This paper has been accepted for publication on IEEE Military Communications Conference (MILCOM 2025). This is the author's accepted version of the article. The final version published by IEEE is CP. Robinson, S. D'Oro, and T. Melodia, "*VeriPHY:* Physical Layer Signal Authentication for Wireless Communication in 5G Environments," Proc. of *IEEE Military Communications Conference (MILCOM)*, Los Angeles, CA, USA, 2025.

VeriPHY: Physical Layer Signal Authentication for Wireless Communication in 5G Environments

Clifton Paul Robinson, Salvatore D'Oro, and Tommaso Melodia
Institute for the Wireless Internet of Things, Northeastern University, Boston, MA, USA
Email: {cl.robinson, s.doro, t.melodia}@northeastern.edu

arXiv:2508.09213v1 [cs.CR] 11 Aug 2025

***Abstract*—Physical layer authentication (PLA) uses inherent characteristics of the communication medium to provide secure and efficient authentication in wireless networks, bypassing the need for traditional cryptographic methods. With advancements in deep learning, PLA has become a widely adopted technique for its accuracy and reliability. In this paper, we introduce *VeriPHY*, a novel deep learning-based PLA solution for 5G networks, which enables unique device identification by embedding signatures within wireless I/Q transmissions using steganography. *VeriPHY* continuously generates pseudo-random signatures by sampling from Gaussian Mixture Models whose distribution is carefully varied to ensure signature uniqueness and stealthiness over time, and then embeds the newly generated signatures over I/Q samples transmitted by users to the 5G gNB. Utilizing deep neural networks, *VeriPHY* identifies and authenticates users based on these embedded signatures. *VeriPHY* achieves high precision, identifying unique signatures between 93% and 100% with low false positive rates and an inference time of 28 ms when signatures are updated every 20 ms. Additionally, we also demonstrate a stealth generation mode where signatures are generated in a way that makes them virtually indistinguishable from unaltered 5G signals while maintaining over 93% detection accuracy.**

I. Introduction

Physical Layer Security (PLS) is crucial in modern communication systems for securing information starting from the RF domain. Within PLS, Physical Layer Authentication (PLA) is an important component to verify the legitimacy of communication entities based on their unique physical characteristics [1]. As wireless networks and the number of devices continue to grow, developing robust PLA mechanisms is increasingly vital to combat unauthorized access and maintain data integrity [2]. Various PLA solutions have been developed over the years [3], including challenge-response protocols based on physical layer parameters, fingerprinting based on hardware imperfections, and RFID-based methods using unique tag responses. These methods form the foundation for advanced PLA in modern communication systems, which ideally exhibit three key characteristics [2]: **covertness**, ensuring undetectability by unauthorized entities; **robustness**, maintaining functionality in adverse conditions; and **security** against breaches.

As 5th generation mobile networks (5Gs) expand to support a vast ecosystem of devices and applications, PLA becomes critical for ensuring secure, reliable communication [3]. By verifying device identity and integrity at the physical layer, PLA mitigates risks from unauthorized access, cyber threats, and misuse of limited radio resources, thereby safeguarding 5G infrastructure and users [3].

This work was partially funded by the U.S. National Science Foundation under grants CNS-1925601 and CNS-2112471.

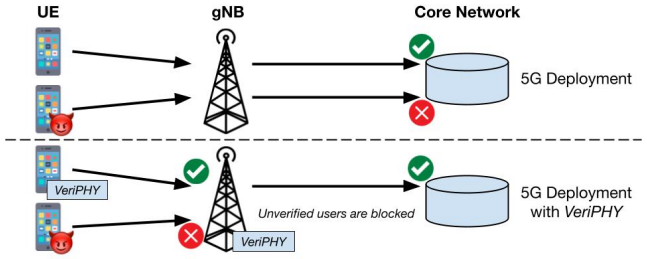


Fig. 1: Comparison of authentication in traditional 5G networks (top) vs. *VeriPHY* (bottom), which blocks unauthorized core access at the physical layer.

Effective PLA designs must address challenges such as accurate device identification, spoofing resistance, and real-time processing. The rise of Deep Learning (DL), particularly Convolutional Neural Networks (CNNs), has advanced the field by enabling adaptive, robust, and efficient authentication [4]. CNNs enhance PLA by distinguishing legitimate from illegitimate signals, adapting to dynamic conditions, and handling complex data with high accuracy. For example, PAST-AI [5] used CNNs to authenticate satellite transducers with up to 100% accuracy, while [6] demonstrated effective node authentication and spoofing detection in wireless sensor networks. These approaches highlight the potential of DL-based methods for practical, real-world PLA deployment.

To achieve covertness in PLA systems, steganography can be used as a way to hide authentication-related data and procedures behind overt data, i.e., data that any node can eavesdrop and decode, such as wireless signals [3]. This approach enhances security by embedding authentication messages within intelligible transmissions that only apparently do not carry any security-related data, thus thwarting interception or tampering [7]. The use of wireless signatures [1, 8], on the other hand, is another approach that relies on unique signal characteristics like variations in strength, timing, or frequency response to authenticate devices to create unique wireless fingerprints. Combining steganography with wireless signatures fortifies PLA systems with dual-layer security through covert data embedding and distinct signal attributes.

In this paper, we present *VeriPHY*, a novel Physical Layer Authentication (PLA) solution for 5G that generates continuously pseudo-random and unique device signatures via

©2025 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

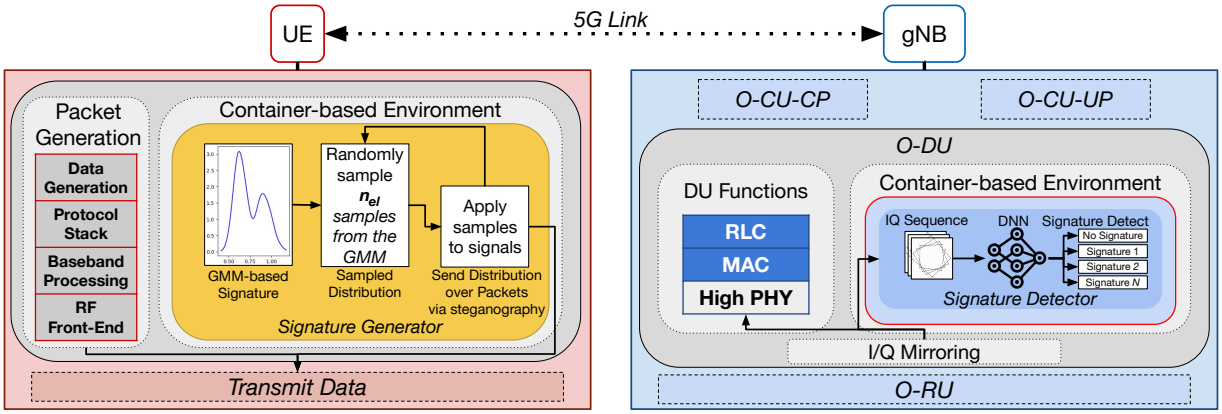


Fig. 2: The high-level design *VeriPHY* in both the User Equipment (UE) and gNB describing how the UE generates the signatures to transmit with their packets and how the gNB uses I/Q mirroring to process and detect potential user signatures continuously throughout communication transmissions.

steganography in wireless I/Q transmissions. *VeriPHY* uses DL-based CNNs to analyze I/Q samples in real time, allowing accurate physical layer authentication and blocking unauthorized users before their attachment requests reach the core network. As shown in Fig. 1, unlike standard 5G procedures that detect unauthorized users at the core, *VeriPHY* intercepts them at the Next Generation Node Base (gNB), enhancing early threat mitigation. Its embedded PLS mechanisms resist identity spoofing, preventing even advanced attackers (e.g., those cloning IMSIs) from replicating device signatures. This strengthens security by ensuring only legitimate devices access 5G resources.

Novel contributions: the important technical contributions of the paper can be summarized as follows:

1) We introduce *VeriPHY*, a novel DL-based 5G PLA solution that enables multi-UE identification by embedding wireless signatures into I/Qs using steganography;
2) We utilize Gaussian Mixture Models (GMMs) to generate pseudo-random unique signatures for each device that cannot be replicated or forged. This randomization guarantees signature uniqueness and enhances the overall security of the *VeriPHY* system;
3) We demonstrate that our trained Deep Neural Networks (DNNs) can accurately detect unique signatures with 93%-100% accuracy and low false positives, achieving detection times as low as 6.5 ms when signatures are sent every 1 ms (below the 5G NR frame duration of 10 ms) and 25.5 ms when sent every 20 ms;
4) We also introduce a ***stealth mode***, where *VeriPHY* 's signatures are altered via a pre-processing function to be practically indistinguishable from standard 5G signals, yet remain detectable by DNNs with over 93% accuracy.

II. Related Work

Physical Layer Authentication (PLA) has emerged as a key technology for enhancing wireless security in 5G by leveraging physical layer attributes, addressing current limitations such as susceptibility to spoofing and unauthorized access, and integrating with existing infrastructure [8]. PLA and security offer a promising approach to safeguard wireless communications by leveraging the randomness and stochasticity of channels, serving as an alternative to complex cryptographic techniques [8].

A key aspect of PLA is authenticating users and devices via unique physical-layer signatures. [9] proposes a method using helper nodes with channel-derived cryptographic signatures for authentication. *SteaLTE* [7] applies wireless steganography to embed data covertly in cellular traffic without degrading performance. In [10], probabilistic modeling of the channel and Gaussian Mixture Models (GMMs) are used to detect spoofing attacks, showing improved detection accuracy.

In [9], the authors introduce an FCC-compliant authentication method for primary users that combines cryptographic and wireless link signatures, using a nearby helper node to authenticate signals without training. [11] presents a GMM-based semi-supervised technique for channel-based authentication, achieving high detection with low false alarms and adapting to network changes without prior intruder data. [12] proposes a real-time anomaly detection framework for 5G RRC-layer vulnerabilities, leveraging Artificial Intelligence (AI) to analyze PHY and cross-layer features. Validated in emulated and real environments, it achieved over 85% detection accuracy with low latency, making it suitable for Open RAN deployment.

In the context of PLA and PLS, deep learning has become a popular method in classifying the wireless spectrum through DNNs. In [13], the authors investigate attacks on CNN-based device identification, proposing evaluation indicators to improve assessment. Higher perturbation levels and iteration steps degrade accuracy, providing insights for resilient DL-based Internet of Things (IoT) systems. [14] proposes a DNN approach using CNNs and DNNs to classify multiple signals in shared-spectrum networks using I/Q samples, validated experimentally with USRP radios. [15] proposes an intrusion detection system for wireless networks, employing feature selection algorithms with conditional random fields and linear correlation coefficients, integrated with CNNs for classification, achieving a validated 99% detection accuracy via tenfold cross-validation.

VeriPHY differs from the literature above as it introduces a novel approach for device authentication via physical layer steganography, embedding ever changing signatures directly

into transmitted packets. Unlike [7], which uses steganography at the application layer, and [9], which requires an additional node, *VeriPHY* streamlines authentication between UEs and gNBs using unique user signatures at the physical layer, which can be hidden using a stealth mode activated by network operators. This advancement integrates PLA into 5G networks, highlighting the importance of high-accuracy signature authentication that can be concealed from eavesdroppers.

III. *VeriPHY* Signature Framework

VeriPHY's architecture is illustrated in Fig. 2. Due to space limitations, in Fig. 2 and in the following we focus on the case where signatures are generated by UEs and retrieved at the gNB. However, we would like to mention that *VeriPHY* is designed to support the execution of signature detection (left) and generation (right) modules at both 5G UEs and gNB, thus providing a framework for mutual authentication between both parties. In the above case, *VeriPHY* uses two container-based environments: the Signature Generator in the UE for generating user signatures, and the Signature Detector in the gNB, which uses a trained DNN to identify these signatures from I/Q samples. Thanks to the cloud-native design, the Signature Detector and Generator can be deployed at both the UE and gNB as software modules running as microservices and containers. This enhances flexibility and scalability, simplifying deployment, management, and integration in diverse environments.

The following subsections detail both components: Subsection III-A covers the Signature Generator, including how it creates and sends signatures, while Subsection III-B explains how the Signature Detector uses DL to detect and verify them.

A. Signature Generator

The Signature Generator creates and stores unique user signatures essential for secure transmission and authentication. Embedded via steganography in I/Q data, these signatures form patterns detectable by allies but difficult for adversaries to replicate or detect. This enhances security across the 5G transceiver chain without disrupting normal operations, enabling fast detection and robust protection.

In a *VeriPHY*-enabled 5G deployment, each User Equipment (UE) holds a unique GMM-based signature distribution. A signature is generated by sampling n_{el} samples from the UE-specific GMM distribution and transmitted every t ms by embedding it on top of user data via wireless steganography as we will describe in detail in Section IV. Since signatures continuously change every few milliseconds (e.g., our prototype updates signatures every 20ms, i.e., 2 5G frames) by randomly sampling from the originating GMM, it is hard for attackers to replicate signatures as they would need (i) to know the underlying generating GMM while only having access to a few samples that change over time; or (ii) a significant computational effort and amount of time to observe the network. Moreover, since signatures are updated every few tens of milliseconds, *VeriPHY* can detect replay attacks by identifying retransmissions of previously used signatures, thus alerting the system regarding ongoing attacks.

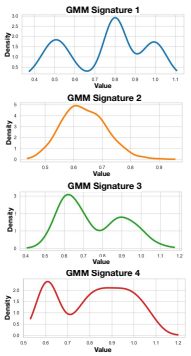


Fig. 3: PDFs of four GMM signatures.

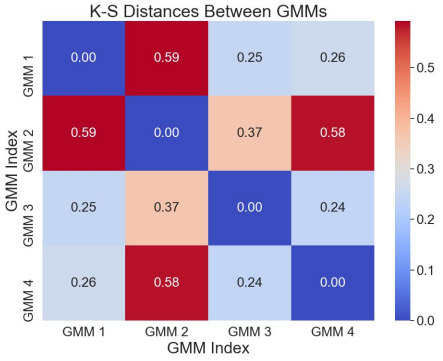


Fig. 4: Confusion matrix of pairwise Kolmogorov-Smirnov (K-S) distances between the four GMMs in Fig. 3.

B. Signature Detector

The Signature Detector receives I/Q data via an I/Q mirroring technique, which replicates I/Q samples across device modules—such as DU Functions and the Signature Detector—enabling asynchronous processes to run in parallel without service interruption [16]. This detector integrates a DL-based DNN to identify and verify signatures in the mirrored I/Q samples. As shown in Fig. 2, I/Q data is simultaneously routed to standard Next Generation Node Base (gNB) functions and the Signature Detector for real-time user authentication.

The Signature Detector flags transmissions based on signature presence. Thus, *VeriPHY* can block authentication requests without valid signatures, preventing unauthorized core network access when stricter security is needed.

IV. Generating and Applying Unique Signatures

In our work, we create uniquely identifiable signatures by generating a set of Gaussian Mixture Models (GMMs) that are significantly different from each other. We achieve this by setting a minimum Kolmogorov-Smirnov (K-S) distance of ϵ between each GMM. The K-S distance measures the maximum difference between the Cumulative Distribution Function (CDF) of these distributions and is an indicator for their similarity. By setting a minimum distance ϵ, we ensure minimal overlap, making each signature distinct.

A. Generating Gaussian Mixture Model Signatures

To generate uniquely identifiable signatures, *VeriPHY* uses GMMs that are sufficiently distinct from one another based on a minimum K-S distance threshold $\epsilon > 0$. The user specifies the

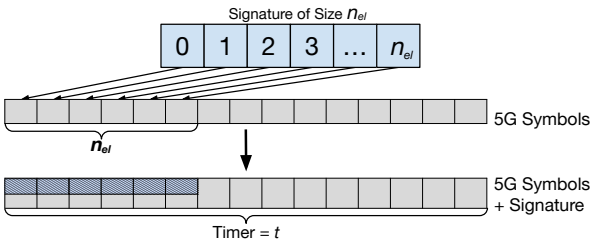


Fig. 5: Visualization of how a signature of size n_{el} is sent sequentially over the specified timer t.

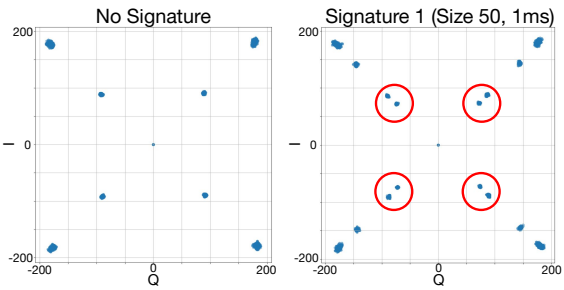


Fig. 6: I/Q constellation comparison with and without signature embedding. The left shows the unmodified signal, while the right displays the same signal with an embedded signature (Signature 1, Size 50, Duration 1 ms).

number of signatures N (e.g., number of UEs), the perturbation value range $[m_{min}, m_{max}]$, and the maximum number of components p per model. Each GMM is generated with randomized peaks and accepted only if its K-S distance from all previously generated models exceeds ϵ. This ensures that all N signatures are statistically distinguishable, enhancing robustness and minimizing overlap. Once the GMMs are generated, they are exported to the Signature Generators.

For signature generation, we set the GMM range to $[0.5, 1]$ to avoid excessive alteration of I/Q samples, leveraging normalization where 1 and 0.5 represent full and half signal levels, respectively. A K-S distance threshold of $\epsilon > 0.2$ was chosen to ensure sufficient distinctiveness between models while maintaining generation feasibility. It is worth mentioning that higher ϵ values enforce differentiation across signatures, but might lead to excessive rejections during model creation, making the process longer. However, unless GMMs need to be generated in real-time, this problem can be neglected in most scenarios.

Fig. 3 shows the Power Spectral Densities (PSDs) of four generated GMM signatures, each exhibiting a distinct profile. Their pairwise K-S distances, shown in Fig. 4, range from 0.24 to 0.59, confirming that the signatures are well-separated and sufficiently dissimilar for robust use in *VeriPHY*.

B. Apply Signatures with Wireless Steganography

To transmit signatures via steganography, a communication channel within the UE or gNB injects sampled GMM distributions on top of user data. Each signature of size n_{el} is sent element by element, followed by a t-millisecond delay before the next transmission. Fig. 5 illustrates this sequence.

To enhance signature uniqueness and concealment, we implement two mechanisms: **(1)** each transmission uses a newly sampled signature from the GMM, making replication possible only for those with access to the model, and **(2)** randomization and a binary switch determine whether to transmit a signature, preventing pattern inference and reconstruction of the underlying distribution. This ensures each transmission follows a uniquely unpredictable pattern.

Transmitting signatures as-is may expose covert activity, as experts could detect anomalies in the I/Q plot. Fig. 6 compares 1 ms of normal (left) and signature-embedded (right) transmissions, with red circles highlighting I/Q alterations. This compromises the covertness essential to advanced PLA systems. To address this, we introduce a stealth mode that preserves signature uniqueness while better concealing their presence.

Stealth Mode with Signature Scaling: To reduce the detectability of GMM signatures, we apply a scaling factor during their generation and embedding, ensuring that modified I/Q samples remain close to the original signal. As shown in Fig. 7, scaled signatures blend seamlessly into the transmission. During transmission (Fig. 5), each I/Q value is scaled to match typical patterns. Without scaling (Fig. 6), signatures are distinct and may reveal user-specific traits. With stealth mode, these differences are minimized, making the signatures nearly indistinguishable from standard traffic, enabling covert yet effective physical-layer authentication.

Another risk to covertness is detection through energy analysis. We compare the Cumulative Distribution Functions (CDFs) of unaltered and scaled GMM signatures against standard I/Q samples (no signature) in Fig. 8. Unaltered signatures show clear deviations from the baseline, revealing energy-level differences. In contrast, scaled signatures closely match the baseline CDF, making them harder to distinguish. This demonstrates that scaling effectively preserves the signal's energy profile, enhancing stealth and overall security.

In Section VI-D, we will show that we can still guarantee 95% accuracy even if stealth mode is active.

V. *VeriPHY* Prototype

We implement our *VeriPHY* prototype on the OpenAirInterface (OAI) RFSim, utilizing its features to simulate realistic 5G network conditions and interactions. To evaluate the capabilities of both the Signature Generator and Detector, we conduct five experiments with varying signature sizes (n_{el}) and transmission intervals (t), and test two different models to assess signature detection. Details of our testbed implementation are provided in V-A, our DL models are described in V-B, and our experimental datasets are discussed in V-C.

A. OpenAirInterface 5G Platform Implementation

OpenAirInterface (OAI) serves as the implementation environment for demonstrating *VeriPHY* within 5G networks [17]. This platform provides an end-to-end, 3GPP-compliant implementation of both the 5G Radio Access Network (RAN) and core network, making it an ideal choice for prototyping and data collection. By leveraging the OAI RFSim, which creates a channel with a bandwidth of 40 MHz on 5G band

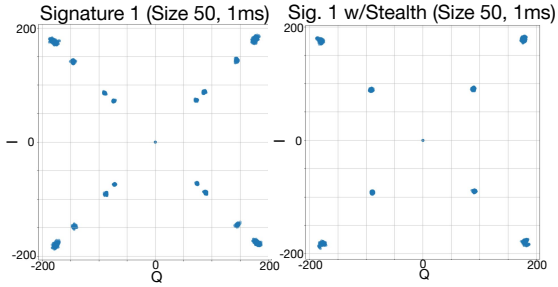


Fig. 7: Effect of stealth mode on signal visibility. The left shows a signal with Signature 1 embedded without stealth mode, where the signature is visibly distinguishable. The right shows the same signature with stealth mode applied, significantly obscuring its presence.

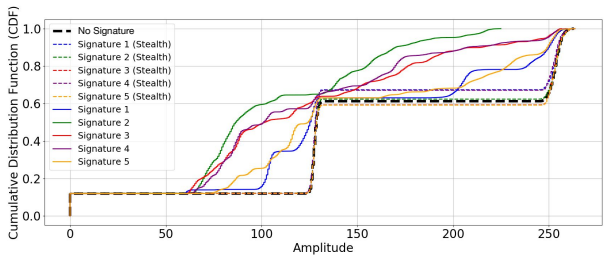


Fig. 8: Plot of the Energy CDFs for all signatures, comparing results with and without the use of the signature stealth mode against a transmission without any signal present.

78, we can thoroughly test and refine the system's performance and features in a controlled environment. This flexible setup allows for the integration of various components and testing of different configurations, ensuring that our prototype can adapt to diverse deployment scenarios within 5G networks.

B. Deep Neural Networks for Signature Detection

To implement the Signature Detector, we employ VGG16 [18] and SENet [19]. Originally designed for image recognition, VGG16 is well-suited for capturing complex 2D I/Q constellation patterns through deep convolutional layers, making it a popular choice for RF signal analysis. SENet enhances performance by applying channel-wise attention to emphasize key spectral features and is known for low false positive rates in signal classification. We use 2D inputs formed from I/Q groups extracted from OAI, which stores 60 samples per group (0.028ms). To analyze 1 ms of data, we require 2160 samples, resulting in an input shape of $(N, 60, 36, 2)$, where N is the number of training examples. This setup aligns with RFSim sampling intervals for accurate 5G signal simulation.

VGG16 is a deep CNN with 16 layers and small 3x3 filters, known for strong feature extraction. When adapted for spectrum-based classification with 2D I/Q inputs, VGG16 can recognize complex frequency components and temporal variations, making it well-suited for leveraging spatial and spectral correlations. Squeeze-and-Excitation Networks (SENet) improvew representational power by modeling interdependencies between channels using a "squeeze" and "excitation" mechanism. This aggregates spatial information into channel-wise statistics and dynamically re-weights features, boosting sensitivity to key spectral and temporal patterns. Applied to 2D I/Q inputs, SENet enhances classification accuracy and reduces false-alarms through more precise feature emphasis.

C. Dataset Generation

To train our DL models, we generate datasets with enough diversity to ensure accurate training of Deep Neural Networks (DNNs) while avoiding overfitting or underfitting. Using our OpenAirInterface (OAI) implementation, we created five unique datasets, each with different signature sizes and send rates, and five signatures per dataset. The datasets were generated using OAI's RFSimulator to model a 40 MHz bandwidth channel on 5G band 78. We implemented a system to manage the storage of I/Q data from RFSim, optimizing file size and organization during post-processing. The signatures, generated with GMMs to have a K-S distance of at least 0.2 for uniqueness, were consistent across all datasets, which included the following parameters: **(1)** $n_{el} = 10$, $t = 1\ ms$, **(2)** $n_{el} = 20$, $t = 1\ ms$, **(3)** $n_{el} = 50$, $t = 1\ ms$, **(4)** $n_{el} = 20$, $t = 20\ ms$, and **(5)** $n_{el} = 50$, $t = 20\ ms$. This approach allowed us to test various parameter sets using the same five signatures, ensuring no bias and optimizing the dataset for training.

VI. Experimental Results

In this section, we present results that illustrate *VeriPHY* effectiveness and accuracy. We begin by profiling the accuracy. Next, we address latency aspects to demonstrate real-time inference. Finally, we assess the performance of *VeriPHY* when stealth mode is active.

A. Model Accuracy

For both VGG16 and SENet, five models were trained across different signature deployments. Three tests used signatures sent every 1ms with n_{el} sizes of 10, 20, and 50, while two tests used 20ms intervals with sizes 20 and 50. These configurations are summarized in Table I. The VGG16 model performs well with 100% accuracy and F1 scores of 1.00 for 1ms signatures with sizes 10 and 50 (Fig. 9c). However, performance drops when signatures are sent every 20ms, with accuracy falling to 57.50% and 78.05% for sizes 20 and 50, respectively (Fig. 9d), indicating that the model struggles when the signature becomes a smaller portion of the longer I/Q data.

The SENet model shows strong performance with some variability depending on the configuration. For 1ms signatures, sizes 10 and 20 achieve accuracies of 90.62% and 89.56% (Fig. 9a), with F1 scores of 0.91 and 0.89. However, it excels in more complex scenarios, achieving 100% accuracy and an F1 score of 1.00 for signature size 50 at 1ms, and for 20ms signatures of sizes 20 and 50 (Fig. 9b).

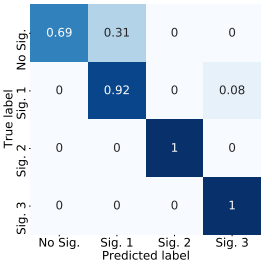
VGG16 performs well with fast signatures (1ms) but has lower performance at 20ms. SENet instead delivers consistent performance across all configurations, making it a more adaptable choice for *VeriPHY*.

B. Model Latency

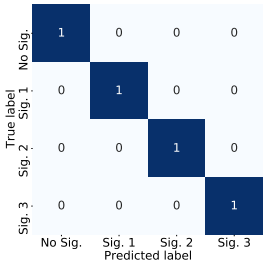
The latency values for the VGG16 and SENet models across varying signal sizes and send intervals demonstrate their computational efficiency. For VGG16, latency remains consistent between 7.36 and 7.41 ms when the send interval is 1 ms, with

TABLE I: Accuracy and F-score metrics for the VGG16 and SENet models across different configurations.

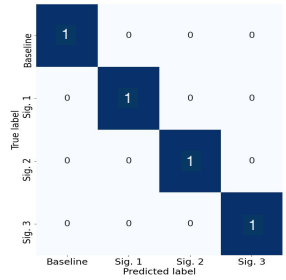
Model	Configuration	Accuracy (%)	F1 Score
VGG16	Sig. Size: 10, time: 1 ms	100	1.00
	Sig. Size: 20, time: 1 ms	99.63	1.00
	Sig. Size: 50, time: 1 ms	100	1.00
	Sig. Size: 20, time: 20 ms	57.50	0.54
	Sig. Size: 50, time: 20 ms	78.05	0.78
SENet	Sig. Size: 10, time: 1 ms	90.62	0.91
	Sig. Size: 20, time: 1 ms	89.56	0.89
	Sig. Size: 50, time: 1 ms	100	1.00
	Sig. Size: 20, time: 20 ms	100	1.00
	Sig. Size: 50, time: 20 ms	100	1.00



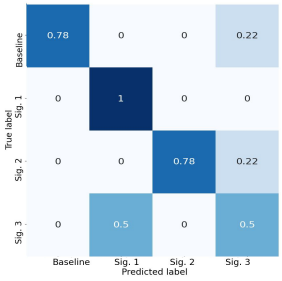
(a) SENet: $n_{el} = 20, t = 1$



(b) SENet: $n_{el} = 20, t = 20$



(c) VGG16: $n_{el} = 50, t = 1$



(d) VGG16: $n_{el} = 50, t = 20$

Fig. 9: Confusion Matrices for four of the trained models across different experimental setups. *(All times, t, reported in milliseconds)*

a slight increase to 7.79 ms at a 20 ms interval. SENet shows similar stability, maintaining latency between 5.29 and 5.36 ms at 1 ms, and rising modestly to 5.32–5.44 ms at 20 ms. Both models handle changes in signal size well, though longer send intervals lead to minor latency increases.

The SENet model consistently shows lower latency than VGG16 across all conditions, suggesting better efficiency for quick-response tasks. Both models exhibit minimal sensitivity to signal size changes but show a slight latency increase with longer send times, highlighting the importance of optimization for real-time applications.

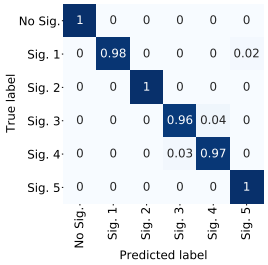
C. VeriPHY Inference Time

Table II shows the inference times for VGG16 and SENet models across all configurations, highlighting the acquisition of signals (I/Q Capture Time), processing, and CNN input times.

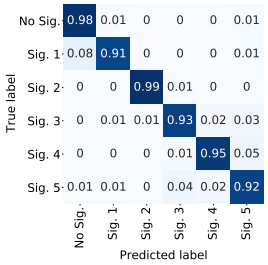
In the 1 ms configuration, VGG16 has a total inference time of 8.562 ms, with 1.00 ms for I/Q capture, 0.037 ms for processing, 0.142 ms for CNN input generation, and 7.377 ms of model latency. In contrast, SENet's total inference time is 6.501 ms, with a model latency of 5.316 ms. For the 20ms configuration, VGG16's total inference time increases to 27.898 ms due to the 20.00 ms I/Q capture time, while processing and CNN input generation remain stable. The model latency slightly rises to 7.712 ms. Similarly, SENet's total inference time increases to 25.564 ms, with model latency at 5.378 ms.

TABLE II: Inference times for models with different time configurations.

Metric	1 ms Configuration	20 ms Configuration
I/Q Capture Time	1.00 ms	20.00 ms
Average Processing Time	0.037 ms	0.038 ms
Average CNN Input Time	0.142 ms	0.147 ms
VGG16 Model Latency	7.377 ms	7.712 ms
VGG16 Total Inference Time	**8.562 ms**	**27.898 ms**
SENet Model Latency	5.316 ms	5.378 ms
SENet Total Inference Time	**6.501 ms**	**25.564 ms**



(a) SENet, 5 Signatures (Normal)



(b) SENet, 5 Signatures (Stealth)

Fig. 10: Confusion matrices: normal vs. stealth *VeriPHY* ($n_{el} = 50$, $t = 50$ ms).

Analyzing the total inference time across signature intervals reveals an important efficiency trade-off. While the 20 ms interval introduces some delay compared to the 1 ms interval, it allows decisions to be made before the I/Q buffer is fully utilized, reducing latency from buffer processing. Therefore, while the 1 ms model has faster inference times, the 20 ms deployment may offer better overall efficiency by optimizing data throughput and minimizing buffer delays.

D. Normal Mode vs Stealth Mode

To evaluate the impact of stealth mode on *VeriPHY* signature detection, we compared detection accuracy using SENet. For a stealth model with $n_{el} = 50$ and $t = 1\ ms$, accuracy drops slightly by 3% to 97%, indicating stealth mode does not significantly disrupt detection.

To further evaluate our stealth mode, we introduced two additional signatures and trained both a standard and a stealth-enhanced model using $n_{el} = 50$ and $t = 1\ ms$. As shown in Fig. 10, there is a slight drop in accuracy from 98.5% in the normal model to 94.6% in the stealth model. Specifically, the accuracy for 'Sig. 1' drops from 0.98 to 0.91 (a 7% decrease), and for 'Sig. 4' from 0.97 to 0.95 (a 2% decrease). Despite this, the stealth model maintains strong classification performance. These results indicate that while stealth characteristics introduce minor degradation, the model remains highly effective and resilient, successfully generalizing to the altered signature patterns with minimal impact on accuracy.

VII. Conclusion

In this paper, we proposed *VeriPHY*, a novel DL-based Physical Layer Authentication (PLA) solution for 5G networks that embeds device signatures into I/Q transmissions using steganography. GMMs generate pseudo-random, uniquely identifiable signatures with distinctiveness ensured by K-S distance, complicating replication. Trained DNNs achieved 93–100% detection accuracy with latencies as low as 6.5 ms. We also introduced a *stealth mode* that conceals signatures while preserving over 93% detection accuracy.

REFERENCES

[1] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authentication in wireless communication networks: A survey," *Journal of Communications and Information Networks*, vol. 5, no. 3, pp. 237–264, Sep. 2020, conference Name: Journal of Communications and Information Networks. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9200889

[2] L. Alhoraibi, D. Alghazzawi, R. Alhebshi, and O. B. J. Rabie, "Physical layer authentication in wireless networks-based machine learning approaches," *Sensors*, vol. 23, no. 4, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/4/1814

[3] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authentication in wireless communication networks: A survey," *Journal of Communications and Information Networks*, vol. 5, no. 3, pp. 237–264, 2020.

[4] L. Alhoraibi, D. Alghazzawi, R. Alhebshi, and O. B. J. Rabie, "Physical Layer Authentication in Wireless Networks-Based Machine Learning Approaches," *Sensors*, vol. 23, no. 4, p. 1814, Jan. 2023, number: 4 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1424-8220/23/4/1814

[5] G. Oligeri, S. Sciancalepore, S. Raponi, and R. D. Pietro, "PAST-AI: Physical-Layer Authentication of Satellite Transmitters via Deep Learning," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 274–289, 2023, conference Name: IEEE Transactions on Information Forensics and Security. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9936663

[6] D. Marabissi, L. Mucchi, and A. Stomaci, "Iot nodes authentication and id spoofing detection based on joint use of physical layer security and machine learning," *Future Internet*, vol. 14, no. 2, 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/2/61

[7] L. Bonati, S. D'Oro, F. Restuccia, S. Basagni, and T. Melodia, "SteaLTE: Private 5G Cellular Connectivity as a Service with Full-stack Wireless Steganography," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, May 2021, pp. 1–10, iSSN: 2641-9874. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9488889

[8] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 152–158, Jun. 2016, conference Name: IEEE Communications Magazine. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7498103

[9] Y. Liu, P. Ning, and H. Dai, "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures," in *2010 IEEE Symposium on Security and Privacy*, May 2010, pp. 286–301, iSSN: 2375-1207. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5504794

[10] X. Qiu, T. Jiang, S. Wu, and M. Hayes, "Physical Layer Authentication Enhancement Using a Gaussian Mixture Model," *IEEE Access*, vol. 6, pp. 53 583–53 592, 2018, conference Name: IEEE Access. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8468974

[11] N. Gulati, R. Greenstadt, K. R. Dandekar, and J. M. Walsh, "GMM Based Semi-Supervised Learning for Channel-Based Authentication Scheme," in *2013 IEEE 78th Vehicular Technology Conference (VTC Fall)*, Sep. 2013, pp. 1–6, iSSN: 1090-3038. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6692216

[12] A. Scalingi, S. D'Oro, F. Restuccia, T. Melodia, D. Giustiniano *et al.*, "Det-ran: Data-driven cross-layer real-time attack detection in 5g open rans," in *IEEE International Conference on Computer Communications*, 2024, pp. 1–10.

[13] Z. Bao, Y. Lin, S. Zhang, Z. Li, and S. Mao, "Threat of Adversarial Attacks on DL-Based IoT Device Identification," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 9012–9024, Jun. 2022, conference Name: IEEE Internet of Things Journal. [Online]. Available: https://ieeexplore.ieee.org/document/9570781

[14] W. Zhang, M. Feng, M. Krunz, and A. Hossein Yazdani Abyaneh, "Signal Detection and Classification in Shared Spectrum: A Deep Learning Approach," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, May 2021, pp. 1–10, iSSN: 2641-9874.

[15] B. Riyaz and S. Ganapathy, "A deep learning approach for effective intrusion detection in wireless networks using CNN," *Soft Computing*, vol. 24, no. 22, pp. 17 265–17 278, Nov. 2020. [Online]. Available: https://doi.org/10.1007/s00500-020-05017-0

[16] C. P. Robinson, D. Uvaydov, S. D'Oro, and T. Melodia, "Narrowband interference detection via deep learning," in *ICC 2023 - IEEE International Conference on Communications*, 2023, pp. 6379–6384.

[17] N. Nikaein, M. K. Marina, S. Manickam, A. Dawson, R. Knopp, and C. Bonnet, "Openairinterface: A flexible platform for 5g research," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 33–38, 2014.

[18] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv:1409.1556*, 2014.

[19] J. Hu, L. Shen, and G. Sun, "Squeeze-and-excitation networks," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 7132–7141.