Secure Multi-Beam Satellite Systems using Adaptive Beamforming for 6G Communications

Yidnekachew Solomon Haile

A Thesis Submitted to

The Department of Electronics and Communication Engineering

School of Electrical and Computing Engineering

Presented in Partial Fulfillment of the Requirement for the Degree of Master's in Electronics and Communication Engineering(Communication Engineering)

Office of Graduate Studies

Adama Science and Technology University

June, 2022

Adama, Ethiopia

Secure Multi-Beam Satellite Systems using Adaptive Beamforming for 6G Communications

Yidnekachew Solomon Haile

Major Advisor: Dr. Rajaveerappa Devadas (PhD)

Co-Advisor: Mr. Bayisa Taye Mulatu

A Thesis Submitted to

The Department of Electronics and Communication Engineering

School of Electrical and Computing Engineering

Presented in Partial Fulfillment of the Requirement for the Degree of Master’s in Electronics and Communication Engineering(Communication Engineering

Office of Graduate Studies

Adama Science and Technology University

June, 2022

Adama, Ethiopia

APPROVAL PAGE FOR M.Sc THESIS

We, the advisors of the thesis entitled "**Secure Multi-Beam Satellite Systems using Adaptive Beamforming for 6G Communications**" and developed by **Yidnekachew Solomon Haile**, hereby certify that the recommendation and suggestions made by the board of examiners are appropriately incorporated into the final version of the thesis.

______________________	____________	____________
Major Advisor	Signature	Date
______________________	____________	____________
Co-advisor	Signature	Date

We, the undersigned, members of the Board of Examiners of the thesis by **Yidnekachew Solomon Haile** have read and evaluated the thesis entitled "**Secure Multi-Beam Satellite Systems using Adaptive Beamforming for 6G Communications**" and examined the candidate during open defense. This is, therefore, to certify that the thesis is accepted for partial fulfillment of the requirement of the degree of **Master of Science in Communication Engineering**.

______________________	____________	____________
Chairperson	Signature	Date
______________________	____________	____________
Internal Examiner	Signature	Date
______________________	____________	____________
External Examiner	Signature	Date

Finally, approval and acceptance of the thesis is contingent upon submission of its final copy to the Office of Postgraduate Studies (OPGS) through the Department Graduate Council (DGC) and School Graduate Committee (SGC).

______________________	____________	____________
Department Head	Signature	Date
______________________	____________	____________
School Dean	Signature	Date
______________________	____________	____________
Office of Post graduate studies, Dean	Signature	Date

DECLARATION

I hereby declare that this Master Thesis entitled "**Secure Multi-Beam Satellite Systems using Adaptive Beamforming for 6G Communications**" is my original work. That is, it has not been submitted for the award of any academic degree, diploma or certificate in any other university. All sources of materials that are used for this thesis have been duly acknowledged through citation.

_________________________________ _____________ _____________

Name of student Signature Date

RECOMMENDATION OF ADVISORS

We, the advisors of this thesis, hereby certify that we have read the revised version of the thesis entitled "**Secure Multi-Beam Satellite Systems using Adaptive Beamforming for 6G Communications**" prepared under my/our guidance by **Yidnekachew Solomon Haile** submitted in partial fulfillment of the requirements for the degree of **Mater's of Science in Communication Engineering**.

Therefore, we recommend the submission of revised version of the thesis to the department following the applicable procedures.

______________________	__________	__________
Major Advisor	Signature	Date
______________________	__________	__________
Co-advisor	Signature	Date

ACKNOWLEDGEMENT

Firstly, my appreciation and gratefulness goes to the Ministry Of Education(MoE) and Adama Science and Technology University in Ethiopia for funding and supporting this study.

I also would like to give my sincere gratitude to my advisor , **Dr. Rajaveerappa Devadas(PhD)**, for his patient guidance, useful advice and encouragement during my study. I have been tremendously lucky to be advised by him, because of his caring about my research progress, useful conversations, enthusiastic support, unyielding belief and his timely and comprehensive respond to my correspondence and questions. Accomplishing my research in time would be have been substantially more challenging without his support and understanding. I also very much appreciate that he gave me the opportunity to decide upon the subject matter of the research for this thesis on my own. I would also like to give sincere thanks to my co-advisor, **Mr. Bayisa Taye Mulatu(MSc)**, for his valuable suggestions and continuous support.

I'd want to express my heartfelt gratitude to **Dr. Demmise Jobir**, **Dr. Dereje Teklu**, **Mr. Tadesse Hailu** and **Mr. Gemechu Dengia** for their encouragement and helpful input during the execution of this thesis work.

I would like to show my gratitude to **Mr. Zewdu Burusa** for his valuable support by arranging the work place open for discussion and laboratory experiment works with taking a lot of responsibility.

Also, I value and most grateful for the support I have received from all my family members. Their inspiration and love have motivated me greatly in the pursuit of successful research outcomes, who have provided unending inspiration during the years of this study.

Finally, I'd want to express my gratitude to my colleagues, friends, and and all of those I have had the pleasure to work with, for they have given me continuous encouragement towards completing this thesis.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

1G:	First generation
2G:	Second generation
3G:	Third generation
3GPP:	Third Generation Partnership Project
4G:	Fourth generation
5G:	Fifth generation
6G:	Sixth Generation
AR:	Augmented Reality
AI:	Artificial Intelligence
BER :	Bit Error Rate
BS :	Base station
CSI :	Channel State Information
eMBB:	enhanced mobile broad-band
ER:	extended reality
Eves :	Eavesdropper
GEO :	Geostationary Earth Orbit
gNB:	Next-generation NodeB
GNSS :	Global navigation satellite system
GPS :	Global positioning system
HBF:	Holographic Beamforming
IoT :	Internet of Things
IRS:	Intelligent reflecting surfaces
LEO:	low Earth orbit
LoS :	Line of Sight
MEO:	Medium Earth Orbit
MIMO :	Multiple-Input Multiple-Output
mmWave:	millimeter wave
mmMIMO :	mmWave MIMO
NFV:	Network function virtualization

NTN:	non-terrestrial network
PLS :	Physical-Layer Security
QoS :	Quality-of-Service
RF :	Radio Frequency
RIS:	reconfigurable intelligent surfaces
SATCOM :	Satellite Communications
SDN:	software-defined networking
SNR :	Signal to noise ratio
SR :	Secrecy Rate
STIN :	Satellite-Terrestrial Integrated Network
THz :	Terahertz
UAV:	unmanned aerial vehicle
VR:	virtual Reality
XR:	eXtended Reality

ABSTRACT

The 6G network will be a fully connected world that integrates terrestrial wireless and satellite communications. With the increasing utility and demand, the need for security increases in satellite communication. The users of this mode of communication along with all sorts of benefits in terms of Quality of Service (QoS) and reduced cost of services also demand confidentiality and integrity of their data. Eavesdropping is a major problem especially for those who send sensitive information through a satellite connection and in satellite networks, these tasks are significantly easier due to the broadcast nature of satellites versus fixed terrestrial. In the open space, the signal is spreading and The information might reach not just the authorized user, but also the nearby eavesdropper(illegal user) could obtain wireless power and retrieve secured information from the power leakage in signals. So, we proposed adaptive beamforming algorithm, it is a signal processing procedure will generate the amplitude and phase in order to guide the tunable element of a holographic array of antenna can be steered to transmit radio signals in a specific direction. The system consisted of an Direction-of-Arrival estimator (MUSIC and Min-Norm) for estimating the location of desired location/earth station, an adaptive beamformer for suppressing eavesdropper and enhancing the earth station beam transmitting signal information. In this thesis, comparison and performance evaluation of these adaptive algorithms i.e LMS and RLS for holographic antenna array in terms of secrecy capacity, speed present. The simulation results shows that, In both DoA algorithm have high-resolution and high-accuracy method, but Min-Norm unsuccessful to suppress the incorrect peaks(affect accuracy), MUSIC have drawback in to estimate the DOAs of more correlated signals(affect resolution). So that, in highly correlated environment Min-Norm perform well but on the other environment MUSIC algorithm better. LMS-beamforming algorithm for increasing number of array elements, has better performance characteristics than RLS-algorithm because of their ability in placing deep null(Lower leakage power) towards the eavesdropper and producing much stronger beam towards the earth station as well as low-side-lobe-levels and increase in secrecy capacity. It is seen that the LMS algorithm has better secrecy capacity performance except that it has a very slow speed than RLS(7.5 μsec).

Key words: – Secrecy, Adaptive Beamforming Algorithm, Holographic Beamforming (HBF), 6G, Satellite Communication, Multi-beam, Eavesdropper, MUSIC, Min-Norm.

CHAPTER ONE
1. INTRODUCTION

1.1 Research Background

The 6G network will connect the entire planet by combining terrestrial wireless and satellite communications as seen in table 1.1. Network signals may reach any location by merging satellite communications into 6G mobile communications to create seamless worldwide coverage. (Chowdhury et al., 2020).

Table 1.1: Comparison of 6G with 4G and 5G communication systems (Chowdhury et al., 2020).

Issue	4G	5G	6G
Per device Peak data rate	1Gpbs	10Gpbs	1Tbps
End-to-End latency	100ms	10ms	1ms
Maximum spectral efficiency	15bps/HZ	30bps/HZ	100ps/HZ
Mobility support	Up to 500 km/hr	Up to 1000 km/hr	Up to 350 km/hr
Satellite Integration	No	No	Fully
AI	NO	Partially	Fully
Autonomous Vehicle	No	Partially	Fully
XR	No	Partially	Fully
Haptic communication	No	Partially	Fully
THz communication	No	Vary limited	Widely
Service Level	Video	VR, AR	Tactile
Architecture	MIMO	Massive MIMO	Intelligent surface
Maximum Frequency	6GHz	90GHz	10THz

With the rise of smart gadgets and the exponential expansion of network traffic, massive and global connection has become a critical technical necessity. Moreover, In the contemporary setting, a wide range of applications with different requirements should be supported. Especially, the sophisticated networking services need to be incorporated into the futuristic use cases such as, the smart transportation, remote connectivity, maritime surveillance, intergalactic communication, smart city, and disaster rescue (Ray, Kumar, & Guizani, 2021).

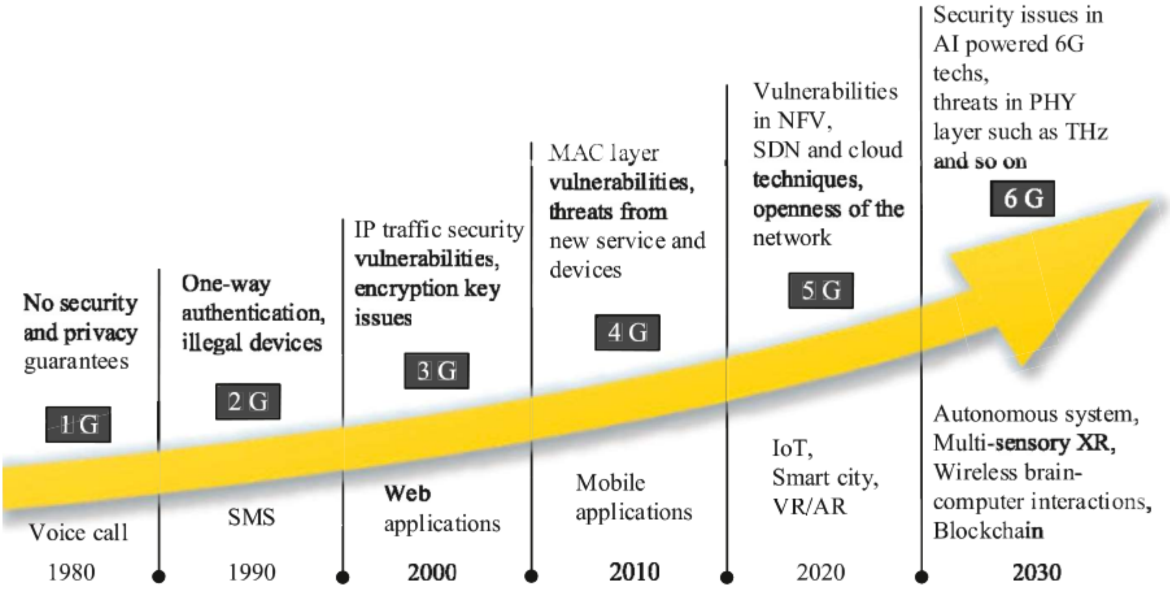


Figure 1.1: Evolution for security and privacy issues (M. Wang et al., 2020).

It is nearly impossible to prohibit unauthorized users from accessing networks due to the broadcast nature of wireless transmission. Enemies or unauthorized users in the coverage area of a satellite may eavesdrop, intercept, invade, distort, or even destroy the satellite network once detecting signals from repeaters or transmitters. In general, these secure problems can be categorized into two classes: one is that in inner regions, unauthorized users or spies detect, intercept, and decode satellite signals (Guo, Li, Liu, Tian, & Kato, 2021). Then they access and attack the networks; the other is that when our soldiers who have penetrated in enemies' region communicate using satellite communication networks, enemies detect and position our satellite down-link signals. Fire strikes may happen. The most common method to ensure security in satellite link is encrypting each data stream which is only decrypted with the secret keys shared between transmitter and legitimate users. Techniques of low probability interception, low probability detection, and anti-jamming also improve the security performance of the networks. Physical layer security techniques belong to the latter, which employ some secure transmission strategies to restrict unauthorized users acquiring information, or prevent them from detecting transmission process between transmitter and the legitimate receiver (Ma, Liu, Wang, Xiong, & Li, 2015).

1.2 Problem Statement

Network signals may reach any location by combining satellite communications with 6G mobile communications for seamless worldwide coverage. The communication via satellites provides ubiquitous services to millions of users that might be hundreds of kilometers apart, but the signals are prone to be overheard by unauthorized users. The broadcast nature of satellite channels, which actually does not limit any unauthorized user to receive the signal and eavesdrop on the unencrypted or poorly secured satellite communication link is easily possible. As security threats such as eavesdropping emerge due to the inherent property of wireless transmission. In the free space, the wireless signal is spreading and not only the authorized user could receive the information but also the adjacent illegal user/eavesdropper could obtain wireless power and retrieve secured information from the power leakage in signals. Therefore, privacy and security concerns in such communication networks have been caught in the spotlight of attention.

1.3 General and Specific Objectives

1.3.1 General Objective

The general objective of this thesis is to secure multi-beam satellite systems using adaptive beamforming algorithms for 6G communication.

1.3.2 Specific Objectives

The specific objectives of this study are as follows:

1. To analyze the performance of adaptive direction of arrival algorithm to track the eavesdroppers(MUSIC and Min-Norm) .
2. To analyze the performance of adaptive beamforming algorithms (LMS and RLS) for holographic array antenna.
3. To evaluate the secrecy capacity of adaptive beamforming algorithms (LMS and RLS) for holographic array antenna.
4. To compare the performance regarding secrecy capacity of adaptive beamforming algorithms (LMS and RLS) for holographic array antenna.

1.4 Significance of Study

Within these expectations, the security of ultra-dense networks of heterogeneous nodes becomes paramount to provide truly scalable, adaptive, safe security solutions towards 6G connectivity. These aspects motivate a bottom-up approach in leveraging all the available security planes over the generic communication stack, and to this end, one key candidate technology is the PLS. adaptive beamforming is poised to play a significant role in the implementation of next generation's wireless communication systems as they have been shown to have the potential for improved capacity, spectral efficiency, security and reliability as compared to single-antenna or conventional terrestrial communication systems.

1.5 Limitation of the Study

The thesis works is:

- Is limited to simulation-based investigation which relies on theoretical analysis.

1.6 Thesis Contribution

- Evaluating the secrecy capacity of adaptive beamforming (LMS and RLS) for the tuning element of holographic array antenna.
- Comparing the secrecy capacity of adaptive beamforming (LMS and RLS) for the tuning element of holographic array antenna.

1.7 Thesis Outline

The outline of this thesis is summarized as follows:

- Chapter Two presents regarding different definitions and concepts of security, satellite system, adaptive algorithm and technology which have been given by different researchers.
- Chapter Three describes the research methods used in this thesis including the mathematical model and evaluating.
- Chapter Four is devoted to discuss the proposed results and discussions.
- Chapter Five presents the conclusions and recommendations.

CHAPTER TWO
2. LITERATURE REVIEW

2.1 Introduction

The rapid development of various emerging applications, such as artificial intelligence (AI), virtual reality (VR), three-dimensional (3D) media, and the Internet of Everything (IoE), has led to a massive volume of traffic (Khan, Yaqoob, Imran, Han, & Hong, 2020). The global mobile traffic volume was 7.462 EB/month in 2010, and this traffic is predicted to be 5016 EB/month in 2030. This statistic shows the importance of improving communication systems. We are heading toward a society of fully automated remote management systems. We are rapidly approaching a civilization dominated by totally automated remote management systems.Autonomous systems are gaining traction in a variety of fields, including industry, health, transportation, the oceans, and space. In order to create a smart life and automated systems, millions of sensors are incorporated into cities, automobiles, houses, industries, food, toys, and other settings. As a result, these apps will demand a high data rate and dependable connectivity. Fifth-generation (5G) wireless networks have already been installed in several regions of the world. 5G is scheduled to be completely operational worldwide by 2020.

New items that may require sixth-generation (6G) system include

1. Massive man-machine interfaces,
2. Ubiquitous computing among local devices and the cloud,
3. Uulti-sensory data fusion to create multi-verse maps and different mixed-reality experiences, and
4. Precision in sensing and actuation to control the physical world (Strinati et al., 2019).

To achieve the 6G target and overcome the limitations of 5G in order to support new challenges, B5G wireless networks will require additional appealing features to be created. By bringing new synthesis of future services, 6G communication networks will address the shortcomings of the 5G system such as sensing-intelligence and new human-human and human-machine interaction, AI and new technology adoption such as Terahertz (THz), three-dimensional (3D) networking, quantum communications, holographic beamforming, backscatter communication, intelligent reflecting surface (IRS), and proactive caching are all terms used to describe technologies that use terahertz (THz). (Strinati et al., 2019).

Satellite communication is a must to provide ubiquitous connectivity. It is almost unconstrained geographical circumstances. It can support a seamless global coverage of various geographic locations such as land, sea, air, and sky to serve the user's ubiquitous connectivity. To reach the aim of 6G, it is intended to link terrestrial and satellite technologies to deliver always-on broadband worldwide mobile connectivity. 6G will need the integration of terrestrial, satellite, and airborne networks into an unified wireless system.

2.2 Satellite Communication

Satellite communication would be seamlessly integrated with the 6G ecosystem. Due to high range coverage and extreme accurate communication aspects, satellite communication would become an inseparable part of 6G. The basic structure of a satellite communication system consists of a space segment that includes the satellite constellation, a ground segment including GW stations and large ground facilities for control, network operations and backhauling, and a user segment with the user terminals deployed on fixed and mobile platforms (e.g., airplanes and ships). Basically three types of satellites participate in digital communications, such as,

1. Low earth orbit (LEO),
2. Medium earth orbit (MEO) and,
3. Geostationary earth orbit (GEO).

LEO satellites orbit earth between 160 and 2000 km above earth. MEO satellites orbit earth between 2000 and 36000 km above earth. GEO satellites have a stationary orbit of 22236 km above earth surface. Different types of satellite communication techniques are used to provision a number of applications, for example, fixed satellite service (FSS) is meant for broadcasting feeds to TV stations, radio channels and broadcast networks (Ray, 2021). Earth to space services is generally imposed by the FSS.

2.2.1 Satellite Frequency Bands

In telecommunications, 6G will be the sixth generation standard for wireless communications technologies supporting networks. The eventual goal is to replace or work alongside 5G networks and will offer significantly faster transmissions, at speeds of $\sim 95 Gbit/s$ ((Mi-Wave), 2020). The satellite frequency bands chart below:

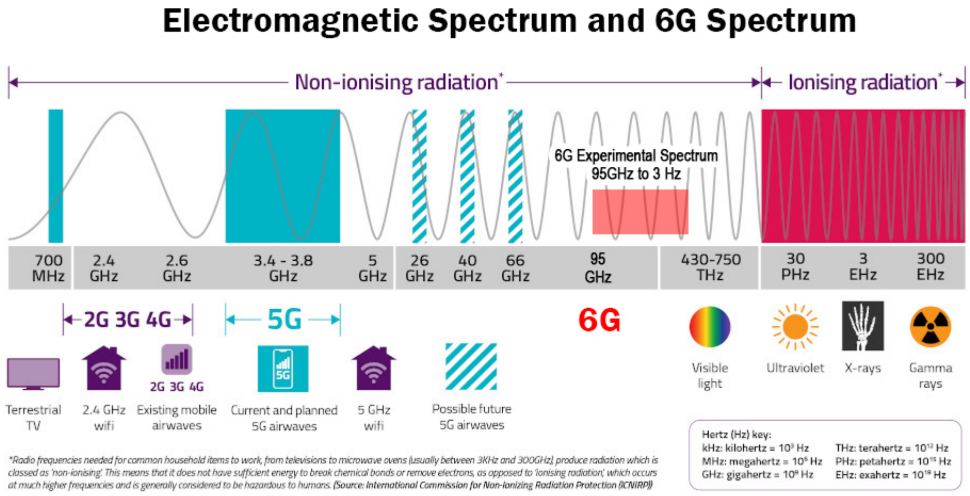


Figure 2.1: Electromagnetic Spectrum and 6G Spectrum ((Mi-Wave), 2020).

Table 2.1: Comparison of microwave frequency bands (Ray, 2021).

Band	Frequency Range (GHz)	Wavelength Range	Use Cases
L	1-2	15-30cm	Military, GPS, GSM
S	2-4	7.5–15 cm	Weather radar, some communication satellites
C	4-8	3.75-7.5 cm	Long range radio communications
X	8-12	25–37.5 mm	Satellite communication, radar, space communication
K_u	12-18	11.3–16.7 mm	Radar, satellite communication
K	18–26.5	16.7–25 mm	Satellite communication
K_a	26.5–40	5–11.3 mm	Satellite communication
Q	33–50	6–9 mm	Satellite communication, terrestrial microwave communication
V	50–75	4–6 mm	mmWave radar search
W	75–110	2.7–4 mm	Satellite communication, mmWave radar search, military radar targeting, automotive radar
F	90–140	2.1–3.3 mm	SHF transmission, WLAN, microwave communications
D	110–170	1.8–2.7 mm	EHF transmission, microwave remote sensing, mmWave scanner

Microwave is a form of radiation that ranges between 0.3 and 300 GHz. It runs over the ultra-high frequency (UHF), extremely high frequency (EHF) and super high frequency (SHF) bands.

As microwaves travel line-of-sight (LoS), it is good for visual horizon up to 64 km terrestrial communication applications. Thus, 6G-SAGIN can be highly benefited by microwaves to provide point-to-point connectivity between UAVs and satellites. Microwave technology offers a vivid range of frequency named after alphabets for formulating specific use cases. For example, 6G-SAGIN may be benefited by using microwave bands like L, S, C, X, K, Q and W. Satellite and UAV communication would be highly reliable by using microwave bands of choice. table 2.1 presents a comparison between microwave bands.

2.2.2 Satellite Security

Like all engineering systems, satellite systems can be subjected to undesirable scenarios that may be brought about intentionally or not. From the very rough conditions of Outer Space to targeted attacks conducted by malicious individuals, there are many risks that can cause adverse effects on the well-being of a satellite. While some effects can be easily and readily reversible, some can prove to be catastrophic and result in a total inability to use the system. In order to properly assess the risks that are involved in any system, it is beneficial to define a set of terms that will help us reliably identify and differentiate between different objects; we will use the following terms as defined in (Matei, 2021):

- **Vulnerability** - a weakness that is present in a system that could cause harm
- **Threat** - a specific set of circumstances that could cause harm
- **Attack** - an intentional exploitation of a vulnerability

Another set of terms that will prove important for our understanding of security threats in satellite systems are the terms that define the principles of good security. They are described in the ISO7498-2:1989 standard and have been recognized as important security principles in space systems, being present in the CCSDS report "Security Threats Against Space Missions"; again, the definitions provided in (Matei, 2021), will serve as our base:

- **Confidentiality** - the ability to be accessed only by authorized parties
- **Integrity** - the ability to be modified only by authorized parties

- **Availability** - the ability to be used by any authorized party
- **Authentication** - the ability to confirm the identity of a person/system that performs an action
- **Accountability (nonrepudiation)** - the ability to confirm that someone/something performed a certain action, without it being possible for them to deny it in any convincing manner.

The above security properties can and, in well-designed systems, should be applied to any valuable asset, such as hardware, software, human personnel, communication channels etc. This section aims to provide a broad analysis of the various dangers that should be taken into account when designing satellite systems, and especially taking a look at intentional cyberattacks and how can they be identified, prevented and mitigated.

2.3 Security Issues and the Evolution of Security Architecture

This section presents our assessment of security attacks and privacy issues for various generations of cellular networks. We then highlight lessons learned from the prior security transitions to envisage potential changes and enhancements for security and privacy preservation features in 6G.

There are many memorable milestones with the development of the first three generations of mobile networks, particularly in security. The first generation (1G) of mobile networks provided neither security nor privacy. Launched in the 1980s and 1990s, respectively, the second generation (2G) and the third-generation (3G) played a critical role in completely transforming the era of analog phone services (1G) to IP-based networks (3G). Although many operators around the world, particularly in developing countries, still offer 2G and 3G services, both networks are scheduled to be entirely switched off in the next five years. 2G and 3G gave many valuable lessons of how security issues can be exploited by attackers. For example, the most infamous attack on 2G and 3G was International Mobile Subscriber Identity (IMSI)- catcher, where the attacker exploited unencrypted identity information during authentication and paging procedures to track mobile subscribers. Many law enforcement and intelligence agencies in some countries still use IMSI- based tracking to follow crimes.

The Long-term Evolution (LTE)- Advanced standard (official technology of 4G in ITU requirements has evolved strongly over the years, resulting in the most widely deployed network. Compared to 3G, 4G security has been enhanced significantly. For example, 4G/LTE.

Evolved Packet System-Authentication and Key Agreement (EPS-AKA) included a series of security enhancements for interconnection between 3GPP and non-3GPP networks.

5G has been upgraded significantly in terms of both security architecture and authentication protocols to satisfy a service- oriented network model as well as fixing many vulnerabilities in 4G. According to the latest specifications, other than the five security features in 4G networks, 5G adds a new domain: service-based architecture (SBA) security. 5G is also the first standard to have its authentication architecture as a unified framework. This platform supports both 3GGP and non-3GPP access networks, e.g., Wi-Fi and cable networks. With a unified platform, 5G enables one authentication execution, in which a UE can be authenticated in a 3GPP access network, and then move to other non-3GPP network without the need for re-authentication (Ahmad et al., 2019).

2.4 Security in the Physical Layer

Since the physical-layer is the cornerstone of wireless communications, protecting physical-layer information can prevent many conventional attacks on radio signals such as eavesdropping and jamming that nearly impact on every 6G application.

The premise of physical-layer-security is to exploit the characteristics of wireless channels (e.g., fading, noise) to enhance confidentiality and perform lightweight authentication. Low complexity of physical layer security will particularly benefit 6G low-cost IoT devices, which often lack energy and computation capacity to run advanced authentication mechanisms. Besides, relying on physical laws, physical layer security is robust against cryptanalysis, which has been the top concern of conventional cryptographic algorithms. Physical layer security can be implemented at the base stations/IoT gateways of the operators or in the signal modulation algorithms. The following subsections look at key security concerns and several prominent defense approaches for enabling technologies in 6G.

2.4.1 Security in 6G mmWave communications

As we noted in the previous section, when 6G networks start to roll out, a substantial number of 5G devices will still be on. Therefore, mmWave and massive MIMO are still crucial physical layer technologies in 6G compatible (non-standalone) networks. Figure 2.2 illustrates three common attacks in mmWave MIMO networks: eavesdropping, jamming, pilot contamination attacks (PCA). Eavesdropping is carried out through inferring and wiretapping (sniffing) open (unsecured) wireless communications.

In 6G mmWave MIMO networks, beamforming technology can benefit security. As illustrated in Figure 2.2, an eavesdropper (Eve) must locate in the beam scope (Figure 2.2.a) or use a reflector (Figure 2.2.b) to wiretap the channel. The eavesdropper can be a legitimate person (internal) of the network (e.g., employee) or someone outside (external). Based on the information about the trans- mission signals (e.g., the frequency f2) between the transmitter (Alice) and the receiver (Bob), the eavesdropper can carry out two other attacks. One is jamming attack (Figure 2.2.c), where the jammer can inject radio signals (same frequency as Bob's f2), so as to occupy a shared wireless channel. Such aggressive injection prevents legitimate users (e.g., Bob) from using a wireless channel to communicate, a kind of DoS.

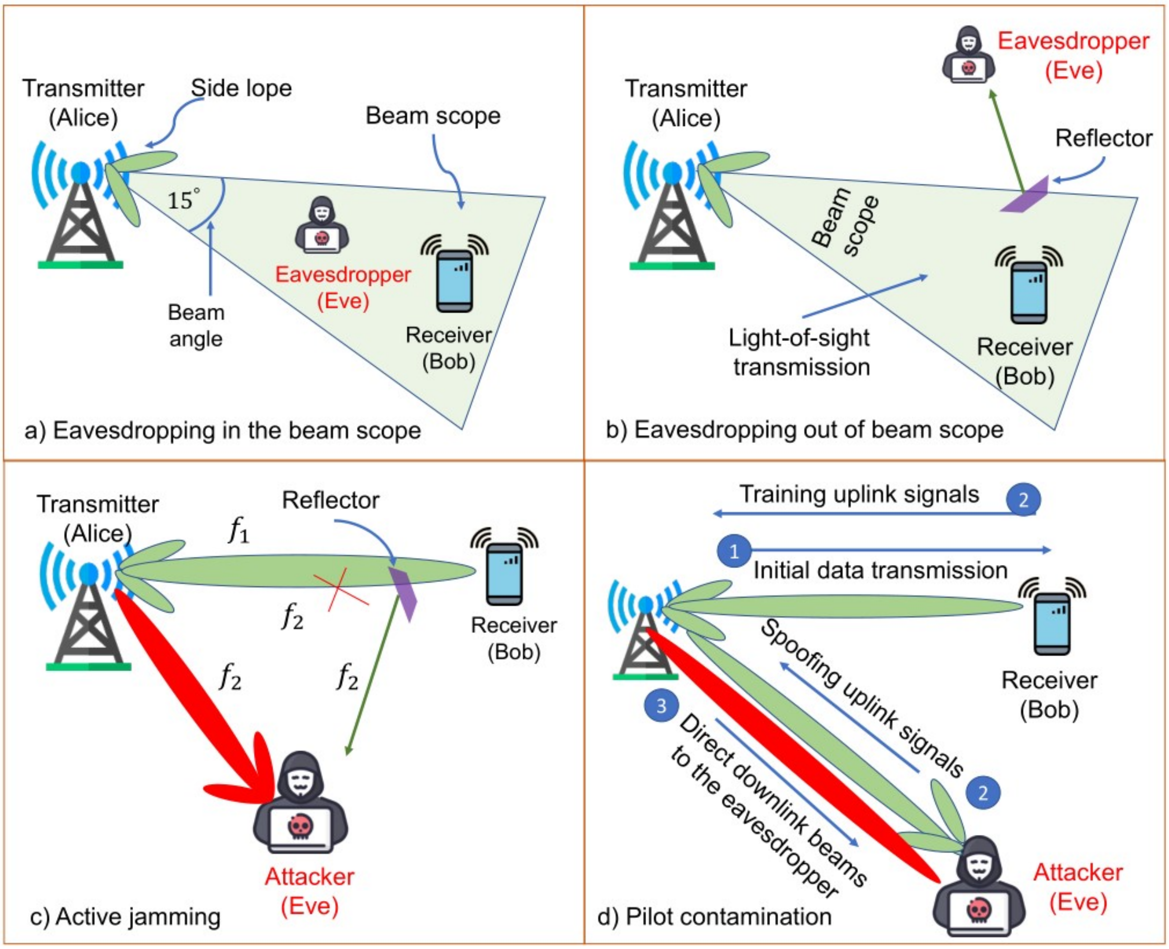


Figure 2.2: Illustration of three common attacks against 5G physical layer technologies that can occur in future 6G compatible networks(Nguyen et al., 2021).

The other one is PCA, where the attacker intentionally transmits identical pilot signals (spoofing uplink signals in step 2 of Figure 2.2.d) to contaminate user detection and channel estimation phase of the transmitter (Alice). In the worst case, the transmitter will steer the partial beam towards the attacker in the manipulated downlink direction (step 3 of Figure 8.d), which practically degrades a legitimate user's transmission or causes signal leakage. Ultra-massive MIMO and Multi-User MIMO are susceptible to PCA (Nguyen et al., 2021).

Besides, a cell-free massive MIMO system can risk itself by exposed location of radio stripes (Björnson, Sanguinetti, Wymeersch, Hoydis, & Marzetta, 2019), i.e., dense antennas are easier to reach by physical attacks.

2.4.2 Eavesdropping Attacks for Satellite Systems

Satellite communication operates similarly to communication across any network. The key layers of the Open Systems Interconnection (OSI) model (Physical, Data Link, Network, Transport, and Application) are still present. However, the most significant difference is the distance that the radio signal has to travel. While there are many types of satellites, this paper will primarily look at those in LEO satellite. Communications satellites are the most likely target of an eavesdropping attack because of the data that can potentially be acquired from them.

First, we briefly define an eavesdropping attack, and how it can be executed on a satellite. An *eavesdropping attack, also known as a man-in-the-middle attack*, is when an unauthorized agent listens in on communication they are not meant to receive. Due to the nature of how a satellite broadcasts a signal back down to earth, with the right equipment it is possible to intercept this communication without even being in close proximity to the satellite's ground receiver as shown in figure 2.2.

This attack was successfully theorized as a potential way to disrupt downlink communications. It could even be modified to modify the bit stream of the communication, manipulating the transmitted information. Tests have even been conducted with equipment that an average person could purchase in which maritime communication was intercepted, including military and government communication (Hayashi & Vázquez-Castro, 2020). If this is possible to execute in an experimental environment, it is also a threat that could originate from someone with more malicious intentions.

2.5 Smart antenna

The signal processing adaptive algorithm has a significant impact on performance of a Smart Antenna system. Although the smart antenna system is sometimes called the "Space Division Multiple Access", it is not the antenna that is smart. An antenna transforms electrical impulses into electromagnetic waves. or vice versa but nothing else (Balanis & Ioannides, 2007).

Two algorithms are used in the signal processing technique: a direction of arrival (DOA) method and an adaptive beamforming algorithm. The DOA algorithm determines the arrival direction of all incoming signals. Then, the adaptive beamforming algorithm is used to update the system parameters (w_0, w_1, w_{N-1} as shown in figure 2.3). The weights of each element change the phase shift and amplitude attenuation of the received signal so that the main beam is steered toward the desired signal direction and nulls are placed in the directions of the interference. Smart antennas have many advantages such as increasing the system capacity, reducing bit-error rate, compatibility with the various multiple access technique, enhancing the beam directivity, decreasing the effects of fading, reducing the signal-to-interference ratio (Alotaibi & Hamdi, 2016).

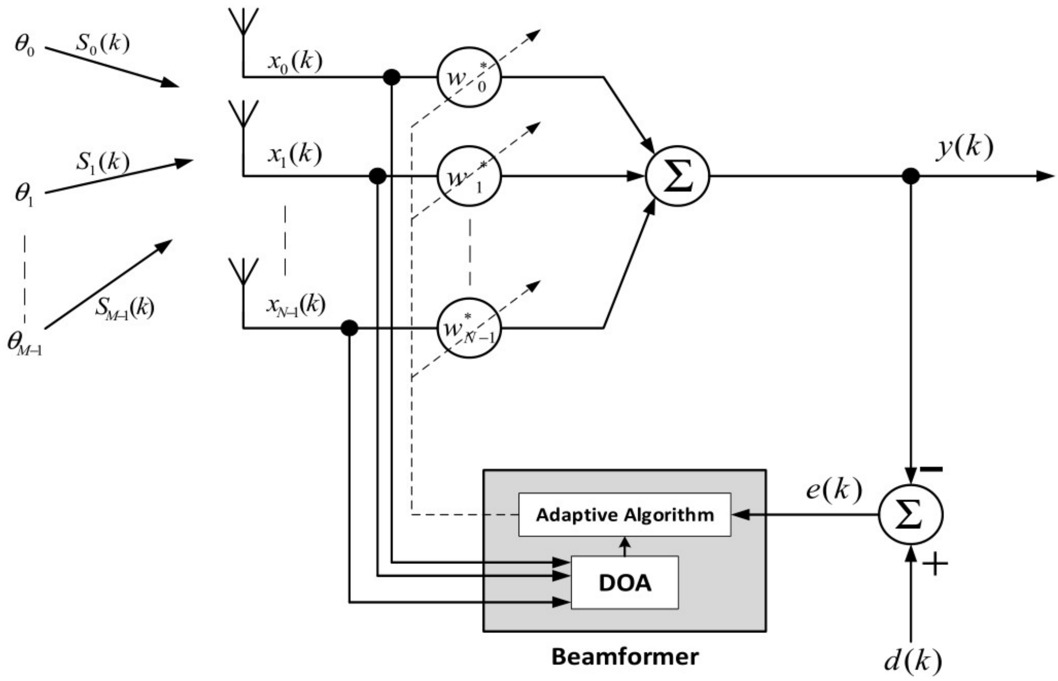


Figure 2.3: The adaptive beamforming array antenna (smart antenna) model block diagram (Khalaf et al., 2016).

2.5.1 Motivations for Adaptive Antenna Application

Traditional wireless network technologies have long investigated the use of adaptive antennas to take advantage of dynamic antenna pattern modification. This function creates enhanced directional beams that dynamically focus the signal in a tighter direction, increasing the wireless signal's directivity. The antenna layout or the number and angle of the components in the array antenna are examples of these antenna alterations. The primary goal of physical modifications is to improve signal quality. The related effects are as follows (Wu & Lai, 2022):

- **Improvements in wireless performance:** Adaptive antenna modification is used to improve signal quality., thereby Increasing the efficiency of wireless transmission.

- **Expansion of coverage:** Increased range and users in the same direction at the same frequency can be achieved with enhanced directed beams.

- **Reduce interference:** The goal of interference reduction is to improve the wireless signal's stability and transmission quality. Therefore, Space diversity, polarization diversity, and frequency diversity can all be employed to minimize interference in physical antenna applications.

- **Enhanced security:** Through a multi-path model, the adaptive antenna creates the beam for transmission. This multi-path transmission makes it more difficult for hackers to steal and intercept data.

2.5.2 Adaptive Beamforming Algorithm

The adaptive algorithm is the one who provides a smart antenna system its intelligence. Without an adaptive algorithm, It is no longer possible to retrieve the original signals. Different adaptive algorithms were developed for different purposes and tasks. The task of the algorithm in a Smart antenna system is to adjust the received signals so that the desired signals are extracted once the signals are combined. Various methods can be used in the implementation of an adaptive algorithm (Wu & Lai, 2022).

2.5.3 Direction of arrival (DoA)

The technique used for estimating the direction of arrival(DOA) of radio signals in wireless system has received considerable attention because estimating the direction of arrival of several radio signals impinging on an array of sensors is required in a variety of other applications, including radar, sonar and seismology (Kwizera, 2018).

2.6 Adaptive Beamforming Technologies

2.6.1 Phased array beam forming

Phased array beam forming is named for and enabled by a phase-shifter behind every radiating element. Transmission mode, the radio signals is made available via a corporate feed network, giving each member in the array the same phase shift. Phase-shifters at each radiating elements then apply the appropriate delay in carrier phase to cause constructive-interference of the radiated fields in desired direction while also causing destructive-interference in others (Black, 2017).

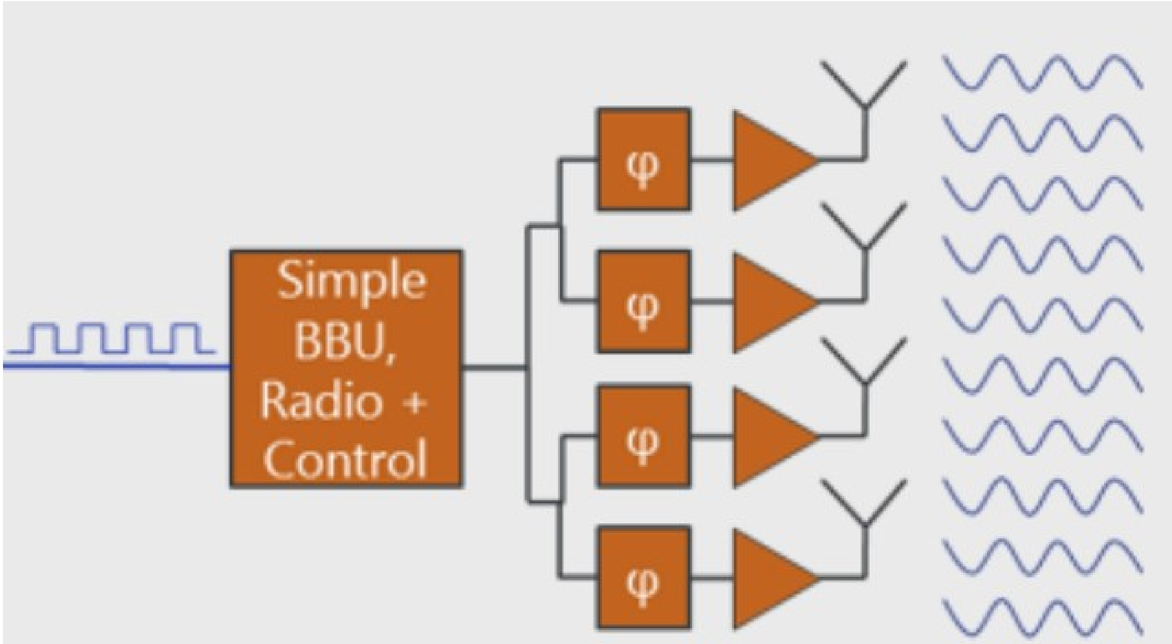


Figure 2.4: Phased array architecture (Black, 2017).

2.6.2 Holographic Beam Forming (HBF)

Holographic beamforming(HBF) is a new technique derived from meta-material concepts. Functionally, HBF is an analog beamformer with performance equivalent to analog phased arrays. As with other planar arrays, the antenna area dictates the achievable beamwidth and maximum realized gain (Eric Black & Andjela Ilic-Savoia, 2020). The HBF technique uses one RF chain that feeds all the elements in the array through a single RF port. Rather than a corporate feed as in phased arrays or digital network in MIMO, HBF uses a series feed that distributes the RF signal along multiple individual antenna elements. dipoles, patches, Slots and other small antenna types have all of the varieties have been proven to operate together the HBF techniques as radiating elements . The energy is transferred from the distribution network to the antenna element through a varactor adjusted feed coupler and this is shown schematically in Figure 2.5. As shown, each elements sees a various progressive phase-shift from the feed-point. Beamforming is accomplished, the capacitance shift in the varactor to change the coupling Applying the to chosen components the proper phase alignment needed to guide the beam in a specific direction (Eric Black & Andjela Ilic-Savoia, 2020), (Staff, 2019), (Black, 2017).

To create a re-configurable antenna, the PIN-diode is used. This device can be incorporated to variate the resonance state of the antenna. A PIN-diode is a semiconductor that is current-controlled. This device works as a variable resistor at RF and MW frequencies. The PIN-diode (PD) can be used in a variety of applications, depending on how its current is controlled. If the current is varied continuously, the PD works as an attenuator or a modulator device. On the other side, if the current is discretely switched, the PD operates as a phase shifters or a switch.

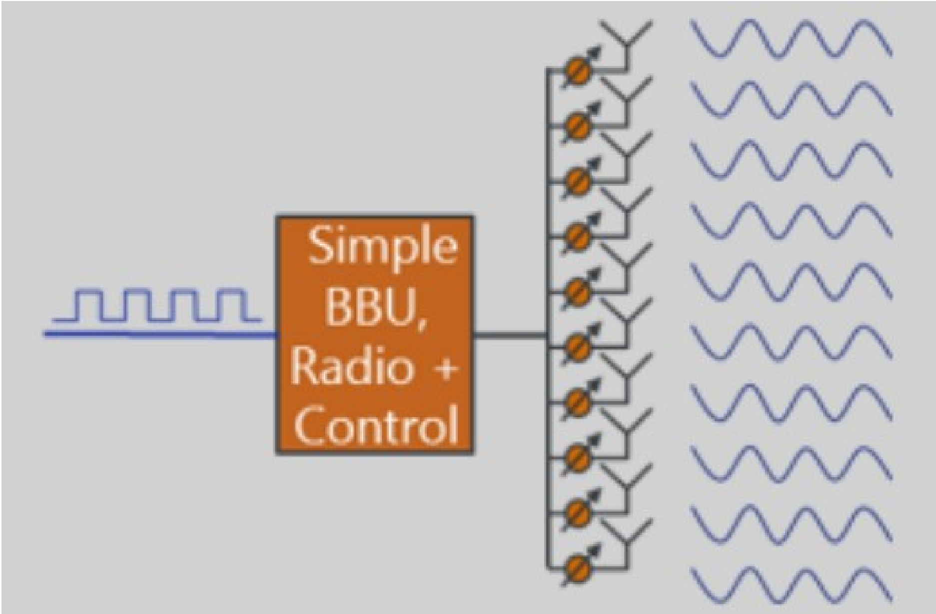


Figure 2.5: Holographic Beam Former architecture (Black, 2017).

2.7 Secure Multi-Antenna Techniques

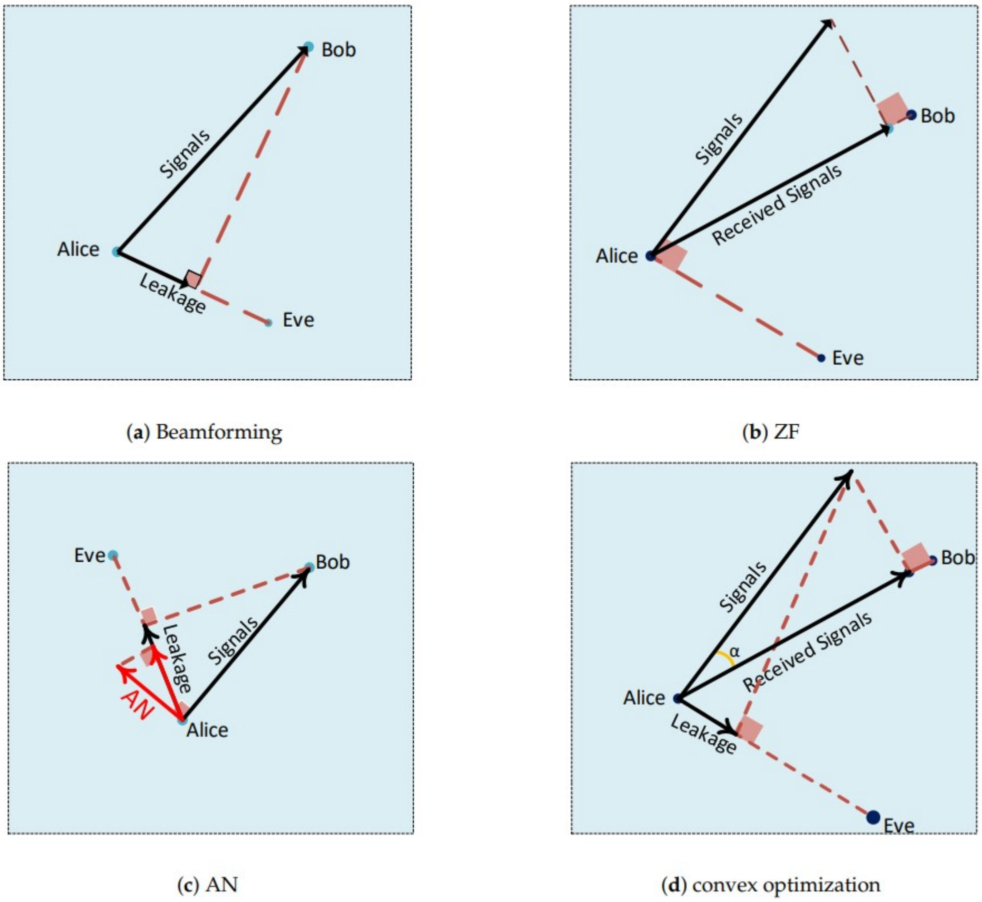
Multi-antenna techniques have been widely considered in wireless communication because they offer higher spatial degrees of freedom, which can be utilized effectively in PLS to ensure secure data transmission. Such techniques either attempt to degrade the eavesdropper's channel relative to the main transmission channel or enhance the quality of the received signal at the legitimate receiver. From the perspective of optimization, the four techniques which are representative of this area are. In figure 2.6, from each technique is described in terms of the transmission's orthogonality to Bob and Eve.

- **Beamforming:** Beamforming is a signal processing technique that is used to transmit signals effectively in intended directions to give a maximum signal difference between the receiver in the intended direction and the one in the unintended direction.

- **Zero-forcing (ZF):** Zero-forcing precoding, or null-steering, is a method of spatial signal processing in which multiple antennas at the transmitter can completely cancel out or null the multiple user interference signals in a wireless communication network.

- **Convex optimization:** Convex optimization can be used in PLS with other secure-multi antenna techniques to find the most favorable transmit solutions that can effectively make the best out of the performance metrics of the wireless communication system.

- **Artificial noise (AN) Precoding:** The technique involves deliberately degrading the quality of the channel of the eavesdropper by generating an interference signal, which is used to interrupt their eavesdropping capabilities.



(a) RLS; N=5; d=0.5λ
Figure 2.6: Secure multi-antenna techniques (Sanenga et al., 2020).

2.8 Physical Layer Security

To stay on top of the difficulties, Recently, a novel way to ensuring secure communication for wireless networking has gotten a lot of attention, i.e., information-theoretic-security. In contrast to cryptographic encryption techniques, whose secret-keeping technique is based on mathematical calculations, Information theory provides the theoretical foundation for information-theoretic security.

Comparing to cryptography encryption and decryption technologies to guarantee secrecy capacity, physical-layer-security approaches have the following features (Sun & Du, 2017):

- The theoretical basis of physical layer security approaches is strictly based on information theory. These approaches achieve provable security regardless of the unlimited computational power the eavesdroppers may possess. Precise measurements can be performed about the information that is successfully transformed to the legitimate destination and leaked to the eavesdropper.
- Physical-layer-security approaches techniques take into account all of the characteristics of wireless channels. Using the intrinsic randomness shared by legitimate terminals, Wireless Physical Layer Security the information-theoretic security approaches are more robust to the man-in-the-middle attack.
- Physical-layer-security approaches eliminate the key generation and distribution issues, thereby resulting in significantly lower complexity and savings in computational resources, which makes it very applicable in decentralized wireless networks that lacks of infrastructure support and mobile wireless networks with dynamic topologies.

Fortunately, physical layer security approaches fit to build a layered security hierarchy system, and provide an additional layer of security that can coexist with those already deployed security schemes in upper layers.

2.9 Related work

In (Zhang, Lin, Ouyang, Zhu, & De Cola, 2021), , the authors proposed a robust-beamforming scheme to enhance physical-layer-security of the down-link of a multi-beam satellite system in the presence of either uncoordinated or coordinated eavesdroppers. Specifically, with knowing only the approximate locations of the Eves, we aim at maximizing the worst-case achievable secrecy-rate of the legitimate-user, subject to the constraints of per-antenna transmit power and quality-of-service requirement of the. Since the optimization problem is non-convex, they first adopt the discretization method to deal with the unknown regions of the Eves and then exploit the log-sum-exp function to approximate the objective function.
In (Yin et al., 2021), the authors investigate the physical-layer-security(PLS) of a multi-beam satellite communication system where the satellite transmits the private signal to a legitimate-user which is intercepted by multiple eavesdroppers (Eves). They consider the imperfect channel state information of Eves channels, they formulating the constrain problem to maximizing the legitimate-user achievable secrecy-rate subject to secrecy rate outage probability constraint.

In (Cui, Zhu, Xu, & Wang, 2020), the authors focused on multibeam satellite communication, since it is an important component for the sixth generation (6G) wireless networks and plays an important role in future integrated satellite-terrestrial communication systems. However, the large area covered by the satellite beams makes itself vulnerable to be wiretapped, especially for the cases that eavesdroppers are located near the legitimate receivers. This paper, cooperative-jamming from both satellite and full-duplex receivers are investigated aim to minimize the power consumed by a multi-beam satellite system with secrecy outage probability. They use, an algorithm of joint-beamforming and power allocation via alternating-optimization(JBFPA-AO).

In (Lu, Liang, An, & Yang, 2018), In this paper, they study the secure beamforming(BF) and artificial noise(AN) techniques for a cognitive-satellite terrestrial systems, where a satellite system termed as the primary-network under the interception of multiple unauthorized eavesdroppers shares the spectrum of resources with multi-cell secondary terrestrial networks. The design objective is to minimize the total transmit power on board the satellite and multi terrestrial base-stations (BSs) while meeting the secrecy-rate constraint of the primary satellite user along with the signal-to-interference-plus-noise ratio constraints of secondary terrestrial users. When exact channel state information at the satellite and terrestrial BS is perfectly known, a zero-forcing scheme is first presented to obtain a sub-optimal solution with low complexity.

In (Liao, Wu, Wu, & Gao, 2019), The power of Beidou satellite-signals is low, so it is vulnerable to interfering sources and in the presence of jamming. Therefore, a robust-constrained inverse beamforming algorithm based on space-time adaptive processing is proposed, which can not only reduce the side-lobe-level to suppress interference better, but also achieve the lower complexity, and then introducing the steering vector uncertainty set model into the algorithm to improve its stability. In the simulation, the proposed algorithm can be verified to have good beamforming capability and higher signal to interference noise ratio(SINR) improvement even in the case of low signal to noise ratio(SNR) and high interference to noise ratio(INR).

In (Y. Wang, Li, Jiao, Wu, & Zhang, 2019), In this paper, They focus on the mmWave band MIMO channel estimation in the satellite based Internet of Things (S-IoT). At first, they establish a sparse geometric-based mm-MIMO channel model between a high-throughput-satellite(HTS) and multiple terrestrial user-equipments for the S-IoT downlink system. Tak-

ing use of the inherent sparsity to the mmWave band channel, they propose an efficient adaptive random selected multi-beamforming (ARM) estimation scheme, which can simultaneously estimate the mm-MIMO channel-state-information(CSI) for multi UEs in angle.
In (Xu, Da, Hu, Ni, & Pan, 2019), the authors makes research on a secure-hybrid satellite-terrestrial network with eavesdroppers at primary receivers and secondary receivers. they adopt null-space beamforming to the amplified and forward(AF) relay protocol and weighted-fractional-data-carrying-artificial-noise(WFDCAN) to the decoded-and-forward(DF) relay protocol at the satellite. The secrecy capacity, the ASER of the uplink channel and the delay constrain of the down-link channel are applied as factors for a three level relay protocol selection scheme.
Related Researches:

Table 2.2: Related Research

No	Contribution and Research Direction	Gap
(Zhang et al., 2021)	To enhance physical-layer-security of the down-link of a multi-beam satellite system Robust-beamforming scheme The optimization problem is non-convex.	Considering fixed beam scenario
(Schraml, Schwarz, & Knopp, 2020)	Precoding algorithm to secure the downlinks of multiple users against multiple eavesdroppers By the use of artificial noise	Demonstrated in Phased array antenna
(Cui et al., 2020)	multi-beam satellite system with secrecy outage probability, for the application 6G For the cases that eavesdroppers are located near the legitimate receivers, Algorithm joint-beamforming and power allocation via alternating-optimization(JBFPA-AO)	Considering fixed beam scenario
(Mun, Kim, Bae, & Hwang, 2018)	They used adaptive beamforming satellite system based on the phased array antenna. Consisted of an Angle-of-Arrival (AOA) estimator,	Only employed on MUSIC algorithm for the AOA estimator.

CHAPTER THREE
3. MATERIALS AND METHODS

3.1 Introduction

In this thesis work, the secrecy capacity is investigated in the multibeam satellite system for 6G communication using adaptive beamforming algorithm. First established the multi-beam satellite system and calculating look angle which consists of one earth station and three eavesdroppers. Then, analyzing direction of arrival(DoA) (MUSIC and Min-Norm) and adaptive beamforming algorithms(LMS and RLS) for the tuning element of holographic array antenna were provided to evaluate the secrecy capacity.

3.2 Materials

In this thesis, a MATLAB/R2021b MEX file package software is used for the simulation. The MATLAB version of the packages necessary for the simulation.

3.3 Methods

In this thesis, presented and evaluate an efficient secure architecture of the adaptive transmission beamformer for multi-beam satellite system for 6G services. the system consisted of an DoA estimator and an adaptive beamforming algorithm. In order to efficiently transmit the signal information to the earth station, we employed the MUSIC and Min-Norm algorithm for the DoA estimator and the LMS and RLS beamformer for the enhancing directivity to earth station and rejecting(minimizing power leakage) eavesdropper. On satellite downlink it is possible for the eavesdropper to be in a separate geographical location and still intercept the communication. Because of this, it is possible for multiple eavesdroppers to be in multiple locations and attempt to intercept or hijack a satellite downlink. The model for this attack shown in Figure 3.1 is comprised of a satellite with an authorized users(Earth station) against multiple eavesdroppers at the same time. In order to enhance the secrecy capacity, tracking the position/location of the earth station look angle calculation is need. This adaptive beamforming algorithm will enhance directivity to the earth station and suppress eavesdropper.

3.3.1 System Design

Involve the following:

- Analyzing the mathematical model for the look angle based on the given satellite orbital parameter.

- Analyzing the mathematical model for direction of arrival(MUSIC and Min-norm).
- Analyzing the mathematical model of adaptive beamforming (LMS and RLS) algorithm for tuning element of holographic array antenna.
- Analyzing the Secrecy capacity of adaptive beamforming algorithm.

3.3.2 System model

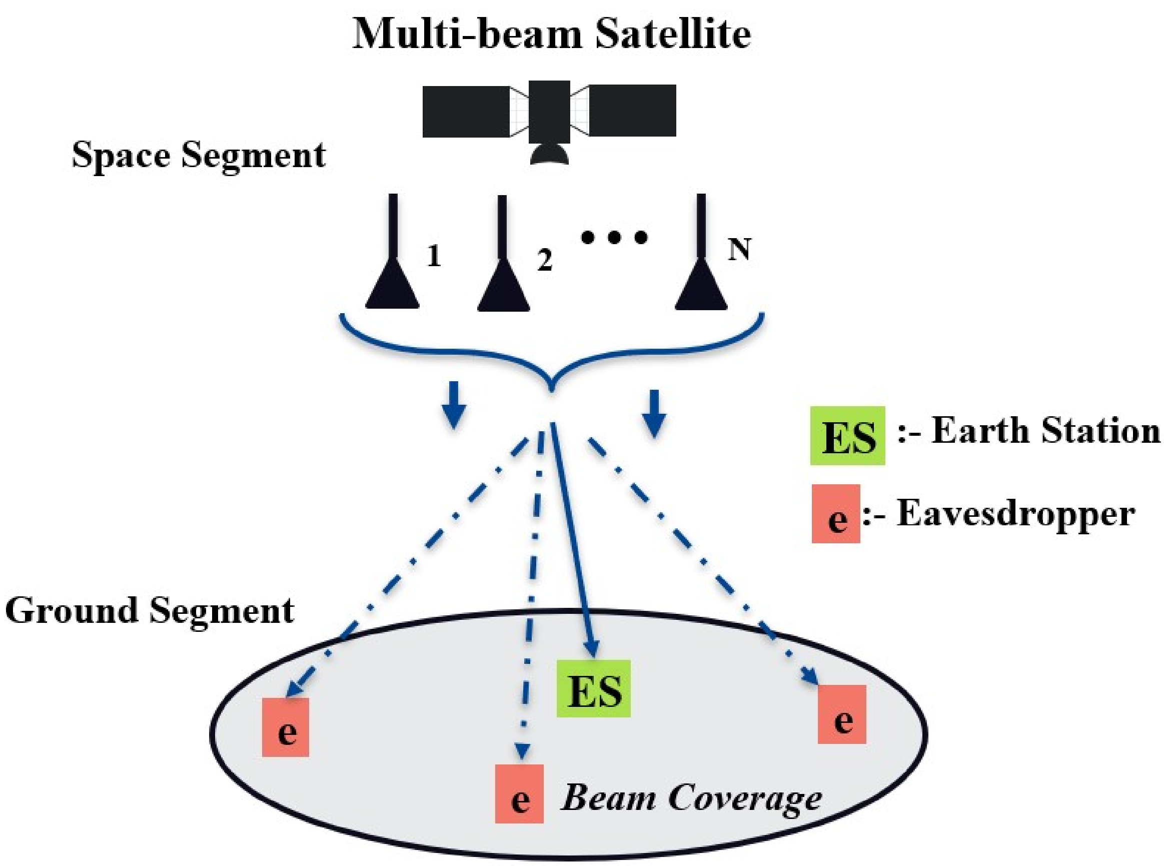


Figure 3.1: Proposed system model.

3.3.3 Simulation Methods

Involve the following:

- Calculating look angle for earth station and eavesdropper.
- Evaluate direction arrival algorithm to estimation of the earth station considering different scenario i.e number of antenna variation, distance between antenna spacing variation and different arrival angle.

- Evaluate adaptive beamforming algorithm holographic array antenna to evaluate the nulling in the antenna radiation pattern towards eavesdropper and a beam towards the desired user(earth station) by considering different scenario i.e number of antenna variation and distance between antenna spacing variation.
- Evaluate and compare the secrecy capacity performance of adaptive beamforming algorithm .

3.4 Simulation Parameters

The simulation parameter of this thesis will be found in table 3.1:

Table 3.1: Simulation Parameters.

Simulation parameters	Parameter values
Frequency Band(In Future)	W-band (75–110)GHz (Ray, 2021)
Number of antennas(N)	5-30
Number of Users	1-ES and 3-Eaves
Earth station	9.80°N and 38.70°(*Garuma etal.*,2020) E
Eavesdropper Location-1	8.24°N and 34.59°E
Eavesdropper Location-2	7.0504°N and 38.49°E
Eavesdropper Location-3	9.31°N and 42.13°E
Antenna Element separation(d)	(0.2-1)λ
SNR	20dB

3.5 Satellite Location

In order to design a satellite constellation for world-wide or partial coverage, a satellite's location in the sky has to be determined. A satellite's position can be identified with different co-ordinate systems, the choice being dependent upon the type of application. For example, radio communication engineers prefer to use look angles, specified in terms of azimuth and elevation, for antenna pointing exercises. The most commonly used co-ordinate systems are described in the following sections.

3.5.1 Satellite Parameters

Ethiopian Remote Sensing Satellite (ETRSS-1) is a 65-kg multi-spectral remote sensing satellite launched into a sun synchronous orbit to provide earth observation data mainly on the areas of Ethiopia, Middle East, and the rest of Africa.

It operates in a Sun-Synchronous Orbit (SSO) with an altitude of 628.61-km and other orbit information can be found from table 3.2.

Table 3.2: Satellite Parameters (ETRSS-1 orbit (Garuma et al., 2020)).

Satellite parameters	Values
Nation	Ethiopia
Type / Application	Earth observation
Operator	Ethiopian Space Science and Technology Institute (ESSTI)
Orbit type	Sun Synchronous Orbit(SSO)
Satellite Orbit	LEO
Altitude	628km
Frequency Band	X-band(8-12)GHz and S-band(2-4)GHz
Orbit Inclination	97.896°
Orbit Period	97.134 minutes
Revisit period	4 days (by 35° roll maneuver)

A set of six orbital parameters is used to fully describe the position of a satellite in a point in space at any given time:

- Ω : – The right ascension of ascending node, the angle in the equatorial plane measured counter-clockwise from the direction of the vernal equinox direction to that of the ascending node;
- i : – inclination angle of the orbital plane measured between the equatorial plane and the plane of the orbit;
- ω : – argument of the perigee, the angle between the direction of ascending node and direction of the perigee;
- e : – eccentricity $(0 \leq e < 1)$;
- a : – semi-major axis of the elliptical orbit;
- ϑ : – true anomaly.

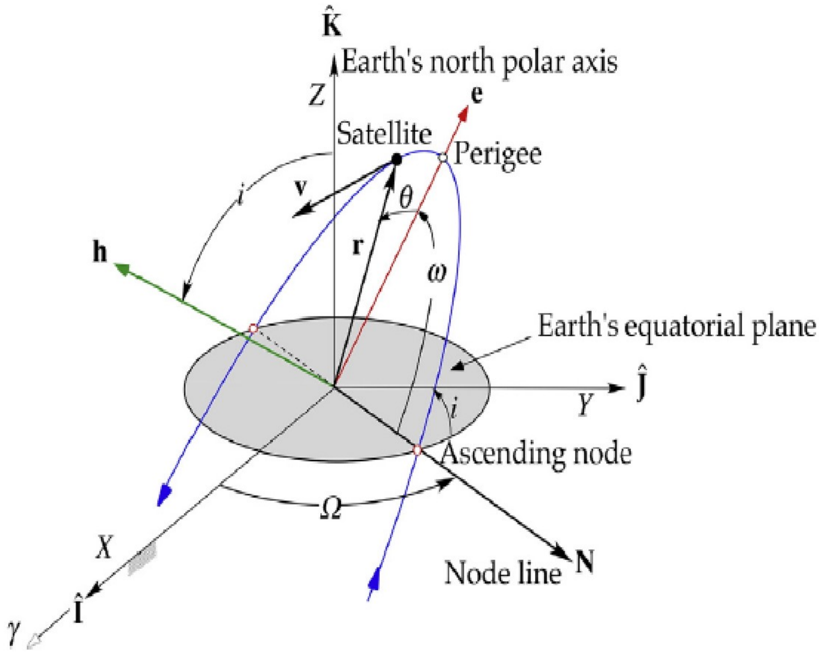


Figure 3.2: Satellite parameters in the geocentric-equatorial co-ordinate system.

The first three parameters, Ω, i and ω define the orientation of the orbital plane. They are used to locate the satellite with respect to the rotating Earth. The latter three parameters e, a and v define the orbital geometrical shape and satellite motion; they are used to locate the satellite in the orbital plane. Figure 3.2 shows the orbital parameters with respect to the Earth's equatorial plane. The co-ordinate system is called the geocentric-equatorial co-ordinate system, which is used to locate the satellite with respect to the Earth.

In this co-ordinate system, the centre of the Earth is the origin, and the xy-plane coincides with the equatorial plane. The z-axis coincides with the Earth's axis of rotation and points in the direction of the North Pole, while the x-axis points to the direction of the vernal equinox. The points at which the satellite moves upward and downward through the equatorial plane are called ascending node and descending node, respectively.

In addition to defining the location of a satellite in space, it is important to determine the direction at which an Earth station's antenna should point to the satellite in order to communicate with it. This direction is defined by the look angles the elevation and azimuth angles in relation to the latitude and the longitude of the Earth station. The following sections discuss the location of the satellite with respect to the different co-ordinate systems.

3.5.2 Algorithm for Satellite Location in the Orbital Plane

For the give earth orbit (Sheriff & Hu, 2001), Step 1

$$\{r\}_{\bar{x}} = \frac{h^2}{\mu}\frac{1}{1+ecos\theta}\begin{pmatrix} cos\theta \\ sin\theta \\ 0 \end{pmatrix} \tag{3.1}$$

Step 2

$$\{v\}_{\bar{x}} = \frac{\mu}{h}\begin{pmatrix} -sin\theta \\ e+cos\theta \\ 0 \end{pmatrix} \tag{3.2}$$

step 3

$$[Q]_{x\bar{x}} = \begin{bmatrix} cos\omega & sin\omega & 0 \\ -sin\omega & cos\omega & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & cosi & sini \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} cos\Omega & sin\Omega & 0 \\ -sin\Omega & cos\Omega & 0 \\ 0 & -sini & cosi \end{bmatrix} \tag{3.3}$$

step 4

First transpose matrix $[Q]_{\bar{x}x}$

The geometric equatorial position vector is

$$\{r\}_X = [Q]_{\bar{x}x}\dot{\{r\}}_{\bar{x}} \tag{3.4}$$

The geometric equatorial velocity vector is

$$\{v\}_X = [Q]_{\bar{x}x}\dot{\{v\}}_{\bar{x}} \tag{3.5}$$

The state vector r and v are shown in figure 3.2, by holding all orbital parameter except the true anomaly fixed and allowing θ to take the range value, we can generate the sequence of position vector $\{r\}_x$ and velocity.

3.5.3 Satellite Location with Respect to the Look Angles

The azimuth angle, ξ is the angle measured North Eastward from the geographic North at the Earth station, G, to the sub-satellite point. The sub-satellite point, S', is defined as the point where the line joining the centre of the Earth, O, and the satellite meets the Earth's surface. The elevation angle, θ, is the angle measured upward from this tangential plane at the Earth station to the direction of the satellite.

Figure 3.3, the angle φ is called the central angle or the coverage angle at the centre of the Earth, O, formed by lines OG and OS, where G denotes the Earth station and S is the satellite. The angle g is called the tilt angle or the nadir angle at the satellite, formed by the lines GS and OS. L_g and l_g represent the latitude and the relative longitude (i.e. relative to the longitude of the sub-satellite point) of the Earth station, respectively and Ls is the latitude of the satellite.

Note: in this co-ordinate system, Northern latitudes and Eastern longitudes are regarded as positive. Furthermore, the latitude of the sub-satellite point is the same as the declination angle, δ, of the satellite with respect to the geocentric-equatorial co-ordinate system, that is $L_s = \delta$. The slant range R of the satellite is its distance from the Earth station.

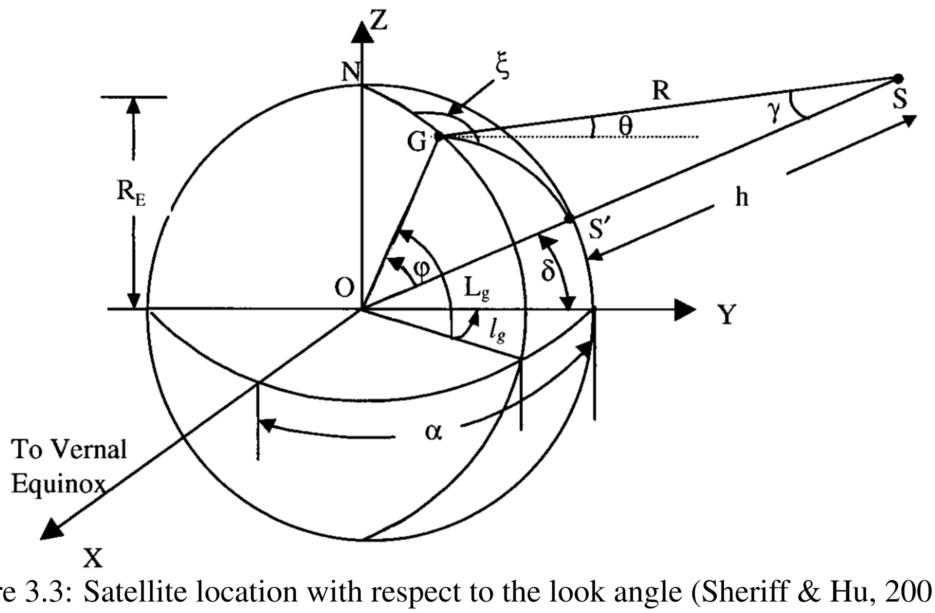


Figure 3.3: Satellite location with respect to the look angle (Sheriff & Hu, 2001).

3.5.3.1 Elevation Angle

In order to calculate the elevation angle θ, the central angle φ and the slant range R have to be determined. The co-ordinates of G in Figure 3.3 are related to its Northern latitude and Eastern longitude by the following (Sheriff & Hu, 2001):

$$\begin{bmatrix} x_g \\ \\ y_g \\ \\ z_g \end{bmatrix} = \begin{bmatrix} R_E cosL_g sinl_g \\ \\ R_E cosL_g cosl_g \\ \\ R_E sinL_g \end{bmatrix} \tag{3.6}$$

where R_E is the radius of the Earth (6378 km).

By analogy, the co-ordinates of the sub-satellite point, $S^{'}$, are related to its Northern latitude and Eastern longitude by the following:

$$\begin{bmatrix} x_s \\ \\ y_s \\ \\ z_s \end{bmatrix} = \begin{bmatrix} 0 \\ \\ R_E cosL_s cosl_s \\ \\ R_E sinL_s \end{bmatrix} \tag{3.7}$$

Consider triangle $OS^{'}G$, the distance, d, between G and $S^{'}$ can be found using the law of cosines:

$$d^2 = 2R_E^2(1 - cos\varphi) \tag{3.8}$$

d can also be obtained from the following equation:

$$d^2 = (x_g - x_s)^2 + (y_g - y_s)^2 + (z_g - z_s)^2 \tag{3.9}$$

Substituting equation (3.6) and (3.7) into equation (3.9) and then equating (3.8) and (3.9) gives:

$$cos\varphi = cosL_g cosL_s cosl_g + sinL_g sinL_s \tag{3.10}$$

Now consider triangle GOS and using the law of cosines again, the slant range, R, is given by

$$R^2 = \sqrt{R_E^2 + (R_E^2 + h)^2 - 2R_E(R_E + h)cos\varphi} \tag{3.11}$$

where h is the altitude of the satellite above the Earth's surface.

By applying the law of sines:

$$\frac{R_e + h}{sin(90\circ + \theta)} R^2 = \frac{R}{sin\varphi} \tag{3.12}$$

where, $sinL_g = \frac{sin\varphi}{sin\gamma} sin\beta$, $cosl_g = \frac{cos\varphi}{cosL_g}$
Substituting above equation into and expressing θ in terms of φ gives:

3.5.3.2 Azimuth Angle

The calculation of the azimuth angle, ξ, is slightly more complicated than that for the elevation angle due to the relative position of the sub-satellite point with respect to the Earth station and the hemisphere on which the sub-satellite point and the Earth station are located. For the time being, consider Figure 3.3 in which the sub-satellite point is in the direction East of the Earth station (Sheriff & Hu, 2001).
Referring to the spherical triangle $GNS^{'}, < GNS^{'} = l_g \ and \ arc(GS^{'}) = \varphi$. Using the law of sines:

$$\frac{sin\varphi}{sin(90 - l_s))} = \frac{sinl_g}{sin\varphi} \tag{3.13}$$

Since $L_s = \delta$, hence

$$\xi = sin^{-1}[\frac{cos\delta sinl_g}{sin\varphi}] \tag{3.14}$$

3.6 Antenna Arrays

An antenna array is a group of similar antennas that are spaced in a regular manner, typically in a line or a grid. It turns out that constructive and destructive interference of the radiation from the individual antennas can create quite desirable radiation patterns for the overall array. In addition, we now have several things we can adjust :

- The number of antennas
- The placement of the antennas
- The amplitude of the signal applied to each antenna
- The phase of the signal applied to each antenna

- The radiation pattern of such an antenna consists of a strong beam in one direction, the main lobe, plus a series of weaker beams at different angles called sidelobes, usually representing residual radiation in unwanted directions. The larger the width of the antenna and the greater the number of component antenna elements, the narrower the main lobe, and the higher the gain which can be achieved, and the smaller the sidelobes will be.

3.7 Array Correlation Matrix

To study the secrecy capacity of mm-Wave systems, we depend on the correlation matrix to reflect the relevance of legitimate receiver's rays and eavesdropper's rays. Moreover, the RF environment decides the elements of correlation matrix. In rich RF setup, such as urban area, the distribution of buildings is very dense, thus the eavesdroppers will receive more paths and have more correlations. In poor RF setup, such as rural area, the distribution of the buildings is sparse, thus the eavesdroppers will receive less paths and have less correlations. Many of the AOA algorithms rely on the array correlation matrix. In order to understand the array correlation matrix, let us begin with a description of the array, the received signal, and the additive noise.

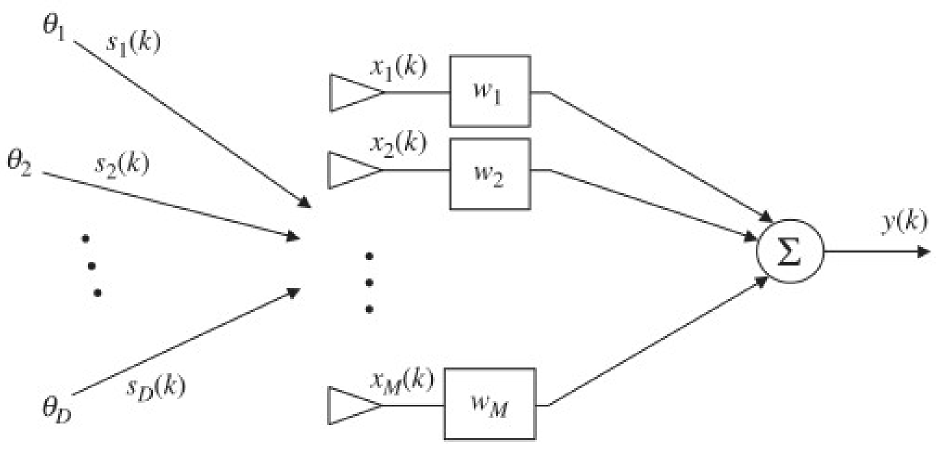


Figure 3.4: M-element array with arriving signals (Nicolaescu & Stoica, 2010).

As shown in Figure 3.4 depicts a receive array with incident plane waves from various directions.

As shown in Figure 3.4 shows D signals arriving from D directions. They are received by an array of M elements with M potential weights. Each received signal $x_m(k)$ includes additive, zero mean, Gaussian noise. Time is represented by the k_{th} time sample. Thus, the array output y can be given in the following form (Nicolaescu & Stoica, 2010):

$$y(k) = \bar{w}^T \cdot \bar{x}(k) \tag{3.15}$$

where

$$\bar{x}(k) = \begin{bmatrix} s_1(k) \\ s_1(k) \\ \vdots \\ s_D(k) \end{bmatrix} \cdot \begin{bmatrix} \bar{a}(\theta_1) & \bar{a}(\theta_2) & \dots & \bar{a}(\theta_D) \end{bmatrix} \tag{3.16}$$

$$= \bar{A} \cdot^T \bar{s}(k) + \bar{n}(k)$$

and

$$\bar{w} = \begin{bmatrix} w_1 & w_2 & \dots & w_D \end{bmatrix}^T = arrayweights$$

$\bar{s}(k)$= vector of incident complex monochromatic signals at time k.

$\bar{n}(k)$ = noise vector at each array element m, zero mean, variance σ_n^2.

$\bar{a}(\theta_i)$ = M-element array steering vector for the θ_i direction of arrival.

$\bar{A} = \begin{pmatrix} \bar{a}(\theta_1) & \bar{a}(\theta_2) & \dots & \bar{a}(\theta_D) \end{pmatrix}$ $M \times D$ matrix of steering vectors $\bar{a}(\theta_i)$

Thus, each of the D-complex signals arrives at angles θ_i and is intercepted by the M-antenna elements. It is initially assumed that the arriving signals are monochromatic and the number of arriving signals $D < M$. It is understood that the arriving signals are time varying and thus our calculations are based upon time snapshots of the incoming signal. Obviously if the transmitters are moving, the matrix of steering vectors is changing with time and the corresponding arrival angles are changing. Unless otherwise stated, the time dependence will be suppressed in equation (3.15) and (3.16). In order to simplify the notation let us define the $M \times M$ array correlation matrix $\bar{R}_{xx}$ as (Chang & Hu, 2012),

$$\bar{R}_{xx} = E[\bar{x} \cdot \bar{x}^H] = E[(\bar{A}\bar{s} + \bar{n})(\bar{s}^H \bar{A}^H + \bar{n}^H)] = \bar{A}\bar{R}_{ss}\bar{A}_H + \bar{R}_{nn} \tag{3.17}$$

Where,

$\bar{R}_{ss}$ =$D \times D$ source correlation matrix

$\bar{R}_{nn}$ = σ_n^2 $\bar{I}$ = $M \times M$ noise correlation matrix(channel model)

$\bar{I}$ = $N \times N$ identity matrix

3.8 DoA Estimation Methods

3.8.1 MUSIC DoA Estimate

MUSIC is an acronym which stands for ***MU**ltiple **SI**gnal **C**lassification*. This approach was first posed by and is a popular high resolution eigenstructure method.

One must search the eigenvalue to determining the number of incoming signals. If the number of signals is D, the number of signal eigenvalues and eigenvectors is D, and the number of noise eigenvalues and eigenvectors is $M-D$ (M is the number of array elements). Because MUSIC exploits the noise eigenvector subspace, it is sometimes referred to as a *sub-space method*.

The noise sub-space eigen-vectors are orthogonal to the antenna array steering-vectors at the angles of arrival θ_1, θ_2, ... , θ_D. Because of this orthogonality condition, one can show that the Euclidean distance d_2= $\bar{a}(\theta)^H$ $\bar{E}_N\bar{E}_N^H$ $\bar{a}(\theta) = 0$ for each and every arrival angle θ_1, θ_2, ... , θ_D. Placing this distance expression in the denominator creates sharp peaks at the angles of arrival (Shen, Liu, Wang, & Liu, 2020). The MUSIC pseudospectrum is now given as

$$P_{MU}(\theta) = \frac{1}{\|\bar{a}(\theta)^H \bar{E}_N \bar{E}_N^H \bar{a}(\theta)\|} \tag{3.18}$$

where

$$\bar{E}_N = \begin{pmatrix} \bar{e}(\theta_1) & \bar{e}(\theta_2) & \dots & \bar{e}(\theta_{M-D}) \end{pmatrix} \tag{3.19}$$

In the more practical application we must collect several time samples of the received signal plus noise, assume ergodicity, and estimate the correlation matrices via time averaging. We can repeat in equation (3.20) without assuming that we know the signal statistics.

$$\hat{R}_{xx} = E[\bar{x}(k)\cdot\bar{x}^H(k)] \approx \frac{1}{k}\sum_{k=1}^{k}\bar{x}(k)\cdot\bar{x}^H(k) \approx \bar{A}\hat{R}_{ss}\bar{A}_H + \bar{A}\hat{R}_{ns} + \hat{R}_{sn}\bar{A}_H + \hat{R}_{nn} \tag{3.20}$$

3.8.2 Min-norm AOA estimate

The min-norm algorithm optimizes the weight vector by solving the optimization problem where (Leong, 2008),

$$\min_{\bar{w}} \bar{w}^H\bar{w} \quad \bar{E}_S^H\bar{w} = 0 \quad \bar{w}^H\bar{u} = 1 \tag{3.21}$$

where

$\bar{w}$= array weights

$\bar{E}_S$ = subspace of D signal eigenvectors = $[\bar{e}_{M-D+1} \;\; \bar{e}_{M-D+2} \; \dots \; \bar{e}_M]$

M = number of array elements

D = number of arriving signals

$\bar{u}_1$ = Cartesian basis vector (first column of the $M \times M$ identity matrix)

=$[1 \; 0 \; 0 \; \dots \; 0]^T$

The solution to the optimization yields the min-norm pseudospectrum

$$P_{MN}(\theta) = \frac{(\bar{u}_1^T \bar{E}_N \bar{E}_N^H \bar{u}_1)^2}{|\bar{a}(\theta)^H \bar{E}_N \bar{E}_N^H \bar{u}_1|^2} \tag{3.22}$$

where

$\bar{E}_N$ = subspace of $M-D$ signal eigenvectors = $[\bar{e}_1 \;\; \bar{e}_2 \; \dots \; \bar{e}_{M-D}]$

$\bar{a}(\theta)$= array steering vector

Since the numerator term in equation (3.22) is a constant, we can normalize the pseudospectrum such that

3.9 Adaptive beamforming Algorithms

The fixed beamformer approaches, which included the maximum SIR, the ML-method, and the MV-method were assumed to apply to fixed-arrival-angle emitters. If the direction of arrival don't changing with time, the optimum antenna array weights will not need to be adjusted. However, if the desired direction change with time, it is necessary to devise an optimization schemes that operates on the fly so as to keep recalculate the optimum antenna array weight. The receiver signal processing algorithms then must allow for the continuous adaptation to an ever change electro-magnetic environment. The adaptive algorithms takes the fixed-beamforming processes one step further and allows for the calculation of continuously updated weights. The adaptation process must satisfy a specified optimization criterion. Several examples of popular optimization techniques will discuss and explain some important one for this work (Ibrahim et al., 2017).

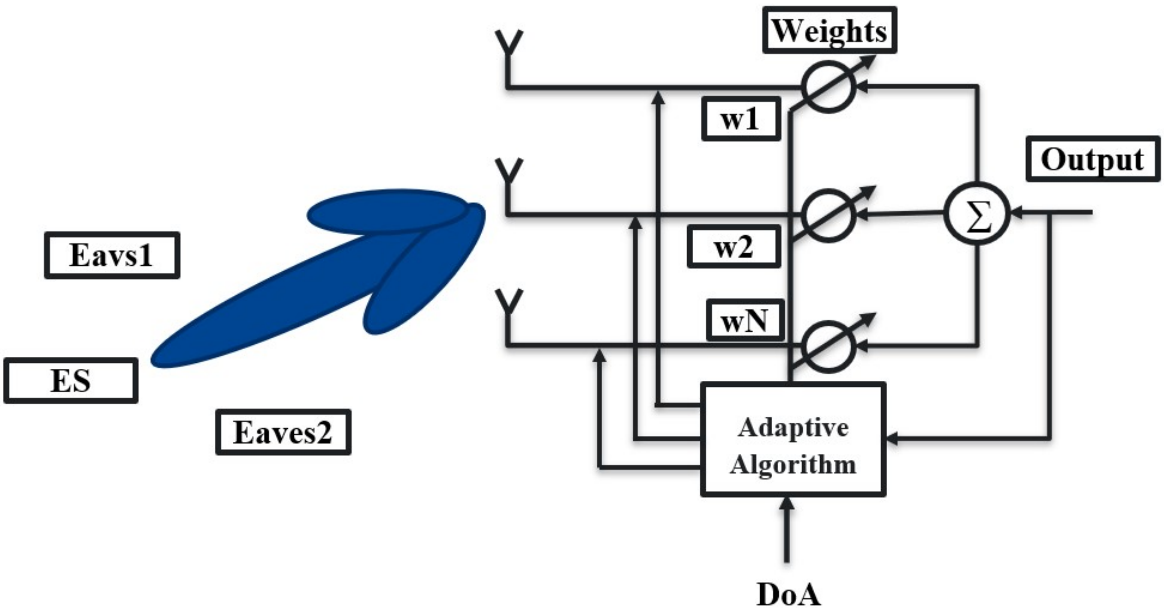


Figure 3.5: Adaptive beamforming system, ES- for Earth station, and Eaves-for Eavesdroppers.

Table 3.3: Summary of Adaptive beamforming algorithms

Algorithm	Advantages	Disadvantages
Least Mean Square(LMS)	Always converges and a simple algorithm	Requires reference signal Slow rate of convergence for large Eigen value spread
Recursive Least Square(RLS)	Always converges and has the fast rate of convergence	Requires initial estimate of $-R_{xx}$ Forgetting factor is dependent on the fading rate of the channel

3.9.1 Least Mean Squares

The least mean squares algorithm is a gradient based approach. Gradient based algorithms assume an established quadratic performance surface. When the performance surface is a quadratic function of the array weights, the performance surface $J(\bar{w})$ is in the shape of an elliptic paraboloid having one minimum. One of the best ways to establish the minimum is through the use of a gradient method. We can establish the performance surface (cost function) by again finding the MSE. The error (Ibrahim et al., 2017), (Balanis & Ioannides, 2007):

$$e(k) = d(k) - \bar{w}^H(k)\bar{x}(k) \tag{3.23}$$

The squared error is given as

$$|e(k)|^2 = |d(k) - \bar{w}^H(k)\bar{x}(k)|^2 \tag{3.24}$$

Momentarily, we will suppress the time dependence. The cost function is given as

$$J(\bar{w}) = D - 2\bar{w}^H\bar{r} + \bar{w}^H\bar{R}_{xx}\bar{w} \tag{3.25}$$

where

$$D = E[|d|^2] \tag{3.26}$$

We may employ the gradient method to locate the minimum of equation (3.25). Thus

$$\Delta(J(\bar{w})) = 2\bar{R}_{xx}\bar{w} - 2\bar{r} \tag{3.27}$$

The minimum occurs when the gradient is zero. Thus, the solution for the weights is the optimum Wiener solution as given by

$$w_{opt} = \bar{R}_{xx}\bar{w}^{-1}\bar{r} \tag{3.28}$$

The solution in equation (3.28) is predicated on our knowledge of all signal statistics and thus in our calculation of the correlation matrix.
In general, we do not know the signal statistics and thus must resort to estimating the array correlation matrix ($\bar{R}_{xx}$) and the signal correlation vector ($\bar{r}$) over a range of snapshots or for each instant in time.
The instantaneous estimates of these values are given as

$$\hat{R}_{xx}(k) \approx \bar{x}(k)\bar{x}^H(k) \tag{3.29}$$

and

$$\hat{r}(k) \approx \bar{d}^*(k)\bar{x}(k) \tag{3.30}$$

We can employ an iterative technique called the method of steepest descent to approximate the gradient of the cost function. The direction of steepest descent is in the opposite direction as the gradient vector. The method of steepest descent can be approximated in terms of the weights using the LMS method advocated. The steepest descent iterative approximation is given as

$$\bar{w}+1 = \bar{w}(k) - \frac{1}{2}\mu\Delta_{\bar{w}}(J(\bar{w}(k))) \tag{3.31}$$

where, μ is the step-size parameter and Δ is the gradient of the performance surface. The gradient of the performance surface is given in equation (3.27). If we substitute the instantaneous correlation approximations, we have the LMS solution.

$$\bar{w}+1 = \bar{w}(k) - \mu[\bar{R}_{xx}\bar{w} - r] = \bar{w}(k) + \mu e*(k)\bar{x}(k) \tag{3.32}$$

where

$$e(k) = \bar{d}(k) - \bar{w}^H(k)\bar{x}(k) \;=\; errorsignal \tag{3.33}$$

The convergence of the LMS-algorithm in equation (3.33) is directly proportional to the step-size parameter μ. If the step size is small, the convergence speed is slow and we can have the overdamped case. If the convergence speed is slower than the changing direction of arrival, it is possible that the adaptive antenna array cannot acquire the signal of interest faster enough to track the changing signal. If the step size is larger, the LMS-algorithm will over-shoot the optimum weight of interest. This is called the underdamped case.

$$0 \;\leq \mu \leq \; \frac{1}{2\lambda_{max}} \tag{3.34}$$

where λ_{max} is the largest eigenvalue of $\hat{R}_{xx}$.

Since the correlation matrix is positive definite, all eigenvalues are positive. If all the interfering signals are noise and there is only one signal of interest, we can approximate the condition in equation (3.34) as

$$0 \;\leq \mu \leq \; \frac{1}{2trace[\hat{R}_{xx}]} \tag{3.35}$$

Table 3.4: Least Mean-Square Algorithm

for each k
{
$e(k) = d(k) - \bar{w}^H(k)\bar{x}(k)$
$\bar{w}_{k+1} = \bar{w}(k) - \mu[\bar{R}_{xx}\bar{w} - r] = \bar{w}(k) + \mu e*(k)\bar{x}(k)$
}

3.9.2 Recursive Least Squares

RLS is one of the most popular adaptive beam-forming algorithms based on recursive least square. This algorithm requires no matrix inversion because correlation matrix is found directly. It uses the sum of squared errors for the inputs to update the complex weights instead of using the mean square error minimization.

The computational burden and potential singularities can cause problems. However, we can easily recursively calculate the require correlation-matrix and the correlation-vector. Recall that in the estimate of the correlation-matrix and vector was taken as the sum of the terms divided by the block length K. When we calculate the weights, the division by K is cancelled by the product $\bar{R}_{xx}^{-1}(k)\bar{r}(k)$. Thus, we can rewrite the correlation-matrix and the correlation-vector omitting K as (Ibrahim et al., 2017) (Balanis & Ioannides, 2007):

$$\hat{R}_{xx} = \sum_{i=1}^{k} \bar{x}(i)\bar{x}^H(i) \tag{3.36}$$

$$\bar{r}(k) = \sum_{i=1}^{k} d^*(i)\bar{x}(i) \tag{3.37}$$

where k is the block length and last time sample k and $\hat{R}_{xx}$, $\bar{r}(k)$ is the correlation estimates ending at time sample k.

Both summations use rectangular windows, thus they equally consider all previous time samples. Since the signal sources can change or slowly move with time, we might want to deem phasize the earliest data samples and emphasize the most recent ones. This can be accomplished such that we forget the earliest time samples. This is called a *weighted estimate*.

$$\hat{R}_{xx}(k) = \sum_{i=1}^{k} \alpha^{k-i}\bar{x}(i)\bar{x}^H(i) \tag{3.38}$$

$$\hat{r}(k) = \sum_{i=1}^{k} \alpha^{k-i} d^*(i)\bar{x}(i) \tag{3.39}$$

where α is the forgetting factor.

The forgetting factor is also sometimes referred to as the exponential weighting factor. α is a positive constant such that $0 \leq \alpha \leq 1$. When $\alpha = 1$, we restore the ordinary least squares algorithm. $\alpha = 1$, also indicates infinite memory. Let us break up the summation in equation (3.38) and (3.38) into two terms: the summation for values up to $i = k-1$ and last term for $i = k$

$$\hat{R}_{xx}(k) = \alpha \sum_{i=1}^{k} \alpha^{k-1-i} \bar{x}(i)\bar{x}^H(i) + \bar{x}(k)\bar{x}^H(k) = \alpha \hat{R}_{xx}(k-1) + \bar{x}(k)\bar{x}^H(k) \tag{3.40}$$

$$\hat{r}(k) = \alpha \sum_{i=1}^{k} \alpha^{k-1-i} d^*(i)\bar{x}(i) + d^*(k)\bar{x}(k) = \alpha \hat{r}(k-1) + d^*(k)\bar{x}(k) \tag{3.41}$$

Thus, future values for the array correlation estimate and the vector correlation estimate can be found using previous values.

Not only can we recursively calculate the most recent correlation estimates, we can also use equation (3.40) to derive a recursion relationship for the inverse of the correlation matrix. The next steps follow the derivation in. We can invoke the Sherman Morrison-Woodbury(SMW) theorem (Van Loan & Golub, 1996) to find the inverse of equation (3.40). Repeating the SMW theorem

$$(\bar{A} + \bar{z}\bar{z}^H)^{-1} = \bar{A}^{-1} - \frac{\bar{A}^{-1}\bar{z}\bar{z}^H\bar{A}^{-1}}{1 + \bar{z}^H\bar{A}^{-1}\bar{z}} \tag{3.42}$$

Applying equation (3.42) to (3.40), we have the following recursion formula:

$$\hat{R}_{xx}(k)^{-1} = \alpha^{-1}\hat{R}_{xx}^{-1}(k-1) - \frac{\alpha^{-2}\hat{R}_{xx}^{-1}(k-1)\bar{x}(k)\bar{x}^H(k)\hat{R}_{xx}^{-1}(k-1)}{1 + \alpha^{-1}\bar{x}^H(k)\hat{R}_{xx}^{-1}(k-1)\bar{x}(k)} \tag{3.43}$$

We can simplify equation (3.43) by defining the gain vector $\bar{g}(k)$

$$\bar{g}(k) = \frac{\alpha^{-1}\hat{R}_{xx}^{-1}(k-1)\bar{x}(k)}{1 + \alpha^{-1}\bar{x}^H(k)\hat{R}_{xx}^{-1}(k-1)\bar{x}(k)} \tag{3.44}$$

Thus

$$\hat{R}_{xx}^{-1}(k) = \alpha^{-1}\hat{R}_{xx}^{-1}(k-1) + \alpha^{-1}\bar{x}^H(k)\hat{R}_{xx}^{-1}(k-1) \tag{3.45}$$

Equation (3.45) is known as the Riccati equation for the recursive least squares (RLS) method. We can rearrange equation (3.44) by multiplying the denominator times both sides of the equation to yield

$$\bar{g}(k) = [\alpha^{-1}\hat{R}_{xx}^{-1}(k-1) + \alpha^{-1}\bar{x}^{H}(k)\hat{R}_{xx}^{-1}(k-1)]\bar{x}(k) \tag{3.46}$$

It is clear that the term inside of the brackets of equation (3.46) is equal to equation (3.45). Thus

$$\bar{g}(k) = \hat{R}_{xx}^{-1}(k)\bar{x}(k) \tag{3.47}$$

Now we can derive a recursion relationship to update the weight vectors. The optimum Wiener solution is repeated in terms of the iteration number k and we can substitute equation (3.47) yielding

$$\bar{w}(k) = \hat{R}_{xx}^{-1}(k)\bar{r}(k) = \alpha\hat{R}_{xx}^{-1}(k)\bar{r}(k-1) + \hat{R}_{xx}^{-1}(k)\bar{x}(k)d^{*}(k) \tag{3.48}$$

We may now substitute equation (3.45) into the first correlation matrix inverse seen in equation (3.48).

$$\begin{aligned} \bar{w}(k) &= \hat{R}_{xx}^{-1}(k-1)\bar{r}(k-1) - \bar{g}(k)\bar{x}^{H}(k)\hat{R}_{xx}^{-1}(k-1)\bar{r}(k-1) + \hat{R}_{xx}^{-1}(k)\bar{x}(k)d^{*}(k) \\ &= \bar{w}(k-1) - \bar{g}(k)\bar{x}^{H}(k)\bar{w}(k-1) + \hat{R}_{xx}^{-1}(k)\bar{x}(k)d^{*}(k) \end{aligned} \tag{3.49}$$

Finally we may substitute equation (3.47) into equation (3.49) to yield. The following equation is used to update the weight values.

$$\begin{aligned} \bar{w}(k) &= \bar{w}(k-1) - \bar{g}(k)\bar{x}^{H}(k)\bar{w}(k-1) + \bar{g}(k)d^{*}(k) \\ &= \bar{w}(k-1) - \bar{g}(k)[d^{*}(k) - \bar{x}^{H}(k)\bar{w}(k-1)] \end{aligned} \tag{3.50}$$

Table 3.5: Recursive Least Squares

$R^{-1}(0) = \delta^{-1}I, \delta smallpositiveconstantand$
$ItheN \times Nidentitymatrix, \delta\ smallpositiveconstantand$
for each k
{
$k(k) = R^{-1}(k-1)x(k)$
$k(k) = \frac{k(k)}{\lambda + x^H(k)k(k)}$
$R^{-1}(k) = \frac{1}{\lambda}[R^{-1}(k-1) - \frac{k(k)k^H(k)}{\lambda + x^H(k)k(k)}]$
$e(k) = d(k) - \bar{w}^H(k)\bar{x}(k)$
$\bar{w}_{k+1} = \bar{w}(k) + e^*(k)k(k)$
}

where $\bar{u}_1^T$ is the Cartesian basis vector whose length equals the total number of sources.

3.10 Secrecy Capacity

The wire-tap channel in Figure 3.6 is considered. Here, the transmitter services two terminals with their own confidential messages. Hence, each terminal acts as an eavesdropper for the other.

The transmitter, the intended receiver and the eavesdropper have n_t, n_r and n_e antennas, respectively. The main channel and the eavesdropper's channel experiences quasi-static Rayleigh fading and Additive White Gaussian Noise (AWGN). The power is constrained according to $\frac{1}{n}\sum_{i=1}^{n} E[x(i)^2] \leq P$.

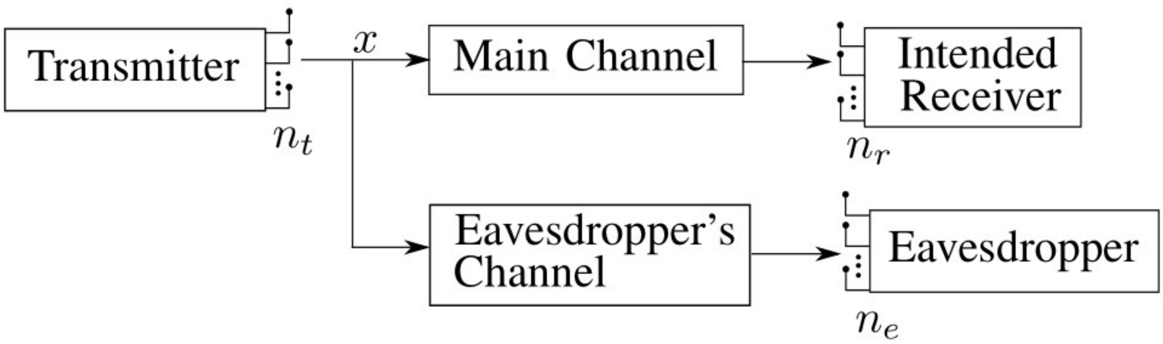


Figure 3.6: The wiretap channel with nt antennas at the transmitter, n_r antennas at the intended receiver and n_e antennas at the eavesdropper (Barros & Rodrigues, 2006).

In a similar way to that for the broadcast channel, the wiretap channel with confidential messages has been subsequently extended into several directions as well.

For this instance, the secrecy capacity is given by (Sreekumar, Bunin, Goldfeld, Permuter, & Shamai, 2020) and (Barros & Rodrigues, 2006):

$$C_s = C_M - C_W, \tag{3.51}$$

where

$$C_M = log_2(1 + \frac{P}{N_M}) \tag{3.52}$$

is the capacity of the main channel and

$$C_W = log_2(1 + \frac{P}{N_W}) \tag{3.53}$$

denotes the capacity of the eavesdropper's channel.

where P corresponds to the average transmit signal power. Furthermore, we denote the power of the noise in the main channel and the eavesdropper's channel as N_M and N_W , respectively.

3.11 System Flowchart

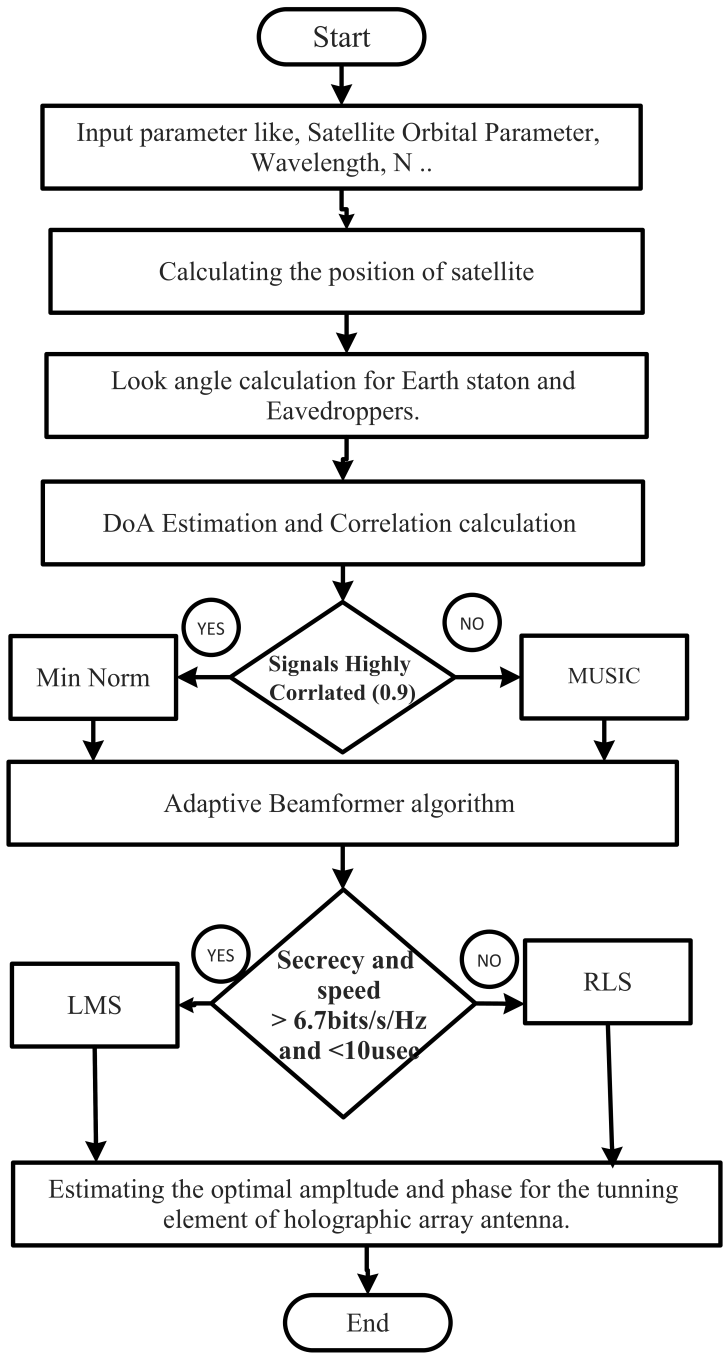


Figure 3.7: System flowchart

CHAPTER FOUR
4. RESULTS AND DISCUSSIONS

4.1 Introduction

In this thesis, presented and evaluate an efficient secure architecture of the adaptive transmission beamformer for multi-beam satellite system for 6G services. the system consisted of an DoA estimator and an adaptive beamforming algorithm. In order to efficiently send the signal information for the earth station, we employed the MUSIC and Min-Norm algorithm for the DoA estimator and the LMS and RLS beamformer for the enhancing directivity to earth station and rejecting(minimizing power leakage) eavesdropper. In order to track the position/location of the earth station look angle calculation is need. this adaptive beamformer will generate error signal, which is the amplitude and phase applicable for the tuning element of holographic array antenna.

4.2 Simulation Results

4.2.1 Antenna Look Angles

Distinct characteristics related to different references complicate the typical conditions of a satellite in an inclined-elliptical-orbit. The orbital elements are recognized in terms of the orbital plane, which has a constant (or slowly varying) location in space, The earth station's position is commonly specified in terms of local geographic coordinates that revolve with the earth. Rectangular coordinate systems are extensively used in space to compute satellite position and velocity, azimuth and elevation angles, as well as the earth station's range, it may be useful. As a result, It is important to perform transformations across coordinate systems. Here, to illustrate how to calculate elliptical inclined orbits, It will be discussed how to determine earth station look angles and eavesdropper range. It's crucial to keep in mind that satellites in inclined orbits are in low Earth orbit(LEO), and therefore, Time will affect the needed look angles and range.

Table 4.1: Satellite Orbital Parameter to calculate state vector

Satellite Orbital Parameter	
Angular Momentum(km^3/s^2)	21867.4
Eccentricity	0.91028
Right ascension(sec)	13361.2
Inclination(deg)	97.134
Argument of perigee(deg)	0
True Anomaly(deg)	0

From the above orbital parameter as shown in table 4.1, From the given parameter we can calculate the state position and velocity vector equation (4.1) and (4.2):

$$r[km] = \begin{bmatrix} 472.3 & 413.905 & 0 \end{bmatrix} \tag{4.1}$$

$$v[km/s] = \begin{bmatrix} 2.85013 & -3.25224 & 34.5511 \end{bmatrix} \tag{4.2}$$

So after getting the position and velocity vector, easily we can find the location of the satellite i.e the latitude and longitude of the satellite as shown in table 4.2 and then we can calculate the look angle(Azimuth and Elevation) of the earth station as shown in table 4.3.

Table 4.2: Satellite location

Satellite location	
Longitude(East)	41.23°
Latitude(North)	0°

The measurements azimuth and elevation are used to determine the position of a satellite flying above. Azimuth indicates which way to gaze, whereas Elevation indicates how far up in the sky to look. Both are expressed in terms of degrees. Azimuth ranges from 0° to 360°. It all begins at 0° North. As you move to the right(in a clockwise direction), The direction you'll be facing is East (which is 90°), then South (which is 180°), then West (which is 270°), and then return to North (which is 360° and also 0°). So, if your satellite's azimuth is, say, 45°, This indicates that your satellite is to the northeast of you. At 0° Elevation, a satellite just just rises over your horizon, and at 90 degrees elevation, a satellite would be straight overhead(”zenith”). This thesis work simulation runs only on the direction of azimuth, since the elevation related to altitude, it will be nearly identical in specific region.

Table 4.3: Antenna Look Angles (Garuma et al., 2020)

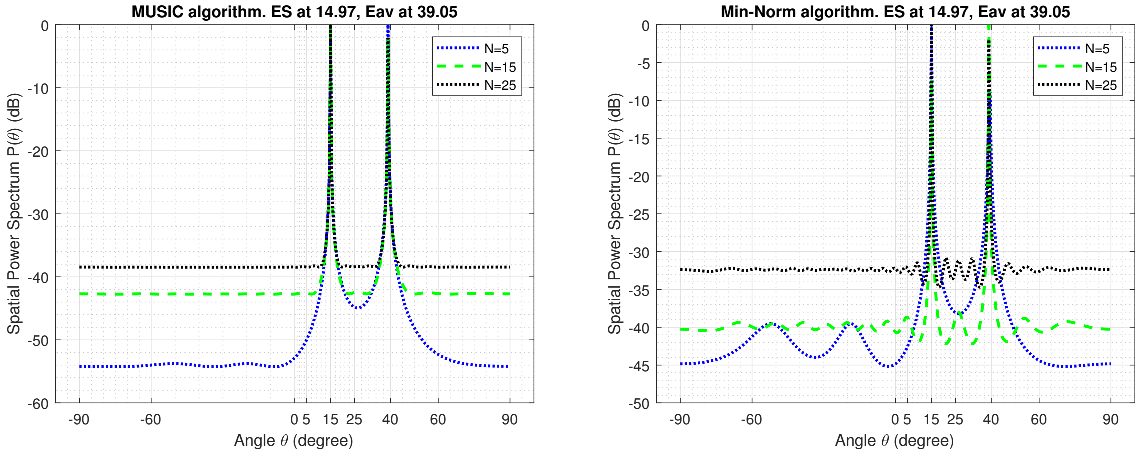
	Latitude and Longitude	Elevation	Azimuth
Earth station	9.80°N and 38.70° E	78.07°	14.97°
Eavs1	8.24°N and 34.59°E	77.56°	39.05°
Eavs2	7.0504°N and 38.49°E	81.10°	21.26°
Eavs3	9.31°N and 42.13°E	78.99°	5.53°

4.3 Direction of Arrival(DOA) estimation Algorithms

For the goal of assisting satellite accuracy by mitigating the effects of earth stations, the use of adaptive arrays antenna can be practical. With adaptive antenna array algorithms, it is feasible to create a beamformer that places nulls in the eavesdropper signal’s direction. Spatial reference beamformer uses to synthesize beam-steering to the earth station using the DoA information included in the received signals and place nulls in the direction of the eavesdropper. Therefore, in order to effectively reject eavesdropper signals, Estimating the angle of arrival of various sources is crucial(earth station) correctly. The capability of DoA techniques such as the MUSIC/Min-Norm algorithm to determine the number of multi-path contribution depends on the number of antenna elements and the aperture of antenna.

4.3.1 Evaluation of DOA estimation with the number of array elements variation

The simulation shows there are earth station and eavesdroppers narrow band signals, the azimuth angle is 14.97° and 39.05° respectively, those two signals are not highly correlated, the noise is ideal Gaussian-white-noise, the SNR is 20dB, the element spacing is half of the input signal wavelength, array element number is 5, 15, and 25. The simulation results MUSIC and MIN-norm algorithms are shown in figure 4.1(a)and (b) respectively:



(a) MUSIC algorithm at $d = \lambda/2$ (b) Min-norm algorithm at $d = \lambda/2$

Figure 4.1: DOA estimation with the variation of number of array elements.

As shown in figure 4.1 (a) and (b) for both algorithm, the blue color shows N=5, the green color shows N=15, and N=25. Other circumstances remained the same and as the number of antenna components grows, DoA estimation spectral beam-width becomes narrow, better the directivity, The capacity to distinguish between earth stations has improved. Hence, to acquire more accurate DOA estimates, the number of array components should be increased, However, the greater the number of array items, the more data processing is required; and the more amount of computation, the lower the speed.

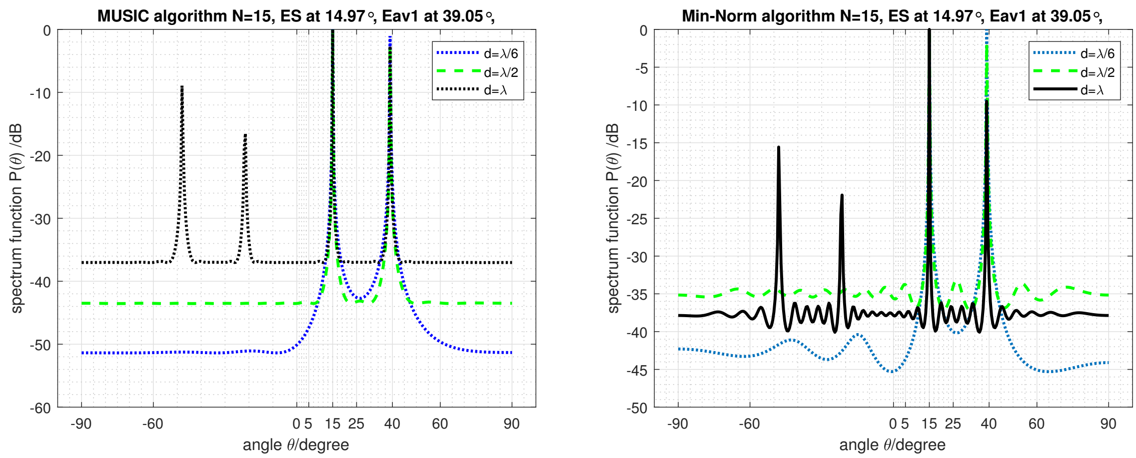
From the above figure 4.1 (a) and (b), in both MUSIC and Min-Norm when the number of the array elements amounts to 5, 15 and 25, their beam width is very similar. Min-Norm fails to suppress the erroneous/incorrect peaks, Consequently, it performs poorly in comparison to the MUSIC algorithm. Therefore, in practice, The number of antenna element can be suitably chosen based on the circumstances, and We ensure that the spectrum estimations are accurate.

Table 4.4: Summary-DoA estimation with the number of array elements variation

Algorithm	Resolution	Accuracy
MUSIC	High	High
Min-Norm	High	Low(incorrect peaks)

4.3.2 Evaluation of DOA estimation with Different array element spacing

As can be seen from Figure 4.2 (a) and (b), the blue line shows at d= $\lambda/6$, the green line shows at d= $\lambda/2$, and the black line shows at d= λ. Other circumstances remained the same, N=15 and as the separation distance of array antenna element grows, The DOA estimate spectrum's beam-width narrows, better directivity, With increasing antenna array element spacing, the MUSIC and Min-Norm algorithms' resolution increases, however, when the antenna array components have a separation of more than 0.5λ, shows false peaks in addition to the signal source direction. As a result, the accuracy of estimate has been compromised. As a result, in real applications, the spacing of the antenna array elements should be given additional consideration. It is recommended that you use a 0.5λ element spacing.

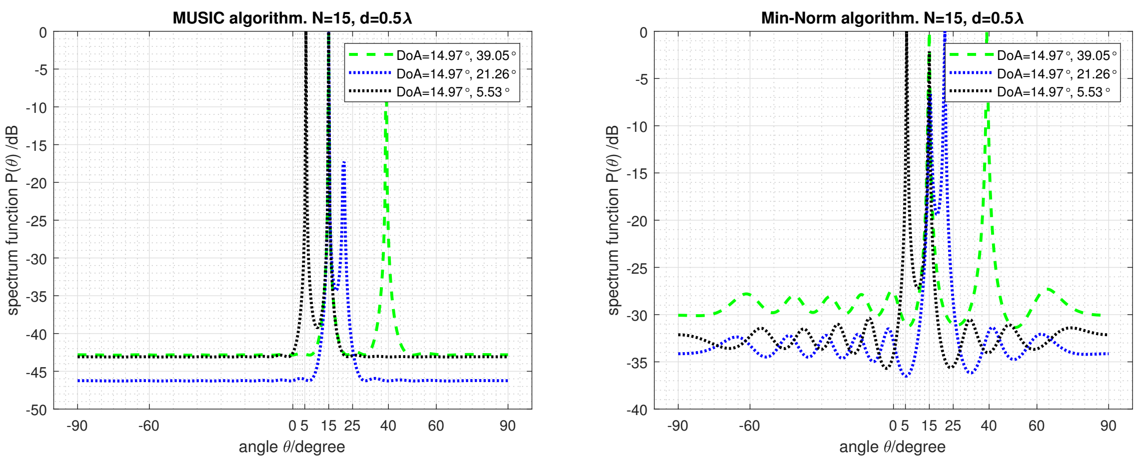


(a) MUSIC algorithm, $N = 10$ (b) Min-norm algorithm, $N = 10$

Figure 4.2: DOA estimation with the variation of array element spacing

4.3.3 Evaluation of DOA estimation with the Signal incident angle variation

As can be seen from Figure 4.3 (a) and (b), Earth station at ES=14.97° the green color shows the azimuth angle of Eaves1= 39.05° , the the blue color shows the azimuth angle Eaves2= 21.26° and the black color line shows the azimuth angle is Eaves3=5.53° the deviation between the earth station to eavesdropper is 24.08°, 6.29° and 9.44°. .



(a) MUSIC algorithm, $N = 15,\ d = \lambda/2$ (b) Min-norm algorithm, $N = 15,\ d = \lambda/2$

Figure 4.3: DOA estimation with the variation of Signal incident angle.

With the other circumstances remaining the same and the DoA difference increasing, The

DOA estimate spectrum's beam width narrows, revealing the signal's direction and MUSIC resolution and the Min-norm algorithm's resolution have both been improved. when the deviation between earth station to eavesdropper smaller(highly correlated) in simulation, Eaves3=5.53° the deviation equal to 6.29°, In this case, the MUSIC algorithm is unable to estimate the number of signal sources in the same way as the Min-norm method can.

Table 4.5: Summary-DoA estimation with the Signal incident angle variation

Algorithm	Resolution	Accuracy
MUSIC	Low(at highly correlated signals)	High
Min-Norm	High	Low(incorrect peaks)

4.4 Holographic Array Antenna

To enable the creation of a global intelligent information network, Antenna array technology must meet strict standards for 6G wireless communications. such as precise beam-steering and capacity expansion. Fortunately, benefiting from the tunability and programm-ability of the meta-material. The holographic pattern, as well as the accompanying desired beam directions, may be readily re-configured by changing the meta-electro-magnetic material's response. As shown in table 4.6, Specifically, To create the appropriate beams according to the holographic pattern, each element may electronically adjust the reference wave's amplitude and phase.

Table 4.6: Amplitude and Phase change for each algorithm

LMS algorithm Amplitude and Phase change		RLS algorithm Amplitude and Phase change	
Amplitude(v)	Phase(rad)	Amplitude(v)	Phase(rad)
1.0000	0	1.0000	0.2366
0.4099	0.1350	0.8646	0.8123
0.2309	1.7043	0.8393	-0.3697
0.5193	-3.0437	1.1445	1.1304
1.0569	-2.8571	4.4605	-3.0268

4.5 Performance Evaluation of Adaptive Beamforming Algorithm

In this section, For simulations, we'll use a with a W-band(75–110)GHz operating frequency is considered for simulations. The Earth station receives a cosine signal from the satellite at an angle of 14.97°. Eavesdroppers is taken into account from various angles. of Eves1= 39.05°, Eves2=21.26° and Eves3=5.53°.

The next section shows how changing the number of antenna elements (N) affects the beamformer of the LMS and RLS algorithms. The beam is steered enhanced directivity to the earth station ES=14.97° and the null-depth is produced along the eavesdroppers' directions at Eves1= 39.05°, Eves2=21.26° and Eves3=5.53°.

4.5.1 Evaluation of varying distance between antenna element spacing

It is dependent on the frequency and is measured relative to the wavelength. Figure 4.4 and Figure 4.5 The influence of antenna element spacing and the occurrence of grating-lobes is shown.

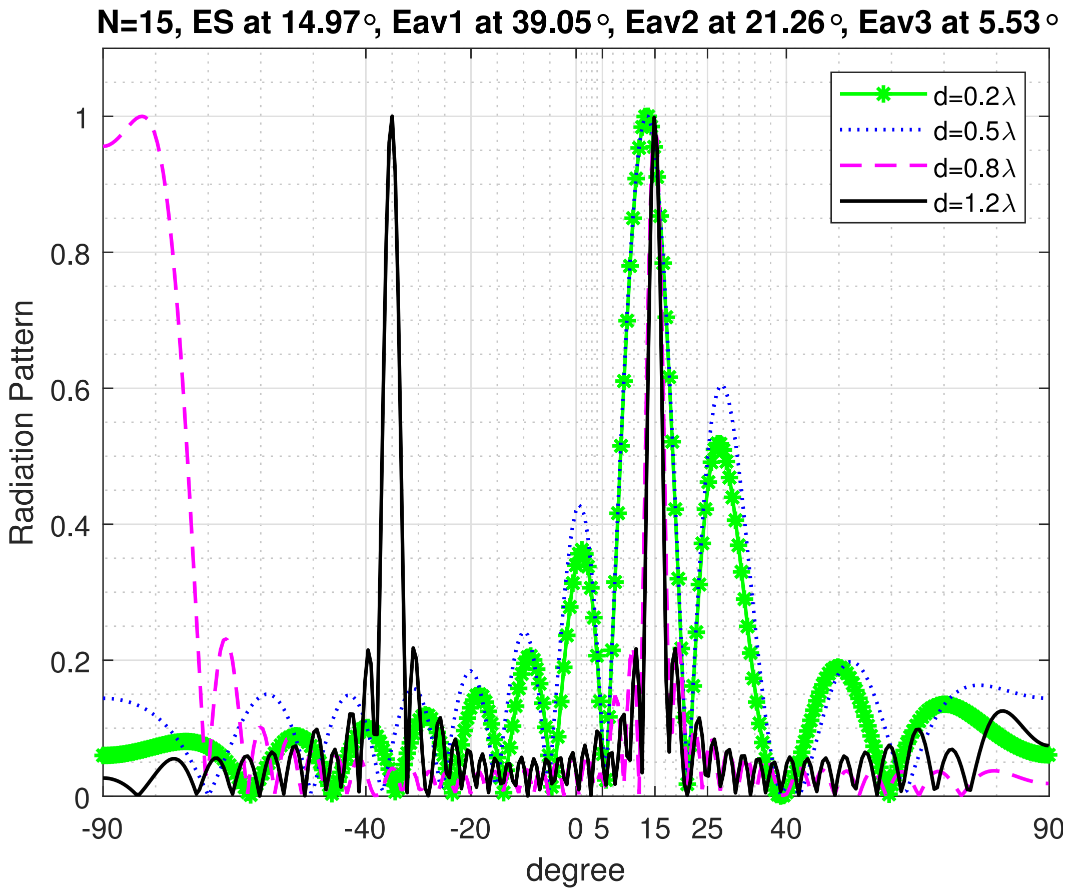


Figure 4.4: LMS beamforming algorithm.

For Both algorithm, When the array antenna element spacing in an array is less than 0.5λ, The null depth is very low(low power leakage) and the side lobe level (SLL) is very high as shown in Figure 4.4 and Figure 4.5 for d=0.2λ. If the array antenna element spacing (d) is increased to a value greater than 0.5λ, As the beamwidth narrows, the directivity increases.

Table 4.7: Relative power level analysis for LMS algorithm with d variation

d	Earth station Main lobe(dB)	Eavesdroppers Null Depth(dB)		
	ES at 14.97°	Eav1 at 39.09°	Eav2 at 21.26°	Eav3 at 5.53°
0.2	-0.2001	-19.065	-15.5259	-16.2342
0.5	-0.0809	-29.1435	-18.7063	-17.7833
0.8	-0.0116	-24.84	-17.724	-19.1487
1	-0.0073	-21.33	-17.2011	-19.0448

Table 4.8: LMS- Beamwidth and Max Sidelobes level(SLL) with d variation

d	Beamwidth	Max. SLL(dB)
0.2	15.46	-0.7418
0.5	15.46	-2.1969
0.8	5.73	-0.0056
1	5.73	-0.0231

In terms of resolution, spacing less than 0.5λ will not be able to improve the array's beamforming performance. Grating-lobes are created by element spacing that is more than 0.5λ. Furthermore, The distance between the points is more than 0.5λ. The performance of the beamformer is being harmed by the appearance of other main unnecessary beams. Thus, the 0.5λ is chosen to get the optimal aperture rather than harming lobes near the horizon.

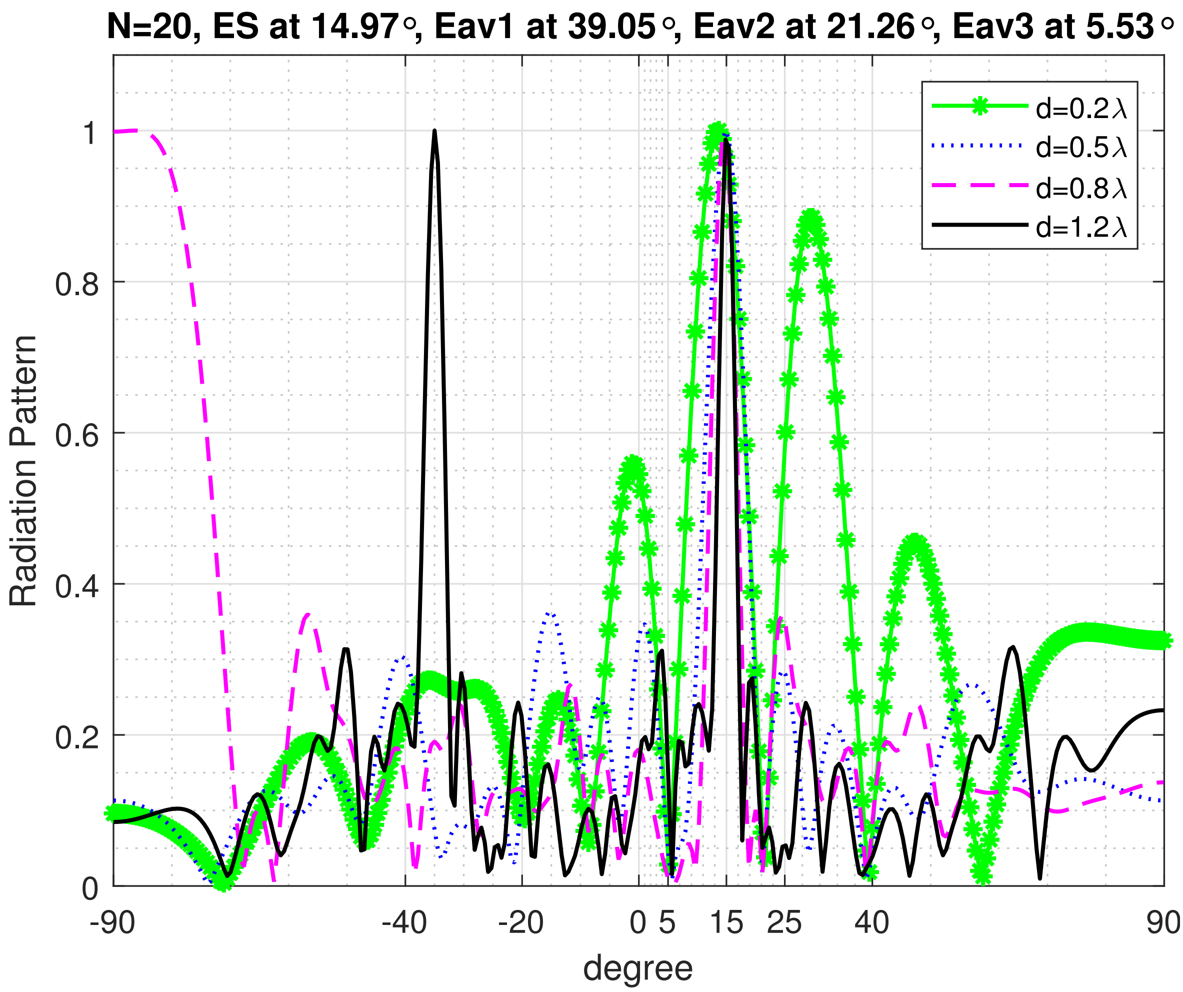


Figure 4.5: RLS beamforming algorithm.

The effect of variation of the separation distance between two antenna elements (d) is analyzed as shown in Figure 4.4 and Figure 4.5. When the antenna element spacing is less than 0.5 of the wavelength (λ), the side lobe level (SLL) is very high and null-depth is very low as shown in table 4.7, table 4.9, table 4.8 and table 4.10 for d=0.2λ. If the antenna element spacing (d) is increased above 0.5λ, the beamwidth decreases resulting in higher directivity.

Table 4.9: Relative power level for RLS algorithm with d variation

d	Earth station Main lobe(dB)	Eavesdroppers Null Depth(dB)		
	ES at 14.97°	Eav1 at 39.09°	Eav2 at 21.26°	Eav3 at 5.53°
0.2	-0.2165	-17.153	-2.2217	-9.20
0.5	-0.0793	-22.24	-17.16	-18.58
0.8	-0.05	-21.05	-16.90	-17.011
1	-0.000088	-19.932	-14.77	-16.56

Table 4.10: RLS- Beamwidth and Max Sidelobes level(SLL) with d varying

d	Beamwidth	Max. SLL(dB)
0.2	6.8760	-0.0087
0.5	8.0220	-4.7110
0.8	12.6058	-0.0043
1	17.7610	-0.0130

However, the null-depth decreases as shown in figure 4.4 and figure 4.5 greater than d=0.5λ. As shown in table 4.7, table 4.9, table 4.8 and table 4.10, When d=0.5λ, the SLL is low and the null-depth is highest resulting in greatest eavesdropper suppression capability. Since, waves cancel out if one wave is half a wavelength late compared to the other. That means that if the distance between two antenna elements is $\lambda/2$, and if both are fed by the same signal, then, There will be no power radiated in the lateral direction. Only one direction will be heavily focused by the beam. If the distance between elements is smaller than $\lambda/2$, then the main lobe will be wider. And finally, if the distance between elements is larger, λ or more, then several main lobes will appear Thus, d=0.5λ is the optimum separation between two antenna array elements. The result shown in figure 4.4 and figure 4.5 are for the LMS and RLS algorithm respectively, however, it is found true for all algorithms and thus d is considered as 0.5λ in all further simulations. Further, the effect of number of antenna array elements and convergence speed of each algorithm are discussed.

4.5.2 Evaluation of varying Number of Antenna Elements

Table 4.11: Relative power level for LMS algorithm with N variation

N	Earth station Main lobe(dB)	Eavesdroppers Null Depth(dB)		
	ES at 14.97°	Eav1 at 39.09°	Eav2 at 21.26°	Eav3 at 5.53°
5	-0.1220	-12.5317	-1.329	-2.84
15	-0.0797	-22.2411	-17.7417	-18.332
25	0	-24.9276	-20.45	-21.66
30	0	-25.4990	-21.7093	-22.946

Beamformer performance is a radiation pattern(RP) of an antenna array. It is controlled by the number of antenna array elements, that represents the gain of the array as a function of arrival angle. In figure 4.6 and figure 4.7 , we show the holographic antenna with 5,15,25 and 30 antenna elements. Thus, by increasing the number of antenna array element more side-lobes have appeared but their levels are very lower. This mitigates Eavesdropper and improves directionality.

Table 4.12: LMS algorithm- Beamwidth and Max Sidelobes level with d varying

N	Beamwidth	Max. SLL(dB)
5	38.36	-1.3436
15	15.47	-4.6528
25	10.89	-6.8382
30	9.165	-6.1654

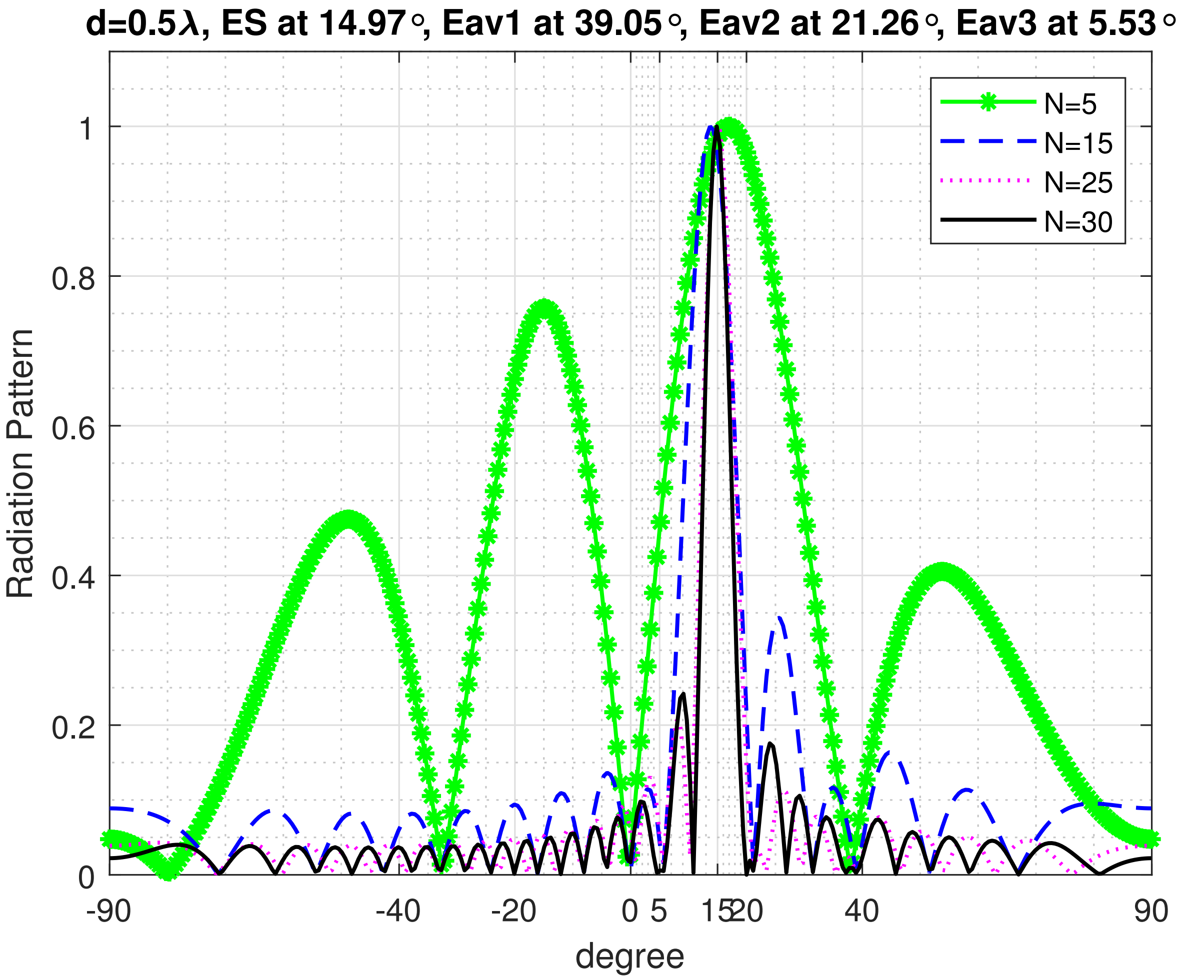


Figure 4.6: LMS beamforming algorithm ; N=5,15,25,30.

As shown in figure 4.6 and Figure 4.7, as the number of antenna elements increases, the beamwidth decreases, thus increasing the directivity of the antenna array. The SLL decreases with increase in the number of antenna array elements as shown in table 4.12, table 4.14, table 4.11 table 4.13.

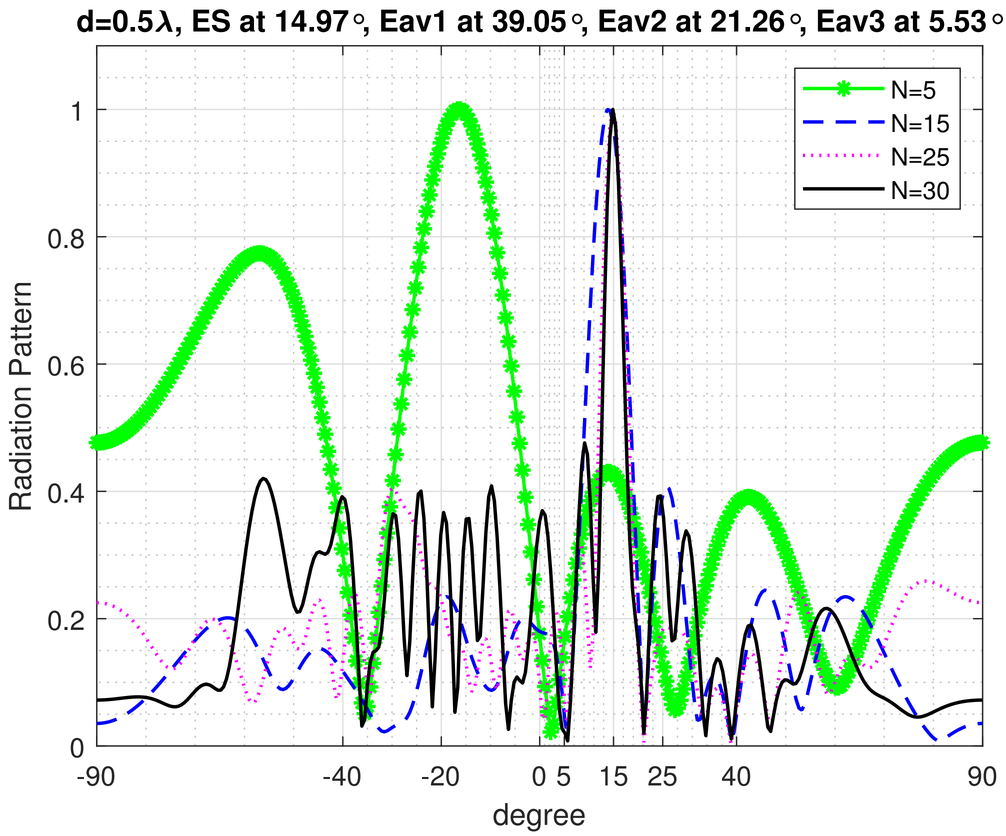


Figure 4.7: RLS beamforming algorithm ; N=5,15,25,30.

As the number of antenna array element increases the beam-width becomes sharper but with cost of increasing number of side-lobes. Figure 4.6 and Figure 4.7 shows that even though the number of side-lobes increases with increasing number antenna, the side-lobe-level is low compared to those generated by array with small number of elements.

Table 4.13: Relative power level for RLS algorithm with N variation

N	Earth station Main lobe(dB)	Eavesdroppers Null Depth(dB)		
	ES at 14.97°	Eav1 at 39.09°	Eav2 at 21.26°	Eav3 at 5.53°
5	-2.69	-4.87	-4.84	-6.64
15	-0.076	-20.54	-17.42	-18.28
25	0	-22.00	-18.33	-18.71
30	0	-23.69	-18.93	-19.73

Table 4.14: RLS algorithm- Beamwidth and Max Sidelobes level(SLL) analysis

N	Beamwidth	Max. SLL(dB)
5	25.78	-0.0026
15	15.46	-4.9894
25	10.31	-3.6063
30	9.16	-2.1141

In Figure 4.6 The Cartesian coordinate system and the related beam pattern may be observed from the angle corresponding to the pattern shape is largely the same for the LMS-algorithm, and It correlates to amplitude attenuation in the target user signal direction that is quite comparable to that of the main beams. The eavesdropper's orientation, which is created sidelines or null, played a role in suppressing the eavesdropper.

Different Cartesian coordinate forgetting factors under the beam pattern for the RLS algorithm seen from the Figure 4.7. If you choose a high forgetting factor, This will make the user's related directions appear null eavesdropper, which is the condition under the user eavesdroppers suppression effect is relatively better.

However, The RLS-algorithm overcomes the correlation-computational matrix's complexity and singularity concerns. The LMS method provides the most null depths at the eavesdropper, as can be observed.

4.6 Secrecy evaluation of adaptive beamforming algorithms for holographic array antenna

In this section, we investigated the secrecy performance of adaptive algorithm in satellite system for 6G communication, where Earth station and multiple eavesdroppers are considered in the system. Particularly, we analyzed three eavesdroppers.

From the Figure 4.6 and Figure 4.7 and from Table 4.11 and 4.13, It is clear that as the number of antenna arrays grows, the beam width narrows. Also, it's clear to see from the simulation results that all have a maximum gain in the direction of a desired use(earth station) and almost all have very low gain of (less than - 25.49dB/-17.56dB, -21.7dB/-18.67dB and -17.599dB/-16.03dB for LMS/RLS each eavesdroppers location respectively,N=30) in the direction of eavesdroppers.

Therefore, when only nullifying capacity is considered the LMS algorithm outperforms the others for the same number of antenna arrays, with RLS being the poorest in comparison.

Again from Figure 4.6 and Figure 4.7 the for maintaining lower side lobes LMS has better result compared to RLS for same number of array. As the nullifying capacity increases, so does the secrecy capability.

4.7 Secrecy Evaluation of Varying Number of Antenna Elements

4.7.1 Secrecy capacity analysis for LMS algorithm

For this work one earth station and 3 eavesdroppers considered, which is earth station at $(14.97°)$ and eavesdroppers at$(39.09°, 21.26° and 5.53°)$. Holographic array antenna of 20 elements and the separation between elements is 0.5 λ and the minimum distance separation of angle of arrival used is 6.29°.

Table 4.15: Secrecy capacity(bps/Hz) LMS algorithm with d variation

N	Eav1 at 39.09°(dB)	Eav2 at 21.26°(dB)	Eav3 at 5.53°(dB)
5	5.07	-6.629	-2.821
10	6.96	3.29	3.549
15	8.05	6.905	7.073
25	8.61	7.622	7.927
30	8.73	7.932	8.21

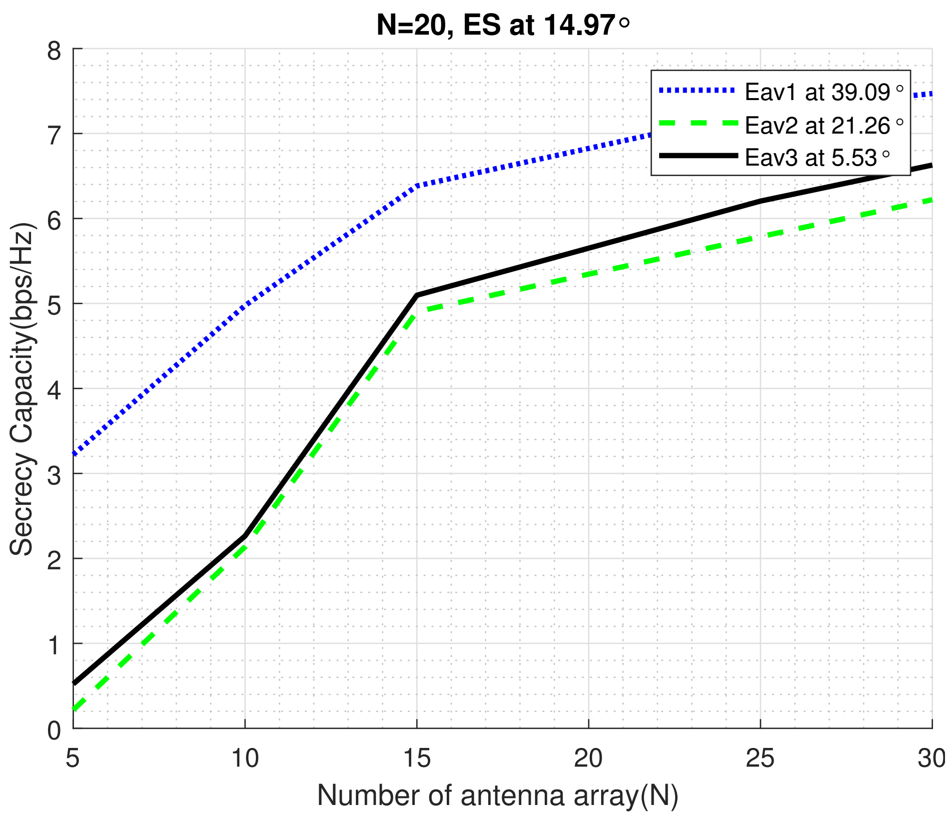


Figure 4.8: Secrecy capacity with LMS algorithm

As shown Figure 4.8, and table 4.15 As the direction of arrival of eavesdroppers moves more away from the earth station, the secrecy capacity increases as well, but When it gets closer, the capacity for secrecy decreases (example ,N=30, for $Eav1 = 39.09°$ the secrecy capacity(dB)= 8.73dB, for $Eav2 = 21.26°$ the secrecy capacity(dB)= 7.932dB, for Eav3=5.53 the secrecy capacity(dB)= 8.21dB). Again, from Figure 4.8, and table 4.15 as the number of antenna increase the secrecy capacity increase as well since as the number of antenna elements increases, The null depth is increasing, The beamwidth narrows and the antenna's directivity improves.

4.7.2 Secrecy capacity analysis for RLS algorithm with d variation

For this work one earth station and 3-eavesdroppers considered, which is earth station at $(14.97°)$ and eavesdroppers at$(39.09°, 21.26° and 5.53°)$. Holographic array antenna of 20 elements and the distance separation between elements is 0.5 λ and the minimum separation of direction of arrival(DoA) used is 6.29°.

Table 4.16: Secrecy capacity(bps/Hz) RLS algorithm

N	Eav1 at $39.09°(dB)$	Eav2 at $21.26°(dB)$	Eav3 at $5.53°(dB)$
5	-2.89	-2.96	-0.102
10	4.597	3.51	3.835
15	7.652	6.81	7.062
25	8.00	7.087	7.196
30	8.37	7.2491	7.460

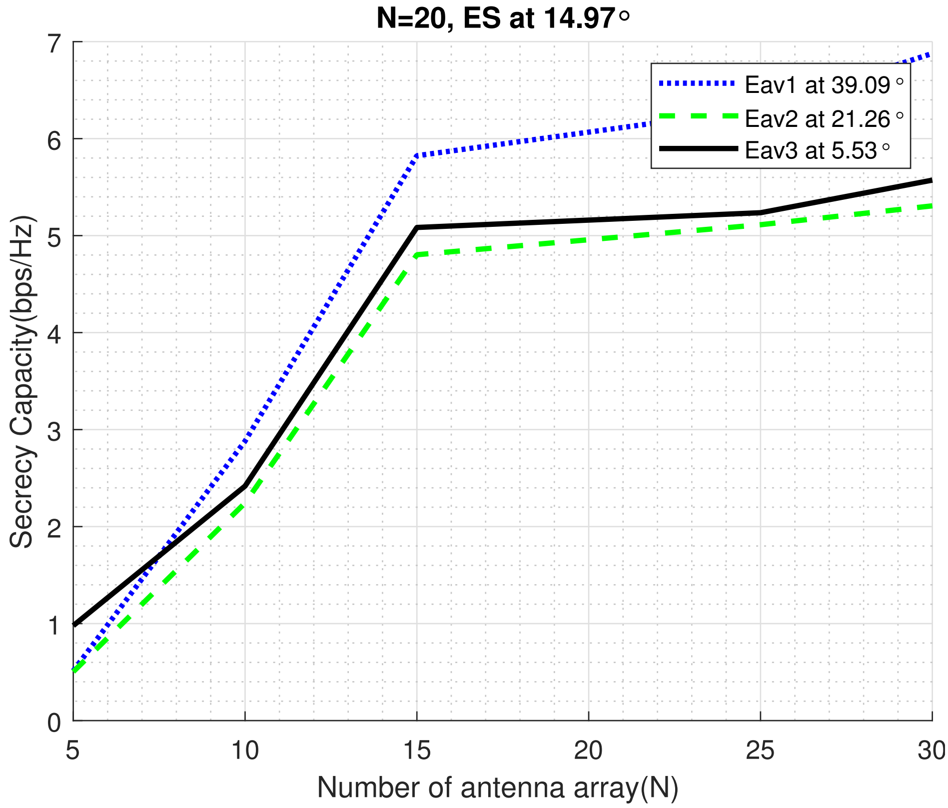


Figure 4.9: Secrecy capacity with RLS algorithm.

As shown Figure 4.9, and table 4.16, As the direction of arrival (DoA) of eavesdroppers moves further away from the earth station, the secrecy capacity increases, but When it gets closer, the capacity for secrecy decreases (example ,N=30, for Eav1=39.09 the secrecy capacity(dB)= 8.37dB, for Eav2=21.26 the secrecy capacity(dB)= 7.249dB, for Eav3=5.53 the secrecy capacity(dB)= 7.46dB). Again, from Figure 4.9, and table 4.16 as the number of antenna array increase the secrecy capacity increase as well since as the number of antenna array elements increases, the null-depth getting more deeper, the beam-width decreases, thus increasing the directivity of the array antenna.

4.7.3 Secrecy capacity comparison of adaptive algorithm

From the Figure 4.6 and Figure 4.7 and from Table 4.11 and 4.13, can easily observe that the beam width gets narrower as the number of antenna increases. And also from simulation result it's easy to observe all have maximum gain in the direction of desired user(earth station) and almost all have very low gain of (less than - 25.49dB/-23.69dB, -21.7dB/-18.93dB and -22.94dB/-19.73dB for LMS/RLS each eavesdroppers location respectively,N=30) in the direction of eavesdroppers.

Therefore, When only nullifying(leakage power) ability is considered, the LMS-algorithm outperforms the others for the same number of antennas, with RLS performing the worst.

Again from Figure 4.6 and Figure 4.7 and also for the same number of arrays, LMS outperforms RLS in terms of preserving lower side lobes. So as the nullifying increase the secrecy capacity also increase accordingly.

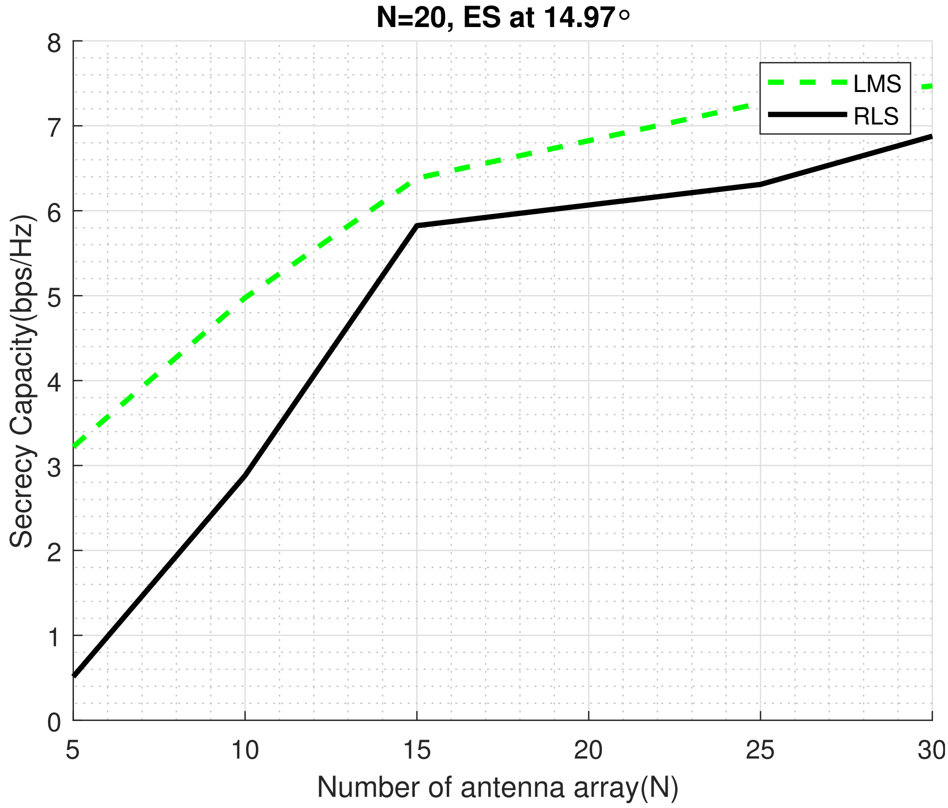


Figure 4.10: Secrecy comparison between LMS and RLS algorithm d=0.5λ.

As can be seen from the simulation results LMS has very narrow beam-width than and RLS-beamforming algorithm, but this comes with cost of increasing number of side-lobes. LMS have null-depth towards the eavesdropper than RLS-algorithm. And it can also be easily observed from the result, the LMS-beamforming algorithm for increasing number of user has better performance characteristics than RLS-algorithm because of their ability in placing null towards the eavesdropper and producing much stronger beam towards the earth station as well as low-side-lobe-levels. Generally some numerical results are summarized on table 4.11 and 4.13. but if the signal characteristics are rapidly changing due to high mobility rate of the user, then the LMS-algorithm may not be able to track the signal due to its slow convergence speed rate.

4.8 Secrecy evaluation of Varying distance between Antenna Elements

The spacing less than 0.5λ is not be able to increase the beamformer performance of antenna array in terms of resolution. Antenna element spacing which is larger than the 0.5λ creates grating lobes. Furthermore, the spacing is larger than λ. Other main beam appear is reduce the performances of beamformer. Thus, the 0.5λ is chosen to cause the perfect aperture than to place lobes at the horizon, without harm.

4.8.1 Secrecy capacity analysis for LMS algorithm with d variation

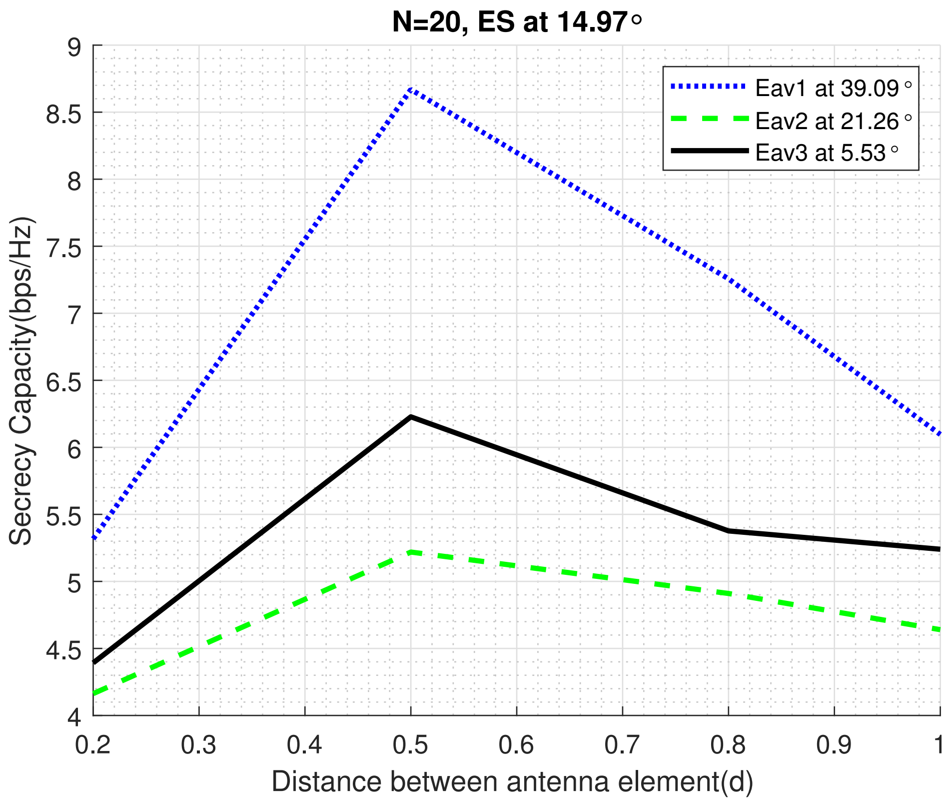


Figure 4.11: Secrecy capacity with LMS algorithm.

Table 4.17: Secrecy capacity(bps/Hz) LMS algorithm

d	Eav1 at 39.09°(dB)	Eav2 at 21.26°(dB)	Eav3 at 5.53°(dB)
0.2	7.25	6.19	6.42
0.5	9.38	7.17	6.91
0.8	8.60	6.91	7.30
1	7.85	6.75	7.27

4.8.2 Secrecy capacity analysis for RLS algorithm with d variation

Table 4.18: Secrecy capacity(bps/Hz) RLS algorithm

d	Eav1 at 39.09°(dB)	Eav2 at 21.26°(dB)	Eav3 at 5.53°(dB)
0.2	7.26	6.19	6.42
0.5	9.38	7.176	7.94
0.8	8.60	6.91	7.30
1	7.85	6.75	7.27

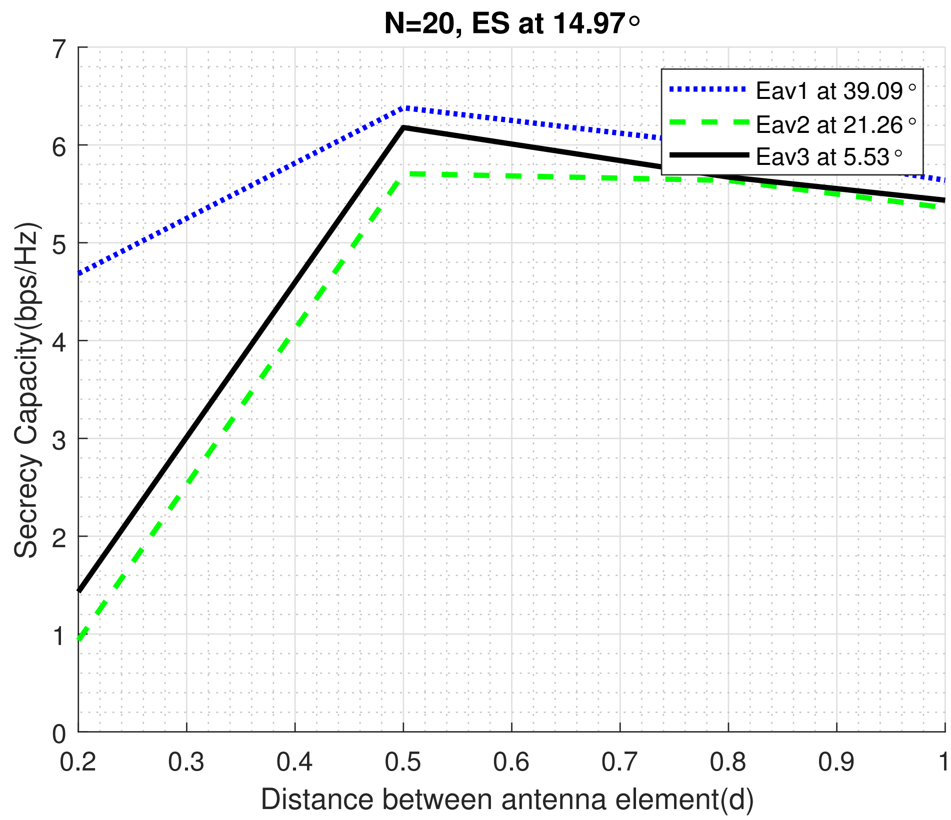


Figure 4.12: Secrecy capacity with RLS algorithm.

4.8.3 Secrecy capacity comparison of adaptive algorithms

The effect of variation of the distance between two antenna elements (d) is evaluated as shown in Figure 4.4 and Figure 4.5. When the antenna array element spacing is less than 0.5 of the wavelength (λ), the side-lobe-level(SLL) is very high and null-depth is very low as shown in Figure 4.4 and Figure 4.5, this make the secrecy capacity also very low as shown in table 4.17 and 4.18 and Figure 4.11 and Figure 4.12 for d=0.2λ. If the antenna element spacing(d) is increased above 0.5λ, the beam-width decreases resulting in higher directivity. When d=0.5λ, the SLL is low and the null-depth is highest resulting in greatest eavesdropper suppression capability which is highest secrecy capacity as shown in Figure 4.11 and Figure 4.12. Thus, d=0.5λ is the optimum separation distance between two antenna elements. The result shown in Figure 4.4 and Figure 4.5 are for the LMS and RLS-algorithm respectively, however, it is found true for all algorithms and thus d is considered as 0.5λ in all further simulations. At greater than d=0.5λ, for LMS-algorithm the secrecy capacity for some extent it will increase but with the cost of additional incorrect peak Figure 4.4 and Figure 4.5, then the secrecy capacity decreases. But for RLS-algorithm at greater than d=0.5λ the secrecy capacity start down as shown in figure 4.12.

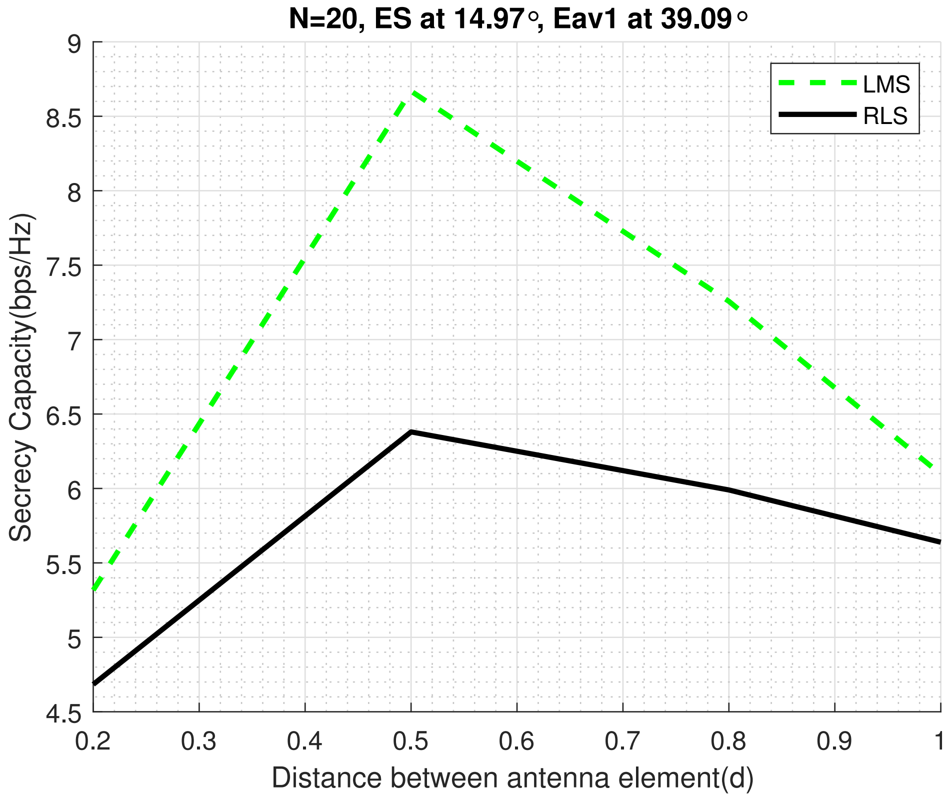


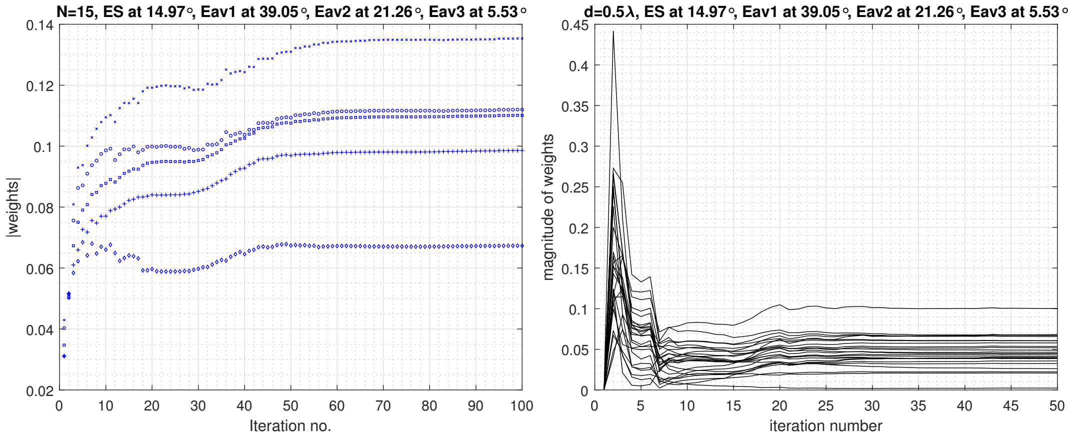
Figure 4.13: Secrecy comparison between LMS and RLS algorithm d=0.5λ.

4.8.4 Evaluation of Convergence Speed of adaptive algorithms

Next, the convergence speed of the algorithms is discussed. For this analysis, N=20 and d=0.5λ are chosen.

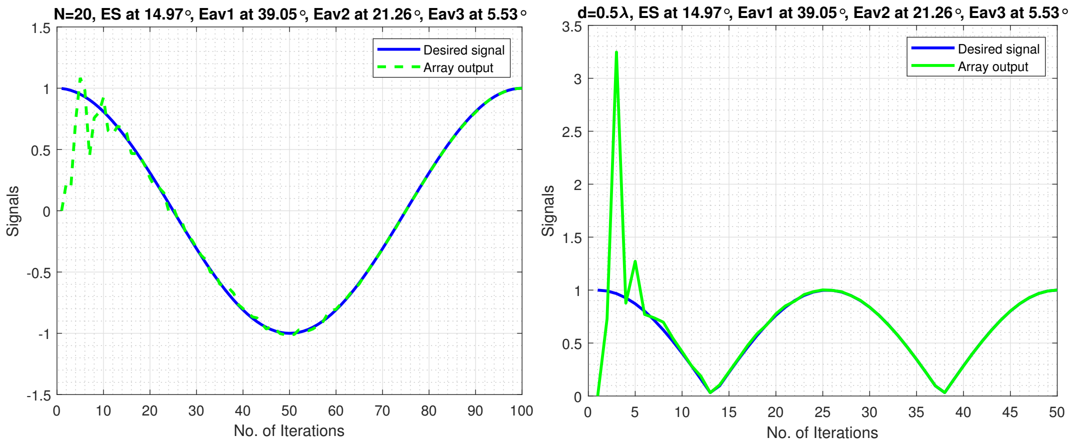
Figure 4.15 (a) and 4.14 (a) shows that the weights of LMS-algorithm converge to their optimum solution after 60-iterations.

If the signal characteristics are rapidly changing due to high mobility rate of the user, then the LMS-algorithm may not be able to track the signal due to its slow convergence rate. This is the main drawback of this algorithm.



(a) LMS; N=15; d=0.5λ (b) RLS; N=15; d=0.5λ

Figure 4.14: (a)Convergence of the weight vectors for LMS algorithm; (b) Convergence of the weight vectors for RLS algorithm.



(a) LMS; N=15; d=0.5λ (b) RLS; N=15; d=0.5λ

Figure 4.15: (a) Desired signal with array output for LMS algorithm; (b) Desired signal with array output for RLS algorithm;

Figure 4.15 (b) and 4.14 (b) shows that the weights of the RLS algorithm converge to their optimum values in just 15 iterations. This convergence is much faster than LMS (60 iterations). The convergence results are summarized in table 4.19.

The delay is calculate for the satellite while is at 628km altitude with a propagation delay of 2.09msec with each iteration takes 0.5μsec.

Table 4.19: Rate of convergence for each algorithm

Algorithm	No. of iterations	time take
LMS	60	30μsec
RLS	15	7.5μsec

5. CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

In this thesis, To investigated the secrecy capacity in the multi-beam satellite system for 6G communication using adaptive beamforming algorithm. We first established the multi-beam satellite communication system which consists of one earth-station and three eavesdroppers. Then, we analyze direction of arrival(DoA) (MUSIC and Min-Norm), first by calculating the lock angle of the earth station and eavesdropper and applying adaptive beamforming algorithms(LMS and RLS) in order to generate the amplitude and phase for tunable element of holographic antenna. To enable intelligent information to be distributed across a global network, 6G communication put antenna technology must meet certain standards such as accurate beam-steering and increase in capacity. Though MIMO technologies rely on large-scale phased-arrays, inherent limitations of phased-arrays severely hinder their future development. Specifically, phased arrays highly rely on power-amplifiers consume high power and numerous phase-shifters, which are expensive in particular in the high-frequency bands. To overcome existing antenna technologies deficiencies, holographic array antennas, as small-size and low-cost planar antennas, have attracted increasing attention due to their capability of multi-beam steering with low power consumption.

For the purpose of earth station mitigation to assist satellite security, the use of adaptive antenna arrays can be practical. with adaptive antenna array algorithms, it is possible to design a beamformer to increase directivity and place nulls (Lowing power leakage to the side lobe) in directions of eavesdropper signals. Spatial reference beam-former uses the AOA information contained in the incoming signals to synthesize beam steering to the earth station and put nulls toward the eavesdropper. Therefore, for effective and eavesdropper rejection, it is important to estimate the angle of arrival of those sources correctly.

MUSIC-algorithm has high performance so it is mostly used in various array processing system, the major drawback of the algorithm is it is fails to estimate the DOAs of highly correlated signals and also the computation complexity is increased because of its search for the peaks of the incoming signals .The Min-Norm technique results shown.It is one of the high-resolution method but it unsuccessful to suppress the incorrect peaks.

In both the receiver and transmitter, the adaptive beamforming technology was primarily responsible for controlling the directionality of the radiation patterns, The main beam of radiation can be shaped and directed toward the earth station using this signal processing technology while suppress other eavesdropper by using adaptive algorithms. By comparing the simulation results, two adaptive beamforming algorithms have been simulated, analyzed and compared on the basis of beamforming, secrecy, and speed. The maximum secrecy capacity is found to be at d=0.5λ, which is the optimal distance between antenna array elements. Since, waves cancel out if one wave is half a wavelength late compared to the other. That means that if the distance between two antenna elements is $\lambda/2$, and if both are fed by the same signal, then, There will be no power radiated in the lateral direction. Only one direction will be heavily focussed by the beam. If the distance between elements is smaller than $\lambda/2$, then the main lobe will be wider. And finally, if the distance between elements is larger, λ or more, then several main lobes will appear Thus, d=0.5λ is the optimum separation between two antenna array elements The effect of number of antenna elements(N) on beamforming is analyzed and it is seen that with increase in N, the secrecy capacity increase. LMS have better deep nullifying towards the eavesdropper than RLS-algorithm. And it can also be easily observed from the result, the LMS beamforming algorithm for increasing number of user has better performance characteristics than RLS-algorithm because of their ability in placing null towards the eavesdropper and producing much stronger beam towards the earth station as well as low-side-lobe-levels.

It is seen that the LMS-algorithm has better secrecy capacity performance except that it has a very slow rate of convergence. RLS improves the convergence speed at the cost of more computational complexity and singularity problem of correlation matrix.

5.2 Recommendations and Future work

In this thesis the performance of adaptive beamforming algorithm for securing multi-beam satellite system for the application of 6G communication. The future scope of this thesis.

- The proposed technique was evaluated under AWGN channel only. The proposed technique can also be evaluated under the different propagation model.
- For securing multi-beam satellite system applying different technique, such as zero-forcing (ZF), convex optimization and artificial noise (AN).
- The proposed technique was evaluated in simulation level only. Its practical performance could also be investigated by combining adaptive beamforming algorithm with holographic array antenna(first fabricating the antenna needed).

REFERENCES

Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M. (2019). Security for 5g and beyond. *IEEE Communications Surveys & Tutorials*, *21*(4), 3682–3722.

Alotaibi, N. N., & Hamdi, K. A. (2016). Switched phased-array transmission architecture for secure millimeter-wave wireless communication. *IEEE Transactions on Communications*, *64*(3), 1303–1312.

Balanis, C. A., & Ioannides, P. I. (2007). Introduction to smart antennas. *Synthesis Lectures on Antennas*, *2*(1), 1–175.

Barros, J., & Rodrigues, M. R. (2006). Secrecy capacity of wireless channels. In *2006 ieee international symposium on information theory* (pp. 356–360).

Björnson, E., Sanguinetti, L., Wymeersch, H., Hoydis, J., & Marzetta, T. L. (2019). Massive mimo is a reality—what is next?: Five promising research directions for antenna arrays. *Digital Signal Processing*, *94*, 3–20.

Black, E. J. (2017). Holographic beam forming and mimo. *Pivotal Commware*.

Chang, D.-C., & Hu, C.-N. (2012). Smart antennas for advanced communication systems. *Proceedings of the IEEE*, *100*(7), 2233–2249.

Chowdhury, M. Z., Shahjalal, M., Ahmed, S., & Jang, Y. M. (2020). 6g wireless communication systems: Applications, requirements, technologies, challenges, and research directions. *IEEE Open Journal of the Communications Society*, *1*, 957–975.

Cui, G., Zhu, Q., Xu, L., & Wang, W. (2020). Secure beamforming and jamming for multibeam satellite systems with correlated wiretap channels. *IEEE Transactions on Vehicular Technology*, *69*(10), 12348–12353.

Eric Black, A. K., & Andjela Ilic-Savoia, K. W., Pivotal Commware. (2020). *Breaking down mmwave barriers with holographic beam forming.* `https://www.microwavejournal.com/articles/33433-breaking down`.

Garuma, G. F., Tessema, S. B., Tiky, A. Y., Eshete, Y. C., Adde, Y. A., Giday, N. M., ... others (2020). First ethiopian remote sensing satellite (etrss-1): Mission information and overview.

Guo, H., Li, J., Liu, J., Tian, N., & Kato, N. (2021). A survey on space-air-ground-sea integrated network security in 6g. *IEEE Communications Surveys & Tutorials*.

Hayashi, M., & Vázquez-Castro, Á. (2020). Physical layer security protocol for poisson channels for passive man-in-the-middle attack. *IEEE Transactions on Information Forensics and Security*, *15*, 2295–2305.

Ibrahim, M., Ramireddy, V., Lavrenko, A., König, J., Römer, F., Landmann, M., … Thomä, R. S. (2017). Design and analysis of compressive antenna arrays for direction of arrival estimation. *Signal Processing*, *138*, 35–47.

Khalaf, A. A., El-Daly, A.-R. B., & Hamed, H. F. (2016). Different adaptive beamforming algorithms for performance investigation of smart antenna system. In *2016 24th international conference on software, telecommunications and computer networks (softcom)* (pp. 1–6).

Khan, L. U., Yaqoob, I., Imran, M., Han, Z., & Hong, C. S. (2020). 6g wireless systems: A vision, architectural elements, and future directions. *IEEE access*, *8*, 147029–147044.

Kwizera, E. (2018). *Performance evaluation of direction of arrival estimation using uniform and non-uniform linear arrays for signal source localization* (Unpublished doctoral dissertation). JKUAT-PAUSTI.

Leong, W. Y. (2008). Angle-of-arrival estimation: beamformer-based smart antennas. In *2008 3rd ieee conference on industrial electronics and applications* (pp. 1593–1598).

Liao, Y., Wu, X., Wu, Z., & Gao, L. (2019). Robust constrained inverse beamforming algorithm based on space time adaptive processing. *IEEE Access*, *7*, 55191–55198.

Lu, W., Liang, T., An, K., & Yang, H. (2018). Secure beamforming and artificial noise algorithms in cognitive satellite-terrestrial networks with multiple eavesdroppers. *IEEE Access*, *6*, 65760–65771.

Ma, D., Liu, X., Wang, X., Xiong, J., & Li, W. (2015). On the performance indexes of physical layer security for multi-beam satellite networks. In *2015 international conference on wireless communications & signal processing (wcsp)* (pp. 1–6).

Matei, V.-C. (2021). *Cybersecurity analysis for the internet-connected satellites.*

(Mi-Wave), M. W. P. I. (2020). *What is 6g?* `https://www.miwv.com/what-is-6g/`.

Mun, J.-Y., Kim, T.-Y., Bae, Y.-C., & Hwang, S.-S. (2018). Performance evaluation of satellite beamforming system with square array antenna. In *2018 joint 10th international conference on soft computing and intelligent systems (scis) and 19th international symposium on advanced intelligent systems (isis)* (pp. 781–784).

Nguyen, V.-L., Lin, P.-C., Cheng, B.-C., Hwang, R.-H., & Lin, Y.-D. (2021). Security and privacy for 6g: A survey on prospective technologies and challenges. *IEEE Communications Surveys & Tutorials*, *23*(4), 2384–2428.

Nicolaescu, I., & Stoica, D. (2010). Smart antennas for wireless communications systems. In *2010 conference proceedings icecom, 20th international conference on applied electromagnetics and communications* (pp. 1–4).

Ray, P. P. (2021). A review on 6g for space-air-ground integrated network: Key enablers, open challenges, and future direction. *Journal of King Saud University-Computer and Information Sciences*.

Ray, P. P., Kumar, N., & Guizani, M. (2021). A vision on 6g-enabled nib: Requirements, technologies, deployments, and prospects. *IEEE Wireless Communications*, *28*(4), 120–127.

Sanenga, A., Mapunda, G. A., Jacob, T. M. L., Marata, L., Basutli, B., & Chuma, J. M. (2020). An overview of key technologies in physical layer security. *Entropy*, *22*(11), 1261.

Schraml, M. G., Schwarz, R. T., & Knopp, A. (2020). Multiuser mimo concept for physical layer security in multibeam satellite systems. *IEEE Transactions on Information Forensics and Security*, *16*, 1670–1680.

Shen, Q., Liu, W., Wang, L., & Liu, Y. (2020). Group sparsity based localization for far-field and near-field sources based on distributed sensor array networks. *IEEE Transactions on Signal Processing*, *68*, 6493–6508.

Sheriff, R. E., & Hu, Y. F. (2001). *Mobile satellite communication networks*. John Wiley & Sons.

Sreekumar, S., Bunin, A., Goldfeld, Z., Permuter, H. H., & Shamai, S. (2020). The secrecy capacity of cost-constrained wiretap channels. *IEEE Transactions on Information Theory*, *67*(3), 1433–1445.

Staff, P. (2019). Holographic beam forming and phased arrays. *Pivotal Commware, Inc., Kirkland, WA, USA*.

Strinati, E. C., Barbarossa, S., Gonzalez-Jimenez, J. L., Ktenas, D., Cassiau, N., Maret, L., & Dehos, C. (2019). 6g: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication. *IEEE Vehicular Technology Magazine*, *14*(3), 42–50.

Sun, L., & Du, Q. (2017). Physical layer security with its applications in 5g networks: A review. *China communications*, *14*(12), 1–14.

Van Loan, C. F., & Golub, G. (1996). Matrix computations (johns hopkins studies in mathematical sciences). *Matrix Computations*.

Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., & Zhou, W. (2020). Security and privacy in 6g networks: New areas and new challenges. *Digital Communications and Networks*, *6*(3), 281–291.

Wang, Y., Li, Q., Jiao, J., Wu, S., & Zhang, Q. (2019). Arm: Adaptive random-selected multi-beamforming estimation scheme for satellite-based internet of things. *IEEE Access*, *7*, 63264–63276.

Wu, C., & Lai, C.-F. (2022). A survey on improving the wireless communication with adaptive antenna selection by intelligent method. *Computer Communications*, *181*, 374–403.

Xu, R., Da, X., Hu, H., Ni, L., & Pan, Y. (2019). A secure hybrid satellite-terrestrial communication network with af/df and relay selection. *IEEE Access*, *7*, 171980–171994.

Yin, Z., Jia, M., Cheng, N., Wang, W., Lyu, F., Guo, Q., & Shen, X. (2021). Uav-assisted physical layer security in multi-beam satellite-enabled vehicle communications. *IEEE Transactions on Intelligent Transportation Systems*.

Zhang, J., Lin, M., Ouyang, J., Zhu, W.-P., & De Cola, T. (2021). Robust beamforming for enhancing security in multibeam satellite systems. *IEEE Communications Letters*, *25*(7), 2161–2165.

Research Fund Acknowledgement

This research project is funded by Adama Science and Technology University under the grant number ASTU/SM-R/409/22, Adama, Ethiopia.