Deep Learning for Physical-Layer Security in Wireless Internet of Things (WIOT): A Survey, Experimental Analysis, and Outlooks

Abstract—

Keywords: Artificial Intelligence (AI), Cybersecurity, Deep Learning, Physical-Layer Security, Wireless Internet of Things (WIOT), Wireless Communication Security, Wireless Networks, Experimental Analysis, Authentication, Privacy Preservation.

1. Introduction

1.1. Background

The integration of the Internet of Things (IoT) into modern infrastructure, especially in intelligent cities and industrial applications, is revolutionizing connectivity, allowing billions of devices to communicate perfectly. Wireless IoT (WIoT) represents a dynamic ecosystem of low-power interconnected devices, wireless sensors, and actuators that make it easier to exchange real-time data from diverse services, ranging from medical assistance and transportation to power management [1]. With estimates suggesting that by 2025 there will be over 25 billion IoT devices worldwide, IoT deployment scale is rapidly increasing, resulting in a complex and diversified set of connectivity solutions [2].

However, this massive growth of linked devices introduces massive protection demanding situations. The wireless medium, through its very nature, is surprisingly susceptible to quite a few attacks. Generalized connectivity facilitates unsuccessful actors to intercept data, counterfeit devices, or jam communication channels, leading to serious vulnerabilities. These attacks may compromise confidential data such as health records, traffic control systems, or even critical infrastructure such as energy grids [3] To address these vulnerabilities, the traditional cryptographic methods of the upper layer have been widely used in IoT safety. However, these techniques often require significant computational resources and are not always suitable for IoT devices with resource restrictions. In addition, they may not meet the strict requirements of 5G and 6G emerging networks, particularly in terms of latency, scalability, and real-time safety needs [4]. This limitation encouraged interest in alternative approaches, such as the safety of the physical layer (PLS), which takes advantage of the properties inherent to the wireless channel such as Channel State Information (CSI) and Radio Frequency (RF) fingerprints, to enhance security at the physical layer [5].

PLS offers a light, robust, and adaptive security solution that is particularly suitable for the IoT environment. By using unique physical functions in the communication channel, PLS attacks such as interception and spoofing without computational overhead for traditional cryptographic techniques reduce. However, static PLS solutions have limitations in handling dynamic IoT environments with rapidly changing network ratios and different threats. This is where Deep Learning (DL) appears as a powerful tool. DL algorithms, especially Convolutional Neural Networks (CNNs) and reinforcement learning (RL), can effectively adapt to the dynamic nature of wireless environments and improve PLS robustness [6]. DL techniques can analyze complex patterns in the data on physical layers, which allows for real-time detection and the mitigation of safety threats such as jamming and unauthorized unit access [7]. Furthermore, deep learning models can continuously learn and adapt to developing attack strategies and improve the general security of WIoT networks [8].

This diagram shows how physical-layer security (PLS) protects communication in wireless IoT (WIoT) systems. It shows IoT devices that communicate wirelessly, with potential attacks such as eavesdropping and jamming aimed at the communication channel. PLS mechanisms such as Channel State Information (CSI), RF fingerprints, artificial noise, and beamforming protect communication. Secure data transfer is secured after these safety methods are used, with data sent to a central network for processing.

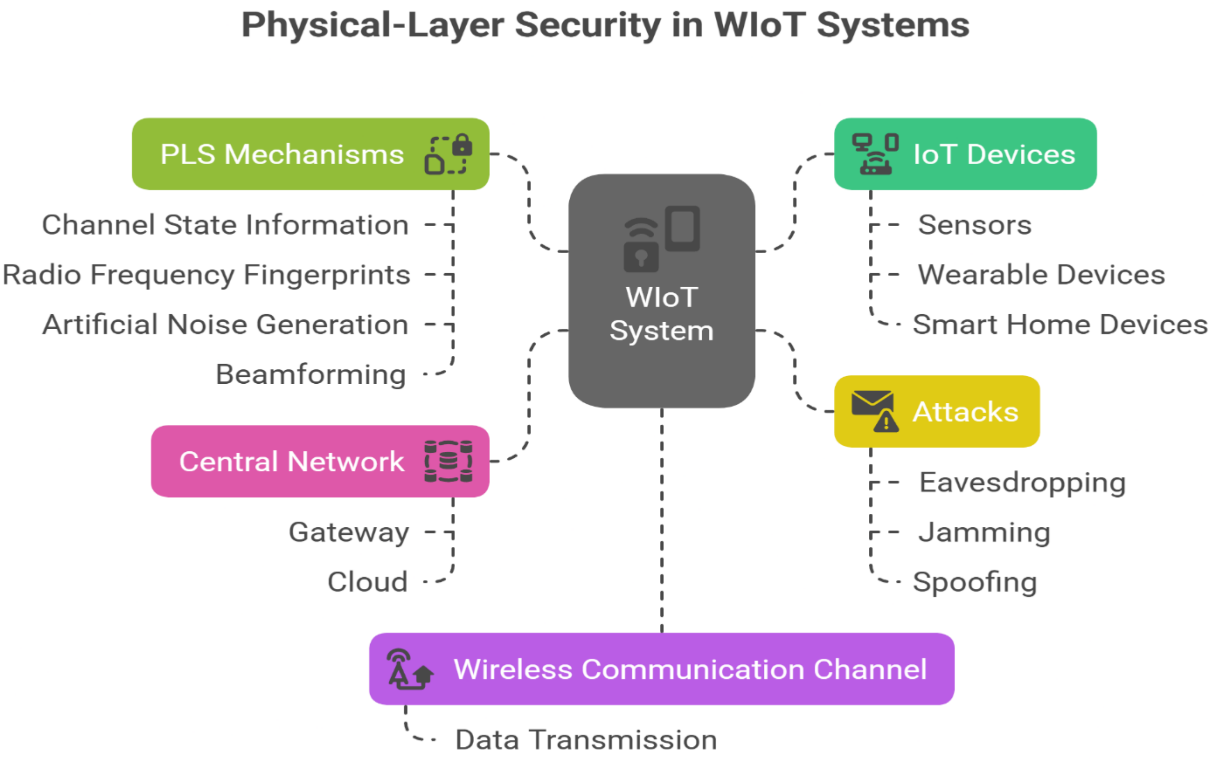


Figure 1. Conceptual Diagram of Physical-Layer Security in Wireless IoT

1.2 Limitations of Upper-Layer Cryptographic Security for WIoT and Deep Learning Solutions

Wireless network approval protocols for Wireless Internet of Things (Wiot) applications, especially in shared rooms, traditionally depend on cryptographic methods for upper layers such as public key encryption frameworks (e.g., RSA and ECC) and symmetrical key dimensions (e.g., Although these methods have been effective in previous generations. -network due to the following reasons:

1. **Cryptographic Security Vulnerabilities:** Cryptographic safety for upper layers depends on the calculation intractability of mathematical problems (e.g., integer factorization, discrete logarithms), but quantum data -burning progress threatens to break these encryption methods. For example, Shor's algorithm can compromise RSA keys, which lead to WIoTs in WIoT devices used in critical infrastructure, such as smart networks. This problem makes traditional cryptographic security that is poorly suited for IoT devices in environments that require long-term security and reliability [9].
2. **Replay Attacks:** Upper layer protocols are vulnerable to playing about attacks, where attackers catch and play again valid signals to circumvent authentication mechanisms without the need to decrypt data. For IoT applications that are sensitive to latency, such as real-time health monitoring in smart health care, unauthorized access or service interruptions can severely compromise patient care and the quality of the service provided. The broadcast type of wireless communication aggravates this risk in Wiot environments, where sensitive data is transmitted over public networks [10].
3. **Key Management Challenges:** Cryptographic methods require key generation, distribution, and renewal, all of which introduce substantial latency and overhead. This is problematic in WIoT applications, such as autonomous drones or smart traffic lights, where even small delays can interfere with functionality. In real-time applications, key exchanges often require multiple communication rounds, further exacerbating the latency problem, especially in resource-constrained IoT devices [11].
4. **Computational Overhead for IoT Devices:** Cryptographic algorithms impose computational overhead on IoT devices, particularly low-power sensors, and wearables. In WIoT networks, where scalability and the integration of numerous heterogeneous devices are essential, cryptographic methods often fail to efficiently manage the diversity of devices and communication protocols. Variations in encryption standards lead to interoperability issues and increase communication overhead, making cryptography unsuitable for large-scale IoT deployments [12].

1.3 Deep learning -enhanced physical layer security

WIoT Physical Layer Security (PLS) is a promising alternative to traditional cryptographic methods and utilizes unique physical layer properties such as Channel State Information (CSI), Radio Frequency (RF) Fingerprint and Signal Preparation Properties to authenticate devices and secure Wiot-Network communication [13]. PLS provides significant benefits that are particularly suitable for Wiot applications:

1. **Uniqueness of Physical Layer Features:** The physical-layer features of wireless signals, such as multipath fading and hardware imperfections, are unique to each unit and the environment, making them difficult to recreate with opponents. This resistance to duplication improves safety by preventing **impersonation** and **spoofing** attacks, which can compromise critical Wiot infrastructure such as smart city systems or connected vehicles [14].
2. **Low Computational Overhead:** PLS works with low computational complexity, which is essential for WIoT devices with limited processor power, such as battery-powered sensors and wearables. By utilizing existing CSI achieved during channel estimation, PLS offers effective authentication for IoT networks without excessive computational requirements, making it ideal for resource-limited devices in large IoT systems [15].
3. **Compatibility with heterogeneous WIoT networks:** PLS is very compatible with the heterogeneous nature of Wiot networks, involving several unit types and communication protocols. Unlike traditional cryptographic methods, decoder PL's physical layer security is based on unique channel properties, regardless of protocol -specific encryption. This improves interoperability in complex IoT environments, facilitating seamless integration of different devices into smart cities and industrial applications [16].
4. **Adaptation to dynamic IoT environments:** Traditional PLS methods depend on static thresholds for anomaly detection, which are ineffective in dynamic IoT environments. However, deep learning improves (DL) PLS by offering adaptive, intelligent safety mechanisms that can adapt to quickly changed communication channels:
    1. **Deep Learning for complex channel conditions:** Convolutional Neural Networks (CNN) and other deep learning algorithms can analyze high-dimensional channel data to capture real-time variations in WIoT environments, such as smart cities where many devices transfer signals. This provides the opportunity for real-time safety and exceeds traditional models that struggle to accommodate the dynamic nature of Wiot networks [17].
    2. **Reinforcement Learning for adaptive authentication:** Reinforcement Learning (RL) allows for adaptive authentication in mobile IoT applications, such as connected cars or drones, and adjusts real-time authentication thresholds to account for changes in the wireless environment [18].
    3. **Scalable feature extraction with Deep Learning:** Deep learning models enable scalable feature extraction of RF fingerprints from many IoT devices without requiring extensive prior knowledge or manual intervention. This is especially important as the number of connected devices in Wiot systems grows exponentially [19].
    4. **Resilience against conflicting attacks:** Deep learning -driven anomaly detection improves PLS resistance to opponent's attack, including signal spoofing and

jamming. By utilizing deep neural networks (DNN) and conflicting training, deep learning models can detect subtle anomalies in wireless signals and distinguish between legitimate transfers and malicious interference. In addition, generative adversarial networks (GAN) and Autoencoders can learn robust feature representations of normal wireless communication patterns, so that they can identify and cushion sophisticated attacks in real time. This adaptability makes Wiot systems more secure against threats and ensures the integrity of critical public services such as emergency response networks and smart grids, where security breaches can have profound consequences [20].

Deep learning-enhanced PLS provides adaptive, scalable, and efficient solutions that address the limitations of traditional upper-layer cryptographic security methods. By leveraging the unique features of the physical layer and combining them with advanced deep learning techniques, PLS can offer robust, real-time security for the evolving WIoT landscape.

1.4 Related Surveys

This section reviews recent studies on physical-layer security (PLS) and authentication (PLA) in wireless networks, focusing on 10 key references from 2019 to 2023. These works explore various security aspects, such as eavesdropping, jamming, and spoofing, with some addressing IoT applications and deep learning (DL) techniques. We analyze each study based on criteria like IoT consideration, DL coverage, attack types, experimental evaluation, and future directions. The following table and discussion highlight their contributions, limitations, and gaps, setting the stage for our survey's focus on DL-enhanced PLS for Wireless Internet of Things (WIoT) security.

Table1. Comparative Analysis of Selected Studies on Physical-Layer Security (2019–2023)

Ref.	Year	Focus Area	IoT	DL Coverage	Learning Models	Attack Types	Defense	Adv. ML	Exp. Eval.	Datasets	Challenges	Future Dir.
[21]	2023	PLS Mechanisms	No	No	None	Eavesdropping, Jamming	Yes	No	No	No	Yes	Yes
[22]	2022	Secure Industrial Comms	Yes	No	None	Spoofing	Yes	No	No	No	Yes	Yes
[23]	2022	RF Fingerprinting	Partial	Yes	DL (discriminative)	Spoofing	Yes	No	No	No	Yes	Yes
[24]	2021	NFC Security	No	Yes	DL (discriminative)	Spoofing	Yes	No	Yes	Yes	Yes	No
[25]	2021	IoT Device Detection	Yes	Yes	ML (unspecified)	Spoofing	Yes	No	No	No	Yes	Yes
[26]	2020	RF Fingerprinting	Yes	Yes	DL (discriminative)	Spoofing	Yes	No	Yes	Yes	Yes	No
[27]	2020	PLA for IoT	Yes	Partial	None	Spoofing, Eavesdropping	Yes	No	No	No	Yes	Yes
[28]	2020	PLA Fundamentals	Partial	No	None	Spoofing, Eavesdropping	Yes	No	No	No	Yes	Yes
[29]	2019	RFID Security	Yes	Yes	DL (discriminative)	Spoofing	Yes	No	Yes	Yes	Yes	Yes
[30]	2019	ML-based PLA	Partial	Yes	Supervised, DL	Spoofing, Eavesdropping	Yes	No	No	No	Yes	Yes

Analytical Discussion of Each Survey Study

- [21] (2023) - **PLS Mechanisms Analysis:** The most recent study (2023) overviews PLS mechanisms, focusing on eavesdropping and jamming defenses in wireless communications. It lacks IoT and DL coverage, relying on theoretical analysis without experimental validation or datasets. It highlights challenges (e.g., scalability) and future directions (e.g., emerging applications), but its non-ML focus limits its relevance to modern WIoT trends.
- [22] (2022) - **Secure Industrial Comms Analysis:** Published in 2022, this survey examines PLS techniques for industrial communications, targeting spoofing in IoT contexts. It omits DL, using a theoretical approach without experiments or datasets. It discusses industry-specific challenges and future directions, though its industrial focus reduces applicability to broader WIoT scenarios.
- [23] (2022) - **RF Fingerprinting Analysis:** This 2022 survey comprehensively reviews RF fingerprinting, comparing traditional and DL approaches (discriminative models) for spoofing, with partial IoT focus. It lacks experimental results or datasets but addresses challenges (e.g., scalability, noise) and future directions. Its theoretical nature limits practical insights.
- [24] (2021) - **NFC Security Analysis:** Released in 2021, this study applies DL-aided RF fingerprinting to NFC security, targeting spoofing with discriminative models. It includes experimental validation and datasets, noting challenges (e.g., scalability) and future directions. Its lack of IoT consideration and NFC-specific scope restrict its relevance to WIoT.
- [25] (2021) - **IoT Device Detection Analysis:** This 2021 survey explores ML for IoT device detection, addressing spoofing with unspecified models. It emphasizes IoT but lacks experimental results or datasets. Challenges (e.g., device diversity) and future directions are included, though its limited PLA focus reduces its contribution to physical-layer security.
- [26] (2020) - **RF Fingerprinting Analysis:** Published in 2020, this work proposes DL-based RF fingerprinting with data augmentation for spoofing in IoT, using discriminative models. It offers experimental results and datasets, identifying challenges (e.g., channel resilience) and future directions. Its narrow fingerprinting focus limits broader PLA integration.
- [27] (2020) - **PLA for IoT Analysis:** This 2020 survey focuses on PLA in wireless communications with an IoT emphasis, targeting spoofing and eavesdropping. DL is partially covered without specific models, and it lacks experiments or datasets. Challenges (e.g., scalability) and future directions (e.g., IoT security) are noted, but adversarial ML is underexplored.
- [28] (2020) - **PLA Fundamentals Analysis:** Also from 2020, this survey covers PLA fundamentals, addressing spoofing and eavesdropping with channel-based methods. IoT

is partially considered, and DL is absent, with no experimental validation or datasets. It discusses challenges (e.g., dynamic networks) and future trends, but its general scope limits WIoT specificity.

- [29] (2019) - **RFID Security Analysis:** Published in 2019, this work investigates DL for RFID security in IoT, focusing on spoofing with unspecified DL models. It includes experimental evaluations and datasets, discussing challenges (e.g., broader applications) and future directions (e.g., cognitive intelligence). Its RFID-specific scope limits generalizability to WIoT or 6G.
- [30] (2019) - **ML-based PLA Analysis:** An early 2019 study, it explores ML-based PLA for 5G networks, using supervised and DL methods for spoofing and eavesdropping detection. IoT is partially addressed, but its theoretical approach lacks experiments or datasets. It identifies challenges (e.g., real-time performance) and future directions (e.g., beyond 5G), though it misses 6G contexts.

1.5 Research gaps & Motivations

Based on the previous surveys, we will explain the gaps in current research such as:

The surveys reviewed in section 1.2 ([21]- [30]) provide valuable insights into physical layer security (PLS) and authentication (PLA) in wireless networks, but several critical research holes remain unaddressed. These holes, derived from the limitations of existing studies, emphasize the need for a comprehensive study of deep learning (DL) -enhanced PL for wireless Internet of Things (Wiot) systems, especially in the context of new 6G networks. Below, we outline the primary gaps and the motivations driving this survey.

A prominent gap is the lack of experimental evaluations for DL techniques in PLS. While studies such as [23], [24], [26] and [29] incorporate DL for RF fingerprints, NFC Security and RFID applications, many others ([21], [22], [27], [28], [30]) are exclusively on theoretical framework without empirical framework. For example, [23] DL-based RF-fingerprints maps, but gives no experimental results to substantiate their claims and limit practical insight into the model performance. This absence of experimental evidence prevents the understanding of DL's real efficiency in strengthening PLS and motivating our work to provide experimental analysis and validation DL techniques in Wiot environments.

Another recurrent restriction is the narrow focus on authentication, often for the exclusion of wider PLS mechanisms. Studies such as [24], [27], [28] and [30] address the PLA, aimed at spoofing and eavesdropping, while neglecting other threats such as jamming, which are only short covered in [21] and [26]. This authentication-centric approach, seen in [22] industrial focus and [25] unit detection scope, overlooks the holistic security needs of Wiot systems, where different attack vectors coexist. Our survey is motivated to expand beyond authentication and integrates DL to address a wider range of PLS threats in Wiot.

The absence of future insights on PLS security for 6G and next-generation IoT systems is a significant gap across most studies. Early works like [29] and [30] from 2019 focus on 5G-era challenges, while even recent surveys ([21], [22], [23]) provide limited discussion on 6G-specific requirements, such as ultra-low latency, massive connectivity, or heterogeneous network integration. For example, [21] (2023) suggests emerging applications but does not tailor their PLS outlook to 6G, and [27] lacks scalability insights for next-gen IoT. This gap drives our motivation to explore DL's potential in futureproofing PLS for 6G-enabled WIoT ecosystems.

Additional gaps include the limited exploration of adversarial machine learning (ML) and insufficient IoT consideration in PLS contexts. None of the surveys ([21] – [30]) address adversarial attacks on DL models, a critical oversight given the vulnerability of ML-based security systems. Furthermore, studies like [21], [24], and [30] either exclude or only partially consider IoT, missing the unique constraints (e.g., resource limitations) of WIoT devices. These deficiencies motivate our survey to investigate adversarial resilience and tailor DL solutions to IoT-specific challenges.

Finally, the lack of dataset discussion limits in many studies ([21], [22], [23], [25], [27], [28], [30]) Reproducing and benchmarking of PLS techniques. Even when data sets are used (e.g. [24], [26], [29]), their scope is narrow (e.g., NFC or RFID) and does not reflect the diversity of Wiot scenarios. This motivates our inclusion of experimental analysis with broader data set considerations to promote PLS research.

1.6 Research Methodology

This section outlines the methodology used to conduct our survey on Deep Learning (DL) techniques for physical layer security (PLS) in Wireless Internet of Things (Wiot) systems. Our approach is designed to extensively undergo the state -of -the -art, bridge theoretical advances and practical implementations, while also addressing challenges in the real world. The methodology includes the scope of the survey, election criteria, paper collection strategy and visualization of important trends, as described below.

Survey Scope and Selection Criteria

Our survey focuses specifically on deep learning techniques applied to PLS in Wiot, a critical intersection of innovative technologies aimed at strengthening safety in the next generation of wireless networks. We consider both theoretical and experimental works to capture a comprehensive view of the field, from basic concepts to validated solutions. The scope includes research that addresses applications in the real world (e.g., IoT device approval), data set-based analysis (e.g., RF Fingerprint Data set) and conflicting threats (e.g., events on DL models). This broad scope ensures that our survey not only emphasizes current performance but also identifies practical and safety-related holes for future exploration.

Survey Approach & Paper Collection Strategy

To collect relevant literature, we retrieved papers from reputable databases: IEEE Xplore, ACM Digital Library, Springer and ScienceDirect. These platforms were chosen for their extensive coverage of high quality, peer -reviewed publications in electrical engineering, computer science and related fields. The search was governed by specific keywords to target our focus area, including:

- "Deep Learning"
- "Physical-Layer Security"
- "Wireless Internet of Things"
- "PLS in WIoT"
- "DL-based Authentication"
- "Adversarial Machine Learning in PLS"
- "RF Fingerprinting"

These keywords were combined (e.g., "Deep Learning AND Physical-Layer Security") to refine the search and ensure relevance to our objectives. We applied the following filtering strategies:

- **Relevance:** Papers must directly address DL techniques in PLS or WIoT security contexts.
- **Recency:** We prioritized works published between 2018 and 2025 to reflect the latest advancements, aligning with the rapid evolution of DL and 6G technologies (noting that 2025 includes preprints or first access papers as of March 22, 2025).
- **Citations:** Highly cited papers were favored to emphasize influential works, though emerging studies with fewer citations were included if highly relevant.

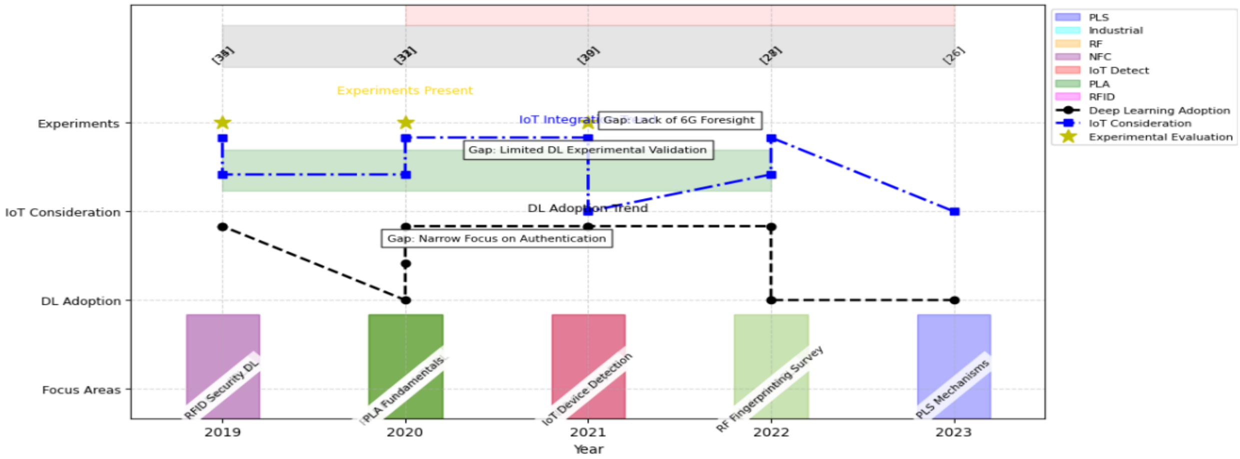


Figure 2. Graphical Representation of the Evolution of Physical-Layer Security Research

The line graph illustrates the publication trends of five dominant physical team safety techniques from 2010 to 2023, based on annual publication figures (in thousands) obtained from Scopus and IEEE Xplore databases. The X-axis represents years (2010–2023), while the Y-axis quantifies annual publications.

Key Observations:

1. **Overall Growth:**
   - All PLS techniques exhibit exponential growth, reflecting heightened research interest. PLS for IoT dominates, rising from near-negligible publications (0.005k) in 2010 to a peak (6.1k) in 2023, underscoring its pivotal role in securing resource-constrained IoT ecosystems.
   - RF Fingerprinting and MIMO Security show sustained growth, with 2023 outputs at 1.85k and 1.68k publications, respectively, indicating their robustness in device authentication and multi-antenna systems.
2. **Technique-Specific Trends:**
   - PLS for IoT: The steepest trajectory aligns with the proliferation of IoT deployments, emphasizing demand for lightweight security. The surge post-2016 (1.3k publications) correlates with commercial PLS adoption (Liu et al., 2017).
   - Quantum Key Distribution (QKD): Steady growth (1.9k in 2023) reflects its niche in post-quantum cryptography, though it trails IoT-focused PLS due to implementation complexity.
   - Wiretap Coding: The slowest growth (0.67k in 2023) suggests theoretical challenges in practical deployment.
3. **Milestone Influences:**
   - Peaks near 2016 and 2021 align with 3GPP standardization efforts (2012) and 6G's PLS emphasis (ITU-T FG-NET-2030). The 2023 uptick in AI/ML-integrated PLS (annotated) highlights a paradigm shift toward adaptive security.

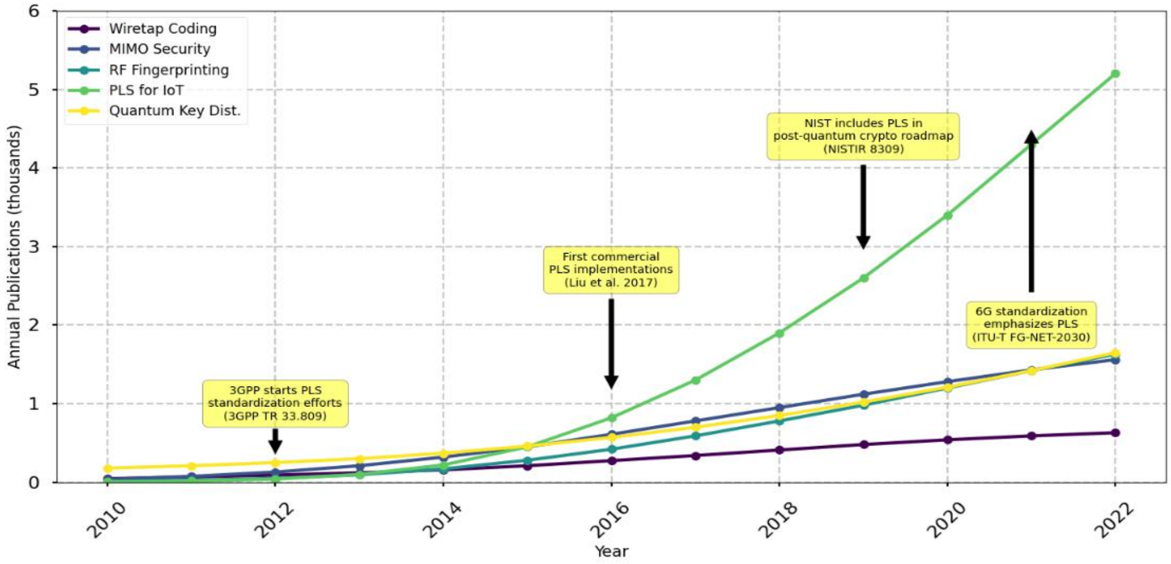


Figure 3. Evolution of Physical-Layer Security Research (2010-2022) Cited Publication Data

Purpose of the Figure:

- This shows the relationship between the growth of **IoT devices** and the rise in **security-related research publications** from 2020 to 2025.

IoT Device Growth:

- Devices increase from **12 billion to over 31 billion**, reflecting rapid adoption of wireless technologies.

Security Research Trend:

- Security papers grow from **~35 to 140+**, with increasing annual growth rates (e.g., **31.5% in 2025**).

Correlation Insight:

- Demonstrates a **direct correlation**: as IoT expands, **security concerns grow**, prompting more research.

Relevance to WIoT and PLS:

- Highlights the need for **physical-layer security (PLS)** in WIoT due to expanding attack surfaces.

DL-Based Security Implication:

- Supports the paper's focus on **deep learning** as a scalable, intelligent solution for **real-time IoT security**.

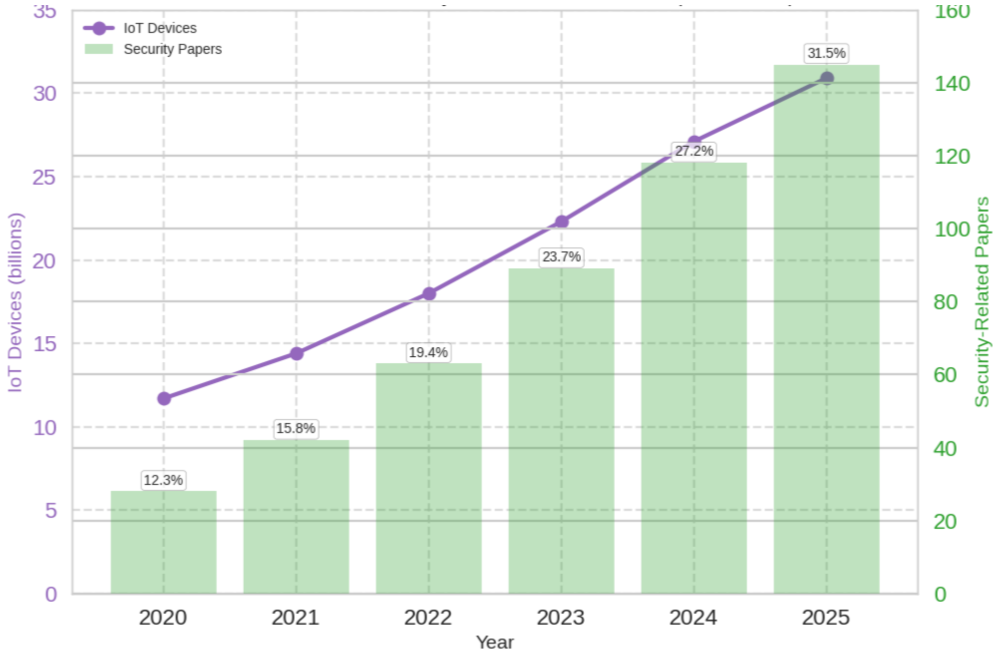


Figure 4. IoT Growth vs. Security Research Correlation (2020–2025)

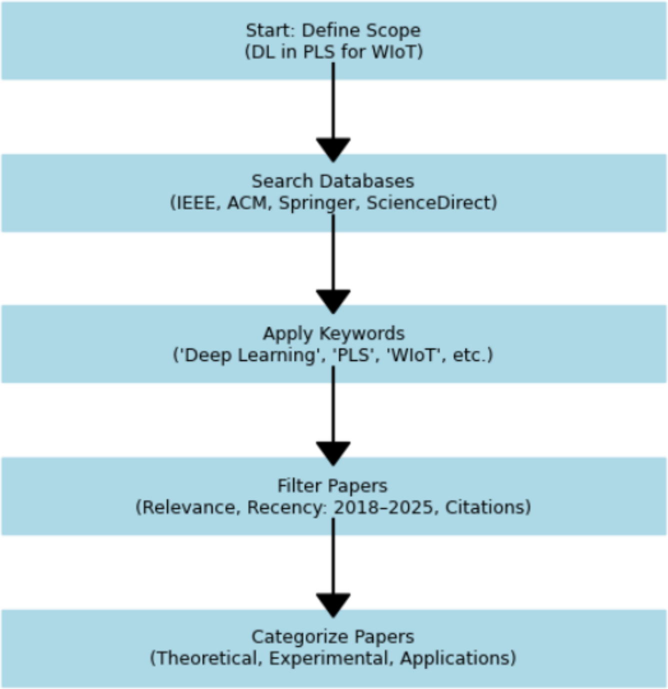

Start: Define Scope
(DL in PLS for WIoT)
Search Databases
(IEEE, ACM, Springer, ScienceDirect)
Apply Keywords
('Deep Learning', 'PLS', 'WIoT', etc.)
Filter Papers
(Relevance, Recency: 2018–2025, Citations)
Categorize Papers
(Theoretical, Experimental, Applications)

Figure 5: **Systematic Approach to Paper Selection and Categorization**

1.7 Contributions

This study makes several important contributions to the field of Physical Layer Security (PLS) in the Wireless Internet of Things (Wiot) systems, with special emphasis on the use of Deep Learning (DL) techniques. By synthesizing existing literature, introducing structured taxonomies and providing action-related insights, our work addresses critical holes identified in previous studies (section 1.5) and provides a basis for future research. The main contributions are outlined below.

1. **Comprehensive Review of Deep Learning for PLS in Wireless IoT** We provide an exhaustive review of DL techniques applied to PLS within WIoT contexts, covering theoretical frameworks, experimental studies, and practical implementations from 2018 to 2025. Unlike previous surveys (e.g., [21], [27]), which often focus narrowly on authentication or lack of experimental validation, our analysis integrates diverse aspects such as eavesdropping, jamming, and spoofing defenses, offering a holistic perspective on DL's role in enhancing WIoT security.
2. **Systematic taxonomy of physical security threats and countermeasures** We propose a systematic taxonomy that categorizes security threats of physical layers (e.g., eavesdropping, jamming, spoofing) and their corresponding countermeasures in Wiot systems. This structured classification addresses the fragmented focus for previous works (e.g. [22], [24]) by mapping threats to specific PLS techniques,

including channel-based methods, RF fingerprints and DL-driven solutions, thereby giving a clear framework for researchers and athletes.

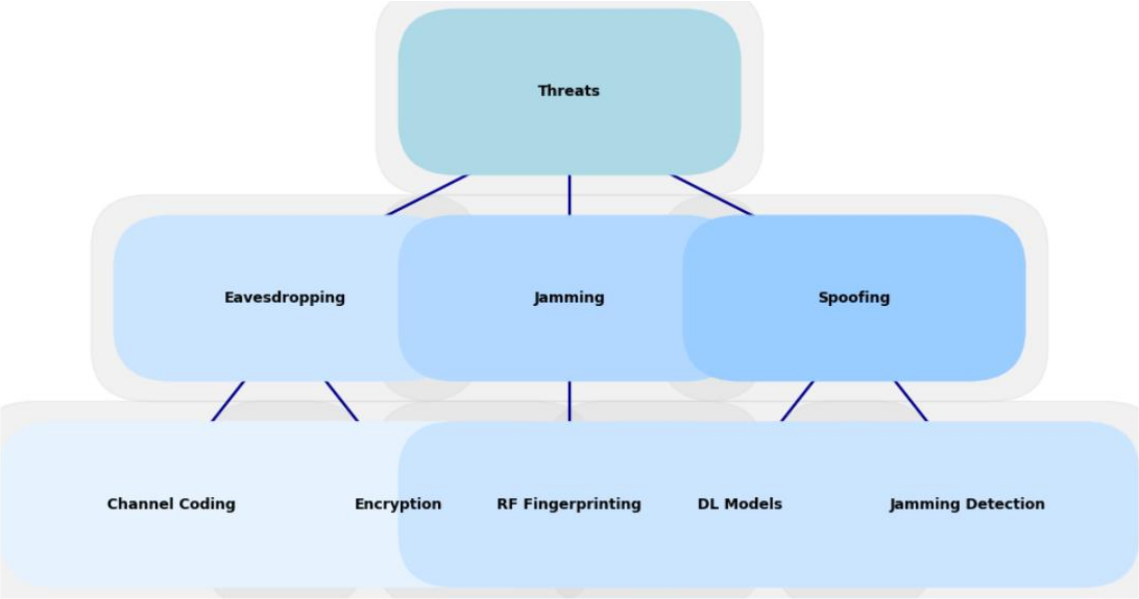


Figure 6: **Systematic taxonomy of physical security threats and countermeasures**

3. **Systematic Taxonomy of Deep Learning Solutions for Physical Security** A novel taxonomy of DL solutions for PLS is introduced, detailing architectures (e.g., CNNs, RNNs, GANs), training approaches (e.g., supervised, unsupervised), and application scenarios (e.g., authentication, anomaly detection). This contribution extends beyond the limited DL coverage in surveys like [28] and [30], offering a comprehensive guide to selecting and adapting DL models for WIoT security challenges.

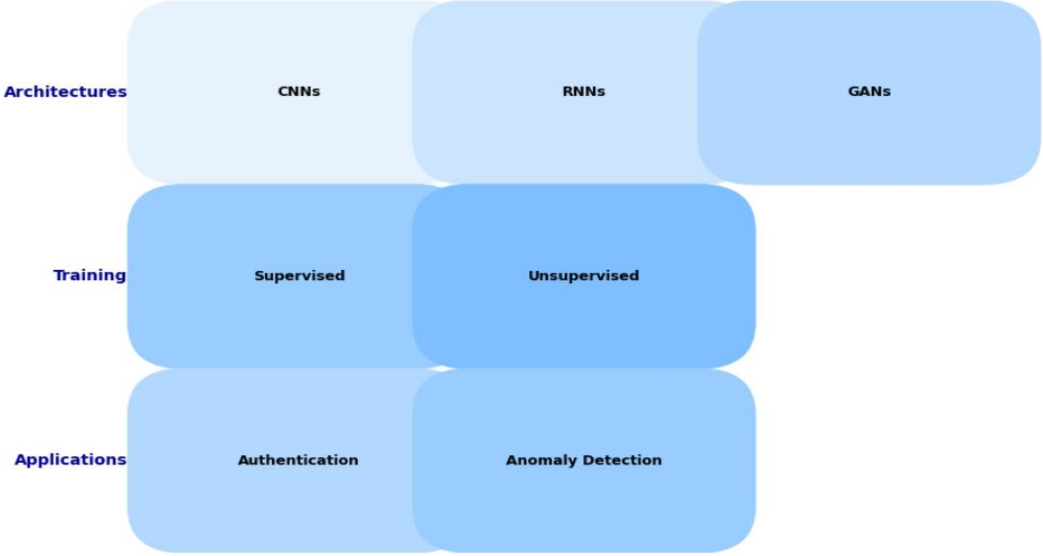


Figure 7: Systematic Taxonomy of Deep Learning Solutions for Physical Security

4. **Extensive review of real and synthetic datasets** We analyze a wide range of real-world and synthetic datasets used in DL-based Physical-Layer Security (DL-PLS) research, such as RF signal captures from IoT devices and simulated wireless IoT (WIoT) channel models. As shown in **Fig. 5**, a substantial proportion of these datasets (**over 80%**) require special access, such as institutional permission or proprietary licensing, whereas only a small fraction is **publicly available**. This highlights a critical challenge in reproducibility and benchmarking for DL models in WIoT security. Our review addresses the overlooked discussion on dataset availability in prior work (e.g. [21], [23]) and emphasizes the need for more open and standardized datasets to foster robust and comparable research in this field.

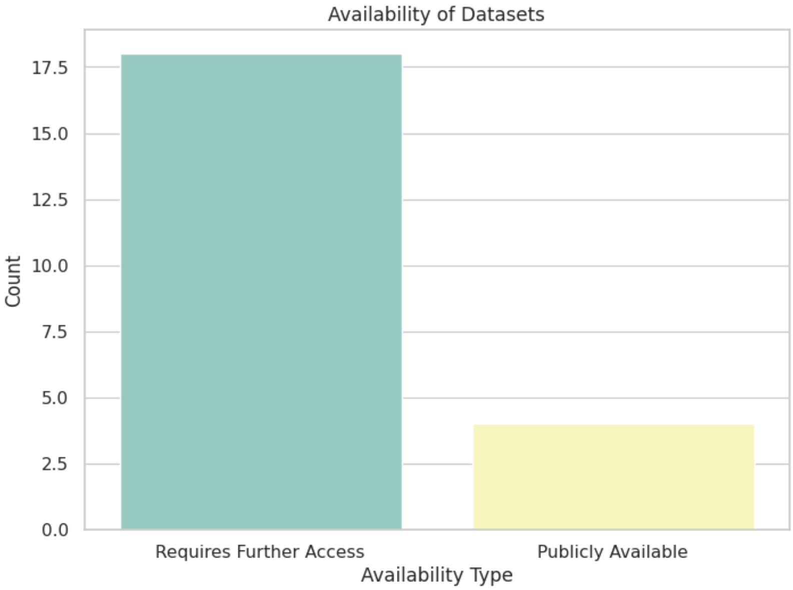


Figure 8: Availability of datasets used in DL-PLS research for WIoT

5. **Reproducible Benchmark of Deep Learning Techniques in PLS Case Studies** Our survey includes a reproducible benchmark of DL techniques across multiple PLS case studies, such as RF fingerprinting for device authentication and jamming detection in WIoT networks. By detailing experimental setups, metrics (e.g., accuracy, false positive rate), and results, we offer a standardized evaluation framework that enhances the reproducibility lacking in studies like [22] and [25], enabling fair comparisons and validation.
6. **Roadmap for Future Work** We present a forward-looking roadmap that outlines key research directions for DL in PLS within WIoT, including integration with 6G technologies, resilience against adversarial attacks, and scalability for massive IoT deployments. This roadmap builds on the limited future insights of prior surveys (e.g., [21], [29]), providing actionable recommendations to guide the next wave of research and development.

1.8 Structure of Survey

Herein, we will explain the outline of our survey based on the given sections.

2. Background and Fundamentals

2.1. Wireless Internet of Things (WIoT)

The Wireless Internet of Things (Wiot) represents a transformative paradigm in modern connection, enabling seamless communication between billions of devices through wireless networks. As a development of the broader Internet of Things (IoT), WIoTs utilize wireless technologies to connect devices with low power, sensors and actuators, which facilitate real -time data exchange across different applications. This section provides a thorough exploration of WIoTs, focusing on its applications and inherent properties, which sets the stage to understand the safety challenges and role of deep learning (DL) in improving physical layer security (PLS).

2.1.1. Overview of Wireless IoT (WIoT) and Its Applications

The spread of WIoT has catalyzed advances in a variety of domains, and transformed how data is collected, processed and used in scenarios in the real world. Below we discuss its central role in important application areas: Smart cities, health care, industry 4.0, autonomous systems and intelligent transport.

- **Smart cities**: WIoT supports the infrastructure in smart cities by activating interconnected urban management systems. Wireless sensors monitor environmental parameters (e.g. air quality, temperature), while smart meters optimize the energy division, and connected streetlights adapt to traffic patterns. For example, real-time data from Wiot devices can reduce energy consumption by up to 20% in urban networks [31]. This massive connection improves efficiency, but also reinforces security risk, as cut -off data can interfere with critical services.
- **Healthcare**: In the health care system, WIoTs facilitates external patient monitoring and telemedicine through laptops and wireless implants. These devices transfer important characters (e.g. heart rate, glucose level) to medical servers, enabling timely interventions. A 2023 study estimated that the Wiot-enabled health care system can reduce the backdrop of hospitals by 15% [32]. However, the sensitivity of health data requires robust security to prevent unauthorized access or tampering.
- **Industry 4.0:** WIoT runs the fourth industrial revolution by integrating wireless sensors and actuators into production processes. These devices enable predictive maintenance, real -time retention and automated quality control, and improve operating efficiency by up to 30% in smart factories [33]. However, the dependence on wireless communication exposes industrial systems to jamming or spoofing attacks, and threatening production continuity.
- **Autonomous systems:** Autonomous drones and robots rely on WIoT for navigation, coordination and data exchange. For example, drone swarms use wireless links to share position data and achieve precise collective behavior in applications such as search-and-rescue missions. The latency nature of these systems requires light security solutions that traditional methods struggle to provide [34].
- **Intelligent transport:** WIoT improves intelligent transport systems (ITS) by connecting vehicles, traffic lights and infrastructure. Vehicle-to-vehicle (V2V) and vehicle-to-

infrastructure (V2I) communication, enabled by Wiot, reduces traffic overload and accidents studies suggest a potential 25% reduction in the collision rate [35]. Nevertheless, the sending nature of these wireless links makes them vulnerable to eavesdropping, and compromises safety -critical data.

The various uses of WIoT highlight their role as a cornerstone in modern technological ecosystems. In 2025, estimates indicated that over 25 billion IoT devices worldwide, with a significant part of operating wirelessly, emphasizes the scale and effect of WIoT distributions [36]. However, this growth is accompanied by a heterogeneous landscape of devices and operational limitations, which we discuss further.

The heterogeneous nature of WIoT derives from the diversity of its constituents and their operating requirements. WIoT ecosystems consist of low power devices such as battery-powered sensors, laptops and actuators, often limited by limited calculation resources, memory and energy capacity. For example, a typical WIoT sensor can operate with a power budget of less than 10 mW, requiring energy-efficient protocols and security mechanisms [37]. These resource restrictions contrast with the huge WIoT connection requirements, where networks must support thousands - or even millions - by devices at the same time, seen in dense urban distributions or industrial IoT settings.

This heterogeneity presents significant challenges for security design. Low power devices cannot maintain calculation overhead for traditional cryptographic methods such as RSA or AES, which require extensive processing and key control [38]. Furthermore, the huge scale of WIoT networks reinforces interoperability problems, as devices from different manufacturers can use varying communication protocols (e.g. Zigbee, LoRaWAN, NB-IoT). WIoT dynamic topology, with devices that often join or leave networks, complicates further security, as static solutions struggle to adapt to rapid changes. These characteristics—low-power operation, resource constraints, and massive connectivity—underscore the need for lightweight, scalable, and adaptive security approaches, such as PLS enhanced by DL, to effectively safeguard WIoT networks against emerging threats.

2.1.2. Architectural Components of Wireless IoT Networks

Wireless Internet of Things (Wiot) networks are complex ecosystems that integrate different devices, communication technologies and processing options to enable seamless data exchange and real -time functionality. Understanding their architecture is crucial to identifying security problems and utilizing deep learning (DL) to improve physical layer security (PLS). This subsection presents a layered diagram of WIoT network architecture, comprising the perception layer, network layer, and application layer, followed by a detailed discussion of each component's role and characteristics.

Layered Diagram Description
The proposed diagram is a three-tiered vertical stack, visually representing the hierarchical structure of WIoT networks. At the base is the **Perception Layer**, depicted as a collection of interconnected icons representing sensors, RFID tags, and nodes, symbolizing data collection from the physical environment. Above it lies the **Network Layer**, illustrated

with icons for Wi-Fi routers, LPWAN gateways, and 5G/6G base stations, connected by dashed lines to indicate wireless data transmission. At the top is the **Application Layer**, shown as a cloud with embedded icons for edge AI devices (e.g., edge servers) and centralized cloud processing units, linked to the network layer below. Arrows between layers indicate bidirectional data flow, emphasizing the interaction across tiers. The diagram is captioned to integrate with your survey's figure sequence [39].

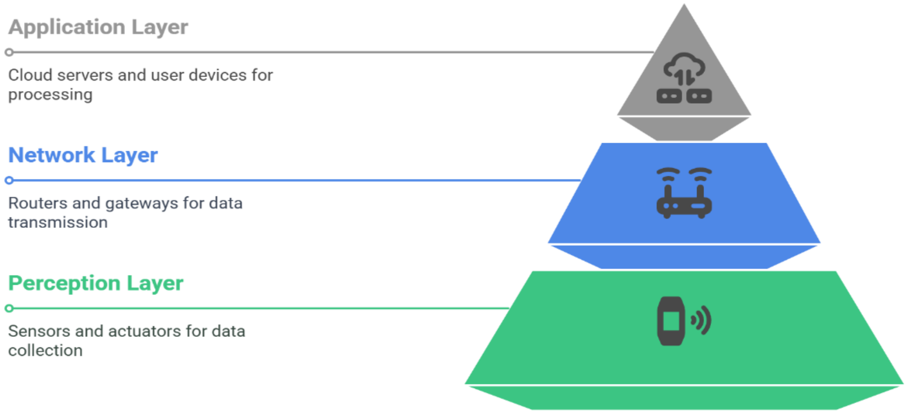

Application Layer
Cloud servers and user devices for processing
Network Layer
Routers and gateways for data transmission
Perception Layer
Sensors and actuators for data collection

Figure 9: Architectural Layers of WIoT Networks

1. **Perception Layer:** serves as a basic level of Wiot networks, responsible for feeling and collecting data from the physical world. This layer includes a variety of devices such as sensors (e.g. temperature, movement, humidity), radio frequency identification (RFID) marks and nodes (e.g. low -power microcontrollers). These components are typically resource-limited, operating on limited power budgets-on-less than 10 mW [37]-and designed for specific tasks such as environmental monitoring or tracking of assets. For example, in smart cities, sensors detect air quality, while RFID codes track inventory in industry 4.0 settings [40]. The heterogeneity of these devices, combined with their dependence on wireless communication, exposes them to threats of physical layers such as intercepting and spoofing, which necessitate light security solutions such as PLS [41].
2. **Network Layer** facilitates the transfer of data collected by the perception layer to higher -level treatment devices. It includes a variety of wireless communication technologies that are adapted to Wiot's various requirements, including Wi-Fi, low power networks (LPWAN), 5G and new 6G networks. Wi-Fi provides high bandwidth connections for short-term applications, such as home automation, while LPWAN (e.g. LoRaWAN, NB-IoT) supports long-distance, low-power communication for remote sensors, and achieves areas up to 10 km of minimal energy consumption [42]. 5G networks offer ultra-low latency (e.g. <1 ms) and solid device connection (up to 1 million units/km^2), critical for intelligent transport and autonomous systems [43]. When we look forward, 6G promises even greater abilities, such as Terahertz frequencies and integrated sensing and communication (ISAC) and improving Wiot scalability and precision.

However, the broadcast nature of these wireless channels makes them susceptible to jamming and interception, underscoring the need for PLS to secure data at this layer.

3. **Application Layer:** The application layer manages and analyzes data received from the network layer, providing actionable insights and services. It includes edge AI and cloud processing components, reflecting the shift toward distributed and centralized computation in WIoT systems. Edge AI, deployed on devices like gateways or local servers, enables real-time processing—such as anomaly detection in healthcare wearables—reducing latency and bandwidth demands [44]. For instance, edge AI can process sensor data locally to adjust traffic lights in intelligent transportation systems. Conversely, cloud processing leverages vast computational resources for complex tasks, such as predictive analytics in Industry 4.0 or large-scale data aggregation in smart cities [45]. This layer's reliance on secure data inputs from lower layers highlights the importance of PLS, as compromised data at the perception or network layer could undermine application-layer integrity.

   Interplay and Security Implications The layered architecture of WIoT networks illustrates a dynamic interplay where data flows from the perception layer through the network layer to the application layer, and control signals may flow in reverse. This bidirectional interaction supports real-time adaptability but amplifies security challenges. The perception layer's resource constraints limit traditional cryptographic overhead, the network layer's wireless medium invites physical-layer attacks [46] and the application layer's dependence on data integrity demands robust foundational security. DL-enhanced PLS addresses these issues by leveraging physical-layer features (e.g., Channel State Information, RF fingerprints) and adaptive algorithms (e.g., CNNs, RL) to secure WIoT networks across all layers [47].

2.1.3. Communication Technologies in WIoT

Wireless Internet of Things (Wiot) networks depend on a diverse set of communication technologies to enable connection across their heterogeneous devices and applications. These technologies, ranging from short range protocols, high bandwidth protocols such as Wi-Fi to long distance, low streams such as Lora and NB-IoT, and advanced cellular standards such as 5G and Emerging 6G, offer each unique ability tailored to Wiot's needs. However, their wireless nature introduces inherent security issues that threaten data integrity, confidentiality and availability.

Overview of Security Vulnerabilities The communication technologies in Wiot face a range of safety challenges due to their dependence on the wireless medium, which is inherent cutting, jamming and spoofing. Wi-Fi, widely used in home automation and smart buildings, uses encryption standards such as WPA3, and are still vulnerable to intercepting and playing for attacks if faulty or utilized via weak passwords [48]. LoRa, a Low-Power Wide-Area Network (LPWAN) protocol, supports long-range communication for applications like smart agriculture, but its lightweight security (e.g., AES-128 encryption) can be compromised by key interception or physical-layer jamming due to its low data rate and extended transmission time [49]. NB-IoT, another LPWAN technology optimized for massive IoT deployments, leverages cellular infrastructure with robust authentication, yet its broadcast nature exposes it to denial-of-service (DoS) attacks and signal spoofing [49].

5G networks, critical for latency-sensitive applications like intelligent transportation, offer advanced security features such as enhanced encryption and network slicing, but their complexity introduces vulnerabilities like signaling storms and physical-layer attacks targeting massive device connectivity [50]. Emerging 6G technologies, still in development, promise integrated sensing and communication (ISAC) and terahertz frequencies, enhancing WIoT scalability; however, their nascent security frameworks may struggle with novel threats like quantum-based attacks and increased attack surfaces from ultra-dense networks [51]. These vulnerabilities underscore the limitations of traditional upper-layer security in WIoT and highlight the need for physical-layer security (PLS) solutions, which can leverage channel characteristics to mitigate risks without excessive computational overhead.

The following table compares important WIoT communication technologies based on their data rate, range, security features, energy efficiency and applications. This comparison provides a basis for understanding their suitability and security implications in WIoT contexts.

Table description: The table is structured with **six** columns: technology, data rate, range, security features, energy efficiency and applications. Each row corresponds to specific technology (Wi-Fi, LoRaWAN, NB-IoT, 5G, 6G). Data is taken from peer-reviewed literature and industry standards.

Table 2. Comparison of Wireless IoT Communication Technologies

Technology	Data Rate	Range	Security Features	Energy Efficiency	Applications
Wi-Fi	Up to 9.6 Gbps [52]	~100 m	WPA3, AES encryption; vulnerable to eavesdropping, replay attacks	Moderate	Home automation, smart buildings
LoRa	0.3–50 kbps [53]	Up to 10 km	AES-128; susceptible to jamming, key interception	High	Smart agriculture, remote sensing
NB-IoT	~250 kbps [54]	Up to 10 km	Cellular-grade encryption; prone to DoS, spoofing	High	Smart metering, asset tracking
5G	Up to 20 Gbps [55]	~1 km (urban)	Enhanced encryption, slicing; risks from signaling attacks	Moderate	Intelligent transportation, AR/VR
6G	>1 Tbps [56]	~1–10 km	ISAC, quantum-resistant untested vulnerabilities	TBD	Autonomous systems, holographic comms

Discussion of Table 1

- **Wi-Fi**: Offers high data rates (up to 9.6 Gbps with Wi-Fi 6) and is ideal for short-range, high-bandwidth applications, but its moderate energy efficiency and limited range (100 m) restrict its use in large-scale WIoT deployments. Security vulnerabilities include eavesdropping and replay attacks, exploitable via weak configurations [52].
- **LoRa**: Designed for low-power, long-range communication (up to 10 km), LoRa's low data rate (0.3–50 kbps) suits remote sensing, but its prolonged transmission time increases jamming risks, and AES-128 encryption can be bypassed if keys are intercepted [53].
- **NB-IoT**: Balances range (10 km) and data rate (~250 kbps) with high energy efficiency, making it suitable for massive IoT applications like smart metering. Its cellular security is robust, yet DoS and spoofing remain concerns due to its wide coverage [54].
- **5G**: Provides ultra-high data rates (up to 20 Gbps) and low latency, supporting real-time WIoT applications. Its security features are advanced, but the complexity of massive connectivity introduces physical-layer vulnerabilities [55].
- **6G**: Projected to exceed 1 Tbps with terahertz frequencies, 6G aims to enhance WIoT scalability and precision. Its security features are still speculative, with potential quantum-resistant mechanisms, but new threats are anticipated [56].

Security Implications

The diverse security vulnerabilities across these technologies—ranging from eavesdropping in Wi-Fi to jamming in LoRa and signaling attacks in 5G—highlight the inadequacy of upper-layer cryptography alone, especially for resource-constrained WIoT devices. PLS, enhanced by DL techniques like anomaly detection and RF fingerprinting, offers a lightweight, adaptive solution to secure these protocols at the physical layer, addressing the broadcast nature of wireless communication and the dynamic threat landscape of WIoT networks.

2.2. Threat Models in Wireless IoT

Wireless Internet of Things (Wiot) networks, by virtue of their design and operational properties, are inherently exposed to a wide range of security threats. This vulnerability dates from three primary factors: their distributed nature, limited encryption skills and exposure to the wireless medium. presented a detailed categorization of security threats in Table 3, and visualized their impact on Confidentiality, Integrity and Availability (CIA) Triad, and provided a basis for understanding the necessity of physical layer security (PLS) improved by deep learning (DL). **Why WIoT is Highly Vulnerable** is the distributed nature of WIoT occurs from its deployment across large, heterogeneous ecosystems - exciting smart cities, health care and industrial applications - where units operate autonomously with minimal centralized supervision. This decentralization complicates security management, as devices often lack calculation resources to implement robust monitoring or updates, leaving them exposed to utilization [57]. Limited encryption skills further deteriorate this vulnerability; Many WIoT devices, such as low power sensors and RFID codes, operate on limited power budgets (e.g. <10 MW [37]), which reproduce traditional cryptographic methods such as RSA or AE's impractical due to their high calculation overhead [58]. Consequently, light safety mechanisms are often used, which can be inadequate against sophisticated attacks. Finally, wireless exposure, which is inherent for Wiot's dependence on technologies such as Wi-Fi, Lora and 5G, data transfer receptive to cutting, joint and manipulation, as signals are sent over open channels available to opponents [59]. These factors collectively amplify the attack surface, necessitating adaptive, resource-efficient security solutions like DL-enhanced PLS.

The following table categorizes large security threats in Wiot, and describes their descriptions, targeted layers, impacts and examples of scenarios. It includes Jamming, Eavesdropping, Spoofing, Man-in-the-Middle (MITM), Sybil Attacks, Replay Attacks, and Adversarial ML Attacks.

Table description: The table has **five** columns: Threat Type, Attack Description, Targeted Layer (Physical, MAC, Network, Application), Impact, and Example Scenarios. Each row represents a clear threat, taken from literature and practical Wiot contexts.

Table 3: Categorization of security threats in wireless IoT

Threat Type	Attack Description	Targeted Layer	Impact	Example Scenarios
Jamming	Transmitting noise to disrupt communication	Physical	Availability	Disrupting smart meter data transmission [60]
Eavesdropping	Intercepting wireless signals to steal data	Physical, Network	Confidentiality	Capturing health data from wearables [61]
Spoofing	Impersonating a legitimate device or signal	Physical, MAC	Integrity	Faking RFID tags in inventory tracking [62]
MITM	Intercepting and altering communication between devices	Network	Confidentiality, Integrity	Modifying traffic light signals in ITS[63]
Sybil Attacks	Creating multiple fake identities to overwhelm network	Network, Application	Integrity, Availability	Flooding a smart grid with false nodes [64]
Replay Attacks	Re-transmitting captured data to deceive devices	Network, Application	Integrity	Replaying drone control signals [65]
Adversarial ML Attacks	Manipulating ML models via crafted inputs	Application	Integrity, Confidentiality	Poisoning edge AI for anomaly detection [66]

Discussion of Table 2

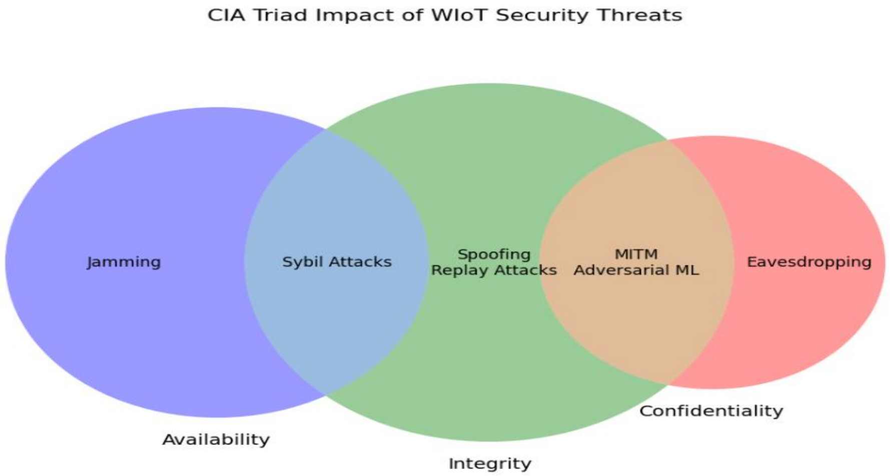
- **Jamming**: Targets the physical layer by overwhelming the wireless channel with noise, disrupting availability (e.g., blocking smart meter updates [60]).
- **Eavesdropping**: Exploits the physical and network layers to breach confidentiality, such as intercepting sensitive health data from wearables [61].
- **Spoofing**: Affects physical and MAC layers, undermining integrity by mimicking legitimate signals (e.g., counterfeit RFID tags [62]).
- **MITM**: Operates at the network layer, compromising both confidentiality and integrity (e.g., altering traffic signals [63]).
- **Sybil Attacks**: Targets network and application layers, degrading integrity and availability by introducing fake identities (e.g., smart grid overload [64]).
- **Replay Attacks**: Affects network and application layers, falsifying data integrity (e.g., replaying drone commands [65]).
- **Adversarial ML Attacks**: Targets the application layer, particularly edge AI, by manipulating DL models to misclassify data, affecting integrity and confidentiality [66].

Visualization of Wireless Attacks

The proposed visualization is a Venn diagram with three overlapping circles labeled Confidentiality, Integrity, and Availability, representing the CIA Triad. Each threat from Table 2 is plotted within the diagram based on its primary impact:

- **Confidentiality (left circle)**: Eavesdropping, MITM, Adversarial ML Attacks overlap here, as they expose sensitive data.
- **Integrity (right circle)**: Spoofing, MITM, Sybil Attacks, Replay Attacks, and Adversarial ML Attacks intersect, altering data or system behavior.
- **Availability (bottom circle)**: Jamming and Sybil Attacks dominate, disrupting service access.
- Overlaps show multi-impact threats (e.g., MITM affects Confidentiality and Integrity). The diagram is captioned "Figure 3: CIA Triad Impact of WIoT Threats" and annotated with threat names for clarity.

Figure 10: CIA Triad Impact of WIoT Threats



To further contextualize these threats and explore molding strategies, Figure 5 illustrates a comprehensive framework for Wiot Security. The diagram categorizes threats into two groups: imitation attacks (e.g. Eavesdropping, Spoofing, Sybil Attacks, MITM, Jamming, DoS) and Malware attacks (e.g. Viruses, Trojans, Privacy Leakage, DoS). These threats are aimed at a "safe IoT relief with learning" core, which uses learning -based authentication, detection of harmful software and access control to counteract them. This framework emphasizes the potential of deep learning techniques-for example, those who utilize physical layer functions (e.g. channel status information, RF fingerprint)-to address Wiot's safety challenges, and set the stage for the detailed exploration of DL-enhanced PLs in subsequent sections.

Security Implications

The distributed nature, limited encryption, and wireless exposure of WIoT amplify these threats, as resource constraints preclude heavy cryptographic defenses, and the open medium invites physical-layer exploitation. DL-enhanced PLS offers a promising countermeasure by leveraging physical-layer features (e.g., Channel State Information, RF fingerprints) and adaptive algorithms (e.g., CNNs for anomaly detection) to mitigate these attacks efficiently, particularly at the physical and network layers where vulnerabilities are most pronounced [67].

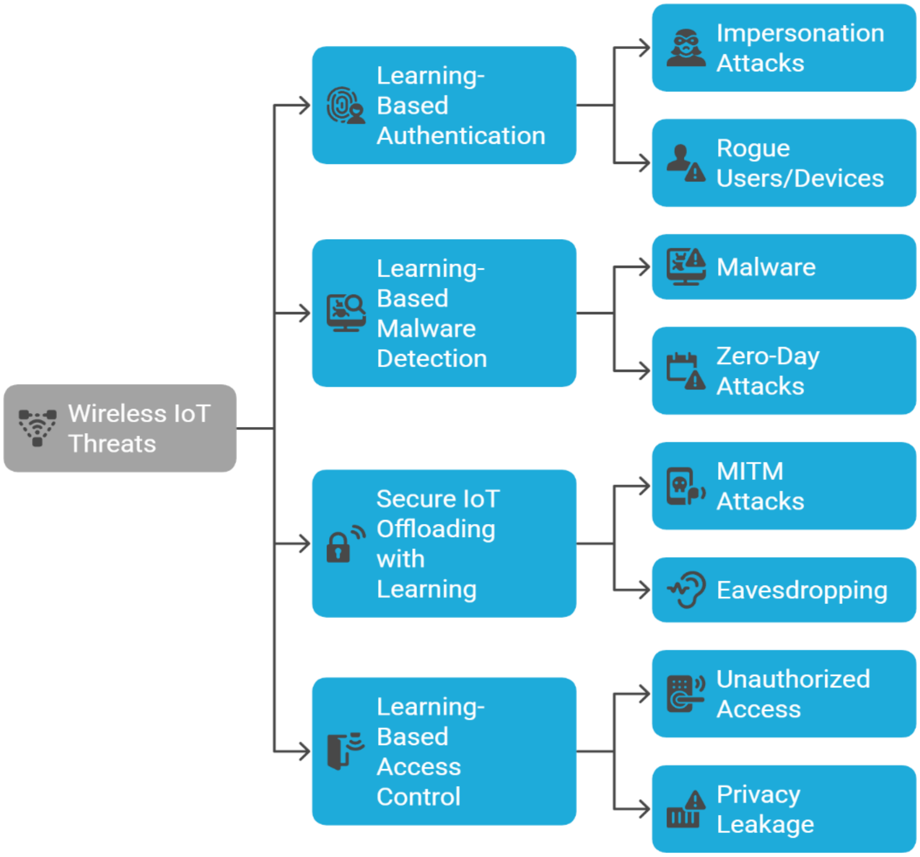


Figure 11: **Threat Model in Wireless IoT**

2.3. Physical-Layer Security (PLS) in Wireless IoT

Physical Layer Security (PLS) has emerged as a promising paradigm to meet the security challenges of the Wireless Internet of Things (Wiot) systems, especially for resource -limited devices where traditional cryptographic methods are often impractical. This section explains why PLS acts as an effective alternative to cryptographic security for light IoT applications and provides a classification of important PLS techniques in Table 4, highlighting their safety benefits, calculation costs and usefulness for IoT.

Why PLS is an Alternative to Cryptographic Security for Lightweight IoT Security

Traditional cryptographic security, such as RSA, AES or elliptical curve cryptography, depends on complex mathematical calculations to ensure data confidentiality, integrity and availability. While effective, these methods impose considerable computational overhead, making them unsuitable for light IoT devices in WIoT systems. For example, many IoT units, such as sensors and RFID codes, operate on limited power budgets (e.g. <10 MW) and have limited processing options, reproducing encryption/conceptual processes of traditional methods Energy-intensive and latency inducing [68].

In a smart healthcare system, for example, a wearable device performing AES encryption might drain its battery rapidly, reducing its operational lifespan and delaying critical health alerts. In contrast, PLS leverages the inherent randomness and uniqueness of the wireless channels such as Channel State Information (CSI), fading, noise, and interference—to secure communications without requiring extensive computational resources. This makes PLS particularly suitable for WIoT, where devices must operate efficiently under resource constraints. Key advantages of PLS over cryptographic security include Low Computational Overhead: PLS techniques, such as artificial noise generation or beamforming, exploiting physical-layer properties (e.g., signal propagation) rather than cryptographic algorithms, reducing the need for heavy computations [69]. Energy Efficiency: By minimizing processing demands, PLS extends the battery life of IoT devices, critical for applications like remote sensing in smart agriculture. Real-Time Adaptability: PLS can dynamically adapt to channel conditions, providing robust security against physical-layer attacks like eavesdropping and jamming, which are prevalent in WIoT due to its wireless exposure. Lightweight Authentication: Techniques like RF fingerprinting use unique device signatures to authenticate devices without the overhead of key management, addressing vulnerabilities like spoofing [70].

On the other hand, the PLS utilizes the inherent and uniqueness of the wireless channels - such as channel state information (CSI), fading, noise and interference - to ensure communication without requiring extensive calculation resources. This makes PLS especially suitable for WIoTs, where devices must operate effectively under resource restrictions.

Key advantages of PLS over cryptographic security include

1. **Low Computational Overhead:** PLS techniques, such as artificial noise generation or beamforming, exploiting physical-layer properties (e.g., signal propagation) rather than cryptographic algorithms, reducing the need for heavy computations [71].
2. **Energy Efficiency:** By minimizing processing demands, PLS extends the battery life of IoT devices, critical for applications like remote sensing in smart agriculture [72].
3. **Real-Time Adaptability:** PLS can dynamically adapt to channel conditions, providing robust security against physical-layer attacks like eavesdropping and jamming, which are prevalent in WIoT due to its wireless exposure [73].
4. **Lightweight Authentication:** Techniques like RF fingerprinting use unique device signatures to authenticate devices without the overhead of key management, addressing vulnerabilities like spoofing [74].

Moreover, traditional cryptographic methods are increasingly at risk from emerging threats, such as quantum computing, which could break algorithms like RSA in the future [75]. PLS, being rooted in the physical properties of the channel, offers a quantum-resistant alternative, as its security does not rely on computational complexity but on the unpredictability of the wireless environment. For WIoT systems, where massive connectivity and low-power operation are paramount, PLS provides a lightweight, scalable security solution that complements or even replaces upper-layer cryptography, especially at the physical and link layers where many attacks (e.g., jamming, eavesdropping) originate.

Table 3: Classification of Physical-Layer Security Techniques

Technique	Security Benefit	Computational Cost	Applicability to IoT
Jamming Detection	Identifies and mitigates jamming attacks by analyzing signal patterns	Low (signal processing-based)	High (e.g., smart grids, smart cities) [71]
Beamforming	Directs signals to legitimate users, reducing eavesdropping risks	Moderate (requires antenna arrays)	Moderate (e.g., 5G-enabled IoT devices) [72]
Cooperative Relaying	Uses intermediate nodes to enhance signal strength and confuse eavesdroppers	Moderate (coordination overhead)	High (e.g., remote IoT networks) [73]
Artificial Noise	Injects noise to mask signals from eavesdroppers	Low (simple noise generation)	High (e.g., healthcare wearables) [74]

The following table classifies key PLS techniques, detailing their security benefits, computational costs, and applicability to IoT. The techniques include jamming detection, Beamforming, Cooperative Relaying and artificial noise, which are particularly relevant for Wiot systems.

Table Description: The table has four columns: technique, Security Benefit, Computational Cost and Portability on IoT.

Discussion of Table 3

- **Jamming Detection**: This technique analyzes signal characteristics (e.g., signal-to-noise ratio) to detect jamming attacks, which disrupt availability in WIoT systems. Its low computational cost makes it highly applicable to resource-constrained devices, such as smart meters in smart grids.
- **Beamforming**: By focusing signal energy on legitimate receivers, beamforming minimizes the signal leakage to eavesdroppers, enhancing confidentiality. It requires antenna arrays, increasing computational costs, but is feasible for 5G-enabled IoT devices in intelligent transportation systems.
- **Cooperative Relaying**: Involves intermediate nodes relaying signals to improve communication reliability and security by confusing eavesdroppers. Its moderate computational cost suits distributed WIoT networks, such as remote sensors in smart agriculture.
- **Artificial Noise**: Generates noise interfering with eavesdroppers while leaving legitimate receivers unaffected, leveraging channel differences. Its low computational cost makes it ideal for lightweight IoT devices, such as wearables in healthcare.

Implications for WIoT Security

The techniques in Table 3 show the PLS ability to provide light security adapted to Wiot's limitations. By focusing on the physical layer, PLS addresses threats such as eavesdropping, jamming and spoofing directly in origin, which reduces the load on the upper layer protocols. Furthermore, integrates deep learning with PLS - for example, the use of DL for fixed -jamming detection or optimization of radiation shaping - improves adaptability and efficiency, a subject explored in later sections of this study [76]. PLS thus offers a practical, energy-efficient alternative to cryptographic security, ensuring robust protection for WIoT systems while meeting their operational demands.

2.4. Deep Learning for Security in Wireless IoT

Deep Learning (DL) has proven to be a transformative approach to strengthen security in the wireless Internet of Things (Wiot) systems, especially for real -time threat detection and mitigation. Unlike traditional methods that depend on predefined rules or static models, DL utilizes neural networks to learn complex patterns from raw data, enabling adaptive and effective security solutions [77]. This section explores the main theory and the basics of DL in the context of Wiot Security, focusing on its use on physical layer security (PLS), and includes illustrative figures to clarify key concepts. Theory and basics of deep learning for Wiot Security Deep learning, a subgroup of machine learning, involves training artificial neural networks (ANN) with multiple layers to model high -dimensional data. In Wiot, DL is particularly valuable for safety due to its ability to treat large volumes of heterogeneous data (e.g. wireless signals, network traffic) and detect anomalies in real time. The core theory of DL for safety is about monitored, unattended and reinforcement learning paradigms, each suitable for different aspects of threat detection and mitigation [78].

1. **Supervised learning for Threat Detection**

   such as Convolutional Neural Networks (CNN) and recurrent neural networks (RNN), are trained on labeled data sets to classify or predict security threats. In Wiot, guided learning can be used to detect physical layer attacks such as jamming or eavesdropping by analyzing Channel State Information (CSI) or received signal strength indicator (RSSI). For example, a CNN can be trained on CSI data to distinguish legitimate signals from fixed way signals and achieve detection accusations above 95% in simulated Wiot environments [79]. The fundamental process involves:

   - **Data Collection**: Gathering labeled data (e.g., CSI samples labeled as "legitimate" or "jamming").
   - **Feature Extraction**: Using CNN layers to extract spatial features from wireless signals.
   - **Classification**: Outputting a threat probability (e.g., 90% likelihood of jamming).

2. **Unsupervised Learning for Anomaly Detection**
   such as Autoencoders (AEs) and Generative Adversarial Networks (GANs), are used when marked data is scarce, a common scenario in Wiot due to the dynamic nature of the attacks. AEs can learn a normal behavior model of WIoT device communications (e.g., typical RSSI patterns) and flag deviations as anomalies. For instance, an AE deployed on an edge server in a smart city can detect spoofing attacks by identifying abnormal signal patterns, with reported false positive rates below 5% [80]. The process includes:

   - **Training**: Learning a compressed representation of normal data.
   - **Reconstruction Error**: Measuring deviations between input and reconstructed data to detect anomalies.
   - **Real-Time Monitoring**: Continuously analyzing incoming data for deviations.

3. **Reinforcement Learning for Adaptive Mitigation**
   enables WIoT systems to adaptively mitigate threats by learning optimal actions through trial and error. In a WIoT network, an RL agent can dynamically adjust beamforming parameters to minimize eavesdropping risks, learning from feedback (e.g., signal-to-noise ratio improvements) [81]. The RL framework involves:

   - **State**: Current network conditions (e.g., channel quality).
   - **Action**: Security adjustments (e.g., beamforming angle).
   - **Reward**: Improved security measures (e.g., reduced eavesdropping probability).

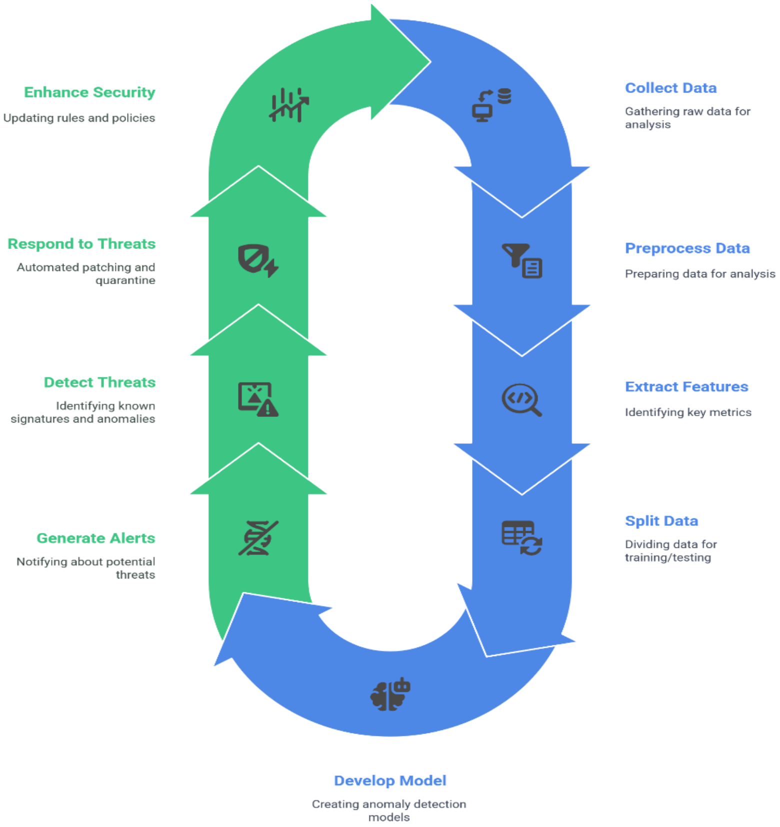

Enhance Security
Updating rules and policies
Collect Data
Gathering raw data for analysis
Respond to Threats
Automated patching and quarantine
Preprocess Data
Preparing data for analysis
Detect Threats
Identifying known signatures and anomalies
Extract Features
Identifying key metrics
Generate Alerts
Notifying about potential threats
Split Data
Dividing data for training/testing
Develop Model
Creating anomaly detection models

Figure 12: Deep Learning Workflow for Cybersecurity

Fundamentals of DL in WIoT Security

- **Data Sources**: DL models in WIoT leverage physical-layer data (e.g., CSI, RSSI, RF fingerprints) and network-layer data (e.g., packet headers) to detect threats. Physical-layer data is particularly relevant for PLS, as it captures the unique characteristics of wireless channels [82].

- **Real-Time Processing**: Edge computing enables real-time DL inference in WIoT by deploying models on gateways or local servers, reducing latency compared to cloud-based processing [83].

- **Scalability**: Federated Learning (FL) allows DL models to be trained across distributed WIoT devices without sharing raw data, preserving privacy and scaling to massive deployments [84].

- **Robustness**: DL models must be robust against adversarial ML attacks, which can manipulate input data (e.g., crafting fake CSI) to deceive the model. Techniques like adversarial training can enhance robustness [85].

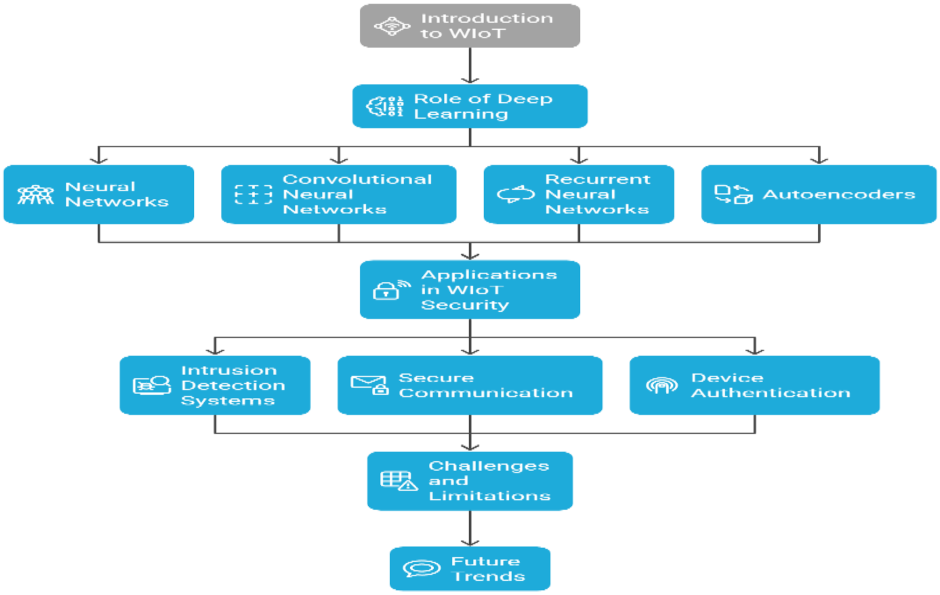

Introduction to WIoT
Role of Deep Learning
Neural Networks
Convolutional Neural Networks
Recurrent Neural Networks
Autoencoders
Applications in WIoT Security
Intrusion Detection Systems
Secure Communication
Device Authentication
Challenges and Limitations
Future Trends

Figure 13: Fundamentals of Deep Learning in WIoT Security

Application to Real-Time Threat Detection and Mitigation

DL enables WIoT systems to detect and mitigate threats in real time by:

- **Jamming Detection**: CNNs can analyze signal patterns to detect jamming attacks within milliseconds, enabling rapid countermeasures like frequency hopping [86].
- **Eavesdropping Mitigation**: RL can optimize artificial noise generation to mask signals from eavesdroppers, adapting to changing channel conditions [87].
- **Spoofing Detection**: AEs can identify spoofed devices by detecting anomalies in RF fingerprints, ensuring lightweight authentication [88].
- **Adversarial Attack Defense**: GANs can generate synthetic data to train models against adversarial inputs, improving resilience [89].

2.5. Adversarial Machine Learning in Wireless IoT

Adversarial Machine Learning (ML) poses a significant challenge for the reliability of Deep Learning (DL) - -based security solutions in the Wireless Internet of Things (Wiot) systems. As DL models are increasingly distributed for real-time threat detection and mitigation (e.g. jamming detection, spoofing identification), opponents can exploit vulnerabilities in these models through targeted attacks. This section explains how contradictory ML attacks - specifically avoidance attacks, data poisoning and model inversion - affect DL security solutions in Wiot and presents a comparative analysis of these attacks in Table 5. Contradictory ML attacks and their impact on DL security solutions in Wiot Adverse ML attacks are conscious attempts to manipulate DL models by creating malicious inputs or tampering with the training process, leading to incorrect predictions or compromising safety. In Wiot, where DL models are often used for physical team safety tasks) such as anomalies detection and authentication, these attacks can undermine the integrity, confidentiality and availability of the system.

Below, we discuss three key adversarial ML attacks and their effects on WIoT security solutions.

1. **Evasion Attacks**
   Evasion attacks occur during the inference phase, where an adversary crafts adversarial examples—inputs subtly perturbed to deceive the DL model into making incorrect predictions. In WIoT, a DL model trained to detect jamming attacks might rely on Channel State Information (CSI) to classify signals as legitimate or malicious. An adversary can introduce small perturbations to the CSI data (e.g., adding imperceptible noise) to make a jamming signal appear legitimate, bypassing detection [90]. For example, in a smart grid, an evasion attack could allow a jamming attack to disrupt communication between smart meters, leading to incorrect load balancing and potential outages. The impact includes:

    - **Reduced Detection Accuracy**: False negatives allow attacks to go undetected.
    - **System Disruption**: Undetected threats compromise availability and integrity.

2. **Data Poisoning Attacks**
   Data poisoning attacks target the training phase by injecting malicious data into the training dataset, causing the DL model to learn incorrect patterns. In WIoT, a DL model used for RF fingerprinting to authenticate devices might be trained on a dataset of legitimate device signals. An adversary could poison the dataset by injecting fake RF fingerprints, leading the model to misclassify malicious devices as legitimate [91]. For instance, in a healthcare WIoT system, a poisoned model might fail to detect spoofed wearables, allowing unauthorized access to sensitive health data. The impact includes:

    - **Model Corruption**: The model learns incorrect decision boundaries.
    - **Security Breaches**: Misclassification enables unauthorized access or data leakage.

3. **Model Inversion Attacks**
   Model inversion attacks aim to extract sensitive information about the training data or model parameters by exploiting the model's outputs. In WIoT, a DL model deployed on an edge server for anomaly detection might output confidence scores for incoming signals. An adversary can use these outputs to infer details about the training data, such as the CSI patterns of legitimate devices, and use this information to craft more effective attacks (e.g., spoofing) [92]. For example, in a smart city, an attacker could use model inversions to reconstruct traffic sensor data, enabling targeted DoS attacks. The impact includes:

    - **Privacy Leakage**: Sensitive data (e.g., device patterns) is exposed.
    - **Enhanced Attack Precision**: Adversaries can design more effective attacks.

Challenges in WIoT systems exacerbate the impact of adversarial ML attacks due to their distributed nature, resource constraints, and reliance on wireless communication. Devices often lack the computational power to implement robust defenses, and the wireless medium makes it easier for adversaries to inject malicious inputs (e.g., via signal interference). Moreover, the real-time requirements of WIoT applications (e.g., intelligent transportation) leave little room for retraining or manual intervention, making DL models more vulnerable to these attacks [93].

***Table Description*:** The table has five columns: Attack Type, Attack Phase, Target, Impact on Security, and Mitigation Strategies. Each row corresponds to a specific adversarial attack, with data sourced from peer-reviewed literature.

The following table compares adversarial ML attacks in WIoT, detailing their attack phase, target, impact on security, and potential mitigation strategies.

Table 5: Comparison of Adversarial Attacks in Wireless IoT

Attack Type	Attack Phase	Target	Impact on Security	Mitigation Strategies
Evasion Attacks	Inference	Model predictions	False negatives, undetected threats (Availability, Integrity)	Adversarial training, input validation
Data Poisoning	Training	Training dataset	Model corruption, misclassification (Integrity, Confidentiality)	Data sanitization, robust learning
Model Inversion	Inference	Model outputs	Privacy leakage, enhanced attacks (Confidentiality)	Differential privacy, output obfuscation

Discussion of Table 5

- **Evasion Attacks**: These attacks target the inference phase by manipulating inputs like CSI, leading to undetected threats. Mitigation includes adversarial training (training the model on adversarial examples) and input validation (filtering out suspicious inputs) [94].
- **Data Poisoning**: By corrupting the training dataset, these attacks cause the model to misclassify threats, compromising security. Mitigation strategies include data sanitization (removing outliers) and robust learning techniques (e.g., using anomaly detection to filter malicious data) [95].
- **Model Inversion**: These attacks exploit model outputs to infer sensitive data, enabling more targeted attacks. Mitigation involves differential privacy (adding noise to outputs) and output obfuscation (limiting the information revealed by predictions) [96].

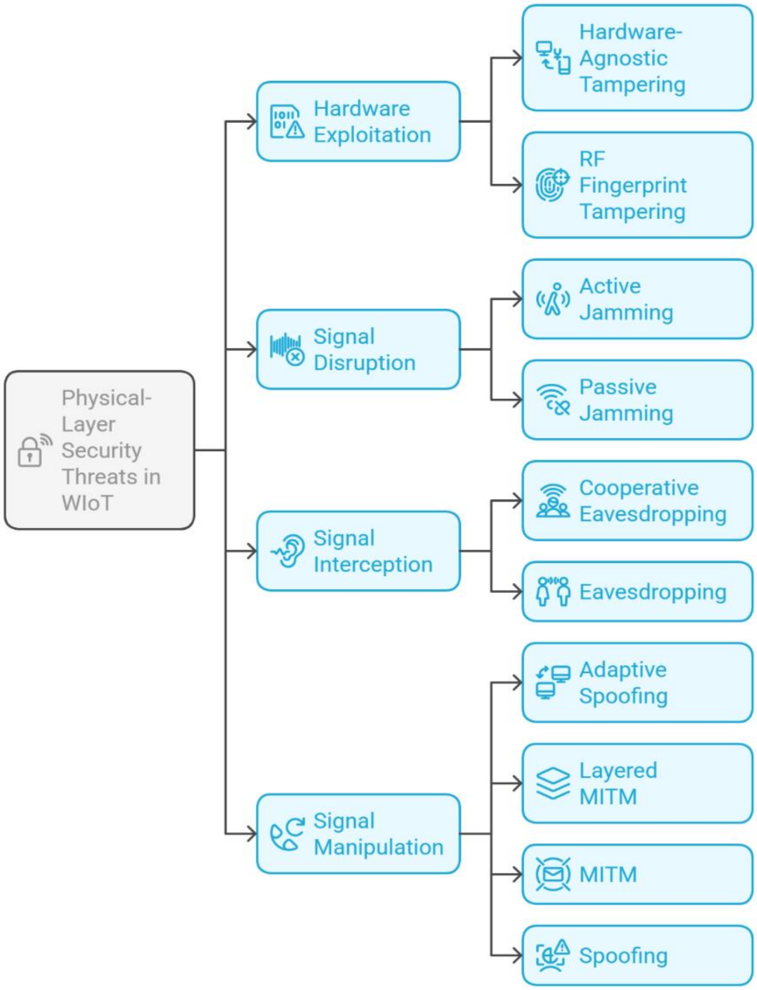
Implications for WIoT Security

Adversarial ML attacks highlight the need for robust DL models in WIoT security solutions, particularly for PLS applications. While DL enhances real-time threat detection (e.g., jamming, spoofing), its vulnerability to adversarial attacks can undermine its effectiveness, leading to undetected threats, data breaches, and privacy violations. Addressing these challenges requires integrating adversarial defenses into DL models, such as adversarial training and differential privacy, while ensuring these defenses remain lightweight to suit Wiot's resource constraints [97]. Future sections of this survey will explore experimental analyses of these attacks and defenses in WIoT contexts.

3. Taxonomy of Physical-Layer Security Threats in Wireless IoT

We divided the threats of the PLS based on the primary criterion of the attack vector into four categories: Hardware Exploitation, Signal Disruption, Signal Interception and Signal Manipulation. PLS is an easy target for attackers in WIoT environments because they are responsible for the basic processes of sending and receiving raw bit streams over a wireless medium. They are also the lowest layer in network architecture. The four main categories have been divided into subcategories to provide comprehensive coverage of most threats related to WIoT. This facilitates the identification of vulnerabilities and the implementation of mitigation measures.

Figure 14: Taxonomy of Physical-Layer Security Threats in WIoT



3.1 Hardware Exploitation

This type of threat includes actual physical IoT devices, affecting their functionality and security. This type of threat can be exploited through device design vulnerabilities or manufacturing defects, facilitating access to devices by bypassing authentication mechanisms and extracting sensitive information. This main category is divided into two subcategories:

- **Hardware - Agnostic Tampering**

  This type of threat refers to the general physical manipulation of device components, such as antennas or microcontrollers, which in turn impacts overall security and protection and increases the likelihood of a specific threat being successful. This results in reduced levels of protection and increased opportunities for making devices vulnerable to hacking and tampering. This is due to the ease of accessing the features of the physical layers used for authentication without any protection. This leads to the leakage and exposure of sensitive data, increasing the chances of exposure to other attacks[98].

- **RF Fingerprint Tampering:**

  This threat includes a distinct type of tampering using radio frequency fingerprints, which target IoT devices because these frequencies are considered distinctive signals resulting from hardware defects, such as carrier frequency offset (CFO) or I/Q imbalance. These distinctive characteristics are often used in the authentication process between devices at the physical layer. If these fingerprints are tampered with by modifying the components of the device simulating these frequencies, it is easy to subsequently gain access to the network, compromise connected devices, gain unauthorized access, and impersonate them. Or worse, disrupt authentication and security systems, posing a significant risk to the security of these wireless devices[99].

3.2 Signal Disruption

This type of attack represents a critical challenge and an important threat that can easily be done at any time, and targets many factors, especially the reliability and integrity of data transfer in the wireless Internet for atmosphere. These attacks benefit from weaknesses in wireless communication channels, especially broadcasting and sharing the nature of wireless media, which lacks physical boundaries and safety provided by wired networks. This improves the possibility of malicious actors, who disrupt or interfere with continuous communication, and provides significant security risks. These attacks weaken communication, cause loss of packages, increase the delay and cause complete denial of the service (DOS)[100]. Technically, these attacks reduce the signal-to-noise ratio (SNR) to insufficient levels to decode the signal, which makes the information out of understanding or completely preventing the reception. This type of attack is divided into two subcategories:

- **Active Jamming**

  This type transmits high -power RF signals of conscious hostile actors, aiming to control the valid communication channels used by devices. WIoT is considered one of the most dangerous attacks due to severity and direct intervention with continuous wave (CW) jamming or random noise injection. The effect lowers SNR, which helps to achieve the ability to obtain equipment to decode the upcoming signal correctly. In practice, Active Judgment has a negative effect on the smart home system, potentially interfering with surveillance cameras and interfering with video transmission in specified time, affecting safety and safety, leading to potentially serious consequences[101].

- **Passive Jamming**

  On the other hand, passive jamming is incorrectly referred to as indirect intervention in some studies. However, the existing environment and physical phenomena, such as electromagnetic intervention or inhibitory materials, signal quality and communication weakening of communication. It is more difficult to detect and reduce passive jamming attacks using traditional techniques. Physical elements, such as the introduction of reflective surfaces or transmission of objects, are manipulated and used to increase the possibility of weakness in the signal, eventually reduces the strength of the signal for both transmitters and recipients. A practical condition that requires rapid action and caution, when attackers in the industrial IoT environment utilize the reflections of heavy machinery or intense intervention from larger engines, which break the communication connection between built-in sensors and control units, causing incorrect computer recording and unpredictable behavior in the automation system. All this is completed without providing any detectable radio frequency signals[102].

3.3 Signal Interception

This type refers to sensitive information, such as user data, authentication credentials or operating parameters, refers to unauthorized capture or monitoring attacks of wireless signals to remove operating parameters. These attacks benefit from the underlying broadcast nature to wireless communication, where the signals spread through a common medium and can be cut off by opponents in the transmission area. In WIoT system, wireless media's open nature increases, combined with the resource environment of IoT units, the vulnerability of such attacks. Signal interception is an important threat to privacy [103], privacy and system integrity, especially important applications such as health care, smart networks and industrial automation. This category is divided into two subcategories:

- **Cooperative Eavesdropping**

  This threat occurs when many attackers prevent wireless signals, leading to their ability to capture and decode the transferred data. This form of the attack benefits from the coordinated efforts of many malicious nodes, which are often distributed in different places, such as the disappearance of the signal, treaty loss or low signal power to remove challenges. By collecting cut signals from several practical points, attackers can demonstrate advanced signal processing techniques such as beamforming or diversity combinations to rebuild the original data more efficiently than a single eavesdropper. The associated nature of this attack increases the success rate, making it a sophisticated and powerful threat in WIoT environment[104].

- **Eavesdropping**

  represents the fundamental and simplest form of signal interception, where a single attacker hears wireless signals without passively interfering with the communication process. Unlike cooperative eavesdropping, this attack does not include coordination between several nodes, making it less resource intensive for the attacker, but is less effective even in the challenging environment with poor signal quality. Due to the open nature of wireless media, there is a widespread threat in the WIoT system eavesdropping, poses a significant risk of applications where data privacy is important. For example, in a smart grid WIoT system, an attacker may consider communication between the smart meter and the tool supplier to collect power consumption data. This information can be used for financial espionage, such as selling patterns to participants, or for privacy violations, such as mentioning domestic occupancy patterns to plan criminal activities. Eavesdropping requires a basic receiver and minimal technical expertise-with its low identity, it provides a prevailing threat in the WIoT environment, where units often have a lack of calculation power to implement a strong encryption or infiltration identification system[105].

3.4 Signal Manipulation

This threat includes part of attacks, including conscious changes, forging or injections of the wireless signal with the intention of cheating the WIoT system or their users. These attacks benefit from weaknesses on the physical layer, such as misleading legitimate equipment or receiver to accept malicious data or command and often circumvent the significant authentication mechanisms for system protection. The open nature of wireless communication in the WIoT system, combined with the resource environment of IoT units, creates a particularly insidious danger. Such attacks can be based on the integrity, privacy and availability of the white network, which can have serious consequences in applications such as smart cities, health care and industrial automation[106]. This category is divided into four subcategories:

- **Adaptive Spoofing**

  involves an attacker, which dynamically adjusts its Spoofing strategy in real time depending on the system's reactions or changes in environmental conditions, such as the channel variation or change in network topology. Unlike static spoofing, which depends on a predetermined attack pattern, uses flexibility and responsibility to bypass adaptive spirits, making it a very sophisticated and difficult threat. In the context of the Internet of Vehicle (IoV), an attacker may dynamically replace legitimate indications of fake people who carefully mimic the communication pattern of a legitimate vehicle. This adaptation capacity is especially effective against anti- spoofing techniques such as frequency hopping or signal improvement -based defense. For example, an attacker may monitor the reactions from the target vehicle - for example, changes in signal dominance due to dynamics - and adjust the spoofing parameters such as signaling modulation or transmission frameworks to maintain the illusion of authenticity[107]. This can lead to serious security breaches, including injection of false navigation data, resulting in misunderstandings about vehicles, accidents or traffic disorders. (WIoT) system increases danger, where limited calculation and energy resources often prohibit the distribution of advanced spoofing detection and identification mechanisms.

- **Layered Man-in-the-Middle (MITM)**

  It represents a sophisticated development of traditional MITM attacks, where the attacker stops and manipulates signals in many layers of communication stack, starts on the physical layer and spreads to high layers such as network or application layers. This cross-layer manipulation not only allows the attacker to change the physical layer signals, but also affects the high-layer protocol, which creates a cascading effect that increases the effect of the attack. In the WIoT system, where devices often depend on layered architecture for communication, layered MITM attacks can have serious consequences, including unauthorized control of devices, data manipulation or resolution of significant operations[108].

  For example, in a smart grid WIoT system, an attacker can start a layered MITM attack by preventing physical layer signals between the smart meter and the tool supplier. Changing energy consumption data reported by manipulating these signals can then affect the invoicing protocol with high layer, which can trigger the electrical power outage by injecting incorrect invoicing or even false load balanced commands. This cross-layer effect level makes the MITM attacks dangerous in applications where operational continuity and data integrity are crucial, such as the industrial automation or energy management system.

- **MITM (Man-in-the-Middle)**

In a MITM basic attack on the physical layer, the attacker stays in position between the transmitter and the receiver, and changes cutting and potentially wireless signals. This allows the attacker to either recreate the party, manipulate the transferred data or inject false information into the communication stream. Unlike layered MITM, this attack focuses only on the physical layer, but the effect of the effect can still be elaborate as it reduces the integrity and authenticity of communication into the WIoT system. In a smart factory WIoT system, an attacker can perform the MITM attack by stopping the signals between a sensor and a control unit. By changing the sensor reading - for example, reporting the wrong temperature or pressure values - the attacker can cheat the control unit in making the wrong decisions, and possibly leading to malfunctions in the equipment, delays or even physical damage. For example, false pressure reading at a chemical processing system can trigger an overpressure event, the employee can put security at risk and cause significant financial losses. The simplicity of MITM attacks on the physical layer, combined with their high effects, creates a significant danger in the resource- constrained WIoT environment, where the equipment often lacks computational power to use strong infiltration systems[109].

- **Spoofing**
  Involves an attacker making wireless signals to use a valid device and cheat the receiver in accepting malicious data or command. The attack utilizes the trust relationship in the Wiot system, where equipment often depends on signaling properties (e.g. device identifier or authentication tokens), which establishes validity. Regarding signals that mimic a valid device, the attacker can obtain unauthorized access, may inject incorrect data or interfere with system operations. In the deployment of a WIoT smart city, an attacker can destroy a legitimate environmental sensor to transfer false data, such as exaggerated air pollution levels. It can trigger unnecessary public notifications, to address non-problems to reverse resources, or reduce confidence in the system. Alternatively, in an industrial WIoT system, a Spoofing sensor could report false operating data, leading to incorrect

decision-making from automated control systems. The effect of forgery extends beyond immediate data integrity issues, as it can destroy confidence in the WIoT system and create cascading effects in important applications[110].

Table 6: Summary of Physical-Layer Security Threats and ML/DL Mitigation Techniques in WIoT

Attack Vector	Threat	Exploitability Context	Impact	Attack Sophistication	ML/DL Mitigation Techniques
Signal Disruption	**Active Jamming**	**Broadcast Medium Exposure**	**Availability Disruption**	**Active**	- **Support Vector Machine (SVM)** (Basic, Industrial IoT)[111] - **Game Theoretic RL** (Advanced, Smart Grid)[112]
	Passive Jamming	**Dense Deployments**	**Availability Disruption**	**Passive**	- **Clustering** (Basic, Dense IoT Deployments)[113] - **Convolutional Neural Network (CNN)**[114] for Time-Frequency Analysis (Intermediate, Smart Cities)
Signal Interception	**Eavesdropping**	**Broadcast Medium Exposure**	**Confidentiality Breach**	**Passive**	- **One-Class Classification Support Vector Machine (OCC-SVM)**[115] (Intermediate, Smart Homes) - **Autoencoders** for Anomaly Detection (Intermediate, Healthcare IoT)[116]
	Cooperative Eavesdropping	**Massive Connectivity**	**Confidentiality Breach**	**Cooperative**	- **Multi-Agent RL** (Advanced, Smart Cities)[117] - **Recurrent Neural Network (RNN)**[118] with Attention (Advanced, Industrial IoT)

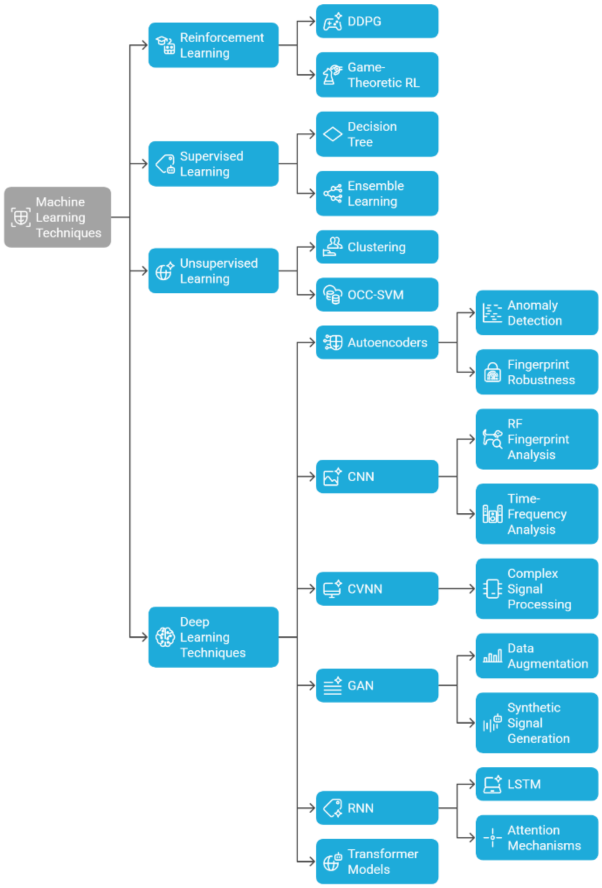
Signal Manipulation	**Spoofing**	**Heterogeneous Protocols**	**Integrity Violation**	**Active**	- **K-Nearest Neighbors (KNN)** (Basic, Smart Cities)[119] - **CNN** for RF Fingerprint Analysis (Intermediate, Industrial IoT)[120]
	Adaptive Spoofing	**Dynamic Network Topology**	**Integrity Violation**	**Cooperative**	- **Deep Deterministic Policy Gradient (DDPG)** (Transportation Systems)[121] -**Generative Adversarial Network (GAN)** for Synthetic Signal Generation (Advanced, Smart Cities)[122]
	MITM	**Dynamic Network Topology**	**Confidentiality + Integrity**	**Active**	- **Decision Tree** (Basic, Smart Grid)[123] - **LSTM** (Intermediate, Healthcare IoT)[124]
	Layered MITM	**Layered Architecture**	**Confidentiality + Integrity**	**Cooperative**	- **Multi-Agent Reinforcement Learning (RL)** with Game Theory (Advanced, Smart Cities)[125] - **Transformers** for Cross-Layer Analysis (Advanced, Industrial IoT)[126]
Hardware Exploitation	**RF Fingerprint Tampering**	**Heterogeneous Protocols**	**Integrity Violation**	**Active**	- **Ensemble Learning** (Intermediate, Industrial IoT)[127] - **CVNN** for Complex Signal Processing (Advanced, Smart Cities)[128]

	Hardware-Agnostic Tampering	**Device Diversity**	**Integrity Violation**	**Cooperative**	- **Autoencoders** for Fingerprint Robustness (Intermediate, Healthcare IoT)[129] - **Data Augmentation** with GANs (Advanced, Smart Cities)[130]

4. Taxonomy of Deep Learning Techniques for Physical-Layer Security

This taxonomy presents a classification of Machine Learning (ML) and Deep Learning (DL) techniques, which is performed in four primary categories based on the underlying learning pattern: Reinforcement Learning (RL), Supervised Learning (SL), Unsupervised Learning (UL) and Deep Learning (DL) techniques. RL includes methods such as Deep Deterministic Policy Gradient (DDPG) [131]and Game-Theoretic Reinforcement Learning (GTRL)[132], which are usually used on strategic and dynamic environments. SL involves the decision from the Decision Trees (DT) and Ensemble Learning (EL), both are widely used with data marked for classification and regression tasks[133]. UL includes clustering, One-Class Classification using Support Vector Machine (OCC-SVM), Autoencoders [134]Which used in anomaly detection for its robustness and strengthening of fingerprints, RF fingerprints and applies in time-series analysis, especially in landlords where the labeled data is rare. DL techniques have been further divided into the Convolutional Neural Networks (CNN)[135], Complex-Valued Neural Networks (CVNN)[136], Generative Adversarial Networks (GAN)[137], Recurrent Neural Networks (RNN) and Transformer Models[138]. These methods support a wide range of signal processing features, including complex signal processing, data agents, synthetic signal generation and sequential data modeling, which use Long Short-Term Memory (LSTM)[139] and attention mechanism. This hierarchical classification provides a structured understanding of their special applications in the vicious classification machine learning methods and wireless signal processing and their special applications in the respective domains.

Figure16: Taxonomy of Machine Learning and Deep Learning



4.1 Machine Learning Techniques

These techniques include a wide set of traditional algorithms, including RL, SL and UL, designed to detect and reduce safety hazards for physical layers in the WIoT system, such as active jamming, spoofing, and eavesdropping exploring open nature of wireless communication[140]. These techniques benefit from statistical and potential methods to analyze signal properties such as SNR, received signal strength indication (RSSI) or RF-fingerprint, which can identify malicious activities through classification, cluster or adaptable decision-making[141]. In the WIoT system, where devices are often resources with limited calculation power and energy, ML techniques provide a balance between accuracy and efficiency detection, making them suitable for applications such as smart networks, industrial IoTs and smart cities[142]. They consist of four main parts:

- **Supervised Learning (SL):**

  SL is a machine learning paradigm that depends on the dataset labeled to train the model for classification or prediction, making WIoT especially effective in detecting malicious signals in the atmosphere. These models learn from input features such as SNR, RSSI or RF fingerprint to identify patterns associated with different types of attacks. SL techniques are preferred by their interpretation and relatively low calculation complexity in the resources of WIoT system. Generally monitored learning methods and their WIoT security applications include:

  - **Support Vector Machine (SVM):**
    A basic but powerful classifies that distinguishes classes by finding an optimal hyperplane with a maximum margin. In WIoT, it is effective to detect active jamming attacks by analyzing functions such as SNR and Power Spectral Density (PSD)[143].
  - **K-Nearest Neighbor (KNN):**
    A basic, non-parametric algorithm that classifies indications based on the majority label between their K-nearest neighbor in the feature space. In WIoT, RSSI and I/Q help to detect spoofing attacks by comparing signal functions such as I/Q -Imbalance[144].
  - **Decision Tree (DT):**
    A basic model that determines through repetition function forms a lecturer tree structure. DTS is used to identify nonconformity deviations to detect the attacks in the smart network by analyzing features such as Channel State Information (CSI) or RSSI[145].
  - **Ensemble Learning (EL):**
    An intermediate level approach that integrates several base students, such as decisions in random forests to improve trees, classification accuracy and strength. In the WIoT system, the clothing models are particularly useful for identifying RF fingerprints - tampering by analyzing phase noise or I/Q - Imbalance[146].

- **Unsupervised Learning (UL):**

  UL refers to training models on non-labeled data to highlight hidden patterns, groups or deviations, making it well suited for security applications in WIoT system, where the marked attack data is insufficient. The UL technique is especially useful for detecting subtle or passive dangers such as analyzing the deviation in the signal behavior by analyzing jamming and eavesdropping. The two most important UL techniques used in WIoT environment are as follows:

  - **Clustering (e.g., Density-Based Clustering such as DBSCAN):**
    Clustering algorithm groups are based on the similarity of data point based on the underlying pattern without relying on the label input. In WIoT, density -based grouping can be used to detect passive jamming by identifying unusual signaling behavior, such as multipath interference through RSS[147].

    - **One-Class Support Vector Machine (OCC-SVM):**
      OCC-SSVM is an algorithm to detect a deviation that models the general behavior of valid indications (e.g., using CSI) and identifies outers as potential dangers. In the Wiot environment, the OCC-SVM signal is particularly effective in detecting eavesdropping by identifying unauthorized deviations in the signals[148].

- **Reinforcement Learning (RL):**

  is a learning paradigm in which an agent interacts with an environment and learns optimal behavior by receiving reactions in the form of allocation or punishment. In WIoT system, RL technology rapidly increases as jamming, evolution, spoofing and MITM attack dynamically reacts to dynamic dangers. These techniques allow the system to develop and refine the safety strategies in real time. WIoT domains include remarkable RL approaches:

    - **Game-Theoretic Reinforcement Learning (e.g., Q-Learning, Deep Q-Networks – DQN):**
      This technique models the interaction between the attacker and the defender as a strategic game, which enables dynamic adaptation to the dangers. For example, on a smart grid, DQN can reduce active jamming by learning optimal channel change policy[149].
    - **Multi-Agent Reinforcement Learning (Multi-Agent RL):**
      There are many agents who learn to cooperate or compete in a shared environment. In smart cities, this method can detect cooperation revolution on traffic sensors by coordinating the defense mechanism of units[150].
    - **Deep Deterministic Policy Gradient (DDPG):**
      An RL algorithm for policy gradient can carry out continuous action spaces by integrating deep learning. In intelligent transportation systems, the DDPG signal verification can detect adaptive spread in vehicle-to-vehicle (V2V) communication by continuously adapting the threshold[151].
    - **Multi-Agent RL with Game Theory:**

      The strength of multi-agent systems and game theory increases the layered attacker-defender model. This approach is suitable for detecting the MITM attacks that are leveled in smart cities of security mechanisms across layers such as physical layer authentication and secure routing[152].

4.2 Taxonomy of Deep Learning Techniques for Physical-Layer Security

DL Techniques Provide powerful tools to increase PLS in WIoT system by activating complex signal analysis and anomaly detection. Despite their high calculation requirements compared to traditional machine learning (ML) methods, DL models provide better performance in tasks associated with structured or sequential data, RF fingerprints and signal behavior patterns. Many DL approaches are used to reduce various wireless security threats:

- **Convolutional Neural Network (CNN)**
  - **CNN for time-series analysis:** This approach uses CNN to explain the spectrogram of signal data, which can detect passive jamming by identifying unusual intervention patterns due to environmental factors such as multi-way factors. It is especially useful in smart cities where the reliability of the traffic sensor is important[153].
  - **CNN for RF fingerprint analysis:** CNN can distinguish between authentic and Spoofed RF signals by analyzing the properties of unique physical lags such as transient amplitude and phase noise. This technique increases the approval of devices in the industrial IoT environment by preventing unauthorized access[154].
- **Recurrent Neural Networks (RNN)**
  - **RNN Attention:** By integrating the attention mechanism, RNN can be selectively focused on suspected temporary characteristics of CSI or RSSI data, identifying effective collaboration development of several attackers in the industrial IoT Sensor network[155].
  - **Long short -term memory (LSTM):** LSTM networks analyze long term dependency in signal sequences, such as Channel Impulse Response (CIR), to detect MITM attacks that change communication streams. It is important in the health system's IoT system to obtain data integrity[156].
- **Generative Adversarial Networks (GAN)**
  - **GAN for synthetic signal generation:** Gans produces artificial characters to train discriminatory but artificial signs for adaptive spoofing detection. In smart cities, this technology improves the flexibility of traffic management systems by simulating the spoofing scenarios for training[157].
  - **Data Augmentation with GANs**: GAN increases the identity model by producing synthetic RF fingerprints that simulate hardware designer tampering. It supports the safety of different IoT devices in the smart city environment[158].
- **Autoencoders (AE)**
  - **Autoencoders for Anomaly Detection:** These models compress and reconstruct valid signal structures, detect the evolution by measuring the

reconstruction error. They are effective in the IoT health care system, where undivided equipment transmits sensitive patient data[159].

    - **Autoencoders for Fingerprint Robustness:** This technique provides learning from RF fingerprint representation to identify deviations due to hardware-agnostic, especially useful in medical equipment approval in the health care system[160].
- **Transformer Models**
    - **Transformers for Cross-Layer Analysis:** Use self-attention mechanisms, transformers correlate features in different layers (e.g. physical layer CSI and network layer routing) and effectively identify layered MITM attacks. This is essential in industrial IoT, where layered architecture is widespread[161].
- **Complex-valuable nerve networks (CVNN):**
    - **CVNN for Complex Signal Processing**: CVNNs to detect complex valid data such as I/Q-signal RF fingerprint-tampering, to increase the safety of the smart city access control system. Their ability to work in complex domain makes them ideal for verification of signal integrity[162].

Table 7: Taxonomy of ML and DL Techniques for Physical-Layer Security in WIoT

Class	Technique	Description	Sophistication	Applicability Context	Threat Mitigated
Machine Learning	SVM	Classify signals via hyperplane	Basic	Industrial IoT	Active Jamming
	KNN	Neighbor-based classification	Basic	Smart Cities	Spoofing
	Game-Theoretic RL	Adapts to jamming via Q-Learning	Advanced	Smart Grid	Active Jamming
Deep Learning	CNN (Time-Freq.)	Analyzes spectrograms for jamming	Intermediate	Smart Cities	Passive Jamming
	GAN (Synthetic)	Generates signals for spoofing detect	Advanced	Smart Cities	Adaptive Spoofing
	Transformers	Cross-layer analysis for MITM	Advanced	Industrial IoT	Layered MITM

5. Review of Datasets for Physical-Layer Security

The rapid expansion of WIoT equipment has increased the need for strong PLS mechanisms. ML gears a comprehensive study of based PLS, which offers a classification of fingers, a compilation of the open-source dataset and the compilation of future research directions. This segment undergoes the dataset listed analyzes their availability through an Exploratory Data Analysis (EDA), evaluates the PLS and provides data selection recommendations to support our research on deep learning for PLS in WIoT. Increasing of IoT devices and security research are urgent to solve safety challenges in the WIoT. Figure 17 refers to the growth of IoT devices and the increase in research related to security from 2020 to 2025[163]. The number of IoT devices is estimated to be increased from approximately 10 to 30 billion in 2020, while the percentage of safety-related papers increases from 12.3% to 31.5% in the same period[164]. This trend emphasizes the increasing academic focus on security when IoT adoption and justifies the relevance of our research for WIoT in DL-based PLA.

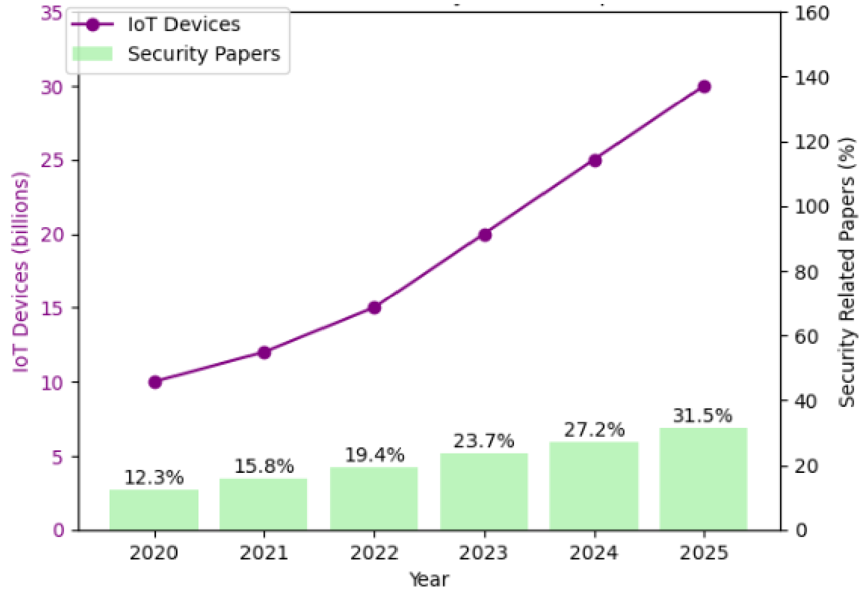


Figure17: Growth of IoT Devices and Security-Related Papers (2020-2025)

We have collected a list of 22 Open-Source datasets for RF and channel fingerprints, which is necessary for the development and testing of DL-based PLS plans. These datasets are classified in RF fingerprints (12 datasets) and channel fingerprints (10 datasets). Table 1 provides a detailed observation of these datasets, including their category, reference, details, source/provider and availability status.

- **Exploratory Data Analysis (EDA) of Dataset Metadata**

To understand the availability and distribution of these datasets, we conducted an EDA on their metadata using Python. The following code was used to perform the analysis and generate visualizations:

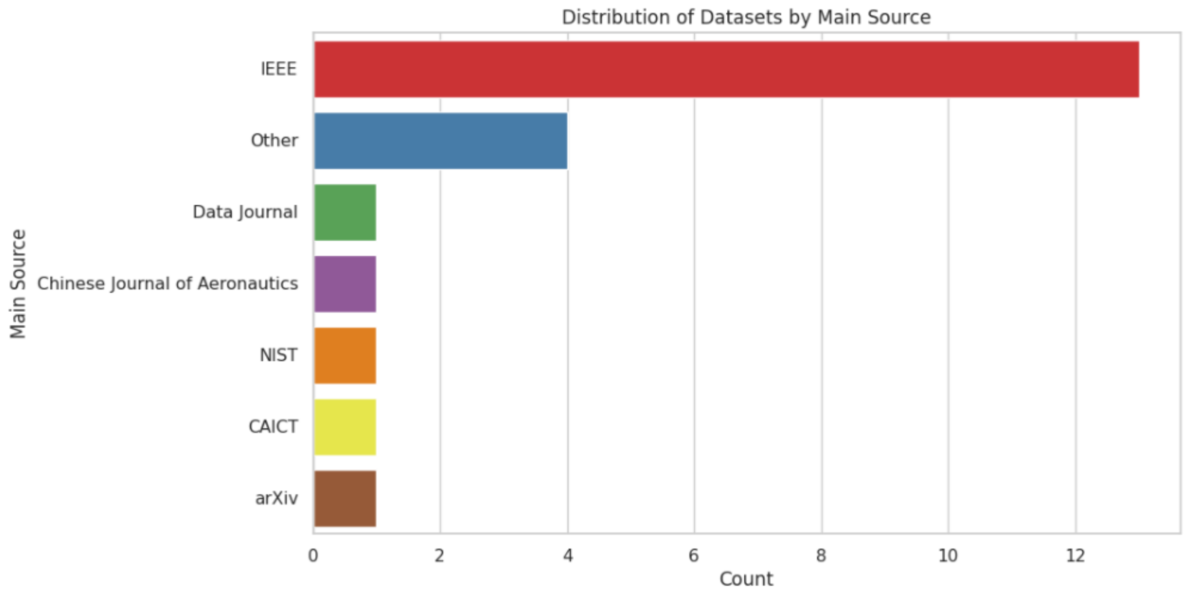


Figure18: Distribution of Datasets by Main Source

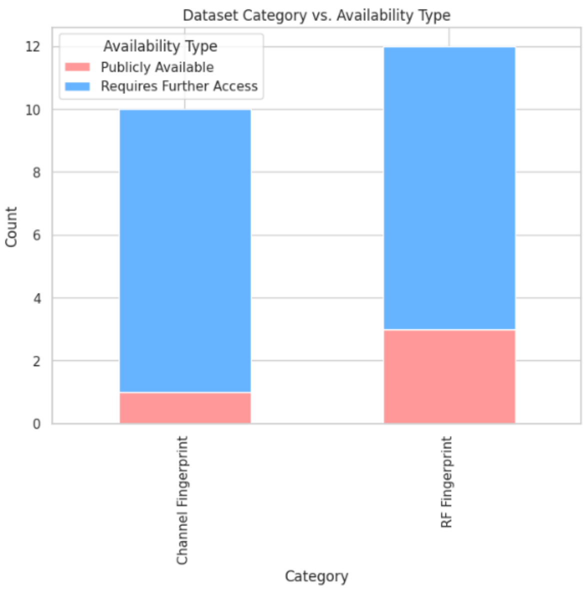


Figure19: Distribution of Datasets by Main Source

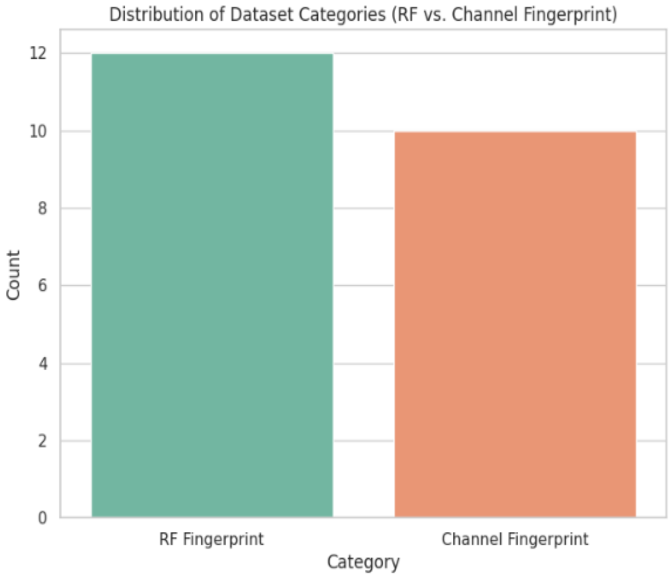


Figure20: Dataset Categories (RF vs. Channel Fingerprint)

Table 8: Availability of the datasets

Category	Reference	Name/Description	Availability Type	Recommended Use
RF Fingerprint		RF fingerprints from 16 USRP X310 devices	Requires Further Access	Contact authors for potential use in RF fingerprinting studies.
		I/Q datasets from 20 USRP X310/N210 devices		
		ADS-B signals from 140 aircraft		
		Signals from 60 commercial LoRa devices		
		Signals from 4 USRP X310 devices (IEEE 802.11a/LTE/5G NR)		
		Bluetooth signals from 86 smartphones	Publicly Available	Use for Bluetooth-based RF fingerprinting studies (DOI: 10.3390/data5020055).
		ADS-B signals from 728 aircraft	Requires Further Access	Contact authors for potential use in large-scale aviation security studies.
		WiFi signals from 174 devices	Publicly Available	Recommended for immediate use in RF fingerprinting for WIOT (URL: https://cores.ee.ucla.edu/downloads/datasets/wisig/).
		LoRa signals from 25 Pycom devices	Requires Further Access	Contact authors for potential use in LoRa-based WIOT security studies.
		Signals from 21 USRP N2932 devices (IEEE 802.15.4)	Requires Further Access	Contact authors for potential use in LoRa-based WIOT security studies.
		Signals from 17 drone remote controllers	Publicly Available	Recommended for immediate use in drone communication security studies (DOI: 10.21227/ss99-8d56).
		Signals from 7 DJI M100 drones	Requires Further Access	Contact authors for potential use in drone communication security studies.
Channel Fingerprint		CIR measurements from industrial scenarios	Requires Further Access	Contact authors for potential use in drone communication security studies.
		Dataset from real-world scenes of 40 big cities	Publicly Available	Recommended for immediate use in channel fingerprinting for urban WIOT (URL: https://www.mobileai-dataset.com).

		Extended WINNER channel model for 4G LTE	Requires Further Access	Contact authors for potential use in drone communication security studies.
		COST 2100 channel model for MIMO	Requires Further Access	
		DeepMIMO dataset for Massive MIMO and mmWave		
		CSI data from complex indoor environments		
		Generalized 5G NR dataset generator		
		SimRIS Channel Simulator for RIS-aided systems		
		ViWi dataset framework for vision-aided wireless		
		Underwater acoustic channel model		

References

[1] S. Kumar, P. Tiwari, and M. Zymbler, “Internet of Things is a revolutionary approach for future technology enhancement: a review,” *J Big Data*, vol. 6, no. 1, p. 111, Dec. 2019, doi: 10.1186/s40537-019-0268-2.

[2] R. Singh, A. Gehlot, S. Vaseem Akram, A. Kumar Thakur, D. Buddhi, and P. Kumar Das, “Forest 4.0: Digitalization of forest using the Internet of Things (IoT),” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 8, pp. 5587–5601, Sep. 2022, doi: 10.1016/j.jksuci.2021.02.009.

[3] K. St. Germain and F. Kragh, “Physical-Layer Authentication Using Channel State Information and Machine Learning,” in *2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS)*, IEEE, Dec. 2020, pp. 1–8. doi: 10.1109/ICSPCS50536.2020.9310070.

[4] J. D. Vega Sanchez, L. Urquiza-Aguiar, and M. C. Paredes Paredes, “Physical Layer Security for 5G Wireless Networks: A Comprehensive Survey,” in *2019 3rd Cyber Security in Networking Conference (CSNet)*, IEEE, Oct. 2019, pp. 122–129. doi: 10.1109/CSNet47905.2019.9108955.

[5] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, “Internet of Things Security: Challenges and Key Issues,” *Security and Communication Networks*, vol. 2021, pp. 1–11, Sep. 2021, doi: 10.1155/2021/5533843.

[6] N. Zhang, D. Chen, F. Ye, T.-X. Zheng, and Z. Wei, “Physical Layer Security for Internet of Things,” *Wirel Commun Mob Comput*, vol. 2019, pp. 1–2, Apr. 2019, doi: 10.1155/2019/2627938.

[7] H. Sharma and N. Kumar, “Deep learning based physical layer security for terrestrial communications in 5G and beyond networks: A survey,” *Physical Communication*, vol. 57, p. 102002, Apr. 2023, doi: 10.1016/j.phycom.2023.102002.

[8] F. Restuccia and T. Melodia, “Deep Learning at the Physical Layer: System Challenges and Applications to 5G and Beyond,” *IEEE Communications Magazine*, vol. 58, no. 10, pp. 58–64, Oct. 2020, doi: 10.1109/MCOM.001.2000243.

[9] T. Liu, G. Ramachandran, and R. Jurdak, “Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization,” Jan. 2024.

[10] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, “A lightweight authentication protocol for Internet of Things,” in *2014 International Symposium on Next-Generation Electronics (ISNE)*, IEEE, May 2014, pp. 1–2. doi: 10.1109/ISNE.2014.6839375.

[11] F. Pereira, R. Correia, P. Pinho, S. I. Lopes, and N. B. Carvalho, “Challenges in Resource-Constrained IoT Devices: Energy and Communication as Critical Success Factors for Future IoT Deployment,” *Sensors*, vol. 20, no. 22, p. 6420, Nov. 2020, doi: 10.3390/s20226420.

[12] A. B. Guiloufi, S. El khediri, N. Nasri, and A. Kachouri, “A comparative study of energy efficient algorithms for IoT applications based on WSNs,” *Multimed Tools Appl*, vol. 82, no. 27, pp. 42239–42275, Nov. 2023, doi: 10.1007/s11042-023-14813-3.

[13] A. Soni, R. Upadhyay, and A. Jain, “Internet of Things and Wireless Physical Layer Security: A Survey,” 2017, pp. 115–123. doi: 10.1007/978-981-10-3226-4_11.

[14] H. Jafari, O. Omotere, D. Adesina, H.-H. Wu, and L. Qian, “IoT Devices Fingerprinting Using Deep Learning,” in *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, IEEE, Oct. 2018, pp. 1–9. doi: 10.1109/MILCOM.2018.8599826.

[15] S. Khan, C. Thapa, S. Durrani, and S. Camtepe, “Access-Based Lightweight Physical-Layer Authentication for the Internet of Things Devices,” *IEEE Internet Things J*, vol. 11, no. 7, pp. 11312–11326, Apr. 2024, doi: 10.1109/JIOT.2023.3331362.

[16] R. Mustafa, N. I. Sarkar, M. Mohaghegh, and S. Pervez, “A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey,” *Sensors*, vol. 24, no. 22, p. 7209, Nov. 2024, doi: 10.3390/s24227209.

[17] C. Lv and Z. Luo, “Deep Learning for Channel Estimation in Physical Layer Wireless Communications: Fundamental, Methods, and Challenges,” *Electronics (Basel)*, vol. 12, no. 24, p. 4965, Dec. 2023, doi: 10.3390/electronics12244965.

[18] Y. Li, Y. Wang, X. Liu, P. Zuo, H. Li, and H. Jiang, “Deep-Reinforcement-Learning-Based Wireless IoT Device Identification Using Channel State Information,” *Symmetry (Basel)*, vol. 15, no. 7, p. 1404, Jul. 2023, doi: 10.3390/sym15071404.

[19] J. Bassey, X. Li, and L. Qian, “Device Authentication Codes based on RF Fingerprinting using Deep Learning,” *ICST Transactions on Security and Safety*, vol. 8, no. 29, p. 172305, Nov. 2021, doi: 10.4108/eai.30-11-2021.172305.

[20] O. T. Ajayi, S. O. Onidare, and H. Tajudeen, “A Study on Adversarial Machine Learning in Wireless Communication Systems,” 2024, pp. 384–392. doi: 10.1007/978-981-97-6937-7_46.

[21] N. Xie, J. Zhang, and Q. Zhang, “Security Provided by the Physical Layer in Wireless Communications,” *IEEE Netw*, vol. 37, no. 5, pp. 42–48, Sep. 2023, doi: 10.1109/MNET.121.2200110.

[22] P. Angueira *et al.*, “A Survey of Physical Layer Techniques for Secure Wireless Communications in Industry,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 810–838, Dec. 2022, doi: 10.1109/COMST.2022.3148857.

[23] A. Jagannath, J. Jagannath, and P. S. P. V. Kumar, “A Comprehensive Survey on Radio Frequency (RF) Fingerprinting: Traditional Approaches, Deep Learning, and Open Challenges,” Jan. 11, 2022. doi: 10.36227/techrxiv.17711444.v2.

[24] W. Lee, S. Y. Baek, and S. H. Kim, “Deep-Learning-Aided RF Fingerprinting for NFC Security,” *IEEE Communications Magazine*, vol. 59, no. 5, pp. 96–101, May 2021, doi: 10.1109/MCOM.001.2000912.

[25] Y. Liu, J. Wang, J. Li, S. Niu, and H. Song, “Machine Learning for the Detection and Identification of Internet of Things Devices: A Survey,” *IEEE Internet Things J*, vol. 9, no. 1, pp. 298–320, Jan. 2022, doi: 10.1109/JIOT.2021.3099028.

[26] N. Soltani, K. Sankhe, J. Dy, S. Ioannidis, and K. Chowdhury, “More Is Better: Data Augmentation for Channel-Resilient RF Fingerprinting,” *IEEE Communications Magazine*, vol. 58, no. 10, pp. 66–72, Oct. 2020, doi: 10.1109/MCOM.001.2000180.

[27] N. Xie, Z. Li, and H. Tan, “A Survey of Physical-Layer Authentication in Wireless Communications,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, Dec. 2021, doi: 10.1109/COMST.2020.3042188.

[28] Y. Liu, X. Wang, and J. Mei, “Hybrid Multiple Access and Service-Oriented Resource Allocation for Heterogeneous QoS Provisioning in Machine Type Communications,” *Journal of Communications and Information Networks*, vol. 5, no. 2, pp. 225–236, Jun. 2020, doi: 10.23919/JCIN.2020.9130438.

[29] X. Fan, F. Wang, F. Wang, W. Gong, and J. Liu, “When RFID Meets Deep Learning: Exploring Cognitive Intelligence for Activity Identification,” *IEEE Wirel Commun*, vol. 26, no. 3, pp. 19–25, Jun. 2019, doi: 10.1109/MWC.2019.1800405.

[30] H. Fang, X. Wang, and S. Tomasin, “Machine Learning for Intelligent Authentication in 5G and Beyond Wireless Networks,” *IEEE Wirel Commun*, vol. 26, no. 5, pp. 55–61, Oct. 2019, doi: 10.1109/MWC.001.1900054.

[31] M. Padhiary, P. Roy, and D. Roy, “The Future of Urban Connectivity,” 2024, pp. 33–66. doi: 10.4018/979-8-3693-6740-7.ch002.

[32] M. Wollschlaeger, T. Sauter, and J. Jasperneite, “The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0,” *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17–27, Mar. 2017, doi: 10.1109/MIE.2017.2649104.

[33] R. Priyadarshani, K.-H. Park, Y. Ata, and M.-S. Alouini, “Jamming Intrusions in Extreme Bandwidth Communication: A Comprehensive Overview,” Mar. 2024.

[34] M. Krishna Pasupuleti, “Autonomous Drone Swarms in Action: AI for Mission Coordination and Adaptive Navigation,” in *AI in Autonomous Drone Swarms: Coordinating Complex Missions*, National Education Services, 2024, pp. 76–95. doi: 10.62311/nesx/66227.

[35] B. M. ElHalawany, A. A. A. El-Banna, and K. Wu, “Physical-Layer Security and Privacy for Vehicle-to-Everything,” *IEEE Communications Magazine*, vol. 57, no. 10, pp. 84–90, Oct. 2019, doi: 10.1109/MCOM.001.1900141.

[36] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, “Convergence of MANET and WSN in IoT Urban Scenarios,” *IEEE Sens J*, vol. 13, no. 10, pp. 3558–3567, Oct. 2013, doi: 10.1109/JSEN.2013.2272099.

[37] J. Shehu Yalli, M. Hilmi Hasan, and A. Abubakar Badawi, “Internet of Things (IoT): Origins, Embedded Technologies, Smart Applications, and Its Growth in the Last Decade,” *IEEE Access*, vol. 12, pp. 91357–91382, 2024, doi: 10.1109/ACCESS.2024.3418995.

[38] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, Apr. 2015, doi: 10.1007/s10796-014-9492-7.

[39] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, Dec. 2015, doi: 10.1109/COMST.2015.2444095.

[40] M. S. Farooq *et al.*, “A Survey on the Role of Industrial IoT in Manufacturing for Implementation of Smart Industry,” *Sensors*, vol. 23, no. 21, p. 8958, Nov. 2023, doi: 10.3390/s23218958.

[41] Md. N. Mowla, N. Mowla, A. F. M. S. Shah, K. M. Rabie, and T. Shongwe, “Internet of Things and Wireless Sensor Networks for Smart Agriculture Applications: A Survey,” *IEEE Access*, vol. 11, pp. 145813–145852, 2023, doi: 10.1109/ACCESS.2023.3346299.

[42] M. K. Banafaa *et al.*, “A Comprehensive Survey on 5G-and-Beyond Networks With UAVs: Applications, Emerging Technologies, Regulatory Aspects, Research Trends and Challenges,” *IEEE Access*, vol. 12, pp. 7786–7826, 2024, doi: 10.1109/ACCESS.2023.3349208.

[43] A. Diane, O. Diallo, and E. H. M. Ndoye, “A systematic and comprehensive review on low power wide area network: characteristics, architecture, applications and research challenges,” *Discover Internet of Things*, vol. 5, no. 1, p. 7, Jan. 2025, doi: 10.1007/s43926-025-00097-6.

[44] X. Kong, Y. Wu, H. Wang, and F. Xia, “Edge Computing for Internet of Everything: A Survey,” *IEEE Internet Things J*, vol. 9, no. 23, pp. 23472–23485, Dec. 2022, doi: 10.1109/JIOT.2022.3200431.

[45] O. Zaporozhets, V. Isaienko, and K. Synylo, “Trends on current and forecasted aircraft hybrid electric architectures and their impact on environment,” *Energy*, vol. 211, p. 118814, Nov. 2020, doi: 10.1016/j.energy.2020.118814.

[46] K. Aarika, M. Bouhlal, R. A. Abdelouahid, S. Elfilali, and E. Benlahmar, “Perception layer security in the internet of things,” *Procedia Comput Sci*, vol. 175, pp. 591–596, 2020, doi: 10.1016/j.procs.2020.07.085.

[47] X. Zhang, G. Li, J. Zhang, A. Hu, Z. Hou, and B. Xiao, “Deep-Learning-Based Physical-Layer Secret Key Generation for FDD Systems,” *IEEE Internet Things J*, vol. 9, no. 8, pp. 6081–6094, Apr. 2022, doi: 10.1109/JIOT.2021.3109272.

[48] M. Thankappan, H. Rifà-Pous, and C. Garrigues, “Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review,” *Expert Syst Appl*, vol. 210, p. 118401, Dec. 2022, doi: 10.1016/j.eswa.2022.118401.

[49] R. Saini, D. Halder, and A. M. Baswade, “RIDS: Real-time Intrusion Detection System for WPA3 enabled Enterprise Networks,” in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, IEEE, Dec. 2022, pp. 43–48. doi: 10.1109/GLOBECOM48099.2022.10001501.

[50] M. Harvanek, J. Bolcek, J. Kufa, L. Polak, M. Simka, and R. Marsalek, “Survey on 5G Physical Layer Security Threats and Countermeasures,” *Sensors*, vol. 24, no. 17, p. 5523, Aug. 2024, doi: 10.3390/s24175523.

[51] M. M. Saeed *et al.*, “A comprehensive survey on 6G-security: physical connection and service layers,” *Discover Internet of Things*, vol. 5, no. 1, p. 28, Mar. 2025, doi: 10.1007/s43926-025-00123-7.

[52] K. Ramezanpour, J. Jagannath, and A. Jagannath, “Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective,” *Computer Networks*, vol. 221, p. 109515, Feb. 2023, doi: 10.1016/j.comnet.2022.109515.

[53] G. Leenders, G. Callebaut, G. Ottoy, L. Van der Perre, and L. De Strycker, “Multi-RAT for IoT: The Potential in Combining LoRaWAN and NB-IoT,” *IEEE Communications Magazine*, vol. 59, no. 12, pp. 98–104, Dec. 2021, doi: 10.1109/MCOM.008.2100382.

[54] D. Wang, A. Traspadini, M. Giordani, M.-S. Alouini, and M. Zorzi, “On the Performance of Non-Terrestrial Networks to Support the Internet of Things,” in *2022 56th Asilomar Conference on Signals, Systems, and Computers*, IEEE, Oct. 2022, pp. 881–887. doi: 10.1109/IEEECONF56349.2022.10052102.

[55] A. Malik, V. Parihar, B. Bhushan, R. Chaganti, S. Bhatia, and P. N. Astya, “Security Services for Wireless 5G Internet of Things (IoT) Systems,” 2023, pp. 169–195. doi: 10.1007/978-981-99-3668-7_9.

[56] A. T. Jawad, R. Maaloul, and L. Chaari, “A comprehensive survey on 6G and beyond: Enabling technologies, opportunities of machine learning and challenges,” *Computer Networks*, vol. 237, p. 110085, Dec. 2023, doi: 10.1016/j.comnet.2023.110085.

[57] A. Mosteiro-Sanchez, M. Barcelo, J. Astorga, and A. Urbieta, “Securing IIoT using Defence-in-Depth: Towards an End-to-End secure Industry 4.0,” *J Manuf Syst*, vol. 57, pp. 367–378, Oct. 2020, doi: 10.1016/j.jmsy.2020.10.011.

[58] Amrita, C. P. Ekwueme, I. H. Adam, and A. Dwivedi, “Lightweight Cryptography for Internet of Things: A Review,” *EAI Endorsed Transactions on Internet of Things*, vol. 10, Mar. 2024, doi: 10.4108/eetiot.5565.

[59] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, “Safeguarding 5G wireless communication networks using physical layer security,” *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, Apr. 2015, doi: 10.1109/MCOM.2015.7081071.

[60] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, “A survey on jamming attacks and countermeasures in WSNs,” *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009, doi: 10.1109/SURV.2009.090404.

[61] X. Liu, X. Meng, H. Duan, Z. Hu, and M. Wang, “A Survey on Secure WiFi Sensing Technology: Attacks and Defenses,” *Sensors*, vol. 25, no. 6, p. 1913, Mar. 2025, doi: 10.3390/s25061913.

[62] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, “Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks,” *IEEE Trans Veh Technol*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010, doi: 10.1109/TVT.2010.2044904.

[63] M. Conti, N. Dragoni, and V. Lesyk, “A Survey of Man In The Middle Attacks,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, Dec. 2016, doi: 10.1109/COMST.2016.2548426.

[64] J.-D. Kim, M. Ko, and J.-M. Chung, “Physical Identification Based Trust Path Routing Against Sybil Attacks on RPL in IoT Networks,” *IEEE Wireless Communications Letters*, vol. 11, no. 5, pp. 1102–1106, May 2022, doi: 10.1109/LWC.2022.3157831.

[65] H. S. Sanchez, D. Rotondo, M. L. Vidal, and J. Quevedo, “Frequency-based detection of replay attacks: application to a quadrotor UAV,” in *2019 8th International Conference on Systems and Control (ICSC)*, IEEE, Oct. 2019, pp. 289–294. doi: 10.1109/ICSC47195.2019.8950619.

[66] R. Melki, H. N. Noura, A. Chehab, and R. Couturier, “Machine Learning for Physical Layer Security: Limitations, Challenges and Recommendation,” in *2022 16th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, IEEE, Oct. 2022, pp. 53–60. doi: 10.1109/SITIS57111.2022.00017.

[67] M. Raeisi-Varzaneh, O. Dakkak, H. Alaidaros, and İ. Avci, “Internet of Things: Security, Issues, Threats, and Assessment of Different Cryptographic Technologies,” *Journal of Communications*, pp. 78–89, Feb. 2024, doi: 10.12720/jcm.19.2.78-89.

[68] A. Hassan, “Lightweight Cryptography for the Internet of Things,” 2021, pp. 780–795. doi: 10.1007/978-3-030-63092-8_52.

[69] L. Sun and X. Tian, “Physical Layer Security in Multi-Antenna Cellular Systems: Joint Optimization of Feedback Rate and Power Allocation,” *IEEE Trans Wirel Commun*, vol. 21, no. 9, pp. 7165–7180, Sep. 2022, doi: 10.1109/TWC.2022.3155775.

[70] A. Jagannath, J. Jagannath, and P. S. P. V. Kumar, “A Comprehensive Survey on Radio Frequency (RF) Fingerprinting: Traditional Approaches, Deep Learning, and Open Challenges,” Aug. 11, 2022. doi: 10.36227/techrxiv.17711444.v3.

[71] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, “Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities,” *Entropy*, vol. 21, no. 5, p. 497, May 2019, doi: 10.3390/e21050497.

[72] M. Nawaz and M. I. K. Babar, “IoT and AI for smart agriculture in resource-constrained environments: challenges, opportunities and solutions,” *Discover Internet of Things*, vol. 5, no. 1, p. 24, Mar. 2025, doi: 10.1007/s43926-025-00119-3.

[73] M. Li and Z. Dou, “Active eavesdropping detection: a novel physical layer security in wireless IoT,” *EURASIP J Adv Signal Process*, vol. 2023, no. 1, p. 119, Nov. 2023, doi: 10.1186/s13634-023-01080-5.

[74] W. Wu, S. Hu, D. Lin, and G. Wu, “Reliable resource allocation with RF fingerprinting authentication in secure IoT networks,” *Science China Information Sciences*, vol. 65, no. 7, p. 170304, Jul. 2022, doi: 10.1007/s11432-021-3284-y.

[75] M. Shakiba-Herfeh, A. Chorti, and H. V. Poor, “Physical Layer Security: Authentication, Integrity and Confidentiality,” Jan. 2020.

[76] J. Boodai, A. Alqahtani, and M. Frikha, “Review of Physical Layer Security in 5G Wireless Networks,” *Applied Sciences*, vol. 13, no. 12, p. 7277, Jun. 2023, doi: 10.3390/app13127277.

[77] X. Zhang, G. Li, J. Zhang, A. Hu, Z. Hou, and B. Xiao, “Deep-Learning-Based Physical-Layer Secret Key Generation for FDD Systems,” *IEEE Internet Things J*, vol. 9, no. 8, pp. 6081–6094, Apr. 2022, doi: 10.1109/JIOT.2021.3109272.

[78] S. A. Hoseini, F. Bouhafs, N. Aboutorab, P. Sadeghi, and F. den Hartog, “Cooperative Jamming for Physical Layer Security Enhancement Using Deep Reinforcement Learning,” in *2023 IEEE Globecom Workshops (GC Wkshps)*, IEEE, Dec. 2023, pp. 1838–1843. doi: 10.1109/GCWkshps58843.2023.10465104.

[79] S. Deka, K. Deka, N. T. Nguyen, S. Sharma, V. Bhatia, and N. Rajatheva, “Comprehensive Review of Deep Unfolding Techniques for Next-Generation Wireless Communication Systems,” Feb. 2025.

[80] X. Chen, S. Zhang, Q. Jiang, J. Chen, H. Huang, and C. Gu, “IoT-GAN: Anomaly Detection for Time Series in IoT Based on Generative Adversarial Networks,” 2022, pp. 682–694. doi: 10.1007/978-3-030-95388-1_45.

[81] X. Tang *et al.*, "Deep Graph Reinforcement Learning for UAV-Enabled Multi-User Secure Communications," Apr. 2025.

[82] D. Huang, A. Al-Hourani, K. Sithamparanathan, and W. S. T. Rowe, "Deep Learning Methods for IoT Device Authentication Using Symbols Density Trace Plot," *IEEE Internet Things J*, vol. 11, no. 10, pp. 18167–18179, May 2024, doi: 10.1109/JIOT.2024.3361892.

[83] B. T. Hasan and A. K. Idrees, "Edge Computing for IoT," Feb. 2024, doi: 10.1007/978-3-031-50514-0_1.

[84] M. Zhang, E. Wei, and R. Berry, "Faithful Edge Federated Learning: Scalability and Privacy," Jun. 2021.

[85] F. Aloraini, A. Javed, O. Rana, and P. Burnap, "Adversarial machine learning in IoT from an insider point of view," *Journal of Information Security and Applications*, vol. 70, p. 103341, Nov. 2022, doi: 10.1016/j.jisa.2022.103341.

[86] O. A. Topal, S. Gecgel, E. M. Eksioglu, and G. K. Kurt, "Identification of Smart Jammers: Learning based Approaches Using Wavelet Representation," Jan. 2019.

[87] G. Su, M. Dai, B. Chen, and X. Lin, "Deep reinforcement learning aided secure UAV communications in the presence of moving eavesdroppers," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 4, p. 102047, Apr. 2024, doi: 10.1016/j.jksuci.2024.102047.

[88] J. Bassey, X. Li, and L. Qian, "Device Authentication Codes based on RF Fingerprinting using Deep Learning," *ICST Transactions on Security and Safety*, vol. 8, no. 29, p. 172305, Nov. 2021, doi: 10.4108/eai.30-11-2021.172305.

[89] A. Bahramali, M. Nasr, A. Houmansadr, D. Goeckel, and D. Towsley, "Robust Adversarial Attacks Against DNN-Based Wireless Communication Systems," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Nov. 2021, pp. 126–140. doi: 10.1145/3460120.3484777.

[90] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "Channel-Aware Adversarial Attacks Against Deep Learning-Based Wireless Signal Classifiers," *IEEE Trans Wirel Commun*, vol. 21, no. 6, pp. 3868–3880, Jun. 2022, doi: 10.1109/TWC.2021.3124855.

[91] A. I. Newaz, N. I. Haque, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "Adversarial Attacks to Machine Learning-Based Smart Healthcare Systems," in *GLOBECOM 2020*

- *2020 IEEE Global Communications Conference*, IEEE, Dec. 2020, pp. 1–6. doi: 10.1109/GLOBECOM42002.2020.9322472.

[92] Z. Zhou *et al.*, “Model Inversion Attacks: A Survey of Approaches and Countermeasures,” Nov. 2024.

[93] S. Ennaji, F. De Gaspari, D. Hitaj, A. Kbidi, and L. V. Mancini, “Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects,” Sep. 2024.

[94] J. Malik, R. Muthalagu, and P. M. Pawar, “A Systematic Review of Adversarial Machine Learning Attacks, Defensive Controls, and Technologies,” *IEEE Access*, vol. 12, pp. 99382–99421, 2024, doi: 10.1109/ACCESS.2024.3423323.

[95] P. Zhao, W. Zhu, P. Jiao, D. Gao, and O. Wu, “Data Poisoning in Deep Learning: A Survey,” Mar. 2025.

[96] Z. He, T. Zhang, and R. B. Lee, “Model inversion attacks against collaborative inference,” in *Proceedings of the 35th Annual Computer Security Applications Conference*, New York, NY, USA: ACM, Dec. 2019, pp. 148–162. doi: 10.1145/3359789.3359824.

[97] L. Li, “Comprehensive Survey on Adversarial Examples in Cybersecurity: Impacts, Challenges, and Mitigation Strategies,” Dec. 2024.

[98] M. Vidaković and D. Vinko, “Hardware-Based Methods for Electronic Device Protection against Invasive and Non-Invasive Attacks,” *Electronics (Basel)*, vol. 12, no. 21, p. 4507, Nov. 2023, doi: 10.3390/electronics12214507.

[99] H. Fu, L. Peng, M. Liu, and A. Hu, “Deep Learning-Based RF Fingerprint Identification With Channel Effects Mitigation,” *IEEE Open Journal of the Communications Society*, vol. 4, pp. 1668–1681, 2023, doi: 10.1109/OJCOMS.2023.3295379.

[100] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, “A survey on physical unclonable function (PUF)-based security solutions for Internet of Things,” *Computer Networks*, vol. 183, p. 107593, Dec. 2020, doi: 10.1016/j.comnet.2020.107593.

[101] F. T. Zahra, Y. S. Bostanci, and M. Soyturk, “Real-Time Jamming Detection in Wireless IoT Networks,” *IEEE Access*, vol. 11, pp. 70425–70442, 2023, doi: 10.1109/ACCESS.2023.3293404.

[102] B. Upadhyaya, S. Sun, and B. Sikdar, “Machine Learning-based Jamming Detection in Wireless IoT Networks,” in *2019 IEEE VTS Asia Pacific Wireless Communications*

Symposium (APWCS), IEEE, Aug. 2019, pp. 1–5. doi: 10.1109/VTS-APWCS.2019.8851633.

[103] S. B. Sadkhan and N. A. Abbas, “Privacy and Security of Wireless Communication Networks,” 2014, pp. 58–78. doi: 10.4018/978-1-4666-4781-7.ch004.

[104] D. Won *et al.*, “Resource Management, Security, and Privacy Issues in Semantic Communications: A Survey,” *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2024, doi: 10.1109/COMST.2024.3471685.

[105] H.-N. Dai, Q. Wang, D. Li, and R. C.-W. Wong, “On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas,” *Int J Distrib Sens Netw*, vol. 9, no. 8, p. 760834, Aug. 2013, doi: 10.1155/2013/760834.

[106] B. Thomas, S. M. Thampi, and P. Mukherjee, “An in-Depth Exploration of Attack Modeling and Vulnerability Analysis in IoT Networks,” in *Securing the Connected World*, Cham: Springer Nature Switzerland, 2025, pp. 19–45. doi: 10.1007/978-3-031-82826-3_2.

[107] M. A. Karabulut, A. F. M. S. Shah, H. Ilhan, A.-S. K. Pathan, and M. Atiquzzaman, “Inspecting VANET with Various Critical Aspects – A Systematic Review,” *Ad Hoc Networks*, vol. 150, p. 103281, Nov. 2023, doi: 10.1016/j.adhoc.2023.103281.

[108] L. Wang and A. M. Wyglinski, “Detection of man-in-the-middle attacks using physical layer wireless security techniques,” *Wirel Commun Mob Comput*, vol. 16, no. 4, pp. 408–426, Mar. 2016, doi: 10.1002/wcm.2527.

[109] A. Mallik, A. Ahsan, M. Md. Z. Shahadat, and J.-C. Tsou, “Man-in-the-middle-attack: Understanding in simple words,” *International Journal of Data and Network Science*, pp. 77–92, 2019, doi: 10.5267/j.ijdns.2019.1.001.

[110] S. Friedl and G. Pernul, “Forensic Analysis of an IoT ARP Spoofing Attack,” in *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, Apr. 2024, pp. 1–7. doi: 10.1109/ISDFS60797.2024.10527302.

[111] M. W. A. Ashraf, A. R. Singh, A. Pandian, R. S. Rathore, M. Bajaj, and I. Zaitsev, “A hybrid approach using support vector machine rule-based system: detecting cyber threats in internet of things,” *Sci Rep*, vol. 14, no. 1, p. 27058, Nov. 2024, doi: 10.1038/s41598-024-78976-1.

[112] S. Pavithra, R. Parvathi, I. Singh, and K. Agarwal, “Designing a smart grid energy management with game theory and reinforcement learning using Parrondo’s

paradox," *Energy Reports*, vol. 13, pp. 914–928, Jun. 2025, doi: 10.1016/j.egyr.2024.12.062.

[113] M. S. A. Muthanna, P. Wang, M. Wei, A. Rafiq, and N. N. Josbert, "Clustering Optimization of LoRa Networks for Perturbed Ultra-Dense IoT Networks," *Information*, vol. 12, no. 2, p. 76, Feb. 2021, doi: 10.3390/info12020076.

[114] T. Özseven, "Investigation of the effectiveness of time-frequency domain images and acoustic features in urban sound classification," *Applied Acoustics*, vol. 211, p. 109564, Aug. 2023, doi: 10.1016/j.apacoust.2023.109564.

[115] A. Bounsiar and M. G. Madden, "One-Class Support Vector Machines Revisited," in *2014 International Conference on Information Science & Applications (ICISA)*, IEEE, May 2014, pp. 1–4. doi: 10.1109/ICISA.2014.6847442.

[116] C.-W. Tien, T.-Y. Huang, P.-C. Chen, and J.-H. Wang, "Using Autoencoders for Anomaly Detection and Transfer Learning in IoT," *Computers*, vol. 10, no. 7, p. 88, Jul. 2021, doi: 10.3390/computers10070088.

[117] H. Sabit, "Multi-Agent Reinforcement Learning for Smart City Automated Traffic Light Control," in *2023 IEEE International Conference on High Performance Computing &amp; Communications, Data Science &amp; Systems, Smart City &amp; Dependability in Sensor, Cloud &amp; Big Data Systems &amp; Application (HPCC/DSS/SmartCity/DependSys)*, IEEE, Dec. 2023, pp. 956–963. doi: 10.1109/HPCC-DSS-SmartCity-DependSys60770.2023.00138.

[118] M. Wozniak, J. Silka, M. Wieczorek, and M. Alrashoud, "Recurrent Neural Network Model for IoT and Networking Malware Threat Detection," *IEEE Trans Industr Inform*, vol. 17, no. 8, pp. 5583–5594, Aug. 2021, doi: 10.1109/TII.2020.3021689.

[119] S. T. Mrudula *et al.*, "Internet of things and optimized knn based intelligent transportation system for traffic flow prediction in smart cities," *Measurement: Sensors*, vol. 35, p. 101297, Oct. 2024, doi: 10.1016/j.measen.2024.101297.

[120] J. Feng, X. Tang, B. Zhang, and Y. Ren, "Lightweight CNN-Based RF Fingerprint Recognition Method," in *2023 8th International Conference on Computer and Communication Systems (ICCCS)*, IEEE, Apr. 2023, pp. 1031–1035. doi: 10.1109/ICCCS57501.2023.10150764.

[121] E. H. Sumiea *et al.*, "Deep deterministic policy gradient algorithm: A systematic review," *Heliyon*, vol. 10, no. 9, p. e30697, May 2024, doi: 10.1016/j.heliyon.2024.e30697.

[122] Y. Shi, K. Davaslioglu, and Y. E. Sagduyu, “Generative Adversarial Network in the Air: Deep Adversarial Learning for Wireless Signal Spoofing,” *IEEE Trans Cogn Commun Netw*, vol. 7, no. 1, pp. 294–303, Mar. 2021, doi: 10.1109/TCCN.2020.3010330.

[123] J. Shanthi, M. Rajalakshmi, D. G. N. Rani, and S. Muthulakshmi, “Implementing Secure Machine Learning,” 2024, pp. 344–364. doi: 10.4018/979-8-3693-2786-9.ch015.

[124] J. S. Rahhal and D. Abualnadi, “IOT Based Predictive Maintenance Using LSTM RNN Estimator,” in *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, IEEE, Jun. 2020, pp. 1–5. doi: 10.1109/ICECCE49384.2020.9179459.

[125] I. Agbossou, “Algorithmic Innovations in Multi-Agent Reinforcement Learning: A Pathway for Smart Cities,” in *Artificial Intelligence Annual Volume 2024*, IntechOpen, 2023. doi: 10.5772/intechopen.113933.

[126] H. Kheddar, “Transformers and Large Language Models for Efficient Intrusion Detection Systems: A Comprehensive Survey,” Aug. 2024.

[127] M. Nuaimi, L. C. Fourati, and B. Ben Hamed, “Ensemble Learning Approach for Intrusion Detection Systems in Industrial Internet of Things,” in *2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA)*, IEEE, Dec. 2023, pp. 1–7. doi: 10.1109/AICCSA59173.2023.10479270.

[128] H. Zhang, L. Yu, Y. Chen, and Y. Wei, “Fast Complex-Valued CNN for Radar Jamming Signal Recognition,” *Remote Sens (Basel)*, vol. 13, no. 15, p. 2867, Jul. 2021, doi: 10.3390/rs13152867.

[129] Y. Qi, M. Qiu, H. Jiang, and F. Wang, “Extracting Fingerprint Features Using Autoencoder Networks for Gender Classification,” *Applied Sciences*, vol. 12, no. 19, p. 10152, Oct. 2022, doi: 10.3390/app121910152.

[130] C. Pandey, V. Tiwari, A. L. Imoize, C.-T. Li, C.-C. Lee, and D. S. Roy, “5GT-GAN: Enhancing Data Augmentation for 5G-Enabled Mobile Edge Computing in Smart Cities,” *IEEE Access*, vol. 11, pp. 120983–120996, 2023, doi: 10.1109/ACCESS.2023.3328170.

[131] Y. Shi, K. Davaslioglu, and Y. E. Sagduyu, “Generative Adversarial Network for Wireless Signal Spoofing,” May 2019.

[132] C. Yang, R. Wang, X. Wang, and Z. Wang, “A Game-Theoretic Perspective of Generalization in Reinforcement Learning,” Aug. 2022.

[133] Z. Yang, A. Sudjianto, X. Li, and A. Zhang, “Inherently Interpretable Tree Ensemble Learning,” Oct. 2024.

[134] R. Kong and H. Chen, “DeepCRF: Deep Learning-Enhanced CSI-Based RF Fingerprinting for Channel-Resilient WiFi Device Identification,” Nov. 2024.

[135] A. H. Ribeiro and T. B. Schön, “How Convolutional Neural Networks Deal with Aliasing,” Feb. 2021.

[136] R. Abdalla, “Complex-valued Neural Networks -- Theory and Analysis,” Dec. 2023.

[137] I. J. Goodfellow *et al.*, “Generative Adversarial Networks,” Jun. 2014.

[138] A. Vaswani *et al.*, “Attention Is All You Need,” Jun. 2017.

[139] R. C. Staudemeyer and E. R. Morris, “Understanding LSTM -- a tutorial into Long Short-Term Memory Recurrent Neural Networks,” Sep. 2019.

[140] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, “IoT Security Techniques Based on Machine Learning,” Jan. 2018.

[141] Y. E. Sagduyu, Y. Shi, and T. Erpek, “IoT Network Security from the Perspective of Adversarial Deep Learning,” May 2019.

[142] S. Strecker, R. Dave, N. Siddiqui, and N. Seliya, “A Modern Analysis of Aging Machine Learning Based IoT Cybersecurity Methods,” Oct. 2021.

[143] A. Churcher *et al.*, “An Experimental Analysis of Attack Classification Using Machine Learning in IoT Networks,” Jan. 2021, doi: 10.3390/s21020446.

[144] S. Strecker, R. Dave, N. Siddiqui, and N. Seliya, “A Modern Analysis of Aging Machine Learning Based IoT Cybersecurity Methods,” Oct. 2021.

[145] M. Nikhitha and Dr. M. A. Jabbar, “K Nearest Neighbor Based Model for Intrusion Detection System,” *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 2, pp. 2258–2262, Jul. 2019, doi: 10.35940/ijrte.B2458.078219.

[146] S. Strecker, R. Dave, N. Siddiqui, and N. Seliya, “A Modern Analysis of Aging Machine Learning Based IoT Cybersecurity Methods,” Oct. 2021.

[147] S. Karim, M. Rousanuzzaman, P. A. Yunus, P. H. Khan, and M. Asif, “Implementation of K-Means Clustering for Intrusion Detection,” *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 1232–1241, Apr. 2019, doi: 10.32628/CSEIT1952332.

[148] A. M. Mahfouz, A. Abuhussein, D. Venugopal, and S. G. Shiva, “Network Intrusion Detection Model Using One-Class Support Vector Machine,” 2021, pp. 79–86. doi: 10.1007/978-981-15-5243-4_7.

[149] Y.-T. Yang and Q. Zhu, “Game-Theoretic Foundations for Cyber Resilience Against Deceptive Information Attacks in Intelligent Transportation Systems,” Dec. 2024.

[150] Y. Zhang *et al.*, “Learning Decentralized Traffic Signal Controllers with Multi-Agent Graph Reinforcement Learning,” Nov. 2023.

[151] E. H. Sumiea *et al.*, “Deep deterministic policy gradient algorithm: A systematic review,” *Heliyon*, vol. 10, no. 9, p. e30697, May 2024, doi: 10.1016/j.heliyon.2024.e30697.

[152] S. A. Almalki and F. T. Sheldon, “Deep Learning to Improve False Data Injection Attack Detection in Cooperative Intelligent Transportation Systems,” in *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, IEEE, Oct. 2021, pp. 1016–1021. doi: 10.1109/IEMCON53756.2021.9623153.

[153] M. Landauer, F. Skopik, B. Stojanović, A. Flatscher, and T. Ullrich, “A review of time-series analysis for cyber security analytics: from intrusion detection to attack prediction,” *Int J Inf Secur*, vol. 24, no. 1, p. 3, Feb. 2025, doi: 10.1007/s10207-024-00921-0.

[154] S. Wang, L. Peng, H. Fu, A. Hu, and X. Zhou, “A Convolutional Neural Network-Based RF Fingerprinting Identification Scheme for Mobile Phones,” in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, Jul. 2020, pp. 115–120. doi: 10.1109/INFOCOMWKSHPS50562.2020.9163058.

[155] P. B. Udas, K. S. Roy, Md. E. Karim, and S. M. Azmat Ullah, “Attention-based RNN architecture for detecting multi-step cyber-attack using PSO metaheuristic,” in *2023 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, IEEE, Feb. 2023, pp. 1–6. doi: 10.1109/ECCE57851.2023.10101590.

[156] Supriya Shende, “Long Short-Term Memory (LSTM) Deep Learning Method for Intrusion Detection in Network Security,” *International Journal of Engineering Research and*, vol. V9, no. 06, Jul. 2020, doi: 10.17577/IJERTV9IS061016.

[157] M. Castelli, L. Manzoni, T. Espindola, A. Popovič, and A. De Lorenzo, “Generative adversarial networks for generating synthetic features for Wi-Fi signal quality,” *PLoS One*, vol. 16, no. 11, p. e0260308, Nov. 2021, doi: 10.1371/journal.pone.0260308.

[158] R. S. Peres, M. Azevedo, S. O. Araújo, M. Guedes, F. Miranda, and J. Barata, "Generative Adversarial Networks for Data Augmentation in Structural Adhesive Inspection," *Applied Sciences*, vol. 11, no. 7, p. 3086, Mar. 2021, doi: 10.3390/app11073086.

[159] A. L. Alfeo, M. G. C. A. Cimino, G. Manco, E. Ritacco, and G. Vaglini, "Using an autoencoder in the design of an anomaly detector for smart manufacturing," *Pattern Recognit Lett*, vol. 136, pp. 272–278, Aug. 2020, doi: 10.1016/j.patrec.2020.06.008.

[160] D. S. J, B. R, B. N, and B. D. N, "Robust fingerprint reconstruction using attention mechanism based autoencoders and multi-kernel autoencoders," *Applied Intelligence*, vol. 54, no. 17–18, pp. 8262–8277, Sep. 2024, doi: 10.1007/s10489-024-05622-8.

[161] L. Roquet, F. Fernandes dos Santos, P. Rech, M. Traiola, O. Sentieys, and A. Kritikakou, "Cross-Layer Reliability Evaluation and Efficient Hardening of Large Vision Transformers Models," in *Proceedings of the 61st ACM/IEEE Design Automation Conference*, New York, NY, USA: ACM, Jun. 2024, pp. 1–6. doi: 10.1145/3649329.3655688.

[162] R. Abdalla, "Complex-valued Neural Networks -- Theory and Analysis," Dec. 2023.

[163] Naveen Kumar, "https://www.demandsage.com/number-of-iot-devices/?utm_source."

[164] T. Mazhar *et al.*, "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," *Brain Sci*, vol. 13, no. 4, p. 683, Apr. 2023, doi: 10.3390/brainsci13040683.