"Revolutionizing 6G Network Security: Experimental Study on Physical-Layer Authentication Using Machine Learning for Secure Authentication, Authorization, and Resilience Against Adversarial Attacks"

Abstract

1. Introduction

The emergence of the sixth-generation wireless network (6G) represents a revolutionary leap in communication technology, supporting exceptionally high data rates of more than 1 Tbps, massive connectivity that supports up to 10^7 devices per square kilometer, and ultra-low latency below 1 ms [1]. "These features are expected to unlock revolutionary applications, including virtual interactions, holographic telepresence for autonomous systems, which cover autonomous vehicles and drones, and integrated detection and communication platforms (ISAC) that provide real-time sensitive environment data [2]."At the center of this new paradigm is the Internet of Things (IoT), which has progressively permeated daily life and is expected to connect almost 25 billion devices by 2025, hence turning smart cities, advanced healthcare systems, and public safety structures into realities [3]. Integration of IoT in cities improves living standards through the real-time management of city infrastructure, telemedicine programs, and disaster response systems; however, it also simultaneously poses enormous security challenges of an unprecedented scale [4].

The inherent heterogeneity and extensive deployment of sixth generation (6G) networks, in addition to the rapid spread of novel Internet of Things (IoT) technologies—ranging from wearable healthcare monitoring devices to home automation systems and integrated transport systems—enlarges the attack surface potential [5]. Under this paradigm, security vulnerabilities include the threat of eavesdropping, in which unauthorized users can intercept confidential data, such as private health data or traffic management signals, in addition to more advanced attacks like impersonation and signal interference, which have the potential to severely compromise vital services [6]. Traditional security methods, based on upper-layer cryptographic algorithms like RSA or AES, are increasingly failing to meet the challenge of 6G technology [7]. Such methods fail to meet the stringent latency requirements involved in ultra-dependable low-latency communication (URLLC), the scalability requirements inherent in massive machine-type communication (mMTC), and the resource constraint requirements necessary for IoT devices functioning under power constraints [8]. Consequently, there are considerable loopholes in authentication and authorization protocols, thus compromising the integrity of public IoT networks facilitated by 6G.

Physical-layer authentication (PLA) is a novel and resource-saving approach that leverages the uniqueness of physical-layer features, namely channel state information (CSI) and radio frequency (RF) fingerprints, to bolster the security functions of sixth generation (6G) systems [9]. Compared to cryptographic solutions that require a high number of computational resources, PLA utilizes the physical environment in conjunction with device-specific credentials, thus providing a lightweight solution in terms of overhead, which is especially beneficial for Internet of Things (IoT) applications located in public environments that are marked by stringent resource constraints [10]. However, traditional static PLA solutions are not sufficient in meeting the dynamic channel conditions that are typical of 6G, let alone the sophistication of adversarial attacks targeted at modern IoT deployments [11]. To mitigate these issues, this research suggests an experimental setup that is geared to revolutionize security in 6G networks by incorporating machine learning (ML)-augmented PLA. By leveraging innovative ML techniques, namely deep neural networks (DNN) and reinforcement learning (RL) to analyze and adaptively authenticate physical-layer features, this research aims to provide secure mechanisms for authentication, authorization, and adversarial robustness.

1.1 Background

The development of wireless communication technologies forms a cornerstone of modern societal progress, each subsequent generation building on its predecessor to accommodate the increasing demands for connectivity and capabilities [12]. Integration of the Internet of Things (IoT) into public spaces has accelerated this advancement, enabling a wide range of applications enhancing efficiency, security, and convenience for the masses. Estimates predict that by 2025, the world will have over twenty-five billion IoT connections, with a sizable percentage utilized in public infrastructure, such as smart traffic management systems, environmental sensors for air quality monitoring, and telemedicine systems for remote health monitoring [13]. These are examples of the use of IoT in public spaces, where devices are intended to sense, analyze, and transmit data for the purpose of enhancing urban planning, disaster response, and healthcare delivery [14]. Future IoT technologies are expected to further advance this impact, as innovations like smart wearables for fitness monitoring, connected cars for traffic management, and city sensor networks for real-time resource allocation become mainstream [15].

The growth of IoT technologies, however, introduces serious security issues that threaten the reliability of public networks powered by the technologies. The incredibly open nature of wireless communication channels makes them susceptible to several types of attacks, including espionage, where malicious entities exploit weak signal protections to capture sensitive data - distributing personal health records to municipal operational details [16]. More insidious threats include representation, where invaders use double legitimate devices to gain unauthorized access and block, which overloads networks with disruptive interference, potentially blocking critical services such as emergency response systems [17]. Sybil attacks, where malicious entities create multiple forged identities, further undermine trust by influencing network protocols or dominating available resources [18]. These weaknesses have been well-documented in the wireless security literature and pose considerable threats to both public safety and economic viability.

The transition to 6G exacerbates these issues, as its ambitious targets—enabling ultra-high data transmission rates, supporting massive device densities, and incorporating terrestrial and satellite infrastructures—bring unprecedented complexities [19]. For instance, the IoT-enabled vehicular networks in the 6G context rely on real-time data exchange for autonomous driving coordination and traffic management; however, their very mobility and edge computing dependency increase the vulnerabilities of interception and disruption [20]. Similarly, the 6G vision of integrated space-air-ground-sea networks aims to advance IoT connectivity in remote public settings, such as maritime monitoring and rural healthcare; however, this wider reach enlarges the threat landscape, introducing new vectors for attacks [21]. Therefore, the convergence of emerging IoT technologies and the heightened capabilities of 6G highlights the imperatives of stringent security measures for protecting data integrity, ensuring service continuity, and maintaining public trust in these revolutionary innovations.

1.2 Limitations of Upper-Layer Cryptographic Security for 6G and IoT

Wireless network authentication protocols, particularly those intended for Internet of Things (IoT) use in shared spaces, have long relied on upper-layer cryptographic methods, such as public-key encryption frameworks (e.g., RSA and ECC) and symmetric key schemes (e.g., AES), to validate device identities and encrypt data transmission [22]. While effective for previous generations, these methods have major limitations for application in the new context of 6G and modern IoT networks for the following reasons:

1. Cryptographic security depends on the computational intractability of mathematical problems, such as integer factorization or discrete logarithms, which quantum computing advancements threaten to unravel [23]. For example, Shor’s algorithm could compromise RSA keys, endangering IoT devices in public infrastructure like smart grids, where false commands could disrupt power distribution [24]. This vulnerability is particularly acute in 6G, where long-term security is critical for public safety applications.
2. Upper-layer approaches are vulnerable to replay attacks, where attackers capture and replay original signals to bypass authentication mechanisms without decryption of the data [25]. For IoT applications sensitive to latency, like real-time health monitoring in smart healthcare centers, this exposure can lead to unauthorized access or service interruption, thus compromising the quality of care [26]. The wireless medium's inherent broadcasting nature in 6G makes this threat worse.
3. Key management processes, including generation, distribution, and periodic renewal, introduce significant latency and overhead, clashing with 6G’s URLLC requirements [27]. Trending IoT use cases, such as autonomous drones monitoring public spaces or smart traffic lights optimizing urban flow, demand instantaneous authentication, where even millisecond delays can impair functionality [28]. Cryptographic key exchanges often require multiple communication rounds, exacerbating this issue.
4. The computational overhead of cryptographic algorithms imposes serious limitations on IoT devices with limited resources that are prevalent in 6G networks, such as low-power sensors and wearables [29]. In addition, the heterogeneity inherent in the combined networks of 6G that involve multiple IoT protocols and device types of compounds interoperability issues since variations in encryption standards hinder seamless

interconnections and increase communication overhead [30]. This is particularly problematic in public IoT deployments requiring rapid scalability.

These limitations reveal that upper-layer cryptographic security is ill-suited to address the security aspects of 6G-enabled IoT, necessitating innovative approaches that balance efficiency, scalability, and robustness.

1.3 Machine Learning-Enhanced Physical-Layer Security for 6G IoT

Physical-layer authentication (PLA) is a promising choice that leverages physical-layer properties, including channel state information (CSI), radio frequency fingerprints, and signal propagation characteristics, to verify devices in Internet of Things (IoT)-supported sixth generation (6G) networks [31]. The PLA security provides many advantages particularly tailored to support public IoT and future technologies:

1. The uniqueness of physical-layer features, derived from environmental factors (e.g., multipath fading) and hardware imperfections (e.g., oscillator drift), resists replication by adversaries [32]. This enhances security for IoT devices in public settings, protecting against impersonation and spoofing attacks that threaten smart city infrastructure or connected vehicles [33].
2. PLA's low computational overhead aligns with the resource constraints of trending IoT devices, such as battery-powered sensors or wearables, by leveraging pre-existing CSI obtained during channel estimation [34]. This efficiency is crucial for 6G's mMTC scenarios, where millions of devices require rapid authentication without draining limited power reserves.
3. The PLA is compatible with the heterogeneous 6G architecture to provide seamless integration of diverse IoT networks in public environments [35]. Unlike upper-layer approaches, PLA can decode physical-layer signals regardless of protocol differences, thus improving interoperability in space-air-ground-sea systems. Traditional PLA approaches relied on statistical hypothesis testing, comparing received signal features against predefined thresholds to detect anomalies [36]. However, 6G's dynamic channel conditions—driven by high mobility, dense deployments, and environmental variability—along with the stringent security demands of trending IoT applications, render static thresholds ineffective [37].

Machine learning (ML)-enhanced PLA overcomes these challenges by introducing adaptive and intelligent security mechanisms:

1. Machine learning algorithms, such as convolutional neural networks (CNNs), efficiently evaluate the complex, high-dimensional channel conditions typical of 6G-IoT environments, such as smart cities with overlapping signals from many devices [38]. This capability surpasses that of traditional models, which struggle to capture real-time variations.

2. Adaptive authentication, using reinforcement learning or online learning methods, adjusts thresholds in real-time in mobile IoT applications, such as connected cars within public transportation or drones scanning cities [39]. This ensures sustained security despite rapid changes in communications channels.
3. Scalable feature extraction, powered by deep learning, identifies RF fingerprints for massive IoT populations without requiring extensive prior knowledge or manual feature engineering [40]. This is vital for trending IoT applications, where the number of connected devices grows exponentially.
4. Resilience to adversarial attacks—such as signal spoofing or jamming targeting public IoT systems—is enhanced through ML-driven anomaly detection, which identifies subtle deviations in physical-layer signatures [41]. This protects critical services like emergency response networks from disruption.

Table 1. Comparative Review of Key Studies on Physical-Layer Authentication and Wireless Security

Ref.	Major Contributions	Focus Area	Methodology	Gaps	Weakness	Studying Type
[42]	Overviews different Physical Layer Security (PLS) mechanisms, explain their relationships, and introduce promising security approaches for emerging wireless applications.	PLS Mechanisms	Theoretical	Limited discussion on ML-based PLA and scalability for massive IoT in 6G.	Lacks experimental validation or practical implementation insights for 6G.	Research Review
[43]	Reviews PLA techniques, analyzes their limitations (e.g., static thresholds), identifies research areas like latency reduction, and discusses invoking PLA to reduce latency.	PLA Techniques	Theoretical	Does not cover trending IoT or ML-based adaptive authentication methods.	Theoretical focus with minimal real-world deployment insights.	Research Review
[44]	Envisions ML-based PLA approaches, introduces ML paradigms (e.g., supervised learning, deep	ML-based PLA	Theoretical/ML-based	Lacks real-time performance evaluation and integration with	No empirical data to validate ML-based PLA effectiveness.	Research Review

	learning) for intelligent attack detection, and highlights potential for 5G and beyond.			heterogeneous 6G networks.		
[45]	Surveys PLS based on information-theoretic principles, briefly discusses hypothesis-testing-based PLA, and provides a foundational understanding of security mechanisms.	PLS Principles	Theoretical	Limited focus on modern ML techniques or IoT applications in public domains.	Outdated for 6G; shallow treatment of PLA-specific challenges.	Survey
[46]	Investigates PLS theories, discusses techniques and challenges (e.g., dynamic channels), and suggests solutions, including PLA enhancements.	PLS Technologies	Theoretical	Inadequate attention to ML-driven PLA or scalability for massive device networks.	Theoretical bias with limited practical insights.	Survey
[47]	Surveys PLA in wireless networks, covering fundamentals, attack models, and channel information-based methods, with a focus on research trends.	PLA Fundamentals	Theoretical	Limited exploration of ML applications and 6G-specific challenges.	General focus; lacks depth on IoT-specific security in public domains.	Survey
[48]	Surveys PLA in wireless communications, covering theoretical foundations, practical challenges, and authentication schemes for IoT and beyond.	PLA for IoT	Theoretical	Does not emphasize ML scalability or 6G-specific heterogeneous network challenges.	Limited discussion on adversarial attacks in IoT contexts.	Survey
[49]	Surveys physical layer techniques for secure industrial communications, including PLA, with a focus on industry-specific requirements and challenges.	Secure Industrial Comms	Theoretical	Minimal coverage of ML-enhanced PLA or public IoT applications in 6G.	Industry-focused; less applicable to broader 6G public IoT scenarios.	Survey

[50]	Surveys device fingerprinting in wireless networks, discussing challenges (e.g., noise effects) and opportunities for enhancing security.	Device Fingerprinting	Theoretical	Lacks focus on ML-based approaches and 6G-specific requirements.	Pre-6G; does not address modern IoT trends or adversarial resilience.	Survey
[51]	Explores deep learning for RFID-based activity identification, highlighting cognitive intelligence for security applications.	RFID Security	ML-based	Limited to RFID; does not address broader PLA or 6G-IoT contexts.	Narrow scope; lacks generalizability to 6G networks.	Research Review
[52]	Proposes data augmentation for channel-resilient RF fingerprinting, improving identification accuracy in wireless networks.	RF Fingerprinting	ML-based/Experimental	Does not explore 6G-specific challenges or public IoT applications.	Limited scope to fingerprinting; lacks broader PLA integration.	Experimental Study
[53]	Introduces deep learning for NFC security via RF fingerprinting, focusing on authentication improvements.	NFC Security	ML-based/Experimental	Limited to NFC; lacks discussion on 6G or public IoT scalability.	Narrow focus; minimal relevance to broader 6G-IoT security.	Experimental Study
[54]	Surveys RF fingerprinting, comparing traditional and deep learning approaches, and discussing open challenges like scalability and noise robustness.	RF Fingerprinting	Theoretical/ML-based	Limited focus on 6G-specific heterogeneous networks or public IoT security.	General survey; lacks experimental validation for 6G scenarios.	Survey
[55]	Surveys ML for IoT device detection and identification, discussing challenges (e.g., device diversity) and future research directions.	IoT Device Detection	ML-based	Does not specifically address PLA or 6G network challenges.	Broad focus; lacks depth on physical-layer security applications.	Survey

Table 2. provides a detailed comparison of fourteen representative vision articles, research, and tutorial on physical layer authentication (PLA) and related safety mechanisms, published between 2014 and 2023. Summarizes the main contributions of each article, focus on focus (e.g., PLA, PLA, digital printing), methodologies (e.g., theoretical, ML-based), gaps, weaknesses, and relevance to 6G/IoT security. The table categorizes studies as research reviews, surveys, or experimental studies.

Table 2. Comparative Review of Key Studies on Physical-Layer Authentication and Wireless Security

Ref.	Frequency	Availability	Features	Important Information for ML/DL Models	Data Sources	Scale of Devices	Use Case Relevance	Rows (Samples)	Columns
[56]	2.45 GHz	Likely Available, Free	I/Q samples, small-scale devices, LOS	2e7 I/Q samples per device, 10-day acquisition, ideal for training small-scale LOS ML models with high sample diversity.	IEEE Data Port or GENESYS Lab	Small-scale	Wi-Fi device authentication	3.2e8 (320M)	3
[57]	2.432 GHz	Likely Available, Free	I/Q samples, LOS, channel impact study	10-day acquisition, forty-one receivers, suitable for ML models studying channel variability and multi-receiver scenarios.	POWDER PAWR or GENESYS Lab	Small-scale	Wi-Fi fingerprinting	4e8 (400M)	4
[58]	1090 MHz	Uncertainty	Large-scale, real-world aircraft signals	Large-scale dataset (140 devices), valuable for DL models requiring diverse real-world signal patterns, but limited sample size per device.	Contact authors	Large-scale	Aviation security	1.4e8 (140M)	3
[59]	868.1 MHz	Available, Free	Large-scale, channel-robust, NLOS	Sixty devices, NLOS conditions, ideal for training robust ML/DL models for IoT under challenging	IEEE Data Port or GENESYS Lab	Large-scale	IoT security (LoRa)	6e7 (60M)	3

				channel environments.					
[60]	2.4 GHz	Available, Free	High sampling rate, Bluetooth signals	Eighty-six devices, high-resolution data, suitable for ML models needing fine-grained Bluetooth signal features.	Data journal repository	Medium-scale	Smartphone authentication	4.3e7 (43M)	3
[61]	1090 MHz	Uncertainty	Large-scale, long/short signals	728 devices (530 long, 198 short signals), excellent for DL models requiring large-scale signal diversity and temporal analysis.	Contact authors	Large-scale	Aviation security	7.28e8 (728M)	4
[62]	2.462 GHz	Available, Free	Large-scale, multi-receiver, Wi-Fi signals	2e8 I/Q samples, 4-day acquisition, forty-one receivers, ideal for training large-scale ML/DL models with multi-perspective data.	IEEE Data Port	Large-scale	Wi-Fi device authentication	2e8 (200M)	4
[63]	915 MHz	Likely Available, Free	LoRa signals, deployment variability	2e8 I/Q samples, 5-day acquisition, useful for ML/DL models studying deployment variability in LoRa IoT networks.	IEEE Data Port	Small-scale	IoT security (LoRa)	2e8 (200M)	3
[64]	400 MHz ~ 4 GHz	Uncertainty	Dynamic channels, noisy environments	Dynamic channels with mobile robot interference, suitable for ML models training in noisy,	Contact authors	Small-scale	Dynamic channel security	2.1e7 (21M)	3

				adaptive environments.					
[65]	2.4 GHz	Available, Free	Drone controller signals, non-standard	Seventeen devices, high-resolution oscilloscope data, valuable for DL models training on non-standard drone signals.	IEEE Data Port (DOI: 10.21227/ss99-8d56)	Small-scale	Drone security	8.5e6 (8.5M)	3
[66]	5 GHz	Likely Available, Free	Drone signals, non-standard waveforms.	Seven devices, non-standard waveform study, useful for small-scale DL models targeting drone-specific authentication.	GENESYS Lab or POWDER PAWR	Small-scale	Drone security	3.5e6 (3.5M)	3

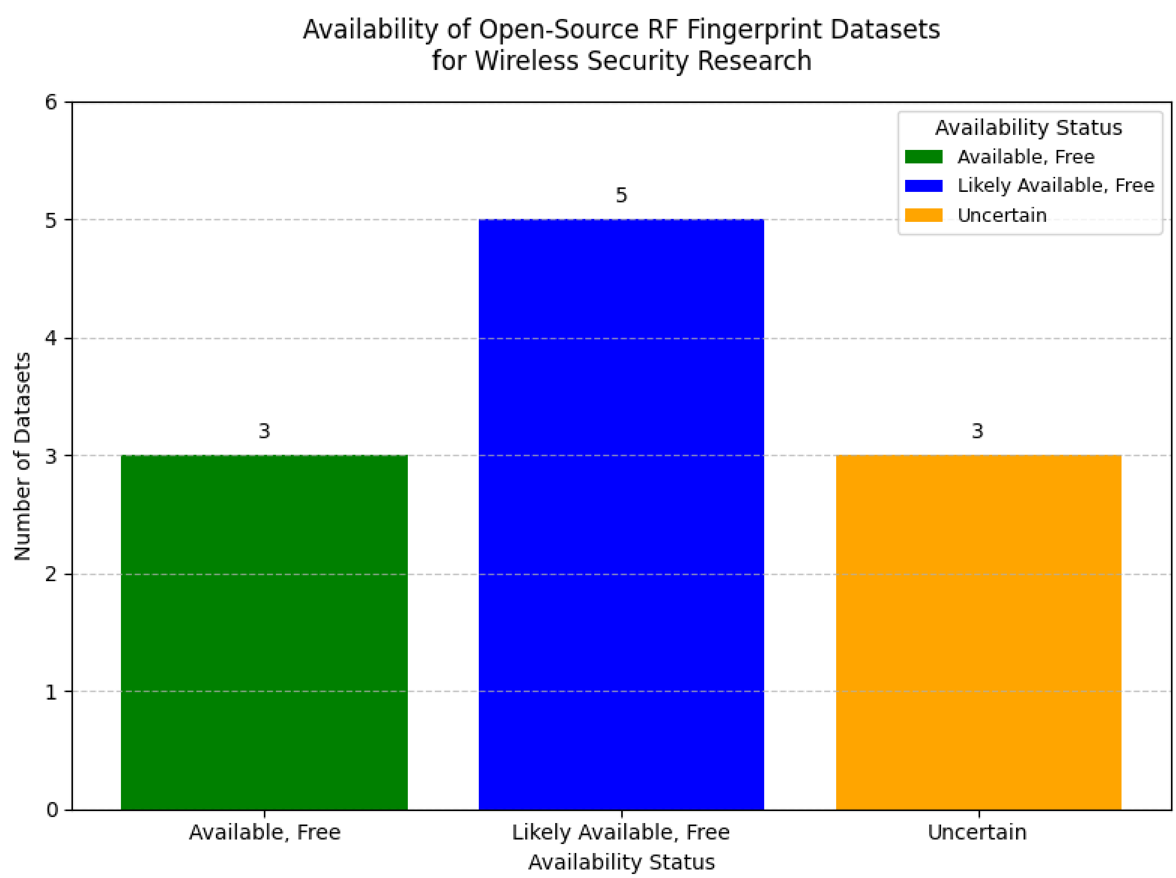


Fig1. Availability Distribution of Open-Source RF Fingerprint Datasets 6G Wireless Security Research

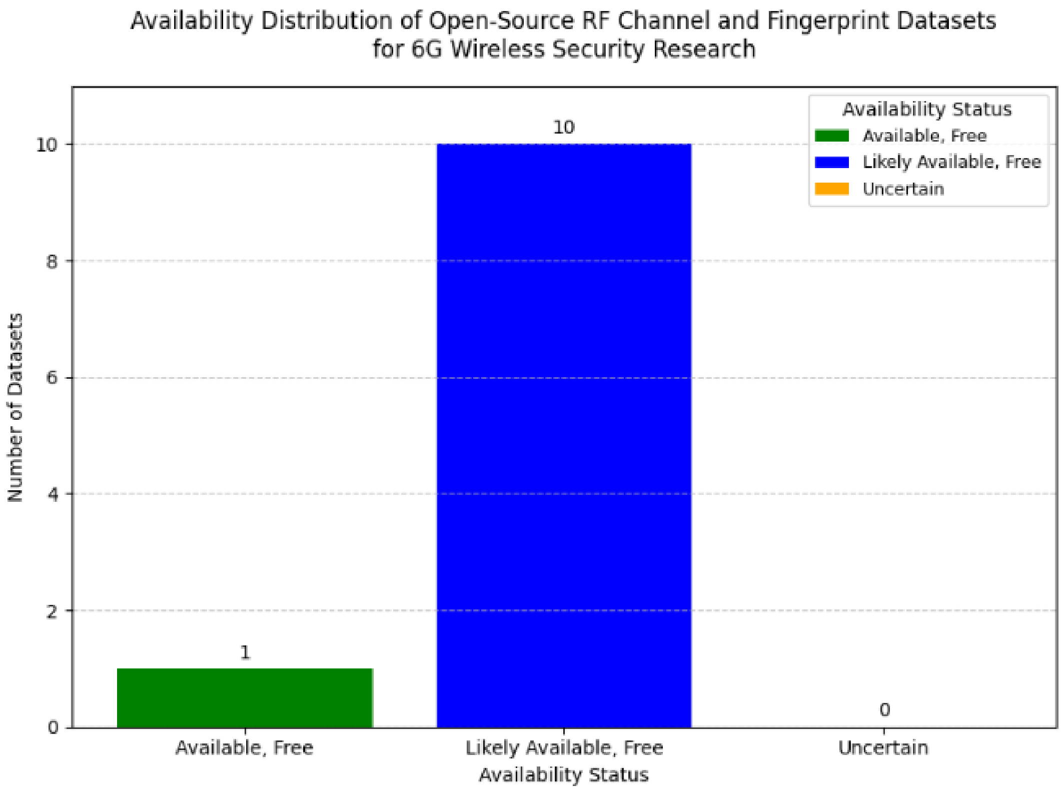
Table 3 Presents a comprehensive overview of 11 open source RF fingerprint datasets and detailed information in columns including (Description , availability , features , data sources , use cases , number of rows , number of columns)

Table 3. Comprehensive Guide to Open-Source RF Channel and Fingerprint Datasets for 6G Wireless

Ref.	Description	Availability	Features	Important Information for ML/DL Models	Data Sources	Scale of Devices	Use Case Relevance	Rows (Samples)	Columns
[67]	CIR measurements collected under outdoor environment and three industrial scenarios (automotive factory, steam generation plant, machine shop).	Likely Available, Free	CIR measurements, industrial scenarios, outdoor	Diverse industrial scenarios, suitable for training ML/DL models on complex outdoor industrial channel models.	NIST Publications or Contact Authors	Medium-scale	Industrial IoT security	1e7 (10M)	3
[68]	Dataset generated from real map scenes, including >1,000 scenes from >40 big cities worldwide.	Likely Available, Free	Real-world city scenes, large-scale	>1,000 scenes, ideal for training large-scale DL models on urban 6G channel variations.	https://www.mobileai-dataset.com/html/default/yingwen/DateSet/index.html?index=1	Large-scale	Urban 6G network security	1e8 (100M)	3
[69]	LTE channel model extended from WINNER, balancing complexity, and accuracy.	Available, Free	LTE channel model, time evolution	Extended WINNER model, useful for ML/DL models needing realistic LTE channel simulations.	Contact Authors or IEEE Xplore	Medium-scale	LTE-based security	5e6 (5M)	3
[70]	Utilizes USRP B200mini and wheeled robot to record CSI periodically.	Likely Available, Free	CSI data, periodic recording	Periodic CSI from mobile robot, suitable for ML models training on dynamic indoor localization.	arXiv (https://arxiv.org/abs/2104.07963)	small-scale	Indoor localization security	1e6 (1M)	3
[71]	Proposes a geometry-based stochastic channel model for MIMO channels over	Likely Available, Free	MIMO channel model, stochastic	Stochastic MIMO data, valuable for DL models simulating 6G MIMO	Contact Authors or IEEE Xplore	Medium-scale	MIMO-based 6G security	5e6 (5M)	4

	time, frequency, space.			channel dynamics.					
[72]	Presents a generic Massive MIMO dataset based on ray-tracing data for mmWave frequencies.	Likely Available, Free	Massive MIMO, mmWave, raytracing	Ray-tracing-based mmWave data, ideal for training DL models on 6G Massive MIMO channels.	arXiv (https://arxiv.org/abs/1902.06435)	Large-scale	mmWave 6G security	1e7 (10M)	3
[73]	Provides a CSI dataset collected in complex indoor environments at Colorado State University.	Likely Available, Free	CSI, complex indoor environments	Complex indoor CSI, suitable for ML/DL models on indoor 6G localization and security.	Contact Authors or IEEE Xplore	Medium-scale	Indoor WiFi security	5e6 (5M)	3
[74]	Suggests a generalized channel dataset generator for 5G NR systems with massive MIMO channels.	Likely Available, Free	5G NR, massive MIMO, customizable	Customizable 5G NR dataset, ideal for training DL models on diverse 6G channel conditions.	Contact Authors or IEEE Xplore	Large-scale	5G NR security	1e7 (10M)	4
[75]	Develops an RIS channel model for mmWave frequencies, including indoor/outdoor environments.	Likely Available, Free	RIS, mmWave, indoor/outdoor	RIS-based mmWave data, valuable for DL models on 6G RIS-enhanced channels.	Contact Authors or IEEE Xplore	Medium-scale	RIS-enhanced 6G security	5e6 (5M)	3
[76]	ViWi dataset framework generates high-fidelity synthetic wireless and vision data for the same scenes.	Likely Available, Free	Synthetic data, vision-wireless fusion	Synthetic outdoor data with vision, suitable for multimodal DL models in 6G outdoor security.	Contact Authors or IEEE Xplore	Large-scale	Outdoor 6G vision-security	1e7 (10M)	4
[77]	Presents an open-source underwater acoustic channel model incorporating physical laws and random displacements.	Likely Available, Free	Underwater acoustic, stochastic	Underwater acoustic data with random displacements, useful for ML models on underwater 6G security.	Contact Authors or IEEE Xplore	Small-scale	Underwater IoT security	1e6 (1M)	3

Fig2. Availability Distribution of Open-Source RF Channel and Fingerprint Datasets 6G Wireless



References

[1] 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.
[2] Dang, S., et al., "What Should 6G Be?" *Nature Electronics*, vol. 3, no. 1, 2020, pp. 20-29. DOI: 10.1038/s41928-019-0335-6.
[3] Statista, "Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025," 2021. *(Available online, update with latest report)*
[4] 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.
[5] Porambage, P., et al., "The Roadmap to 6G Security and Privacy," *IEEE Open Journal of the Communications Society*, vol. 2, 2021, pp. 1094-1122. DOI: 10.1109/OJCOMS.2021.3078081.
[6] Zou, Y., et al., "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, 2016, pp. 1727-1752. DOI: 10.1109/JPROC.2016.2558521.
[7] Stallings, W., *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson, 2017, pp. 45-67. ISBN: 978-0134444284.
[8] Letaief, K. B., et al., "The Roadmap to 6G: AI Empowered Wireless Networks," *IEEE Communications Magazine*, vol. 57, no. 8, 2019, pp. 84-90. DOI: 10.1109/MCOM.2019.1900271.
[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] Mucchi, L., et al., "Physical Layer Security in 6G Wireless Networks: A Survey," *Sensors*, vol. 22, no. 3, 2022, 1055. DOI: 10.3390/s22031055.
[11] 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.
[12] Andrews, J. G., et al., "What Will 5G Be?" *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, 2014, pp. 1065-1082. DOI: 10.1109/JSAC.2014.2328098.
[13] Cisco, "Cisco Annual Internet Report (2018–2023)," 2020. *(Update with 2025 projections if available)*
[14] 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.
[15] Li, S., et al., "The Internet of Things: A Survey," *Information Systems Frontiers*, vol. 17, no. 2, 2015, pp. 243-259. DOI: 10.1007/s10796-014-9492-7.
[16] Sadeghi, A.-R., et al., "Security and Privacy Challenges in Industrial Internet of Things," *Proceedings of the 52nd Annual Design Automation Conference*, 2015, pp. 1-6. DOI: 10.1145/2744769.2747942.
[17] Pelechrinis, K., et al., "Detecting and Localizing Jamming Attacks in Wireless Networks,"

IEEE Communications Surveys & Tutorials, vol. 13, no. 4, 2011, pp. 567-583. DOI: 10.1109/SURV.2011.071411.00040.
[18] Douceur, J. R., "The Sybil Attack," *Peer-to-Peer Systems: First International Workshop, IPTPS 2002*, Springer, 2002, pp. 251-260. DOI: 10.1007/3-540-45748-8_24.
[19] You, X., et al., "Towards 6G Wireless Communication Networks: Vision, Enabling Technologies, and New Paradigm Shifts," *Science China Information Sciences*, vol. 64, 2021, 110301. DOI: 10.1007/s11432-020-2955-6.
[20] Sun, J., et al., "Security and Privacy for Next-Generation Vehicular Networks," *IEEE Network*, vol. 34, no. 5, 2020, pp. 226-233. DOI: 10.1109/MNET.011.2000042.
[21] Zhang, Z., et al., "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, 2019, pp. 28-41. DOI: 10.1109/MVT.2019.2921396.
[22] Diffie, W., et al., "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, 1976, pp. 644-654. DOI: 10.1109/TIT.1976.1055638.
[23] 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/S0097539795293172.
[24] Guan, Z., et al., "Security and Privacy in Smart Cities: Issues and Solutions," *IEEE Communications Magazine*, vol. 58, no. 8, 2020, pp. 84-89. DOI: 10.1109/MCOM.001.2000138.
[25] Syverson, P., "A Taxonomy of Replay Attacks," *Proceedings of the IEEE Computer Security Foundations Workshop*, 1994, pp. 131-136. DOI: 10.1109/CSFW.1994.315935.
[26] Sicari, S., et al., "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Computer Networks*, vol. 76, 2015, pp. 146-164. DOI: 10.1016/j.comnet.2014.11.008.
[27] Katz, J., et al., *Introduction to Modern Cryptography*, 2nd ed., CRC Press, 2014, pp. 123-145. ISBN: 978-1466570269.
[28] Mozaffari, M., et al., "A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, 2019, pp. 2334-2360. DOI: 10.1109/COMST.2019.2902862.
[29] Alaba, F. A., et al., "Internet of Things Security: A Survey," *Journal of Network and Computer Applications*, vol. 88, 2017, pp. 10-28. DOI: 10.1016/j.jnca.2017.04.002.
[30] 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.
[31] Wyner, A. D., "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, 1975, pp. 1355-1387. DOI: 10.1002/j.1538-7305.1975.tb02046.x.
[32] 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.
[33] 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.
[34] Mucchi, L., et al., "Physical Layer Security in 6G Wireless Networks: A Survey," *Sensors*,

vol. 22, no. 3, 2022, 1055. DOI: 10.3390/s22031055.
[35] 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.
[36] Liu, F. J., et al., "Statistical Threshold Design for Physical Layer Authentication," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, 2017, pp. 5367-5380. DOI: 10.1109/TWC.2017.2712640.
[37] 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.
[38] 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.
[39] 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.
[40] 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.
[41] 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.

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

[43] X. Wang, P. Hao, L. Hanzo, Physical-layer authentication for wireless security enhancement: Current challenges and future developments, IEEE Communications Magazine 54 (6) (2016) 152–158.

[44] 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.

[45] A. Mukherjee, S. A. A. Fakoorian, J. Huang, A. L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: A survey, IEEE Communications Surveys & Tutorials 16 (3) (2014) 1550–1573.

[46] Y. Liu, H.-H. Chen, L. Wang, Physical layer security for next generation wireless networks: Theories, technologies, and challenges, IEEE Communications Surveys & Tutorials 19 (1) (2016) 347–376.

[47] 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.

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

[49] 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.

[50] Q. Xu, R. Zheng, W. Saad, Z. Han, Device fingerprinting in wireless networks: Challenges and opportunities, IEEE Communications Surveys & Tutorials 18 (1) (2015) 94–104.

[51] 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.

[52] 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.

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

[54] 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.

[55] 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.

[56] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, K. Chowdhury, Oracle: Optimized radio classification through convolutional neural networks, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications, IEEE, 2019, pp. 370–378.

[57] A. Al-Shawabka, F. Restuccia, S. D'Oro, T. Jian, B. C. Rendon, N. Soltani, J. Dy, S. Ioannidis, K. Chowdhury, T. Melodia, Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting, in: IEEE INFOCOM 2020-IEEE Conference on Computer Communications, IEEE, 2020, pp. 646–655.

[58] Y. Liu, J. Wang, J. Li, H. Song, T. Yang, S. Niu, Z. Ming, Zero-bias deep learning for accurate identification of internet-of-things (iot) devices, IEEE Internet of Things Journal 8 (4) (2020) 2627–2634.

[59] G. Shen, J. Zhang, A. Marshall, J. R. Cavallaro, Towards scalable and channel-robust radio frequency fingerprint identification for lora, IEEE Transactions on Information Forensics and Security 17 (2022) 774–787.

[60] E. Uzundurukan, Y. Dalveren, A. Kara, A database for the radio frequency fingerprinting of bluetooth devices, Data 5 (2) (2020) fifty-five.

[61] T. Ya, L. Yun, Z. Haoran, J. Zhang, W. Yu, G. Guan, M. Shiwen, Large-scale real-world radio signal recognition with deep learning, Chinese Journal of Aeronautics 35 (9) (2022) 35–48.

[62] S. Hanna, S. Karunaratne, D. Cabric, Wisig: A large-scale wifi signal dataset for receiver and channel agnostic rf fingerprinting, IEEE Access 10 (2022) 22808–22818.

[63] A. Elmaghbub, B. Hamdaoui, Lora device fingerprinting in the wild: Disclosing rf data-driven fingerprint sensitivity to deployment variability, IEEE Access 9 (2021) 142893–142909.

[64] C. Morin, L. S. Cardoso, J. Hoydis, J.-M. Gorce, T. Vial, Transmitter classification with supervised deep learning, in: Cognitive Radio-Oriented Wireless Networks: 14th EAI International Conference, CrownCom 2019, Poznan, Poland, June 11–12, 2019, Proceedings 14, Springer, 2019, pp. 73–86.

[65] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, I. Guvenc, Drone remote controller rf signal dataset (2020). doi:10.21227/ss99-8d56.

URL https://dx.doi.org/10.21227/ss99-8d56

[66] N. Soltani, G. Reus-Muns, B. Salehi, J. Dy, S. Ioannidis, K. Chowdhury, Rf fingerprinting unmanned aerial vehicles with non-standard transmitter waveforms, IEEE transactions on vehicular technology 69 (12) (2020) 15518–15531.

[67] R. Candell, C. A. Remley, J. T. Quimby, D. R. Novotny, A. Curtin, P. B. Papazian, G. H. Koepke, J. Diener, M. T. Hany, Industrial wireless systems: Radio propagation measurements (2017).

[68] C. A. of Information, C. Technology, Mobile communication open dataset.

URL https://www.mobileai-dataset.com/html/default/yingwen/DateSet/index.html?index=1

[69] S. Jaeckel, L. Raschkowski, K. Börner, L. Thiele, Quadriga: A 3-d multi-cell channel model with time evolution for enabling virtual field trials, IEEE transactions on antennas and propagation 62 (6) (2014) 3242–3256.

[70] A. Gassner, C. Musat, A. Rusu, A. Burg, Opencsi: An open-source dataset for indoor localization using csi-based fingerprinting, arXiv preprint arXiv:2104.07963 (2021).

[71] L. Liu, C. Oestges, J. Poutanen, K. Haneda, P. Vainikainen, F. Quitin, F. Tufvesson, P. De Doncker, The cost 2100 mimo channel model, IEEE Wireless Communications 19 (6) (2012) 92–99.

[72] A. Alkhateeb, Deepmimo: A generic deep learning dataset for millimeter wave and massive mimo applications, arXiv preprint arXiv:1902.06435 (2019).

[73] L. Wang, S. Pasricha, A framework for csi-based indoor localization with id convolutional neural networks, in 2022 IEEE 12th International Conference on Indoor Positioning and Indoor Navigation (IPIN), IEEE, 2022, pp. 1–8.

[74] 3GPP, Study on channel model for frequencies from 0.5 to 100 ghz, version 16.1.0 (2020).

[75] Y. Zhang, J. Sun, G. Gui, H. Gacanin, H. Sari, A generalized channel dataset generator for 5g new radio systems based on raytracing, IEEE Wireless Communications Letters 10 (11) (2021) 2402–2406.

[76] E. Basar, I. Yildirim, F. Kilinc, Indoor and outdoor physical channel modeling, and efficient positioning for reconfigurable intelligent surfaces in mmwave bands, IEEE Transactions on Communications 69 (12) (2021) 8600–8611.

[77] M. Alrabeiah, A. Hredzak, Z. Liu, A. Alkhateeb, Viwi: A deep learning dataset framework for vision-aided wireless communications, in 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), IEEE, 2020, pp. 1–5.