RADemics

Machine Learning for Intrusion Detection and Secure Communication in Antenna Networks

R. Sundar, G. Rohini, Sridhar
AMET DEEMED TO BE UNIVERSITY, ST. JOSEPH'S INSTITUTE OF TECHNOLOGY, S-VYASA DEEMED TO BE UNIVERSITY

Machine Learning for Intrusion Detection and Secure Communication in Antenna Networks

[1]R. Sundar, Associate Professor, Department of Marine Engineering, AMET Deemed to be University, 135, ECR Road, Kanathur, Chennai – 603112. sundar.r@ametuniv.ac.in

[2]G. Rohini, Professor, Department of Electronics and Communication Engineering, St. Joseph's Institute of Technology, OMR, Chennai- 600119. rohini.manoharan@gmail.com

[3]Sridhar, Professor and Director Academics, Department of Computer Science, S-VYASA Deemed to be University, Bengaluru - 560059. drsridhar@svyasa.edu.in

Abstract

The rapid advancement of antenna-based wireless communication systems, including MIMO, IoT, and emerging 5G/6G networks, has intensified the need for intelligent and resilient security mechanisms capable of addressing sophisticated and dynamic cyber threats. Conventional intrusion detection and cryptographic techniques face limitations in adapting to evolving attack patterns, high-dimensional data, and resource-constrained environments. This chapter presents a comprehensive exploration of machine learning and deep learning approaches for intrusion detection and secure communication in antenna networks, emphasizing their ability to analyze complex network traffic and radio frequency signal characteristics for accurate and real-time threat detection. The study examines supervised, unsupervised, and hybrid learning models, along with advanced techniques such as transfer learning and reinforcement learning, to enhance detection performance and system adaptability. In parallel, the integration of physical layer security mechanisms, including beamforming and channel-based authentication, with intelligent learning frameworks enables robust protection against eavesdropping, jamming, and spoofing attacks. Critical challenges such as dataset limitations, computational complexity, adversarial threats, and model interpretability are analyzed, highlighting the need for efficient, scalable, and explainable solutions. The chapter further outlines emerging research directions, including federated learning, edge intelligence, and next-generation secure communication frameworks, providing a unified perspective for developing adaptive and resilient antenna network security systems suitable for real-world deployment.

Keywords: Machine Learning, Intrusion Detection, Antenna Networks, Secure Communication, Deep Learning, Physical Layer Security.

Introduction

Rapid growth of antenna-based wireless communication systems has reshaped modern connectivity, enabling high-speed data transmission, massive device integration, and seamless global communication [1]. Technologies such as multiple-input multiple-output architectures, Internet of Things ecosystems, and emerging fifth and sixth generation networks rely heavily on intelligent antenna configurations to enhance spectral efficiency and signal reliability [2]. Smart antennas equipped with adaptive beamforming and spatial diversity techniques support dynamic

communication environments where users, devices, and network conditions continuously change [3]. Such capabilities play a crucial role in addressing increasing demands for bandwidth, low latency, and reliable connectivity across applications including healthcare, transportation, industrial automation, and smart cities. Expansion of these systems has introduced complex operational environments where communication channels remain open and highly distributed, creating multiple vulnerabilities within the network structure [4]. Exposure to external interference and unauthorized access highlights the importance of integrating advanced security mechanisms directly into antenna-based communication frameworks. Strong and adaptive protection strategies remain essential to ensure uninterrupted operation and safeguard sensitive information within these rapidly evolving wireless ecosystems [5].

Security challenges in antenna networks have intensified due to the inherent characteristics of wireless communication, where signals propagate through shared and often unpredictable environments [6]. Transmission over open air allows adversaries to intercept, manipulate, or disrupt communication without requiring physical access to network infrastructure [7]. Threats such as eavesdropping, jamming, spoofing, and denial-of-service attacks target different layers of the communication process, affecting both data confidentiality and network availability. Dynamic channel conditions, mobility of users, and heterogeneous device connectivity further complicate the detection of malicious activities [8]. Traditional security techniques based on fixed rules and predefined signatures struggle to adapt to such variability, leading to reduced effectiveness against emerging and sophisticated attack strategies. Increasing scale of connected devices amplifies the attack surface, making manual monitoring and static defense mechanisms insufficient [9]. Continuous evolution of attack methodologies demands intelligent systems capable of understanding complex patterns and responding in real time. Integration of adaptive security solutions becomes a fundamental requirement to address these challenges within antenna-driven wireless communication environments [10].

Machine learning has emerged as a powerful approach to address the limitations of conventional security mechanisms in antenna networks [11]. Data-driven models analyze large volumes of network traffic and radio frequency signals to identify patterns associated with normal and malicious behavior. Supervised learning techniques enable accurate classification of known attack types by leveraging labeled datasets, while unsupervised methods facilitate detection of anomalies without prior knowledge of specific threats [12]. Deep learning models enhance this capability by extracting hierarchical and temporal features from complex communication data, allowing improved identification of subtle and multi-stage attacks [13]. Such techniques support real-time intrusion detection and enable automated response mechanisms that reduce reliance on manual intervention [14]. Adaptation to changing network conditions and evolving threat landscapes enhances the effectiveness of machine learning-based systems in maintaining secure communication. Continuous learning and model refinement contribute to improved resilience and accuracy, making machine learning an integral component of modern intrusion detection frameworks within antenna networks [15].