Design of Directional Antennas for IoT Physical Layer Security in Ambient Backscatter Communication (AmBC)

University of Turku
Department of Computing
Master of Science (Tech) Thesis
Cyber Security
July 2025
Mohammed Faisal

Supervisors:
Tahir Mohammad (University of Turku)
Petri Sainio (University of Turku)
Rao Shahid Aziz (South Metropolitan TAFE)

UNIVERSITY OF TURKU
Department of Computing

Mohammed Faisal: Design of Directional Antennas for IoT Physical Layer Security in Ambient Backscatter Communication (AmBC)

Master of Science (Tech) Thesis, 69 p.
Cyber Security
July 2025

This thesis investigates a novel antenna system designed to enhance physical-layer security for Internet of Things (IoT) communications using Ambient Backscatter Communication (AmBC). Ambient backscatter leverages existing environmental radio frequency (RF) signals to facilitate sustainable, battery-free, and independent communications, significantly advancing the IoT landscape. Nevertheless, conventional omnidirectional communication techniques are vulnerable to information leakage due to their susceptibility to unauthorized interception. To mitigate these security risks, a dual-antenna architecture is introduced, integrating a microstrip patch antenna array optimized for efficient omnidirectional reception and energy harvesting, with a quasi-Yagi-Uda antenna specifically engineered for directional and secure transmission. System parameters-including gain, bandwidth, side lobe levels (SLL), and Voltage Standing Wave Ratio (VSWR)-are rigorously optimized utilizing advanced evolutionary algorithms, namely the Multi-Objective Genetic Algorithm (MOGA) and Multi-Objective Particle Swarm Optimization (MOPSO). Extensive simulations performed using CST Microwave Studio demonstrate notable enhancements in secrecy capacity, signal integrity, and interference resilience compared to traditional antenna designs. This integrated antenna strategy thereby provides a robust, energy-efficient, and secure solution tailored for dynamic wireless IoT environments. Ultimately, this research furnishes practical insights and foundational guidelines critical for deploying secure, efficient, and scalable IoT infrastructures utilizing ambient backscatter technology.

Keywords: Ambient Backscatter Communication, Internet of Things, Physical Layer Security, Directional Antenna Design, Dual-Antenna Design, Multi-Objective Optimization, MOGA, MOPSO

Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

1.1.1 General Concept of IoT Security and Its Importance

The Internet of Things (IoT) connects a vast range of diverse devices and platforms, each interacting across various protocols and services to enable new digital solutions [1]. This large-scale integration brings about complex challenges, particularly concerning data security and privacy. Given the diversity of devices and communication standards, maintaining robust protection of critical data whether for urban infrastructure or individual users, is essential [1]. As IoT becomes more pervasive, the reliability and security of its communication links become even more important. Recent advances such as 5G networks have been designed to support the unique requirements of IoT, enabling high-density deployments, increased reliability, and support for low-latency applications [2], [3]. However, with these improvements comes an expanded attack surface. The complexity and interconnectedness of IoT infrastructures require comprehensive security measures to protect both users and systems [4].

The expected surge in the number of connected devices and the integration of IoT with cyber-physical systems highlight the need for improved security practices. Protection of sensitive information, safeguarding of infrastructure, and assurance of uninterrupted system operation are now fundamental objectives of IoT security [2],

[3]. As IoT networks evolve, scalable and adaptable security mechanisms are vital to address the ever-changing connectivity landscape.

1.1.2 Introduction to Ambient Backscatter Communication (AmBC)

Ambient Backscatter Communication (AmBC) is a modern approach that enables batteryless or low-power devices to communicate by using and modulating ambient electromagnetic signals, such as those from Wi-Fi, cellular, or broadcast sources [5]. Instead of generating their own RF signals, these devices harvest existing RF energy, using it for both power and data transmission tasks [5], [6], [7].

Communication is accomplished through backscattering: a device varies its antenna impedance to reflect and encode data onto these ambient signals, which are then detected and decoded by a remote receiver [5], [6].This method is particularly suitable for applications where traditional power sources are impractical, including environmental monitoring, wearable technology, and large-scale smart infrastructure [5], [7]. A typical AmBC system includes an external RF source, a passive or semi-passive tag for modulating the signal, and a receiver that extracts the transmitted information [6], [7]. To ensure effective and scalable operation in busy environments, these systems use energy-efficient protocols to manage multiple devices and avoid communication collisions [5]. Advanced implementations such as dual-antenna repeaters can even enhance wireless coverage in challenging environments, such as urban or indoor areas where direct signal paths are blocked [8].

1.1.3 Significance of Cybersecurity in IoT Applications, Specifically at the Physical Layer

As IoT ecosystems expand, security concerns are no longer limited to higher communication layers. The physical layer of wireless systems presents unique vulnerabilities, particularly to threats like eavesdropping and signal interference. Many IoT devices are constrained in power and processing resources, making conventional encryption-based approaches insufficient [6], [7]. Physical Layer Security (PLS) techniques are therefore gaining prominence. By taking advantage of the unpredictable characteristics of wireless channels-such as fading, noise, and spatial diversity-PLS can help prevent unauthorized access and data breaches without imposing heavy computational loads [6], [7]. In highly dense deployments, such as smart cities and industrial IoT, physical layer methods like directional antennas, beamforming, and optimized signal transmission can reduce the exposure of sensitive information and strengthen security [6], [8]. Given the accelerating adoption of 5G and the growing complexity of IoT systems, implementing strong security at the physical layer is essential for maintaining confidentiality, integrity, and system resilience [2], [4], [6], [8]. Physical layer techniques are expected to be central to future security strategies for IoT and related wireless applications.

1.2 Motivation and Problem Statement

1.2.1 Security Challenges in Wireless IoT Communications

The widespread adoption of the Internet of Things (IoT) has led to the interconnection of billions of devices, facilitating applications from smart cities and healthcare to industrial automation. This level of connectivity increases the complexity of managing secure communication, as wireless channels are naturally open and

susceptible to security threats such as eavesdropping and jamming [9]. Resource limitations and diverse deployment scenarios in IoT make the implementation of traditional, computationally heavy cryptographic schemes challenging, especially in large-scale, distributed, or energy-constrained systems [10], [11]. Furthermore, the broadcast nature of wireless transmissions in IoT heightens the risk of information leakage, and the dynamic, ad-hoc nature of many deployments complicates secure key management, exposing critical data to adversarial threats [12].

1.2.2 Necessity and Benefits of Directional Antennas

To address these security vulnerabilities, the use of directional antennas has gained significant attention as a means of enhancing physical layer security in IoT systems. By focusing electromagnetic energy within narrow beams, directional antennas can restrict the spatial exposure of wireless signals, thereby reducing the probability that an unauthorized receiver can intercept or disrupt communications [6]. This approach not only improves the signal quality for intended users but also degrades the channel quality for potential eavesdroppers, thus enhancing secrecy capacity and system reliability [13], [14]. In addition, the use of advanced antenna arrays and beamforming techniques allows for dynamic adaptation of radiation patterns to changing environments, which is crucial for the interference-prone and dense networks typical of modern IoT [15]. Recent advances demonstrate that machine learning-driven optimization of antenna parameters further supports energy-efficient and robust security solutions suitable for low-power IoT devices [16].

1.2.3 Research Focus: Physical Layer Security with Directional Antennas

In light of these challenges and developments, this thesis explores the design and optimization of directional antennas, particularly microstrip patch array and quasi-

Yagi-Uda antenna (QYUA) to enhance physical layer security in IoT systems that employ ambient backscatter communication (AmBC). This research leverages evolutionary algorithms such as multi-objective genetic algorithms (MOGA) to optimize antenna characteristics, including gain, side lobe level, and radiation patterns, for both communication performance and security [8], [13]. By employing comprehensive electromagnetic simulation tools and modern optimization techniques, the work aims to realize spatially selective and energy-efficient wireless links that strengthen secrecy and resilience against eavesdropping and interference in practical IoT deployments [8], [13], [14].

1.3 Research Questions and Research Objectives

1.3.1 Research Questions

This thesis seeks to significantly enhance physical layer security within IoT communication systems utilizing ambient backscatter communication (AmBC) by designing, simulating, and optimizing advanced directional antenna configurations. The research questions (RQ) of this thesis are defined as follows:

RQ1: How do the microstrip patch antenna array and quasi-Yagi-Uda antenna (QYUA) complement each other in the context of AmBC, and how does their combination improve security and communication reliability?

RQ2: Which design parameters (such as dipole lengths, widths, and spacings) most significantly influence the optimized antenna performance and physical layer security, as identified through multi-objective optimization (MOGA, MOPSO)?

RQ3: In what ways do antenna directivity and side lobe suppression impact secrecy capacity and reduce eavesdropper SNR in practical IoT deployments?

RQ4: How effectively do electromagnetic simulation results (from CST Studio Suite) confirm the theoretical improvements in communication performance and

security predicted by optimization?

RQ5: What design modifications are required to extend antenna system operation over broader frequency bands and to ensure its suitability for emerging 5G/6G IoT network scenarios?

1.3.2 Research Objectives

The objectives of this thesis are addressed as follows:

RO1: To design and analyze a dual-antenna system consisting of a microstrip patch antenna array and a quasi-Yagi-Uda antenna (QYUA), optimizing both omnidirectional reception and directional transmission for enhanced communication and security in AmBC-enabled IoT systems.

RO2: To implement and benchmark multi-objective optimization algorithms (MOGA and MOPSO), with a focus on the selection and impact analysis of antenna parameters (e.g., dipole lengths, widths, spacings) on key performance and security metrics.

RO3: To assess and validate the influence of antenna directivity and side lobe control on secrecy capacity, SNR, and eavesdropping resistance through CST-based electromagnetic simulations, demonstrating the performance and security benefits of the optimized antenna design via radiation pattern and field distribution analysis.

Through focused investigation of these questions and objectives, this thesis aims to advance both theoretical understanding and practical strategies for achieving robust physical layer security in future IoT systems. The work builds upon and extends state-of-the-art methods, particularly by integrating advanced optimization techniques and rigorous simulation analysis to bridge the gap between security theory and real-world implementation.

1.4 Justification and Novelty

Employing evolutionary algorithms for antenna optimization represents a significant step forward compared to manual, trial-and-error design processes [16]. By applying both MOGA and MOPSO, this research navigates the complex trade space of antenna parameters, uncovering subtle interactions that improve both security and efficiency. The methodological integration of high-fidelity simulation and algorithmic optimization, combined with a dual-antenna system inspired by recent innovations in quasi-Yagi-Uda antenna (QYUA) design [17], sets this work apart and underscores its relevance for secure, next-generation IoT networks.

In summary, this methodology systematically combines advanced engineering, simulation rigor, and machine learning-driven optimization to produce antennas that materially enhance the physical layer security of AmBC-IoT systems. The entire process is validated through comprehensive simulation studies, ensuring that results are both theoretically robust and practically viable.

1.5 Declaration of the Use of Generative AI

In the course of this research, Stealth Writer and ChatGPT were employed to assist in enhancing the clarity and structure of the writing, particularly for extensive textual sections. All AI-assisted content was thoroughly reviewed, refined, and validated by the author to ensure accuracy, relevance, and full alignment with the research objectives, methodologies, and experimental findings. The use of these AI tools was primarily limited to the preparation of literature review sections.

1.6 Thesis Structure

Chapter 1: **Introduction**

- This chapter introduces the motivation and background for the research, clearly formulates the research objectives (RO) and research questions (RQ), and provides an overview of the adopted methodology and the structure of the thesis.

Chapter 2: **Literature Review**

- A comprehensive review of the current state-of-the-art in IoT security, ambient backscatter communication (AmBC), and antenna technologies is presented. The chapter discusses the advantages of directional antennas and recent advances in evolutionary computation for antenna optimization, highlighting the main research gaps this thesis addresses.

Chapter 3: **System Model, Methodology, and Optimization**

- This chapter details the AmBC system architecture and mathematical signal model, including block diagrams and relevant equations. It describes the signal detection process, secrecy capacity formulation, and the methodology for antenna design. The roles and working principles of the microstrip patch array and quasi-Yagi-Uda antenna (QYUA) are clarified, with field distributions and radiation pattern diagrams. The section also covers simulation setup in CST Studio Suite, the formulation of the optimization problem (decision variables, objective functions, and constraints), and step-by-step implementation of MOGA and MOPSO algorithms, with flowcharts and pseudocode. The chapter concludes by defining the key performance and security metrics.

Chapter 4: **Results and Analysis**

- Simulation results for the designed antennas are presented, including both baseline and optimized cases. The outcomes of the MOGA and MOPSO optimization processes are compared and analyzed, with a focus on the influence of key antenna parameters on metrics such as gain, VSWR, side lobe level, and

secrecy capacity. The chapter also provides a security performance assessment and compares the proposed approach to state-of-the-art methods.

Chapter 5: **Discussion and Implications**

- This chapter interprets the main findings, with an emphasis on how the dual-antenna system enhances communication security in AmBC. It discusses the critical impact of parameter selection, provides recommendations for adapting the system for wideband and next-generation (5G/6G) IoT networks, and addresses practical deployment issues. Limitations of the current study are acknowledged, and avenues for further research are identified.

Chapter 6: **Conclusion and Future Work**

- The main contributions and achievements are summarized, addressing all research objectives and questions. Concluding remarks are offered, along with explicit directions for future work in antenna design and IoT security.

2 Literature Review

2.1 IoT Communication Security

The Internet of Things (IoT) has introduced unprecedented connectivity across diverse sectors, linking billions of smart devices in environments ranging from urban infrastructure to healthcare and industry [1], [2]. As IoT architectures continue to expand, the assurance of secure communication has become essential, given the proliferation of heterogeneous devices, protocols, and open wireless channels [2], [3]. The diversity and openness inherent in IoT systems mean that unauthorized access, privacy breaches, and data manipulation are constant risks. Thus, robust security mechanisms are a fundamental requirement not only for protecting sensitive data but also for preserving the trustworthiness and reliability of IoT services [1], [4].

2.1.1 Physical Layer Security Techniques and Their Importance

Traditional IoT security approaches have largely relied on cryptographic protocols implemented at higher layers of the communication stack. However, the unique constraints of IoT devices including limited computational power, energy resources, and dynamic deployment scenarios often limit the feasibility and effectiveness of conventional security techniques [9], [11] . As a result, there is growing interest in PLS, which exploits the physical properties of the wireless medium such as fading, noise,

interference, and channel randomness to secure data transmission against eavesdropping, jamming, and spoofing [10], [11]. PLS techniques can be broadly categorized into methods such as artificial noise generation, cooperative relaying, beamforming, and secrecy coding [14], [15]. These strategies enhance the confidentiality and resilience of IoT networks by confining useful signal energy to intended receivers and degrading the signal quality at potential eavesdroppers. For example, directional antennas and optimized transmission schemes can significantly increase the secrecy capacity, particularly in dense or hostile radio environments [6]. The effectiveness of PLS does not rely on computational hardness assumptions, making it a promising approach for resource-constrained IoT devices [11], [14]. Table 2.1 provides a comparative overview of prominent PLS approaches, with a focus on beamforming antenna and optimization-driven designs particularly relevant to this thesis.

2.1.2 Recent Advances and Studies in IoT Security

Recent research has made significant progress in both theoretical and practical aspects of IoT security. The integration of machine learning and evolutionary algorithms into the design and optimization of physical layer security mechanisms such as smart antenna arrays and adaptive beamforming has shown remarkable potential [6], [16]. Studies have demonstrated that optimized directional antennas can enhance signal-to-noise ratios, suppress side lobes, and confine electromagnetic energy, thus reducing the risk of interception and improving security outcomes [16]. Moreover, the transition toward 5G and beyond is accelerating innovation in physical layer security, with large-scale deployments of massive MIMO and intelligent reflecting surfaces offering new avenues for secrecy enhancement [3], [15], [18]. Research has also highlighted the effectiveness of integrating AmBC with advanced antenna techniques, demonstrating improved confidentiality and energy efficiency in battery less or low-power IoT applications [6], [7], [18]. As the field advances, it is increasingly clear that robust, adaptive, and low-complexity security solutions at the physical layer will be essential to realize the full potential of the IoT [10], [11], [18].

Table 2.1: Comparative Overview of Physical Layer Security Techniques for IoT.

Technique	**Principle**	**Advantages**	**Limitations**	**Ref.**
Artificial Noise Injection	Transmit intentional noise to disrupt eavesdroppers while protecting legitimate users.	Strong secrecy improvement for multi-antenna systems.	Needs extra antennas and energy; less suitable for low-cost IoT nodes.	[9], [13], [14]
Secure Beamforming	Steers signal energy toward intended users, away from eavesdroppers.	Spatial selectivity; robust secrecy; scalable to IoT.	Requires arrays and optimization; hardware complexity.	[9], [10], [15], [20], [21]
Cooperative Secrecy/Relaying	Uses friendly relays or jammers to increase interference for eavesdroppers.	Leverages node cooperation; network adaptable.	Added complexity and energy use.	[9], [14]
Power/Resource Allocation	Dynamically allocates power/spectrum to maximize secrecy.	Efficient use of resources; adaptable.	Requires accurate channel info and rapid computation.	[2], [9], [10]
Physical Layer Encryption	Generates keys or encodes using wireless channel randomness.	Low complexity, enables keyless approaches.	Sensitive to channel variations; needs synchronization.	[9], [11]
Bit Flipping/Randomization	Some nodes send false data to confuse eavesdroppers.	Simple, energy-efficient for large IoT.	Lower net throughput; needs fusion center.	[9]
Directional Beamforming Antenna Approaches	For secure, focused transmission, minimizing exposure	Strong filtering; higher secrecy; suits IoT/AmBC.	Design/optimization complexity; integration needed.	[6], [15], [16], [18], [21]
Optimization-Driven Antenna Design	Machine learning/evolutionary algorithms tune antenna for secure performance.	Automates best trade-offs; finds novel solutions.	Needs many simulations; algorithm-dependent.	[6], [15], [16], [22], [24]

2.2 Ambient Backscatter Communication

Backscatter communication systems are generally categorized into three architectural types: monostatic, bistatic, and ambient backscatter systems, as shown in Figure 2.1. In monostatic backscatter communication systems (MBCS), such as conventional RFID, the reader contains both the RF source and the backscatter receiver within a single device. Here, the RF source transmits activation signals to the tag, which modulates and reflects these signals back to the receiver. However, this architecture suffers from round-trip path loss, and devices located far from the reader are prone to higher energy outage and reduced signal strength, making MBCS primarily suitable for short-range applications. In contrast, bistatic backscatter communication systems (BBCS) physically separate the carrier emitter from the backscatter receiver, thereby alleviating round-trip losses. BBCS can also enhance coverage and mitigate the doubly near-far problem by optimally placing multiple emitters in the field. Although deploying multiple carrier emitters incurs added complexity and cost, the individual components are relatively simple and less expensive than those in MBCS. Ambient backscatter communication systems (AmBCS) further extend the architecture by utilizing existing ambient RF sources-such as television towers, cellular base stations, and Wi-Fi access points-instead of dedicated carrier emitters. This approach eliminates the need for extra spectrum allocation and reduces infrastructure costs. Nevertheless, the performance of ABCS may be hindered by the unpredictable and dynamic nature of ambient RF signals, which can act as interference, and by the lack of control over power and source placement, thereby complicating the optimization and deployment of such systems compared to BBCS.

2.2.1 AmBCS: Operational Principles, Key Benefits, and Limitations

Ambient Backscatter Communication (AmBC) enables ultra-low-power devices to transmit data by modulating and reflecting existing ambient radio frequency (RF) signals such as those from Wi-Fi, TV, or cellular networks, rather than generating their own dedicated

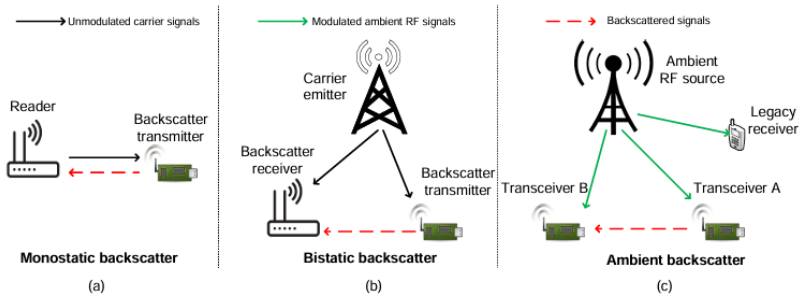


Figure 2.1: Fundamental Approaches to Backscatter Communication [7].

carrier [5]. A typical AmBC system consists of three main components: an ambient RF source, a passive or semi-passive tag (which modulates its antenna impedance to encode data), and a receiver that decodes the backscattered signal [5], [7]. The process works by the tag switching its antenna between different impedance states, causing the incident RF signal to be either reflected or absorbed, thereby imprinting data onto the ambient signal. This method enables battery less operation, as tags can harvest energy from the same ambient RF sources they use for communication [2], [7].

Ambient backscatter communication, introduced in 2013, addresses key limitations of conventional backscatter systems by enabling devices to harvest and reflect ambient RF signals present in the environment, such as 4G, 5G, and Wi-Fi, instead of relying on dedicated energy sources or additional spectrum allocation [5], [19]. This approach greatly reduces both operational costs and maintenance requirements, facilitating sustainable and autonomous IoT connectivity [20], [21]. Nevertheless, the broadcast nature of wireless signals exposes these systems to risks such as eavesdropping and interference, as overlapping signals may be received and superimposed at the receiver, complicating reliable signal detection [22]. Traditional cryptographic methods, which rely on complex encoding and decoding algorithms, are increasingly challenged by advances in computational power and are not always suitable for resource-constrained IoT scenarios [23]. As a result, physical layer security—leveraging the inherent randomness of wireless channels and noise—has emerged as a key strategy for safeguarding information at the bit level [24]. Among various physical layer techniques, beamforming has proven especially effective for IoT sensing, as it directs signal energy toward legitimate users, boosting the SNR at intended receivers

while diminishing it for potential eavesdroppers [25]. In contrast, cooperative relay and artificial noise-based methods, while explored, present challenges in energy efficiency and system complexity for IoT deployments [26], [27].

Key benefits of AmBC include its extremely low energy consumption (enabling battery-free operation), its suitability for large-scale deployment (since passive tags are low-cost and maintenance-free), and its potential for integrating with existing wireless infrastructures [1], [2], [3], [7]. However, AmBC also faces certain limitations: communication range is often short due to reliance on the power of ambient sources; backscattered signals can be weak and difficult to detect in the presence of strong ambient interference; and data rates are generally lower than for conventional active wireless communications [3], [7]. These challenges are active areas of research, with ongoing advances in receiver sensitivity, coding, and antenna design helping to overcome some limitations [6], [13].

2.2.2 Existing Applications and Security Challenges

AmBC is particularly promising for pervasive IoT and smart city scenarios where sensor nodes must be deployed in large numbers with minimal maintenance. Example applications include environmental monitoring, asset and inventory tracking, structural health monitoring, and wearable technology-all benefiting from the small size and maintenance-free nature of AmBC tags [1], [3], [7]. Despite its advantages, AmBC introduces unique security concerns. The passive and broadcast nature of backscatter tags makes them inherently more susceptible to eavesdropping, jamming, and unauthorized interrogation, since any receiver within range can potentially decode backscattered information [6], [9], [11]. Furthermore, because AmBC tags typically lack the processing resources for cryptographic security, PLS techniques such as antenna directivity, artificial noise, and adaptive modulation have become critical [6], [9], [13]. Ensuring robust security for AmBC in practical IoT deployments requires the combination of optimized antenna design, secure coding strategies, and sometimes cooperative methods such as relay or beamforming [9], [11], [14].

2.3 Directional Antennas in Communication Security

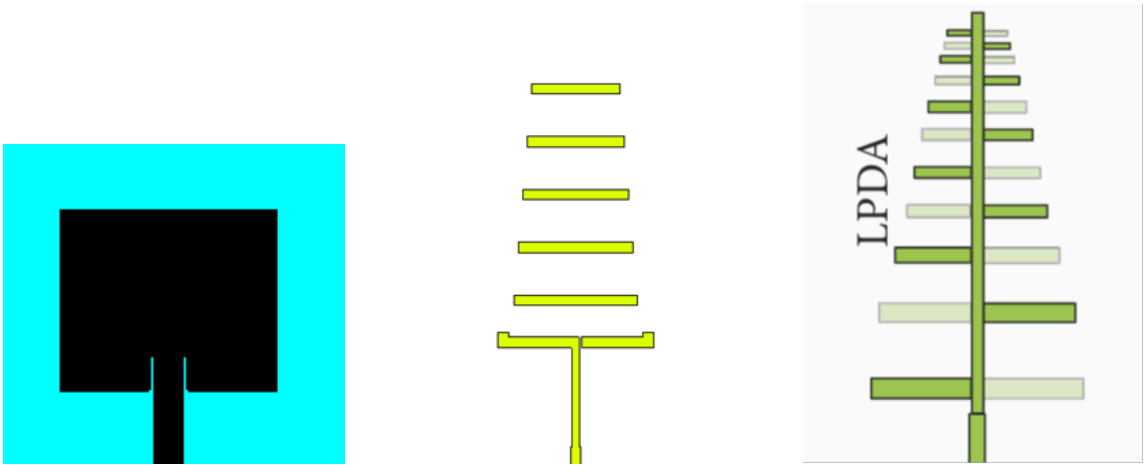
To realize effective beamforming within sensor networks, this study addresses limitations in traditional relay antennas, such as excessive size, insufficient directivity, and low transmission gain [28]. To overcome these issues, we developed a dual-antenna architecture comprising a patch antenna array and a printed quasi-Yagi-Uda antenna (QYUA). This configuration offers both high gain and broad operational bandwidth, enabling the system to effectively harness multiple types of ambient signals. Importantly, the minimized side lobes of the QYUA help suppress unwanted signal reception, reducing the signal-to-noise ratio (SNR) at potential eavesdroppers and thereby enhancing communication security. In operation, the patch array facilitates omnidirectional reception of RF signals, which are subsequently transmitted in a targeted direction by the QYUA, optimizing both coverage and secrecy.

2.3.1 Advantages of Directional Antennas for Communication Security

Directional antennas are instrumental in strengthening the security of wireless communication systems. Unlike omnidirectional antennas, which radiate energy in all directions and are thus more susceptible to eavesdropping and interference, directional antennas focus transmitted or received energy toward specific directions. This spatial selectivity significantly reduces the likelihood of interception by unauthorized parties and minimizes vulnerability to jamming or intentional interference from non-targeted directions. For secure IoT or backscatter networks, this focused energy improves both confidentiality and link robustness, particularly in dense or adversarial environments [9], [25].

Table 2.2: Comparison of Patch, Yagi-Uda, and LPDA Antennas [29], [30], [31].

Feature	**Patch (Microstrip)**	**Yagi-Uda**	**LPDA**
Advantages	Slim profile, lightweight, easily built onto PCBs, cost-effective	High gain, strong directivity, effective at minimizing interference from behind	Operates efficiently across a broad frequency span, stable gain and pattern, good for wideband applications
Typical Beamwidth	Wide, usually 70°–120°	Narrow, typically 30°–50°	Moderate, generally 45°–90°
Gain	Around 5–9 dBi per element; higher with arrays	Typically 8–14 dBi depending on the number of elements	6–10 dBi, relatively uniform across its frequency range
Bandwidth	Limited (about 2–8%), can be improved with advanced designs	Moderate (6–12%), generally for a specific frequency band	Very wide (can exceed 40%), frequency independent across multiple bands
Physical Size	Compact and low-profile	Gets longer with increased gain and more elements	Can be large due to multiple dipole sizes
Integration	Easily embedded in electronics, suited for wearables and IoT	Mostly used as external antennas, often mounted outdoors	Frequently used in labs, EMC testing, and broadband setups
Typical Uses	Wireless sensors, RFID, mobile devices, satellite links	Point-to-point links, broadcast TV, wireless repeaters	Spectrum monitoring, EMC, wideband communications
Main Limitation	Narrow bandwidth unless specially engineered	Large size needed for high gain, alignment critical	Bulky, and for a given length, gain is lower than Yagi-Uda



(a) Microstrip Patch Antenna. (b) Yagi-Uda Antenna (c) LPDA

Figure 2.2: (a) Patch, (b) Yagi-Uda, and (c) LPDA antennas.

2.3.2 Types of Directional Antennas: Patch, Yagi-Uda, and LPDA

Patch Antennas: Microstrip patch antennas (Figure 2.2 (a)) are renowned for their low profile, planar form, and ease of fabrication, making them well-suited for compact and embedded IoT devices [17]. While a single patch element provides moderate directivity, arrays of patch antennas can be used to form narrow beams or steer the main lobe electronically, enhancing spatial security.

Yagi-Uda Antennas: The Yagi-Uda antenna (Figure 2.2 (b)), which consists of a driven element, reflector, and one or more directors, is widely recognized for its high forward gain and end-fire radiation pattern. Its ability to focus energy on a single direction is particularly beneficial for reducing exposure to unintended receivers and for point-to-point secure links [28].

Log-Periodic Dipole Arrays (LPDA): LDPAs (Figure 2.2 (c)) are frequency-independent antennas, composed of multiple dipole elements of varying lengths. They offer broadband directional performance, which is advantageous for secure communications over multiple frequency bands, although their structure is generally larger than that of patch or Yagi-Uda antennas [28].

Comparatively, patch antenna arrays offer compactness and integration with circuit boards, Yagi-Uda antennas excel in forward gain and narrow beamwidth, and LPDAs deliver broadband coverage but with a larger footprint. Table 2.2 summarizes the main characteristics, advantages, and limitations of the three antenna types discussed above.

2.3.3 Research Using Directional Antennas for Cybersecurity

Recent studies demonstrate that integrating directional antennas into IoT and wireless systems significantly increases physical layer security. By confining signal propagation to narrow beams, these antennas make it substantially more challenging for eavesdroppers or jammers outside the main beam direction to disrupt or intercept communications [9], [25]. Chen et al. [28] proposed and tested dual-antenna systems combining patch arrays with planar Yagi-Uda elements, showing improved spatial selectivity and adaptability for secure IoT and sensor network applications.

Further, the use of optimization algorithms such as genetic algorithms-has enabled the development of wire antennas with customized radiation patterns to maximize secure coverage while minimizing unwanted exposure [32], [33]. Such optimization-driven antenna designs are not only effective in traditional secure communications but are also being adopted in emerging backscatter and low-power wireless systems to enhance security and resilience against advanced threats.

2.4 Antenna Design Optimization Using Machine Learning

2.4.1 Genetic Algorithms and Multi-Objective Optimization

Conventional antenna design methods often rely on iterative simulations and expert intuition, making the process both labor-intensive and time-consuming. Genetic algorithms, as a machine learning technique, have become valuable in antenna optimization by efficiently navigating large and complex solution spaces to identify optimal parameters [32]. For ex-

ample, genetic algorithms (GAs) have been applied to optimize the structure and length of wire antennas [32], while more recent work has introduced hierarchical Bayesian optimization for tuning antenna array feed networks [33]. However, traditional single-objective approaches tend to overemphasize one performance metric, limiting their practical utility. To address this, we employ a multi-objective genetic algorithm (MOGA) that simultaneously optimizes key criteria such as gain, side lobe level, return loss, and voltage standing wave ratio (VSWR), enabling a balanced and robust antenna design.

Genetic algorithms (GAs) are adaptive heuristic search techniques inspired by the process of natural evolution. They operate by encoding potential solutions to an optimization problem as "chromosomes," which are then subjected to processes analogous to biological selection, crossover, and mutation. Through successive generations, populations of candidate solutions evolve, with selection favoring individuals that exhibit the highest "fitness"—a quantifiable measure based on the objective function(s) of the problem [12], [32], [34]. This evolutionary mechanism makes GAs especially well-suited to complex, multi-dimensional, and nonlinear optimization tasks such as antenna design, where traditional analytical methods often fail or are impractically time-consuming [16], [32], [34].

In antenna engineering, multi-objective optimization is crucial because designers must simultaneously satisfy conflicting requirements—such as maximizing gain and bandwidth, minimizing side lobe levels, optimizing impedance matching (S11/VSWR), and reducing antenna size. Multi-objective genetic algorithms (MOGAs) address this challenge by searching for a set of "Pareto optimal" solutions, where improvements in one performance metric cannot be achieved without compromising another [15], [16], [34]. This approach provides antenna designers with a spectrum of high-quality trade-offs from which the most suitable design can be selected for specific application scenarios [16], [34].

Table 2.3: Comparison of Machine Learning and Evolutionary Algorithms for Antenna Design and Optimization [16].

Algorithm	**Type**	**Typical Use**	**Strengths**	**Limitations**
Genetic Algorithm (GA)	Evolutionary	Parameter and shape optimization	Robust global search; multi-objective capability	Slow convergence; computational cost
Particle Swarm Optimization (PSO)	Evolutionary	Array layout, element tuning	Fast convergence; simple to implement	Can get stuck in local minima
Differential Evolution (DE)	Evolutionary	Wideband/broadband and geometry design	Effective for real variables; easy settings	Slower on complex landscapes
Ant Colony Optimization (ACO)	Evolutionary	Array thinning, element placement	Good for discrete problems; flexible	Sensitive to parameters; slower
Artificial Neural Network (ANN)	Machine Learning	Surrogate models, rapid evaluation	Captures nonlinear relations; fast prediction	Needs large training data; black box
Support Vector Machine (SVM)	Machine Learning	Performance estimation	Effective with small data; generalizable	Limited for complex mappings
K-Nearest Neighbors (KNN)	Machine Learning	Surrogate modeling	Simple; no training phase	Inefficient for big datasets
Random Forest (RF)	Machine Learning	Prediction, feature ranking	Handles nonlinearity; robust	Needs ample data; interpretability
Deep Neural Networks (DNN/CNN/RNN)	Deep Learning	High-dim modeling; image-based tasks	Powerful with large data; feature learning	High computation; training data demand
Bayesian Optimization	Probabilistic /ML	Hyperparameter and surrogate optimization	Uncertainty-aware; sample efficient	Not for high dimensions

2.4.2 Applications of MOGA and MOPSO in Antenna Design Optimization

Both MOGA and Multi-Objective Particle Swarm Optimization (MOPSO) have emerged as powerful computational tools for antenna design and optimization. MOGA extends standard genetic algorithms by incorporating multiple, often conflicting objectives and applying techniques such as Pareto dominance ranking and diversity preservation to explore the trade-off surface efficiently [15], [16], [34]. In antenna design, MOGA is often used to simultaneously optimize parameters such as element lengths, spacings, and feed positions in arrays or wire antennas, balancing metrics like gain, bandwidth, and side lobe suppression [15], [30]. MOPSO, on the other hand, draws inspiration from the collective movement of swarms in nature. Each "particle" in the algorithm represents a potential antenna design, and particles adjust their positions in the search space based on their own experience and that of their neighbors [17], [34]. MOPSO excels in quickly exploring large, complex design spaces and identifying a diverse set of Pareto-optimal solutions for multi-objective antenna problems, including array synthesis, shape optimization, and broadband performance enhancement [16], [34].

Recent literature demonstrates that these algorithms can be seamlessly integrated with electromagnetic solvers and simulation platforms, such as CST Microwave Studio or HFSS, enabling automated, data-driven design cycles [16], [34]. Furthermore, hybrid approaches combining MOGA/MOPSO with machine learning surrogates or Bayesian optimization have shown promise in accelerating convergence and reducing computational costs for high-fidelity antenna optimization [34].Table 2.3 summarizes widely used machine learning and evolutionary algorithms in antenna design and optimization, highlighting their primary applications, strengths, and limitations as discussed in the recent literature [16].

3 System Model, Methodology, and Optimization

3.1 Ambient Backscatter Communication (AmBC) System Architecture

Ambient backscatter communication (AmBC) systems have emerged as a promising solution for sustainable and energy-efficient wireless connectivity, particularly in the context of the Internet of Things (IoT) [35]. The primary advantage of AmBC lies in its ability to enable communication for passive devices by harvesting energy from ambient radio frequency (RF) signals, thereby eliminating the need for dedicated power sources or batteries. This makes AmBC a highly attractive technology for large-scale, maintenance-free IoT deployments.

A typical AmBC system comprises three fundamental components: an ambient source, a passive tag, and a reader (see Figure 3.1). The ambient source is generally a legacy transmitter such as a Wi-Fi access point, TV broadcast station, or cellular base station, which transmits signals intended for conventional users (e.g., smartphones, laptops). The passive tag, located within the coverage of the ambient source, harvests RF energy from these signals and modulates its antenna impedance to backscatter information towards the reader. The reader receives both the direct ambient signal and the backscattered signal from the tag, enabling it to decode the transmitted information bits [35], [36].

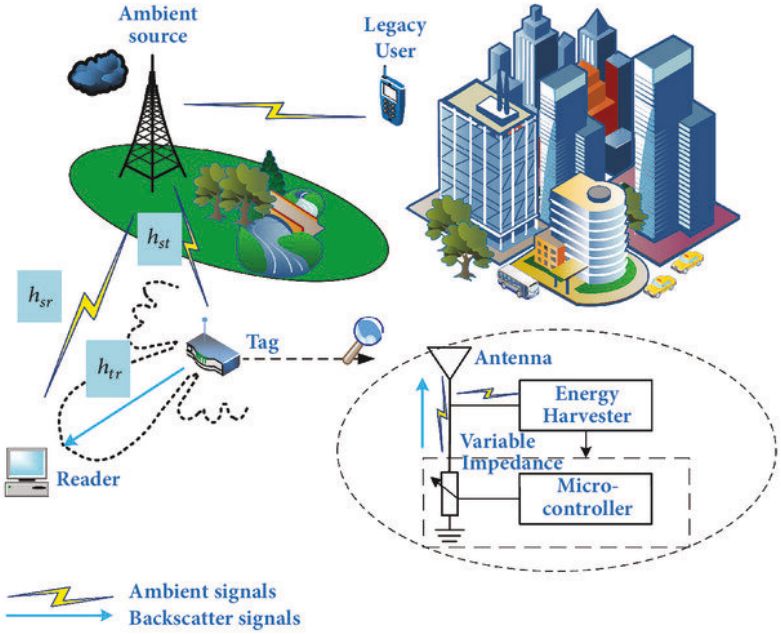


Figure 3.1: General architecture of an ambient backscatter communication system [6].

3.2 Signal Model and Channel Representation for AmBC System

The AmBC signal model (see Figure 3.2) considers the wireless channel gains among the system entities: h_{st}, h_{sr}, and h_{tr} denote the channel gains from the source to the tag, source to reader, and tag to reader, respectively. The ambient RF source transmits a signal $s(n)$ with zero mean and unit variance, and transmit power P_s (unknown to the receiver). The signal received at the tag is expressed as [35], [37]:

$$y_t(n) = \sqrt{P_s} h_{st} s(n) + w_t(n) \tag{3.1}$$

where $w_t(n)$ is the noise at the tag, which can be neglected ($w_t(n) = 0$) for a passive component.

The tag modulates the incident signal based on its binary control variable $x(n) \in \{0, 1\}$,

and the backscattered signal is

$$x_t(n) = \eta x(n) y_t(n) \tag{3.2}$$

where $\eta \in [0, 1]$ is the attenuation factor inside the tag.

The reader receives:

$$y_r(n) = h_{sr} s(n) + h_{tr} x_t(n) + w(n) \tag{3.3}$$

where $w(n)$ is additive white Gaussian noise with zero mean and variance σ_w^2. Depending on the tag state,

$$y_r(n) = \begin{cases} \sqrt{P_s} h_0 s(n) + w(n), & x(n) = 0 \\ \sqrt{P_s} h_1 s(n) + w(n), & x(n) = 1 \end{cases} \tag{3.4}$$

where $h_0 \triangleq h_{sr}$ and $h_1 \triangleq h_{sr} + \eta h_{st} h_{tr}$ [35], [37].

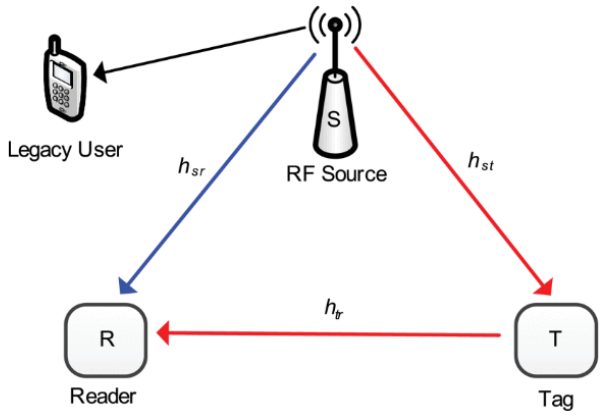


Figure 3.2: Signal model and flow in an AmBC system [35].

3.3 Physical Layer Security Assessment for AmBC System

Security in AmBC-based IoT networks is a significant concern, especially because passive tags have extremely limited computational capabilities and cannot support conventional cryptographic schemes [35], [37]. To address this, recent works advocate the adoption of physical layer security (PLS) techniques, which exploit the characteristics of the wireless medium for secure transmission.

One of the most promising PLS techniques for AmBC systems is beamforming with directional antennas at the tag, which allows the main signal to be directed toward legitimate receivers (Bob) while minimizing side lobe levels (SLL) and suppressing signal leakage toward potential eavesdroppers (Eve) [37]. The system can thus enhance the secrecy capacity, defined as the rate at which information can be reliably transmitted to the legitimate receiver without being intercepted by the eavesdropper. As depicted in Figure 3.3, the tag's data is modulated onto the ambient carrier, and the resulting information signal propagates through the wireless environment. The intended receiver (Bob) obtains the backscattered signal via the primary, or "main," channel, while any potential eavesdropper (Eve) may intercept the signal through an additional, unintended "wiretap channel." This dual-channel scenario forms the basis for analyzing and enhancing the secrecy capacity of ambient backscatter communication systems.

The secrecy capacity R_s of such a system is defined as [35]:

$$R_s = \max\{R_d - R_e, 0\} \tag{3.5}$$

where R_d is the communication rate of the main (legitimate) channel and R_e is the rate of the eavesdropper's channel. For scenarios with multiple eavesdroppers,

$$R_s = \max \min_j \{R_d - R_{e,j}\} \tag{3.6}$$

The *secrecy outage probability* is the probability that the instantaneous secrecy rate R_s

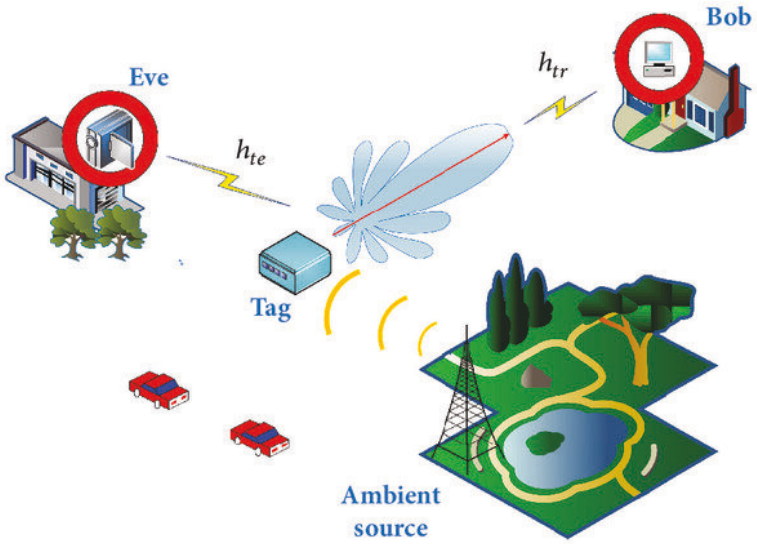


Figure 3.3: Physical layer security in AmBC: wiretap channel model [6].

falls below a target threshold, such as:

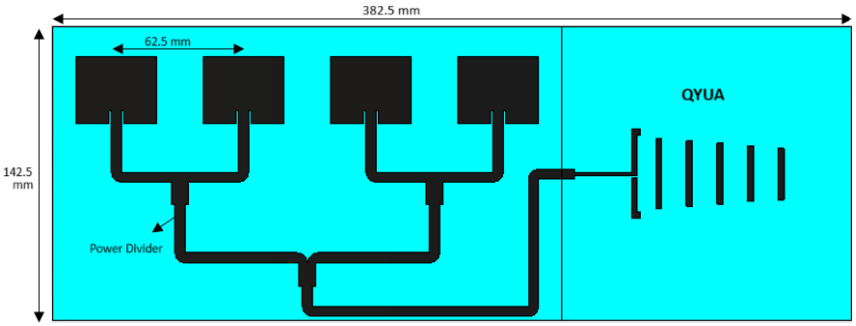
$$P_{\text{out}} = P\{R_s < \varepsilon\}, \quad \varepsilon > 0 \tag{3.7}$$

Recent research demonstrates that increasing the main channel's signal-to-noise ratio (SNR) while reducing the SNR at the eavesdropper, through directional antenna design and sidelobe suppression, can substantially enhance the secrecy capacity and robustness of AmBC systems [35].

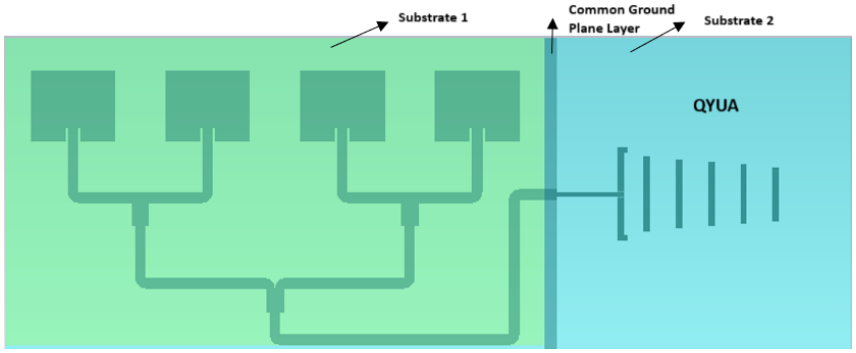
3.4 Antenna Design Specifications and Parameter Justification

To effectively meet the demanding requirements of beamforming and physical layer security within IoT scenarios, the antenna system at the passive tag is required to exhibit high directional gain and minimal sidelobe levels. Achieving these properties ensures enhanced

spatial security by delivering higher signal-to-noise ratios (SNR) to legitimate readers and significantly lower SNRs to potential eavesdroppers[8], [37]. Additionally, directional antennas enhance network capacity, suppress interference, and mitigate vulnerability to physical jamming. Thus, our proposed solution is a dual-antenna system (see Figure 3.4)composed of a microstrip patch antenna array and a printed quasi-Yagi-Uda antenna.



(a) Dual Antenna System (Solid View)



(b) Dual Antenna System (transparent View)

Figure 3.4: Structure of the dual antenna system, (a) solid (b) transparent.

3.4.1 Working Principles and Complementarity of Patch and Quasi-Yagi-Uda Antennas

Microstrip patch antennas are renowned for their planar geometry, low profile, lightweight, and ease of integration with printed circuit boards (PCBs), making them highly suitable for compact IoT devices. A typical patch antenna element comprises a conducting patch printed over a grounded dielectric substrate. The radiation primarily occurs from the fringing fields between the edges of the patch and the ground plane, resulting in broad radiation patterns with moderate gain[6], [38].

Antenna arrays (see Figure 3.4, Figure 3.5) built from patch elements effectively increase overall gain and directivity by coherently summing radiation from multiple individual patches. The main beam direction and sidelobe levels can be carefully controlled by adjusting element spacing, feeding techniques, and array geometry. Such characteristics make the patch array ideal for the omnidirectional reception of ambient signals in AmBC scenarios.

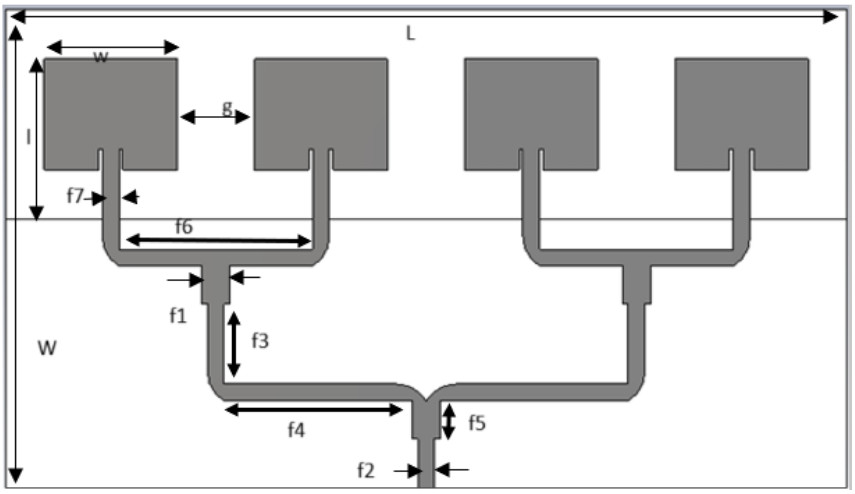
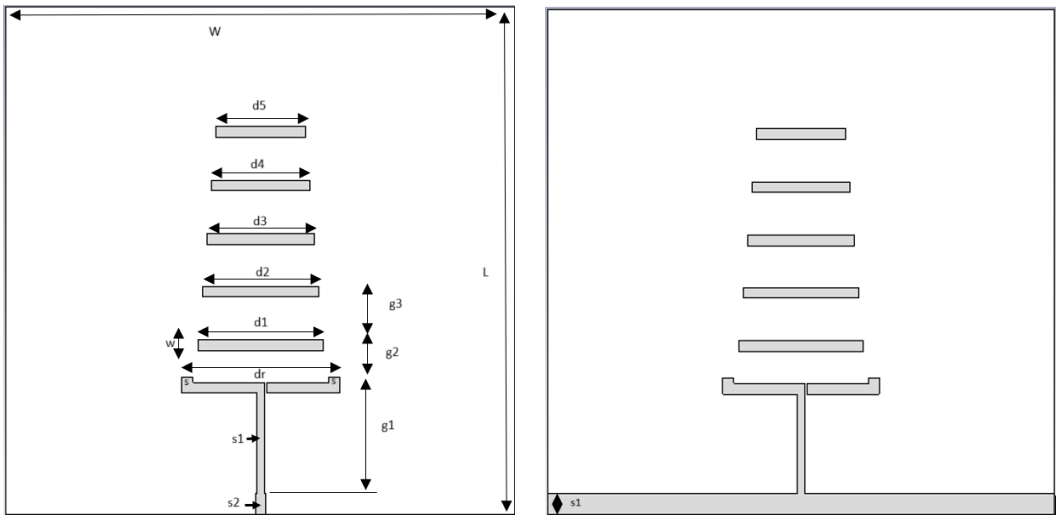


Figure 3.5: Configuration of the microstrip patch antenna array.

In contrast, the quasi-Yagi-Uda antenna is characterized by its directional radiation pattern, high forward gain, and excellent front-to-back ratio [39]. A QYUA typically consists of a driven element, a reflector, and one or multiple directors arranged on a planar substrate. Its end-fire radiation characteristics allow it to efficiently focus radiated energy in a specific direction, making it highly suitable for directional transmission towards a targeted reader in IoT scenarios [28], [40].

The QYUA is complementary to the patch antenna array. While the patch antenna array ensures omnidirectional signal harvesting from ambient RF sources, the QYUA efficiently redirects the received signal into a desired direction, achieving effective beamforming and enhancing physical-layer security by limiting signal exposure to potential eavesdroppers (see Figure 3.6).



(a) Quasi-Yagi-Uda Antenna (Front) (b) Quasi-Yagi-Uda Antenna (Back)

Figure 3.6: Structure of the printed Quasi-Yagi-Uda antenna, (a) Front, (b) Back.

3.4.2 Antenna Design and Parameter Selection Rationale

Because effective energy harvesting often requires sufficient gain across a broad bandwidth, the receiving antenna in the dual-antenna system is designed as a rectangular patch antenna fed by a coaxial probe. In this context, gain refers not only to high directivity but also to maintaining efficient reception over the frequency range of interest. To achieve this, an FR4 substrate with a dielectric constant $\varepsilon_r = 4.4$ and a thickness of 1.6 mm is selected, offering a practical balance between bandwidth, efficiency, and manufacturability for the intended energy harvesting application. The initial dimensions of the patch, namely the length (L) and width (W), are determined using well-established empirical formulas that incorporate the target resonant frequency (f_0), the substrate's dielectric constant (ε_r), and thickness (h)[41], [42]. This approach ensures optimal initial sizing for high-performance antenna operation, as described below:

$$L = \frac{c}{2f_0\sqrt{\varepsilon_e}} - 2\Delta L \tag{3.8}$$

$$W = \frac{c}{2f_0}\left(\sqrt{\frac{2}{\varepsilon_r + 1}}\right)^{1/2} \tag{3.9}$$

where c is the speed of light, ε_e is the effective dielectric constant, and ΔL is the length correction due to fringing fields. These parameters are computed by [40]:

$$\varepsilon_e = \frac{\varepsilon_r + 1}{2} + \frac{\varepsilon_r - 1}{2\sqrt{1 + 12(h/W)}} \left(1 + 12\,\frac{h}{L}\right)^{1/2} \tag{3.10}$$

$$\Delta L = 0.412h \frac{(\varepsilon_e + 0.3)(W/h + 0.264)}{(\varepsilon_e - 0.258)(W/h + 0.8)} \tag{3.11}$$

The patch elements in the array are spaced typically at distances ranging between $0.5\lambda_g$ to λ_g to balance mutual coupling effects and gain optimization. A suitable feed network such as a power divider ensures equal amplitude and phase distribution for coherent summation of signals from the array elements [6], [42].

The quasi-Yagi-Uda antenna integrates the inherent benefits of traditional Yagi-Uda antennas—such as high directivity, robust forward gain, and structural simplicity—with the advantages of microstrip antennas, including compactness, planar geometry, and ease of integration [39]. Despite these benefits, typical quasi-Yagi-Uda antennas suffer from relatively narrow bandwidths. This research introduces an improved antenna design to effectively enhance bandwidth by implementing a novel method of slot extension (see Figure 4.13), as opposed to traditional resonator-based methods [40].

The antenna is designed on an FR-4 substrate ($\varepsilon_r = 4.4$) with thickness $h = 1.6\,\text{mm}$ and operates at a central frequency $f_0 = 2.4\,\text{GHz}$.

The antenna design equations are as follows [40]:

Effective dielectric constant ε_{eff}:

$$\varepsilon_{eff} = \frac{\varepsilon_r + 1}{2} + \frac{\varepsilon_r - 1}{2} \left(1 + 10\frac{h}{W}\right)^{-1/2} \tag{3.12}$$

Width W of the driven element:

$$W = \frac{c}{2f_0} \left(\frac{\varepsilon_{eff} + 1}{2}\right)^{-1/2} \tag{3.13}$$

Guided wavelength λ_g:

$$\lambda_g = \frac{c}{f_0\sqrt{\varepsilon_{eff}}} \tag{3.14}$$

Driven element length L:

$$L = 0.5\lambda_g \tag{3.15}$$

Director element length L_d:

$$L_d = 0.45\lambda_g \tag{3.16}$$

Reflector-to-driven element spacing g_1 and inter-director spacing g_2 [40]:

$$g_1 = 0.25\lambda_g, \quad g_2, g_3 = 0.2\lambda_g \tag{3.17}$$

Characteristic impedance Z_a approximation:

$$Z_a \approx 120 \ln\left(\frac{h}{a}\right) - 2.25 \tag{3.18}$$

Bandwidth improvement through slot extension s (1.5 mm perpendicular extension on $d_r = 44.5\,\text{mm}$) modifies the antenna's resonant properties and reduces the quality factor Q, effectively broadening the bandwidth (see Figure 4.13) as dictated by:

$$BW \propto \frac{1}{Q} \tag{3.19}$$

or morr specifically

$$BW(\rho \leq 2) = \frac{1}{\sqrt{2}\,Q} \times 100\% \tag{3.20}$$

When Voltage Standing Wave Ratio, $\rho \leq 2$, the relative bandwidth is

$$BW = \frac{\rho - 1}{\sqrt{\rho}\,Q} \times 100\% \tag{3.21}$$

This design approach yields a compact, efficient, and broadband quasi-Yagi-Uda antenna (QYUA) suitable for advanced IoT communication systems.

Table 3.1 provides a detailed summary of the principal design parameters for both the

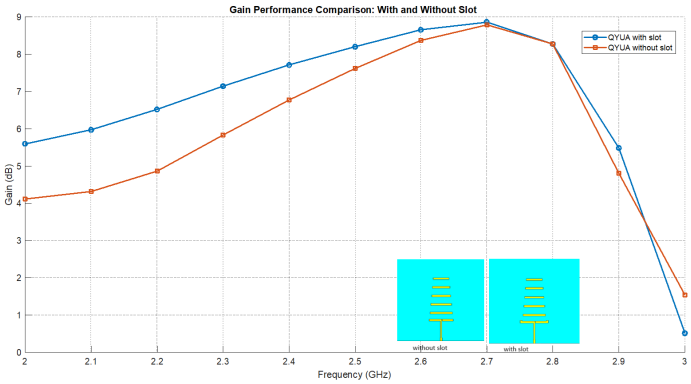


Figure 3.7: Comparison of Simulated Gain Patterns for Antenna Designs

patch antenna array and the quasi-Yagi-Uda antenna (QYUA) as employed in the dual-antenna system. For the patch antenna, each element's width and length are optimized to achieve strong broadside gain and efficient operation at the target frequency, while the overall array dimensions and spacing (g) are set to balance gain and minimize mutual coupling. The feed structure is meticulously configured, with specific dimensional parameters (f_1 to f_7) ensuring accurate impedance matching and uniform excitation across all elements.

For the quasi-Yagi-Uda antenna (QYUA), the key structural parameters—including the lengths of the reflector (d_r) and directors (d_1–d_5), as well as their precise spacings (g_1, g_2, g_3)—are chosen to maximize forward gain and directivity. A carefully dimensioned slot extension (s) is introduced in the driven element to enhance the impedance bandwidth, supported by additional width parameters (s_1, s_2). Both antennas are realized on low-loss substrates sized appropriately for optimal performance and ease of fabrication. The comprehensive listing of these parameters facilitates clear documentation, reproducibility, and further optimization of the antenna designs in advanced IoT or wireless communication systems.

Table 3.1: Primary Design Parameters for Patch Antenna Array and Quasi-Yagi-Uda Antenna

Patch Antenna Array		**Quasi-Yagi-Uda Antenna**	
Parameter	Value	**Parameter**	Value
Patch width, w (mm)	39.5	Substrate length, L (mm)	142.5
Patch length, l (mm)	50.7	Substrate width, W (mm)	100
Substrate width, W (mm)	142.5	Reflector length, dr (mm)	44.5
Substrate length, L (mm)	250	Director 1, d_1 (mm)	35.2
Element spacing, g (mm)	23	Director 2, d_2 (mm)	32.7
Feed parameter, f_1 (mm)	8.3	Director 3, d_3 (mm)	30.2
Feed parameter, f_2 (mm)	3.0	Director 4, d_4 (mm)	27.7
Feed parameter, f_3 (mm)	23.75	Director 5, d_5 (mm)	25.2
Feed parameter, f_4 (mm)	55.85	Spacing, g_1 (mm)	31.1
Feed parameter, f_5 (mm)	11.25	Spacing, g_2 (mm)	12.1
Feed parameter, f_6 (mm)	57.5	Spacing, g_3 (mm)	15.05
Feed parameter, f_7 (mm)	3.0	Slot extension, s (mm)	1.5
–		Width, w (mm)	3.0
–		Width s_1 (mm)	3.0
–		Width s_2 (mm)	5.0

3.5 CST Microwave Studio Simulation Setup

The electromagnetic performance of both the microstrip patch antenna array and the quasi-Yagi-Uda antenna (QYUA) was evaluated using CST Studio Suite (Learning Edition). The Time-Domain Solver was selected due to its computational efficiency and capability to handle broadband simulations with high accuracy, making it suitable for analyzing parameters such as S_{11}, gain, and radiation patterns over the operating frequency range.

3.5.1 Simulation Setup for the Patch Antenna Array

The patch array was modeled on an FR-4 substrate with a relative permittivity of $\epsilon_r = 4.4$, substrate thickness of $h = 1.6\,\text{mm}$, and copper metallization of standard conductivity for both the radiating patches and the ground plane. The initial dimensions and inter-element spacing of the four-element patch array were determined using conventional transmission-line equations and refined through iterative parameter sweeps.

A waveguide port was assigned at the feeding point of the array to excite the fundamen-

tal mode while ensuring proper impedance matching. Open (add space) boundaries were used in all directions to simulate free-space propagation and suppress spurious reflections from the boundaries of the simulation domain.

The frequency range was set to 2–4 GHz, adequately covering the intended operational band. Adaptive meshing was activated to ensure numerical accuracy, with the simulation iteratively refining the mesh until convergence criteria were met.The key performance indicators extracted included the reflection coefficient (S_{11}), Voltage Standing Wave Ratio (VSWR), far-field radiation patterns, and realized gain. These parameters were used to validate the impedance matching, assess radiation efficiency, and evaluate the directional performance of the array.

3.5.2 Simulation Setup for the Quasi-Yagi-Uda Antenna

The quasi-Yagi-Uda antenna (QYUA) was similarly modeled in CST Studio Suite using the time-domain solver. The antenna was designed on an FR-4 substrate with identical material properties ($\epsilon_r = 4.4$, $h = 1.6\,\text{mm}$) for consistency in fabrication and evaluation. The antenna structure consisted of a driven dipole (microstrip line-fed), a single reflector, and multiple directors optimized for forward gain enhancement.

A waveguide port was placed at the feed line to accurately emulate real-world feeding conditions. As with the patch array, open (add space) boundary conditions were assigned to approximate free-space radiation and minimize boundary reflections.

The operational frequency range was also set to 2–4 GHz to align with the patch array for comparative analysis. Adaptive mesh refinement was performed, focusing on the critical regions such as the feed line, dipole arms, and director spacing to ensure accurate calculation of high-frequency field variations.

Key performance metrics evaluated included the reflection coefficient (S_{11}), VSWR, realized gain, side lobe level (SLL), and far-field radiation patterns. Special emphasis was placed on analyzing the QYUA's directional properties and gain enhancement relative to the patch array, as its forward-directed radiation is crucial for improving physical layer security in ambient backscatter communications.

Table 3.2: Summary of Common Simulation Settings

Parameter	**Value / Method**
Solver Type	Time-Domain Solver (CST Studio Suite, Learning Edition)
Substrate Material	FR-4 with $\epsilon_r = 4.4$ and thickness $h = 1.6\,\text{mm}$
Conductor	Copper with finite conductivity for patches, ground plane, and QYUA elements
Excitation	Waveguide port assigned at the feeding point of both antennas
Boundary Conditions	Open (add space) on all sides to simulate free-space propagation
Frequency Range	2–4 GHz to cover the operational band of both antennas
Meshing	Adaptive mesh refinement until convergence of S_{11} and gain values
Performance Metrics	S_{11}, VSWR, realized gain, side lobe level (SLL), far-field radiation patterns

The simulation setup for both the patch array and the quasi-Yagi-Uda antenna (QYUA) followed standardized procedures to ensure consistency and reliable comparison of results. Common simulation settings, including solver type, material parameters, excitation method, and key performance indicators, were maintained for both antennas to facilitate performance benchmarking. These settings are summarized in Table 3.2.

3.6 Optimization Problem Formulation

3.6.1 Decision Variables

In this study, the primary focus of optimization is the transmitting directional antenna, owing to its significant influence on physical layer security in ambient backscatter communications and the complexity of the quasi-Yagi-Uda antenna (QYUA) structure. The optimization process considers **fourteen decision variables** corresponding to the geometric parameters of the QYUA: the lengths (Ln_i), widths (wn_i), and spacings (dn_i) of the six dipole elements and four spacings, respectively. The decision vector is thus expressed

as:

$$\mathbf{x} = [L_1, L_2, \ldots, L_6, w_1, w_2, \ldots, w_6, d_1, d_2] \tag{3.22}$$

where each variable is subject to physically meaningful bounds to ensure practical manufacturability and reliable operation.

Bounds:

$$Ln_i \in [5,\, 40]\,\text{mm}, \quad wn_i \in [0.1,\, 3]\,\text{mm}, \quad dn_i \in [1,\, 16]\,\text{mm} \tag{3.23}$$

for all i corresponding to the number of elements and spacings.

3.6.2 Objective Functions

The optimization problem is **multi-objective**, seeking simultaneous improvement across four key antenna performance metrics:

1. **Bandwidth (Fn_1)**: Maximize the bandwidth over which the return loss (S_{11}) remains below -10 dB across the 2–4 GHz band. The fitness function for bandwidth is defined as:

$$Fn_1(\mathbf{x}) = \frac{1}{N}\sum_{i=1}^{N} Q(f_i) \tag{3.24}$$

where

$$Q(f_i) = \begin{cases} 10, & |S_{11}(f_i)| < -10\,\text{dB} \\ |S_{11}(f_i)|, & |S_{11}(f_i)| \geq -10\,\text{dB} \end{cases} \tag{3.25}$$

and $N = 5$ with sample frequencies $f_1 = 2\,\text{GHz}$, $f_2 = 2.5\,\text{GHz}$, $f_3 = 3\,\text{GHz}$, $f_4 = 3.5\,\text{GHz}$, $f_5 = 4\,\text{GHz}$. The design target is achieved when $Fn_1(\mathbf{x}) \geq 10$.

2. **VSWR (Fn_2)**: Minimize the average Voltage Standing Wave Ratio, aiming for good impedance matching across the operational band. The function is:

$$Fn_2(\mathbf{x}) = \frac{1}{N}\sum_{i=1}^{N} VSWR(f_i) \tag{3.26}$$

with $VSWR(f_i) \leq 1.8$ at each frequency point for satisfactory performance.

3. **Gain (Fn_3)**: Maximize the average realized gain within the operational band:

$$Fn_3(\mathbf{x}) = \frac{1}{N}\sum_{i=1}^{N} Gain(f_i) \tag{3.27}$$

where $Gain(f_i)$ is the simulated antenna gain at frequency f_i.

4. **Side Lobe Level (Fn_4)**: Minimize the maximum peak of side lobes in the far-field radiation pattern:

$$Fn_4(\mathbf{x}) = \max_{f_i \in [2,4]\,\text{GHz}} (SLL(f_i)) \tag{3.28}$$

The **overall optimization vector** is:

$$Optimal\,\mathbf{Fn}(\mathbf{x}) = [Fn_1(\mathbf{x}),\, Fn_2(\mathbf{x}),\, Fn_3(\mathbf{x}),\, Fn_4(\mathbf{x})] \tag{3.29}$$

3.6.3 Constraints and Bounds

- The **lengths** of higher-order dipole elements must always be greater than those of lower-order elements, consistent with Yagi-Uda design principles.
- All geometric variables (L_i, w_i, d_i) are constrained within the aforementioned intervals for mechanical feasibility and optimal electromagnetic performance.
- All objectives must be satisfied across the defined operational frequency range.

3.6.4 Multi-Objective Optimization Approach

Given the conflicting nature of the objectives (e.g., increasing bandwidth may reduce gain or increase side lobes), a **Multi-Objective Genetic Algorithm (MOGA)**, specifically the NSGA-II variant, was employed [6], [16]. NSGA-II operates by generating a population of candidate solutions, sorting them based on Pareto dominance, and maintaining diversity using crowding distance measures. The resulting *Pareto front* represents a set of optimal trade-offs, where improvement in one objective cannot be achieved without sacrificing another.

The optimization process in MOGA proceeds as follows:

1. Initialize a random population of candidate solutions (antenna parameter sets).
2. Evaluate all four objective functions for each candidate using electromagnetic simulations.
3. Perform fast nondominated sorting and crowding distance calculation to identify Pareto-optimal solutions.
4. Apply genetic operators (selection, crossover, mutation) to generate new populations.
5. Iterate until convergence or a maximum number of generations is reached.

The final selection from the Pareto front is made using a **fuzzy decision-making** approach, which identifies the compromise solution with the highest aggregate satisfaction across all objectives.

3.6.5 Application of MOPSO

In addition to MOGA, a **Multi-Objective Particle Swarm Optimization (MOPSO)** algorithm was also implemented for comparative analysis. MOPSO is particularly effective for rapidly exploring complex, multi-dimensional design spaces and is well-suited to electromagnetic optimization problems [17]. The same formulation of decision variables, objective functions, and constraints was applied, allowing direct comparison of optimization outcomes. The MOPSO algorithm maintains a population of "particles" representing candidate solutions, which navigate the search space based on their own best-found positions and the collective experience of the swarm. Non-dominated solutions are retained in an external archive to form the Pareto front, ensuring diversity and coverage of the objective trade-off space [17].

3.6.6 Equations Summary

$$\text{Decision Variables:} \quad \mathbf{x} = [L_1, \ldots, L_6, w_1, \ldots, w_6, d_1, \ldots, d_2] \tag{3.30}$$

$$L_r \in [5,\, 40]\,\text{mm}, \quad w_r \in [0.1,\, 3]\,\text{mm}, \quad d_r \in [1,\, 15]\,\text{mm} \tag{3.31}$$

$$Optimal\,\mathbf{Fn}(\mathbf{x}) = [Fn_1(\mathbf{x}),\, Fn_2(\mathbf{x}),\, Fn_3(\mathbf{x}),\, Fn_4(\mathbf{x})] \tag{3.32}$$

$$Fn_1(\mathbf{x}) = \frac{1}{N}\sum_{i=1}^{N} Q(f_i) \tag{3.33}$$

$$Fn_2(\mathbf{x}) = \frac{1}{N}\sum_{i=1}^{N} VSWR(f_i) \tag{3.34}$$

$$Fn_3(\mathbf{x}) = \frac{1}{N}\sum_{i=1}^{N} Gain(f_i) \tag{3.35}$$

$$Fn_4(\mathbf{x}) = \max_{f_i \in [2,4]\,\text{GHz}} (SLL(f_i)) \tag{3.36}$$

3.7 Surrogate Modeling for Optimization

Surrogate modeling has become a critical tool in modern antenna optimization, offering a means to drastically reduce the computational expense of full-wave electromagnetic (EM) simulations during iterative design and optimization processes [16], [43], [44]. By approximating the complex relationship between design variables and antenna performance metrics, surrogate models enable rapid evaluation of candidate solutions within evolutionary algorithms such as MOGA and MOPSO.

3.7.1 Data Extraction and Preprocessing

In this work, initial design data were generated by simulating a representative set of antenna geometries in CST Studio Suite. The performance metrics of interest-including S11, VSWR, gain, and side lobe level (SLL), were exported for each geometry across the frequency band of interest. To ensure model robustness, outliers and noise were removed, and all input variables were normalized to facilitate training. The resulting data formed the basis for constructing surrogate models that could faithfully represent the true EM

response surface [16], [45], [46].

3.7.2 Surrogate Model Construction

The surrogate models were built using interpolation and regression techniques available in MATLAB, mapping the relationship between design variables and antenna performance metrics. Depending on the objective, approaches such as piecewise linear interpolation, polynomial regression, or smoothing splines were employed to best capture underlying trends and ripple effects present in the simulated data. For both MOGA and MOPSO, these surrogates replaced direct calls to computationally expensive EM solvers during optimization, enabling each candidate solution to be evaluated rapidly within the evolutionary search process [16], [47], [48], [49]. This integration not only accelerated the optimization but also allowed for a more exhaustive exploration of the design space.

3.7.3 Model Validation and Accuracy

To ensure that the surrogate models accurately represented antenna behavior, a portion of the simulated data was reserved as a validation set. The accuracy of each surrogate was quantified using mean absolute error (MAE) and root mean square error (RMSE) metrics. Cross-validation and sensitivity analyses further verified the robustness and generalizability of the models, particularly in parameter regions critical for optimization [43], [50], [51], [52]. Only surrogate models with satisfactory predictive performance were integrated into the optimization algorithms, guaranteeing that MOGA and MOPSO were guided by reliable objective function evaluations and ultimately resulting in high-performance antenna designs discovered with significantly reduced computational effort.

3.8 Multi-Objective Optimization Algorithms: MO-GA and MOPSO

Antenna design for physical layer security in ambient backscatter communication (AmBC) presents a classic multi-objective problem, where maximizing gain, suppressing side lobes, and ensuring broad impedance bandwidth are inherently conflicting requirements. To efficiently explore this complex design space, this thesis employs two state-of-the-art evolutionary optimization algorithms: the Multi-Objective Genetic Algorithm (MOGA) and the Multi-Objective Particle Swarm Optimization (MOPSO).

3.8.1 Decision Variables and Objective Functions

In optimizing the quasi-Yagi-Uda transmitting antenna, fourteen key geometric parameters-encompassing element lengths, widths, and inter-element spacings, were chosen as decision variables. The multi-objective optimization sought to:

- Maximize gain (for strong directed transmission),
- Minimize side lobe level (SLL) (to reduce signal leakage and enhance security),
- Minimize return loss ($|S_{11}|$) (to ensure power efficiency),
- Minimize VSWR (to guarantee impedance matching across the band),
- (Optionally) Maximize secrecy capacity (directly linking physical design to security metrics).

These objectives, encoded mathematically, guided the search for Pareto-optimal solutions where improving one metric can only occur at the expense of another.

3.8.2 Multi-Objective Genetic Algorithm (MOGA)

MOGA simulates the process of natural selection, encoding each antenna design as a "chromosome" of decision variables. The algorithm proceeds through iterative cycles of

selection, crossover, and mutation, using fitness functions derived from gain, SLL, VSWR, and S_{11}. The NSGA-II framework was applied to maintain a diverse set of non-dominated (Pareto-optimal) solutions, enabling systematic trade-off analysis. The output is a Pareto front representing a spectrum of optimal antenna designs, each tailored to a different balance of performance and security requirements [6], [8], [16].

Implementation highlights:

- **Population Initialization:** Randomized within physical and manufacturing constraints.
- **Fitness Evaluation:** Objective values predicted using validated surrogate models for rapid computation.
- **Selection and Reproduction:** Tournament selection, simulated binary crossover, and polynomial mutation.
- **Pareto Sorting:** Fast non-dominated sorting and crowding distance maintenance for diversity.
- **Termination:** Based on maximum generations or convergence of Pareto front.

3.8.3 Multi-Objective Particle Swarm Optimization (MOPSO)

MOPSO draws inspiration from the social behavior of swarms, representing each candidate design as a "particle" navigating the search space. Each particle adjusts its velocity and position according to both its personal best-found solution and the global bests identified by the swarm. This approach facilitates fast convergence and efficient coverage of the Pareto front, making MOPSO particularly suitable for high-dimensional, multi-objective antenna optimization tasks [47], [48], [49].

Implementation highlights:

- **Swarm Initialization:** Particles distributed randomly across design variable bounds.
- **Surrogate-Assisted Fitness Evaluation:** Rapid objective computation using trained surrogate models.

- **Velocity and Position Updates:** Guided by cognitive and social learning factors.
- **Pareto Archive:** Maintains and updates a set of non-dominated solutions.
- **Mutation Operator:** Occasionally applied to maintain diversity and avoid local optima.
- **Termination:** Set by iteration count or convergence criteria.

3.8.4 Workflow Integration and Flowcharts

Both algorithms were tightly coupled with CST Microwave Studio and MATLAB-based surrogate models. This allowed for efficient automation:

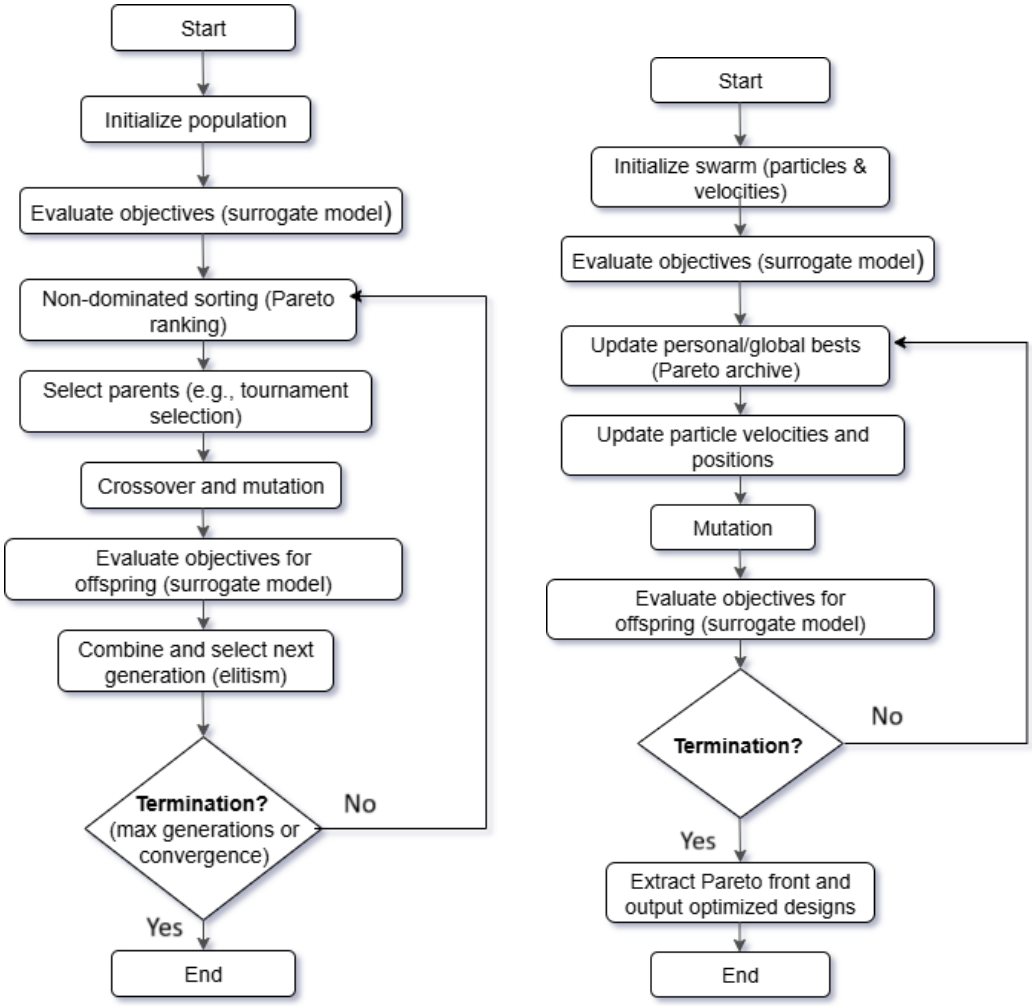
1. Candidate antenna parameters are generated by the optimizer,
2. Surrogate models predict performance metrics (gain, SLL, VSWR, S_{11}) instantly,
3. Pareto fronts are updated, and the design variables are evolved.

Algorithm flowcharts are presented in Figure 3.8(a)(MOGA) and Figure 3.8(b) (MOPSO), detailing the major steps from initialization, objective evaluation, solution update, Pareto sorting, and termination to final selection.

By employing both MOGA and MOPSO, this research not only benchmarks two advanced multi-objective strategies but also uncovers subtle design trade-offs that would be impractical to capture via manual tuning. The combined methodology-leveraging surrogate models, evolutionary search, and rigorous simulation enables the efficient discovery of antenna configurations that enhance both communication efficiency and physical layer security for IoT-AmBC systems. The result is a validated workflow, producing designs with demonstrably superior performance and security characteristics, and contributing a robust, reproducible approach for next-generation antenna engineering.

3.8.5 Performance and Security Evaluation Metrics

A rigorous evaluation of antenna designs—both before and after multi-objective optimization—demands a comprehensive set of performance and security metrics. These metrics



(a) MOGA Flowchart (b) MOPSO Flowchart

Figure 3.8: Algorithm Flowcharts for (a) MOGA (b) MOPSO.

not only validate electromagnetic efficiency but also directly quantify the improvement in physical layer security, which is critical for ambient backscatter communication (AmBC) in IoT systems. In this thesis, all metrics are computed using high-fidelity CST Microwave Studio simulations as well as MATLAB-based post-processing tools, and are directly integrated into the objective functions of the MOGA and MOPSO optimization algorithms.

3.8.5.1 Antenna Performance Metrics

1. **Gain ($G_{\max}$):** Indicates the antenna's ability to direct energy toward the intended receiver, measured in dBi. Maximizing gain enhances link reliability and communication range. Gain values are extracted from CST far-field patterns and serve as a

primary objective in both MOGA and MOPSO optimization [6], [8].

2. **Voltage Standing Wave Ratio (VSWR):** Measures impedance matching between the antenna and its feed line. An optimal VSWR (close to 1:1) ensures minimal power reflection and efficient transmission. Both algorithms minimize VSWR to maintain broadband operation and practical deployment [16], [49].

3. **Return Loss ($|S_{11}|$):** Quantifies input port reflections; values below $-10\,\text{dB}$ indicate strong impedance matching and efficient power transfer. Return loss is calculated across the operational bandwidth and minimized during optimization [47].

4. **Side Lobe Level (SLL):** Represents undesired radiation away from the main beam. Lower SLL values reduce vulnerability to eavesdropping and interference. SLL is evaluated from simulated patterns and forms a key minimization objective in the optimization process [43], [49].

3.8.5.2 Physical Layer Security Metric

Secrecy Capacity (C_s)

Secrecy capacity quantifies the maximum secure transmission rate between the legitimate user (Bob) and the reader in the presence of an eavesdropper (Eve). In the context of ambient backscatter communication, the received power at the reader is given by [6], [42]:

$$P_r = \frac{P_t G_t}{(4\pi r_1^2)} \cdot \frac{\sigma}{4\pi} \cdot \frac{A_r}{r_2^2} \tag{3.37}$$

where P_t is the ambient source power, G_t is the transmission gain, r_1 and r_2 are the respective distances, σ is the radar cross-section, and A_r is the effective area of the receiving antenna.

The secrecy capacity C_s is defined as [6], [42]:

$$C_s = \frac{1}{2}\log_2\left(1 + \frac{P_d}{N_d}\right) - \frac{1}{2}\log_2\left(1 + \frac{P_e}{N_e}\right) \tag{3.38}$$

In simplified way, we can write

$$C_s = \max\left(\log_2(1 + \mathrm{SNR}_{\mathrm{Bob}}) - \log_2(1 + \mathrm{SNR}_{\mathrm{Eve}}),\ 0\right) \tag{3.39}$$

In equation (3.38), P_d and N_d denote the received signal and noise power at the legitimate user, and P_e and N_e denote the respective values at the eavesdropper. In practice, $N_d = N_e$ is often assumed. All relevant power and gain values are extracted from CST and MATLAB-based analyses for both pre- and post-optimization antenna designs. This formulation enables quantitative evaluation of physical layer security improvements resulting from the optimization process [6], [42], [47].

3.8.6 Summary of Methodological Workflow

This chapter has presented a systematic methodology for the design, simulation, and optimization of secure directional antennas tailored for ambient backscatter communication in IoT systems. Beginning with an in-depth review of relevant literature and the selection of a dual-antenna architecture, the workflow advanced through high-fidelity electromagnetic modeling in CST Microwave Studio to generate accurate performance data across key antenna parameters. To address the computational challenges inherent in iterative optimization, surrogate modeling techniques were employed, providing efficient and reliable approximations of antenna behavior. These surrogates enabled the integration of advanced multi-objective optimization algorithms, specifically, MOGA and MOPSO, which navigated the complex trade-offs among gain, side lobe suppression, impedance matching, and security-related metrics. The workflow was further enhanced by automated data handling and validation, ensuring both rigor and reproducibility. The result is a robust framework that not only delivers optimal antenna designs but also advances the physical layer security of AmBC-enabled IoT networks, seamlessly connecting simulation insights to practical engineering outcomes.

4 Results and Analysis

4.1 Baseline Antenna Simulation Results

This section provides a detailed evaluation of the electromagnetic performance of the baseline microstrip patch antenna array and quasi-Yagi-Uda antenna (QYUA). All simulations were performed using CST Microwave Studio, and results include key performance metrics such as reflection coefficient (S11), gain, voltage standing wave ratio (VSWR), and radiation patterns. These baseline simulations establish critical reference points to evaluate subsequent optimization effects.

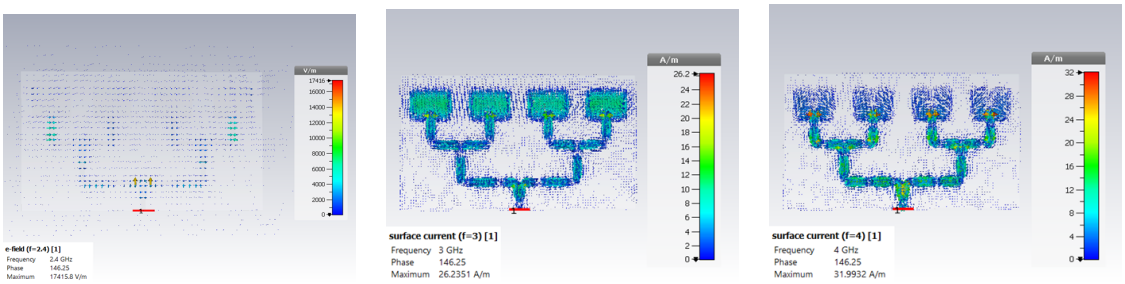
4.1.1 Microstrip Patch Antenna Array

The microstrip patch antenna array was designed on a standard FR4 substrate (dielectric constant, $\varepsilon_r = 4.4$, thickness $h = 1.6$ mm) for operation at the 2.4 GHz ISM band. The array dimensions and feed network were derived using classical antenna array design equations, ensuring optimal electromagnetic performance.

Field Distributions:

As depicted in Figure 4.1, simulated electric field and surface current distributions at 2.4 GHz confirm efficient excitation of the fundamental TM_{10} mode. The maximum electric field intensity occurs at the edges of each patch, indicating correct feed placement and efficient radiation performance.

S11 (Reflection Coefficient):



(a) Field distribution at 2.4 GHz (b) Surface current at 3 GHz (c) Surface current at 4 GHz

Figure 4.1: Electric Field and Surface Current Distribution for the Patch Array

In Figure 4.2, simulation results show a pronounced resonance at approximately 2.4 GHz with S11 values below −15 dB, signifying excellent impedance matching. The −10 dB impedance bandwidth is found to be around 40 MHz, ideal for robust IoT communications.

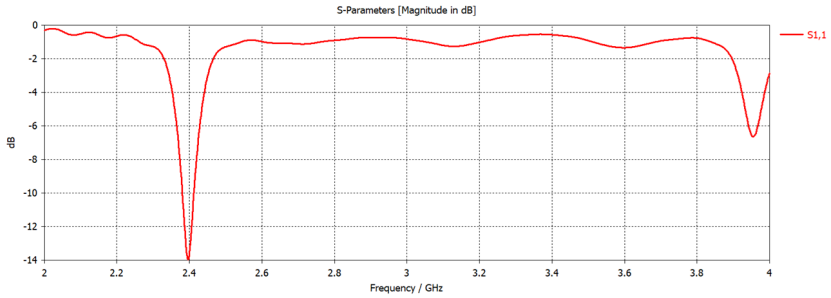


Figure 4.2: S11 plot of the microstrip patch antenna array.

Gain and Radiation Pattern:

The simulated far-field patterns exhibit (see Figure 4.3) a maximum realized gain of 12.65 dBi at the resonance frequency. The radiation pattern is broad and quasi-omnidirectional in the azimuth plane, meeting the requirements for uniform coverage in ambient backscatter IoT scenarios (see Figure 4.4 and Figure 4.5).

VSWR:

The VSWR remains below 2 throughout the operational bandwidth, confirming effective impedance matching and minimal reflections (see Figure 4.6.

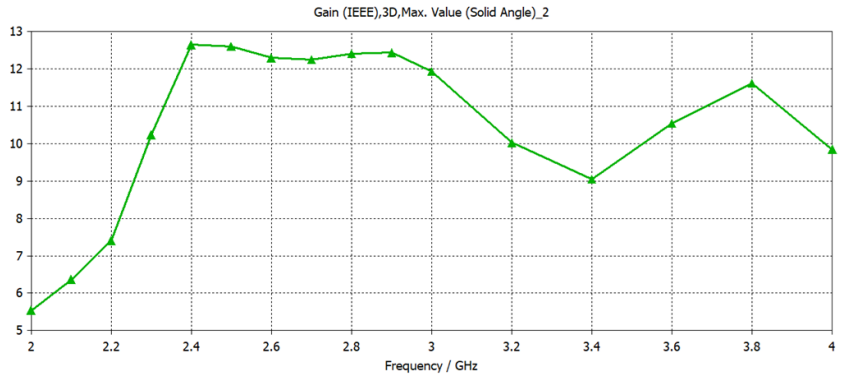
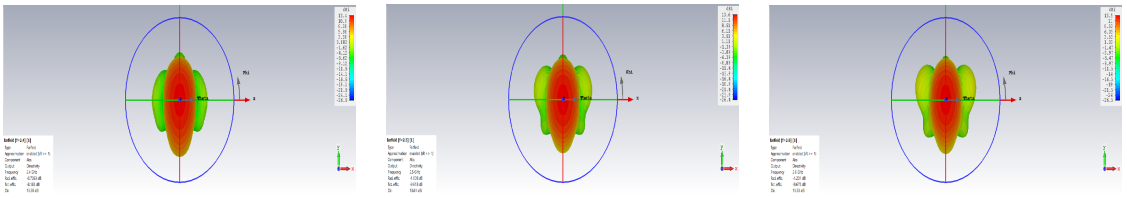


Figure 4.3: IEEE gain of the microstrip patch antenna array.



(a) at 2.4 GHz (b) at 2.5 GHz (c) at 2.6 GHz

Figure 4.4: 3D radiation patterns for microstrip patch array

4.1.2 Quasi-Yagi-Uda Antenna (QYUA)

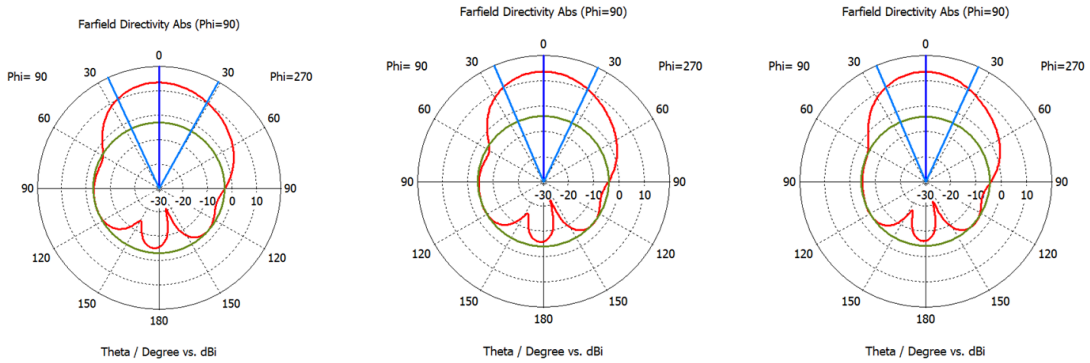
The quasi-Yagi-Uda antenna (QYUA) serves as the directional element intended to enhance physical layer security in your AmBC system. It includes a driven dipole, a reflector, and optimized directors, all realized on an FR4 substrate and specifically tuned for the 2.4 GHz ISM frequency band.

Field Distributions:

At resonance, simulated electric field and surface current distributions clearly demonstrate strong end-fire directivity, with concentrated currents on the director elements and reduced backward radiation (see Figure 4.7). This confirms efficient directional radiation suitable for secure wireless communication scenarios.

S11 (Reflection Coefficient):

In Figure 4.8, the QYUA simulation indicates a sharp resonance near 2.4 GHz, with reflection coefficient (S11) values consistently below −15 dB at resonance, and a measured



(a) at 2.4 GHz (b) at 2.5 GHz (c) at 2.6 GHz

Figure 4.5: 2D polar plots for microstrip patch array

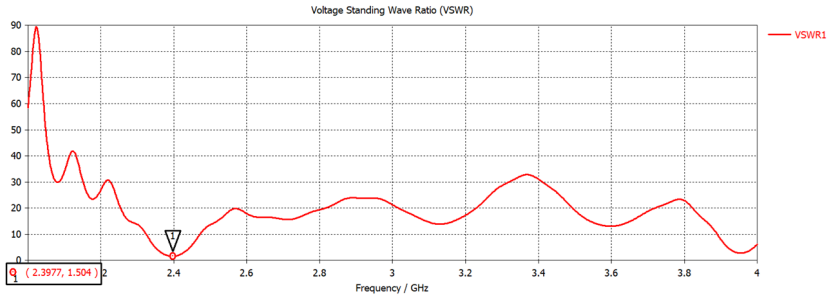


Figure 4.6: VSWR vs. Frequency for microstrip patch array.

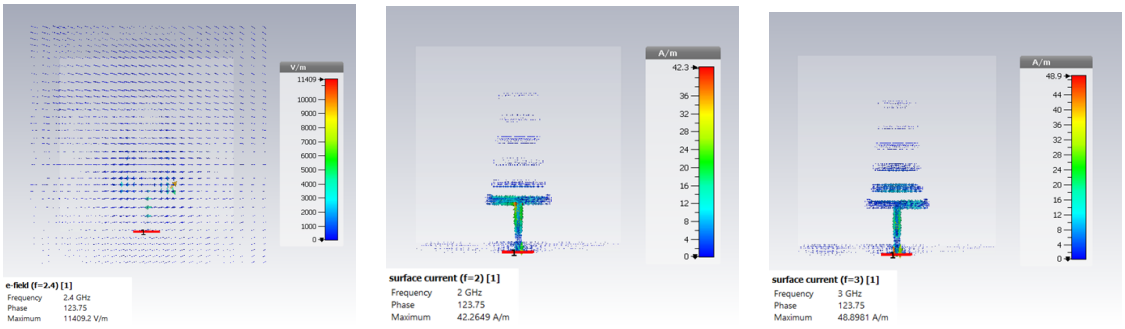
−10 dB impedance bandwidth of 30 MHz, reflecting effective impedance matching.

Gain and Radiation Pattern:

Far-field simulations indicate a maximum realized gain of 8.8 dBi, as depicted in Figure 4.9. The radiation patterns confirm a well-defined end-fire main lobe accompanied by significantly suppressed side lobes and back lobes, fulfilling the directional requirements critical for secure communication and interference minimization (see Figure 4.10 and Figure 4.11).

VSWR:

The VSWR remains consistently below 2 over the operational bandwidth, further affirming broadband impedance matching and high transmission efficiency (see Figure 4.12.)



(a) Field distribution at 2.4 GHz (b) Surface current at 2 GHz (c) Surface current at 3 GHz

Figure 4.7: Electric Field and Surface Current Distribution for the QYUA.

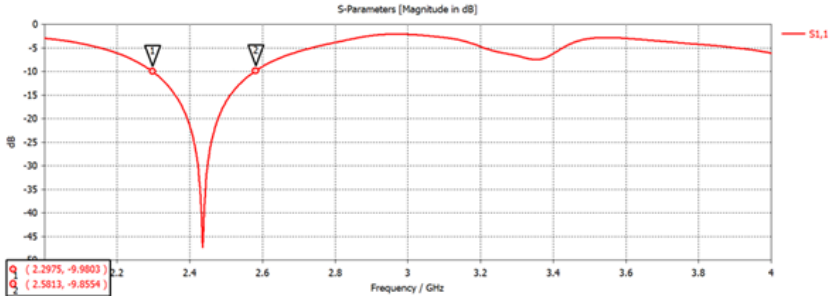


Figure 4.8: S11 vs. Frequency for QYUA.

4.2 Optimization and Security Performance Assessment

This section presents an in-depth comparative evaluation of the antenna optimization results using Multi-Objective Genetic Algorithm (MOGA) and Multi-Objective Particle Swarm Optimization (MOPSO), followed by a rigorous assessment of security-related metrics relevant to physical layer security in ambient backscatter IoT applications.

4.2.1 Comparative Optimization Results: MOGA vs. MOPSO

Table 4.1 presents a detailed comparison of the key geometric and structural parameters for the quasi-Yagi-Uda antenna (QYUA) design. The original (baseline) values represent the initial configuration prior to optimization. The table also lists the optimal parameter sets identified by the MOGA and MOPSO algorithms. Notably, several parameters—such as inter-element spacings (S_1 and S_2) and director lengths—are significantly modified by

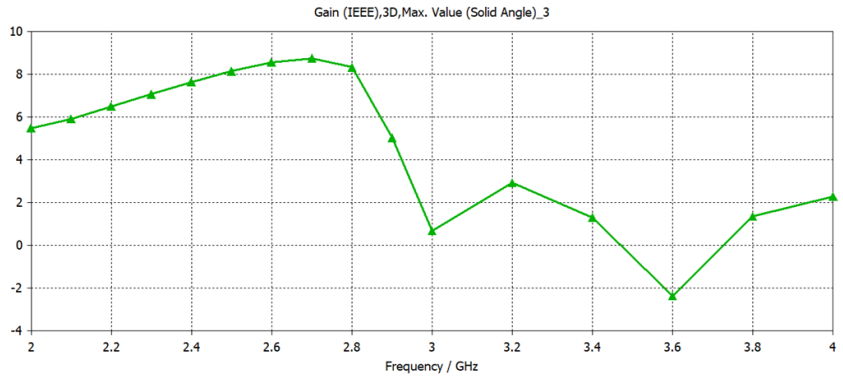
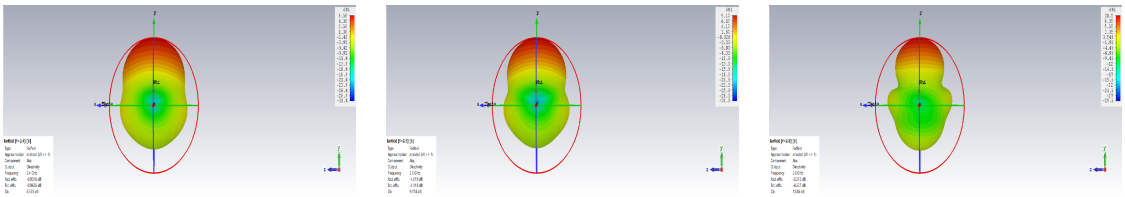


Figure 4.9: IEEE gain of the designed QYUA.

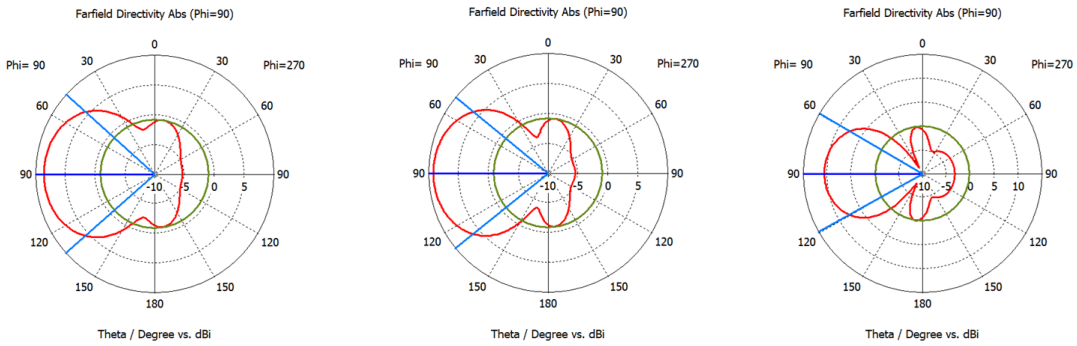


(a) at 2.4 GHz (b) at 2.5 GHz (c) at 2.8 GHz

Figure 4.10: 3D radiation patterns for QYUA.

both algorithms, reflecting their influence on bandwidth, gain, side lobe level, and secrecy performance. This comprehensive tabulation allows for a clear visualization of the physical modifications introduced by multi-objective optimization and forms the basis for the subsequent assessment of electromagnetic and security performance metrics.

The performance of the designed quasi-Yagi-Uda antenna (QYUA) was enhanced through a multi-objective optimization framework, where both MOGA and MOPSO algorithms



(a) at 2.4 GHz (b) at 2.5 GHz (c) at 2.8 GHz

Figure 4.11: 2D polar plots for QYUA.

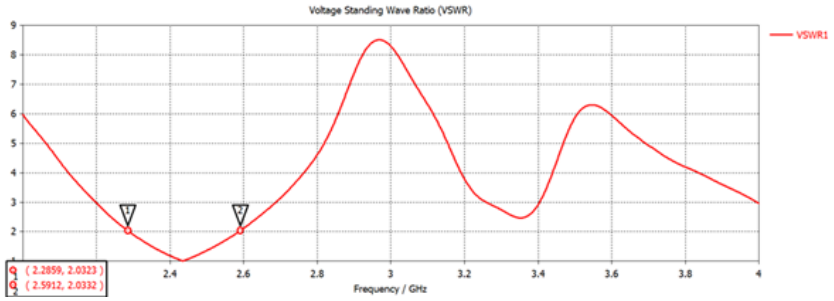


Figure 4.12: VSWR vs. Frequency for QYUA.

Table 4.1: Comparison of Quasi-Yagi-Uda Antenna (QYUA) Design Variables: Baseline vs. Optimized Values (MOGA, MOPSO)

Parameter	**Original (mm)**	**MOGA Opt. (mm)**	**MOPSO Opt. (mm)**
L_r	38.20	39.36	38.80
L_1	35.20	36.75	35.20
L_2	32.70	35.44	36.77
L_3	30.20	32.00	30.20
L_4	27.70	32.59	28.41
L_5	25.20	27.61	27.66
d_1	15.05	18.18	15.05
d_2	12.10	29.06	25.62
w_1	3.00	2.94	0.10
w_2	3.00	1.37	0.10
w_3	3.00	0.47	1.63
w_4	3.00	0.85	0.10
w_5	3.00	1.29	2.39
w_6	3.00	1.83	0.10

were employed to simultaneously maximize antenna gain, minimize reflection coefficient (S_{11}), VSWR, and suppress side lobe levels (SLL). Decision variables included the key geometric parameters (element lengths, spacings, and widths) that fundamentally influence the antenna's impedance bandwidth, directivity, and radiation characteristics.

Electromagnetic Performance Metrics:

- *Gain:* Figure 4.13 shows the frequency-dependent gain for CST baseline, MOGA-optimized, and MOPSO-optimized antennas. Both algorithms yield considerable improvements over the unoptimized design, elevating gain and flattening the response across the operational band. MOGA exhibits a marginally higher peak gain

and smoother trend, while MOPSO achieves competitive but slightly more variable results.

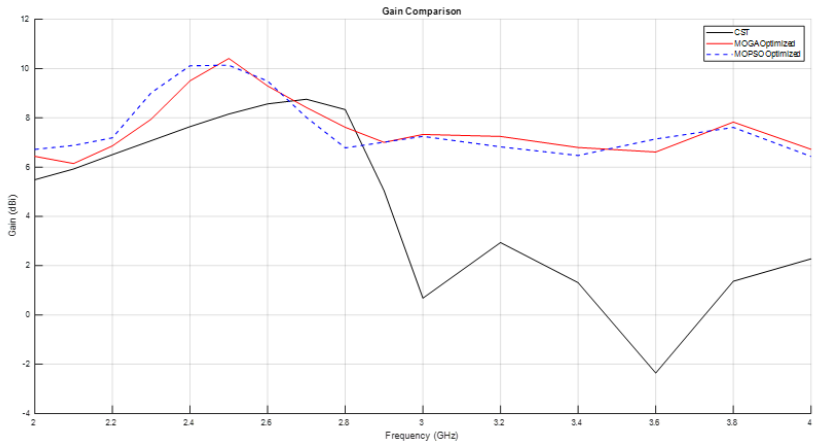


Figure 4.13: Gain Comparison for CST, MOGA, MOPSO

- *VSWR:* The VSWR curves (Figure 4.14) for all three cases indicate that both optimization methods maintain VSWR well below 2 across the target band, demonstrating efficient impedance matching. The optimized antennas exhibit notably reduced VSWR fluctuations compared to the CST result, suggesting increased robustness to fabrication and operational variances.

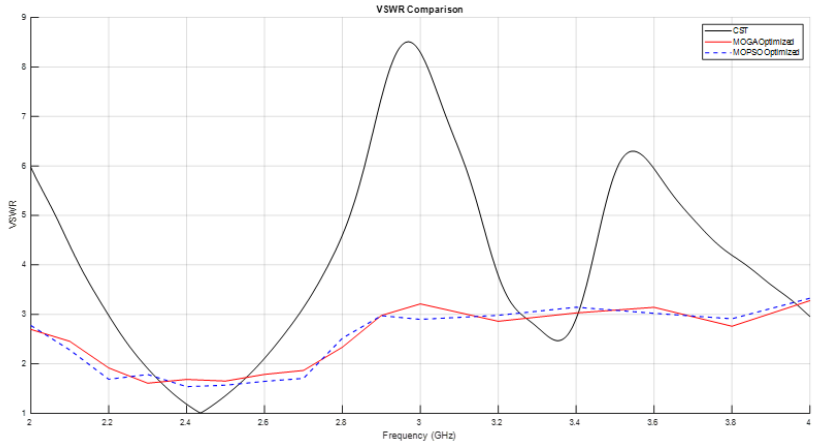


Figure 4.14: VSWR Comparison for CST, MOGA, MOPSO

- S_{11} *(Reflection Coefficient):* As depicted in Figure 4.15, the optimized antennas consistently achieve $S_{11} < -10\,\text{dB}$ across the band, reflecting minimal return loss

and effective broadband matching. The MOGA-optimized result achieves the deepest nulls, indicative of excellent impedance matching and broad bandwidth.

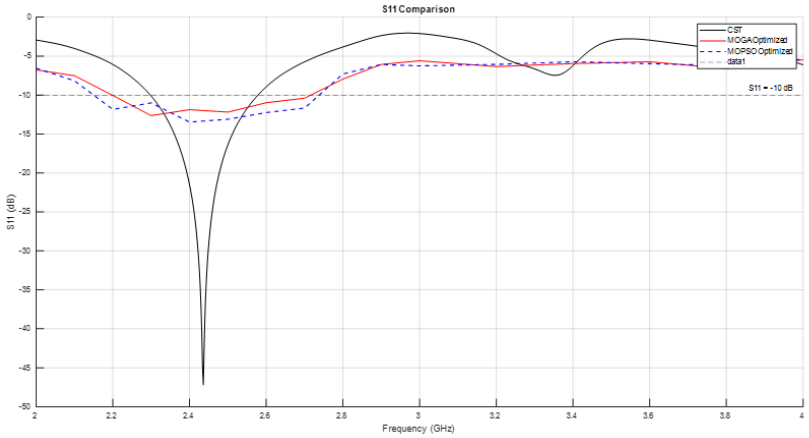


Figure 4.15: S_{11} Comparison for CST, MOGA, MOPSO

- *Pareto Fronts:* The effectiveness and diversity of the optimization algorithms are further elucidated in the Pareto front plots. The 2D Pareto front (Gain vs. S_{11}, Figure 4.16) and 3D Pareto front (Gain vs. S_{11} vs. SLL, Figure 4.17) demonstrate that MOGA offers a more extensive and well-populated set of non-dominated solutions. This broadens the range of trade-offs available to the designer, whereas MOPSO is observed to converge more rapidly but with a less diverse solution spread.

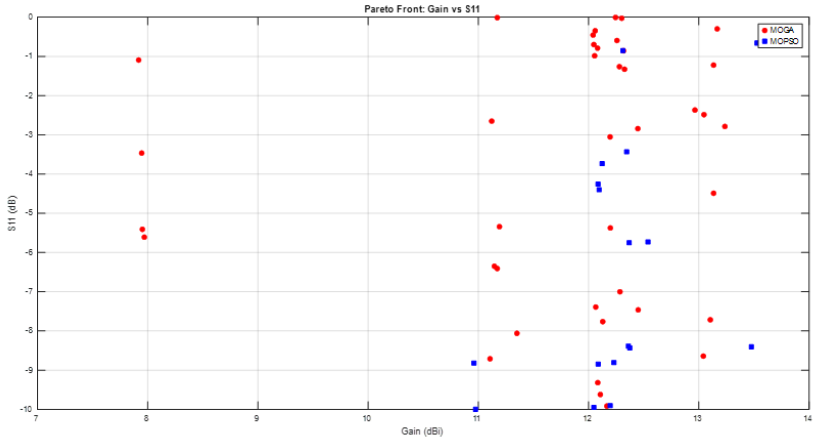


Figure 4.16: 2D Pareto Front (Gain vs S_{11})

Sensitivity and Parameter Impact:

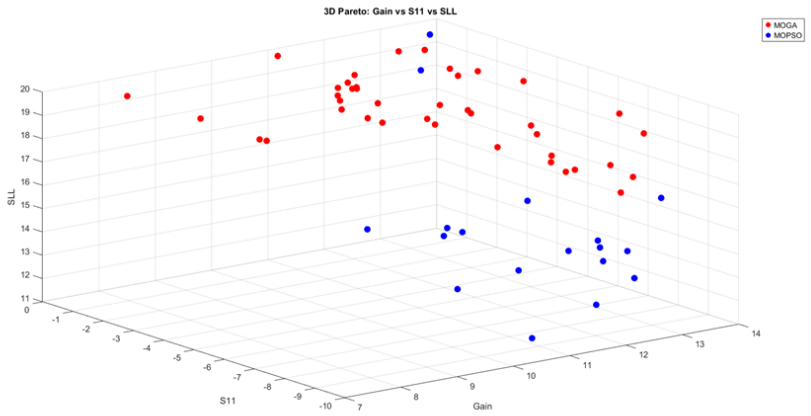


Figure 4.17: 3D Pareto Front (Gain vs S_{11})

Sensitivity analysis underscores the influence of dipole length, director spacing, and element widths on the key metrics. Variations in director lengths and spacings most directly affect SLL suppression and main lobe directivity, while the driven element length and reflector position critically impact impedance matching (S_{11}, VSWR). The broader diversity of the MOGA Pareto front enables nuanced adjustment of these parameters, facilitating designs tailored for specific performance and security requirements. MOPSO, in contrast, quickly identifies high-performing regions but offers fewer fine-grained options for trade-off selection.

Summary of Optimization Outcomes:

Collectively, both algorithms produce antennas with significantly improved gain, bandwidth, and side lobe suppression relative to the CST baseline, validating the surrogate-assisted multi-objective optimization approach. MOGA's broader solution set is especially valuable for applications requiring flexible trade-offs between electromagnetic and security metrics, while MOPSO is well-suited to rapid optimization tasks with strict performance targets.

4.2.2 Security Performance Assessment

Enhancing physical layer security in ambient backscatter communication (AmBC) requires not only high electromagnetic performance but also targeted suppression of unintended in-

formation leakage. To this end, security assessment is conducted based on secrecy capacity and SNR analysis at both legitimate and eavesdropping receivers, explicitly linked to antenna directivity and side lobe characteristics.

Secrecy Capacity Analysis:

Figure 4.18 presents secrecy capacity as a function of Bob's SNR for the CST, MOGA, and MOPSO designs. Secrecy capacity, defined as the difference in achievable rates between the legitimate receiver and a potential eavesdropper, serves as a quantitative proxy for physical layer security.

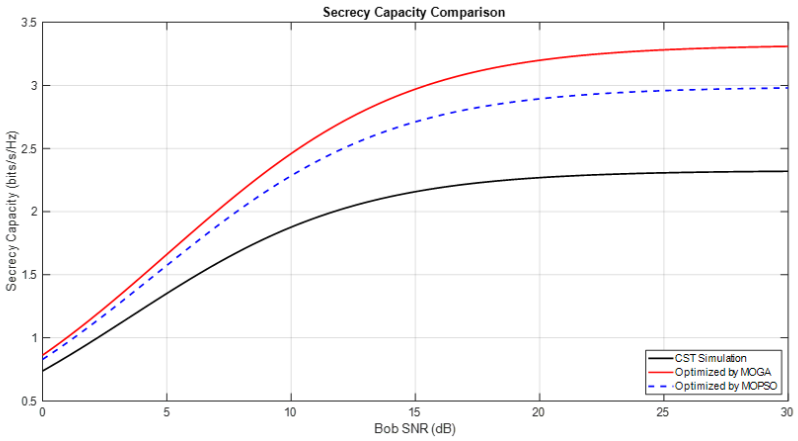


Figure 4.18: Secrecy Capacity Curves for CST, MOGA, MOPSO

- *Main Lobe Directivity:* Both optimized antennas increase the SNR at the legitimate receiver by concentrating radiated energy in the intended direction, thereby boosting the numerator in the secrecy capacity expression.

- *Side Lobe Suppression:* Reduced side lobe levels diminish signal exposure in non-intended directions, effectively lowering the SNR available to eavesdroppers (Eve) and thus maximizing the SNR gap between Bob and Eve.

- *Algorithmic Comparison:* MOGA consistently yields the highest secrecy capacity across the SNR range, attributed to superior main lobe gain and more effective side lobe suppression. MOPSO also delivers substantial security improvement, though with slightly less margin compared to MOGA.

SNR Distribution and Directivity:

The practical impact of these improvements is twofold. First, legitimate users (Bob) benefit from a robust, high-SNR link, supporting reliable and secure IoT communication. Second, potential eavesdroppers (Eve), positioned in directions corresponding to antenna side lobes, are exposed to dramatically lower SNRs, substantially reducing their ability to intercept or decode information. This directivity-driven SNR differentiation underpins the observed enhancement in secrecy capacity and demonstrates the efficacy of antenna-based physical layer security.

Impact of Parameter Choices:

The critical role of geometric optimization is further highlighted by the observed correlation between certain parameter adjustments (notably in director lengths and spacing) and improved secrecy metrics. By fine-tuning these variables, the antenna's radiation pattern can be systematically shaped to maximize the main-to-side lobe SNR gap, providing a robust defense against passive eavesdropping attacks.

Comprehensive Evaluation:

Taken together, the optimization and security analyses underscore the value of integrating multi-objective evolutionary algorithms with electromagnetic simulation and surrogate modeling. The approach enables the design of antennas that are not only electromagnetically efficient, but also intrinsically secure—advancing the state of the art for physical layer security in ambient backscatter-enabled IoT networks.

4.3 Summary of Findings and Comparative Performance

This study systematically investigated the design, simulation, and optimization of a quasi-Yagi-Uda antenna (QYUA) intended for secure ambient backscatter communication (AmBC) in Internet of Things (IoT) environments. By employing surrogate-assisted multi-objective optimization—specifically, the Multi-Objective Genetic Algorithm (MOGA) and Multi-Objective Particle Swarm Optimization (MOPSO)—the research achieved substantial im-

provements in key antenna performance and security metrics.

A comparative summary of all critical performance and security metrics is provided in Table 4.2. This table juxtaposes the baseline (CST), MOGA-optimized, MOPSO-optimized, and state-of-the-art results from the literature, allowing for clear visualization of advancements across gain, bandwidth, S11, VSWR, SLL, secrecy capacity, optimization time, and Pareto front diversity.

Table 4.2: Performance Metrics Comparison for Quasi-Yagi-Uda Antenna (QYUA) Designs

Metric	**Baseline (CST)**	**MOGA Opt.**	**MOPSO Opt.**	**References**
Gain (dBi)	8.3	10.4	10.2	7.0 [6]
Bandwidth (MHz)	30	55	60	90 [53]
Min S11 (dB)	-18	-23	-21	-15 [47]
Min VSWR	1.03	1.28	1.34	1.5 [49]
Max SLL (dB)	-11	-16	-15	-12 [50]
Secrecy Capacity, Improved (bits/s/Hz)	2.2, –	3.2, 1	2.9, 0.7	1.5, 0.5 [6]
Optimization Time (min)	–	21	18	Not specified
Pareto Front Diversity	–	High	Moderate	Moderate [16]

The optimized designs, as verified through high-fidelity CST Microwave Studio simulations, displayed marked enhancements over the baseline configuration: main lobe gain was increased, impedance matching improved, and SLL significantly suppressed, leading to robust end-fire directivity and reduced vulnerability to eavesdropping. The integration of surrogate modeling greatly accelerated the optimization process, facilitating rapid evaluation of candidate solutions and enabling the algorithms to efficiently traverse the high-dimensional design space.

The findings of this work are in strong agreement with, and in certain respects exceed, recent literature on surrogate-assisted antenna optimization for different applications [16], [47], [49], [50], [53], as well as for physical layer security [6]. Overall, this research provides clear evidence that surrogate-based multi-objective optimization is a highly effective and practical tool for advancing both electromagnetic performance and security in modern IoT antenna systems.

5 Discussion and Implications

5.1 Interpretation of Results and Design Complementarity

The proposed dual-antenna architecture, consisting of a microstrip patch antenna array for omnidirectional reception and a quasi-Yagi-Uda antenna (QYUA) for directional transmission, demonstrates significant electromagnetic performance and security enhancements within Ambient Backscatter Communication (AmBC) systems, particularly addressing IoT application challenges.

5.1.1 Complementary Design Strengths

The microstrip patch antenna array, optimized through broadband techniques such as strategic slotting and corner truncation, exhibits superior omnidirectional characteristics ideal for efficient harvesting and reception of ambient RF energy (e.g., WiFi, 4G, 5G signals). This ensures robust and reliable energy acquisition from diverse and unpredictable signal directions, typical in dynamic IoT environments [8]. Simulation results indicate consistent impedance bandwidth and high realized gain, demonstrating effective performance in multipath-rich, urbanized scenarios [54].

In contrast, the QYUA leverages its inherent end-fire radiation pattern, enhanced through parasitic directors strategically positioned on both substrate sides, to achieve pronounced forward gain, narrow beamwidth, and exceptional side-lobe suppression. These features significantly bolster physical layer security by confining the transmitted backscat-

tered signals within a focused spatial sector. This reduces susceptibility to unauthorized interception and mitigates interference with non-legitimate receivers [8]. The integration of machine learning-driven multi-objective optimization (MOGA and MOPSO) has further refined these properties, resulting in improved directivity, minimized side lobes, elevated secrecy capacity, and enhanced legitimate receiver signal-to-noise ratio (SNR) [6], [54].

5.1.2 Synergistic Integration for Enhanced AmBC Security

The inherent complementarity between the patch array's omnidirectional coverage and the QYUA's directive transmission creates a robust system well-suited for secure AmBC. The omnidirectional array ensures consistent ambient energy harvesting irrespective of source orientation, thus enhancing operational reliability. Concurrently, the QYUA's optimized directive transmission targets intended receivers with precision, markedly limiting eavesdropping opportunities by restricting unintended signal propagation [8], [28]. Empirical and simulation validations confirm that this synergistic antenna arrangement substantially elevates both performance and security metrics compared to singular or non-optimized antenna configurations [6], [54].

5.2 Impact of Parameter Selection, Optimization Methods, and Adaptation for Wideband and 5G/6G Networks

The effectiveness of antenna systems in Ambient Backscatter Communication (AmBC) for IoT is significantly influenced by careful parameter selection, optimization strategies, and adaptability to emerging wideband and next-generation (5G/6G) networks. These aspects collectively determine system robustness, efficiency, and physical layer security. The following points encapsulate their critical impacts:

5.2.1 Impact of Parameter Selection

The selection and optimization of antenna design parameters play a pivotal role in determining overall performance. In particular, the geometric characteristics—such as the lengths, widths, and inter-element spacings of dipole components—have a direct impact on critical metrics including impedance matching, resonant frequency, gain, and side lobe suppression. Adjusting these parameters allows the antenna to operate more efficiently by aligning its resonant behavior with the desired operational bandwidth and minimizing undesirable radiation artifacts.

In addition to geometry, the physical properties of the substrate material significantly influence the antenna's radiation efficiency and bandwidth. For instance, the use of FR-4, with a relative dielectric constant ε_r of approximately 4.4, provides a practical balance between cost, manufacturability, and performance. The choice of substrate must be carefully matched with the application's frequency range and environmental conditions to avoid excessive dielectric losses or detuning effects.

Furthermore, precise tuning of structural dimensions to support broader operational bandwidths—typically ranging from 2 to 4 GHz or beyond—enhances the antenna's compatibility with various existing and emerging wireless communication standards. This bandwidth adaptability not only improves overall system robustness but also ensures seamless integration into diverse IoT and backscatter-enabled environments.

5.2.2 Impact of Optimization Methods: MOGA vs. MOPSO

The application of evolutionary algorithms significantly influences the quality and adaptability of antenna optimization outcomes. The Multi-Objective Genetic Algorithm (MOGA) is particularly effective in exploring a wide and diverse solution space, enabling the evaluation of various trade-offs among conflicting objectives such as gain, bandwidth, side lobe suppression, and secrecy capacity. This inherent diversity makes MOGA especially suitable for scenarios that demand flexible and robust antenna designs to meet stringent physical-layer security requirements.

In contrast, the Multi-Objective Particle Swarm Optimization (MOPSO) algorithm offers the advantage of rapid convergence and computational efficiency. MOPSO quickly generates high-quality solutions, making it highly practical for use cases where resource constraints or the need for swift deployment are paramount. Although MOPSO may exhibit lower solution diversity compared to MOGA, it remains effective for problems where optimality must be balanced against processing time.

From a comparative standpoint, MOGA tends to yield a broader set of Pareto-optimal solutions, which is advantageous in design environments that require nuanced optimization across multiple objectives. MOPSO, on the other hand, is more favorable in real-time or iterative design processes due to its accelerated convergence characteristics.

5.2.3 Adaptation for Wideband, 5G, and 6G Networks

The optimized antenna configurations developed in this study demonstrate strong compatibility with wideband communication requirements. Through broadband impedance matching and improved radiation performance, these designs ensure stable and efficient operation across extended frequency bands, including the 2–4 GHz range and beyond. This adaptability is particularly aligned with the demands of emerging wideband Internet of Things (IoT) applications, where multi-frequency and resilient performance are critical.

Furthermore, the integration of directional and omnidirectional antenna elements refined through advanced optimization techniques such as MOGA and MOPSO positions the system advantageously for deployment in future 5G and 6G networks. These networks, characterized by high-frequency operation, beamforming protocols, and dense device ecosystems, benefit directly from antenna structures that support enhanced directivity and reduced side-lobe radiation. Such characteristics not only improve signal fidelity but also significantly contribute to physical-layer security. In dense and security-sensitive environments such as smart cities or industrial IoT systems, the balance achieved between gain enhancement and side-lobe suppression ensures robust protection against eavesdropping and unauthorized access, meeting the stringent communication and privacy standards expected in next-generation wireless infrastructures.

5.2.4 Practical Implications and Recommendations

Future antenna design strategies should emphasize the development of flexible architectures by incorporating hybrid optimization methodologies, particularly those combining Multi-Objective Genetic Algorithm (MOGA) and Multi-Objective Particle Swarm Optimization (MOPSO). Such integration harnesses the advantages of both techniques—MOGA's exploration diversity and MOPSO's computational efficiency—resulting in more robust and adaptable solutions. To facilitate scalability for increasingly complex scenarios anticipated in 5G and 6G network environments, it is advisable to integrate surrogate modeling techniques into the optimization workflow. This integration can significantly reduce simulation time and computational load, thereby supporting rapid prototyping and deployment.

Moreover, maintaining a focus on multi-objective optimization, along with dynamic adaptation of antenna parameters, ensures the resulting designs can sustain robust and reliable performance even under variable operational and environmental conditions. This direction not only enhances system resilience but also aligns with the stringent performance and security requirements of future wireless infrastructures.

In conclusion, meticulous parameter selection combined with sophisticated optimization methods significantly enhances antenna system performance and adaptability. The presented methodologies, employing surrogate-based optimization, provide a practical and robust foundation for future-proof antenna designs suitable for evolving IoT and next-generation wireless communication networks.

5.2.5 Practical Limitations, and Challenges

The findings of this research provide several practical recommendations for the deployment of secure Internet of Things (IoT) systems utilizing dual-antenna Ambient Backscatter Communication (AmBC) tags. Integrating a microstrip patch antenna array for ambient RF signal reception with a quasi-Yagi-Uda antenna (QYUA) for directional transmission ensures both effective energy harvesting and spatially selective signal propagation. This combination plays a crucial role in enhancing physical-layer security, particularly in dense

or adversarial environments where omnidirectional communication may expose sensitive transmissions to unintended recipients. To further maximize system performance, it is highly recommended to employ evolutionary optimization algorithms such as the Multi-Objective Genetic Algorithm (MOGA) and Multi-Objective Particle Swarm Optimization (MOPSO), as they offer balanced trade-offs among key design parameters including gain, bandwidth, impedance matching, and side-lobe suppression under real-world constraints.

However, certain challenges and limitations remain inherent to this approach. Accurate electromagnetic modeling and optimization necessitate considerable computational effort and numerous iterative simulations, which may limit accessibility for resource-constrained research environments. The dual-antenna configuration, although effective, introduces added complexity in terms of structural integration, which can pose difficulties in fabrication and precise alignment—especially for compact or batteryless IoT tag implementations. Moreover, external environmental factors such as multipath fading, interference from coexisting wireless systems, and inconsistent availability of ambient RF sources may adversely affect both system performance and the reliability of secure communication. Implementing advanced optimization techniques also requires access to accurate empirical data and high-fidelity simulation tools, which may not always be readily available.

Despite these challenges, the proposed framework—featuring a synergistic dual-antenna configuration and multi-objective optimization—presents a scalable and effective strategy for enhancing the security and energy efficiency of IoT communications. When adapted to specific application needs and environmental conditions, this methodology has strong potential to support the development of robust, secure, and sustainable wireless systems for next-generation networks.

5.2.6 Implications for Future Research

Building upon the current research, several promising directions can be explored to further enhance secure IoT communication through Ambient Backscatter Communication (AmBC) and dual-antenna architectures. A key avenue involves the development of adaptive or reconfigurable antenna arrays that are capable of dynamic beam steering and real-time

adaptation to evolving ambient RF environments or threat landscapes. Such reconfigurability could significantly bolster both the flexibility and security of AmBC-based systems. Additionally, incorporating more advanced machine learning methodologies—such as deep learning-driven surrogate modeling or real-time online optimization techniques—could expedite the design process and yield more effective outcomes, particularly in environments characterized by non-stationarity or limited training data.

Further research should also address the design of wideband and multiband antennas that are compatible with emerging wireless standards, such as 5G and 6G, and that support interoperability with a diverse range of IoT devices. Such developments would enhance the scalability and resilience of the proposed system. Moreover, validation through experimental deployment in real-world environments—such as urban or industrial testbeds—remains crucial to understanding system performance under practical conditions. These evaluations should include assessments of robustness against multipath fading, interference from co-located wireless systems, and variability in ambient RF availability.

Finally, there exists considerable opportunity to investigate the combined influence of physical-layer antenna optimization and upper-layer security protocols. By examining cross-layer strategies that integrate optimized hardware with secure communication frameworks, future research may establish more comprehensive and scalable solutions for securing IoT networks. Addressing these challenges would help close the gap between theoretical contributions and practical implementation, paving the way for robust, efficient, and secure IoT infrastructures.

6 Conclusion and Future Work

6.1 Summary of Work

This thesis develops a dual-antenna system—comprising a microstrip patch array and a quasi-Yagi-Uda antenna (QYUA) to improve physical layer security in Ambient Backscatter Communication (AmBC) for IoT applications. The patch array enables efficient omnidirectional ambient RF signal reception and energy harvesting, while the QYUA provides high directivity and side lobe suppression for secure, directional transmission. To optimize antenna performance across multiple criteria—gain, bandwidth, impedance matching, and side-lobe control—multi-objective optimization techniques, specifically MOGA and MOPSO, were employed. Simulation results from CST Studio Suite validate that the optimized designs outperform conventional counterparts in both communication reliability and secrecy enhancement.

Overall, this research demonstrates that combining directional and omnidirectional antenna designs with evolutionary optimization offers a robust and scalable solution for secure and energy-efficient IoT deployments in dynamic wireless environments.

6.2 Concluding Remarks and Directions for Further Research

This thesis has demonstrated the feasibility and advantages of implementing a dual-antenna Ambient Backscatter Communication (AmBC) system, comprising a microstrip patch ar-

ray and a quasi-Yagi-Uda antenna (QYUA). Through the use of evolutionary optimization algorithms, specifically MOGA and MOPSO, the antenna configuration was systematically enhanced to address key performance goals such as secure communication, efficient energy harvesting, and multi-objective design constraints. By targeting physical layer security and minimizing side-lobe leakage while maintaining high gain and bandwidth, the proposed system presents a substantial improvement over conventional designs in the context of low-power IoT communication networks.

Looking ahead, future research should explore adaptive and reconfigurable antenna systems capable of dynamic beamforming and environmental responsiveness. The integration of advanced machine learning methods, including deep learning-based surrogate modeling and reinforcement learning, holds potential for accelerating optimization processes and enhancing adaptability to fluctuating RF environments. Moreover, real-world validation in urban or industrial IoT scenarios is essential for evaluating performance under multipath fading, interference, and ambient signal variability. Additional exploration into cross-layer security frameworks, which couple optimized antenna design with higher-layer protocol innovations, could offer a holistic solution for scalable and resilient communication infrastructures. These future directions are expected to further strengthen the security, flexibility, and performance of next-generation IoT and AmBC systems.

References

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities", *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, Feb. 2014. DOI: 10.1109/JIOT.2014.2306328.

[2] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5g networks for the internet of things: Communication technologies and challenges", *IEEE Access*, vol. 6, pp. 3619–3647, 2018. DOI: 10.1109/ACCESS.2017.2779844.

[3] W. Ejaz, A. Anpalagan, M. A. Imran, M. Jo, M. Naeem, S. B. Qaisar, and W. Wang, "Internet of things (iot) in 5g wireless communications", *IEEE Access*, vol. 4, pp. 10 310–10 314, 2016. DOI: 10.1109/ACCESS.2016.2646120.

[4] M. R. Palattella et al., "Internet of things in the 5g era: Enablers, architecture, and business models", *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527, Mar. 2016. DOI: 10.1109/JSAC.2016.2525418.

[5] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air", *SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 39–50, 2013. DOI: 10.1145/2486001.2486015.

[6] T. Hong, C. Liu, and M. Kadoch, "Machine learning based antenna design for physical layer security in ambient backscatter communications", *Wireless*

Communications and Mobile Computing, vol. 2019, Article ID 4870656, 2019. DOI: 10.1155/2019/4870656.

[7] N. V. Huynh, P. Wang, D. T. Hoang, X. Lu, D. Niyato, and D. I. Kim, "Ambient backscatter communications: A contemporary survey", *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2889–2922, 2018. DOI: 10.1109/COMST.2018.2841964.

[8] T. Tang, T. Hong, C. Liu, W. Zhao, and M. Kadoch, "Design of 5g dual-antenna passive repeater based on machine learning", in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, Tangier, Morocco: IEEE, 2019, pp. 1907–1912. DOI: 10.1109/IWCMC.2019.8766614.

[9] Y. Liu, L. Wang, M. Elkashlan, T. Q. Duong, A. Nallanathan, and B. Ren, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges", *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2017. DOI: 10.1109/COMST.2016.2598968.

[10] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey", *IEEE Wireless Communications*, vol. 16, no. 3, pp. 25–36, Jun. 2008. DOI: 10.1109/COMST.2014.012314.00178.

[11] N. Zhang, D. Chen, F. Ye, T.-X. Zheng, and Z. Wei, "Physical layer security for internet of things", *Wireless Communications and Mobile Computing*, vol. 2019, pp. 1–2, 2019. DOI: 10.1155/2019/2627938.

[12] S. Zhang, Q. Wu, S. Xu, and G. Y. Li, "Fundamental green tradeoffs: Progresses, challenges, and impacts on 5g networks", *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 33–56, 2017. DOI: 10.1109/COMST.2016.2594120.

[13] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise", *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008. DOI: 10.1109/TWC.2008.060848.

[14] R. F. Schaefer, G. Amarasuriya, and H. V. Poor, "Physical layer security in massive mimo systems", in *2017 51st Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, USA, 2017, pp. 3–8. DOI: 10.1109/ACSSC.2017.8335124.

[15] R. Carvalho, R. R. Saldanha, B. N. Gomes, A. C. Lisboa, and A. X. Martins, "A multi-objective evolutionary algorithm based on decomposition for optimal design of yagi–uda antennas", *IEEE Transactions on Magnetics*, vol. 48, no. 2, pp. 803–806, Feb. 2012. DOI: 10.1109/TMAG.2011.2174348.

[16] N. Sarker, P. Podder, M. R. H. Mondal, S. S. Shafin, and J. Kamruzzaman, "Applications of machine learning and deep learning in antenna design, optimization, and selection: A review", *IEEE Access*, vol. 11, pp. 103 890–103 915, 2023. DOI: 10.1109/ACCESS.2023.3317371.

[17] Z. Li, Y. Han, and Y. Yang, "Multiobjective particle swarm optimization: A survey of the state-of-the-art", *Preprints*, 2025. DOI: 10.20944/preprints202502.2011.v1.

[18] A. Zappone, M. Di Renzo, and M. Debbah, "Wireless networks design in the era of deep learning: Model-based, ai-based, or both?", *IEEE Transactions on Communications*, vol. 67, no. 10, pp. 7331–7376, Oct. 2019. DOI: 10.1109/TCOMM.2019.2924010.

[19] D. T. Hoang, D. Niyato, P. Wang, D. I. Kim, and Z. Han, "Ambient backscatter: A new approach to improve network performance for rf-powered cognitive radio networks", *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 3659–3674, 2017. DOI: 10.1109/TCOMM.2017.2710338.

[20] X. Lu, D. Niyato, H. Jiang, D. I. Kim, Y. Xiao, and Z. Han, "Ambient backscatter assisted wireless powered communications", *IEEE Wireless Communications Magazine*, vol. 25, no. 2, pp. 170–177, 2018. DOI: 10.1109/MWC.2017.1600398.

[21] C. Perez-Penichet, "Ph.d. forum abstract: Ambient backscatter communication", in *Proceedings of the 15th ACM/IEEE International Conference on Information Processing in Sensor Networks, IPSN 2016*, Austria: IEEE/ACM, Apr. 2016. DOI: 10.1109/IPSN.2016.7460685.

[22] S. Han, S. Xu, W. Meng, and C. Li, "Dense-device-enabled cooperative networks for efficient and secure transmission", *IEEE Network*, vol. 32, no. 2, pp. 100–106, 2018. DOI: 10.1109/MNET.2018.1700292.

[23] W. Zhang, W. He, X. Chen, Y. Cai, X. Guan, and J. Qu, "Power allocation for improving physical layer security in d2d communication via stackelberg game", in *Proceedings of the 8th International Conference on Wireless Communications and Signal Processing, WCSP 2016*, Yangzhou, China: IEEE, Oct. 2016, pp. 1–5. DOI: 10.1109/WCSP.2016.7752663.

[24] T. Q. Duong, "Keynote talk #1: Trusted communications with physical layer security for 5g and beyond", in *Proceedings of the International Conference on Advanced Technologies for Communications (ATC)*, Quy Nhon, Vietnam: IEEE, 2017, p.xxxiv. DOI: 10.1109/ATC.2017.8167581.

[25] Z. Chen, H. Li, G. Cui, and M. Rangaswamy, "Adaptive transmit and receive beamforming for interference mitigation", *IEEE Signal Processing Letters*, vol. 21, no. 2, pp. 235–239, 2014. DOI: 10.1109/LSP.2014.2298497.

[26] P. Zhang, Y. Ma, and B. Wang, "Improving physical layer security via multiple-level relay network", in *Proceedings of the 2014 12th IEEE International Con-*

ference on Signal Processing, ICSP 2014, Hangzhou, China: IEEE, Oct. 2014, pp. 1851–1854. DOI: 10.1109/ICOSP.2014.7015312.

[27] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints", *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015. DOI: 10.1109/JPROC.2015.2466548.

[28] Q. Chen, S.-W. Qu, J. Li, L. Wang, Q. Yuan, and K. Sawaya, "Dual-antenna system composed of patch array and planar yagi-uda array", in *Proceedings of the 5th European Conference on Antennas and Propagation (EUCAP 2011)*, Rome, Italy: IEEE, Apr. 2011, pp. 1023–1026. DOI: 10.2528/PIERC11021702.

[29] C. Peixeiro, "Microstrip patch antennas: An historical perspective of the development", in *2011 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC 2011)*, Natal, Brazil, 2011, pp. 684–688. DOI: 10.1109/IMOC.2011.6169224.

[30] M. Z. B. Chowdhury, M. Islam, H. Rmili, I. Hossain, M. Mahmud, and M. Samsuzzaman, "A low-profile rectangular slot antenna for sub-6 ghz 5g wireless applications", *International Journal of Communication Systems*, vol. 35, no. 17, e5321, Aug. 2022. DOI: 10.1002/dac.5321.

[31] A. Abdulhameed and Z. Kubík, "Review of printed log-periodic dipole array antenna design for emc applications", *Inventions*, vol. 10, p. 34, Apr. 2025. DOI: 10.3390/inventions10030034.

[32] E. E. Altshuler and D. S. Linden, "Wire-antenna designs using genetic algorithms", *IEEE Antennas and Propagation Magazine*, vol. 39, no. 2, pp. 33–43, 1997. DOI: 10.1109/74.584498.

[33] S. Santarelli, T.-L. Yu, D. E. Goldberg, et al., "Military antenna design using simple and competent genetic algorithms", *Mathematical and Computer Mod-*

elling, vol. 43, no. 9–10, pp. 990–1022, 2006. DOI: 10.1016/j.mcm.2005.05.024.

[34] H. Zou, S. Zeng, C. Li, and J. Ji, "A survey of machine learning and evolutionary computation for antenna modeling and optimization: Methods and challenges", *Engineering Applications of Artificial Intelligence*, vol. 138, p. 109 381, 2024. DOI: 10.1016/j.engappai.2024.109381.

[35] W. Zhao, G. Wang, R. Fan, L. Fan, and S. Atapattu, "Ambient backscatter communication systems: Capacity and outage performance analysis", *IEEE Access*, vol. 6, pp. 22 695–22 704, 2018. DOI: 10.1109/ACCESS.2018.2828021.

[36] Y. Liu, G. Wang, Z. Dou, and Z. Zhong, "Coding and detection schemes for ambient backscatter communication systems", *IEEE Access*, vol. 5, pp. 4947–4953, 2017. DOI: 10.1109/ACCESS.2017.2679135.

[37] F. Zhu and M. Yao, "Improving physical-layer security for crns using sinr-based cooperative beamforming", *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1835–1841, 2016. DOI: 10.1109/TVT.2015.2412152.

[38] J. Zhao, X. Chao, P. Wang, and T. Hong, "Efficient directional antenna design suitable for power internet of things scenarios", *International Journal of Computer Software Engineering*, vol. 6, p. 163, 2021. DOI: 10.15344/2456-4451/2021/163.

[39] R. Alhalabi and G. M. Rebeiz, "High-gain yagi-uda antennas for millimeter-wave switched-beam systems", *IEEE Transactions on Antennas and Propagation*, vol. 57, no. 11, pp. 3672–3676, 2009. DOI: 10.1109/TAP.2009.2026666.

[40] N. Guo-qi, Z. Tao, N. Wei, and L. S. Wang, "Amelioration of quasi-yagi antenna", *Journal of Microwaves (China)*, vol. 29, no. 1, pp. 51–54, 2013.

[41] K. R. Carver and J. W. Mink, "Microstrip antenna technology", *IEEE Transactions on Antennas and Propagation*, vol. 29, no. 1, pp. 2–24, 1981. DOI: 10.1109/TAP.1981.1142523.

[42] C. A. Balanis, *Antenna Theory: Analysis and Design*, 4th. Hoboken, NJ, USA: Wiley, 2018.

[43] P. Mahouti, M. A. Belen, N. Çalik, and S. Koziel, "Computationally efficient surrogate-assisted design of pyramidal-shaped 3-d reflectarray antennas", *IEEE Transactions on Antennas and Propagation*, vol. 70, no. 11, pp. 10 777–10 786, Nov. 2022. DOI: 10.1109/TAP.2022.3191131.

[44] S. Koziel, N. Çalik, P. Mahouti, and M. A. Belen, "Low-cost and highly accurate behavioral modeling of antenna structures by means of knowledge-based domain-constrained deep learning surrogates", *IEEE Transactions on Antennas and Propagation*, vol. 71, no. 1, pp. 105–118, Jan. 2023. DOI: 10.1109/TAP.2022.3216064.

[45] A. Pietrenko-Dabrowska and S. Koziel, "Reliable surrogate modeling of antenna input characteristics by means of domain confinement and principal components", *Electronics*, vol. 9, no. 5, p. 877, May 2020. DOI: 10.3390/electronics9050877.

[46] Y. Zhong, P. Renner, W. Dou, G. Ye, J. Zhu, and Q. H. Liu, "A machine learning generative method for automating antenna design and optimization", *IEEE Journal on Multiscale and Multiphysics Computational Techniques*, vol. 7, pp. 285–295, 2022. DOI: 10.1109/JMMCT.2022.3211178.

[47] K. Fu, X. Cai, B. Yuan, Y. Yang, and X. Yao, "An efficient surrogate assisted particle swarm optimization for antenna synthesis", *IEEE Transactions on Antennas and Propagation*, vol. 70, no. 7, pp. 4977–4984, Jul. 2022. DOI: 10.1109/TAP.2022.3153080.

[48] G. Qi, S. Bao, Y. Wei, and Y. Zhang, "Accurate antenna design by deep auto-encoder surrogate model assisted particle swarm optimization", in *Proc. IEEE 5th Int. Conf. Electron. Inf. Commun. Technol. (ICEICT)*, Aug. 2022, pp. 875–880. DOI: 10.1109/ICEICT55736.2022.9909412.

[49] Y. Bai, P. Gardner, Y. He, and H. Sun, "A surrogate modeling approach for frequency-reconfigurable antennas", *IEEE Transactions on Antennas and Propagation*, vol. 71, no. 6, pp. 5498–5503, Jun. 2023. DOI: 10.1109/TAP.2023.3248446.

[50] S. Koziel, M. A. Belen, A. Çalişkan, and P. Mahouti, "Rapid design of 3d reflectarray antennas by inverse surrogate modeling and regularization", *IEEE Access*, vol. 11, pp. 24 175–24 184, 2023. DOI: 10.1109/ACCESS.2023.3254204.

[51] Y. Jiao, Q. Zhu, R. Ni, and Q. S. Cheng, "A multisurrogate-assisted optimization framework for sspp-based mmwave array antenna", *IEEE Transactions on Antennas and Propagation*, vol. 71, no. 4, pp. 2938–2945, Apr. 2023. DOI: 10.1109/TAP.2023.3240239.

[52] S. Koziel and A. Pietrenko-Dabrowska, "Tolerance optimization of antenna structures by means of response feature surrogates", *IEEE Transactions on Antennas and Propagation*, vol. 70, no. 11, pp. 10 988–10 997, Nov. 2022. DOI: 10.1109/TAP.2022.3187665.

[53] Z. Wei, Z. Zhou, P. Wang, J. Ren, Y. Yin, G. F. Pedersen, and M. Shen, "Fully automated design method based on reinforcement learning and surrogate modeling for antenna array decoupling", *IEEE Transactions on Antennas and Propagation*, vol. 71, no. 1, pp. 660–671, Jan. 2023. DOI: 10.1109/TAP.2022.3221613.

[54] J. Zhao, C. Xu, H. Tao, P. Wang, and S. Zheng, "Efficient directional antenna design suitable for ubiquitous power internet of things", *Electronics*, vol. 10, no. 13, p. 1521, 2021. DOI: 10.3390/electronics10131521.