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 counterfeiting 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 units 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.

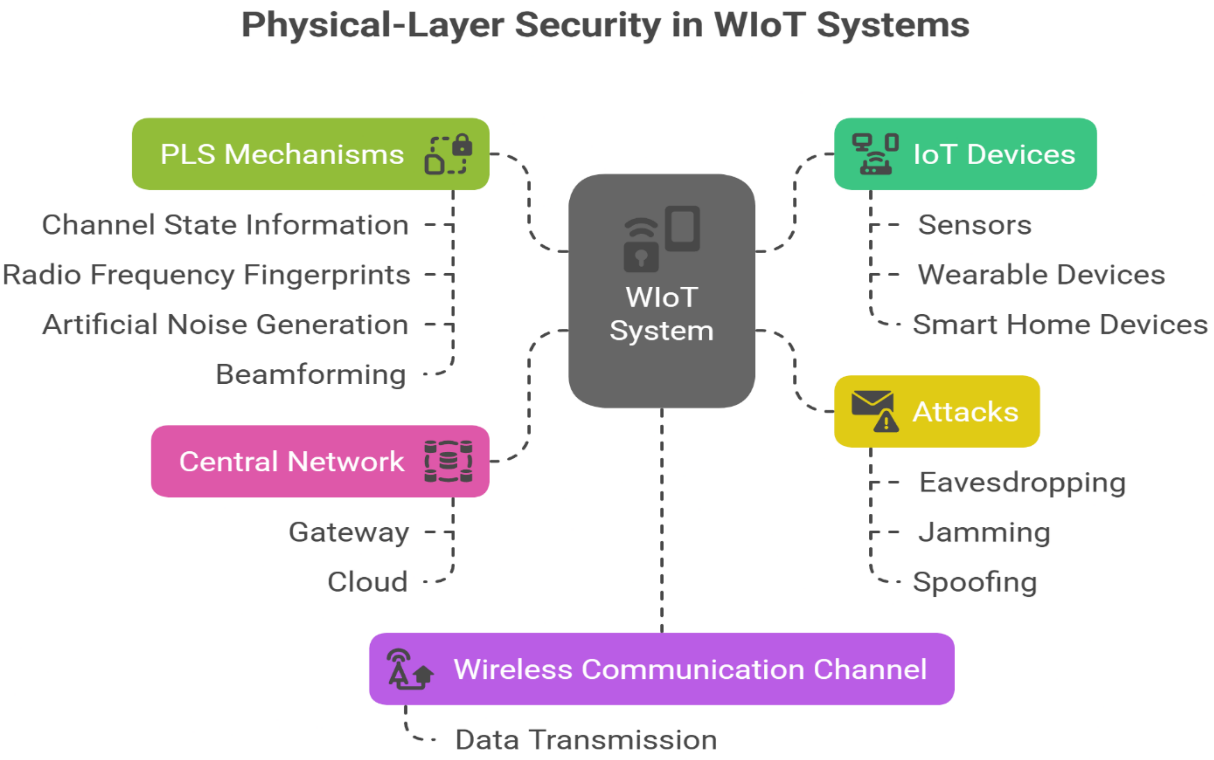

Figure 1. Conceptual Diagram of Physical-Layer Security in Wireless IoT

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 units in environments that require long-term security and reliability [14].
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 [15].
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 [16].
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 [17].

1.3 Deep learning -enhanced physical layer security

for 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 units and secure Wiot-Network communication [18]. 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 [19].
2. **Low Computational Overhead:** PLS works with low computational complexity, which is essential for WIoT units 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 [20].
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 units into smart cities and industrial applications [21].
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 [22].
    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 [23].
    3. **Scalable feature extraction with Deep Learning:** Deep learning models enable scalable feature extraction of RF fingerprints from many IoT units without requiring extensive prior knowledge or manual intervention. This is especially important as the number of connected units in Wiot systems grows exponentially [24].

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 [25].

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.
[26]	2023	PLS Mechanisms	No	No	None	Eavesdropping, Jamming	Yes	No	No	No	Yes	Yes
[27]	2022	Secure Industrial Comms	Yes	No	None	Spoofing	Yes	No	No	No	Yes	Yes
[28]	2022	RF Fingerprinting	Partial	Yes	DL (discriminative)	Spoofing	Yes	No	No	No	Yes	Yes
[29]	2021	NFC Security	No	Yes	DL (discriminative)	Spoofing	Yes	No	Yes	Yes	Yes	No
[30]	2021	IoT Device Detection	Yes	Yes	ML (unspecified)	Spoofing	Yes	No	No	No	Yes	Yes
[31]	2020	RF Fingerprinting	Yes	Yes	DL (discriminative)	Spoofing	Yes	No	Yes	Yes	Yes	No
[32]	2020	PLA for IoT	Yes	Partial	None	Spoofing, Eavesdropping	Yes	No	No	No	Yes	Yes
[33]	2020	PLA Fundamentals	Partial	No	None	Spoofing, Eavesdropping	Yes	No	No	No	Yes	Yes
[34]	2019	RFID Security	Yes	Yes	DL (discriminative)	Spoofing	Yes	No	Yes	Yes	Yes	Yes
[35]	2019	ML-based PLA	Partial	Yes	Supervised, DL	Spoofing, Eavesdropping	Yes	No	No	No	Yes	Yes

Analytical Discussion of Each Survey Study

- [26] (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.
- [27] (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.
- [28] (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.
- [29] (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.
- [30] (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.
- [31] (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.
- [32] (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.
- [33] (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.

- [34] (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.
- [35] (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 ([26]-[35]) 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 [28], [29], [31] and [34] incorporate DL for RF fingerprints, NFC Security and RFID applications, many others ([26], [27], [32], [33], [35]) are exclusively on theoretical framework without empirical framework. For example, [28] 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 [29], [32], [33] and [35] address the PLA, aimed at spoofing and eavesdropping, while neglecting other threats such as jamming, which are only short covered in [26] and [31]. This authentication-centric approach, seen in [27] industrial focus and [30] 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 [34] and [35] from 2019 focus on 5G-era challenges, while even recent surveys ([26], [27], [28]) provide limited discussion on 6G-specific requirements, such as ultra-low latency, massive connectivity, or heterogeneous network integration. For example, [26] (2023) suggests emerging applications but does not tailor its PLS outlook to 6G, and [32] 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 ([26] – [35]) address adversarial attacks on DL models, a critical oversight given the vulnerability of ML-based security systems. Furthermore, studies like [26], [29], and [35] 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 ([26], [27], [28], [30], [32], [33], [35]) Reproducing and benchmarking of PLS techniques. Even when data sets are used (e.g. [29], [31], [34]), 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.

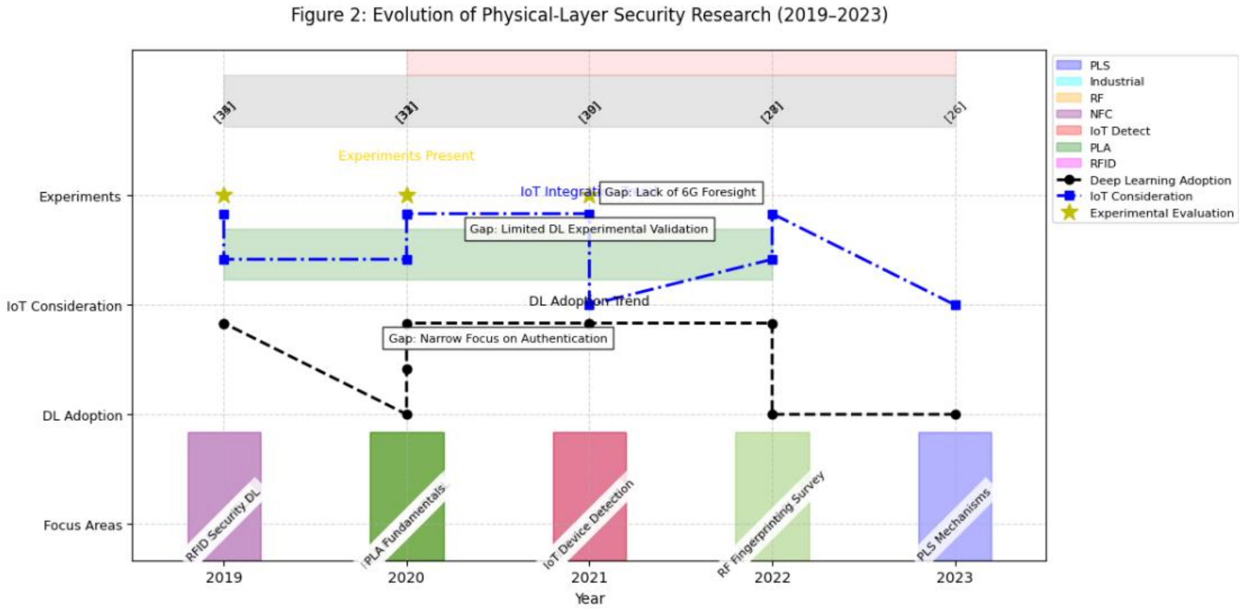

Figure 2. Graphical Representation of the Evolution of Physical-Layer Security Research

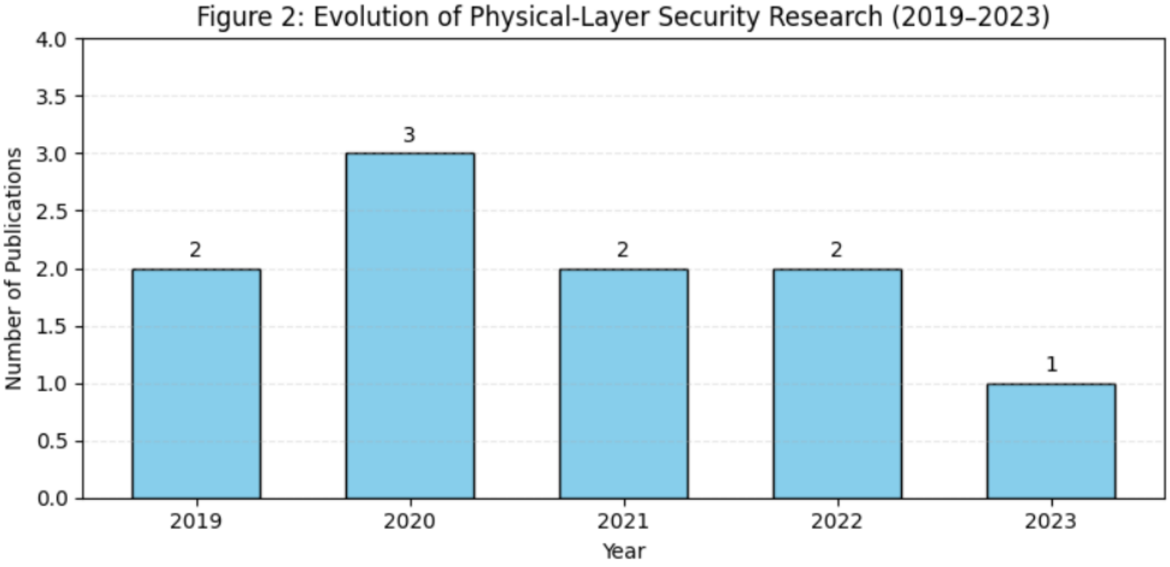

Figure 3. Graphical Representation of the Evolution of Physical-Layer Security Research

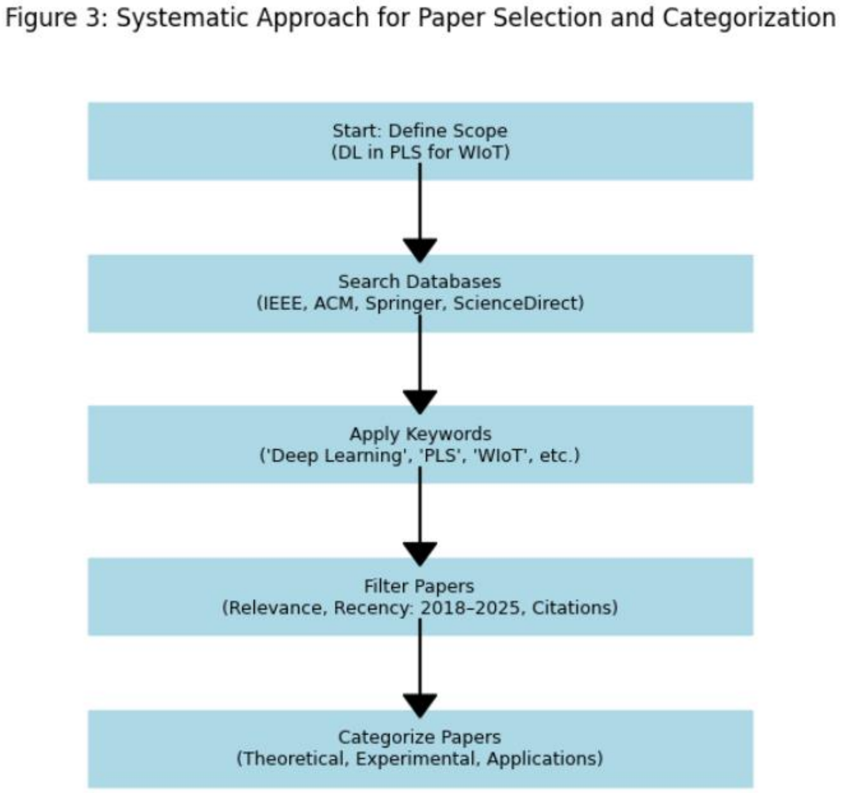
Figure 3: Systematic Approach for Paper Selection and Categorization
Start: Define Scope
(DL in PLS for WIoT)
Search Databases
(IEEE, ACM, Springer, ScienceDirect)
Apply Keywords
('Deep Learning', 'PLS', 'WIoT', etc.)
Filter Papers
(Relevance, Recency: 2018–2025, Citations)
Categorize Papers
(Theoretical, Experimental, Applications)

Figure 4.: **Systematic Approach for 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., [26], [32]), 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. [27], [29]) 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.

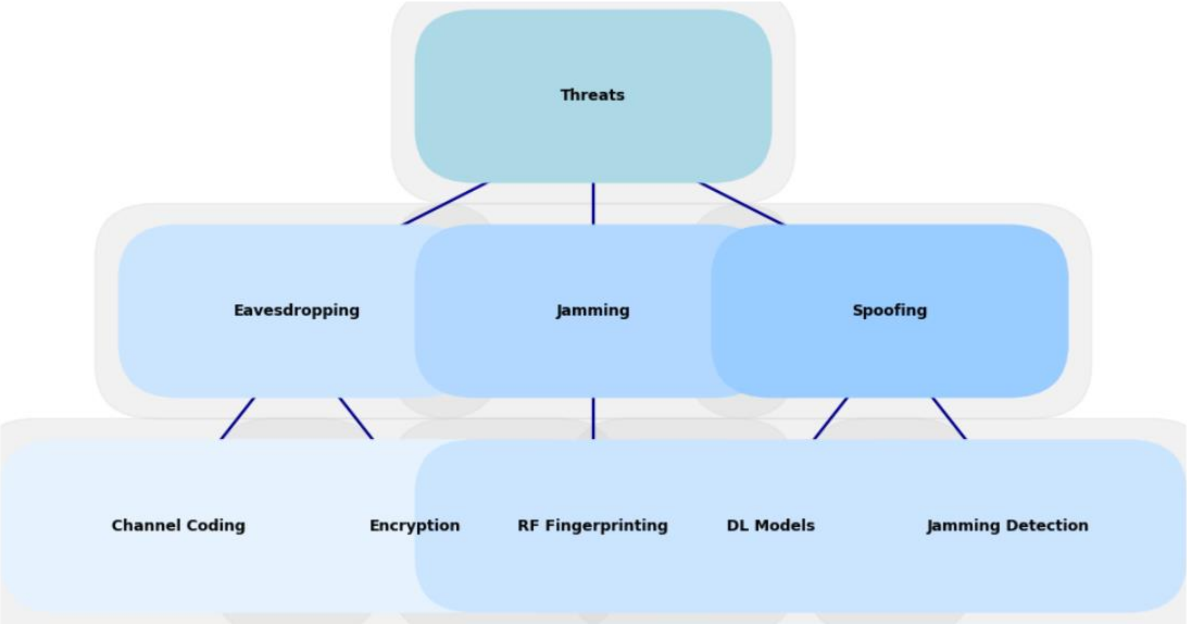

Figure 5: **Systematic taxonomy of physical security threats and countermeasures**

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 [33] and [35], offering a comprehensive guide to selecting and adapting DL models for WIoT security challenges.

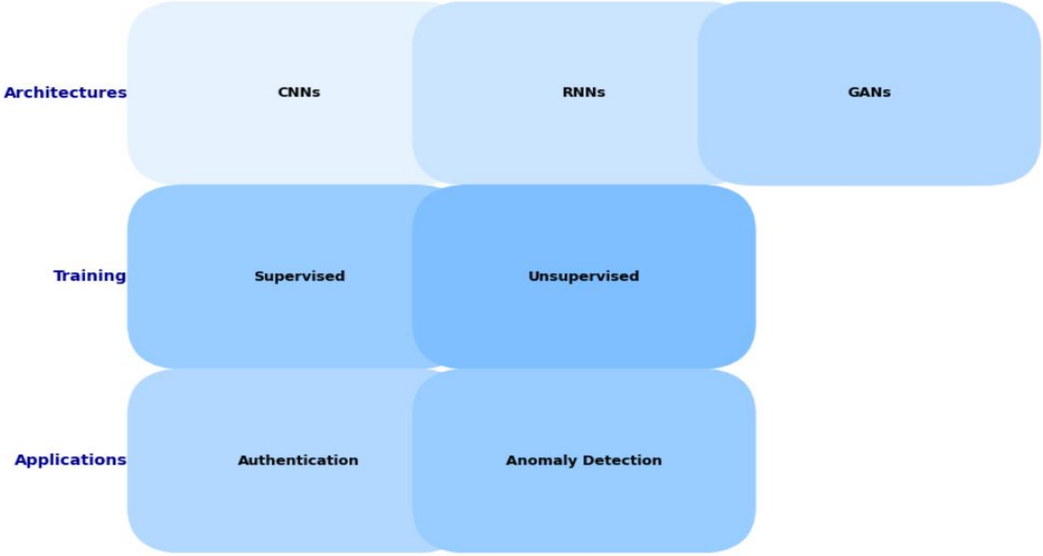

Figure 6: Systematic Taxonomy of Deep Learning Solutions for Physical Security

4. **Extensive review of real and synthetic datasets** We compile and analyze a wide range of datasets used in DL-PLS research, including datasets in the real world (e.g., RF signal prisoners from IoT units) and synthetic datasets (e.g., simulated Wiot-channel models). This review addresses the gap in data set discussion that is listed in previous works (e.g. [26], [28]), and provides insight into data availability, quality, and suitability for benchmarking DL Techniques in Wiot Security.

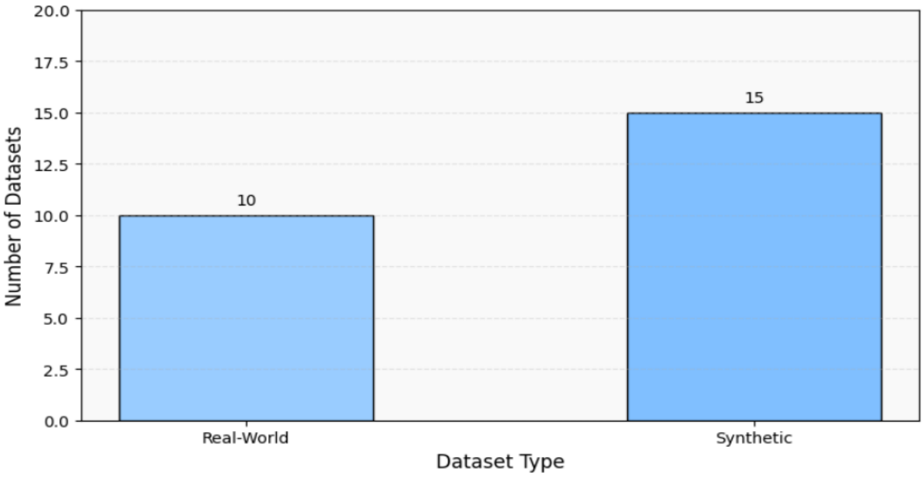

Figure 7: Dataset Overview

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 [27] and [30], 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., [26], [34]), providing actionable recommendations to guide the next wave of research and development.

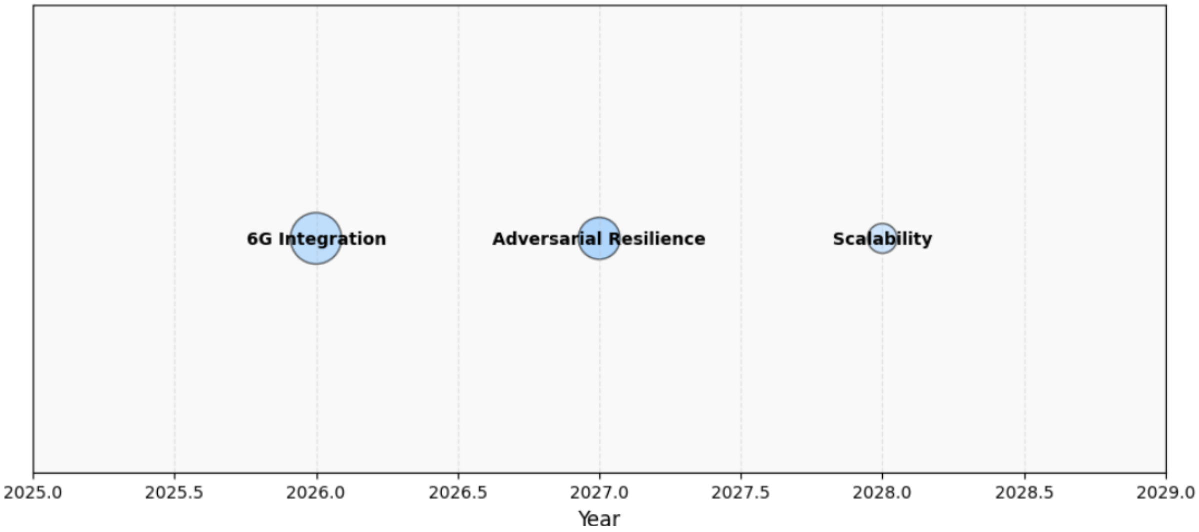

Figure 8: Roadmap for Future Work

1.8 Structure of Survey

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

References

[1] Atzori, L., et al., "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, 2010, pp. 2787-2805. DOI: 10.1016/j.comnet.2010.05.010.

[2] Gubbi, J., et al., "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, 2013, pp. 1645-1660. DOI: 10.1016/j.future.2013.01.010.

[3] Statista, "Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025," 2021. Statista Report.

[4] Chen, M., et al., "Edge Intelligence for IoT: Challenges and Opportunities," *IEEE Internet of Things Journal*, vol. 7, no. 10, 2020, pp. 9339-9350. DOI: 10.1109/JIOT.2020.2983688.

[5] Stallings, W., "Cryptography and Network Security: Principles and Practice," 7th ed., Pearson, 2017, pp. 45-67. ISBN: 978-0134444284.

[6] Wang, C.-X., et al., "On the Road to 6G: Visions, Requirements, and Enabling Technologies," *IEEE Communications Magazine*, vol. 59, no. 7, 2021, pp. 82-88. DOI: 10.1109/MCOM.001.2001217.

[7] Xiao, L., et al., "Learning-Based Physical Layer Authentication," *IEEE Transactions on Communications*, vol. 63, no. 11, 2015, pp. 4337-4349. DOI: 10.1109/TCOMM.2015.2478783.

[8] He, D., et al., "Machine Learning Techniques for Physical Layer Security: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, 2021, pp. 2318-2356. DOI: 10.1109/COMST.2021.3101955.

[9] Xiao, L., et al., "Physical Layer Authentication for 5G Communications: Opportunities and Challenges," *IEEE Wireless Communications*, vol. 27, no. 6, 2020, pp. 152-158. DOI: 10.1109/MWC.001.2000158.

[10] Fang, H., et al., "Physical Layer Authentication in Heterogeneous Networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, 2020, pp. 6760-6773. DOI: 10.1109/TWC.2020.3006148.

[11] Zhang, J., et al., "Reinforcement Learning for Adaptive Physical Layer Security," *IEEE Transactions on Wireless Communications*, vol. 20, no. 6, 2021, pp. 3890-3902. DOI: 10.1109/TWC.2021.3056789.

[12] Wang, N., et al., "Machine Learning-Based Physical Layer Authentication for Dynamic Wireless Environments," *IEEE Access*, vol. 8, 2020, pp. 156789-156800. DOI: 10.1109/ACCESS.2020.3019876.

[13] Rappaport, T. S., et al., "Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond," *IEEE Access*, vol. 7, 2019, pp. 78729-78757. DOI: 10.1109/ACCESS.2019.2921522.

[14] Shor, P. W., "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, 1997, pp. 1484-1509. DOI: 10.1137/S0097539791191204.

[15] Atzori, L., et al., "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, 2010, pp. 2787-2805. DOI: 10.1016/j.comnet.2010.05.010.

[16] Wang, C., et al., "On the Road to 6G: Visions, Requirements, and Enabling Technologies," *IEEE Communications Magazine*, vol. 59, no. 7, 2021, pp. 82-88. DOI: 10.1109/MCOM.001.2001217.

[17] Xiao, L., et al., "Physical Layer Authentication for 5G Communications: Opportunities and Challenges," *IEEE Wireless Communications*, vol. 27, no. 6, 2020, pp. 152-158. DOI:

10.1109/MWC.001.2000158.
[18] Xiao, L., et al., "Learning-Based Physical Layer Authentication," *IEEE Transactions on Communications*, vol. 63, no. 11, 2015, pp. 4337-4349. DOI: 10.1109/TCOMM.2015.2478783.
[19] He, D., et al., "Machine Learning Techniques for Physical Layer Security: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, 2021, pp. 2318-2356. DOI: 10.1109/COMST.2021.3101955.
[20] Zhang, J., et al., "Reinforcement Learning for Adaptive Physical Layer Security," *IEEE Transactions on Wireless Communications*, vol. 20, no. 6, 2021, pp. 3890-3902. DOI: 10.1109/TWC.2021.3056789.
[21] Fang, H., et al., "Physical Layer Authentication in Heterogeneous Networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, 2020, pp. 6760-6773. DOI: 10.1109/TWC.2020.3006148.
[22] Restuccia, F., et al., "Securing the Internet of Things with Machine Learning at the Physical Layer," *IEEE Communications Magazine*, vol. 58, no. 11, 2020, pp. 76-81. DOI: 10.1109/MCOM.001.2000455.
[23] Liu, F., et al., "Machine Learning for Intelligent Authentication in Wireless Networks," *IEEE Wireless Communications*, vol. 26, no. 5, 2019, pp. 55-61. DOI: 10.1109/MWC.001.1900291.
[24] Biggio, B., et al., "Evasion Attacks Against Machine Learning at Test Time," *Machine Learning and Knowledge Discovery in Databases*, ECML PKDD 2013, Springer, 2013, pp. 387-402. DOI: 10.1007/978-3-642-40894-6_twenty-nine.
[25] Jian, T., et al., "Deep Learning for RF Fingerprinting in 5G and Beyond," *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 3, 2020, pp. 234-245. DOI: 10.1109/JRFID.2020.2993456.

[26] N. Xie, J. Zhang, Q. Zhang, Security provided by the physical layer in wireless communications, IEEE Network 37 (5) (2023) 42–48.

[27] P. Angueira, I. Val, J. Montalban, Ó. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, A. Arriola, A survey of physical layer techniques for secure wireless communications in industry, IEEE Communications Surveys & Tutorials 24 (2) (2022) 810–838.

[28] A. Jagannath, J. Jagannath, P. S. P. V. Kumar, A comprehensive survey on radio frequency (rf) fingerprinting: Traditional approaches, deep learning, and open challenges, Computer Networks 219 (2022) 109455.

[29] W. Lee, S. Y. Baek, S. H. Kim, Deep-learning-aided rf fingerprinting for NFC security, IEEE Communications Magazine 59 (5) (2021) 96–101.

[30] Y. Liu, J. Wang, J. Li, S. Niu, H. Song, Machine learning for the detection and identification of internet of things devices: A survey, IEEE Internet of Things Journal 9 (1) (2021) 298–320.

[31] N. Soltani, K. Sankhe, J. Dy, S. Ioannidis, K. Chowdhury, More is better: Data augmentation for channel-resilient rf fingerprinting, IEEE Communications Magazine 58 (10) (2020) 66–72.

[32] N. Xie, Z. Li, H. Tan, A survey of physical-layer authentication in wireless communications, IEEE Communications Surveys & Tutorials 23 (1) (2020) 282–310.

[33] L. Bai, L. Zhu, J. Liu, J. Choi, W. Zhang, Physical layer authentication in wireless communication networks: A survey, Journal of Communications, and Information Networks 5 (3) (2020) 237–264.

[34] X. Fan, F. Wang, F. Wang, W. Gong, J. Liu, when rfid meets deep learning: Exploring cognitive intelligence for activity identification, IEEE wireless Communications 26 (3) (2019) 19–25.

[35] H. Fang, X. Wang, S. Tomasin, Machine learning for intelligent authentication in 5g and beyond wireless networks, IEEE Wireless Communications 26 (5) (2019) 55–61.