IRS configuration, acting as the challenge, and then estimates the channel through which the received signal has passed - the response - to ensure that it is consistent with the modified configuration. Indeed, the CR PLA protocol can be described as follows, as shown in Figure 2.1 [3]:

1. *Step 1, CSI measurements:* Alice sends several pilot signals to Bob over a partially controllable channel, correspondingly to several channel configurations properly selected by Bob. These transmissions are secured using higher-layer authentication mechanisms. Using the pilot signals, Bob estimates the Channel State Information (CSI) and records both the estimated CSIs and the corresponding channel configurations.

2. *Step 2, random configuration:* Bob issues a challenge to Alice by randomly selecting a channel configuration. This configuration mighthave already been encountered during Step 1 or could be a completely new one. In the latter case, Bob must be able to predict the expected CSI based on the previous observations from Step 1.

3. *Step 3, message transmission:* Alice transmits the message, and Bob estimates the CSI from the received signal, which consists in the response of Alice to the challenge.

4. *Step 4, channel check:* Bob compares the estimated CSI from Step 3 (the response) with the predicted CSI from Step 2 (the expected response). If the two CSIs match, the message is considered authentic.

Moreover, in [6] the new hybrid-IRS (H-IRS) structures are presented, containing elements that can simultaneously reflect wireless signals and operate as receive antennas. In order to do that, part of the energy of the signal impinging on an element is absorbed by the radio-frequency chain, operating as a receiver, while part is reflected in the desired direction, operating as a passive IRS. It is shown that, by exploiting the H-IRS, the PLA mechanism improve.

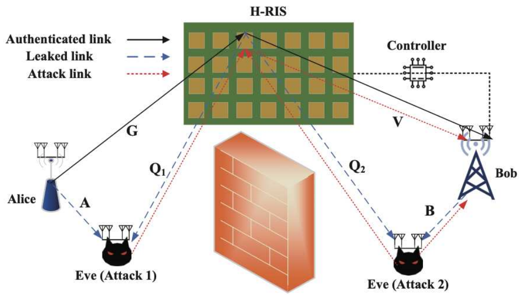


Figure 2.2: H-RIS PLA system model. [6]

Besides all the advantages that IRSs ensure in PLA, there are still several practical issues that need to be solved. First of all, in order to exploit IRS passive beamforming for reducing the eavesdropper's rates, the CSI of the links between the receiver and eavesdroppers as well as between the IRS and eavesdroppers are required, and this is practically difficult to obtain for two main reasons: (i) IRS usually has a huge number of passive reflecting elements, and (ii) the eavesdropper could intentionally remain covert or their CSI could be imprecise or outdated if their signal leakage is used for channel estimation. As a consequence, new channel estimation procedures as well as robust or secure IRS passive beamforming design are required, where incomplete or imperfect CSI at the eavesdropper is considered. Furthermore, in a large-scale secure communication network with many legitimate users and eavesdroppers, along with densely deployed IRSs, the strategic placement of IRSs is crucial for maximizing network secrecy throughput, which asks for further investigation.

Chapter 3

Challenge-Response Authentication with IRSs

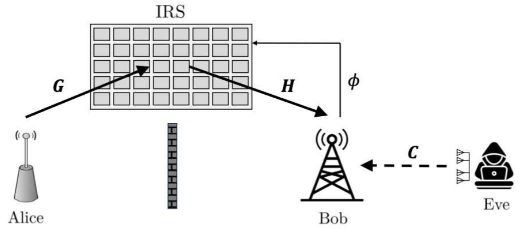


Figure 3.1: Communication scenario. [5]

The new communication technologies, specifically, the controllable nature of wireless channels, made possible a further evolution of PLA. In particular, the propagation of wireless signals can be modified using intelligent reflecting surfaces (IRSs), which are controllable devices that change the phase shift introduced by their elements. Hence, when the IRS is under Bob's control, he can set a random configuration of the IRS, unknown to the attacker, and verify that the channel estimated from a received message corresponds to the set configuration. This approach consists in a *challenge response PLA (CR-PLA)* mechanism, where the random configuration is the challenge and the predicted channel is the expected response.

We analyze the performance of the CR-PLA scheme in terms of false alarm (FA) and missed detection (MD) probabilities, while to measure the communication performance we consider the signal-to-noise ratio (SNR) averaged over the random IRS configuration.

3.1 System Model

We consider the scenario where a legitimate receiver Bob authenticates messages from a legitimate transmitter Alice. An attacker Eve aims to impersonate Alice by forging messages and transmitting them to Bob. We assume that Alice, Eve and Bob are equipped with a uniform linear array (ULA) of N_A, N_B and N_E antennas, respectively, and the number of elements of the IRS is large.

The communication between Alice and Bob is supported by an IRS with N reflecting elements, each acting as a receive and transmit antenna. Each element has unitary gain and introduces a phase shift $\phi_n = e^{j\Theta_n}$, $n = 1, 2, ..., N$, on the equivalent baseband impinging signal. We define the *configuration* collecting the phase shifts introduced by the IRS on each element through the vector $\boldsymbol{\phi} = [\phi_1, \phi_2, ..., \phi_N]^T$, and we define the NxN diagonal matrix $\mathbf{\Phi}$ as

$$\mathbf{\Phi} = \text{diag}\{\boldsymbol{\phi}\} = \text{diag}\{\phi_1, \phi_2, ..., \phi_N\}. \tag{3.1}$$

Bob controls the IRS by choosing $\boldsymbol{\Phi}$ using a secure dedicated channel not accessible to Eve. We assume, then, that communication between Alice and Bob only happens through the IRS without any additional direct link. We define $\boldsymbol{G} \in \mathbb{C}^{N\text{x}N_A}$ as the vector for the baseband equivalent channel from Alice to the IRS, and $\boldsymbol{H} \in \mathbb{C}^{N_B\text{x}N}$ as the vector of the channel from the IRS to Bob. Hence, the resulting Alice-IRS-Bob cascade channel gain is

$$\boldsymbol{Q} = \boldsymbol{H}\boldsymbol{\Phi}\boldsymbol{G}. \tag{3.2}$$

We assume that Eve can transmit messages to Bob through a direct channel with gain $\boldsymbol{C} \in \mathbb{C}^{N_B\text{x}N_E}$, known by Eve.

All the channels are assumed to be time-invariant and reciprocal, while the IRS configuration (i.e., matrix $\boldsymbol{\Phi}$) is under Bob's control and can be changed over time, making the cascade channels $\boldsymbol{Q}$ controllable.

Communication Channel: We consider the communication channel modeled as follows

$$\boldsymbol{y} = \boldsymbol{Q}\boldsymbol{x} + \boldsymbol{w}, \tag{3.3}$$

where $\boldsymbol{x}$ is the vector of transmitted data and $\boldsymbol{w}$ is the additive white Gaussian noise (AWGN) vector. We assume here that $\boldsymbol{x}$ is a complex Gaussian vector with zero mean and correlation matrix $\boldsymbol{P} = \mathbb{E}[\boldsymbol{X}\boldsymbol{X}^H]$.

3.1.1 CR-PLA with IRS

The CR-PLA mechanism introduced before works as follow in our scenario. In the *association* phase Alice transmits authenticated pilot signals to Bob, who estimates the cascade channel $\boldsymbol{Q}$ for several IRS configurations. We assume that, through this phase, Bob will obtain estimates $\overline{\boldsymbol{Q}}(\boldsymbol{\Phi}')$ of the cascade channel for any IRS configuration $\boldsymbol{\phi}'$.

$$\overline{\boldsymbol{Q}}(\boldsymbol{\Phi}') = \boldsymbol{Q}(\boldsymbol{\Phi}') + \overline{\boldsymbol{W}} \tag{3.4}$$

where $\overline{\boldsymbol{W}}$ is the estimation error at Bob, modeled as additive white Gaussian noise (AWGN) matrix with independent entries, each with zero mean and power σ_B^2.

In the *verification* phase, Bob sets a random configuration $\boldsymbol{\Phi}$ of the IRS as described here. Bob modifies the IRS configuration around the communication-optimal one $\overline{\theta}_n$, $n = 1, ..., N$, obtaining a new configuration as

$$\phi_n' = e^{j(\overline{\theta}_n + \epsilon_n)},\ n = 1, ..., N, \tag{3.5}$$

with ϵ_n random variable with support $[-\gamma, \gamma]$, where γ stands for the maximum deviation from the communication-optimal IRS configuration. This means that a larger γ increases the randomness in the IRS configuration making it more difficult for Eve to build a successful attack. Besides, ϵ_n are independent for each $n = 1, ..., N$, and regenerated independently at each new verification phase. Whenever Bob receives a message, he estimates the cascade channel $\boldsymbol{R}$ and verifies if it corresponds to the expected channel $\overline{\boldsymbol{Q}}(\boldsymbol{\Phi})$. Pilot signals are assumed to be known by all parties.

Under legitimate conditions, given the configuration ϕ of the IRS, when

Alice is transmitting, Bob estimates the Alice-IRS-Bob cascade channel, i.e.,

$$\hat{\boldsymbol{Q}} = \boldsymbol{Q} + \boldsymbol{W}_B, \tag{3.6}$$

where $\boldsymbol{W}_B$ is the estimation error at Bob, modeled as additive white Gaussian noise (AWGN) with zero mean, independent entries and power σ_B^2 per entry.

We suppose that Bob knows perfectly both the channel matrices and can decide the IRS configuration $\boldsymbol{\Phi}$. Hence, Bob during the association phase obtains $\overline{\boldsymbol{Q}}(\boldsymbol{\Phi}) = \boldsymbol{Q}(\boldsymbol{\Phi})$.

Bob's goal is to figure out whether the estimated channel $\boldsymbol{R}$ is authentic ($\hat{\boldsymbol{Q}}$), or forged ($\boldsymbol{V}$), by exploiting his knowledge of $\boldsymbol{Q}$. To recognize the attack, Bob performs an authentication test, that, given $\boldsymbol{Q}$ and $\boldsymbol{R}$, decides between the following hypothesis:

$$\mathcal{H}_0 : \text{ the message is from Alice,} \tag{3.7}$$

$$\mathcal{H}_1 : \text{ the message is from Eve,} \tag{3.8}$$

The authentication procedure is represented in block D of Figure 3.2, which has $\boldsymbol{r}$ as input and the Boolean value $\hat{b}$ as outputs. Proper verification is accomplished if $\hat{b} = b$.

3.1.2 Attack Model

Eve's goal is to impersonate Alice and pass the authentication test at the legitimate receiver (i.e., Bob). We consider that Eve knows some side information, represented by the matrix $\boldsymbol{Z}$. We also assume that $\boldsymbol{C}$ is correlated

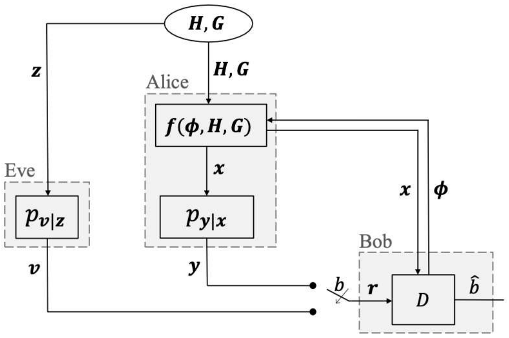


Figure 3.2: Block scheme. [2]

with $\boldsymbol{H}$ and/or $\boldsymbol{G}$, thus, Eve can estimate these channel matrices and compute the communication-optimal IRS configuration $\boldsymbol{\Phi}^\star = \text{diag}\{e^{j\bar{\theta}_1}, ..., e^{j\bar{\theta}_N}\}$. The corresponding resulting estimate at Eve of the Alice-IRS-Bob cascade channel with communication-optimal IRS configuration is

$$\boldsymbol{Z} = \boldsymbol{H}\boldsymbol{\Phi}^\star\boldsymbol{G} + \boldsymbol{W}_{\boldsymbol{z}}, \tag{3.9}$$

where $\boldsymbol{W}_{\boldsymbol{z}}$ is an AWGN matrix modeling the resulting estimation error.

Moreover, we assume that Eve knows: i) the actual realization of $\boldsymbol{Z}$, ii) the probability density function (pdf) of the channel matrices $\boldsymbol{H}$ and $\boldsymbol{G}$, and of the IRS configuration vector $\boldsymbol{\phi}$, and iii) the pdf of noise at both receivers. We also suppose that Eve transmits precoded pilot signals and can induce any channel estimate to Bob. Thus, when under attack, Bob estimates

$$\boldsymbol{V} = \boldsymbol{V}_0 + \boldsymbol{W}_B, \tag{3.10}$$

where $\boldsymbol{V}_0$ is the channel forged by Eve. To preserve generality, we consider that Eve adopts a probabilistic strategy, characterized by the conditional pdf

$p_{\mathbf{V_0}|\boldsymbol{Z}}$. Besides, since Eve knows the statistics of $\boldsymbol{W}_B$, the attack strategy can be described by $p_{\boldsymbol{V}|\boldsymbol{Z}}$.

3.1.3 Authentication Test

Lastly, let the channel estimate at Bob be

$$\boldsymbol{R} = \begin{cases} \hat{\boldsymbol{Q}} & \text{if Alice is transmitting } (b = 0), \\ \boldsymbol{V} & \text{if Eve is transmitting } (b = 1), \end{cases} \tag{3.11}$$

with b indicating the legitimate/attack state. Thus, Eve's goal is to prevent Bob from distinguishing between the attack $\boldsymbol{V}$ and the legitimate $\hat{\boldsymbol{Q}}$. To simplify, let $\boldsymbol{v} = \text{vec}(\boldsymbol{V})$ and $\boldsymbol{r} = \text{vec}(\boldsymbol{R})$, as in Figure 2.2. Due to the variety of the possible Eve's attack $\boldsymbol{V}_0$, we consider that the receiver employs a GLRT (Generalized Likelihood Ratio Test), appropriate in case of unknown $\boldsymbol{V}$ statistics. Let $f_{\hat{\boldsymbol{Q}}|\mathcal{H}_0}$ be the pdf of $\hat{\boldsymbol{Q}}$ under hypothesis $\mathcal{H}_0$. The generalized log-likelihood function is

$$\Psi = \text{log} f_{\hat{\boldsymbol{Q}}|\mathcal{H}_0}(\boldsymbol{R}) \tag{3.12}$$

Under hypothesis $\mathcal{H}_0$, and conditioned on the configuration $\mathbf{\Phi}'$ chosen by Bob, form (3.4), (3.6) and (3.10) $\boldsymbol{R}$ has a Gaussian distribution with mean $\overline{\boldsymbol{Q}}$ and we can write

$$\boldsymbol{R} = \overline{\boldsymbol{Q}}(\mathbf{\Phi}') + \boldsymbol{W}_{\text{B}} - \overline{\boldsymbol{W}}. \tag{3.13}$$

Let $\boldsymbol{W} = \boldsymbol{W}_{\mathrm{B}} - \overline{\boldsymbol{W}}$ be the overall noise matrix with independent entries, each with zero mean and variance $\sigma^2 = 2\sigma_B^2$. Hence, (3.12) can be written as

$$\Psi = \frac{2}{\sigma^2}||\boldsymbol{R} - \overline{\boldsymbol{Q}}(\boldsymbol{\Phi}')||^2, \tag{3.14}$$

neglecting irrelevant constants. In line with the GLRT, Ψ is compared with a treshold τ, and the authentication outputs

$$\hat{b} = \begin{cases} 0 & \Psi < \tau, \\ 1 & \Psi \geq \tau. \end{cases} \tag{3.15}$$

3.2 Authentication Strategy Design

In the CR-PLA mechanism Bob has to randomly select the IRS configuration to generate the challenge. On the other hand, the random IRS configuration selected in the verification phase, while providing authentication capabilities, affects the data rate of the communication link between Alice and Bob. Thus, we aim to properly design the pdf of the IRS configuration $p_{\boldsymbol{\Phi}}(\boldsymbol{\Phi})$ to obtain a tradeoff between the security metrics and the resulting achievable rate of the legitimate channel. Furthermore, under the two hypotheses (3.12) becomes

$$\Psi = \frac{2}{\sigma^2}|\boldsymbol{\delta}|^2, \tag{3.16}$$

with

$$\boldsymbol{\delta} = \begin{cases} \boldsymbol{W}, & \text{under hypothesis } \mathcal{H}_0 \\ \boldsymbol{V}_0 - \boldsymbol{H}\boldsymbol{\Phi}\boldsymbol{G} + \boldsymbol{W}, & \text{under hypothesis } \mathcal{H}_1. \end{cases} \tag{3.17}$$

3.2.1 Communication Performance

In our system with multi-antenna transmitter and receiver, for a given IRS configuration $\boldsymbol{\Phi}$, the resulting achievable rate of the Alice-Bob channel is

$$C_{A,B}(\boldsymbol{\Phi}) = \log_2 \left[\det \left(\boldsymbol{I} + \frac{1}{\sigma_B^2}\boldsymbol{Q}\boldsymbol{P}\boldsymbol{Q}^H\right)\right] \tag{3.18}$$

where $\boldsymbol{I}$ is the identity matrix, $\boldsymbol{Q}$ is the Alice-IRS-Bob cascade channel (i.e. $\boldsymbol{H}\boldsymbol{\Phi}\boldsymbol{G}$), $\boldsymbol{Q}^H$ represents its complex conjugate and transpose, and $\boldsymbol{P}$ is the correlation matrix of the vector of transmitted data (3.3), that can be chosen in order to maximize the capacity.

In the verification phase, we assume Bob modifies the IRS configuration around the optimal one, obtaining a new phase shift as

$$\theta_n = \overline{\theta}_n + \epsilon_n, \tag{3.19}$$

with ϵ_n a random variable, that are assumed independent and identically distributed (i.i.d.) for all the IRS elements and with even pdf. Hence, the problem of designing $p_{\boldsymbol{\Phi}}(\boldsymbol{\Phi})$ becomes the problem of designing the pdf of p_ϵ of ϵ_n.

For communication performance evaluation we consider the average capacity for given $\boldsymbol{H}$ and $\boldsymbol{G}$, for which we now derive an approximate expression depending on some statistical properties of ϵ_n.

In particular, let us consider the asymptotic case $N \to \infty$. Then, let us define

$$m = \mathbb{E}[e^{j\epsilon_n}] = \mathbb{E}[\cos\epsilon_n] + j\mathbb{E}[\sin\epsilon_n]. \tag{3.20}$$

Assuming that p_ϵ is even, the second term vanishes and

$$m = \mathbb{E}[\cos \epsilon_n]. \tag{3.21}$$

In [7] and [8] are presented some methods to find the communication-optimal IRS configuration $\overline{\theta}$ for given $\boldsymbol{H}$ and $\boldsymbol{G}$. Note that the generic entry of the cascade channel matrix $\boldsymbol{Q}$ is

$$Q_{r,c} = \sum_n^N H_{r,n}\Phi_n G_{n,c} = \sum_n^N H_{r,n} e^{j\bar{\theta}_n} e^{j\epsilon_n} G_{n,c}. \tag{3.22}$$

Under the asymptotic assumption, for $N \to \infty$, the generic entry $Q_{r,c}$ has a Gaussian distribution with mean

$$m_{r,c} = \mathbb{E}[Q_{r,c}] = m \sum_n^N H_{r,n} e^{j\bar{\theta}_n} G_{n,c}, \tag{3.23}$$

and variance

$$\begin{aligned} \sigma_{r,c}^2 = \mathbb{E}[|Q_{r,c} - \mathbb{E}[Q_{r,c}]|^2] = \mathbb{E}\left[\left|\sum_n^N H_{r,n} e^{j\bar{\theta}_n} G_{n,c}(e^{j\epsilon_n} - m)\right|^2\right] = \\ \mathbb{E}\left[\sum_n^N H_{r,n} e^{j\bar{\theta}_n} G_{n,c}(e^{j\epsilon_n} - m) \sum_{n'}^{N'} H_{r,n'}^* e^{-j\bar{\theta}_{n'}} G_{n',c}^*(e^{-j\epsilon_{n'}} - m)\right] = \\ \sum_n^N \sum_{n'}^{N'} H_{r,n} H_{r,n'}^* e^{j\bar{\theta}_n} e^{-j\bar{\theta}_{n'}} G_{n,c} G_{n',c}^* \mathbb{E}[(e^{j\epsilon_n} - m)(e^{-j\epsilon_{n'}} - m)], \end{aligned} \tag{3.24}$$

so we have to study $\mathbb{E}[(e^{j\epsilon_n} - m)(e^{-j\epsilon_{n'}} - m)]$ distinguishing the two cases, i.e., $n = n'$ and $n \neq n'$. Hence,

$$\mathbb{E}[(e^{j\epsilon_n} - m)(e^{-j\epsilon_{n'}} - m)] = \begin{cases} \mathbb{E}[|e^{j\epsilon_n} - m|^2] = 1 - m^2, & \text{if } n = n', \\ \mathbb{E}[e^{j\epsilon_n} - m]\mathbb{E}[e^{-j\epsilon_{n'}} - m] = 0, & \text{if } n \neq n'. \end{cases} \tag{3.25}$$

Thus, the variance is

$$\sigma_{r,c}^2 = (1 - m^2) \sum_{n}^{N} |H_{r,n}|^2 |G_{n,c}|^2. \tag{3.26}$$

Furthermore, in general, different entries Q_{r_1,c_1} and Q_{r_2,c_2}, with $r_1 \neq r_2$ and $c_1 \neq c_2$, are correlated, i.e., by changing row and column, hence by changing $H_{r,n}$ and $G_{n,c}$, the entries are still defined by ϵ_n. Therefore, we're interested in $\mathbb{E}[Q_{r_1,c_1} Q^*_{r_2,c_2}], \forall r_1, r_2, c_1, c_2$, where $Q^*_{r_2,c_2}$ is the complex conjugate. Hence, $\boldsymbol{Q}$ is a matrix with correlated Gaussian elements, with correlation

$$\begin{aligned} Cov(Q_{r_1,c_1}, Q_{r_2,c_2}) &= \mathbb{E}[Q_{r_1,c_1} Q^*_{r_2,c_2}] - \mathbb{E}[Q_{r_1,c_1}]\mathbb{E}[Q^*_{r_2,c_2}] = \\ &= \mathbb{E}\left[\sum_{n}^{N} \sum_{n'}^{N'} P_{n,n'} e^{j\epsilon_n} e^{-j\epsilon_{n'}}\right] - m_{r_1,c_1} m_{r_2,c_2}, \end{aligned} \tag{3.27}$$

where $P_{n,n'} = H_{r_1,n} H^*_{r_2,n'} G_{n,c_1} G^*_{n',c_2} e^{j\bar{\theta}_n} e^{-j\bar{\theta}_{n'}}$, and m_{r_1,c_1}, m_{r_2,c_2} are computed as (3.23). So we obtain

$$Cov(Q_{r_1,c_1}, Q_{r_2,c_2}) = \sum_{n}^{N} \sum_{n'}^{N'} P_{n,n'} \mathbb{E}[e^{j\epsilon_n} e^{-j\epsilon_{n'}}] - m_{r_1,c_1} m_{r_2,c_2}. \tag{3.28}$$

As we did before, we have to distinguish in the two cases,

$$\mathbb{E}[e^{j\epsilon_n}e^{-j\epsilon_{n'}}] = \begin{cases} \mathbb{E}[|e^{j\epsilon_n}|^2] = 1, & \text{if } n = n', \\ \mathbb{E}[e^{j\epsilon_n}]\mathbb{E}[e^{-j\epsilon_{n'}}] = m^2, & \text{if } n \neq n'. \end{cases} \tag{3.29}$$

Thus, the correlation is

$$\begin{aligned} Cov(Q_{r_1,c_1}, Q_{r_2,c_2}) = \sum_n^N P_{n,n} + m^2 \sum_n^N \sum_{n'}^{N'} \sum_{n \neq n'} P_{n,n'} - m_{r_1,c_1} m_{r_2,c_2} = \\ (1 - m^2) \sum_n^N P_{n,n}. \end{aligned} \tag{3.30}$$

Finally, we're interested in $\mathbb{E}[C]$, i.e., ergodic capacity, of a random Gaussian channel with mean and correlation matrix, which is a Rice channel, and, as stated in [9] and [10], it is possibile to find the mean capacity.

3.2.2 Security Performance

The authentication mechanism is affected by two possible error events, that are FAs when Bob discards a message as forged by Eve while it is coming from Alice, and MDs when Bob accepts a message coming from Eve as legitimate. Precisely, an FA occurs when, under hypothesis $b = 0, \Psi \geq \tau$, while, an MD occurs when, under hypothesis $b = 1, \Psi < \tau$. Hence, the probabilities of FA and MD characterize the security metrics of the CR-PLA mechanism.

For a given Alice-IRS-Bob channel and any configuration $\mathbf{\Phi}'$. we define the probability of FA and MD respectively as

$$P_{FA} = P[\Psi \geq \tau | \hat{b} = 0], \tag{3.31}$$

$$P_{MD}(\zeta(\boldsymbol{V}, \boldsymbol{\Phi}')) = P[\Psi < \tau | \hat{b} = 1]. \tag{3.32}$$

Under the legitimate condition $\mathcal{H}_0$, by plugging (2.12) into (2.13), Ψ becomes a central chi-square variable with $2N_AN_B$ degrees of freedom and

$$P_{FA} = 1 - F_{\chi^2_{2N_AN_B},0(\tau)}, \tag{3.33}$$

where $F_{\chi^2_{2N_AN_B},a(\cdot)}$ is the cumulative distribution function (CDF) of a non-central chi-square variable with $2N_AN_B$ degrees of freedom and non-centrality parameter a.

Under hypothesis $\mathcal{H}_1$ with attack $\boldsymbol{V}_0$, using (2.10) and replacing (2.9) in (2.13) Ψ becomes a non-central chi-square random variable with $2N_AN_B$ degrees of freedom and non-centrality parameter

$$\zeta(\boldsymbol{V}, \boldsymbol{\Phi}') = \frac{2}{\sigma^2}||\boldsymbol{V} - \overline{\boldsymbol{Q}}(\boldsymbol{\Phi}')||^2, \tag{3.34}$$

for a given IRS configuration $\boldsymbol{\Phi}'$. The P_{MD} represents the CDF of this variable evaluated at τ, that is

$$P_{MD}(\zeta(\boldsymbol{V}, \boldsymbol{\Phi}')) = F_{\chi^2_{2N_AN_B},\zeta(\boldsymbol{V},\boldsymbol{\Phi}')}(\tau). \tag{3.35}$$

Where the choice of τ is tipically set to reach a desired P_{FA}, i.e.,

$$\tau = F^{-1}_{\chi^2,0}(1 - P_{FA}), \tag{3.36}$$

and the MD probability becomes

$$P_{MD}(\zeta(\boldsymbol{V}, \boldsymbol{\Phi}')) = F_{\chi^2_{2N_A N_B},\zeta(\boldsymbol{V},\boldsymbol{\Phi}')}(F^{-1}_{\chi^2,0}(1 - P_{FA})). \tag{3.37}$$

We now consider the average P_{MD}, i.e., $\overline{P}_{MD} = \mathbb{E}[F_{\chi^2_{2N_A N_B},\zeta(\boldsymbol{V},\boldsymbol{\Phi}')}(\tau)]$, assuming that $\boldsymbol{V}$ is fixed (i.e., Eve performs deterministic attacks), while $\boldsymbol{\Phi}'$ is random, and we express it as a function of key statistical parameters for ϵ_n, similarly to what we did for the average capacity.

Attack Strategy: Since Eve does not know the IRS configuration, we assume that Eve uses as attack the average channel seen by Bob when Alice is transmitting, i.e., she sets the attack channel as $\boldsymbol{V}_0 = \mathbb{E}[\boldsymbol{Q}]$, where the mean is evaluated with respect to the random IRS configuration. So,

$$\boldsymbol{V}_0 = \boldsymbol{H}\mathbb{E}[\boldsymbol{\Phi}]\boldsymbol{G} = \boldsymbol{H}\overline{\boldsymbol{\Phi}}\mathbb{E}[\mathrm{diag}\{e^{j\epsilon_n}\}]\boldsymbol{G} = m\boldsymbol{H}\overline{\boldsymbol{\Phi}}\boldsymbol{G}. \tag{3.38}$$

Test Variable: Under attack $\boldsymbol{V}_0$ (2.16) becomes

$$\boldsymbol{\delta} = m\boldsymbol{H}\overline{\boldsymbol{\Phi}}\boldsymbol{G} - \boldsymbol{H}\boldsymbol{\Phi}'\boldsymbol{G} + \boldsymbol{W} = \boldsymbol{H}(m\mathrm{diag}\{e^{j\overline{\theta}_n}\} - \mathrm{diag}\{e^{j\overline{\theta}_n}e^{j\epsilon_n}\})\boldsymbol{G} + \boldsymbol{W}. \tag{3.39}$$

MD Probability: Similarly to what we did with the cascade channel's matrix $\boldsymbol{Q}$, we note that the generic entry of the matrix $\boldsymbol{\delta}$ is

$$\delta_{r,c} = W_{r,c} + \sum_{n}^{N} H_{r,n}(me^{j\bar{\theta}_n} - e^{j\bar{\theta}_n}e^{j\epsilon_n})G_{n,c}, \tag{3.40}$$

where the term $e^{j\epsilon_n}$ is the only one changing. Under the asymptotic assumption, for $N \to \infty$, the generic entry $\delta_{r,c}$ has a Gaussian distribution with mean

$$\begin{aligned} m'_{r,c} = \mathbb{E}[\delta_{r,c}] = \mathbb{E}[W_{r,c}] + \mathbb{E}\left[\sum_{n}^{N} H_{r,n}(me^{j\bar{\theta}_n} - e^{j\bar{\theta}_n}e^{j\epsilon_n})G_{n,c}\right] = \\ = 0 + \sum_{n}^{N} H_{r,n}e^{j\bar{\theta}_n}G_{n,c}\mathbb{E}[(m - e^{j\epsilon_n})] = 0, \end{aligned} \tag{3.41}$$

and variance

$$\begin{aligned} \sigma'^2_{r,c} = Var[\delta_{r,c}] = Var[W_{r,c}] + Var\left[\sum_{n}^{N} H_{r,n}\left(me^{j\bar{\theta}_n} - e^{j\bar{\theta}_n}e^{j\epsilon_n}\right)G_{n,c}\right] = \\ = 2\sigma_B^2 + \mathbb{E}\left[\left|\sum_{n}^{N} H_{r,n}(me^{j\bar{\theta}_n} - e^{j\bar{\theta}_n}e^{j\epsilon_n})G_{n,c} - \mathbb{E}\left[\sum_{n}^{N} H_{r,n}(me^{j\bar{\theta}_n} - e^{j\bar{\theta}_n}e^{j\epsilon_n})G_{n,c}\right]\right|^2\right] = \\ = 2\sigma_B^2 + \mathbb{E}\left[\left|\sum_{n}^{N} H_{r,n}(me^{j\bar{\theta}_n} - e^{j\bar{\theta}_n}e^{j\epsilon_n})G_{n,c}\right|^2\right] = \\ 2\sigma_B^2 + \sum_{n}^{N}\sum_{n'}^{N'} H_{r,n}H^*_{r,n'}e^{j\bar{\theta}_n}e^{-j\bar{\theta}_{n'}}G_{n,c}G^*_{n',c}\mathbb{E}\left[(m - e^{j\epsilon_n})(m - e^{-j\epsilon_{n'}})\right]. \end{aligned} \tag{3.42}$$

As before, we distinguish the two cases, obtaining as in (3.25)

$$\mathbb{E}[(m - e^{j\epsilon_n})(m - e^{-j\epsilon_{n'}})] = \begin{cases} \mathbb{E}[|m - e^{j\epsilon_n}|^2] = 1 - m^2, & \text{if } n = n', \\ \mathbb{E}[(m - e^{j\epsilon_n})]\mathbb{E}[(m - e^{-j\epsilon_{n'}})] = 0, & \text{if } n \neq n'. \end{cases} \tag{3.43}$$

Hence, the variance becomes

$$\sigma'^2_{r,c} = 2\sigma_B^2 + (1 - m^2) \sum_n^N |H_{r,n}|^2 |G_{n,c}|^2. \tag{3.44}$$

We observe that, similarly to the matrix $\boldsymbol{Q}$, the entries are correlated, since ϵ_n appears in all of them, with correlation

$$\begin{gathered} Cov[\delta_{r_1,c_1}, \delta_{r_2,c_2}] = \mathbb{E}[\delta_{r_1,c_1}\delta^*_{r_2,c_2}] - \mathbb{E}[\delta_{r_1,c_1}]\mathbb{E}[\delta_{r_2,c_2}] = \\ \mathbb{E}[W_{r_1,c_1}W^*_{r_2,c_2}] + \sum_n^N \sum_{n'}^{N'} P_{n,n'}\mathbb{E}[(m - e^{j\epsilon_n})(m - e^{-j\epsilon_{n'}})], \end{gathered} \tag{3.45}$$

so we have to study all the cases.

$$\mathbb{E}[W_{r_1,c_1}W^*_{r_2,c_2}] = \begin{cases} \mathbb{E}[|W_{r,c}|^2] = 2\sigma_B^2, & \text{if } r_1 = r_2, c_1 = c_2, \\ \mathbb{E}[W_{r_1,c_1}]\mathbb{E}[W_{r_2,c_2}] = 0, & \text{if } r_1 \neq r_2, c_1 \neq c_2. \end{cases} \tag{3.46}$$

and, as in (3.25)

$$\mathbb{E}[(m - e^{j\epsilon_n})(m - e^{-j\epsilon_{n'}})] = \begin{cases} \mathbb{E}[|m - e^{j\epsilon_n}|^2] = 1 - m^2, & \text{if } n = n', \\ \mathbb{E}[m - e^{j\epsilon_n}]\mathbb{E}[m - e^{-j\epsilon_{n'}}] = 0, & \text{if } n \neq n'. \end{cases} \tag{3.47}$$

Thus, the correlation is

$$Cov[\delta_{r_1,c_1}, \delta_{r_2,c_2}] = \begin{cases} 2\sigma_B^2 + (1-m^2)\sum_n^N P_{n,n}, & \text{if } r_1 = r_2, c_1 = c_2, \\ (1-m^2)\sum_n^N P_{n,n}, & \text{if } r_1 \neq r_2, c_1 \neq c_2. \end{cases} \tag{3.48}$$

Hence, from (2.15), Ψ is a sum of squares of correlated Gaussian variables with mean not null. We're interested in the MD probability, i.e., $P(\Psi < \tau)$, and in its CDF. In [11], it is shown how to calculate the CDF of a linear combination of chi-square random variables.

3.2.3 Design of the pdf p_ϵ

For a desired $\overline{P}_{FA}$, we derived that m is the only parameter on which the communication and security metrics depend. Our goal is to find the optimal p_ϵ balancing the communication metrics and security requirements. From (2.18), we aim at finding a feasible p_ϵ such that $C_{A,B}$ is maximized assuring that $\overline{P}_{MD}(m,\tau)$ is kept below a certain threshold η.

Thus, we consider the following optimization problem

$$\begin{aligned} \arg\max_m \quad & C \\ \text{s. t.} \quad & \overline{P}_{MD}(m,\tau) < \eta \\ & \int_{-\infty}^{\infty} p_\epsilon = 1 \\ & P_{FA}(\tau) = \overline{P}_{FA} \\ & p_\epsilon \geq 0. \end{aligned} \tag{3.49}$$

Chapter 4

Conclusion

In this thesis, we have investigated the integration of an IRS in a CR-PLA mechanism, where the IRS is under the control of the receiver (Bob), whose goal is to verify the identity of the transmitter. In particular, our goal was to obtain a trade-off between communication and security performance, by properly designing the IRS configuration. Thus, we have derived the channel statistic, maximizing its capacity to enhance the communication performance. We then derived approximate expressions for the false alarm (FA) and missed detection (MD) probabilities, focusing on the channel statistic when under attack. Results show that by solving an optimization problem, a trade-off between communication and security performance can be obtained.

In conclusion, the integration of IRS in PLA presents a promising technology for enhancing wireless network security. In fact, significant improvements can be achieved in preventing Eve's attacks. This research demonstrates that IRS technology, when carefully optimized, can provide both robust security and improved communication performance. However, challenges remain in terms of practical implementation, particularly concerning the estimation of channel state information (CSI) and the optimal deployment of IRSs in large-scale networks. Future work should focus on these challenges and explore further innovations in IRS-assisted authentication mechanisms to meet the evolving security requirements of next-generation wireless networks.

Bibliography

[1] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless communications: A tutorial," *IEEE Transactions on communications*, vol. 69, no. 5, pp. 3313–3351, 2021.

[2] L. Crosara, A. V. Guglielmi, N. Laurenti, and S. Tomasin, "Divergence-minimizing attack against challenge-response authentication with IRS," *IEEE Inter. Conf. on Comm. (ICC Work.)*, 2024.

[3] S. Tomasin, H. Zhang, A. Chorti, and H. Poor, "Challenge-response physical layer authentication over partially controllable channels," *IEEE Communications Magazine*, pp. 138–144, 2022.

[4] S. Tomasin, T. N. M. M. Mohamed Elwakeel, A. V. Gugliemi, R. Maes, N. Noels, and M. Moeneclaey, "Analysis of challenge-response authentication with reconfigurable intelligent surfaces," *Submitted to IEEE Trans. Information Forensics and Security.*

[5] A. V. Guglielmi, L. Crosara, N. Laurenti, and S. Tomasin, "Physical-layer challenge-response authentication with IRS and single-antenna devices," *IEEE International Conference on Communications Workshops (ICC Workshops)*, 2024.

[6] M. M. Selim and S. Tomasin, "Physical layer authentication with simultaneous reflecting and sensing RIS," *IEEE 97th Vehicular Technology Conf. (VTC2023-Spring)*, 2023.

[7] Z. Yigit, E. Basar, and I. Altunbas, "Low complexity adaptation for reconfigurable intelligent surface-based MIMO systems," *IEEE Commun.*

[8] A. M. Sayeed, "Optimization of reconfigurable intelligent surfaces through trace maximization," *Proc. IEEE Inter. Conf. on Comm. (ICC Work.)*, pp. 1–6, 2021.

[9] L. Cottatellucci and M. Debbah, "On the capacity of MIMO Rice channels," *Proc. of the 42nd Allerton Conf.*, 2004.

[10] M. K. Ibraheem and H. M. AlSabbagh, "A comparison study for channel capacity of MIMO systems with Nakagami-M, Weibull, and Rice distributions," *International Journal of Science and Engineering Investigations*, 2013.

[11] S. J. Press, "Linear combinations of non-central chi-square variates," *The Annals of Mathematical Statistics*, 1966.

Grazie alla mia mamma,

che mi ha accompagnata in questo percorso mano nella mano, sopportando le mie innumerevoli crisi, ricordandomi sempre che ero in grado di affrontare tutto e che ero all'altezza di tutto. Grazie per tutte le volte che mi hai detto di essere orgogliosa di me.

Grazie al mio papa',

che con meno dolcezza ma ugual affetto, mi ha sempre spronata a fare il meglio che potessi, a diventare la miglior versione di me, anche se ovviamente il meglio rimane solo lui. Grazie per i baci sulla fronte che mi davi quando mi vedevi disperata sui libri.

Grazie alla Stefy,

sempre presente nei momenti di sconforto come in quelli di gioia, pronto all'occorrenza con un abbraccio e una parola di incoraggiamento.

Grazie alle mie amichette, Margherita e Agnese,

presenti in questo mio percorso fin dal giorno zero, sempre pronte ad ascoltare le mie lamentele, le mie paure, e sempre pronte a rassicurarmi e a supportarmi, congratulandovi con me per ogni piccolo traguardo, senza mai invidia, ma solo con pura amicizia.

Grazie ai miei amiconi, Giacomo e Sofia,

compagni di viaggio da ormai tanti anni, so che sono spalle su cui potro' sempre contare.

Grazie a tutta la mia grande famiglia allargata,
garanzia di poter trovare un sorriso, un abbraccio o una parola dolce
ovunque io mi giri.

Grazie alla mia dolce meta', Pietro,
che se la gioca con la mamma per le crisi che ha dovuto sopportare, che non manca mai occasione di ricordami che sono la migliore e che posso fare tutto, che mi supporta in ogni maniera possibile e che c'e' sempre per me.

E infine, grazie a me,
che ho vinto questa battaglia contro me stessa, sconfiggendo quella vocina che mi diceva che non ero in grado, e dimostrandole che si sbagliava.
Guarda dove sei arrivata Giulia con le tue forze, e guarda la strada che ti aspetta, pronta a essere percorsa con la stessa forza e determinazione con cui hai percorso questa.