

AMERICAN UNIVERSITY OF BEIRUT

PHYSICAL LAYER SECURITY FOR
COMBATING JAMMERS AND
EAVESDROPPERS

by
MAHDI CHEHIMI

A thesis
submitted in partial fulfillment of the requirements
for the degree of Master of Engineering
to the Department of Electrical and Computer Engineering
of the Faculty of Engineering and Architecture
at the American University of Beirut

Beirut, Lebanon
May 2020

AMERICAN UNIVERSITY OF BEIRUT

PHYSICAL LAYER SECURITY FOR
COMBATING JAMMERS AND
EAVESDROPPERS

by
MAHDI CHEHIMI

Approved by:



Dr. Ali Chehab, Professor
Electrical and Computer Engineering

Advisor



Dr. Karim Kabalan, Professor
Electrical and Computer Engineering

Member of Committee



Dr. Rouwaida Kanj, Associate Professor
Electrical and Computer Engineering

Member of Committee

Date of thesis defense: May 12, 2020

AMERICAN UNIVERSITY OF BEIRUT

THESIS, DISSERTATION, PROJECT RELEASE FORM

Student Name: Chehimi Mahdi Mohammad
Last First Middle


Master's Thesis Master's Project Doctoral Dissertation

I authorize the American University of Beirut to: (a) reproduce hard or electronic copies of my thesis, dissertation, or project; (b) include such copies in the archives and digital repositories of the University; and (c) make freely available such copies to third parties for research or educational purposes.

I authorize the American University of Beirut, to: (a) reproduce hard or electronic copies of it; (b) include such copies in the archives and digital repositories of the University; and (c) make freely available such copies to third parties for research or educational purposes after: One ___ year from the date of submission of my thesis, dissertation or project.

Two ___ years from the date of submission of my thesis, dissertation or project.

Three ___ years from the date of submission of my thesis, dissertation or project.


Signature

18/5/2020
Date

This form is signed when submitting the thesis, dissertation, or project to the University Libraries

Acknowledgements

First of all, I thank God for his mercy and guidance all the way in my life. I am thankful for having this great opportunity to do my Master's study at AUB. I would like to thank my family, friends, colleagues, and my loved ones for always being there and for their endless support which have always been motivating me to do my best and achieve my goals in life. Special thanks for my father who have always been a great influencer in my life, and to my mother who is the real blessing in my life.

I would like to thank my advisor Prof. Ali Chehab for his guidance, support, understanding, and kindness, all of which enhanced my graduate experience. Also, many thanks to my committee members Prof. Kareem Kabalan and Prof. Rouwaida Kanj for their support all over this journey.

Also, special thanks to Dr. Elias Yaacoub for his guidance and support since the beginning of my Master's study. I would love to thank him for motivating me and believing in my capabilities.

A big thank you to Dr. Mohammed Al-Husseini who provided me with support, guidance, and knowledge during the second year of my Master's study.

Finally, the computations for this thesis have been performed with the support of AUB's IT Research Computing team and powered by AUB's HPC. In addition to the IT team at Beirut Research and Innovation Center (BRIC). Special thanks to both teams, especially Dr. Mher Kazandjian for his dedication, and support, and for the great efforts he spent helping in optimizing the codes.

An Abstract of the Thesis of

Mahdi Chehimi for Master of Engineering
Major: Electrical and Computer Engineering

Title: Physical Layer Security for Combating Jammers and Eavesdroppers

Wirelessly connected devices play a vital role in people's daily life, especially with the rapid increase in the number of devices connected to the internet and the huge data being generated everyday. However, the open nature of the wireless channels makes them vulnerable to several threats. Two major threats are: eavesdropping attacks in which an adversary side tries to capture the transmitted data between two communicating parties, and jamming attacks in which an adversary side tries to disrupt the reception of useful signals by a legitimate receiver. The concept of physical layer security is gaining more and more attention from the research community nowadays. It makes use of the open nature and randomness of the wireless channel to achieve security in the communications system. In this thesis, the problem of combating passive eavesdroppers and jammers is studied. Multiple different scenarios are considered and security solutions based on the physical layer are proposed. The proposed solutions are based on the usage of massive planar antenna arrays. First, a solution for combating a single passive eavesdropper at a known location is proposed. It is based on dedicating some antenna sub-arrays for the communication link between the legitimate parties, while simultaneously sending jamming signals towards the eavesdropper. Next, a look-up table-based physical layer solution is proposed to perform anti-jamming against a single jammer at a known location. The solution is based on performing beamforming by maximizing the receiver's gain towards the transmitter, and simultaneously placing a null in the direction of the jammer, thus, achieving a high signal-to-interference-plus-noise-ratio (SINR). Finally, the proposed anti-jamming technique is extended, and machine learning (ML) and deep learning (DL) algorithms are deployed in order to build a robust, and cognitive anti-jamming system. The dataset on which the models were trained and tested was generated, and efficient anti-jamming performance was achieved. The proposed models are scalable and can be extended to scenarios with multiple jammers. In-

sights for an effective method for detecting the location of the jammer are drawn from the proposed ML/DL models and left for future investigation.

Contents

Acknowledgements	v
Abstract	vi
Abbreviations	xiii
1 Introduction	1
2 Literature Review	4
2.1 Combating Passive Eavesdroppers	4
2.2 Anti-Jamming Techniques at The Physical Layer	7
2.3 Massive MIMO Technology and Physical Layer Security	10
2.4 Cryptographic Security Techniques at The Physical Layer	11
2.5 Machine Learning and Deep Learning in Wireless Communications and Physical Layer Security	13
2.6 Thesis Contributions	16
3 Planar Antennas & Wireless Channel Overview	18
3.1 Planar Antenna Arrays	18
3.1.1 Array Factor	19
3.1.2 Beamforming	20
3.1.3 Directivity	21
3.2 Linear Antenna Arrays	21
3.2.1 Uniform Amplitude Linear Arrays	21
3.2.2 Non-uniform Amplitude Binomial Linear Arrays	21
3.2.3 Non-uniform Amplitude Dolph-Chebyshev Linear Arrays	22
3.3 Wireless Channel Model	22
3.3.1 Uncorrelated Rayleigh Fading	23
4 Proposed Solutions for Combating Passive Eavesdroppers	24
4.1 Single Passive Eavesdropper at a Known Location	24
4.1.1 System Model	24
4.1.2 Capacity Calculations and System Parameters	27
4.1.3 Simulation Results	29

5	Proposed Anti-jamming Techniques at The Physical Layer	33
5.1	Look-up Table Based Anti-jamming Technique	33
5.1.1	System Model	34
5.1.2	Generating The Database of Antenna Array Configurations	34
5.1.3	Performance Metrics	35
5.1.4	Searching Methods	36
5.1.5	Simulation Results	37
5.2	Machine Learning Based Anti-jamming Technique	41
5.2.1	Motivation	41
5.2.2	System Model	42
5.2.3	Dataset Generation	43
5.2.4	Deployed Machine Learning Algorithms	44
5.2.5	Data Pre-processing and Experimental Setup	47
5.2.6	Experimental Results and Discussion	47
6	Conclusion and Future Work	52
	References	55

List of Figures

3.1	Planar antenna array in the x-y plane.	18
4.1	System Model with planar antenna array at Alice only “Source Only case”.	25
4.2	System model with planar antenna array at Alice and Bob with “Common Configuration case”.	25
4.3	System model with planar antenna arrays at Alice and Bob using the “Complementary Configuration case”.	26
4.4	System model when Eve is equipped with a directive antenna steered toward Alice.	26
4.5	Capacity between Source (Alice) and Destination (Bob).	29
4.6	Capacity between Source (Alice) and Eavesdropper (Eve).	30
4.7	Secrecy Capacity between Alice and Bob.	31
5.1	Proposed system model.	34
5.2	Average SINR in dB using both searching methods vs jammer’s location in azimuth plane ϕ_{JR} , compared to omni-directional antenna receiver, transmitter at $(\theta_{TR}, \phi_{TR})=(90,45)$	38
5.3	Average SINR in dB using both searching methods vs jammer’s distance from receiver, transmitter at $(\theta_{TR}, \phi_{TR})=(90,45)$ degree, jammer at $(\theta_{JR}, \phi_{JR})=(90,65)$ degree	39
5.4	Average SINR in dB using both searching methods vs jammer’s elevation angle θ_{JR} , transmitter at $(\theta_{TR}, \phi_{TR})=(45,45)$ degree, $\phi_{JR} = 45$ & 145 degree	39
5.5	Average SINR in dB using Max-to-Null Ratio searching method vs jammer’s location in azimuth plane ϕ_{JR} , varying transmitter’s location	40
5.6	Studied scenario with single jammer.	42
5.7	System model showing inputs and outputs.	43
5.8	MSE score of training and testing data of decision trees vs maximum tree depth.	48
5.9	MSE score on testing data for every output using random forest regressor	49
5.10	ANN adopted architecture	50

5.11 MSE using ADAM optimizer vs number of training epochs.	51
5.12 MSE using SGD optimizer vs number of training epochs.	51

List of Tables

4.1	Definitions of Model Parameters for Combating Eavesdroppers . .	27
5.1	Definitions of Anti-jamming Model Parameters	35

Abbreviations

PLS	Physical Layer Security
MIMO	Multiple Input Multiple Output
IoT	Internet of Things
IoE	Internet of Everything
AI	Artificial Intelligence
ML	Machine Learning
DL	Deep Learning
AN	Artificial Noise
SNR	Signal to Noise Ratio
SINR	Signal to Interference plus Noise Ratio
CSI	Channel State Information
GPS	Global Positioning System
GNSS	Global Navigation Satellite System
PCA	Pilot Contamination Attacks
ISI	Inter-Symbol Interference
SDoF	Secure Degrees of Freedom
FD	Full-duplex
HD	Half-duplex
DoS	Denial of Service
RFI	Radio Frequency Interference
BS	Base Station
MMSE	Minimum Mean Square Error
CR	Cognitive Radio
UE	User Equipment
ZF	Zero Forcing
MRT	Maximum Ratio Transmission
USK	Unshared Secret Key
QoS	Quality of Service
NN	Neural Networks
AoA	Angle of Arrival
TAS	Transmit Antenna Selection
DQN	Deep Q Network
RF	Radio Frequency

DNN	Deep Neural Network
DBN	Deep Belief Network
SVM	Support Vector Machine
UAV	Unmanned Aerial Vehicles
ANN	Artificial Neural Networks
mmWave	millimeter wave
SDR	Software Defined Radio
CNN	Convolutional Neural Network
IoV	Internet of vehicles
SGD	Stochastic Gradient Descent

Chapter 1

Introduction

Wirelessly connected devices became an indispensable part of people's daily life. New Technologies are nowadays playing a vital role in our work environments, sport activities, health systems, transportation networks and vehicles, navigation systems, and even in the education systems [1]. The number of physical devices connected to the Internet is rapidly increasing forming what is known as the Internet-of-Things (IoT) which will converge to the Internet of Everything (IoE) [2]. The IoT is creating a huge network of trillions of "Things" or devices that are communicating with each other [3]. It includes both human-to-machine and machine-to machine (M2M) communications. M2M is a very promising trend that is expected to transform various vertical sectors such as smart cities, smart homes, and car networking because of its advantages which include low-cost, low power consumption and narrow bandwidth [4]. Another technology that is gaining more and more interest is Device-to-Device (D2D) communications which is a key technology in 5G cellular communication networks. In D2D communications, two communication devices close to each other communicate directly through spectrum sharing, without relying on a base station [5]. In addition to the rapid development of smart self-driving cars and the usage of Unmanned-Aerial-Vehicles and drones in delivering goods and in extending the coverage of wireless networks. These technologies, among others such as large intelligent surfaces and edge Artificial Intelligence (AI), are expected to play a vital role in the next generation of wireless communication networks (6G) [2].

According to [6], the number of IoT devices is expected to reach 20.8 billion by 2020, and the number of M2M devices is expected to reach 50 billion by the next decade. Thus, the market of IoT devices is expected to keep expanding in the foreseen future. According to McKinsey's report on disruptive technologies and advances that will transform life, business, and the global economy [7], the estimated potential economic impact of IoT in 2025 will range between 2.7\$ and 6.2\$ trillion.

With the massive amounts of data that is generated on a daily basis, deploying artificial intelligence (AI) and big data handling algorithms become a

necessity [8]. In fact, machine learning (ML) and deep learning (DL) algorithms are attracting the attention of researchers in the wireless communications and networking communities [2], since they have a huge potential in the future wireless networks. Further details on this issue will be given in section 2.5.

This increasing reliance on wirelessly connected devices comes along with many security threats more than the traditional wired systems. The open nature of the wireless channels makes them vulnerable to malicious threats and attacks. In this thesis, we consider two types of attacks. First, eavesdropping, where the adversary side tries to capture the legitimate transmitted information [9]. The second one is jamming attacks where the adversary side tries to disrupt the reception of the legitimate transmitted signals [10] by sending jamming signals towards the receiver. It is apparently a great challenge to keep the wireless communication link safe and reliable.

In general, wireless communication networks adopt the OSI reference model for their architecture [11]. This model divides the network into seven layers. Vulnerabilities and threats attack all the layers of the protocol. In general, security solutions are proposed separately for each of these layers to meet its requirements of security and confidentiality [10].

Traditionally, cryptographic algorithms and cipher schemes are the most employed techniques to achieve security and confidentiality in wireless communication links [12, 13]. These techniques are generally applied at the upper layers of the protocol stack [14]. The performance of cryptographic encryption/decryption security methods is efficient and, in many cases, they provide security to wireless links. However, these methods suffer from serious vulnerabilities such as heavy computation and key management costs. Thus, the system may suffer from high complexity and resource consumption [15].

Recently, new techniques for securing wireless communication links were proposed. An interesting new method, that is gaining more attention from the research community, makes use of the open nature and the randomness of the wireless channels to achieve information theoretic-based security. The method is known as Physical Layer Security (PLS) [10]. PLS aims to clarify the fundamental ability of the physical layer to support secure wireless communications [13, 16]. The advantages of working on the physical layer are the small effect it has on the system and the fact that it only needs one round of operation working on its signals. Thus, it is the fastest layer among the others [17]. Also, because of the features of the physical layer, PLS techniques are able to accommodate any changes in the wireless channel by flexibly adjusting the transmission strategies and parameters [14].

Developed from the early work of Wyner [18, 19], PLS is useful for improving the performance of a huge variety of applications including but not limited to 5G networks, IoT applications, Device-to-Device communication, and military applications [20]. Regarding 5G networks, employing PLS is advantageous over cryptographic techniques at upper layers. This is because unlike cryptographic

techniques which are computation-based, PLS techniques do not depend on computational complexity. Thus, if the adversary side (e.g. eavesdropper) is equipped with powerful computational tools, the PLS solution can keep the communication link reliable, while the security provided by cryptographic solutions becomes questionable [21]. For IoT applications, appealing PLS solutions are the robust methods supplementing lightweight cryptographic protocols [22, 23]. In general, these methods try to improve the legitimate signal reception while degrading the ability of illegitimate users to receive useful information. This is done by making use of the differences between legitimate and illegitimate channel conditions [24]. Moreover, PLS is being an effective candidate for securing D2D communication as shown in [25, 26].

In general, PLS techniques include both cryptographic and non-cryptographic solutions. Non-cryptographic solutions include applying beamforming algorithms, and Artificial Noise (AN)-aided techniques using antenna arrays, especially large arrays like Massive MIMO [27, 28]. On the other hand, cryptographic solutions include data integrity, source authentication, and key generation techniques among others [20, 29, 30, 31].

In this thesis, several PLS solutions for combating eavesdroppers and jammers are proposed. Different scenarios are considered and solutions to secure the legitimate communication link in each of them are proposed. Finally, ML and DL algorithms are deployed in an anti-jamming system in order to secure the system in an intelligent way.

The outline of this thesis is as follows: Chapter 2 presents a review of other works done in the literature regarding the technologies and systems studied in this thesis. In Chapter 3, an overview of planar antenna arrays and the wireless channel model adopted in this thesis is given. Chapter 4 summarizes the proposed solution for combating passive eavesdroppers. In Chapter 5, the proposed anti-jamming techniques based on the physical layer are described. The conclusion and future works are described in Chapter 6. Finally, the references are given.

Chapter 2

Literature Review

The objective of this literature survey is to give a general overview about some important concepts related to this thesis work and to discuss the existing works in the literature. We start by giving an overview about the existing PLS techniques for combating passive eavesdroppers. Then, we present some of the anti-jamming techniques at the physical layer. Next, massive MIMO technology and its role in PLS is discussed. After that, we briefly discuss some cryptographic security techniques at the physical layer. Finally, we discuss the role of machine learning and deep learning in the future of wireless communications and focus on their applications in PLS.

2.1 Combating Passive Eavesdroppers

Eavesdropping has always been an important problem that grabbed the attention of the research community. It plays a vital role in battlefields since every side tries to capture as much information as possible from its adversary. Thus, several countermeasures for eavesdropping are proposed in the literature. As we mentioned in the introduction, two types of eavesdropping attacks exist in reality. Passive and active attacks. Passive attacks are more suitable for someone who is hiding and does not want to expose his location to his enemy. Thus, he stays passive trying to capture some of the transmitted data without sending any signal. He needs to be located close to the receiver or in the direction of a side-lobe of the transmitter so that he gets some information. This type of eavesdropping attacks keeps the eavesdropper safe, but can be combated using different techniques. Among the important physical layer techniques proposed to enhance the security of wireless networks is the use of multiple antenna technology since it is powerful in terms of beamforming and achieving diversity gain [32]. The literature is rich with works on PLS for combating passive eavesdroppers using MIMO and massive MIMO technologies. In fact, massive MIMO technology is believed to be resilient against passive eavesdropping. This is considered true assuming

that the eavesdropper's channel and the uplink channel estimation of the receiver are independent. Thus, the eavesdropper is motivated to launch active attacks on the channel estimation process in order to affect the transmitter's beamforming design [9]. These active attacks are referred to as Pilot Contamination Attacks (PCA). In this thesis, we will only focus on combating passive eavesdropping attacks.

Among the famous techniques to achieve secret communications in the presence of passive eavesdroppers is employing friendly jammer nodes which interfere with the eavesdroppers and confuse them [33]. The achievable secrecy rates in multi-antenna wiretap channels depend on the rate of information received by the eavesdroppers. Relays and jamming nodes are added to the wireless networks to improve the system's performance, achieve secrecy in data transmission, and minimize the amount of information the eavesdropper is able to obtain [34, 35]. The authors in [36] study the power minimization and secrecy rate maximization optimization problems for a MIMO system, where a multi-antenna eavesdropper is present in the system. Secret communication is improved by employing a multi-antenna cooperative jammer. The authors deploy game-theoretic techniques to improve the secrecy of the system.

An essential point in designing the PLS techniques for combating eavesdroppers is the assumption taken regarding the knowledge of the channel state information (CSI) at the transmitter and the receiver. Many works take the simplified assumption of perfect CSI of both the receiver and the eavesdropper at the transmitter. In fact, the assumption that the transmitter has perfect CSI of the receiver is somehow realistic, since it can be known by sending and receiving pilots. However, the assumption of perfect CSI of the passive eavesdropper is not very practical since it is very difficult for the transmitter to detect the presence of a passive eavesdropper or to identify its location. However, in some special cases, the assumption of knowing the location of the eavesdropper can be realistic. For example, in a battlefield, if you know that your enemy has a military point at a specific location, then it is most expected that the enemy will try to eavesdrop from this point and try to capture any information transmitted in its vicinity. In conclusion, the less information about CSI is assumed, the more practical the proposed PLS solution is. An example of the practical assumptions regarding CSI is the work of Mutangana and Tandon in [37] where they consider the MIMO wiretap channel in the presence of a multi-antenna cooperative jammer and study the secure degrees of freedom (SDoF) taking into consideration the inter-symbol interference (ISI) in the channel. The authors assume no CSI at the legitimate transmitter and the cooperative jammer and only statistical knowledge of the channel is assumed. That is, the knowledge of the channel impulse response lengths which is the effective number of ISI channel taps toward both the eavesdropper and the legitimate receiver. It was shown that positive SDof can be achieved under special conditions with no knowledge of CST at the transmitters and a secure scheme is proposed where the transmitter sends a mixture

of useful data and artificial noise in addition to the specially designed jamming signals sent by the cooperative jammer. The imperfect CSI is studied by Yang et al. [38] considering a multi-user massive MIMO system where channel estimation errors are considered, in addition to the delay during the data transmission and processing phases which causes the CSI to be outdated. Moreover, the different effects of the imperfect CSI on the system's performance in terms of secrecy, in addition to its effects on the ergodic secrecy capacity of the system are analyzed and discussed in details. Also, the authors propose a scheme for predicting the channel state trying to overcome the imperfections in the predicted CSI. Finally, the harmful effect of the imperfect CSI on the system's secrecy and the secrecy improvements gained from using the proposed scheme for channel prediction are validated by simulation results.

In order to further enhance the security of wireless systems, an artificial noise (AN)-aided approach was introduced by Goel and Negi [39]. It is a well-known technique to confuse eavesdroppers where the transmitter transmits confidential messages and embeds noise in them. Liu et al. [40] studied the use of artificial noise to achieve secrecy in a MIMO system. The authors proposed the concept of practical secrecy as a new criterion to evaluate the secrecy of the communication system in the presence of an eavesdropper. This concept studies how the error probability of the eavesdropper behaves as the SNR goes to infinity. The authors show that practical secrecy can be achieved even in the case where the eavesdropper is equipped with a larger number of antennas than the legitimate transmitter. Hu et al. [41] consider a scenario of combating multiple passive eavesdroppers by deploying a cooperative jammer in the wireless network. Perfect receiver CSI is assumed available while only statistical CSIs of the eavesdroppers is available. Also, the transmitter performs beamforming and embeds artificial noise in its data transmission. First, an exact closed-form expression of the secrecy outage probability was derived, conditions to achieve positive secrecy were established and secrecy rate is maximized. The authors also studied the effects of the channel quality and the number of passive eavesdroppers on the design of the transmission scheme and the system's performance in terms of secrecy. It was noted that the optimal ratio between the power of the useful information carrying signal and the power of the artificial noise signal increases when the quality of the available wireless channel increases. Also, this ratio is degraded when the number of eavesdroppers is increased. That is, a stronger AN signal is required when there is a large number of eavesdroppers in order to mislead them. Simulation results proved the secure system performance under the proposed scheme, in addition to the importance of the cooperative jammer in securing the wireless network.

Another interesting idea for enhancing the security of wireless systems using PLS solutions is the deployment of a full-duplex (FD) jamming receiver which was proposed in [42]. It is shown that a better secrecy performance is achieved if the AN signal is sent by the FD receiver instead of the legitimate transmitter. In [43], a FD receiver is considered to combat passive eavesdropping. Enhancements

in the secrecy performance of the system were noted compared to the case when a half-duplex (HD) receiver was used. In [44], the FD receiver dedicates some of its multiple antennas to send AN signals toward a multi-antenna eavesdropper. In addition to the AN signals the transmitter sends. Ma et al. [45] consider a scenario of multiple passive eavesdroppers that do not collude with each other. A multi-antenna FD receiver and a multi-antenna cooperative jammer are considered in the system to improve the secrecy performance. Here too, perfect CSI of the receiver is assumed available, while only statistical CSI of the eavesdropper's channels is considered. The proposed scheme proves secure in simulation results.

Finally, in order to improve the secrecy performance of the wireless systems with multiple antennas against passive eavesdropping, transmit antenna selection is a well studied technique. In this method, the antenna elements in the antenna array which experience the best channel conditions are considered for data transmission, while the antennas with bad channel conditions are not used for data transmission. In [46], transmit antenna selection is performed over $\alpha - \mu$ fading wireless channels and different assumptions regarding the knowledge of the CSI of the receiver and the eavesdropper are considered. In many cases, the optimization problem of antenna selection is combined with the power allocation optimization problem in massive MIMO systems. An example is the work of Li et al. [47] where joint antenna selection and power allocation is studied to achieve an energy-efficient Massive MIMO system. An intelligent implementation of the antenna selection problem in massive MIMO systems using Monte Carlo Tree Search technique is proposed in [48]. Thus, antenna selection is an important concept to be taken into consideration when designing a PLS solution based on massive MIMO systems.

2.2 Anti-Jamming Techniques at The Physical Layer

In electronic warfare, the attackers try to make use of any tool capable of disrupting the communication links of their adversaries [49]. In this regard, jamming attacks are considered the strongest Denial of Service (DNS) attacks in terms of wireless communications disruption [50]. Generally speaking, jamming attacks may be intentional from an adversary side that tries to prevent the legitimate receiver from correctly receiving the actual transmitted signals from the legitimate transmitter by sending noise signals towards the receiver [10, 50]. However, jamming may be unintentional too. An example is radio frequency interference (RFI) which comes from other telecommunication devices and may act like jamming signals [51]. The victims of jamming attacks range from IoT devices and e-health devices which help monitoring the health of humans [24], to satellite based navigational systems like the Global Positioning System (GPS) and the

Global Navigation Satellite System (GNSS) [52, 53]. In addition to smart cities and smart homes [54], among many others like transportation networks, and police radars. These are some civil victims of jamming attacks. On top of that, jamming attacks and their countermeasures known as anti-jamming techniques play a very critical role in military applications and battlefields [55, 56]. Actually, victory in modern wars is achieved by winning the electronic warfare. Defence institutions all over the world are rushing to possess the most advanced electronic countermeasures to deceive, confuse and disable the defence systems of their enemies while keeping their own communication infrastructure covert [56].

There is huge variety of jamming models and techniques. Among the effective attacks which proved an efficient jamming performance are four famous jamming models which were described in [57]:

- The constant jammer which continuously emits radio signals.
- The deceptive jammer which injects regular packets constantly and does not send random bits. No gap is left between the transmitted packets in order to deceive the legitimate receiver and make it believe that a real message is being transmitted.
- The random jammer which alternates its state between jamming and sleeping. So, it sends jamming signals for a specific period of time, then it turns off and stops sending any signal for another specific time period. When jamming, the jammer behaves like either a constant or a deceptive jammer.
- The three mentioned jammer models are considered to be active jammers since they all try to block the channel and keep it busy without checking if data packets are being sent or not. These types of jammers are considered to be effective, however, they risk being easily detected. The fourth type of jammers is not an active jammer, it is rather a reactive jammer that spies on the channel to sense if data packets are being transmitted. Whenever it detects data transmission on the channel, it sends jamming signals to interfere with the legitimate data and disrupt its reception. This is one of the most powerful jammers that is difficult to be detected.

There are several methods for combating jamming attacks, also known as anti-jamming, which happen at different layers of the protocol stack depending on the nature of the attack [50]. Conventional anti-jamming techniques include transmit power control and frequency hopping [58]. Do et al. [59] considers a scenario where a single-antenna jammer is jamming a legitimate user with single antenna while communicating with a massive MIMO Base Station (BS). An anti-jamming technique based on pilot re-transmission in the uplink is proposed. Both random and deterministic jamming scenarios are studied and an efficient anti-jamming performance is obtained.

The physical layer plays a major role in the anti-jamming process, especially with the use of antenna arrays. Anti-jamming techniques that are completely performed at the physical layer [50] include the famous spread spectrum communications technique which is a signal processing based technique [60]. In addition to the usage of directive antennas and beamforming algorithms to perform anti-jamming [61], which is the method adopted in this thesis. In particular, in anti-jamming beamforming using planar antenna arrays, the legitimate signal is added constructively, while the jamming signal is added destructively in the same time. Another famous anti-jamming strategy that is based on multi-antenna wireless communication systems is the optimum joint design of both the transmit and receive beamforming [62]. The literature is rich with anti-jamming techniques using antenna arrays. For example, some anti-jamming methods apply for GNSS systems such as inertial aiding, spatial filtering, time and frequency filtering, and vector tracking [51]. An approach for chirp-style jamming signal suppression in GNSS receivers using an adaptive-partitioned subspace projection is developed in [63]. Also, adaptive antenna array systems are used to achieve reliable GNSS signals quality where the antenna outputs are weighted and summed to perform beamforming and null steering in specific directions. In order to maximise the array output signal-to-interference-plus-noise-ratio (SINR), the minimum variance distortionless response (MVDR) method [64] and minimum mean square error (MMSE) method [65] have been proved to be optimum for GPS signals. The performance of the MMSE method was improved in [66].

As mentioned previously, reactive jammers are very powerful and difficult to be detected. Many of the existing techniques to combat reactive jammers require modifying the physical layer protocols, which is difficult to implement in commercially available devices, or require specialized hardware, that is expensive [67]. Lim et al. [68] exploit the decoy signal which means transmitting fake information in order to deceive the enemy. By properly designing the beamforming strategy at the transmitter and receiver, the proposed anti-jamming scheme successfully deceives reactive jammers. Authors in [67] propose an anti-jamming protocol, named “BitTransfer”, that preserves the legitimate communication link in the presence of powerful reactive jamming attacks. In BitTransfer, information bits are embedded in radio activity operations, the absence of any radio activity is represented by a 0, and the reception of a corrupted packet at the receiver is represented by a 1. The proposed protocol proved an efficient performance in a wide class of commercial wireless devices. It is open-source, robust, and has a superior performance compared with the existing jamming countermeasures. Finally, an important system that can play an effective role in launching and mitigating jamming attacks is Software Defined Radio (SDR) and Cognitive Radio (CR) networks. Baldini et al. [69] study and summarize the security challenges including jamming attacks in SDR and CR.

2.3 Massive MIMO Technology and Physical Layer Security

Massive MIMO is considered to be the key enabler of the 5G technology because of its ability to provide high spectral efficiency in the coverage tier [70]. Massive MIMO ensures the serving of multiple user equipments (UEs) in the same time-frequency resources and has a large number of antennas at the base station than UEs per cell to suppress interference efficiently [71]. The BS needs to perform beamforming efficiently in order to benefit from the large number of antennas. Generally, MIMO communication systems use digital beamforming techniques aiming to provide the full capacity of the communication systems. In order to achieve beamforming using the multiple antennas of the system, simple precoding is required at the transmitter. Then, decoding is applied by the receiver. Several precoding techniques exist for digital beamforming such as zero forcing beamforming (ZF) and maximum ratio transmission (MRT) [72]. However, when massive MIMO is considered, deploying digital beamforming techniques becomes highly expensive and is infeasible in lower frequency bands [73],[74]. This is why millimeter wave (mmWave) frequencies were studied in the literature and considered as one of the promising technologies for the fifth generation 5G. To achieve the high antenna gain needed to handle the required huge capacity of 5G, the use of mmWave alone is not enough and we need to overcome the large cost of massive MIMO beamforming. In order to overcome the problems of digital beamforming, analog beamforming was introduced where low cost phase shifters were deployed instead of the expensive analog to digital converters and frequency converters [75]. Analog beamforming is also unable to give the full potential of spacial multiplexing gain because of the constraints that phase shifters have on their constant modulus in addition to their performance [76]. In order to achieve a better performance in terms of throughput and spectral efficiency, in addition to low cost of implementation that makes massive MIMO systems practically realizable, hybrid beamforming is introduced at both the analog and digital domains. In fact, hybrid beamforming achieves a performance that is close to the digital beamforming performance but with much lower complexity. The authors in [77] studied hybrid beamforming for a downlink massive MIMO system. They compared the performances of fully digital and fully analog beamforming with the hybrid beamforming. Both uniform and nonuniform linear arrays were considered in the system. The non-uniform linear arrays considered are binomial and Dolph-Chebyshev arrays which help reducing the side-lobe level and maximizing the antenna directivity, respectively. Further details about non-uniform antenna arrays will be given in chapter 3. Simulation results in [77] indicate that the performances of hybrid beamforming and fully digital beamforming are very similar to each other. Also, results show that deploying non-uniform antenna arrays with hybrid beamforming significantly improves the performance and makes it closer

to the performance of the fully digital beamforming system while it requires a lower power complexity.

An important aspect of Massive MIMO that has yet only received limited attention is PLS [78]. Massive MIMO provides robustness against passive eavesdropping which improves the physical layer security [9]. Researches have shown the ability of Massive MIMO to provide a secure communication between the transmitter and receiver in the presence of an eavesdropper. Having a large number of antennas at the transmitter facilitates beamforming of the transmitted signals in the direction of the intended users while weakening the signals' intensities in other directions; thus, reducing the capability of eavesdroppers to detect the secret key, encrypted messages or even unencrypted messages [70, 79]. In this way, the main beam of the array will be directed toward the receiver, whereas the eavesdropper would be placed at side-lobes or nulls.

Also, similar to the work [45] mentioned in section 2.1 that uses MIMO antennas, massive MIMO antenna arrays can be used to provide transmission of data to the receiver while jamming the eavesdropper simultaneously. This can be achieved by dedicating part of the antenna elements at the transmitter for sending jamming signals toward the eavesdropper while the other elements would be used to transmit the useful signals to the legitimate destination [80]. In this way, Massive MIMO limits the ability of eavesdroppers to detect useful signals [79].

The design of the antennas in massive MIMO systems is a major factor especially when the purpose of the system is to provide physical layer security. Several aspects need to be taken into consideration such as the array configuration, type and number of antenna elements, and mutual coupling, all of which play a role in the system performance. Some antenna configurations in Massive MIMO for physical layer security have been studied such as massive cylindrical antenna arrays in [81]. In Chapter 3 of this thesis, we will describe a very important type of massive MIMO antennas which is planar antenna arrays that will be used in the proposed security solutions.

2.4 Cryptographic Security Techniques at The Physical Layer

In the majority of work done in the literature, the proposed PLS solutions generally focus on one of the aforementioned techniques to provide security. The authors in [20] showed that it is not optimal to depend only on the randomness of the wireless channel to secure wireless systems. Thus, combining cryptographic and non-cryptographic PLS solutions should be adopted to provide further security and robustness for wireless systems. In fact, developing a chain of security mechanisms at different layers may make the communication system only as strong as the weakest security mechanism at one layer [82]. However, combining

cryptographic and non-cryptographic techniques at the physical layer strengthens the system's security at the physical layer.

Mucchi et al. [82] try to answer the question: "How to measure the benefit that PLS can bring to cryptography?" The authors investigate an eavesdropping attack where they combine PLS with traditional cryptography of wireless systems. Simulation results show the advantages of combining both techniques since PLS increases the detection error of the eavesdropper and, in the same time, the data received by the eavesdropper is encrypted. In spatial modulation massive MIMO systems, existing PLS techniques usually result in degradation in the spectral efficiency and require a predefined secret key and perfect channel state information. In order to enhance the security of spatial modulation massive MIMO systems and to overcome the problems in existing PLS techniques, Wang et al. [83] propose an encryption approach at the physical layer, named chaotic antenna-index three-dimensional modulation and constellation points rotated (CATMCPR). The proposed approach exploits the chaotic theory and spatial modulation techniques. It is proven that the CATMCPR scheme overcomes the drawbacks in conventional PLS techniques and guarantees secure communication links.

Generally, wireless systems apply public key cryptography in order to generate and exchange secret keys between the transmitter and the receiver so that the communication link is secured. These public keys require complex computations to achieve the specified secrecy level of the key bits. Usually, extracting the secret keys depend on the reciprocity of the channel state between the transmitter and the receiver. Taha and Alsusa [84] propose a key exchange technique that is based on the physical layer. In this technique, the key bits are transmitted by encoding them within some phase randomization sequences which are "privately indexed to a specific channel criterion". The authors tested the proposed technique on an OFDM MIMO system. Simulation results demonstrate that the proposed technique achieves superior key error rate performance at a lower computational complexity with better secrecy performance.

Liu et al. [85] proposed the unshared secret key (USK) cryptosystem that combines PLS with traditional cryptographic security solutions. In USK, the injected AN is redesigned so that it is aligned within the null space between the legitimate transmitter and the receiver. The proposed USK cryptosystem is proven to guarantee Shannon's perfect secrecy without requiring secret key exchanging.

2.5 Machine Learning and Deep Learning in Wireless Communications and Physical Layer Security

The future of wireless networks and wireless communications includes the deployment of massive amounts of sensors and wearables where everything around us will become connected transmitting data streams [86]. Thus, achieving ultra-reliable low-latency communications is a must in order to handle the vast amount of data being generated and to guarantee good performance of the different wireless services [5]. This rapid development of the IoT and the evolution of new wireless services lead to the development of the 5G technologies like massive MIMO, millimeter wave(mmW) communications, and device-to-device communications (D2D) which promise to handle the large amounts of data that is being generated [86]. These technologies have been identified and some of them are already implemented [87, 88]. However, intelligence is required in order to integrate these technologies in a way that handles the IoT requirements and meets its challenges. The intelligent functions are required at both the core and the edge of the wireless network and they must be able to optimize its performance to achieve the required Quality of Service (QoS) by the emerging IoT and wireless services. This is achieved by properly exploiting the available wireless resources and handling the generated data [86]. In order to achieve this intelligence, the research community must focus on deploying the concepts and the fundamentals of artificial intelligence (AI) [89] in wireless communications and networking infrastructure and within consumer devices. The true potential of AI in wireless communications began with the recent developments in machine learning (ML)[90] and neural networks (NN)[91]. In order to build wireless networks that are based on AI, researchers must focus on exploiting the various ML techniques and NN architectures. In fact, the most important task to be performed is to choose the right ML and NN tools and tailor them so that they become compatible with the special characteristics of the wireless medium [92]. An example of applying ML algorithms in IoT sensor networks is the work of AlHajri et al. [93] which applied ML techniques for classifying the surrounding objects in the indoor environment for IoT sensor networks. In fact, classifying the surroundings brings large enhancements to the performance of positioning and tracking tasks, in addition to optimizing power consumption. The ML classifier model is trained on actual real-time measurements of RF signals. The authors studied multiple classification algorithms including decision trees, support vector machine, and k-nearest neighbors. Various RF features were considered in training and testing the ML models. The obtained results indicate that k-nearest neighbors method achieved the best performance with highest accuracy. This is achieved when the chosen input features were the channel transfer function and frequency coherence function. The required prediction time satisfies the requirements of real-time

applications.

ML and DL algorithms have a huge potential in a wide area of applications in wireless communications, antennas, and RF circuits. In fact, some of these algorithms are already deployed in designing some RF components and circuits [94, 95]. In [96], a hybrid beamforming mmWave communication system is considered and ML and DL are exploited in order to extract information about the Angle of Arrival (AoA) to ease the process of beam selection in the uplink data transmission.

In the field of Transmit Antenna Selection (TAS), the authors in [97] were first to try utilizing machine learning technology into wireless communication. They mapped the TAS in wireless communication into multi-class classifications, and compared the effects of TAS on communication performance based on the k-nearest neighbors and support vector machine algorithms. After that, in [98], the authors discussed the optimal antenna selected by using support vector machine and the naive Bayesian scheme to maximize privacy performance. Gecgel et al. [99] consider large-scale MIMO systems where they deploy ML algorithms in a proposed dynamic generalized spatial modulation framework. The authors adopt the decision tree and multi-layer perceptron algorithms to perform the TAS task. The proposed framework was tested in an SDR testbed and achieved superior performance in terms of channel estimation errors. Hu et al. [100] considered a MIMO wiretap channel with outdated CSI and propose a deep reinforcement learning framework of Deep Q Network (DQN) to perform optimal TAS. The legitimate receiver depends on the SNR of the received pilot signals transmitted by each antenna at the legitimate transmitter. Then, the DQN is used to make predictions regarding the optimal transmit antenna at the next moment. The system showed effective performance in simulation results.

Due to the crowdedness of the electromagnetic spectrum, and in order to secure the communication links, it is crucial to identify the different RF transmitters both in terms of the content of their transmitted data and their physical characteristics. Youssef et al. [101] deploys ML and DL algorithms to perform this classification and identification of RF transmitters. The authors tested four different models to perform the classification task. The model which achieved the most accurate performance with 100% accuracy with 12 classes is Deep Neural Network (DNN) with multi-stage training.

Wang et al. [102] studied signal demodulation techniques based on DL. They also proposed the first open dataset for wireless communications consisting of real modulated signals. In order to build the dataset, a flexible communication prototype platform is proposed and the real modulated signals are measured. Then, two demodulators are proposed. The first demodulator combines deep belief network (DBN) and support vector machine (SVM) where DBN is used for feature extraction and SVM is used for classification. The second demodulator is based on adaptive boosting (AdaBoost) algorithm in which the k-nearest neighbor algorithm is considered to be the weak classifier. The two models are trained

and tested on the generated dataset. Simulation results indicate the superiority of the proposed demodulators when compared with demodulators that include single classification algorithms like DBN, SVM, and maximum likelihood.

An interesting idea that will be integrated into the future wireless cellular networks is cellular-connected Unmanned Aerial Vehicles (UAVs) since they will play a vital role in applications as delivery systems and online video streaming among others. Challita et al. [103] study the challenges that must be addressed in order to ensure reliable performance for the cellular-connected UAVs, in addition to the security threats facing them. In order to tackle these challenges, several solutions that make use of artificial intelligence, deep learning and Artificial Neural Networks (ANN) are proposed. Simulation results prove the effectiveness of the proposed solutions. An important enabler for vehicular communications is mmWave systems supporting high mobility. Implementing such systems is practically challenging especially in terms of the training overhead required for choosing the optimal beamforming antenna vectors in large arrays. Alkhateeb et al. [104] proposed a solution that integrates deep learning and coordinated beamforming to overcome these challenges. Simulation results indicate that the proposed scheme achieves lower training overhead and higher rates in high mobility systems when compared with the traditional beamforming techniques. Authors in [105] provide a detailed survey of all proposed techniques in the literature where ML is deployed in cellular UAV wireless networks in order to improve system's performance from several perspectives such as management of resources, wireless security, and positioning.

With the increasing interest in the wireless community in applying machine learning techniques in wireless communications and wireless networks, researchers started studying the role that machine learning can play in security. This includes both launching and mitigating physical layer security attacks. The type of machine learning that studies scenarios where an adversary is present is named: adversarial machine learning [106].

An interesting area of applications for machine learning that has a huge potential is cognitive radios where it leads to effective performance of several tasks like enemy detection, object classification, in addition to making predictions, channel estimation, and spectrum sensing. This is done by making use of the received information about the spectrum environment and adapting to it [107, 108]. Also, software defined radio (SDR) is another technology where ML can play a vital role. Riyaz et al. [109] combines both the SDR sensing capabilities and DL algorithms in order to uniquely detect a certain radio signal among similar signals from other devices. The adopted DL model is convolutional neural network (CNN) and the dataset on which the model was trained was collected from a testbed of SDRs. Deploying this model requires no high-level decoding, feature engineering, or knowledge of protocols, since the DL model depends on signal modifications of the transmitter that are induced by the hardware. This proposed model showed effective performance when simulated and it enhanced the

system's security against spoofing attacks.

Erpek et al. [106] applied adversarial machine learning techniques in designing a jamming technique and proposing an anti-jamming method. In the proposed jamming technique, the transmitter depends on recent sensing data of the channel status and uses a pre-trained classification model to decide to transmit or not. On the other hand, the jammer tries to predict the next successful transmission of the transmitter by building a deep learning classifier based on the collected data of channel state information and acknowledgment bits. In order to reduce the time spent by the jammer collecting data to build its dataset for training the model, a generative adversarial network is adopted where the collected dataset is augmented with synthetic samples. The proposed anti-jamming scheme technique in order to secure the data transmission is that the transmitter takes some wrong actions in terms of spectrum access, thus, preventing the jammer from building a reliable deep learning classifier. This way, the jammer is misled and will make many wrong predictions wasting its power. Kumar et al. [110] considered a jamming system model in vehicular networks with a focus on vehicle's localization in environments where delimited jamming is present. The authors propose a Delimited Anti-jamming protocol that is based on machine learning and deployed in vehicular traffic environments. They make use of the open-source ML algorithm named CatBoost which relies on decision trees in order to make predictions about the locations of the jamming vehicle. This type of networks, named Internet of vehicles (IoV), is a promising area of research that is receiving increasing interest from the research community since it promises to address traffic incidences and supports green mobility.

2.6 Thesis Contributions

The main contributions of this thesis compared to the existing security solutions in the literature are summarized next.

- Joint jamming-transmission solution against passive eavesdropping using planar antenna arrays is investigated. Multiple scenarios are considered at both the transmitter and receiver where the importance of sending jamming signals toward the eavesdropper is confirmed and the number of required antennas to perform this task is identified.
- A simple and fast look-up table-based anti-jamming technique is proposed where the required antenna configuration of a planar antenna array is identified based on the location of the transmitter and jammer. Good SINR is achieved and effective anti-jamming solution is achieved.
- A scalable and effective anti-jamming ML model is proposed. The dataset is generated, including the locations of the transmitter and jammer as input

features, in addition to the channel gain between the transmitter and receiver. The outputs are the antenna excitation coefficients of the planar antenna array. The model is different from any other ML-based anti-jamming model existing in the literature and the dataset generated is unique.

Chapter 3

Planar Antennas & Wireless Channel Overview

In this chapter, an overview of planar antenna arrays is given, beamforming using these antennas is introduced and the directivity of these arrays is investigated. Then, three different types of linear arrays that will be used throughout this thesis are discussed. Finally, the wireless channel model adopted in this thesis is presented.

3.1 Planar Antenna Arrays

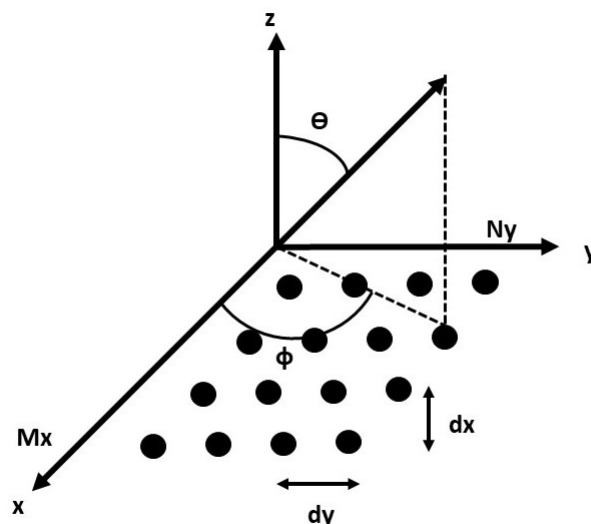


Figure 3.1: Planar antenna array in the x-y plane.

The radiation patterns of planar antenna arrays (Figure.3.1) are controllable and can be shaped as required. These antennas can provide more symmetrical patterns with lower side-lobes. In addition, they are a perfect candidate for beamforming since their beams can be directed to any specific direction while directing the low side-lobes and nulls to other directions where it is undesired to communicate. Planar arrays can play a great role in PLS. They can provide very directive beams. Some of the radiating elements can be directed towards the legitimate users while the rest of the antennas is used to send jamming signals to eavesdroppers for example. The applications of planar arrays include tracking radar, search radar, remote sensing, communications, and many others [111].

3.1.1 Array Factor

In planar antenna arrays, single antenna elements are positioned along a rectangular grid to form a planar array. If M elements are initially placed along the x-axis with spacing d_x and progressive phase shift β_x between the elements, the array factor of this linear array of elements along the x-axis is shown in [111] to be:

$$\text{AF}_{\text{linear,x}}(\theta, \phi) = \sum_{m=1}^M I_{m1} e^{j(m-1)(kd_x \sin \theta \cos \phi + \beta_x)} \quad (3.1)$$

Where I_{m1} is the excitation coefficient of element m . Moreover, if N such arrays are placed above each other in the y-direction, a distance d_y apart and with a progressive phase shift β_y , a rectangular array will be formed. The array factor of the rectangular array is the product of the array factors of the arrays along the x- and y-directions. The array factor of a linear array of N elements along the y-axis is given by:

$$\text{AF}_{\text{linear,y}}(\theta) = \sum_{n=1}^N I_{1n} e^{j(n-1)(kd_y \sin \theta \sin \phi + \beta_y)} \quad (3.2)$$

The planar antenna array (Figure 3.1) at the receiver is considered as a combination of linear subarrays along the x- and y- axes. The array factor of the planar array is the multiplication of the array factors of the corresponding linear subarrays. Thus, a unique radiation pattern is produced from every combination of linear subarrays. The array factor of the planar array is given by [111] to be:

$$\text{AF}_{\text{planar}}(\theta, \phi) = \text{AF}_{\text{linear,x}}(\theta, \phi) \times \text{AF}_{\text{linear,y}}(\theta) \quad (3.3)$$

$$\text{AF}(\theta, \phi) = \sum_{n=1}^N I_{1n} \left[\sum_{m=1}^M I_{m1} e^{j(m-1)(kd_x \sin \theta \cos \phi + \beta_x)} \right] e^{j(n-1)(kd_y \sin \theta \sin \phi + \beta_y)} \quad (3.4)$$

For uniform planar arrays, all elements have the same excitation amplitudes, i.e., $I_{m1} = I_{1n} = I_o$ for all m and n . So, the array factor becomes:

$$\text{AF}_{\text{linear,x}}(\theta, \phi) = I_o \sum_{m=1}^M e^{j(m-1)(kd_x \sin \theta \cos \phi + \beta_x)} \times \sum_{n=1}^N e^{j(n-1)(kd_y \sin \theta \sin \phi + \beta_y)} \quad (3.5)$$

The normalized array factor can be obtained as:

$$\text{AF}_n(\theta, \phi) = \left\{ \frac{1}{M} \frac{\sin(M \frac{\psi_x}{2})}{\sin(\frac{\psi_x}{2})} \right\} \left\{ \frac{1}{N} \frac{\sin(N \frac{\psi_y}{2})}{\sin(\frac{\psi_y}{2})} \right\} \quad (3.6)$$

Where:

$$\psi_x = kd_x \sin \theta \cos \phi + \beta_x \quad (3.7)$$

$$\psi_y = kd_y \sin \theta \sin \phi + \beta_y \quad (3.8)$$

It is noticed from equation 3.4 that the array factor of planar arrays is a function of the geometry of the array (number of antenna elements, the axes on which they are distributed and the distances separating them), the excitation amplitudes and the phases. In the previous equations, the antenna elements are assumed to be isotropic. However, if the type of antennas used in the array is changed so they are no longer isotropic, the total field of the array will be equal to the product of the field of a single element usually at the origin, and the array factor of that array. That is,

$$E(\text{total}) = \left[E(\text{single element at reference point}) \right] \times \left[\text{arrayfactor} \right] \quad (3.9)$$

3.1.2 Beamforming

To achieve beamforming, the major lobe (principal maximum) is located at angles such that:

$$kd_x \sin \theta_o \cos \phi_o + \beta_x = 0 \quad (3.10)$$

$$kd_y \sin \theta_o \sin \phi_o + \beta_y = 0 \quad (3.11)$$

The main beam is in the direction: $\theta = \theta_o$ and $\phi = \phi_o$.

And the progressive phases β_x and β_z must satisfy:

$$\beta_x = -kd_x \sin \theta_o \cos \phi_o \quad (3.12)$$

$$\beta_y = -kd_y \sin \theta_o \sin \phi_o \quad (3.13)$$

3.1.3 Directivity

In general, since the relation between the antenna gain and directivity is only a loss factor, that is the antenna efficiency, then we can use the directivity instead of the gain to evaluate the antenna performance. The general expression for calculating the directivity of the array factor $AF(\theta, \phi)$ that has its main beam directed towards $\theta = \theta_o$ and $\phi = \phi_o$ is given by [111]:

$$D_o = 4\pi \frac{|AF(\theta_o, \phi_o)|^2}{\int_0^{2\pi} \int_0^\pi |AF(\theta, \phi)|^2 \sin\theta d\theta d\phi} \quad (3.14)$$

3.2 Linear Antenna Arrays

The linear antenna arrays that form the planar arrays have different possible configurations. The first way to differentiate linear arrays is considering the spacing between the antenna elements. The element spacing is either uniform when all the elements are separated by the same distance, or non-uniform when the separating distance between the elements is inconsistent. In this thesis, only uniformly spaced linear arrays are considered. The second way to differentiate linear arrays is the distribution of the array amplitude among the antenna elements. Each antenna configuration implies unique ratios between the excitation coefficients of the linear array antenna elements. In this sense, three linear array configurations are considered in this thesis and are described next [111]:

3.2.1 Uniform Amplitude Linear Arrays

In this type of linear arrays, all the radiating elements are excited with the same amplitude, thus the name uniform amplitude. The phase shift for each element is based on the direction toward which the main beam is directed using equations 3.12 & 3.13. Uniform linear arrays usually possess the largest directivity and yield the smallest half-power beamwidth. However, the main drawback of uniform linear arrays is that they generally have high side-lobe levels.

3.2.2 Non-uniform Amplitude Binomial Linear Arrays

The reason behind using non-uniform excitation coefficients is to estimate the array's beamwidth and to produce side-lobes with smaller power levels. In the case of binomial linear arrays, the objective is to remove secondary side lobes. In order to achieve this goal, different distribution function for the amplitudes of the excitation currents of the antenna array elements are deployed [112].

The excitation coefficients of a binomial array are given based on the binomial expansion:

$$(1+x)^{m-1} = 1 + (m-1)x + \frac{(m-1)(m-2)}{2!}x^2 + \frac{(m-1)(m-2)(m-3)}{3!}x^3 + \dots$$

The positive coefficients obtained from the binomial series expansion for different values of m form the Pascal's triangle. When the values of m are considered to be the number of antenna array elements, then the coefficients resulting from the expansion of the binomial series represent the relative amplitudes of the antenna array elements. Since the obtained excitation coefficients resulted from a binomial series expansion, then the array is known as a binomial array. Usually, binomial arrays possess the smallest side-lobe levels.

3.2.3 Non-uniform Amplitude Dolph-Chebyshev Linear Arrays

In Dolph-Chebyshev linear antenna arrays, the amplitudes of the excitation coefficients for the antenna array radiating elements are found based on Chebyshev's polynomial. While the phase shift for each radiating element is based on the direction towards which the main beam is directed based on equations 3.12 & 3.13. The main objective in this type of linear arrays is to maximize the gain of secondary lobes to a certain fixed level [112].

The Chebyshev's polynomials follow the following recursion formula:

$$T_m(z) = 2zT_{m-1}(z) - T_{m-2}(z)$$

where $z = \cos(u)$ and $T_0(z) = T_1(z) = 1$.

In Dolph-Chebyshev linear arrays, the desired side-lobe level (SLL) is specified during the design process. The SLL has a huge impact on the resulting excitation coefficients amplitudes. The range of SLL is generally between -10 dB and -60 dB.

3.3 Wireless Channel Model

An important point to consider when proposing a PLS solution that is based on multi-antenna technology is the adopted wireless channel model between antenna elements. A common assumption made in the literature is that the channels are independent. This assumption is considered realistic when the separating distance between the antenna elements is sufficient. However, from a practical point of view, the antenna elements may be correlated because of the space constraints [32]. However, when the far-field of the antenna array is considered, a valid assumption that eases the computations is to look at the antenna array as a single unit having a single wireless channel. This is a simplified model of the wireless channel which simplifies the simulation process of the proposed security solutions

and the analysis of the obtained results. The wireless channel model adopted in this thesis is the uncorrelated Rayleigh fading channel model considered in the far-field of the antenna array, which is described next.

3.3.1 Uncorrelated Rayleigh Fading

The wireless channel between two entities i and j that models the open nature of the wireless channel and the various propagation and environmental conditions is given by [113]:

$$H_{i,j,\text{dB}} = (\kappa - 10\gamma \log_{10} d_{i,j}) + \psi_{i,j} + 10 \log_{10} F_{i,j} \quad (3.15)$$

Where κ is the pathloss constant, $d_{i,j}$ is the distance between the two entities i and j , γ is the path loss exponent, $\psi_{i,j}$ represents log-normal shadowing with zero mean and a standard deviation σ_ψ , and $F_{i,j}$ corresponds to Rayleigh fading with a Rayleigh parameter b (usually selected such that $E[b^2] = 1$).

Chapter 4

Proposed Solutions for Combating Passive Eavesdroppers

In this chapter, we propose a physical layer security solution for combatting a single passive eavesdropper at a known location. We study the effect of jamming the eavesdropper and transmitting legitimate data simultaneously and we investigate the effects of varying the number of antennas dedicated to each task. Then, we extend our model and propose a physical layer security solution capable of combating multiple passive eavesdroppers at unknown locations. Our solution combines antenna arrays with secret key generation. The details of the proposed solutions are discussed in the following sections.

4.1 Single Passive Eavesdropper at a Known Location

This section considers the scenario of combating a single eavesdropper at a known location. The work done in this scenario resulted in the conference paper [114].

4.1.1 System Model

The system model presented in this scenario consists mainly of a source Alice that aims to transmit messages to a target destination Bob in the presence of an eavesdropper Eve with a known location. Alice is assumed to have a planar antenna array whereas two cases are depicted for Bob. Case 1, as shown in Figure 4.1, assumes that the destination Bob, as well as the eavesdropper Eve, are equipped with an omni-directional antenna. This case will be referred to as the “Source only” case since only the source Alice is equipped with a planar array

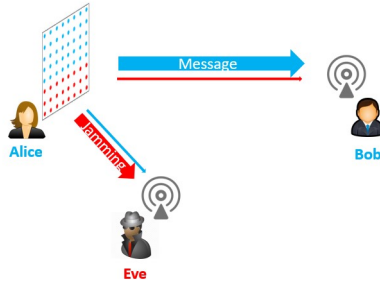


Figure 4.1: System Model with planar antenna array at Alice only “Source Only case”.

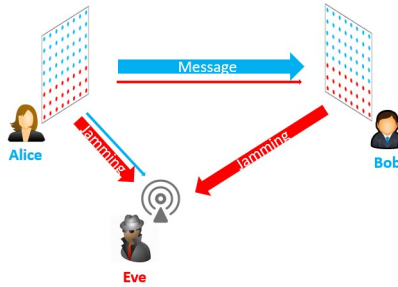


Figure 4.2: System model with planar antenna array at Alice and Bob with “Common Configuration case”.

antenna. The planar array antenna used by Alice performs covert communication without the help of relays. In specific, the planar array is considered as a set of horizontal linear subarrays and can be split to handle two missions: first, to transmit the useful signal to Bob, while the second is to transmit a jamming signal to Eve. In the depicted cases, the main beam of the planar array transmitting the useful signal is directed toward the destination with appropriate beamforming leading to only very small sidelobes. Similarly, the main beam of the array transmitting the jamming signal is directed toward the eavesdropper with very little leakage of the jamming signal toward the destination through antenna’s sidelobes.

On the other hand, case 2 assumes that both Alice and Bob use planar antenna array whereas an omni-directional antenna is used by Eve as shown in Figure 4.2. Moreover, Bob is assumed to be equipped with the appropriate circuitry to transmit and receive simultaneously. In this way, Bob’s array is also split into two parts: one used to receive the signal from Alice and the second can be used to transmit an additional jamming signal to Eve; hence, increasing the secrecy of the communication system. Furthermore, two configurations of the number of linear antenna subarrays used for reception, transmission, and jamming are going to be considered within case 2 to optimize the system performance. To elaborate, let M_A and M_B be the number of linear horizontal subarrays forming

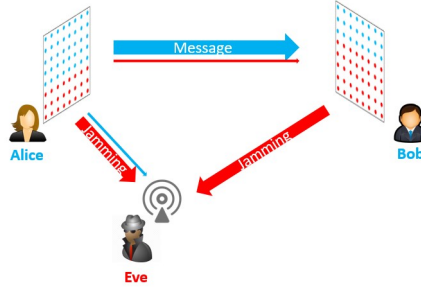


Figure 4.3: System model with planar antenna arrays at Alice and Bob using the “Complementary Configuration case”.

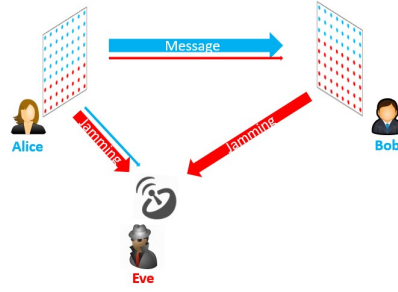


Figure 4.4: System model when Eve is equipped with a directive antenna steered toward Alice.

the planar arrays of Alice and Bob, respectively, with $M_A = M_B = M$. The numbers of subarrays used for transmission and jamming by Alice are $M_{A,t}$ and $M_{A,j}$, respectively. Moreover, $M_{B,r}$ and $M_{B,j}$ represent the number of subarrays used by Bob for reception and jamming, respectively. The first configuration, referred to as the “Common Configuration” and shown in Figure 4.2, depicts using the same number of linear subarrays for transmission and reception by Alice and Bob, respectively, i.e., $M_{A,t} = M_{B,r}$ and $M_{A,j} = M_{B,j}$. The second configuration, referred to as the “Complementary Configuration” and shown in Figure 4.3, consists of setting $M_{A,t} + M_{B,r} = M$ and $M_{A,j} + M_{B,j} = M$; which means that $M_{A,t} = M_{B,j}$ and $M_{A,j} = M_{B,r}$. In the previous cases, the eavesdropper is assumed to be equipped with an omni-directional antenna, having a unit gain in all directions. However, the eavesdropper in actual cases has a strong desire to capture the information sent from the source that may drive him to use a directional antenna in the direction of the source to maximize the capacity of the link. Therefore, the above cases (Source Only, Common Configuration and Complementary Configuration) are going to be reconsidered taking into account that Eve is equipped with a directional antenna steered in the direction of the source, as depicted in Figure 4.4.

Table 4.1: Definitions of Model Parameters for Combating Eavesdroppers

Variable	Description
$P_{A,B}$	Power of signal transmitted from source Alice to destination Bob
$P_{A,E}$	Power of jamming signal transmitted by Alice to Eve
$P_{B,E}$	Power of jamming signal transmitted by Bob to Eve
$H_{A,B}$	Channel gain between Alice and Bob
$H_{A,E}$	Channel gain between Alice and Eve
$H_{B,E}$	Channel gain between Bob and Eve
$G_{A,B}$	Gain of the transmission array of Alice in the direction of Bob (its main beam steered in the direction of Bob (ϕ_B, θ_B))
$G_{B,A}$	Gain of the reception array of Bob, with its main beam steered in the direction of Alice (ϕ_A, θ_A)
$G_{A,E}$	Gain of the jamming array of Alice in the direction of Eve (with its main beam steered in the direction of the Eve (ϕ_E, θ_E))
$G_{B,E}$	Gain of the jamming array of Bob in the direction of Eve (with its main beam steered in the direction of Eve (ϕ_E, θ_E))
$G_{E,A}$	Gain of Eve's antenna in the direction of Alice (main beam steered to (ϕ_A, θ_A) and equal to 1 when an omni-directional antenna is used)
σ^2	Noise power

4.1.2 Capacity Calculations and System Parameters

The following part shows how to calculate the communication capacity between Alice and Bob as well as between Alice and Eve in the presence of the jamming signals in the above cases. The parameters used in the next equations are listed in Table 4.1. The capacities calculated will indicate the efficiency of the proposed model to achieve physical layer security.

The channel capacity, in bits per second per Hertz(bps/Hz), between the source Alice and destination Bob is given by [81]:

$$C_{A,B} = \log_2 \left(1 + \frac{P_{A,B}H_{A,B}G_{A,B}(\phi_B, \theta_B)G_{B,A}(\phi_A, \theta_A)}{I_{A,B} + \sigma^2} \right) \quad (4.1)$$

With $I_{A,B}$ is the jamming signal power received by Bob due to the sidelobes of

the planar antenna array. It is given by:

$$I_{A,B} = P_{A,E}H_{A,B}G_{A,E}(\phi_B, \theta_B)G_{B,A}(\phi_A, \theta_A) \quad (4.2)$$

In (4.1), $G_{A,B}$ is maximum in the direction of Bob, i.e. at (ϕ_B, θ_B) and $G_{A,E}$ is maximum in the direction of Eve and minimum in the direction of the destination Bob, which will fall under sidelobes of the jamming array directed toward Eve. Moreover, in case of the planar array used by Bob, $G_{B,A}$ is maximum in the direction of Alice (ϕ_A, θ_A) to enhance the received signal power, it will also boost the received signal jamming power as shown in the equation of $I_{A,B}$. Note that when a single omni-directional antenna is used by Bob, $G_{B,A}$ is set to one in all directions.

Similarly, the capacity between Alice and the eavesdropper Eve is given by [16]:

$$C_{A,E} = \log_2 \left(1 + \frac{P_{A,B}H_{A,E}G_{A,B}(\phi_E, \theta_E)G_{E,A}(\phi_A, \theta_A)}{I_{A,E} + I_{B,E} + \sigma^2} \right) \quad (4.3)$$

With $I_{A,E}$ is the jamming signal power received by Eve due to the main beam of the planar antenna array used for jamming by Alice and $I_{B,E}$ is the jamming signal power received by Eve due to the main beam of the planar antenna array used for jamming by Bob in case 2. The signal powers are given by:

$$I_{A,E} = P_{A,E}H_{A,E}G_{A,E}(\phi_E, \theta_E)G_{E,A}(\phi_A, \theta_A) \quad (4.4)$$

$$I_{B,E} = P_{B,E}H_{B,E}G_{B,E}(\phi_E, \theta_E)G_{E,A}(\phi_B, \theta_B) \quad (4.5)$$

In (4.3), $G_{A,B}$ is minimum in the direction of the eavesdropper (ϕ_E, θ_E) that will fall under sidelobes of the useful array directed toward Bob (ϕ_B, θ_B) . Moreover, $G_{A,E}$ is maximum in the direction of Eve (ϕ_E, θ_E) leading to high received jamming power by the eavesdropper. Moreover, $G_{E,A}$ is maximum in the direction of Alice so that Eve can maximize the useful information from Alice while Bob (ϕ_B, θ_B) may fall under sidelobes of the directional antenna directed toward Alice. Note that in case of planar array used by Bob, $G_{B,E}$ is maximum in the direction of the eavesdropper (ϕ_E, θ_E) and in case of a single omni-directional antenna used by Eve, $G_{E,A}$ is set to one in all directions.

Secrecy Capacity

In the first scenario, the aim is to maintain a secure communication between the source Alice and the destination Bob regardless of the presence of the eavesdropper; therefore, the secrecy capacity is used as an indication of the system performance. As shown in [81], the secrecy capacity is given by:

$$C_{\text{sec}} = C_{A,B} - C_{A,E} \quad (4.6)$$

Equation (4.6) clearly demonstrates the fact that the channel between the source and the destination is said to be secure if the capacity between Alice and Bob

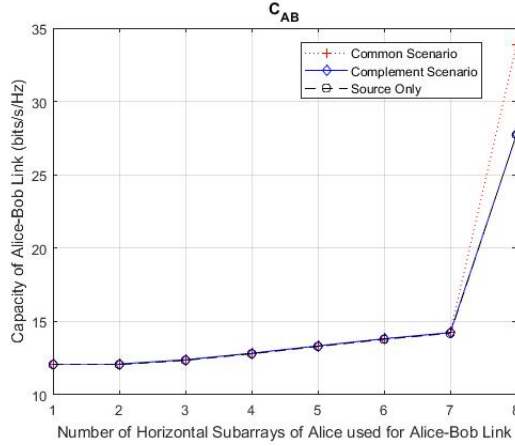


Figure 4.5: Capacity between Source (Alice) and Destination (Bob).

is high and the capacity between Alice and Eve has low values. The proposed model aims to achieve a high secrecy capacity by using the planar antenna arrays with a large number of elements leading to highly directive beams of the useful array in the target destination and highly directive beams of the jamming array toward the eavesdropper.

4.1.3 Simulation Results

To simulate the proposed method and system model, the eavesdropper is assumed to be located in the same plane as the destination Bob in a suburban area. Alice is communicating with Bob using the planar array that is steered toward the location of Bob at $\theta = \phi = 45$ degrees. The communication is done over a channel with zero-mean log-normal shadowing of standard deviation $\sigma_\psi = 8$ dB and Rayleigh fading with parameter b selected such that $E[b^2] = 1$. The empirical path loss is also considered with a pathloss exponent $\gamma = 3.5$ and a pathloss constant $\kappa = -38.46$ dB. Furthermore, the planar antenna array used is made up of eight horizontal antenna subarrays stacked above each other in the z -plane separated by $d_z = 0.5\lambda$ (where λ is the wavelength). Each array consists of eight isotropic antenna elements placed along the x -direction such that $d_x = 0.5\lambda$.

The results of the simulation are averaged over 10^6 iterations. Figures 4.5, 4.6, and 4.7 demonstrate the capacity between Alice and Bob, $C_{A,B}$, the capacity between Alice and Eve, $C_{A,E}$ and the secrecy capacity, C_{sec} , respectively, with respect to the number of linear horizontal subarrays used for transmission by Alice. These three figures consider all the cases of Eve, i.e, whether equipped with omni-directional or directive antenna. The directive antenna is assumed to be steered in the direction of the source Alice (Figure 4.4) with a maximum directivity of 15dB. In this case, Bob is assumed to be located at a sidelobe of the directive antenna used by Eve (at 5dB directivity).

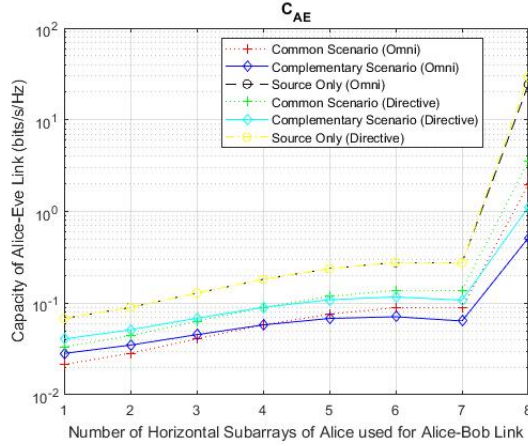


Figure 4.6: Capacity between Source (Alice) and Eavesdropper (Eve).

Figure 4.5 clearly shows that the capacity between the source and the destination increases as the number of antenna subarrays used for transmission increase for all configurations. However, when the number of antenna arrays used for transmission is $M = 8$, all arrays of Alice are used for transmission and none for jamming. Bob is also assumed to be using all the antenna arrays for reception but along with an omni-directional antenna used for jamming the eavesdropper in the “Common Configuration” case. Whereas in the “Complementary Configuration”, when $M = 8$, Bob is assumed to be using an omni-directional antenna for reception while sending jamming signals toward Eve using the planar antenna array. In this case, when $M = 8$, the capacity between Alice and Bob is the same for the “Source Only” and “Complementary Configuration” cases. This explains the results of Figure 4.5 when M increases to 8. Because both Alice and Bob are using planar antenna array for transmission and reception respectively, the capacity of their link increases significantly; hence, the “Common Configuration” case shows best performance for $C_{A,B}$. As expected, $C_{A,B}$ does not change when the Eavesdropper is equipped with a directive antenna since Eve is passive and the antenna used does not affect the communication link between Alice and Bob.

On the other hand, the capacity between Alice and Eve records highest values when jamming is done at the source only and decreases significantly when both Alice and Bob send jamming signals as illustrated in Figure 4.6. In the “Source only” case, jamming is performed by the source only. Hence, when the number of transmit subarrays increases from 7 to 8, i.e., no jamming is performed, then $C_{A,E}$ increases by more than an order of magnitude. This is explained by the fact that no jamming signal is sent toward Eve while the latter is receiving part of the useful signal from the sidelobes of the transmitter antenna subarrays, regardless of the beamforming. It is noteworthy that when Bob performs jamming using an omni-directional antenna in the “Common Configuration” case with $M = 8$, $C_{A,E}$ decreases. This result proves the importance of jamming to combat the effect of

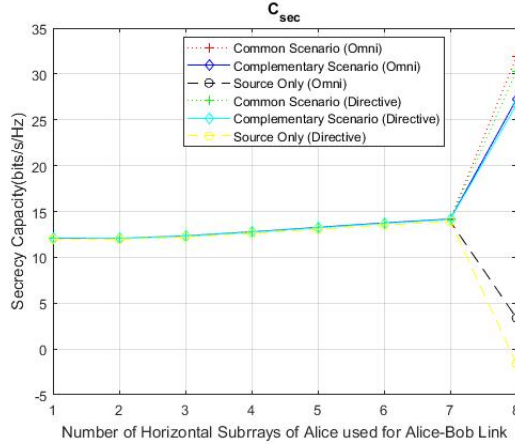


Figure 4.7: Secrecy Capacity between Alice and Bob.

eavesdropping even when using only an omni-directional antenna for jamming. Moreover, $C_{A,E}$ records even more reduction in the “Complementary Configuration” case when Bob uses the planar antenna array for jamming when $M = 8$. This means that the jamming signal power increases significantly to suppress the reception of the useful signal by Eve. This is why the “Complementary Configuration” case has the lowest channel capacity between Alice and Eve in Figure 4.6. When the eavesdropper is equipped with a directive antenna, $C_{A,E}$ records relatively higher values than when an omni-directional antenna was used by Eve. This is because using a directive antenna increases the power of the useful signal in the direction of the eavesdropper. However, the increase in the $C_{A,E}$ values is not that significant since the jamming signal is also amplified by the gain of the directive antenna. This means that, when the eavesdropper uses a directive antenna, both the useful signal and the jamming signal received from the source Alice are amplified.

The results of Figures 4.5 and 4.6 are used to generate the results of the secrecy capacity shown next in Figure 4.7. The secrecy capacity between Alice and Bob increases when the number of transmit antenna subarrays increases for all configurations but records highest values in the “Common Configuration” case. Therefore, the “Common Configuration” has the best secrecy capacity performance followed by the “Complementary Configuration”. However, the latter configuration has the best performance if the main objective is to reduce the useful signal leakage to Eve since in this case, $C_{A,E}$ records minimal values while maintaining relatively good secrecy capacity. Moreover, the secrecy capacity with “Source Only” case shows an important behavior in Figure 4.7 when all the transmit antenna subarrays are used for transmission. In this case, C_{sec} decreases suddenly by more than 10 bits/s/Hz due to the rapid increase in $C_{A,E}$ by more than an order of magnitude. This behavior confirms the importance of physical layer security through simultaneous transmission and jamming to provide secured

and confidential communication. When Eve uses a directive antenna, C_{sec} records relatively lower values for all configurations since $C_{A,E}$ has relatively increased, as mentioned earlier. Furthermore, in the case of “Source Only”, the secrecy capacity decreases significantly when all the antennas are used for transmission and no jamming is performed. In fact, C_{sec} records a negative value which indicates that the secrecy of the link between Alice and Bob is null and the link between Alice and Eve is better than the link between Alice and Bob. Thus, Eve can receive all the information from Alice. This shows that the joint jamming and transmission can efficiently combat passive eavesdropping.

However, passive eavesdroppers are still able to capture the legitimate information in two cases:

- 1- If the eavesdropper is present in the direction of the main beam of the legitimate transmitter i.e. in close proximity to the legitimate receiver.
- 2- If the eavesdropper is present in the direction of a side lobe of the legitimate transmitter

A scenario where multiple passive eavesdroppers at unknown locations are assumed to be present is considered as a future work of this thesis, where an idea of a PLS solution that combines cryptographic and non-cryptographic techniques is proposed.

Chapter 5

Proposed Anti-jamming Techniques at The Physical Layer

After proposing PLS solutions for combating eavesdroppers in the previous chapter, this chapter tackles the problem of jamming attacks, where we propose two anti-jamming techniques. The proposed systems discuss combating a single jammer, and can be extended to scenarios with multiple jammers. The first anti-jamming technique is based on creating a look-up table of possible antenna configurations. Assuming the jammer is detected and its location is identified, the receiver searches in the look-up table for the best antenna configuration in order to mitigate the jamming effect and maintain a secure communication link achieving a high Signal-to-Interference-plus-Noise-Ratio (SINR). Then, the idea of having a look-up table of antenna configurations brought machine learning into our thoughts. In the second anti-jamming technique, we deploy ML algorithms in order to combat jamming attacks, extending the look-up table solution and creating a scalable anti-jamming model.

5.1 Look-up Table Based Anti-jamming Technique

A major objective of any receiver performing anti-jamming at the physical layer is to perform beamforming to maximize the gain towards the legitimate transmitter while steering a null in the direction of the jammer. Some array pattern synthesis methods like Schelkunoff method are used to produce patterns with nulls in desired directions [111]. However, using such methods does not give perfect control on the location of the main beam. Instead, in this proposed anti-jamming technique, a large database of possible antenna array configurations, each with a certain radiation pattern, is generated. Anti-jamming is performed by searching through the database for the best antenna array configuration that produces a null towards the jammer's location and simultaneously directs the

main beam towards the legitimate transmitter, achieving a high SINR. The large number of antenna elements allows dynamic adaptation of the antenna configuration. The main novelty of this solution is in the proposed anti-jamming technique which is easy to implement, does not require strong computational power, and is completely based on the physical layer. The task of detecting and locating jammers is left for further investigations in the future. Throughout this chapter, the presence of jammers and their locations are assumed to be known. Various methods for performing these tasks exist in the literature such as [115, 116, 117]. The work done in this scenario resulted in the accepted conference paper [118].

5.1.1 System Model

The studied system model is shown in Figure 5.1, where the transmitter equipped with a directive antenna is communicating with a receiver equipped with an 8x8 massive planar antenna array in the presence of a single jammer equipped with a directive antenna similar to the one with the transmitter. The receiver tries to maximize its gain toward the transmitter and place a null toward the jammer simultaneously.

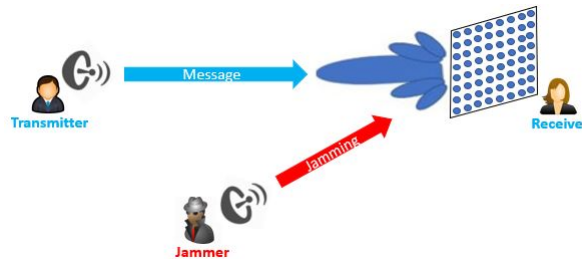


Figure 5.1: Proposed system model.

5.1.2 Generating The Database of Antenna Array Configurations

The receiver is assumed to have an 8x8 massive MIMO planar antenna array as described in section 3.1. All possible combinations of the different types of linear antenna arrays, described in section 3.2, along the x- and y- axes were formed to produce the different antenna array configurations used to generate the database. Although the considered receiver has an 8x8 planar array, the linear sub-arrays considered in the database have different numbers of antenna elements, i.e. not necessarily 8 elements. In these sub-arrays, some of the radiating elements on the sides were considered to be turned off, having zero excitation coefficients. Reducing the number of elements in linear arrays widens their main beam which

is undesirable if the jammer is in close proximity to the legitimate transmitter. However, if the jammer is far away from the transmitter, widening the main beam may not be harmful. When Dolph-Tschebyscheff linear arrays were used, several versions of them were formed each having a different value for the Side-Lobe-Level (SLL) ranging between 10 and 60 dB. Thus, a large database of around 70,000 possible antenna array configurations was created.

5.1.3 Performance Metrics

Before discussing the two proposed searching methods through which the best antenna configuration is chosen from the generated database, the performance metrics used to evaluate the performance of the system are described in this section. In both searching methods, the gain of the receiver's antenna array towards the transmitter and jammer needs to be evaluated as described in section 3.1.3. The SINR is the adopted metric to effectively evaluate the performance of the proposed searching methods when put into practice. Calculating the SINR requires information about the antenna gains, the wireless channel gain, the transmitted power, and the receiver's noise. Table 5.1 lists the parameters used in the upcoming equations.

Table 5.1: Definitions of Anti-jamming Model Parameters

Variable	Description
$P_{T,R}$	Power of signal from legitimate transmitter towards the receiver.
P_J	Power of jamming signal transmitted by the jammer towards the receiver.
$H_{T,R}$	Channel gain between legitimate transmitter and receiver.
$H_{J,R}$	Channel gain between jammer and receiver.
$G_{T,R}$	Gain of the antenna of the legitimate transmitter with its main beam steered in the direction of the receiver (ϕ_R, θ_R)
$G_{R,T}$	Gain of the antenna array of the receiver in the direction of the legitimate transmitter (ϕ_T, θ_T)
$G_{J,R}$	Gain of the antenna of the jammer in the direction of the receiver (ϕ_R, θ_R)
$G_{R,J}$	Gain of the antenna array of the receiver in the direction of the jammer (ϕ_J, θ_J)
σ^2	Noise power

The transmitter, receiver, and jammer are assumed to experience Rayleigh fading independent wireless channels as described in section 3.3.

The SINR, in bits per second per Hertz(bps/Hz), is given by [119]:

$$SINR = \frac{P_T H_{T,R} G_{T,R}(\phi_R, \theta_R) G_{R,T}(\phi_T, \theta_T)}{I_J + \sigma^2} \quad (5.1)$$

Where I_J is the jamming interfering signal sent by the jammer towards the receiver. It is given by:

$$I_J = P_J H_{J,R} G_{J,R}(\phi_R, \theta_R) G_{R,J}(\phi_J, \theta_J) \quad (5.2)$$

In (5.1) and (5.2), when a single omni-directional antenna is used by the transmitter and the jammer, $G_{T,R}$ AND $G_{J,R}$ are set to one in all directions. Otherwise, if the antenna used is directional, then its maximum will be directed towards the location of the receiver.

5.1.4 Searching Methods

After building the database of the antenna array configurations, two searching methods are proposed to search through the database to find the configuration that achieves the best performance at every possible location of the jammer. A look-up table covering the azimuth and elevation space is produced using both methods. Each method has a different criterion for defining a good configuration, as described next.

Deepest Null Searching Method

In the first searching method, searching is done for the array configuration that produces the deepest null at the location of the jammer. After detecting the presence of the jammer and identifying its location, this methods searches through the receiver's gains toward the jammer's location in the database and picks the configuration with the lowest gain value, i.e. deepest null as formulated by:

$$\arg \min_i G_i(\theta_J, \phi_J) \quad (5.3)$$

where $i \in \{1, 2, \dots, 70000\}$ represents the index of the antenna configurations in the database. Note that although the main-lobe of all configurations is directed towards the transmitter, this method is not concerned with maximizing the gain towards the transmitter, rather, it only focuses on nulling the jammer to receive the minimum possible power from its direction.

Max-to-Null Ratio Searching Method

In the second searching method, searching is done for the array configuration that produces the largest difference in dB between the receiver's gain towards the transmitter (i.e. its max) and its gain towards the jammer (i.e. its null). After

the detection of the jammer and specifying its location, this method searches through the database and finds the difference in dB between the gain towards the transmitter and the gain towards the jammer for every receiver antenna configuration in the database. The configuration with the largest difference in dB between the two gains is picked according to the following formulation:

$$\arg \max_i G_i(\theta_T, \phi_T) - G_i(\theta_J, \phi_J) \quad (5.4)$$

where $i \in \{1, 2, \dots, 70000\}$ represents the index of the antenna configuration in the database.

5.1.5 Simulation Results

To simulate the proposed system model, the transmitter, receiver, and jammer are assumed to be located in a suburban area. The wireless channel model considered has an empirical path loss with a pathloss exponent $\gamma = 3.5$ and $\kappa = -38.46\text{dB}$ which is the pathloss constant. Rayleigh fading is considered with parameter b such that $E[b^2] = 1$. In addition to zero-mean log-normal shadowing with standard deviation $\sigma_\psi = 8$ dB. Both the transmitter and jammer are equipped with a single directive antenna with 5dB gain directed towards the receiver. The location of the transmitter is known to the receiver. Thus, its main beam is steered to the direction of the transmitter. The distances separating the isotropic radiating elements along x- and y- axes in the planar antenna array at the receiver are $d_y = 0.5\lambda$ and $d_x = 0.5\lambda$ where λ is the wavelength. The operating frequency is chosen to be 2 GHz. The receiver's thermal noise is set to -174dBm/Hz [120].

The receiver is considered as if it is at the origin of the 3D space. Then, the transmitter is located at $(d_{TR}, \theta_{TR}, \phi_{TR})$ and the jammer is located at $(d_{JR}, \theta_{JR}, \phi_{JR})$ in spherical coordinates, where d_{JR} & d_{TR} represent the corresponding distances of the transmitter and jammer from the receiver, respectively.

Jammer and Transmitter on Same Elevation ($\theta_{TR} = \theta_{JR}$)

In Figure 5.2, the transmitter's location is fixed at $(\theta_{TR}, \phi_{TR}) = (90, 45)$ degree. And the distances from the receiver are assumed to be $d_{TR} = 800$ m and $d_{JR} = 300$ m. The jammer is assumed present in the same plane as the transmitter (i.e. $\theta_{TR} = \theta_{JR}$) and it moves around a circle centered at the receiver, changing its azimuth angle.

Figure 5.2 shows the resulting average SINR in dB from both searching methods versus the jammer's location in the azimuth plane. The performance of both methods is compared with the performance of a receiver equipped with an omni-directional antenna having unity gain. Since the jammer keeps changing its location by moving around a circle centered at the receiver, Monte-Carlo simulations with $N = 10^5$ are performed for the jammer's wireless channel and the

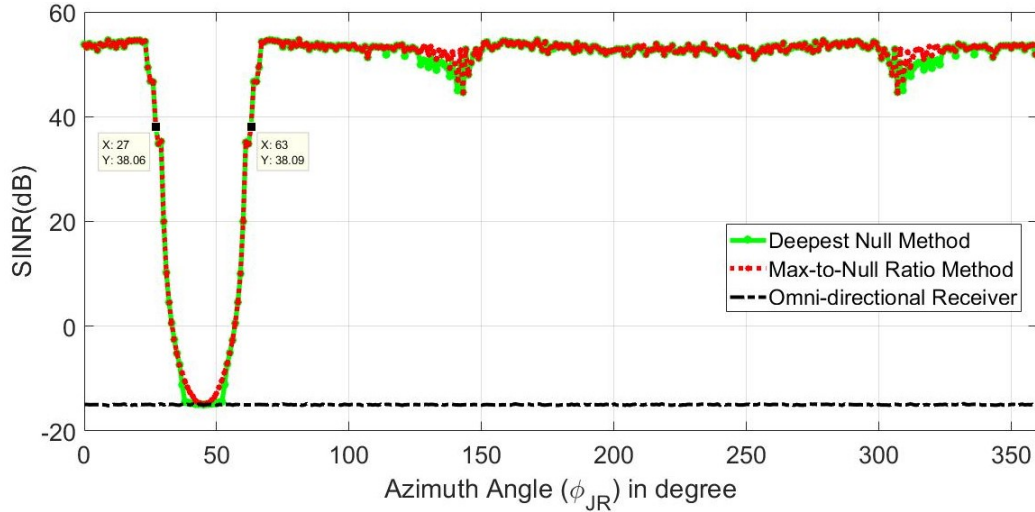


Figure 5.2: Average SINR in dB using both searching methods vs jammer's location in azimuth plane ϕ_{JR} , compared to omni-directional antenna receiver, transmitter at $(\theta_{TR}, \phi_{TR})=(90,45)$

average values for the SINR are calculated. The figure clearly shows the effective anti-jamming performance of the system. The performance of the two searching methods is shown to be very similar to each other and provides an excellent enhancement in the performance of the receiver equipped with an omni-directional antenna. However, Max-to-Null Ratio searching method slightly outperforms the Deepest Null searching method. Note that as long as the jammer is not in close proximity to the transmitter, the achieved SINR of the system is very high, achieving around 55dB, which means that the jammer is unable to disrupt the communication link. While if the jammer moves closer to the transmitter (i.e. within angles $\phi_{JR} = \phi_{TR} \pm 18$ degree, the SINR degrades and drops below 38dB. We start having negative SINR values in the range where $\phi_{JR} = \phi_{TR} \pm 12$ degree.

Figure 5.3 shows the achieved average SINR when the distance between the jammer and the receiver is varied while the azimuth and elevation locations are fixed for the transmitter at $(\theta_{TR}, \phi_{TR})=(90,45)$ degree and the jammer is close to the transmitter at $(\theta_{JR}, \phi_{JR})=(90,65)$ degree. As expected, the achieved SINR improves greatly as the distance between the receiver and the jammer increases. Also, we notice that the performance of the two searching algorithms is almost the same. This is expected based on the results found in Figure 5.2.

Jammer at a Different Elevation Angle Than Transmitter ($\theta_{TR} \neq \theta_{JR}$)

In Figure 5.4, the jammer's elevation angle is varied while fixing its distance from the receiver. The transmitter is located at $(\theta_{TR}, \phi_{TR})=(45,45)$ degree. Figure 5.4 shows the achieved average SINR when the elevation angle of the jammer is

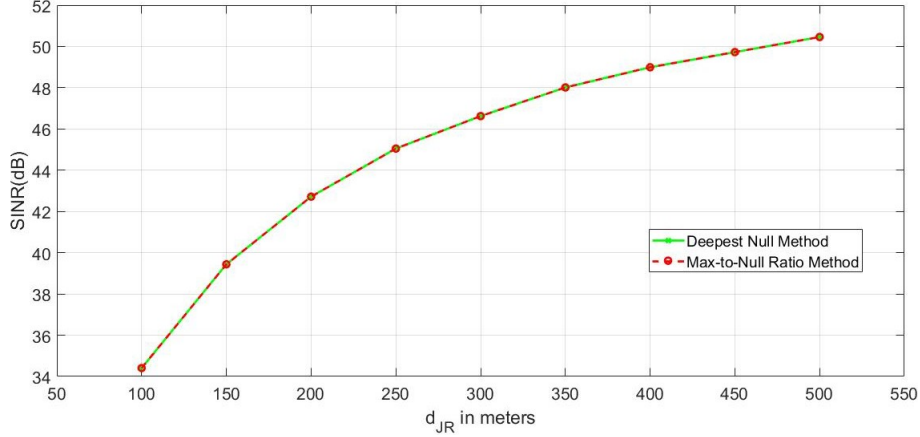


Figure 5.3: Average SINR in dB using both searching methods vs jammer's distance from receiver, transmitter at $(\theta_{TR}, \phi_{TR})=(90,45)$ degree, jammer at $(\theta_{JR}, \phi_{JR})=(90,65)$ degree

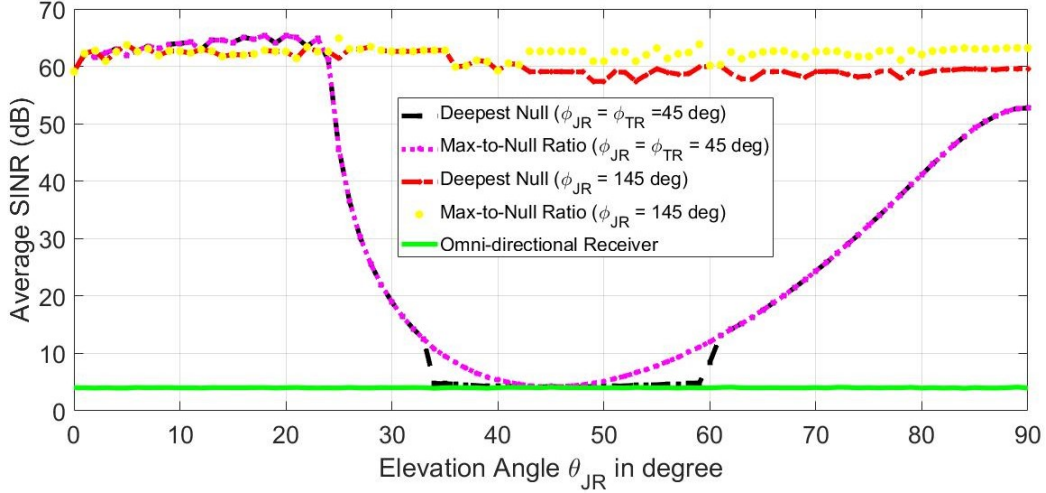


Figure 5.4: Average SINR in dB using both searching methods vs jammer's elevation angle θ_{JR} , transmitter at $(\theta_{TR}, \phi_{TR})=(45,45)$ degree, $\phi_{JR} = 45$ & 145 degree

varied while fixing its azimuth angle. Two values of the azimuth angle of the jammer are considered, $\phi_{JR} = \phi_{TR} = 45$ and $\phi_{JR} = 145$ degree. The anti-jamming performance is compared with the performance of a unity gain omni-directional antenna receiver. The system is totally secure over all elevation planes when the jammer is present at an azimuth angle which is far from the transmitter's azimuth angle. When the jammer and the transmitter are present at the same azimuth angle, system's security is confirmed when the jammer is at an elevation angle of around $\theta_{JR} = \theta_{TR} \pm 25$ degree. In both cases, the Max-to-Null Ratio searching method outperforms the Deepest Null searching method and both methods achieve an acceptable level of secrecy.

Finally, to guarantee accuracy in performance and to prove that the results

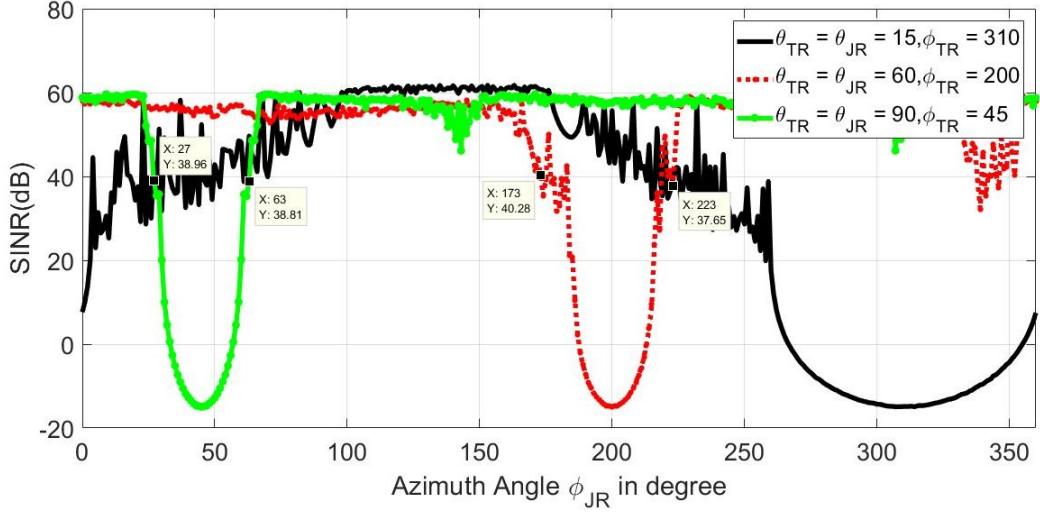


Figure 5.5: Average SINR in dB using Max-to-Null Ratio searching method vs jammer's location in azimuth plane ϕ_{JR} , varying transmitter's location

are not biased to the used transmitter's location i.e. $(\theta_{TR}, \phi_{TR}) = (90, 45)$ degree, two different random locations of the transmitter were chosen, and simulations varying the jammer's azimuth angle while it is located in the same elevation plane as the transmitter were conducted. The studied locations for the transmitter are: $\theta_{TR} = 60, \phi_{TR} = 200$ degree and $\theta_{TR} = 15, \phi_{TR} = 310$ degree. The performance at these locations was compared with the performance when transmitter was at $\theta_{TR} = 90, \phi_{TR} = 45$ degree. Simulations were conducted using the Max-to-Null Ratio searching method alone, since it outperformed the Deepest Null searching method in all previous simulations. The results of the simulations are presented in Figure 5.5. When the transmitter is at $\theta_{TR} = 15, \phi_{TR} = 310$ degree, we note that the jammer must be located at $\phi_{JR} \geq \phi_{TR} \pm 50$ degree so that the system is secure. While when the transmitter is located at $\theta_{TR} = 60, \phi_{TR} = 200$ degree, security is guaranteed if the jammer is located at around $\phi_{JR} \geq \phi_{TR} \pm 25$ degree. And as shown in Figure 5.2, when the transmitter is at $\theta_{TR} = 90, \phi_{TR} = 45$ degree, we note that the jammer must be located at $\phi_{JR} \geq \phi_{TR} \pm 18$ degree in order to secure the communication link. We can conclude from the figure that the proposed anti-jamming technique has a relatively good performance at different locations of the transmitter. Conclusion and proposed future enhancements of the system are described next.

5.2 Machine Learning Based Anti-jamming Technique

5.2.1 Motivation

The proposed look-up table-based anti-jamming technique suffers from multiple issues when it comes to scalability and generalization. In fact, the considered single jammer scenario includes a large number of parameters that, if varied, require performing new computations to build new look-up tables or extend the existing ones. These parameters include: the distance between the jammer and the receiver, the distance between the transmitter and the receiver, the channel gain between the transmitter and the receiver, the location of the transmitter w.r.t. the receiver, the location of the jammer w.r.t. the receiver, and the antenna gain of the transmitter and jammer toward the receiver. Relying on look-up tables require having a stored strategy to combat jamming attacks for every possible value of each of the system's parameters. Next is a quick computation of the required storage space required to store a look-up table containing an anti-jamming strategy for every possible combination of the system's parameters (with simplified assumptions). In fact, if a single jammer scenario is considered, the following are realistic variations of each parameter of the system:

- θ_{TR} & θ_{JR} each takes 90 values (assuming planar antenna radiation is performed only from the top of the array).
- ϕ_{TR} & ϕ_{JR} each takes 360 values to cover the azimuth space.
- d_{TR} & d_{JR} each taking 20 values (This choice is simplified since much more distances could be considered).
- H_{TR} could take 1000 values if Monte-Carlo simulations are considered since this value is a random number resulting from the pathloss wireless channel model including log-normal shadowing and Rayleigh fading.
- G_{TR} & G_{JR} each takes 5 values (simplified assumption).

If all these features are considered, the look-up table would be of size $(1.04976 \times 10^{16}) \times 21$

Storing this data would require more than 783 PB of storage capacity, which is a very huge space. Searching through this dataset every time one of the system's parameters changes would require a long time. Spending a long time searching through the look-up table for the right strategy to combat a jamming attack is incompatible with the critical nature of the anti-jamming operation which requires making quick decisions that are adaptive and vary according to the input parameters from the field. Also, if scenarios of multiple jammers are considered,

the storage space required for the look-up tables would become extremely large. Thus, it can be concluded that the look-up table-based anti-jamming technique is highly difficult to be generalized or scaled to larger systems.

Based on the previous facts, producing a more reliable anti-jamming solution that does not require huge storing capacity or long run-time is a must. The proposed solution must be scalable and must generalize well. With the large amounts of data required, deploying ML and DL algorithms on the system becomes more attractive. Such algorithms do not require data about every possible value of each system's parameter. The only requirement is to have a dataset that is varied enough to truly represent the possible values of each of the system's parameters. The ML/DL model is trained and tested on the dataset even if it is large. After the model is generated, there is no need for the dataset to be stored, and the model performs predictions on new input data instantaneously in real-time and within a second. Thus, the storage space, required to store the look-up tables, and the operation time, required to search through look-up tables whenever a system's parameter is varied, are saved when ML/DL algorithms are deployed. These are the motivations behind using ML/DL algorithms to extend the previous anti-jamming method based on look-up tables.

5.2.2 System Model

The studied scenario in the ML/DL anti-jamming solution is similar to the one considered in the look-up table-based anti-jamming solution which was presented in Figure 5.1. A more detailed drawing of the system model where the system's parameters are indicated is presented next in Figure 5.6.

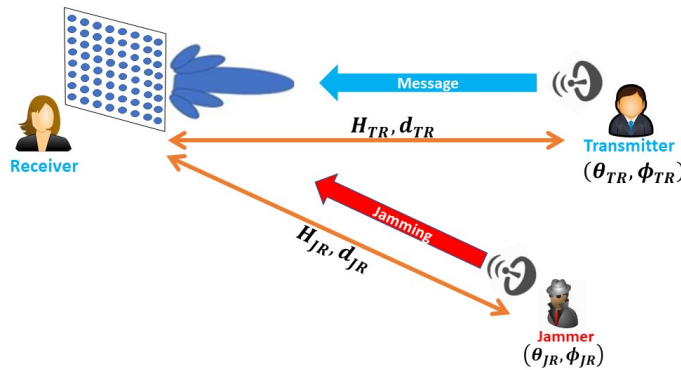


Figure 5.6: Studied scenario with single jammer.

The overall system model of the receiver, where the anti-jamming process is performed, is shown in Figure 5.7. Five out of the nine possible system's parameters mentioned in section 5.2.1 were considered to build the model. The

proposed model is a proof of concept that is compatible with the available computational resources at AUB. Initially, the system model takes information about the location of the transmitter and the jammer, in addition to information about the quality of the channel between the transmitter and the receiver. Namely, the input features to the system are:

- The location of the transmitter both in elevation and azimuth planes (θ_{TR}, ϕ_{TR}).
- The location of the jammer both in elevation and azimuth planes (θ_{JR}, ϕ_{JR}).
- The channel gain between the transmitter and the receiver (H_{TR}).

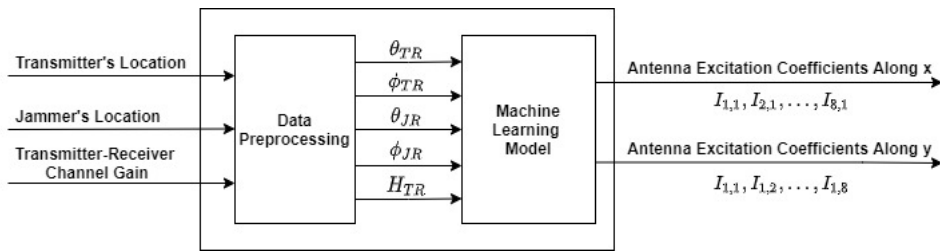


Figure 5.7: System model showing inputs and outputs.

First, a dataset containing training and testing samples is generated. The input data is pre-processed before being fed as inputs to the ML/DL model. Next, the model architecture is trained on the dataset and its performance is validated. Finally, the ML/DL model makes predictions regarding the values of the antenna excitation coefficients of the planar array required to secure the system and combat the jammer. The details of the dataset generation process and the pre-processing operations performed on the dataset are presented in the next sections.

5.2.3 Dataset Generation

The process of building the dataset for the ML/DL model starts by looping over the locations of the transmitter and the jammer (by varying $\theta_{TR}, \phi_{TR}, \theta_{JR}$, and ϕ_{JR}). In every iteration, i.e. at each location of the transmitter and the jammer, a table similar to the one generated in section 5.1.2 is generated. This table includes the receiver's gain towards both the transmitter (G_{RT}) and the jammer (G_{RJ}) resulting from all possible combinations of linear antenna array configurations (Uniform, Binomial, & Dolph-Chebyshev) in an 8x8 massive MIMO planar antenna array deployed at the receiver. In fact, the table consists of more than 70,000 configurations corresponding to the different combinations of linear antenna arrays with different numbers of elements and different side-lobe levels in

the case of Dolph-Chebyshev linear arrays. Also, the excitation coefficients of the antenna elements resulting from each configuration of the planar antenna array are included for every configuration in the table. Although the 8x8 planar antenna array has 64 antenna elements, it is enough to have the values of the excitation coefficients of a linear array of 8 elements along the x-axis, and another one along the y-axis in order to be able to obtain the excitation coefficients of the remaining antenna elements. Assuming m to be the number of elements along the x-axis and n to be the number of elements along the y-axis, the excitation coefficient for an antenna element at position (i, j) is called: $I_{i,j}$, and is found according to the formula:

$$I_{i,j} = I_{1,i} \times I_{j,1}$$

where $I_{1,i}$ is the excitation coefficient of the antenna element at position i in the linear array known along the x-axis. Similarly, $I_{j,1}$ is the excitation coefficient of the antenna element at position j in the linear array known along the y-axis.

After this table is generated, a random value of the wireless channel gain between the transmitter and the receiver (H_{TR}) is generated according to the pathloss wireless channel model including log-normal shadowing and Rayleigh fading presented in equation (3.15). The distance between the transmitter and the receiver (d_{TR}) was fixed to 800m, while the distance between the jammer and the receiver (d_{JR}) was set to 300m. The transmitter and jammer were both assumed to have a single directive antenna directed toward the receiver with gain $G_{TR} = G_{JR} = 1.7dB$. Since the channel gain between the jammer and the receiver is hard to be identified due to the jamming signals the jammer is transmitting, a worst case scenario was considered assuming a good quality of the wireless channel between the jammer and the receiver. 10,000,000 simulations of the wireless channel model were run, and the best achieved channel gain was assumed to be the value of H_{JR} ($H_{JR} = 1.0797 \times 10^{-10}$). The values of these parameters, along with the receiver gains from the produced table, are plugged into equation (5.1) to compute the SINR. Then, the SINR values resulting from each antenna configuration are compared, and the antenna excitation coefficients from the antenna configuration achieving the highest SINR are used as outputs of the system model and put in the dataset. The dataset generated consists of 70,000 samples. Each sample includes five input features and sixteen outputs, where the first eight elements, along the x-axis, were normalized w.r.t. their maximum, and the same thing is applied for the other eight elements along the y-axis.

5.2.4 Deployed Machine Learning Algorithms

Supervised learning algorithms are deployed and their performance on the dataset is compared. The problem is a regression problem with 16 outputs, where each output takes a continuous value. Next, a brief description of the deployed

algorithms is given and the hypothesis model for each algorithm is described.

- **Linear Regression:**

Linear regression is the simplest regression model that could be used to model the relation between certain inputs and outputs. In order for it to achieve a good performance with low error, the inputs and outputs must have some kind of a linear relation at some level. The hypothesis function of linear regression is given in equation (5.5), where θ represents the vector of model's parameters corresponding to the input features, including the bias term, and x represents the input sample. The model tries to learn the model's parameters θ by minimizing a cost function that accounts for the error between predictions and true output values. The adopted cost function is the mean squared error (MSE) function which is shown in equation (5.6). The gradient descent algorithm is used to optimize the cost function and learn the model's parameters.

$$h_{\theta}(x) = \theta_0 + \theta_1 \cdot x \quad (5.5)$$

$$J(\theta_0, \theta_1) = \frac{1}{2m} \sum_{i=1}^m (h_{\theta}(x)^{(i)} - y^{(i)})^2 \quad (5.6)$$

- **Polynomial Regression:**

In order to account for any non-linearity in the relation between the inputs and the outputs, and give a better modeling of the data, non-linear regression models are studied rather than the simple linear regression model. One of the simplest non-linear regression models is the polynomial regression model. The hypothesis of polynomial regression is given in equation (5.7). The same cost function (equation 5.6) of linear regression is applied to polynomial regression. And again, the model's parameters are learned by minimizing the cost function using the gradient descent algorithm.

$$h_{\theta}(x) = \theta_0 + \theta_1 \cdot x + \theta_2 \cdot x^2 + \theta_3 \cdot x^3 \dots \quad (5.7)$$

- **Decision Trees:**

Decision Tree learning is a famous algorithm deployed in ML to perform both tasks of classification and regression. In the case of regression, decision trees represent a non-linear regression algorithm in which the created regression model is obtained by partitioning the dataset into smaller subsets in a recursive manner. Then, a simple prediction model is fitted within each partition [121]. This way, the resulting regression model takes the structure of a tree.

- **Random Forests:**

Random forests algorithm, proposed by Breiman [122], belong to the class of ensemble learning algorithms which include two main methods: **Boosting** [123] and **Bagging** [124]. In this type of learning algorithms, many predictors, e.g. decision trees, are generated and their results are aggregated. Finally, majority vote is taken in order to make predictions in case of classification, and the predictions are averaged in the case of regression. The difference between boosting and bagging is that in boosting algorithms, successive trees depend on the predictions of previous trees and modify their weighting accordingly. While in bagging algorithms, there is no dependency on previous trees and all predictors (trees) are constructed independently using different bootstrap samples of the dataset. Random forests is a bagging algorithm [122] with an additional layer of randomness since every node is split using the best among a subset of predictors, not all of them. Also, these predictors are randomly chosen at that node. This algorithm performs very well when compared to other well known algorithms [125].

- **Artificial Neural Networks:**

The final algorithm tested on the generated dataset is neural networks (NN) since it is one of the most powerful algorithms used to build accurate predictors. Since the dataset generated is of tabular form, the most suitable structure of NN for this type of data is known as Artificial Neural Networks (ANN).

The ANN fully connected structure consists of an input layer, an output layer, and some hidden layers in between. Each layer consists of a number of neurons. The model's parameters are the weights (W) associated with the neurons in the layers. The inputs are linearly multiplied with the weights of the input layer resulting in z as follows:

$$z = Wx \tag{5.8}$$

then non-linearity is added by applying an activation function to z as follows:

$$a = \text{activation}(z) = g(z) \tag{5.9}$$

several activation functions exist such as the sigmoid function, tanh, ReLu, among many others. The model's parameters are learned through forward and backward propagation algorithms. There are several optimizers used in learning the parameters, such as the stochastic gradient descent (SGD) optimizer, and the famous ADAM optimizer. The general hypothesis to make predictions of Neural Networks can be found in equation (5.10).

$$h_{\theta}(x) = g(\theta^{(L-1)T} a^{(L-1)}) = \frac{1}{1 + e^{-(L-1)T a^{(L-1)}}} \quad (5.10)$$

where L is the number of layers.

5.2.5 Data Pre-processing and Experimental Setup

The dataset was generated using Matlab. Then, the studied ML/DL models were coded using Google Colab platform in Python programming language. The ML models were based on Scikit Learn library, while the DL models were based on Tensorflow (Keras). Multiple other libraries were used to manipulate the data and present the results, such as pandas, numpy and matplotlib.

The outliers in the dataset were removed, and the cleaned dataset included 130,634 samples. The dataset was split into training and testing datasets with a ratio of splitting equal to 0.8:0.2. The five different inputs were pre-processed before being fed into the ML/DL models. The input features were all normalized to have zero mean, and scaled to have unit variance.

As mentioned earlier, the measure of performance adopted in this regression problem is the mean squared error (MSE) which is presented next in equation (5.11).

$$error(MSE) = \sum_{t=1}^m \frac{(y_{predicted} - y_{test})^2}{m} \quad (5.11)$$

5.2.6 Experimental Results and Discussion

Models using the five discussed algorithms were built, trained, and tested using the pre-processed dataset. The MSE was calculated for each model on both the training and testing data in order to compare the performance of the models and to check issues of overfitting or underfitting.

First, a simple linear regression model was created. It achieved $MSE_{train} = 0.07066$ and $MSE_{test} = 0.07061$ averaged over the 16 outputs. Generally, the obtained results are acceptable, and since the performance on both training and testing datasets is similar, then we can conclude that the model is generalizing well. However, the performance is still poor and is expected to improve when other models that account for non-linearities in the data are studied.

The second model tested was the polynomial regression model. The order of the polynomial is the tuned hyper-parameter. The model achieved the best performance with order of polynomial $n = 3$, the obtained results were: $MSE_{train} = 0.06786$ and $MSE_{test} = 0.06792$ averaged over the 16 outputs. Which is, as expected, better than linear regression. If the order of the polynomial is further increased, the model starts suffering from overfitting the training data. For example, when the order of polynomial $n = 4$, the obtained results were

$MSE_{train} = 0.0635$ and $MSE_{test} = 0.0722$ averaged over the 16 outputs. And when $n = 5$, the obtained results were $MSE_{train} = 0.0561$ and $MSE_{test} = 5.0815$ averaged over the 16 outputs. These results clearly indicate that as the model is getting more complex, it is overfitting the training data, which explains why the performance on training data is improving while the performance on testing data is becoming worse.

The next model tested was the regression decision tree model. The hyper-parameter tuned in the decision tree model is the maximum depth of the tree. The obtained MSE on both training and testing data was plotted versus the depth of the tree. The results are shown in Figure 5.8.

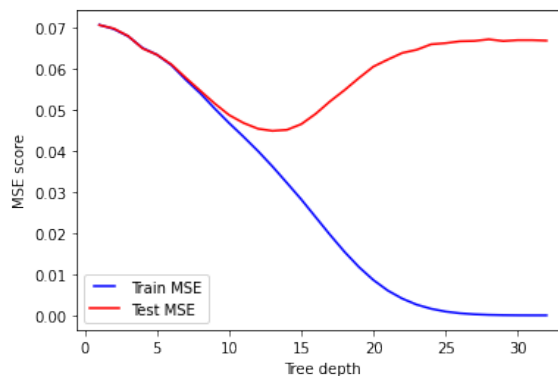


Figure 5.8: MSE score of training and testing data of decision trees vs maximum tree depth.

It is easily noted from Figure 5.8 that as the depth of the tree increases, the gap between the MSE on training data and the MSE on testing data starts to increase, resulting in an overfitting issue at large tree depths. In order to obtain the value of the maximum depth of the tree optimizing the model performance without overfitting the training data, the training data was split into training and validation data using the concept of k-fold cross-validation. Five-fold and ten-fold cross-validation were applied, and grid search was performed over the maximum depth of the tree. The best performance of the decision tree was obtained when the maximum depth of the tree = 13 where the results were: $MSE_{train} = 0.0362$ and $MSE_{test} = 0.0448$ averaged over the 16 outputs.

In order to further enhance the obtained results from the decision tree, random forest regressors with decision tree estimators were tested next. The hyper-parameters tuned were the number of tree estimators and the maximum depth of the trees. Grid search with five-fold cross-validation was done on these two hyper-parameters in order to obtain the best combination of them without overfitting the training data. The optimal model performance was achieved when the parameters were: maximum depth = 19, and number of estimators = 330. These

values resulted in $MSE_{train} = 0.0107$ and $MSE_{test} = 0.035$ averaged over the 16 outputs. This is the best achieved model performance. The achieved MSE on testing data for every output out of the 16 outputs using the chosen random forest regression model is shown in Figure 5.9 and the average value is indicated by the orange line.

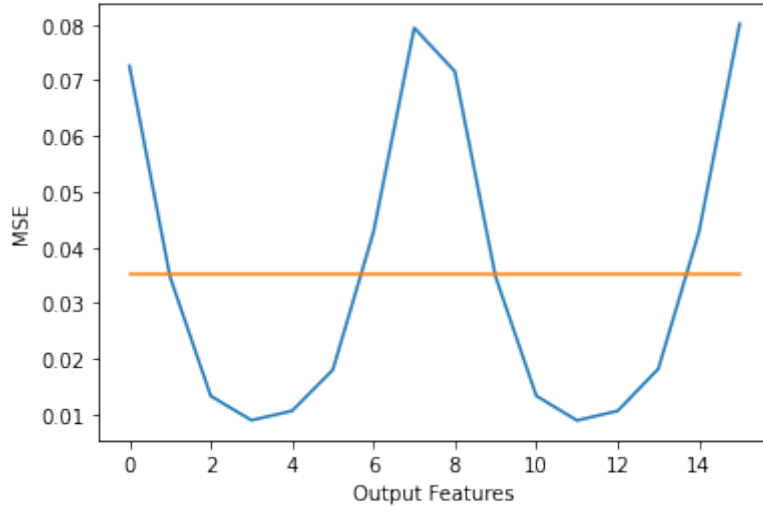


Figure 5.9: MSE score on testing data for every output using random forest regressor

Finally, an ANN model was built. The hyper-parameters of the model that were tuned are:

- The number of layers.
- The number of neurons in each layer.
- The number of epochs through the dataset.
- The optimizer used while training the model.

After performing grid search, tuning the hyper-parameters, with 5-fold cross-validation, the architecture that achieved the lowest error on both training and testing data consists of ten hidden layers, in addition to the input and output layers. The activation function for all layers is the hyperbolic tangent function (tanh). Detailed description of the adopted ANN architecture is given in Figure 5.10.

The performance of the model was evaluated using two optimizers, namely: Stochastic Gradient Descent (SGD) and ADAM optimizers. Figure 5.11 shows the MSE performance of the model with ADAM optimizer versus the number

ANN Architecture
Input Layer (5 neurons)
1 st Hidden Layer (110 neurons)
2 nd Hidden Layer (70 neurons)
3 rd Hidden Layer (50 neurons)
4 th Hidden Layer (50 neurons)
5 th Hidden Layer (50 neurons)
6 th Hidden Layer (50 neurons)
7 th Hidden Layer (50 neurons)
8 th Hidden Layer (50 neurons)
9 th Hidden Layer (50 neurons)
10 th Hidden Layer (50 neurons)
Output Layer (16 neurons)

Figure 5.10: ANN adopted architecture

of training epochs. The MSE performance of the model using SGD optimizer is shown in Figure 5.12 versus the number of training epochs. It can be noticed that the SGD optimizer achieved a better performance than ADAM optimizer. The obtained MSE averaged over the 16 output using the SGD optimizer was $MSE_{train} = 0.0357$ and $MSE_{test} = 0.0362$ which is very close to the performance of the random forest. To conclude, the random forest regressor is the model which achieved the best performance over the generated dataset, and almost a similar performance is achieved by ANNs.

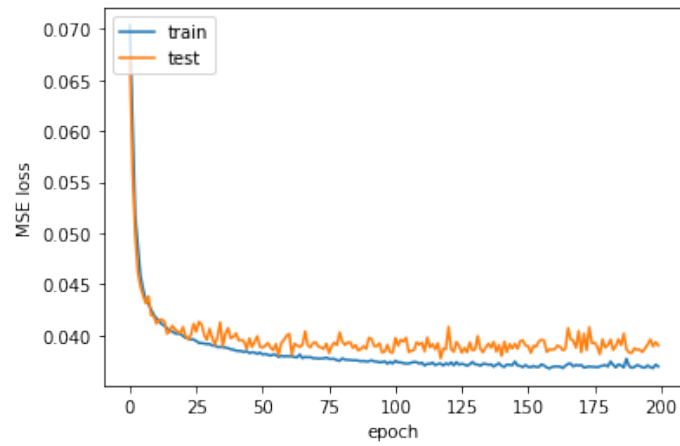


Figure 5.11: MSE using ADAM optimizer vs number of training epochs.

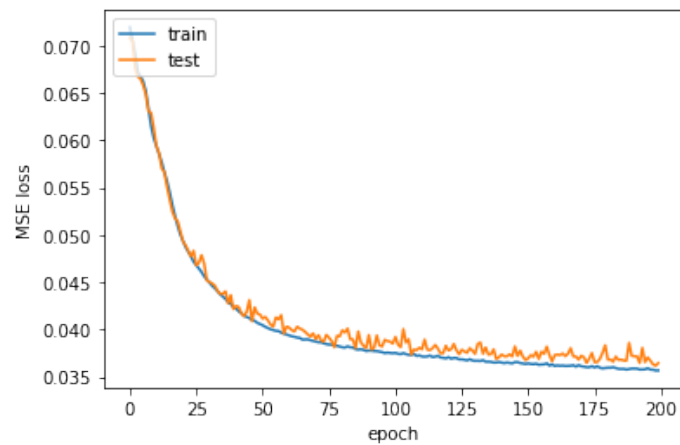


Figure 5.12: MSE using SGD optimizer vs number of training epochs.

Chapter 6

Conclusion and Future Work

This thesis proposes PLS solutions to combat passive eavesdroppers and jammers. Several scenarios are considered and solutions based on the physical layer, and using massive planar antenna arrays are proposed and simulated. Regarding passive eavesdropping, a scenario of a single passive eavesdropper at a known location is considered. The proposed security solution is based on dedicating linear sub-arrays of the the planar array to sending jamming signals toward the eavesdropper, while the rest of the sub-arrays are used for the legitimate communications. Multiple configurations are investigated, and the proposed solutions achieve good secrecy capacity and secure the communication link. After that, two anti-jamming techniques are proposed. The studied scenario consists of a single jammer, at a known location, disrupting the legitimate communication link. The first proposed anti-jamming technique is based on creating a look-up table and searching through it, based on the locations of the transmitter and jammer w.r.t. the receiver, for the antenna configuration that maximizes the receiver's gain toward the transmitter, and simultaneously places a null toward the jammer, thus, achieving a high SINR. Simulation results prove effective anti-jamming performance. However, the model is not scalable, and building a cognitive scalable system model using look-up tables would require huge storing capacity, in addition to spending a long time searching through the table to perform anti-jamming. Thus, the look-up table-based anti-jamming technique is extended in order to overcome the scalability issue. Thus, in the second proposed anti-jamming technique, ML and DL algorithms are deployed to build a scalable anti-jamming model. The dataset on which the ML/DL models are trained and tested was generated based on the look-up table technique. The input features for the proposed models are the locations of the transmitter and the jammer in both azimuth and elevation planes, in addition to the channel gain between the transmitter and the receiver. Five different algorithms were trained and tested on the dataset. The models make predictions of 16 outputs corresponding to the antenna excitation coefficients. The optimal performance, achieving the minimum MSE on the testing data without overfitting the training data, was achieved using

the random forest regressor with decision tree estimators ($MSE = 0.0351$). Also, a very similar performance was achieved using ANNs. Thus, a robust, cognitive, scalable, and efficient anti-jamming system was built.

Because of the interesting results achieved by advanced DL models in fields like computer vision and others, it is expected that a better anti-jamming performance with lower MSE can be achieved by applying advanced DL models. This is part of the future work on this model. Also, based on the proposed ML/DL anti-jamming models, an idea for localizing the single jammer and perform anti-jamming is proposed and left for further investigation in the future. The proposed method is as follows: the receiver chooses a random location for the jammer, and inputs it along with the location of the transmitter and the channel gain between the transmitter and the receiver to the built ML model. The ML model will predict the required antenna excitation coefficients in order to maximize the gain toward the transmitter and to put a null toward the chosen location of the jammer, achieving a high SINR. The receiver keeps track of the achieved SINR, if it is not satisfying, the assumed location of the jammer is changed, and the resulting SINR is checked. If a jammer is present in the system, at an unknown location, the achieved SINR will degrade dramatically. In this case, the receiver will start tuning the assumed location of the jammer, and keep checking the achieved SINR. When the achieved SINR increases again, it means that either the jammer stopped sending jamming signals, or that the assumed location of the jammer is correct. Thus, the model becomes cognitive in terms of detecting the jammer's location, and performing anti-jamming to secure the communication link. Further investigations in the future include increasing the size of the dataset, building ML/DL models with a larger number of input features. Finally, scenarios of multiple jammers will be investigated.

Regarding combating eavesdroppers, the case of multiple passive eavesdroppers at unknown locations will be investigated in the future. An idea combining both cryptographic and non-cryptographic physical layer solutions is proposed for future work. The proposed approach is as follows: The transmitter applies beam-forming techniques to maximize the gain toward the legitimate receiver. Each antenna element is considered to have an independent wireless channel. Thus, each single antenna element from the transmitter communicates with a single antenna element from the receiver. Here comes the cryptographic security solution which is necessary in case the eavesdropper receives some of the legitimate transmitted data. This solution is based on agreement between the transmitter and the receiver on a dynamic secret key obtained from the wireless channels since each antenna has its independent wireless channel. In fact, the transmitter and receiver may specify a threshold to which the channel gain of each wireless channel is compared. If the channel gain is greater than the threshold, then it is encoded as a 1, while if it is below the threshold, then it is encoded as a 0. The quality of the different wireless channels and their gains vary with time. Thus, the obtained key is dynamic and provides security to the system since it will

be difficult to the eavesdropper to decode the legitimate transmitted message. This way, even if the passive eavesdropper is present in close proximity of the legitimate receiver, it will be difficult to correctly understand the signals that it is receiving. Further investigations of this solution are left for future work.

References

- [1] S. Talwar, D. Choudhury, K. Dimou, E. Aryafar, B. Bangerter, and K. Stewart, “Enabling technologies and architectures for 5g wireless,” in *2014 IEEE MTT-S International Microwave Symposium (IMS2014)*, pp. 1–4, June 2014.
- [2] W. Saad, M. Bennis, and M. Chen, “A vision of 6g wireless systems: Applications, trends, technologies, and open research problems,” *IEEE Network*, pp. 1–9, 2019.
- [3] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, “A vision of iot: Applications, challenges, and opportunities with china perspective,” *IEEE Internet of Things Journal*, vol. 1, pp. 349–359, Aug 2014.
- [4] X. Zhang, F. Labeau, Y. Liang, and J. Fang, “Compressive sensing-based multiuser detection via iterative reweighed approach in m2m communications,” *IEEE Wireless Communications Letters*, vol. 7, pp. 764–767, Oct 2018.
- [5] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, “Five disruptive technology directions for 5g,” *IEEE Communications Magazine*, vol. 52, pp. 74–80, February 2014.
- [6] B.-L. Chen, S.-C. Huang, Y.-C. Luo, Y.-C. Chung, and J. Chou, “A dynamic module deployment framework for m2m platforms,” in *2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2)*, pp. 194–200, IEEE, 2017.
- [7] J. Manyika, M. Chui, R. D. J. Bughin, and, P. Bisson, and A. Marrs, “Disruptive technologies: Advances that will transform life, business, and the global economy,” in *McKinsey Glob. Inst. San Francisco, CA, USA*, vol. 180, McKinsey, May 2013.
- [8] D. E. O’Leary, “Artificial intelligence and big data,” *IEEE Intelligent Systems*, vol. 28, pp. 96–99, March 2013.

- [9] D. Kapetanovic, G. Zheng, and F. Rusek, “Physical layer security for massive mimo: An overview on passive eavesdropping and active attacks,” *IEEE Communications Magazine*, vol. 53, pp. 21–27, June 2015.
- [10] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” *Proceedings of the IEEE*, vol. 104, pp. 1727–1765, Sep. 2016.
- [11] J. D. Day and H. Zimmermann, “The osi reference model,” *Proceedings of the IEEE*, vol. 71, pp. 1334–1340, Dec 1983.
- [12] Y. Liu, H. Chen, and L. Wang, “Physical layer security for next generation wireless networks: Theories, technologies, and challenges,” *IEEE Communications Surveys Tutorials*, vol. 19, pp. 347–376, Firstquarter 2017.
- [13] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, “A survey of physical layer security techniques for 5g wireless networks and challenges ahead,” *IEEE Journal on Selected Areas in Communications*, vol. 36, pp. 679–695, April 2018.
- [14] D. Wang, B. Bai, W. Zhao, and Z. Han, “A survey of optimization approaches for wireless physical layer security,” *IEEE Communications Surveys Tutorials*, vol. 21, pp. 1878–1911, Secondquarter 2019.
- [15] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Upper Saddle River, NJ, USA: Prentice Hall Press, 6th ed., 2013.
- [16] Z. Zhang, D. Guo, B. Zhang, and J. Yuan, “Research on physical layer security technology of multi-antenna system,” in *2017 First International Conference on Electronics Instrumentation Information Systems (EIIS)*, pp. 1–4, June 2017.
- [17] F. Huo and G. Gong, “A new efficient physical layer ofdm encryption scheme,” in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pp. 1024–1032, April 2014.
- [18] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct 1975.
- [19] L. H. Ozarow and A. D. Wyner, “Wire-tap channel ii,” *AT T Bell Laboratories Technical Journal*, vol. 63, pp. 2135–2157, Dec 1984.
- [20] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, “A survey on OFDM physical layer security,” *Physical Communication*, vol. 32, pp. 1 – 30, 2019.

- [21] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, “A survey of physical layer security techniques for 5g wireless networks and challenges ahead,” *IEEE Journal on Selected Areas in Communications*, vol. 36, pp. 679–695, April 2018.
- [22] A. F. Skarmeta, J. L. Hernández-Ramos, and M. V. Moreno, “A decentralized approach for security and privacy challenges in the internet of things,” in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pp. 67–72, March 2014.
- [23] K. Zhang, X. Liang, R. Lu, and X. Shen, “Sybil attacks and their defenses in the internet of things,” *IEEE Internet of Things Journal*, vol. 1, pp. 372–383, Oct 2014.
- [24] A. Mukherjee, “Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints,” *Proceedings of the IEEE*, vol. 103, pp. 1747–1761, Oct 2015.
- [25] L. Wang, J. Liu, M. Chen, G. Gui, and H. Sari, “Optimization-based access assignment scheme for physical-layer security in d2d communications underlying a cellular network,” *IEEE Transactions on Vehicular Technology*, vol. 67, pp. 5766–5777, July 2018.
- [26] O. Nait Hamoud, T. Kenaza, and Y. Challal, “Security in device-to-device communications: a survey,” *IET Networks*, vol. 7, no. 1, pp. 14–22, 2018.
- [27] Y. Zhang, J. Zhang, and H. Yu, “Physically securing energy-based massive mimo mac via joint alignment of multi-user constellations and artificial noise,” *IEEE Journal on Selected Areas in Communications*, vol. 36, pp. 829–844, April 2018.
- [28] F. Zhu, F. Gao, H. Lin, S. Jin, J. Zhao, and G. Qian, “Robust beamforming for physical layer security in bdma massive mimo,” *IEEE Journal on Selected Areas in Communications*, vol. 36, pp. 775–787, April 2018.
- [29] S. Tomasin, “Analysis of channel-based user authentication by key-less and key-based approaches,” *IEEE Transactions on Wireless Communications*, vol. 17, pp. 5700–5712, Sep. 2018.
- [30] Y. Dang, Y. Chen, H. Wu, Y. Shen, and X. Jiang, “Physical layer authentication and identification in wireless network via the locations of surrounding noise sources,” in *2017 International Conference on Networking and Network Applications (NaNA)*, pp. 30–35, Oct 2017.
- [31] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, “Physical layer security for the internet of things: Authentication and key generation,” *IEEE Wireless Communications*, pp. 1–7, 2019.

- [32] J. Si, Z. Li, J. Cheng, and C. Zhong, “Secrecy performance of multi-antenna wiretap channels with diversity combining over correlated rayleigh fading channels,” *IEEE Transactions on Wireless Communications*, vol. 18, no. 1, pp. 444–458, 2019.
- [33] G. Zheng, L. Choo, and K. Wong, “Optimal cooperative jamming to enhance physical layer security using relays,” *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, 2011.
- [34] J. Huang and A. L. Swindlehurst, “Robust secure transmission in mimo channels based on worst-case optimization,” *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1696–1707, 2012.
- [35] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, “Joint relay and jammer selection for secure two-way relay networks,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 310–320, 2012.
- [36] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, “Secrecy rate optimizations for a mimo secrecy channel with a cooperative jammer,” *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, pp. 1833–1847, 2015.
- [37] J. de Dieu Mutangana and R. Tandon, “Blind mimo cooperative jamming: Secrecy via isi heterogeneity without csit,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 447–461, 2020.
- [38] T. Yang, R. Zhang, X. Cheng, and L. Yang, “Secure massive mimo under imperfect csi: Performance analysis and channel prediction,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1610–1623, 2019.
- [39] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.
- [40] S. Liu, Y. Hong, and E. Viterbo, “Practical secrecy using artificial noise,” *IEEE Communications Letters*, vol. 17, no. 7, pp. 1483–1486, 2013.
- [41] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, and R. Liao, “Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 3, pp. 2108–2117, 2018.
- [42] W. Li, M. Ghogho, B. Chen, and C. Xiong, “Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis,” *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628–1631, 2012.

- [43] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, “Improving physical layer secrecy using full-duplex jamming receivers,” *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, 2013.
- [44] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, “Application of full-duplex wireless technique into secure mimo communication: Achievable secrecy rate based optimization,” *IEEE Signal Processing Letters*, vol. 21, no. 7, pp. 804–808, 2014.
- [45] R. Ma, S. Yang, M. Du, H. Wu, and J. Ou, “Improving physical layer security jointly using full-duplex jamming receiver and multi-antenna jammer in wireless networks,” *IET Communications*, vol. 13, no. 10, pp. 1530–1536, 2019.
- [46] J. M. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. N. Nkouatchah, and U. S. Dias, “Transmit antenna selection in secure mimo systems over $\alpha - \mu$ fading channels,” *IEEE Transactions on Communications*, vol. 67, no. 9, pp. 6483–6498, 2019.
- [47] H. Li, J. Cheng, Z. Wang, and H. Wang, “Joint antenna selection and power allocation for an energy-efficient massive mimo system,” *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 257–260, 2019.
- [48] J. Chen, S. Chen, Y. Qi, and S. Fu, “Intelligent massive mimo antenna selection using monte carlo tree search,” *IEEE Transactions on Signal Processing*, vol. 67, no. 20, pp. 5380–5390, 2019.
- [49] A. E. Spezio, “Electronic warfare systems,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 50, no. 3, pp. 633–644, 2002.
- [50] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, “Denial of service attacks in wireless networks: The case of jammers,” *IEEE Communications Surveys Tutorials*, vol. 13, pp. 245–257, Second 2011.
- [51] G. X. Gao, M. Sgammini, M. Lu, and N. Kubo, “Protecting gns receivers from jamming and interference,” *Proceedings of the IEEE*, vol. 104, pp. 1327–1338, June 2016.
- [52] D. Borio, F. Dovis, H. Kuusniemi, and L. Lo Presti, “Impact and detection of gns jammers on consumer grade satellite navigation receivers,” *Proceedings of the IEEE*, vol. 104, pp. 1233–1245, June 2016.
- [53] A. Purwar, D. Joshi, and V. K. Chaubey, “Gps signal jamming and anti-jamming strategy — a theoretical analysis,” in *2016 IEEE Annual India Conference (INDICON)*, pp. 1–6, Dec 2016.

- [54] Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, "Securing consumer iot in the smart home: Architecture, challenges, and countermeasures," *IEEE Wireless Communications*, vol. 25, pp. 53–59, December 2018.
- [55] A. Kott, A. Swami, and B. J. West, "The internet of battle things," *Computer*, vol. 49, pp. 70–75, Dec 2016.
- [56] A. K. Maini, *Electronic Warfare*, pp. 475–554. Wiley, 2018.
- [57] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pp. 46–57, 2005.
- [58] A. Mpitiopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE Communications Surveys Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.
- [59] T. T. Do, H. Q. Ngo, T. Q. Duong, T. J. Oechtering, and M. Skoglund, "Massive mimo pilot retransmission strategies for robustification against jamming," *IEEE Wireless Communications Letters*, vol. 6, no. 1, pp. 58–61, 2017.
- [60] A. J. Viterbi, *CDMA: Principles of Spread Spectrum Communication*. Redwood City, CA, USA: Addison Wesley Longman Publishing Co., Inc., 1995.
- [61] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys Tutorials*, vol. 19, pp. 1027–1053, Secondquarter 2017.
- [62] Q. Liu, M. Li, X. Kong, and N. Zhao, "Disrupting mimo communications with optimal jamming signal design," *IEEE Transactions on Wireless Communications*, vol. 14, no. 10, pp. 5313–5325, 2015.
- [63] P. Wang, Y. Wang, E. Cetin, A. G. Dempster, and S. Wu, "Gnss jamming mitigation using adaptive-partitioned subspace projection technique," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, pp. 343–355, Feb 2019.
- [64] Y. D. Zhang and M. G. Amin, "Anti-jamming gps receiver with reduced phase distortions," *IEEE Signal Processing Letters*, vol. 19, pp. 635–638, Oct 2012.
- [65] M. Li, A. G. Dempster, A. T. Balaei, C. Rizos, and F. Wang, "Switchable beam steering/null steering algorithm for cw interference mitigation in gps c/a code receivers," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 47, pp. 1564–1579, July 2011.

- [66] F. Chen, J. Nie, S. Ni, Z. Li, and F. Wang, “Combined algorithm for interference suppression and signal acquisition in gnss receivers,” *Electronics Letters*, vol. 53, no. 4, pp. 274–275, 2017.
- [67] S. Sciancalepore and R. Di Pietro, “Bittransfer: Mitigating reactive jamming in electronic warfare scenarios,” *IEEE Access*, vol. 7, pp. 156175–156190, 2019.
- [68] S. Lim, S. Han, J. Lee, Y. Eun, and J. Choi, “Decoy signal based strategic beamforming against high-power reactive jamming,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 10054–10058, 2018.
- [69] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor, and M. Street, “Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead,” *IEEE Communications Surveys Tutorials*, vol. 14, no. 2, pp. 355–379, 2012.
- [70] E. Björnson, J. Hoydis, and L. Sanguinetti, *Massive MIMO Networks: Spectral, Energy, and Hardware Efficiency*. now, 2017.
- [71] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, “Massive mimo for next generation wireless systems,” *IEEE Communications Magazine*, vol. 52, pp. 186–195, February 2014.
- [72] M. Rao, A. Kazerouni, and O. Aryan, “Precoding schemes for mimo downlink transmission,” *Stanford University, Stanford, CA, EE360 Paper Summary*, 2007.
- [73] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, “An overview of massive mimo: Benefits and challenges,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, pp. 742–758, Oct 2014.
- [74] M. A. Sedaghat and R. R. Mueller, “Large system analysis of low-cost mimo transmitters,” in *WSA 2013; 17th International ITG Workshop on Smart Antennas*, pp. 1–4, March 2013.
- [75] V. Venkateswaran and A. van der Veen, “Analog beamforming in mimo communications with phase shift networks and online channel estimation,” *IEEE Transactions on Signal Processing*, vol. 58, pp. 4131–4143, Aug 2010.
- [76] T. E. Bogale and L. B. Le, “Beamforming for multiuser massive mimo systems: Digital versus hybrid analog-digital,” in *2014 IEEE Global Communications Conference*, pp. 4066–4071, Dec 2014.

- [77] Z. C. Phyo and A. Taparugssanagorn, “Hybrid analog-digital downlink beamforming for massive mimo system with uniform and non-uniform linear arrays,” in *2016 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pp. 1–6, June 2016.
- [78] D. Kapetanovic, A. Al-Nahari, A. Stojanovic, and F. Rusek, “Detection of active eavesdroppers in massive mimo,” in *2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*, pp. 585–589, Sep. 2014.
- [79] E. Yaacoub, M. Husseini, and H. Ghaziri, “An overview of research topics and challenges for 5g massive mimo antennas,” in *2016 IEEE Middle East Conference on Antennas and Propagation (MECAP)*, pp. 1–4, Sep. 2016.
- [80] E. Yaacoub, M. Al-Husseini, A. Chehab, K. Abualsaud, T. Khattab, and M. Guizani, “3d beamforming with massive cylindrical arrays for physical layer secure data transmission,” *IEEE Communications Letters*, vol. 23, pp. 830–833, May 2019.
- [81] E. Yaacoub, “On the use of massive cylindrical antenna arrays for physical layer security,” in *MILCOM 2016 - 2016 IEEE Military Communications Conference*, pp. 198–203, Nov 2016.
- [82] L. Mucchi, F. Nizzi, T. Pecorella, R. Fantacci, and F. Esposito, “Benefits of physical layer security to cryptography: Tradeoff and applications,” in *2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 1–3, June 2019.
- [83] S. Wang, W. Li, and J. Lei, “Physical-layer encryption in massive mimo systems with spatial modulation,” *China Communications*, vol. 15, no. 10, pp. 159–171, 2018.
- [84] H. Taha and E. Alsusa, “Secret key establishment technique using channel state information driven phase randomisation in multiple-input multiple-output orthogonal frequency division multiplexing,” *IET Information Security*, vol. 11, no. 1, pp. 1–7, 2017.
- [85] S. Liu, Y. Hong, and E. Viterbo, “Unshared secret key cryptography,” *IEEE Transactions on Wireless Communications*, vol. 13, no. 12, pp. 6670–6683, 2014.
- [86] M. Chen, U. Challita, W. Saad, C. Yin, and M. Debbah, “Machine learning for wireless networks with artificial intelligence: A tutorial on neural networks,” *ArXiv*, vol. abs/1710.02913, 2017.

- [87] S. Morisawa, K. Nishimori, F. Muramatsu, R. Taniguchi, T. Mitsui, and T. Hiraguri, “Experimental testbed for massive mimo at 2.4/5.1/19.5 ghz bands,” in *2017 IEEE Conference on Antenna Measurements Applications (CAMA)*, pp. 288–290, 2017.
- [88] S. Sharma, N. Gupta, and V. Ashok Bohara, “Ofdma-based device-to-device communication frameworks: Testbed deployment and measurement results,” *IEEE Access*, vol. 6, pp. 12019–12030, 2018.
- [89] J. Ferber, *Multi-Agent Systems: An Introduction to Distributed Artificial Intelligence*. USA: Addison-Wesley Longman Publishing Co., Inc., 1st ed., 1999.
- [90] T. Segaran, *Programming Collective Intelligence: Building Smart Web 2.0 Applications*. Beijing: O’Reilly, 2007.
- [91] B. YEGNANARAYANA, *ARTIFICIAL NEURAL NETWORKS*. PHI Learning, 2009.
- [92] M. Chen, U. Challita, W. Saad, C. Yin, and M. Debbah, “Artificial neural networks-based machine learning for wireless networks: A tutorial,” *IEEE Communications Surveys Tutorials*, vol. 21, no. 4, pp. 3039–3071, 2019.
- [93] M. I. AlHajri, N. T. Ali, and R. M. Shubair, “Classification of indoor environments for iot applications: A machine learning approach,” *IEEE Antennas and Wireless Propagation Letters*, vol. 17, no. 12, pp. 2164–2168, 2018.
- [94] B. Liu, H. Aliakbarian, Z. Ma, G. A. E. Vandenbosch, G. Gielen, and P. Excell, “An efficient method for antenna design optimization based on evolutionary computation and machine learning techniques,” *IEEE Transactions on Antennas and Propagation*, vol. 62, no. 1, pp. 7–18, 2014.
- [95] Z. Wang, S. Fang, Q. Wang, and H. Liu, “An ann-based synthesis model for the single-feed circularly-polarized square microstrip antenna with truncated corners,” *IEEE Transactions on Antennas and Propagation*, vol. 60, no. 12, pp. 5989–5992, 2012.
- [96] C. Antón-Haro and X. Mestre, “Learning and data-driven beam selection for mmwave communications: An angle of arrival-based approach,” *IEEE Access*, vol. 7, pp. 20404–20415, 2019.
- [97] J. Joung, “Machine learning-based antenna selection in wireless communications,” *IEEE Communications Letters*, vol. 20, no. 11, pp. 2241–2244, 2016.

- [98] D. He, C. Liu, T. Q. S. Quek, and H. Wang, “Transmit antenna selection in mimo wiretap channels: A machine learning approach,” *IEEE Wireless Communications Letters*, vol. 7, no. 4, pp. 634–637, 2018.
- [99] S. Gecgel, C. Goztepe, and G. Karabulut Kurt, “Transmit antenna selection for large-scale mimo gsm with machine learning,” *IEEE Wireless Communications Letters*, vol. 9, no. 1, pp. 113–116, 2020.
- [100] Y. Hu, L. Li, J. Yin, H. Zhang, W. Liang, A. Gao, and Z. Han, “Optimal transmit antenna selection strategy for mimo wiretap channel based on deep reinforcement learning,” in *2018 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 803–807, 2018.
- [101] K. Youssef, L. Bouchard, K. Haigh, J. Silovsky, B. Thapa, and C. V. Valk, “Machine learning approach to rf transmitter identification,” *IEEE Journal of Radio Frequency Identification*, vol. 2, no. 4, pp. 197–205, 2018.
- [102] H. Wang, Z. Wu, S. Ma, S. Lu, H. Zhang, G. Ding, and S. Li, “Deep learning for signal demodulation in physical layer wireless communications: Prototype platform, open dataset, and analytics,” *IEEE Access*, vol. 7, pp. 30792–30801, 2019.
- [103] U. Challita, A. Ferdowsi, M. Chen, and W. Saad, “Machine learning for wireless connectivity and security of cellular-connected uavs,” *IEEE Wireless Communications*, vol. 26, no. 1, pp. 28–35, 2019.
- [104] A. Alkhateeb, S. Alex, P. Varkey, Y. Li, Q. Qu, and D. Tujkovic, “Deep learning coordinated beamforming for highly-mobile millimeter wave systems,” *IEEE Access*, vol. 6, pp. 37328–37348, 2018.
- [105] P. S. Bithas, E. T. Michailidis, N. Nomikos, D. Vouyioukas, and A. G. Kanatas, “A survey on machine-learning techniques for uav-based communications,” *Sensors*, vol. 19, p. 5170, Nov 2019.
- [106] T. Erpek, Y. E. Sagduyu, and Y. Shi, “Deep learning for launching and mitigating wireless jamming attacks,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 1, pp. 2–14, 2019.
- [107] C. Clancy, J. Hecker, E. Stuntebeck, and T. O’Shea, “Applications of machine learning to cognitive radio networks,” *IEEE Wireless Communications*, vol. 14, no. 4, pp. 47–52, 2007.
- [108] K. M. Thilina, K. W. Choi, N. Saquib, and E. Hossain, “Machine learning techniques for cooperative spectrum sensing in cognitive radio networks,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 11, pp. 2209–2221, 2013.

- [109] S. Riyaz, K. Sankhe, S. Ioannidis, and K. Chowdhury, “Deep learning convolutional neural networks for radio identification,” *IEEE Communications Magazine*, vol. 56, no. 9, pp. 146–152, 2018.
- [110] S. Kumar, K. Singh, S. Kumar, O. Kaiwartya, Y. Cao, and H. Zhou, “Delimitated anti jammer scheme for internet of vehicle: Machine learning based security approach,” *IEEE Access*, vol. 7, pp. 113311–113323, 2019.
- [111] C. A. Balanis, *Antenna Theory, Analysis and Design*. John Wiley and Sons, 2016.
- [112] S. J. Orfanidis, “Electromagnetic waves and antennas,” 2002.
- [113] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.
- [114] M. Chehimi, R. A. A. Matar, E. Yaacoub, A. Chehab, and H. Noura, “Massive planar antenna arrays for physical layer security,” in *2019 Fourth International Conference on Advances in Computational Tools for Engineering Applications (ACTEA)*, pp. 1–6, July 2019.
- [115] J. Wang, P. Urriza, Y. Han, and D. Cabric, “Weighted centroid localization algorithm: Theoretical analysis and distributed implementation,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3403–3413, 2011.
- [116] X. Wang, M. Amin, F. Ahmad, and E. Aboutanios, “Interference doa estimation and suppression for gnss receivers using fully augmentable arrays,” *IET Radar, Sonar Navigation*, vol. 11, no. 3, pp. 474–480, 2017.
- [117] M. G. Amin, X. Wang, Y. D. Zhang, F. Ahmad, and E. Aboutanios, “Sparse arrays and sampling for interference mitigation and doa estimation in gnss,” *Proceedings of the IEEE*, vol. 104, pp. 1302–1317, June 2016.
- [118] M. Chehimi, E. Yaacoub, A. Chehab, and M. Al-Husseini, “Physical layer anti-jamming technique using massive planar antenna arrays,” in *IWCMC 2020 Security Symposium (IWCMC 2020 Security Symp)*, (Limassol, Cyprus), June 2020.
- [119] B. Wang, Y. Chang, and D. Yang, “On the sinr in massive mimo networks with mmse receivers,” *IEEE Communications Letters*, vol. 18, pp. 1979–1982, Nov 2014.
- [120] C. D’Andrea, A. Garcia-Rodriguez, G. Geraci, L. G. Giordano, and S. Buzzi, “Cell-free massive mimo for uav communications,” in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, May 2019.

- [121] W.-Y. Loh, “Classification and regression trees,” *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 1, no. 1, pp. 14–23, 2011.
- [122] L. Breiman, “Random forests,” *Mach. Learn.*, vol. 45, p. 5–32, Oct. 2001.
- [123] R. E. Schapire, Y. Freund, P. Bartlett, and W. S. Lee, “Boosting the margin: a new explanation for the effectiveness of voting methods,” *Ann. Statist.*, vol. 26, pp. 1651–1686, 10 1998.
- [124] L. Breiman, “Bagging predictors,” *Mach. Learn.*, vol. 24, p. 123–140, Aug. 1996.
- [125] A. Liaw, M. Wiener, *et al.*, “Classification and regression by randomforest,” *R news*, vol. 2, no. 3, pp. 18–22, 2002.