University of Padova

Department of Information Engineering "DEI"

Master Thesis in Telecommunications Engineering

Physical Layer Authentication Using Intelligent Reflective Surfaces

Supervisor
Prof. Stefano Tomasin
University of Padova

Master Candidate
Tarek Nashat Mohamed Mohamed Elwakeel

Student ID
2004330

Academic Year
2021-2022

"You cannot provide total security, so the question is not just about how to prevent attacks, but how to survive them."
— Professor Holger Mey, Head of Advanced Concepts, Airbus Defence & Space, Germany.

Abstract

The Intelligent Reflective Surface (IRS) is one of the key technologies that will increase the coverage of cellular networks and enhance their performance at a low cost. Moreover, the IRS will improve the performance of the Channel-based Physical layer Authentication security mechanism. In this thesis, we propose an authentication scheme that takes advantage of the presence of the IRS in the IRS-assisted multiple input multiple output (MIMO) system to improve the security performance of the system. The proposed cascaded channel estimation authentication scheme has been developed and compared with a systematic channel estimation authentication scheme. We consider a non-line of sight communication between the transmitter and the receiver through the IRS. We will also demonstrate the efficiency of the proposed scheme by comparing it with one of the commonly used schemes. Moreover, we will formulate the optimal attack strategies to test the security of the proposed scheme. The performance of the proposed scheme is evaluated, and the numerical results show the merit of the proposed approach that can be adopted as a Physical layer authentication mechanism.

Contents

Listing of figures

Listing of tables

Listing of acronyms

3GPP ..... 3rd Generation Partnership Project
IoT ..... Internet of Things
IoE ..... Internet of Everything
TCP ..... Transmission Control Protocol
IP ..... Internet Protocol
TCP/IP ..... Transmission Control Protocol/Internet Protocol
SIM ..... Subscriber Identity Module
GSM ..... Global System for Mobile communications
MAC ..... Message Authentication Code
Mac ..... Media Access Control
UE ..... User Equipment
4G ..... Fourth Generation
LTE ..... Long-term Evolution
5G ..... Fifth-generation
PHY ..... Physical Layer
AFE ..... Analog Front End
CSI ..... Channel State Information
RSSI ..... Received Signal Strength Indicator
Node B ..... Radio Base Station Receiver
gNB ..... Next Generation Node B
IRS ..... Intelligent Reflecting Surface
IDFT ..... Inverse Discrete Fourier Transform
DFT ..... Discrete Fourier Transform
SISO ..... Single Input Single Output
SIMO ..... Single Input Multiple Output
MISO ..... Multiple Input Single Output
MIMO ..... Multiple Input Multiple Output
FA ..... False Alarm
MD ..... Missed Detection

LRT ..... Likelihood Ratio Test

GLRT ..... General Likelihood Ratio Test

ML ..... Maximum Likelihood

PDF ..... Probability Density Function

LLR ..... Logarithm of the Likelihood Ratio

I.I.D ..... Independent and Identically Distributed

CDF ..... Cumulative Distribution Function

MMSE ..... Minimum Mean Square Error

FHSS ..... Frequency Hopping Spread Spectrum

DSSS ..... Direct Sequence Spread Spectrum

THSS ..... Time Hopping Spread Spectrum

SNR ..... Signal-to-noise ratio

OSI ..... Open Systems Interconnection

AKA ..... Authentication and key agreement

IMSI ..... International Mobile Subscriber Identity

RAND ..... Random challenge

SRES ..... Challenge expected response

SRES' ..... Challenge response

UMTS ..... Universal Mobile Telecommunications System

AUTN ..... Authentication token

IK ..... Integrity key

XMAC ..... UE MAC

AMF ..... Authentication management field

AuC ..... Authentication center

EPS ..... Evolved Packet System

AV ..... Authentication vector

ASME ..... Access security management entity

USIM ..... User Services Identity Module

KDF ..... key derivation function

NAS ..... Non access stratum

AS ..... Access stratum

RRC ..... Radio resource control

RES ..... UE response

XRES ..... Expected response

eMBB ..... Enhanced Mobile Broadband

mMTC ..... Massive Machine-Type Communications

URLLC ..... Ultra reliable and low latency communications

LOS ..... line of sight

NLOS ..... Non line of sight

mmWave ..... Millimetre waves

RSS ..... Received signal strength

OFDM ..... Orthogonal frequency-division multiplexing

THz ..... TeraHertz

P2P ..... Peer-to-peer

SE ..... Spectral efficiency

EE ..... Energy efficiency

TA ..... Transmitter antenna

RA ..... Receiver antenna

MSE ..... Mean-squared error

SEAF ..... Security Anchor Function

AUSF ..... Authentication Server Function

UDM ..... Unified Data Management

ARPF ..... Authentication Repository and Processing Function

SUPI ..... Subscriber Permanent Identifier

SUCI ..... Subscription Concealed Identifier

1 Introduction

The transformation toward the digital world relies on the cable-free concept. Cellular networks starting from 5G are a suitable solution to replace cable networks, as 5G provides high data and low latency. The range of the 5G frequencies are expanded from 410 MHz to 71 GHz, and the higher the frequency, the higher the data rate is achieved. Short-range, obstruction, and object penetration are considered the most significant problems of high-frequency signals. IRS is one of the key technologies that will not only increase the coverage of cellular networks but also enhance its performance at a low cost. In this thesis, we will study the benefits of using IRS in cellular networks from a security perspective. We will develop an authentication mechanism that will take advantage of the IRS features.

In Chapter 2, we reviewed the cellular network security. Security rules in cellular networks are divided dependingly on which nodes on the networks are communicating. We will briefly review the concept of security in networks. We will study the security services provided in cellular networks. Cellular network security is divided into upper layers security and physical layer security. Upper layers security relies on AKA protocol, which is responsible for authentication and key agreements. Different versions of AKA protocol have been used in GSM, UMTS, LTE, and 5G. We will discuss the procedures of AKA protocol in all generations of cellular networks. One of the important aspects is physical layer security is securing the wireless part of the network. We will list different security mechanisms used in the physical layer. We focus on the channel-based authentication mechanism.

The IRS is discussed in Chapter 3. We will start with the hardware design of the IRS. We will study the different architectures of the IRS. We make a comparison between different architectures to facilitate choosing the most appropriate type for each cellular network implementation scenario. We will also study the advantages of using the IRS in cellular networks. We will discuss, from a security perspective, how IRS-aided the physical layer security solutions in protecting the communication content against eavesdroppers.

In Chapter 4, we consider our system model. Our system model is an IRS-assisted MIMO system including the transmitter, receiver, IRS, and attacker. We will develop a channel estimation scheme based on the IRS configuration. Moreover, we will develop an authentication scheme in the framework of hypothesis testing. Also,

we will apply two different attack strategies to evaluate the proposed authentication scheme. In the first strategy, the attacker knows the configuration of the IRS while in the second strategy, the attacker does not know the configuration of the IRS.

In Chapter 5, we will discuss the result of our simulation. We will evaluate the performance of the proposed channel-based authentication scheme for the IRS-assisted MIMO system. The results will be divided into two parts, the first one includes the investigation results of how accurate the proposed channel estimation scheme will be for the cascaded channel from Alice (UE) to Bob (gNB) through the IRS. In the second part, the proposed scheme will be evaluated against different attack strategies.

2

Cellular Network Security

Information security has become one of the most highlighted topics in the telecommunication field since the beginning of information transmission. Despite the effort of developing and implementing mechanisms to secure transmissions in cellular networks, the risk of attacks and information leakage during transmission always exists [8]. The digital revolution aims are connecting more things to the Internet from IoT to IoE through several communication channels. The increasing number of connected things will lead to more temps of attacks and threats. Thus, will drive to more sophisticated challenges to guarantee network security. To prevent the known vulnerability from being exploited, the need to corporate with new technologies and develop new security features has become mandatory to restrain attackers from entering the network. Cellular network security is one of the main vital topics, always under research and development.

The main security goals for any communication system are: confidentiality, integrity, availability, accountability, and privacy [9]. Any activity that can threaten one of the mentioned security goals is considered an attack. Security services are implemented by specific security mechanisms to prevent attacks and threats that might intimidate a security goal. Attacks may be performed on one or more security goals. The ontology of the goals, threats, services, and mechanisms is described in fig. 2.1 [1].

There are different cellular network security zones with different roles and security aspects. As in fig. 2.2, security zones can be categorized as internal and external. Zone 1 includes two different scenarios: 1) the communication between the home core network and external mobile network. 2) the communication between the home core network and the internet. Zone 2 refers to the communications between two nodes within the same core network. Zone 3 refers to the communication between the base station and the core network since they are geographically separated. Zone 4 refers to the wireless communication between the mobile network and the user equipment (UE).

In this thesis, zone 4 security will be discussed. Zone 4 includes security services between the cellular network and the user equipment, which is the wireless part of cellular networks. The authentication service will be the main focus of the thesis work. An authentication service aims are constraining forgery and masquerading threats

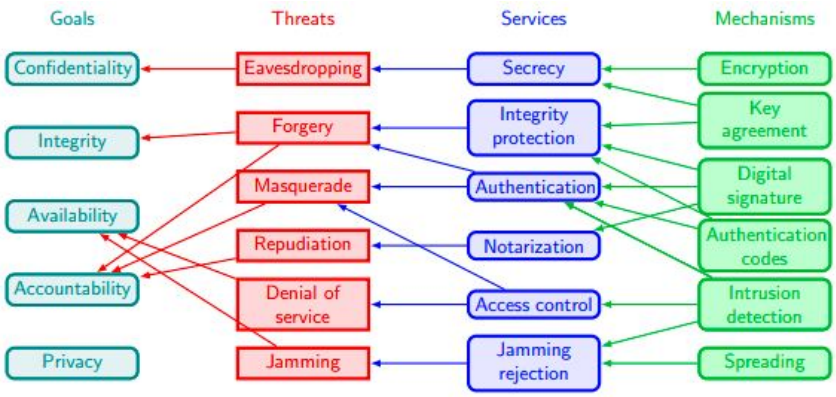

Figure 2.1: Security goals, threats, services and mechanisms [1].

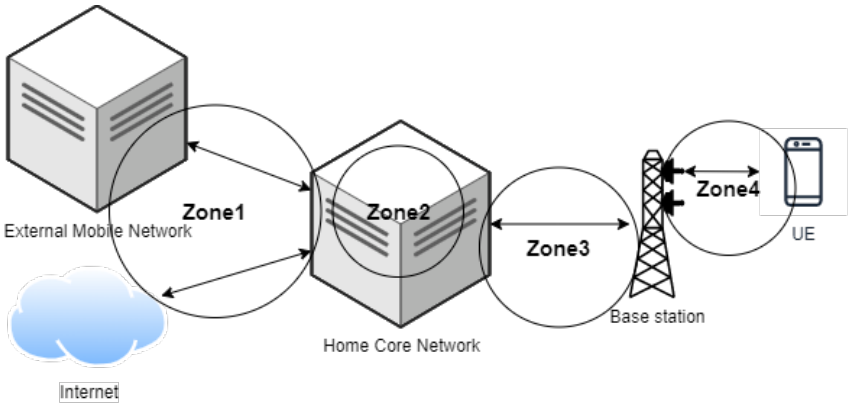

Figure 2.2: Mobile Network Security Zones Architecture.

to achieve the integrity goal of the network. An authentication security service allows the receiver to detect if the message that had been received was forged. In the cellular network, there are various mechanisms for different layers to achieve authentication service. On the other way, authentication services can relay on non-cryptographic mechanisms in the physical layer and cryptographic mechanisms in the upper layer. Mechanisms used in upper layers will be briefly discussed in section 2.1. More attention will be given to PLS in sections 2.2, 3.3, as it became a priority in the scientific research community for the last few years dedicating more efforts and time to developing security mechanisms at the physical layer.

2.1 Upper layer security

Upper layers refer here to all layers involved in data transmission between UE and cellular networks except the physical layer. Authentication has to be the first security service to be performed when UE requests access to the cellular network, however, authorization and further authentication might be requested from the UE to access other services. The act of confirming the validity of users is known as authentication, and it is the first step toward secure communication. Typically, the nodes agree on the same symmetric key after successful authentication to encrypt the communication channel. As a result, authentication data such as challenge and response are typically sent over the air in plain text, which adversaries can exploit. The AKA protocol is usually used to create mutual authentication and session keys for secure communication across a wireless channel between the UE, the serving node, and the authentication node, guaranteeing network access security. Although the serving node and the authentication node belong to the same security zone (Zone 2 in fig. 2.2), security rules between the nodes are being applied and the master key is not known to the serving node [10], [11].

AKA is a protocol suite defined to offer security features including authentication, integrity protection, and confidentiality. However, not all mentioned features were activated in the first version of the AKA protocol in GSM. The AKA protocol has been improved in parallel with each generation of the mobile network. The main nodes that follow the AKA protocol in all mobile network generations are UE, the serving node, and the authentication node. These nodes may have different names in each generation or the node functions could be divided into two independent nodes. UE and authentication nodes are always the same in all generations. The authentication procedures cannot be established without the interaction of these two nodes.

In fig. 2.3 [2], GSM authentication is a one-way authentication mechanism that allows the UE to connect to the cellular network. The algorithm uses a secret key K shared by the GSM authentication node and the UE. By submitting its IMSI to the BS, the UE identifies itself to the cellular network. The IMSI is routed through the BS to the authentication node. The authentication node retrieves the corresponding key K from its database, which is used in conjunction with the challenge $RAND$ to construct a session key $Kc = A8(RAND, K)$ and the expected response to the challenge $SRES = A3(RAND, K)$, where $A8$ and $A3$ are two hashing functions. The authentication node delivers the $(RAND, SRES, Kc)$ authentication vector to the BS, which will be used to authenticate the user. The UE generates as well the same session key Kc that has been generated by the authentication node; since it has the same hash function installed in its SIM card. The UE sends the $SRES'$ to the BS. The BS compares the $SRES'$ with the other $SRES$ received from the authentication node. If the two responses are matched, the UE identity is verified, otherwise, the connection will be discarded.

In fig. 2.4 [2], Mutual authentication is introduced in UMTS networks, where the UE authenticates the cellu-

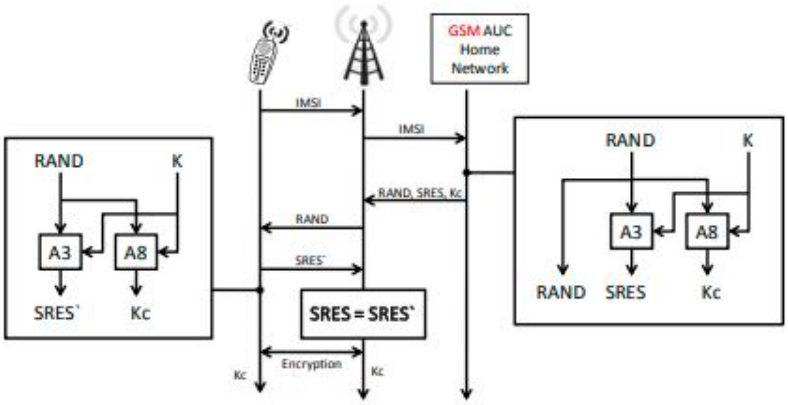

Figure 2.3: GSM AKA protocol scheme [2].

lar network and the cellular network authenticates the UE. This mutual authentication helps the UE to determine whether or not the network it is connecting to is legitimate. When choosing encryption and integrity algorithms, the AKA protocol uses integrity to ensure that the communication is not tampered with. With a few key differences, the authentication process follows many of the same network stages as the GSM standard. The authentication node sends both the *AUTN* and the *IK*. The *AUTN* token is transmitted to the UE, which processes the *RAND* with the key *K* to validate the *AUTN* token by verifying the *MAC* section of the token sent from the cellular network against the *XMAC* constructed with the key *K*, *sequence*, *AMF*, and *RAND*. The *AMF* token is a subset of the *AUTN* token. The sequence is also validated by the UE to ensure that it falls within the specified range. This verification allows the UE to trust the cellular network connection.

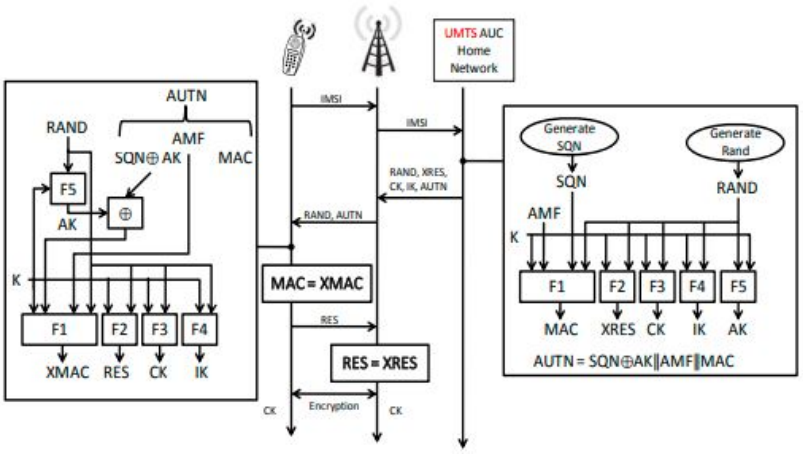

Figure 2.4: UMTS AKA protocol scheme [2].

The AKA used in UMTS has evolved in LTE networks as shown in fig. 2.5 [2] . The process begins with the BS forwarding an IMSI request to the authentication node. The modifications begin from the EPS AV vector, which contains $RAND$, $AUTN$, $XRES$, and K_{ASME}. K_{ASME} replaces CK and IK that were used in UMTS. The CK and IK values in the USIM, as well as the identification of the serving network, are the KDF inputs to generate K_{ASME}. The UE then validates the MAC and, in case of matching between MAC and $XMAC$, the UE responds with the RES for the network to verify the authentication procedure by comparing it to $XRES$, similar to the UMTS protocol. The $KASME$ is being utilized to generate keys in a key hierarchy, which is a significant shift in EPS. NAS, AS, and RRC are new different traffic kinds that will rely on different security keys that have been derived from the K_{ASME}.

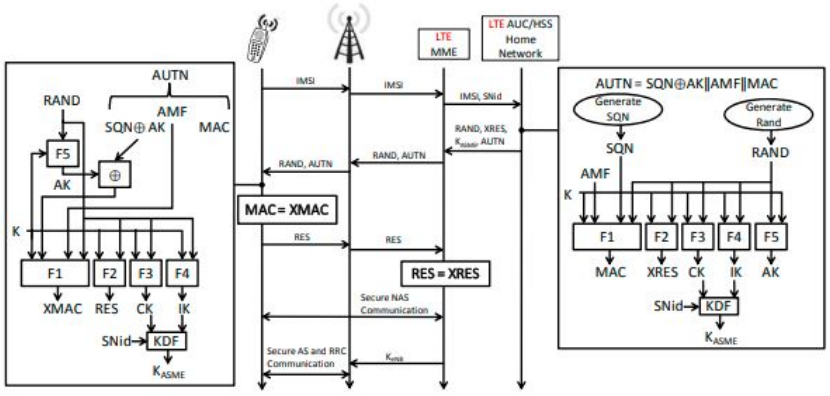

Figure 2.5: LTE AKA protocol scheme [2].

In fig. 2.6 [3], the UE, the SEAF, the AUSF, and the UDM/ARPF will be involved in the 5G-AKA authentication process. The SEAF will be included in the AMF and interacts with AUSF to get authentication data from UDM. It accomplishes UE authentication for different access networks. The ARPF stores subscribers' profiles and the information that is related to security. At the beginning of the authentication process, the UE will send its SUPI to the SEAF. Then, the SEAF will send the 5G-AIR (Authentication Initiation Request) to the AUSF. 5G-AIR contains SUCI or SUPI of the UE, the name of the serving network. This message also indicates that the UE has 3GPP access or non-3GPP access. After receiving authentication information requests from AUSF, UDM/ARPF generates AVs just like in the 4G system and then, transforms them into new AVs that are specific to 5G systems. In the case of the UE's successful authentication, the SEAF will send a 5G-AC (Authentication Confirmation) message in the 5G-AKA process. These messages are useful but not enough in protecting the system against some frauds like fraudulent Update Location requests for subscribers (a link is needed between the authentication result and the location update procedure)

On the other hand, AKA stands for cryptographic techniques that use digital keys. The level of security is determined by the computational difficulty. From a performance standpoint, it causes time delays and computational overhead [12]. Such a solution works when attackers have limited storage and computational capabilities; however, this is not always the case for high-capacity machines like quantum computers. All of the authentication challenges and responses are sent in plain text. Furthermore, data performance is limited because some bits

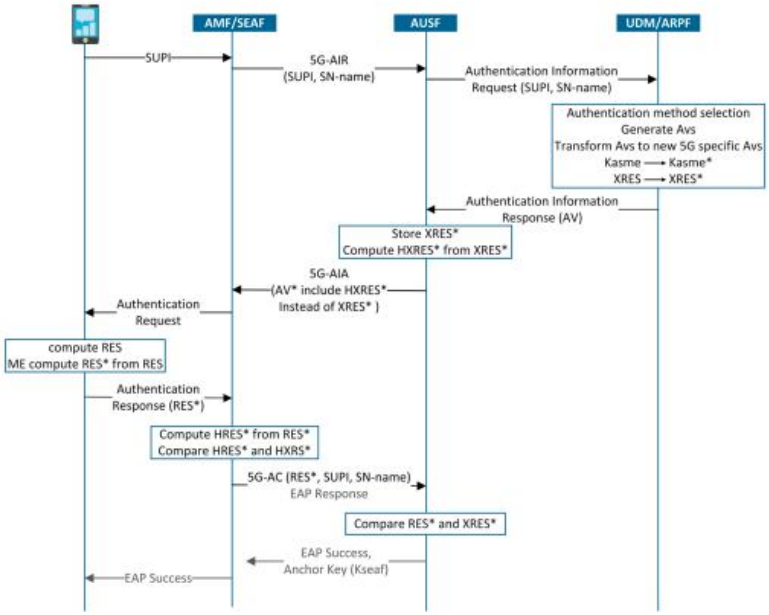

Figure 2.6: 5G AKA protocol scheme [3].

contain authentication rather than data. Attackers can listen in on them and obtain knowledge about the secret key. As a result, as the authentication time increases, the information entropy of the secret key falls, resulting in a high success rate of attacks [13].

2.2 Physical layer security

Frequency selection, signal detection, and modulation are all managed and selected by the physical layer. Physical layer security in wireless communication relies on advanced signal processing to control the air interface and does not require encryption or decryption using keys, resulting in some obvious benefits such as minimal complexity, low computational overhead, and low power consumption. The theoretical foundation for information security in physical layer security transmission is based on Shannon's notion of perfect secrecy from 1949 [14]. Shannon's absolute secrecy was established by ensuring that the key length is greater than or equal to the transferred data. The mutual information between the transmitted information between two legitimate nodes and the information received by the eavesdropper is used to measure the wiretap channel secrecy via the Wyner theorem [15]. On the same hand, when the legal user's channel condition is superior to the eavesdropper, the source and destination can securely transfer information. Csiszar and Korner demonstrated that the possible secrecy capacity for any memory-less channel is equal to the difference between the channel capacity between the source and the destination and the channel capacity between the source and the eavesdropper [16]. Physical layer attacks are divided into several categories. As described in fig. 2.7 [4], the authors of [4] outline the ontology of the attacks. These attacks fall

into two categories active attacks and passive attacks.

Interference and jamming are the most common active attacks. In essence, these two types of active attacks work in the same way by broadcasting interference signals on specified frequency bands. The failure of the transmitter is caused by jamming attacks that continue to occupy the channel. Interference attacks cause the receiver's failure by degrading the channel efficiency of the signal. The majority of jamming attempts are intended attacks, and interference is caused not only by attackers but also by other users on the same channel.

Eavesdropping and traffic analysis are the two most common types of passive attacks. The two attacks are caused via broadcast signals, which is a fundamental feature of wireless networks. Wireless communication's broadcast nature makes it harder to conceal transmitted signals from undesired recipients, while these legal or unlawful users inside the transmission range analyze and use wireless broadcast signals. Eavesdropping on other users' communication information causes information exposure issues and is simple to accomplish owing to open wireless channels. Traffic analysis attacks are based on determining changes in the flow of information in the network. Some attacks are provoked by extracting information from the ongoing transmission. In wireless networks, for example, an attacker can determine the position of the BS based on changes in channel conditions. In other words, the attacker interferes with the base station, causing the wireless network to collapse.

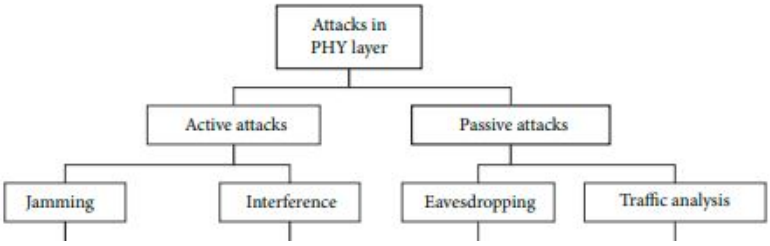

Figure 2.7: Attacks in PHY layer [4].

There are several techniques that have been developed to secure wireless networks against these types of attacks. These methods can be classified into three categories: spatial, frequency, and temporal domain. Directional antennas and some advanced beam-forming technologies are examples of spatial domain approaches. The system can achieve anti-interference and anti-jamming, as well as resist wiretapping, by using appropriate antenna technology to avoid signal interference or by realizing channel parameter randomization. The most widely used physical layer defense technology operates in the frequency domain, particularly the spread spectrum. It usually lowers or eliminates carrier frequency band interference by utilizing the carrier frequency's wide range and variability. Spread spectrum works on the premise of modulating the transmitted signal with a pseudo-random sequence, then demodulating the signal with the same pattern to retrieve the original signal. The SNR is increased during this procedure, and the interference's influence is reduced. In Time-domain, the main technique is channel coding. The inclusion of some check code in the channel coding can play an important function in rectifying the transmission of information. The receiver can utilize these symbols to check whether transmission information has an error or not and correct the error to reduce the influence of jamming attacks.

In table 2.1 [4], a comparison between different security techniques in the three domains is provided. It has been noted the techniques using randomness have a high ability to resist eavesdroppings like random antennas,

random parameters, and FHSS. An eavesdropper cannot effectively demodulate the proper information due to the randomization of weighting factors, channel characteristics, and carrier frequency. A combination of different techniques is necessary to reach a good probability of resistance against different types of attacks. Still, the combination of different techniques will lead to more complexity. The complexity is referring to the required storage spaces, computing capabilities, energy, or in some cases additional hardware units. Moreover, most of these techniques are depending on the channel condition and cannot be used in bad channel conditions.

Table 2.1: Comparison of PHY layer's security technique in wireless networks [4]

Secure technique	Type	Technical characteristics	Ability to defend against eavesdropping attacks	Ability to defend against jamming attacks	Ability to defend against interference attacks	Complexity
Directional antenna	Spatial domain	Increased receive gain in particular direction of space	low	Medium	low	low
Beam-forming		Superimposed multi-antenna signal	Medium	–	Low	High
Random antennas		Increased channel randomness	Higher	–	–	High
Artificial noise		Increased channel diversity	High	–	–	High
Random parameters	–	Increased signal randomness	Higher	–	–	High
FHSS	Frequency domain	Fast hopping of carrier frequency	Higher	High	–	Medium
DSSS		Increased bandwidth	–	Higher	Medium	Medium
Channel coding	Time domain	Powerful error correction capability	–	–	High	Low

2.2.1 Channel-based authentication

The communication channel is the medium by which signals pass through from the transmitter to the receiver. Typically, the signal is attenuated and noise is added to it during transmission. Many obstructions reflect radio waves transmitted in wireless channels and multiple propagation paths result from these obstructions. Direct

waves, diffracted waves, and, reflected waves are the three types of received waves with different time delays, phases, amplitudes, and additive noise. They will create significant fading. The receiver will need to recover the original signal by removing the channel's distortion. The information that the receiver receives regarding the channel characteristic is used to determine distortion and mitigate the effects of noise. The information provided can be reliably recovered as long as the receiver can predict the channel's effect on the transmitted signal. Channel estimation is the technique of categorizing the transmitter signal channel [17].

The channel estimation is a method of obtaining an estimate of the impulse response as quickly as feasible in order to recover the received signal. Fig. 2.8 [5] describes the position of channel estimation in a cellular network. Different methods of modulation, demodulation, and, detection have an impact on channel estimation. The modulation mode with variable amplitude is always employed in communication networks to maximize spectrum efficiency [18]. In this case, the receiver first should determine the exact CSI and then demodulate the received signal coherently. Estimating the channel is crucial. Regarding channel estimation technology, there are two main channel estimation approaches. The first is a training-sequence-based or pilot-based algorithm that can enable both rapid acquisition and accurate tracking. The channel's transmission efficiency is low as a result of the pilot occupying time slots or bandwidths elsewhere [5]. The second is blind channel estimation, which is based on the statistical feature of signal transmission. It has a high transmission efficiency and can save spectrum resources however; it takes a long time to obtain a good estimate [19].

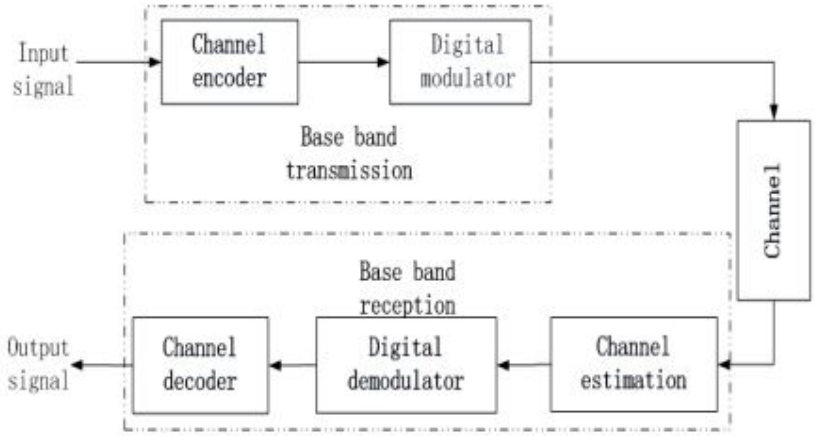

Figure 2.8: Transmitter and receiver operation chain [5]

The environment-dependent radiometric properties of a given transceiver pair, for instance, CSI or RSSI, are used in channel-based physical layer authentication [20]. The channel impulse response is often indicated by the CSI, whereas the RSS is normally defined by both the transmission power and the CSI. The CSI and RSS are location-specific due to path loss and channel fading, which is the basis for the authentication schemes [21]. The tracing of the dynamic properties of the channel linked with the sender (UE) and the receiver (BS) will ensure the legitimate sender (UE) identity and validity. Assuming that the AKA protocol completes the first authentication phase successfully as described in section 2.1, the receiver (BS) will begin comparing the estimated channel values of the newly received signals with the previous signals. Any irregular change in the channel's characteristics indi-

cates that the signal received is not from a legitimate user. On the same hand, the attacker who is in a different location than the legitimate user will have different CSI or RSS profiles as observed by the BS.

The authors of [22] introduced a channel-based authentication schema for time-invariant channels. This authentication scheme has been developed in the framework of hypothesis testing that suits MIMO systems in multiple wiretap channels environment. The model has studied three different agents: legitimate transmitter, intended receiver, and adversary. Each agent has access to multiple flat fading channels. GLRT has been used to distinguish the difference between the two hypotheses of the received signal at the intended receiver. Moreover, the assumption that the adversary estimated the channel between the adversary and the intended receiver and the channel between the adversary and the legitimate transmitter has been considered. Different attack strategies have been performed considering the above assumption to maximize the probability of breaking the authentication scheme and cracking the system to evaluate the developed scheme. The mentioned scheme showed good results in detecting the unauthorized signals that have been received from the attackers.

Although channel-based authentication schemes can be used to detect identity-spoofing attacks or authenticate/identify a particular user, they cannot achieve a 100 percent detection rate without raising false alarms. There is always a trade-off between the detection rate and the false alarm rate in these schemes. Moreover, channel-based authentication cannot be an independently utilized mechanism regarding that the BS will not have a first trusted CSI without using AKA protocol.

3

Intelligent Reflective Surfaces

The evolution of 5G technologies in the last decade enables the implementation of various applications through eMBB, mMTC, and URLLC 5G network's slices [23]. The demand for data rate and channel capacity has increased. The use of high frequencies that support a high data rate has become a necessity. The range of the 5G frequencies is expanded from 410 MHz to 71 GHz [24]. The plan includes achieving an upper range of frequencies up to 114.25 GHz. Short-range, obstruction, and object penetration are considered the most significant problems of high-frequency signals. A promising solution for future wireless communication systems is the IRS [25]. An IRS is a 2D reflecting meta-surface that consists of large numbers of sub-wavelength reflecting elements (meta-atom). The IRS can tune the phase shift of all incoming signals to control the angle of reflection. The IRS provides real-time manipulation to the wireless propagation environment. The use of an IRS-assisted 5G cellular network will reduce the cost and energy consumption. IRS is remarkably compatible with other existing physical layer wireless technologies as it focuses on signal propagation over wireless channels, whereas the other techniques are primarily implemented at transceivers. There is a significant consistency between the low-complexity property of physical layer security and the low-complexity hardware of IRS, which enhances the capability of integration as an ideal technique guaranteeing a convinced level of secrecy in low-complexity or dynamic wireless networks (e.g., IoT, IoE, D2D networks). Furthermore, their incorporation is beneficial in a variety of URLLC application scenarios due to their low complexity, which requires little signal processing time and thus helps reduce communication latency. The IRS will also hold more difficult competitions for attackers.

3.1 IRS architectures

There are different architectures of the IRS under development and examination. The studies included the differences of each IRS architecture design enumerating their pros and cons. This would help to choose the most appropriate type for each cellular network implementation scenario [26]. The first comparison is between passive-IRS

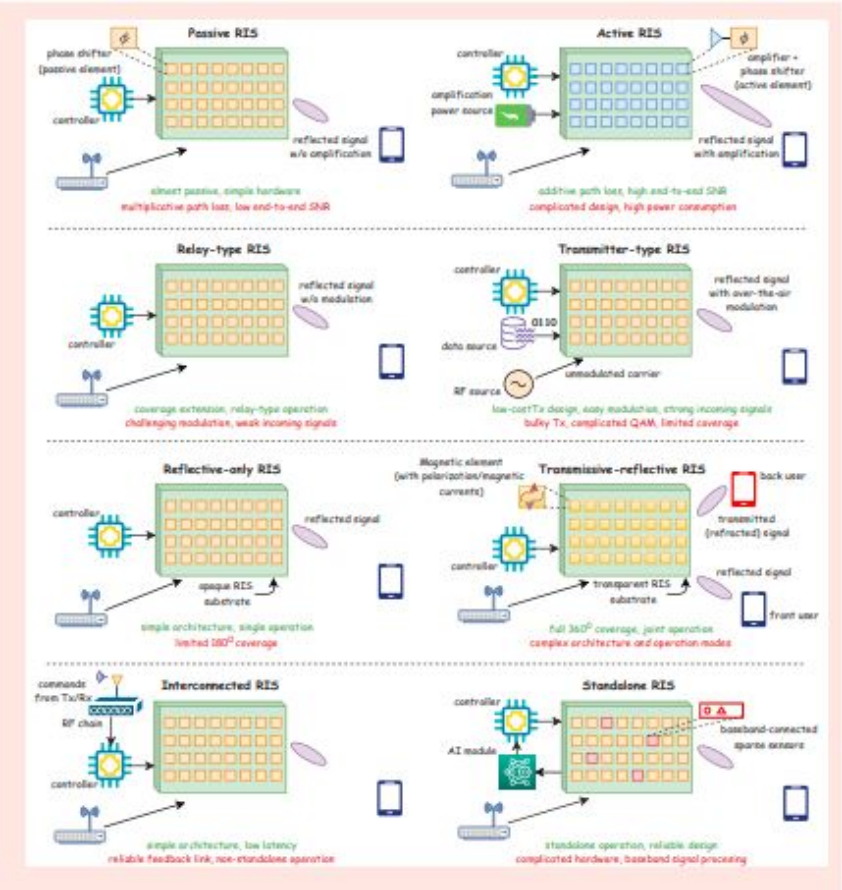

Figure 3.1: A comparison of different IRS architectures with their pros and cons [5].

and active-IRS. The main difference is that the active-IRS amplifies the power of the signal by its active RF electronics. The power amplification feature in active-IRS solves the multiplication path loss effect limitation problem in passive-IRS. The second comparison is between relay-IRS and transmitter-type-IRS. The transmitter-type-IRS is able to create virtual signal constellations for the incoming modulated carrier signal. The transmitter-type-IRS has two main advantages over traditional systems. The first advantage is that the hardware implementation is simpler by using an RF digital to analog converter with internal memory. The second advantage is that the multiplicative path loss effect is delimited. The third comparison is between reflective-only-IRS and transmissive-reflective-IRS. The reflective-only-IRS improves the signal condition only if the transmitter and the receiver are on the same side of the IRS. The transmissive-reflective-IRS is able to reflect the incoming signal on the frontal side and retransmit it from the backside. The transmissive-reflective-IRS will provide full 360-degree coverage. The fourth comparison is between interconnected-IRS and standalone-IRS. The interconnected-IRS interacts with the transmitter through a communication link; the transmitter provides guidance to the IRS with the required phase shift and amplitude modification for the incoming signal. The main idea of the standalone IRS is to replace the information coming from the transmitter through the communication link with an artificial intelligence algorithm; ending the need for that communication link. An artificial intelligence algorithm will optimize the configuration of the controller for the incoming signal in real time. Moreover, the integration between two or more IRS architectures is still under research.

The main pros and cons of each IRS architecture have been highlighted in fig. 3.1 [5]. Moreover, the future image of the upcoming IRS architecture is a combination of various architectures cons. The IRS architecture combination might be settled by splitting the surface of the IRS into areas meanwhile each area retains its own architecture as shown in fig. 3.2 [5]. The different implementations of the IRS architectures will not affect the process of channel estimation that will be used for authentication. In this thesis, the combination of passive-IRS and interconnected-IRS architecture has been implemented in IRS-assisted MIMO cellular networks to study the impact of IRS presence during the channel estimation process.

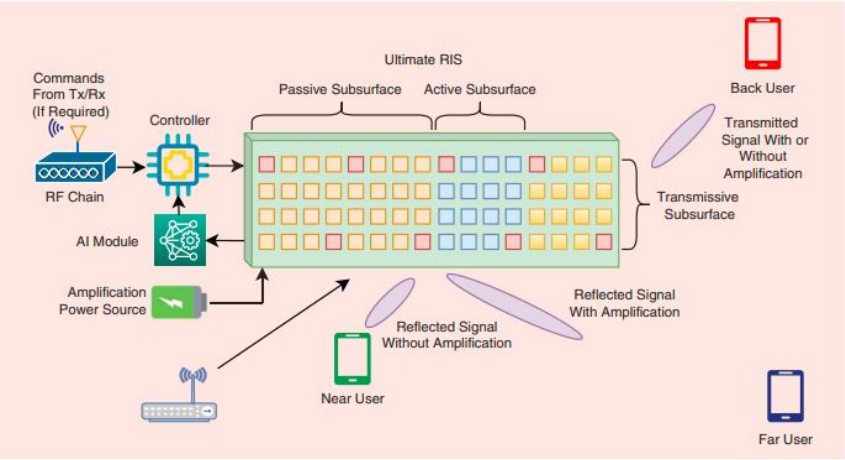

Figure 3.2: The ultimate RIS architecture composed of different sub-surfaces for improved flexibility [5].

3.2 IRS in cellular networks

In cellular systems, the IRS is placed between the BS and UE with different use cases despite the best position of the IRS is to be adjacent to the BS or the UE in order to avoid the multiplicative path loss effect, especially with passive-IRS. The IRS enhances the communication rate in LOS and NLOS scenarios. The IRS manipulates the radio environment by tuning the meta-surface elements with low-noise amplification and does not require either analog-to-digital converters or power amplifiers. The meta-surface elements tuning is executed by the IRS's controller. The IRS's controller is devoted to receiving and communicating the reconfiguration requests after that, distributing the phase shift decisions to all the tunable elements. As discussed in [7], different works studied several use cases of IRS implementation in cellular networks. The case studies include varieties of systems: THz system, OFDM system, mmWave system, Wide-band system under Beam Squint, and Sub-6 GHz Narrow Band system. Moreover, different communication scenarios (SISO scenario, MISO/SIMO scenario, and MIMO scenario) are considering single user and multiple users in up-link and down-link with different characteristics, such as narrow-band or wide-band transmissions, LOS or NLOS links, perfect or imperfect CSI, and different metrics to optimize the overall system performance has been discussed as well. As a result, an improvement in the performance metrics has been noted by implementing the IRS in the network including all use cases. In this thesis, the up-link signals in IRS-assisted MIMO system cellular networks will be discussed.

The fact that the presence of the IRS in the cellular network improved the performance inspires a lot of scientific research. Moreover, the development of different schemes has been done to enhance the performance of the IRS in cellular networks. The implementation of IRS in P2P MIMO communication networks in LOS environments has been studied in [27], [28]. The improvement of the channel capacity using IRS-assisted MIMO networks has been proven. An optimization scheme has been proposed to optimize the IRS configuration that aims to maximize the channel capacity. The channel rank improvement ability of the IRS-assisted technology to a P2P MIMO communication system has also been demonstrated using a specific optimization scheme [29].

In [6], an IRS-aided MIMO cellular network is proposed with M BS' transmitter antennas, K UE' receiver antennas, and L IRS' elements. IRS elements are co-located on an IRS array mounted on the same building positioned at the center of the disc, where IRS elements simultaneously serve the users as shown in fig. 3.3 [6]. The mmWave network operates in a NLOS scenario, where there are obstacles blocking the direct link between BS and all users. Moreover, a direct communication link between the BS and the IRS controller has been considered. Stochastic geometry-based performance analysis has been performed considering Outage Probability, Ergodic Rate, spectral efficiency, and energy efficiency. The explanation of how these parameters have been obtained in the proposed system has been proved by the authors.

The numerical results of performance analysis proved important facts to be considered [6]. First, increasing the number of IRS elements will significantly reduce the OP. Second, as the SNR increases, the OP decreases. Third, the fading parameter of the IRS-user link has almost no effect on the OP, which mainly depends on the channel between the BS and the IRS. Fourth, the ergodic rate can be significantly increased by employing more IRS elements, which are capable of effectively enhancing the spatial diversity gain. Fifth, the increasing number of TAs and IRS elements will lead to the network's throughput increase. Note that no solution exists at the IRS in the case of $L < MK$, hence the network's SE is zero. Sixth, as the number of TAs, RAs, and IRS elements increases, the network's EE increases, since the increase in numbers of RAs, TAs, and IRS elements is capable of

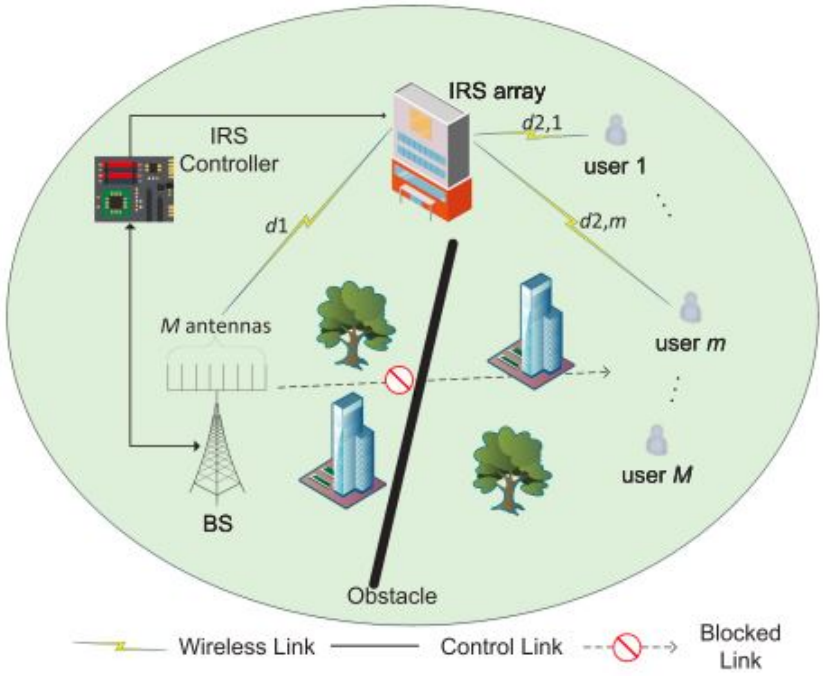

Figure 3.3: IRS assisted wireless transmission model [6].

increasing the spatial diversity gain.

3.3 IRS-assisted cellular networks PLS

IRS yields a significant improvement in wireless communication not only by improving signal quality but also by improving security. IRS-aided physical layer security solutions can protect the communication content against an eavesdropper. IRS is able to hide the existence of wireless transmission to preserve a user's privacy against an eavesdropper. The IRS's ability to tune phase shifts and amplitudes guiding the signal toward the receiver makes the legitimate channel better than the eavesdropper. With a periodically changeable configuration of the IRS, eavesdroppers will not be able to select the correct channel. IRS can be also utilized to confuse eavesdroppers by emitting artificial noise [30].

The advantage of using the IRS in wireless systems from the security point of view has been highlighted in fig. 3.4 [7]. The figure includes the effects of using the IRS against four types of attacks, explained before in section 2.2. Fig. 2a clarifies a baseline system model where the legitimate transmitter (Alice) intermittently transmits data to both the intended receiver (Bob) and the adversary (Willie). The IRS can be used to accomplish signal intensification at Bob and signal cancellation at Willie in this case. As a result, an enhanced transmission rate at Bob and a low probability of detection at Willie might both be achieved at the same time. Alice can also do wireless power transfer or simultaneous wireless information and power transfer to supply energy to Bob in a wireless-powered covert communication system when Bob has RF energy harvesting capacity. The IRS can also be used to assist wireless power transmission in addition to establishing cover communications. Fig. 2b clarifies a scenario in which Alice uses mmWave for covert transmission, which is prone to obstructions due to high penetration losses and poor diffraction of NLOS links. When a blockage exists between Alice and Bob, as demonstrated, deploying an IRS with LOS links to both Alice and Bob can be used to mitigate the negative impact of the obstruction on mmWave covert communication. Fig. 2c shows a scenario in which the baseline system is harmed by co-channel interference, such as that caused by malicious jammers. To keep the signal hidden from Alice, the IRS can be programmed to do interference cancellation at Bob and interference intensification at Willie. Legitimate users may face an eavesdropping attack, as demonstrated in Fig. 2d, in addition to the harmful effects of co-channel interference. To deal with the simultaneous attacks, signal cancellation at both the eavesdropper and Willie is required [31].

The advantages of involving the IRS in the cellular network to enhance the physical layer security was first demonstrated by considering a challenging scenario, where the quality of the main channel from a legitimate transmitter (Alice) to an intended receiver (Bob) is lower than that of the eavesdropper's channel from Alice to an eavesdropper (Eve). According to the Csiszar-Korner theorem in secrecy capacity, the maximum achievable secrecy capacity is the difference between the maximum capacity achieved in the channel between Alice and Bob, which is called the main channel capacity, and the maximum capacity achieved in the channel between Alice and Eve, which called eavesdropper's channel capacity. In such a scenario without the aid of the IRS, secrecy capacity is not achievable if each of the legitimate transceivers is equipped with a single antenna, since the main channel capacity is lower than the eavesdropper's channel capacity. The increasing numbers of IRS elements increase the efficiency of the IRS in such a scenario [32].

Many works have been done on the development of the secure techniques that were used in a regular wireless

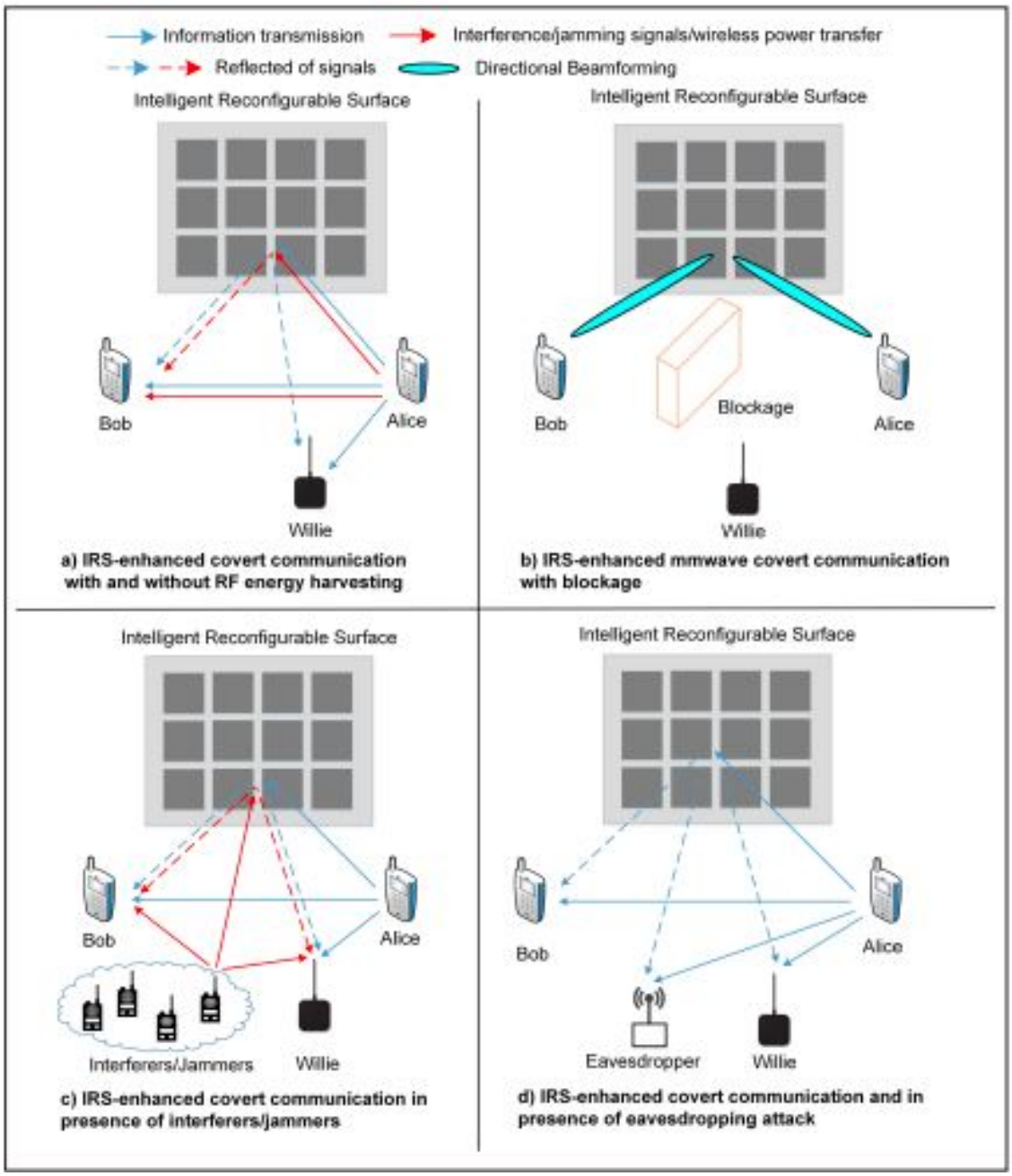

Figure 3.4: IRS-enhanced covert communication systems [7].

network as explained in table 2.1. These new works developed new schemes to maximize the advantage of using the mentioned techniques in the presence of the IRS in the cellular network. The use of the beam-forming technique in IRS-assisted MIMO systems, while an active eavesdropper is available in the network, has been experimented. In this scenario, the eavesdropper performs an active pilot attack to corrupt the channel estimation at the base station. An algorithm has been developed that designs beam-forming vectors, as well as the phase shifts at the IRS, meanwhile, the active attacker is blinded [33]. Moreover, the study indicates that as long as the legitimate and malicious are statistically distinguishable in the presence of the IRS, eavesdroppers are significantly restrained using the proposed technique for beam-forming and phase-shift tuning. Other algorithms have been proposed to improve the IRS security against both jamming and eavesdropping attacks with uncompleted information, exploring the joint active transmit and passive reflecting beam-forming optimization approach to maximize the system attainable rate given transmit power and secrecy rate restrictions [34].

The targets of the attacks mentioned above are: first, distract the network by enforcing the legitimate receiver to reject legitimate messages (such as jamming, interference, etc..), and second, increase the probability that forged messages could be accepted as legitimate by collecting any lack of information (for instance, eavesdropping, traffic analysis, etc.). Although the work on the developed techniques to prevent these types of attacks archived great results, there is a probability that these attacks can successfully archive their targets. Eavesdropping attacks could be an initiation for collecting information regarding specific channel communication to commence a forgery attack. Channel-based authentication mechanisms mitigate forgery attacks. The presence of IRS in the cellular network will alter the channel estimation scheme' procedures that have been discussed in section 2.2 and necessarily alter the channel-based authentication schemes that are used in regular cellular networks.

Many works have been done on channel estimation in cellular networks regarding the presence of the IRS in cellular networks. In [35] a channel estimation for IRS-assisted MIMO systems has been developed considering the UE possesses exclusively one antenna which is not the regular case in most 5G UE hardware. In [36], the development of a two-stage algorithm has been explained which includes a sparse matrix factorization stage and a matrix completion stage for channel estimation of IRS-assisted MIMO systems. Moreover, the evidence of the proposed two-stage method's accuracy has been proved despite the complexity of two-stage algorithm procedures. However, the evaluation of the available channel-based authentication schemes against forgery attacks is not considered in most of the published work. In the next chapter, we propose a low-complex channel estimation scheme and the evaluation of the proposed channel-based authentication scheme against different types of attacks.

4

Authentication with IRS

We consider a simple case where there is no direct link between the gNB (intended receiver/BS) and UE (legitimate transmitter). The IRS will enable the connection between them and will change the channel, since it affects the phase shift and the attenuation of the signal.

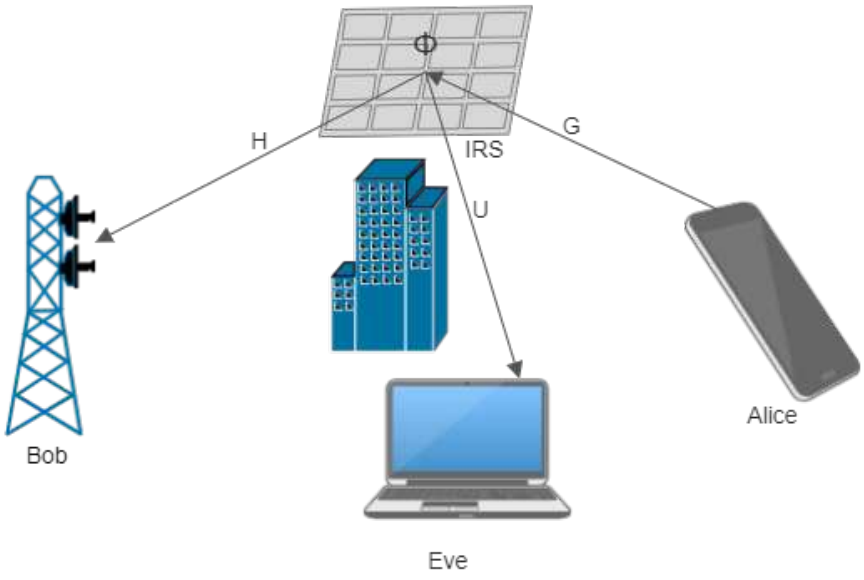

Figure 4.1: An IRS-assisted MIMO communication system

In Fig. 4.1, we model our system as follows:

- Alice: The legitimate transmitting UE with K antennas.
- IRS: The reflecting surface with N elements.
- Bob: The intended receiving gNB with M antennas.
- Eve: The attacker with V antennas.

We have

- $\boldsymbol{H}$: the $M \times N$ channel from the IRS to Bob
- $\boldsymbol{G}$: the $N \times K$ channel from Alice to the IRS
- $\boldsymbol{U}$: the $V \times N$ channel from the IRS to Eve.

4.1 Channel Estimation

For the IRS, the signal received by element n is reflected by the element with a complex gain φ_n. Let us define the matrix of IRS configuration

$$\Phi = \text{diag}(\varphi_0, \ldots, \varphi_{N-1}) = \text{diag}(\varphi). \tag{4.1}$$

Let

$$\boldsymbol{Q}^{(A,I,B)} = \boldsymbol{H}\Phi\boldsymbol{G} \tag{4.2}$$

be the cascaded channel from Alice to Bob through the IRS.

When Alice transmits the K-size column vector signal $\boldsymbol{X}$, the received M-size column vector signal at Bob is

$$\boldsymbol{Y} = \boldsymbol{Q}^{(A,I,B)}\boldsymbol{X} + \boldsymbol{W}, \tag{4.3}$$

where $\boldsymbol{W}$ is the M-size vector of additive white Gaussian noise (AWGN) with zero mean and variance σ_r^2 per entry.

4.1.1 IRS

As we have mentioned before, the IRS configuration affects the phase shift and the power attenuation. Each φ_n in (4.1) is called the reflection coefficient and consists of two parts

$$\varphi_n = A_n(\theta_n)e^{j\theta_n}, \tag{4.4}$$

where $A_n(\theta_n)$ affects the amplitude of the signal and $e^{j\theta_n}$ adjusts the phase shift, and $\theta_n \in [-\pi, \pi]$.

We notice here that the parts related to amplitude and phase shift adjustments both depends on θ_n. For the amplitude part, from [37], we have

$$A_n(\theta_n) = (1 - A_{min})\left(\frac{\sin(\theta_n - \Omega) + 1}{2}\right)^{\upsilon} + A_{min}, \tag{4.5}$$

where A_{min}, Ω and $\upsilon \geqslant 0$. A_{min} is the minimum amplitude, Ω is the horizontal distance between $-\pi/2$, and υ controls the steepness of the function curve. The three parameters are related to circuit design, manufacture, and fabrication of the IRS elements, and are considered constant for all elements of the same IRS.

In the upcoming sections, we will also consider a simplified model where $A_n(\theta_n) = 1$ and φ_n will depend only on $e^{j\theta_n}$.

4.1.2 Cascaded Channel estimation proposed scheme

Channel estimation is a process to figure out the characteristics of the cascaded channels that signals passed through. Channel estimation is the base reference for authentication. The estimated cascaded channels reference is based on a pilot signals sent from Alice to Bob. The pilot signals are the pre-known signals to all users. let $\boldsymbol{X}_p$ be a $K \times K$ matrix of the K pilot vectors transmitted by Alice. Correspondingly, Bob will receive the $M \times K$ matrix $\boldsymbol{Y}$. By multiplying both sides of (4.3) by $\boldsymbol{X}_p^{-1}$, we have

$$\hat{\boldsymbol{Q}}(\Phi) = \boldsymbol{Y}\boldsymbol{X}_p^{-1} = \boldsymbol{Q}^{(A,I,B)} + \boldsymbol{W}\boldsymbol{X}_p^{-1}, \tag{4.6}$$

where $\boldsymbol{X}_p$ and $\boldsymbol{Y}$ are known. Thus, (4.6) provides an estimate of the cascaded channel $\boldsymbol{Q}^{(A,I,B)}$. Note that from the estimate of the cascade, it is not possible to estimate channels $\boldsymbol{H}$ and $\boldsymbol{G}$, thus whenever we change the IRS configuration we must re-estimate the cascade. Here we consider a procedure by which estimating the cascade for a finite number of configurations, we can then infer the cascade for any other configurations.

Let $\boldsymbol{F}$ be the $N \times N$ Fourier matrix with entries

$$[\boldsymbol{F}]_{m_1,m_2} = e^{-2\pi j \frac{m_1 m_2}{N}} \qquad \begin{matrix} m_1 = 0,1,\ldots,N-1 \\ m_2 = 0,1,\ldots,N-1 \end{matrix}, \tag{4.7}$$

By reshaping the Inverse Discrete Fourier Transform (IDFT) of vector φ, we define vector

$$\beta = [\beta_0,\ldots,\beta_{N-1}]^T = \boldsymbol{F}^{-1}\varphi. \tag{4.8}$$

Now, matrix Φ can be written as

$$\Phi = \operatorname{diag}\left(\sum_{n=0}^{N-1} \beta_n \boldsymbol{b}_n\right), \tag{4.9}$$

where $\boldsymbol{b}_n$ is the n-th columns of matrix $\boldsymbol{F}$.

We also have

$$\hat{\boldsymbol{Q}}_n = \boldsymbol{H}\Phi_n\boldsymbol{G} + \boldsymbol{W}\boldsymbol{X}_p^{-1} = \boldsymbol{H}\operatorname{diag}\{\boldsymbol{b}_n\}\boldsymbol{G} + \boldsymbol{W}\boldsymbol{X}_p^{-1}. \tag{4.10}$$

From (4.6), the cascaded channel for any IRS configuration Φ can be written as the linear combination of the cascaded channels with IRS configurations $\Phi_n = \operatorname{diag}\{\boldsymbol{b}_n\}$ by coefficients given by the DFT of the vector φ. Therefore, a channel estimation procedure maybe written as follows :

- estimate the cascaded channels $\hat{\boldsymbol{Q}}(\Phi_n)$ from (4.6), when $\{\Phi_n = \operatorname{diag}\{\boldsymbol{b}_n\}\}$, for $n = 0,1,\ldots,N-1$.

- For any configuration $\Phi = \text{diag}\{\varphi\}$, the estimate of the cascaded channel for this IRS configuration is

$$\hat{\boldsymbol{Q}} = \sum_{n=0}^{N-1} \beta_n \hat{\boldsymbol{Q}}_n. \tag{4.11}$$

4.2 Channel-based authentication

From security perspective, the use of IRS will improve the security of the system. One of security authentication methods is the physical layer authentication using channel estimation. The use of IRS will increase the information needed by the attacker Eve to estimate the cascaded channel between Bob and Alice and break the authentication system.

4.2.1 Authentication

The initial step for Alice is to establish a connection with Bob. There will be an upper layer authentication procedure (AKA protocol) that we assume it's already obtained. Alice will send to Bob a training sequence and form (4.6), Bob will be able to estimate the channels, therefore Bob will build his own channel estimation code-book. After, a random IRS configuration $\Phi^{'} = \text{diag}\{\varphi^{'}\}$ will be chosen. Bob will receive a new signal and estimate the cascaded channel of the signal with two different procedures. From (4.6), Bob will estimate the exact cascaded channel $\hat{\boldsymbol{Q}}^{(A,I,B)}$ from the received signal and will be defined as

$$\hat{\boldsymbol{Q}}^{(A,I,B)} = \boldsymbol{Q}^{(A,I,B)} + \boldsymbol{W}^{B}. \tag{4.12}$$

From (4.11), Bob will predict the channel of the received signal $\hat{\boldsymbol{Q}}$ using the channel estimation reference table. Bob will compare the estimated cascaded channel $\hat{\boldsymbol{Q}}$ with the predicted channel $\hat{\boldsymbol{Q}}^{(A,I,B)}$. Bob should accept the signals coming from Alice and reject any other received signals.

Eve's aim is to know the IRS configuration and estimate the channel between her and Bob, her and Alice. we will discuss different attack scenarios in attack strategies section. For now, we will focus on how can Bob distinguish between Alice's signals and unknown signals. Let's assume that Eve will try to break the authentication system by a matrix $\boldsymbol{Z}$ which is a combination between the observed channels multiplied by another matrix aiming to have Bob's channel estimation of $\boldsymbol{Z}$ equivalent to the cascaded channel between Alice and Bob $\hat{\boldsymbol{Q}}^{(A,I,B)}$.

4.2.2 Distinguishability

Let $\hat{\boldsymbol{Q}}$ be the channel estimated by Bob for the new received signal. The two hypotheses for Bob are :

- H_0 : packet is from Alice,

$$\hat{\boldsymbol{Q}} = \hat{\boldsymbol{Q}}^{(A,I,B)} + \boldsymbol{W}^{''}, \tag{4.13}$$

- H_1 : packet is not from Alice,

$$\hat{\boldsymbol{Q}} = \boldsymbol{Z} + \boldsymbol{W}'' . \tag{4.14}$$

where $\boldsymbol{W}''$ is AWGN with zero mean and variance $\sigma_{''}^2$ per entry and $\boldsymbol{Z}$ is the equivalent channel forged by Eve at transmission t. We allow $\sigma_{'}^2 \neq \sigma_{''}^2$ because the channel estimation for $\hat{\boldsymbol{Q}}^{(A,I,B)}$ and $\hat{\boldsymbol{Q}}$ could have different noise levels on the estimates.

In the upcoming sections, we will highlight the single channel estimation, neglecting the transmission index t.

Generalized Likelihood Ratio Test

In order to decide between the hypothesis H_0 and H_1, a suitable test must be applied as in [22]. Since there is noise in channel estimation, no test is error free. The errors are divided in two types that can happen : a) a false alarm (FA) and b) a missed detection (MD). FA occurs when Bob rejects an incoming message from Alice. MD occurs when Bob accepts an incoming message from Eve. Moreover the idea of avoiding the two errors are conflicting. The test that reduces the MD probability, for a given FA probability, is the likelihood ratio test (LRT). The LRT requires the awareness of $\boldsymbol{Z}$. Considering that Eve will perform the best attack for a given test statistic operated by Alice, Bob does not know neither the exact value nor the statistics of $\boldsymbol{Z}$. Therefore we utilize the General Likelihood Ratio Test (GLRT), where the unknown vector $\boldsymbol{Z}$ is replaced by it's maximum likelihood (ML) estimate, which is $\hat{\boldsymbol{Q}}$ from (4.14). Specifically , let $f_{\hat{\boldsymbol{Q}}|H_0}(\boldsymbol{a})$ be the probability density function (PDF) of $\hat{\boldsymbol{Q}}$ under hypothesis H_0. Then it defined as

$$\Psi = \log \frac{1}{f_{\hat{\boldsymbol{Q}}|H_0}(\hat{\boldsymbol{Q}})} . \tag{4.15}$$

The LRT compare the LLR with a threshold $\theta > 0$, i.e.,

$$\begin{cases} \Psi \leq \theta : & \text{decide for } H_0 \\ \Psi > \theta : & \text{decide for } H_1 \end{cases} . \tag{4.16}$$

To be able to obtain a closed form expression of Ψ, we note from (4.13) that under hypothesis H_0, $\hat{\boldsymbol{Q}}$ is Gaussian distributed around $\hat{\boldsymbol{Q}}^{(A,I,B)}$ with per-dimension variance $\sigma^2 = \sigma_{'}^2 + \sigma_{''}^2$. Then we have

$$\Psi \propto \frac{2}{\sigma^2} \sum_{n=0}^{2(K\times M)-1} |\hat{\boldsymbol{Q}}_n - \hat{\boldsymbol{Q}}_n^{(A,I,B)}|^2, \tag{4.17}$$

where the proportionality stems from ignoring multiplicative constants. Be mindful that the test statistic (4.17) is identical as promoted in [38], [39]. Even so, while in that case only a certain attack was considered by modeling $\boldsymbol{Z}$ in (4.14) as a complex Gaussian vector with i.i.d. entries having zero mean and known variance, now we can see that this test is the GLRT, even when no attacker strategy information is available, Moreover it has a much more reliability.

By substituting (4.13) in (4.17), we obtain that under the hypothesis H_1, Ψ is a central chi-square random

variable with $2(K \times M)$ degrees of freedom and non-centrality parameter

$$\zeta = \frac{2}{\sigma^2} \left|\left| \boldsymbol{Z} - \boldsymbol{Q}^{(A,I,B)} \right|\right|^2 \tag{4.18}$$

Probabilities of False Alarm and Missed Detection

For the GLRT, FA occurs when $\Psi|H_0 > \theta$ while MD occurs when $\Psi|H_1 < \theta$ considering the statistics of Ψ attained in the previous section, for given threshold θ and attack $\boldsymbol{Z}$, the FA probability P_{FA} and MD probability $P_{MD}(\zeta)$ are

$$P_{FA} = P[\Psi > \theta | H_0] = 1 - F_{x^2,0}(\theta), \tag{4.19a}$$

$$P_{MD}(\zeta) = P[\Psi < \theta | H_1] = F_{x^2,\zeta}(\theta), \tag{4.19b}$$

where $F_{x^2,\zeta}(.)$ denotes the cumulative distribution function (CDF) of the chi-square random variable with $2(K \times M)$ degrees of freedom and non-centrality parameter ζ. By forcing a target P_{FA}, the threshold is set from (4.19a) as

$$\theta = F^{-1}_{x^2,0}(1 - P_{FA}), \tag{4.20a}$$

and in this case the MD probability can be written as

$$P_{MD}(\zeta) = F_{x^2,\zeta}\big(F^{-1}_{x^2,0}(1 - P_{FA})\big). \tag{4.20b}$$

If we consider $\boldsymbol{Z}$ and $\hat{\boldsymbol{Q}}^{(A,I,B)}$ as a random variables, then also ζ and the MD probability (4.20b) must be considered random.

4.3 Attack Strategies

In this section, we consider the strategies adopted by Eve to break the authentication system. The generalized attack strategy is that Eve find estimates of the channels a) from Alice to her $\hat{\boldsymbol{Q}}^{(A,I,E)}$ and b) from bob to her $\hat{\boldsymbol{Q}}^{(B,I,E)}$ through the IRS. Then estimates the channel $\boldsymbol{Q}^{(A,I,B)}$ from the estimates $\hat{\boldsymbol{Q}}^{(A,I,E)}$ and $\hat{\boldsymbol{Q}}^{(B,I,E)}$. We define $\boldsymbol{Z}$ as the estimated version of $\boldsymbol{Q}^{(A,I,B)}$.

In the upcoming subsections, our goal is to obtain $\boldsymbol{Z}$ that maximizes the probability of breaking the authentication system. We have two different cases to consider. Firstly we assume that, Eve either knows the IRS configurations or not. Then we assume that, Eve either perform a single attack or multiple attacks.

We now consider that knows the IRS configuration Φ. Eve estimates of the cascaded channel from Alice to her as

$$\hat{\boldsymbol{Q}}^{(A,I,E)} = \boldsymbol{U}\Phi\boldsymbol{G} + \boldsymbol{W}^{AE}, \quad V \times K \tag{4.21a}$$

where $\boldsymbol{W}^{AE}$ has independent Gaussian entries with zero mean and variance $\sigma_{\prime\prime}^2$. Eve estimates of the cascaded channel from Bob to her as

$$\hat{\boldsymbol{Q}}^{(B,I,E)} = \boldsymbol{U}\Phi\boldsymbol{H}^T + \boldsymbol{W}^{BE}, \quad V \times M \tag{4.21b}$$

where $\boldsymbol{W}^{BE}$ has independent Gaussian entries with zero mean and variance $\sigma_{\prime\prime}^2$.

We assume that the sizes of the three cascaded channels reciprocity, that can be obtained with time division duplexing over the same frequency band, and defined the cross correlation matrices for the cascaded channel of each two agents as

$$\boldsymbol{R}^{(A,I,B)} = E[vec(\boldsymbol{Q}^{(A,I,B)})vec(\boldsymbol{Q}^{(A,I,B)})^H], \quad KM \times KM \tag{4.22a}$$

$$\boldsymbol{R}^{(B,I,E)} = E[vec(\boldsymbol{Q}^{(B,I,E)})vec(\boldsymbol{Q}^{(B,I,E)})^H], \quad VM \times VM \tag{4.22b}$$

$$\boldsymbol{R}^{(A,I,E)} = E[vec(\boldsymbol{Q}^{(A,I,E)})vec(\boldsymbol{Q}^{(A,I,E)})^H], \quad KV \times KV \tag{4.22c}$$

and between the cross correlation matrices for two different cascaded channel of each two agents as

$$\boldsymbol{R}^{((A,I,B),(A,I,E))} = E[vec(\boldsymbol{Q}^{(A,I,B)})vec(\boldsymbol{Q}^{(A,I,E)})^H], \quad KM \times KV \tag{4.23a}$$

$$\boldsymbol{R}^{((A,I,E),(B,I,E))} = E[vec(\boldsymbol{Q}^{(A,I,E)})vec(\boldsymbol{Q}^{(B,I,E)})^H], \quad KV \times MV \tag{4.23b}$$

$$\boldsymbol{R}^{((A,I,B),(B,I,E)} = E[vec(\boldsymbol{Q}^{(A,I,B)})vec(\boldsymbol{Q}^{(B,I,E)})^H], \quad KM \times MV \tag{4.23c}$$

where *vec* converts any matrix to a column vector, by indexing the matrix by rows (top to bottom) and element of each row from right to left. Therefor, for an $R \times C$ matrix $\boldsymbol{X}$. We have $(vec(\boldsymbol{X}))_i = (\boldsymbol{X})_{\lfloor \frac{i}{C} \rfloor, i \mod C}$. Moreover, we have

$$[vec(\boldsymbol{A}\Phi\boldsymbol{B}]_i = \sum_{\ell} [\boldsymbol{A}]_{\lfloor \frac{i}{C} \rfloor, \ell} \varphi_\ell [\boldsymbol{C}]_{\ell, i \mod C}. \tag{4.24}$$

We have

$$[\boldsymbol{R}^{(A,I,B)}]_{i,j} = \sum_{l_1} \sum_{l_2} E\left\{ \boldsymbol{H}_{\lfloor \frac{i}{K} \rfloor, l_1} \boldsymbol{H}^*_{\lfloor \frac{j}{K} \rfloor, l_2} \varphi_{l_1} \varphi^*_{l_2} \boldsymbol{G}_{l_1, i \mod K} \boldsymbol{G}^*_{l_2, j \mod K} \right\} \tag{4.25a}$$

$$[\boldsymbol{R}^{(B,I,E)}]_{i,j} = \sum_{l_1} \sum_{l_2} E\left\{ \boldsymbol{U}_{\lfloor \frac{i}{M} \rfloor, l_1} \boldsymbol{U}^*_{\lfloor \frac{j}{M} \rfloor, l_2} \varphi_{l_1} \varphi^*_{l_2} \boldsymbol{H}_{i \mod M, l_1} \boldsymbol{H}^*_{j \mod M, l_2} \right\} \tag{4.25b}$$

$$[\boldsymbol{R}^{(A,I,E)}]_{i,j} = \sum_{l_1} \sum_{l_2} E\left\{ \boldsymbol{U}_{\lfloor \frac{i}{K} \rfloor, l_1} \boldsymbol{U}^*_{\lfloor \frac{j}{K} \rfloor, l_2} \varphi_{l_1} \varphi^*_{l_2} \boldsymbol{G}_{l_1, i \mod K} \boldsymbol{G}^*_{l_2, j \mod K} \right\} \tag{4.25c}$$

$$[\boldsymbol{R}^{((A,I,B),(A,I,E))}]_{i,j} = \sum_{l_1} \sum_{l_2} E\left\{ \boldsymbol{H}_{\lfloor \frac{i}{K} \rfloor, l_1} \boldsymbol{U}^*_{\lfloor \frac{j}{K} \rfloor, l_2} \varphi_{l_1} \varphi^*_{l_2} \boldsymbol{G}_{l_1, i \mod K} \boldsymbol{G}^*_{l_2, j \mod K} \right\} \tag{4.25d}$$

$$[\boldsymbol{R}^{((A,I,E),(B,I,E))}]_{i,j} = \sum_{l_1} \sum_{l_2} E\left\{ \boldsymbol{U}_{\lfloor \frac{i}{K} \rfloor, l_1} \boldsymbol{U}^*_{\lfloor \frac{j}{M} \rfloor, l_2} \varphi_{l_1} \varphi^*_{l_2} \boldsymbol{G}_{l_1, i \mod K} \boldsymbol{H}^*_{j \mod M, l_2} \right\} \tag{4.25e}$$

$$[\boldsymbol{R}^{((A,I,B),(B,I,E))}]_{i,j} = \sum_{l_1}\sum_{l_2} E\left\{\boldsymbol{H}_{\lfloor \frac{i}{K} \rfloor, l_1}\boldsymbol{U}^*_{\lfloor \frac{j}{M} \rfloor, l_2}\varphi_{l_1}\varphi^*_{l_2}\boldsymbol{G}_{l_1,i \mod K}\boldsymbol{H}^*_{j \mod M, l_2}\right\} \tag{4.25f}$$

Let us assume $\boldsymbol{H}$ and $\boldsymbol{G}$ with independent entries (within each matrix and among the two matrices), each entry being Gaussian zero-mean with unitary variance. Moreover, let us assume $K = V$ and

$$\boldsymbol{U} = \rho\boldsymbol{G}^T + \sqrt{1-\rho^2}\boldsymbol{U}' \tag{4.26}$$

where ρ is a coefficient factor entries of $\boldsymbol{U}'$ are independent from those of both $\boldsymbol{G}$ and $\boldsymbol{H}$ and entries of $\boldsymbol{U}'$ are independent Gaussian zero-mean with unitary variance.

From (4.17), we know that Bob will accept a message only if its corresponding channel estimate $\hat{\boldsymbol{Q}}$ lies inside the sphere S (in the $(K \times M)$-dimensional complex space $(C^{K \cdot M})$ centered around $\hat{\boldsymbol{Q}}^{(A,I,B)}$ and having radius $r = \sqrt{\frac{\theta}{2}\sigma^2}$. the maximum probability of a successful attack is achieved by having $\boldsymbol{Z}$ obtaining the highest probability that the channel estimated by Bob lies in the sphere, i.e.,

$$\hat{\boldsymbol{Z}} = \arg\max_{\boldsymbol{a} \in C^{K \cdot M}} P\big[\hat{\boldsymbol{Q}} \in S | \boldsymbol{Z} = \boldsymbol{a}\big]. \tag{4.27}$$

However, since $\hat{\boldsymbol{Q}}^{(A,I,B)}$ is not known to Eve, the maximum probability of the attack success is achieved with ML estimate of $\hat{\boldsymbol{Q}}^{(A,I,B)}$ based on observations $\hat{\boldsymbol{Q}}^{(A,I,E)}$ and $\hat{\boldsymbol{Q}}^{(B,I,E)}$ available to Eve. We will now follow the steps of [37]. For N large and $N >> M, K, V$, by invoking the law of large numbers, we can consider the random vector $\hat{b} = \big[vec(\boldsymbol{Q}^{(A,I,B)})^T, vec(\hat{\boldsymbol{Q}}^{(A,I,E)})^T, vec(\hat{\boldsymbol{Q}}^{(B,I,E)})^T\big]^T$ as zero-mean Gaussian distributed with correlation matrix

$$\boldsymbol{R}^{(I)} = \begin{bmatrix} \boldsymbol{R}^{(A,I,B)} + \sigma_I^2\boldsymbol{I}_{KM\times KM} & \boldsymbol{R}^{((A,I,B),(A,I,E))} & \boldsymbol{R}^{((A,I,B),(B,I,E))} \\ \boldsymbol{R}^{((A,I,B),(A,I,E))^H} & \boldsymbol{R}^{(A,I,E)} + \sigma_{II}^2\boldsymbol{I}_{VM\times VM} & \boldsymbol{R}^{((A,I,E),(B,I,E))} \\ \boldsymbol{R}^{((A,I,B),(B,I,E))^H} & \boldsymbol{R}^{((A,I,E,(B,I,E))^H} & \boldsymbol{R}^{(B,I,E)} + \sigma_{II}^2\boldsymbol{I}_{VK\times VK} \end{bmatrix}. \tag{4.28}$$

From (4.25) we have

$$\boldsymbol{R}^{(A,I,B)} = \left[\sum_l |\varphi_l|^2\right]\boldsymbol{I} \tag{4.29a}$$

$$\boldsymbol{R}^{(B,I,E)} = \left[\sum_l |\varphi_l|^2\right]\boldsymbol{I} \tag{4.29b}$$

$$\begin{aligned}[\boldsymbol{R}^{(A,I,E)}]_{i,j} &= \sum_{l_1}\sum_{l_2}\varphi_{l_1}\varphi^*_{l_2}|\rho|^2 E\{\boldsymbol{G}_{l_1,\lfloor \frac{i}{K} \rfloor}\boldsymbol{G}^*_{l_2,\lfloor \frac{j}{K} \rfloor}\boldsymbol{G}_{l_1,i \mod K}\boldsymbol{G}^*_{l_2,j \mod K}\} \\ &= \begin{cases} \sum_l |\varphi_l|^2\rho^2, & \text{if } i = k_1K + k_2, j = k_2K + k_1 \\ \sum_l |\varphi_l|^2 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}\end{aligned} \tag{4.29c}$$

$$[\boldsymbol{R}^{((A,I,B),(A,I,E))}]_{i,j} = 0 \tag{4.29d}$$

$$[\boldsymbol{R}^{((A,I,E),(B,I,E))}]_{i,j} = 0 \tag{4.29e}$$

$$\begin{aligned}
[\boldsymbol{R}^{((A,I,B),(B,I,E)}]_{i,j} &= \sum_l |\varphi_l|^2 \rho^* E\left\{\boldsymbol{H}_{\lfloor \frac{i}{K} \rfloor,l} \boldsymbol{U}^*_{\lfloor \frac{j}{M} \rfloor,l} \boldsymbol{G}_{l,i \mod K} \boldsymbol{H}^*_{j \mod M,l}\right\} \\
&= \sum_l |\varphi_l|^2 \rho^* E\left\{\boldsymbol{H}_{\lfloor \frac{i}{K} \rfloor,l} \boldsymbol{G}^*_{l,\lfloor \frac{j}{M} \rfloor} \boldsymbol{G}_{l,i \mod K} \boldsymbol{H}^*_{j \mod M,l}\right\} \\
&= \begin{cases} \sum_l |\varphi_l|^2 \rho^* & \text{if } i = k_1 K + k_2, j = k_2 M + k_1 \\ 0 & \text{otherwise} \end{cases}
\end{aligned} \tag{4.29f}$$

By defining $\hat{\boldsymbol{A}}(\boldsymbol{a}) = \left[\boldsymbol{a}^T, vec(\hat{\boldsymbol{Q}}^{(A,I,E)^T}), vec(\hat{\boldsymbol{Q}}^{(B,I,E)^T})\right]^T$, the ML estimate of $\boldsymbol{Q}^{(A,I,B)}$, given $\hat{\boldsymbol{Q}}^{(A,I,E)}$ and $\hat{\boldsymbol{Q}}^{(B,I,E)}$ is

$$\begin{aligned}
\hat{\boldsymbol{Z}} &= \arg \max_{\boldsymbol{a} \in C^{K \cdot M}} P[\hat{\boldsymbol{A}}(\boldsymbol{a}) | \hat{\boldsymbol{Q}}^{(A,I,E)}, \hat{\boldsymbol{Q}}^{(B,I,E)}] \\
&= \arg \min_{\boldsymbol{a} \in C^{K \cdot M}} \hat{\boldsymbol{A}}^*(\boldsymbol{a}) \boldsymbol{R}^{(I)^{-1}} \hat{\boldsymbol{A}}(\boldsymbol{a}).
\end{aligned} \tag{4.30}$$

Note that for the considered channel model, the ML estimator in (4.30) becomes the linear minimum mean square error (MMSE) estimator [40], which is optimal for the test statistic employed by Bob (4.17). For the sake of clarity, we partition $\boldsymbol{S} = \boldsymbol{R}^{(I)^{-1}}$ into blocks with sizes as in (4.28), i.e.,

$$\boldsymbol{S} = \begin{bmatrix} \boldsymbol{S}_{11} & \boldsymbol{S}_{12} & \boldsymbol{S}_{13} \\ \boldsymbol{S}_{12}^H & \boldsymbol{S}_{22} & \boldsymbol{S}_{23} \\ \boldsymbol{S}_{13}^H & \boldsymbol{S}_{23}^H & \boldsymbol{S}_{33} \end{bmatrix}. \tag{4.31}$$

By setting to zero the gradient of $\hat{\boldsymbol{A}}^*(\boldsymbol{a}) \boldsymbol{S} \hat{\boldsymbol{A}}(\boldsymbol{a})$ with respect to $\boldsymbol{a}$ we obtain

$$\hat{\boldsymbol{Z}} = -\boldsymbol{S}_{11}^{-1}\left(\boldsymbol{S}_{12} \hat{\boldsymbol{Q}}^{(A,I,E)} + \boldsymbol{S}_{13} \hat{\boldsymbol{Q}}^{(E,I,B)}\right). \tag{4.32}$$

Now, from (4.29) we observe that if $|\varphi_l| = 1$ for all configurations and all l, matrix $\boldsymbol{R}^{(I)}$ does not depend on the IRS configuration, and also $\boldsymbol{S}$ will not depend on the IRS configuration. Still, $\boldsymbol{Z}$ depends on the configuration through $\hat{\boldsymbol{Q}}^{(A,I,E)}$ and $\hat{\boldsymbol{Q}}^{(E,I,B)}$

First Scenario

We assume that the attacker is able to observe the IRS configuration and estimate the channel between him and Bob, him and Alice. Moreover, the attacker know the current configuration of the IRS. The attacker will be able to perform the procedures that have been described from equation (4.21) to equation (4.32).

Second Scenario

We still assume that attacker will be able to estimate the channel between him and Bob, him and Alice but he will not be able to know the IRS configuration. Considering that the attacker know the structure of the IRS and the number of it's element. The attacker will compute the attack for each configuration and then it will take the average of the attacks as

$$E(\hat{\boldsymbol{Z}}) = -\boldsymbol{S}_{11}^{-1}\left(\boldsymbol{S}_{12}E(\hat{\boldsymbol{Q}}^{(A,I,E)}) + \boldsymbol{S}_{13}E(\hat{\boldsymbol{Q}}^{(E,I,B)})\right) \tag{4.33}$$

and with our assumptions on the channels we have

$$E(\hat{\boldsymbol{Z}}) = \boldsymbol{0} \tag{4.34}$$

5

Simulation results

By numerical results, we have evaluated the performance of the proposed channel-based authentication scheme for the IRS-assisted MIMO network. The results are divided into two segments, the first one includes the investigation results of the proposed channel estimation scheme accuracy for the cascaded channel from Alice (UE) to Bob (gNB) through the IRS. In the second segment, the proposed scheme has been evaluated against different attack strategies. Monte Carlo simulations have been conducted to endorse the correctness of the analytical results.

5.1 Channel estimation

In fig. 5.1, the proposed scheme (4.10) for cascaded channel estimation has been analyzed using a systematic channel estimation scheme (4.6) as a reference. It was noted that with low SNR values, the proposed scheme channel estimation performance is more accurate. Also, we note that the MSE values of the proposed scheme remained constant against all values of the SNR. Thus, we proved the fact that the proposed scheme is a partially blinded predictable scheme that is not affected by the current level of noise or distortion of the channel. As the SNR values exceeded zero, the accuracy of the systematic scheme results improved monotonically. Although the systematic scheme results with high SNR are more accurate than the proposed scheme, the proposed scheme results are still in the acceptable range. Considering that, in a high-frequency environment, a low SNR often happened, and considering the trade-off between high accuracy and low complexity as well. Thus will lead to the superiority of the proposed scheme.

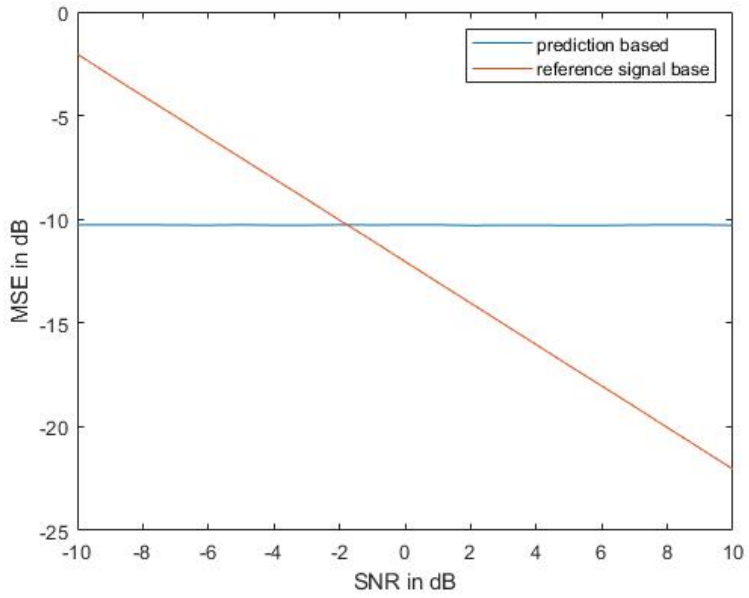

Figure 5.1: Accuracy Comparison between between the proposed scheme (prediction based) and the systematic scheme (reference signal based)

5.2 Attacks evaluation

During the evaluation, we assumed different values for the correlation factor which represent the correlation between the channel between the attacker (Eve) and the IRS and the channel between the legitimate transmitter (Alice) and the IRS (4.26).

In the first scenario, although the channel between the attacker (Eve) and the IRS was mostly identical to the channel between Alice and the IRS, the proposed scheme could achieve a low probability of MD as shown in fig. 5.2. Moreover, a low probability MD has been noted with lower values of the correlation factor. The proposed scheme showed a significantly low probability of both MD and FA even if the attacker has known the configuration of the IRS under the condition of positioning the attacker's antenna in a different position, managed by the correlation factor, than the transmitter's antenna. In the second scenario when the attacker does not know the configuration of the IRS, the proposed scheme achieved the best security performance which was constantly fixed within all values of the correlation factor. To conclude, the proposed scheme is robust against attacks even if the attacker is placed in the same place of the transmitter unless the attackers do not know the configuration of the IRS.

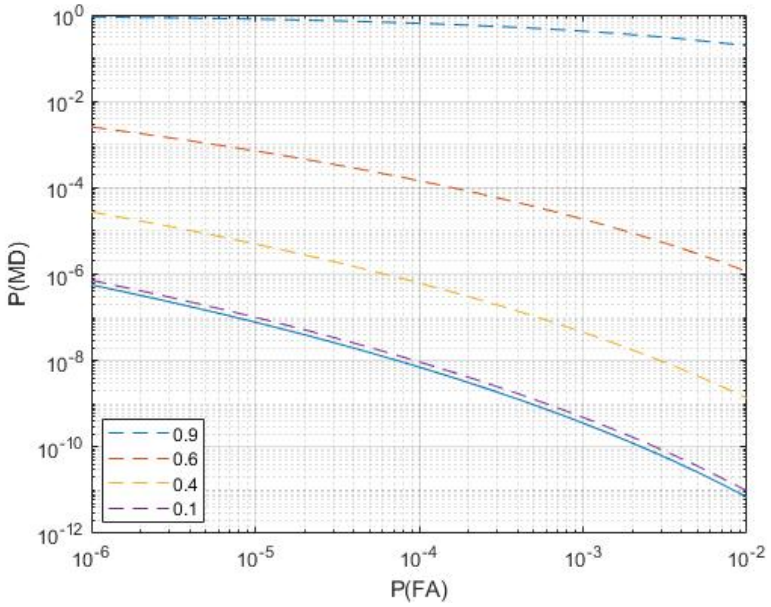

Figure 5.2: Comparison between different scenarios of attacks against the proposed scheme. Here ρ (correlation factor) $= 0.9, 0.6, 0.4$ and 0.1 respectfully

6 Conclusion

In this thesis, we have developed a Channel-based Physical layer security scheme to provide communication authentication between Alice and Bob through the IRS with the precision channel estimation and assuming a general model for the attack employed by Eve. In particular, we provided the optimal Eve strategies in the case of a single attack, and we performed an analytical computation of the MD probability averaged over channel statistics. Numerical results confirm the merit of the considered method as it performs well against the attack strategy when Eve does not know the IRS configuration for the channel between Alice and Bob.

All proposed authentication schemes are based on either upper layer cryptography mechanisms such as AKA protocol or physical layer mechanisms such as the proposed scheme. Moreover, it is not possible to depend completely on only one of the two mechanisms. Integration of these two primitives is desirable to enhance security in highly dynamic networks such as those planned in beyond-5G wireless networks. There are few papers on the cross-layer protocol. For future work, we aim to develop a cross-layer authentication scheme integrating upper layer authentication with physical layer authentication considering the advantages of IRS presence in the physical layer part of the cross-layer protocol.

References

[1] N. Laurenti, "Introduction to information security," 2021.

[2] E. Southern, A. Ouda, and A. Shami, "Securing usim-based mobile communications from interoperation of sim-based communications," *International Journal for Information Security Research (IJISR)*, vol. 2, 2012.

[3] S. Behrad, E. Bertin, and N. Crespi, "Securing authentication for mobile networks, a survey on 4g issues and 5g answers," in *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, 2018, pp. 1–8.

[4] W. Fang, F. Li, Y. Sun, L. Shan, S. Chen, and M. L. C. Chen, "Information security of phy layer in wireless networks," *Journal of Sensors*, 2016.

[5] L. Pu, J. Liu, Y. Fang, W. Li, and Z. Wang, "Channel estimation in mobile wireless communication," vol. 2, 2010, pp. 77–80.

[6] T. Hou, Y. Liu, Z. Song, X. Sun, Y. Chen, and L. Hanzo, "Mimo assisted networks relying on intelligent reflective surfaces: A stochastic geometry based analysis," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 1, pp. 571–582, 2022.

[7] D. Perez-Adan, O. Fresnedo, J. P. Gonzalez-Coma, and L. Castedo, "Intelligent reflective surface for wireless networks: An overview of applications, approached issues, and open problems," *MDPI, Basel, Switzerland*, 2021.

[8] D. P. Moya Osorio, I. Ahmad, J. D. V. Sánchez, A. Gurtov, J. Scholliers, M. Kutila, and P. Porambage, "Towards 6g-enabled internet of vehicles: Security and privacy," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 82–105, 2022.

[9] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[10] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, "5g security challenges and solutions: A review by osi layers," *IEEE Access*, vol. 9, pp. 116 294–116 314, 2021.

[11] M. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101, no. 1, 2018.

[12] X. Qiu, X. Sun, and M. Hayes, "Enhanced security authentication based on convolutional-lstm networks," *Sensors*, vol. 21, no. 16, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/16/5379

[13] F. Zheng, Z. Xiao, S. Zhou, J. Wang, and L. Huang, "Identity authentication over noisy channels," *Entropy*, vol. 17, no. 7, pp. 4940–4958, 2015. [Online]. Available: https://www.mdpi.com/1099-4300/17/7/4940

[14] U. M. Maurer, "Conditionally-perfect secrecy and a provably-secure randomized cipher," *Journal of Cryptology*, vol. 5, p. 53–66, 1992.

[15] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[16] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[17] J. Liu, Y. Fang, W. Li, and Z. Wang, "Channel estimation in mobile wireless communication," *International Conference on Communications and Mobile Computing*, 2010.

[18] H. Arslan and G. E. Bottomley, "Channel estimation in narrowband wireless communication systems," *WIRELESS COMMUNICATIONS AND MOBILE COMPUTING*, vol. 1, p. 201–219, 2001.

[19] Y. Xiong, M. Wei, Y. Gong, and Y. Gong, "A novel blind channel estimation method for mimo system," 2007, pp. 1–5.

[20] K. Zeng, K. Govindan, , and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, 2010.

[21] C. Pei, N. Zhang, X. Shen, and J. Mark, "Channel-based physical layer authentication," *Wireless Communications Symposium*, 2014.

[22] P.Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over mimo fading wiretap channels," *IEEE Transactions on Wireless Communications*, vol. 11, no. 7, 2012.

[23] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6g networks: Use cases and technologies," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 55–61, 2020.

[24] 3GPP and T. 38.912, "5g; study on new radio (nr) access technology," *3 GPP*, 2017.

[25] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, 2020.

[26] E. Basar and H. V. Poor, "Present and future of reconfigurable intelligent surface-empowered communications," *IEEE SIGNAL PROCESSING MAGAZINE*, 2021.

[27] E. Ibrahim, R. Nilsson, and J. van de Beek, "Intelligent reflecting surfaces for mimo communications in los environments," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, 2021, pp. 1–6.

[28] S. Zhang and R. Zhang, "On the capacity of intelligent reflecting surface aided mimo communication," in *2020 IEEE International Symposium on Information Theory (ISIT)*, 2020, pp. 2977–2982.

[29] . Özdogan, E. Björnson, and E. G. Larsson, "Using intelligent reflecting surfaces for rank improvement in mimo communications," in *ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2020, pp. 9160–9164.

[30] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.

[31] X. Lu, E. Hossain, T. Shafique, S. Feng, H. Jiang, and D. Niyato, "Intelligent reflecting surface enabled covert communications in wireless networks," *IEEE Network*, vol. 34, no. 5, pp. 148–155, 2020.

[32] S. Yan, X. Zhou, D. W. K. Ng, J. Yuan, and N. Al-Dhahir, "Intelligent reflecting surface for wireless communication security and privacy," *CoRR*, vol. abs/2103.16696, 2021. [Online]. Available: https://arxiv.org/abs/2103.16696

[33] A. Bereyhi, S. Asaad, R. R. Müller, R. F. Schaefer, and H. V. Poor, "Secure transmission in irs-assisted mimo systems with active eavesdroppers," in *2020 54th Asilomar Conference on Signals, Systems, and Computers*, 2020, pp. 718–725.

[34] Y. Sun, K. An, J. Luo, Y. Zhu, G. Zheng, and S. Chatzinotas, "Intelligent reflecting surface enhanced secure transmission against both jamming and eavesdropping attacks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 10, pp. 11 017–11 022, 2021.

[35] Z. Wang, L. Liu, and S. Cui, "Channel estimation for intelligent reflecting surface assisted multiuser communications: Framework, algorithms, and analysis," *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, pp. 6607–6620, 2020.

[36] Z.-Q. He and X. Yuan, "Cascaded channel estimation for large intelligent metasurface assisted massive mimo," *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 210–214, 2020.

[37] A. Rech, F. Moretto, and S. Tomasin, "Maximum-rate optimization of hybrid intelligent reflective surface and relay systems," *IEEE 22nd International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2021.

[38] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," *IEEE Conf. on Sensor, Mesh and Ad Hoc Commun. and Networks*, 2007.

[39] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Finger prints in the ether: using the physical layer for wireless authentication," *IEEE Int. Conf. on Communications*, 2007.

[40] S. Kay, "Fundamentals of statistical signal processing: Estimation theory," *Prentice Hall*, 1993.

Acknowledgments

First of all, I would like to express my sincere gratitude to Regional Scholarships, the Veneto Region's scholarship program, funded by the regional company for the Right to University Education (ESU) and partner organizations, for letting me be part of this incredible leaders' network. Further, I would like to express my deep gratitude to my supervisor Professor Stefano Tomasin for his dedicated support and guidance. Professor Stefano continuously provided encouragement and was always willing and enthusiastic to assist in any way he could throughout the research project. I am also thankful to the School of Information Engineering and all its member's staff for all the considerate guidance. To conclude, I cannot forget to thank my family and friends for all the unconditional support in this very intense academic year.