

# Optic Fingerprint: Enhancing Security in Visible Light Communication Networks

Xuanbang Chen<sup>§,†</sup>, Ziqi Liu<sup>§</sup>, Xun Zhang<sup>§</sup>, Yuhao Wang<sup>†</sup>, Dayu Shi<sup>§</sup>, Xiaodong Liu<sup>†,§</sup>,

<sup>§</sup>Institut Supérieur D'électronique de Paris, France, <sup>†</sup>Nanchang University, China

Email: [chenxuanbang@email.ncu.edu.cn](mailto:chenxuanbang@email.ncu.edu.cn), [ziqi.liu@isep.fr](mailto:ziqi.liu@isep.fr), [xun.zhang@isep.fr](mailto:xun.zhang@isep.fr),  
[wangyuhao@ncu.edu.cn](mailto:wangyuhao@ncu.edu.cn), [dayu.shi@ext.isep.fr](mailto:dayu.shi@ext.isep.fr), [xiaodongliu@whu.edu.cn](mailto:xiaodongliu@whu.edu.cn)

**Abstract**—In addressing physical layer security issues, hardware fingerprinting has been proven to be a reliable method. Additionally, Visible Light Communication (VLC) technology offers a solution to the spectrum congestion in next-generation wireless communications and is noteworthy for its high security. However, there is currently a lack of a comprehensive and systematic description of the hardware fingerprints and their extraction mechanisms for VLC devices. This study aims to bridge this gap by thoroughly analyzing the hardware fingerprints of VLC devices and proposing an innovative extraction mechanism, thereby enhancing the security and reliability of the physical layer. An Optic Fingerprint (OF) model is proposed based on the LED's inherent circuit characteristics, capable of extracting and processing unique feature vectors with high precision. Through extensive experiments, we demonstrate the model's efficacy, achieving up to 99.3% accuracy in identifying the same manufactured white LEDs under variable conditions, marking a significant improvement in authentication robustness and interference resistance.

**Index Terms**—Visible light communication, physics-based LED circuit model, optic fingerprint, machine learning.

## I. INTRODUCTION

THE transaction from 5G to 6G networks marks a significant leap in communication technology but raises emergent and complex security challenges [1], [2]. The classical cryptographic solutions fall short in these novel challenges due to their complexity-based paradigms. Consequently, innovative security approaches, particularly tailored for 6G systems, are desired from both the industry and academia. Device Fingerprint (DF) is the most potential technology in Physical Layer Security (PLS) enhancing approaches, owing to its unique and secure identification capabilities. It leverages the inherent hardware characteristics of devices, guaranteeing non-replicability and distinctive identification [3], [4], offers a more robust and adaptable security framework, well-suited to meet the demands of 6G and IoT applications [5]–[9].

Most of the existing research on DF focuses on Radio Frequency (RF) application scenarios. Researchers proposed the concept of Radio Frequency Fingerprint (RFF) to achieve the 92.29% accuracy of base station authentication for Wi-Fi, LTE, ZigBee, and etc. [10]–[15]. Whereas in the future 6G era,

the available spectrum extended to the optical band promoting heterogeneous physical layer technologies [16]. Visible Light Communication (VLC) [17], leveraging signal spectrum from 380nm to 780nm to transmit signal through the optical wireless channel, possesses attributes like high capacity, ultra-high data rates, low latency, and inherent security due to the limited penetration of optical signals.

However, few researches address the issues of DF in the VLC domain. Existing studies utilize frequency response measurements, notably the S21 parameter, to develop a DF model [18] [19] and employ machine learning or deep learning approaches [20] to detect DF features, aiming to authenticate device identities effectively. These studies, however, are largely limited to static environments, overlooking the impact of environmental and spatial fluctuations, such as distance, angle, and signal noise interference. Such neglect results in compromised anti-noise and spatial stability, thereby undermining the adaptability of these models in complex environments.

This paper proposes a new DF model in the VLC system, which is named the Optic Fingerprint (OF) model, and the corresponding machine learning-based feature extraction mechanism. Significant contributions of this study include:

- An OF model is proposed to characterize the unique nonlinearity attributes of LEDs to form a reliable feature vector.
- The extraction scheme for OF and the security identification framework is developed, utilizing power spectrum analysis and a machine learning classifier for precise device identification against an authorized fingerprint database.
- Numerous experiments are performed to validate our proposed OF model. The proposed OF model shows a high accuracy of 99.3% in identifying commercial white LEDs. Compared to the traditional S21 fingerprint, the proposed OF model presents a lower complexity with better performance of anti-environmental interference.

The rest of this paper is organized as follows. Section II outlines the OF model and extraction methodology. Section III details the feature extraction and verification process. Section IV presents the identification accuracy of the proposed fingerprint. Section V concludes the paper, discussing the implications of our future directions.

This work was supported by a grant of the EU Horizon 2020 program, under the 6G BRAINS project H2020-ICT 101017226. (Corresponding author: Xun ZHANG.)

X. Chen and Z. Liu contributed to the work equally and should be regarded as co-first authors.

## II. PHYSICS-BASED OPTIC FINGERPRINT MODEL

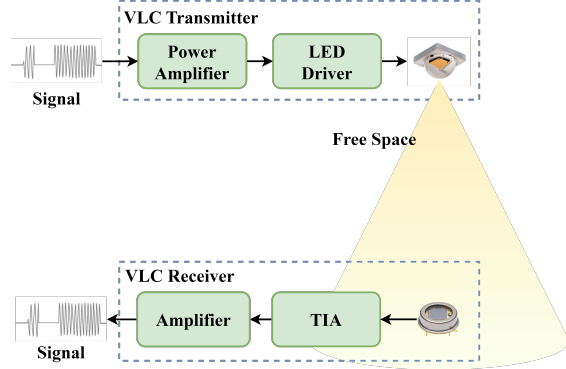


Fig. 1: The typical VLC link diagram.

A novel OF model is proposed based on the physics variations of LED devices for security enhancement in this context. Generally, as shown in Fig. 1, an LED-based VLC system comprises a VLC transmitter, Free Space, and VLC receiver. Specifically, the power amplifier amplifies the signal to drive LEDs with lower AC impedance, while the LED driver converts the voltage signal into a current signal, achieving amplitude modulation of the LED luminous intensity. The optical modulated signal emitted by the VLC transmitter travels through the channel and is intensity-detected by the VLC receiver. It is noteworthy that despite belonging to the same batch, the hardware components of the VLC transmitter, including the power amplifier, driver, and LED, may exhibit slight variations due to manufacturing tolerances. These hardware differences influence the optical signal, which is subsequently transmitted to the receiver. The received optical signal, denoted as  $y(t)$ , can be expressed as

$$y(t) = G_{PA}G_D H_C G_{Re} \int_{-\infty}^{\infty} x(t)h_{LED}(t - \tau)d\tau, \quad (1)$$

$x(t)$  denotes the electrical signal source.  $G_{PA}$ ,  $G_D$  represent the gain of the power amplifier and driver, respectively. Moreover,  $h_{LED}(t)$  is the impulse response of the LED. It is worth noting that the LED, as a bandwidth-limited communication device, is the main source of hardware nonlinearity and variance. Since the non-line of sight (NLoS) component of the VLC channel is very weak, the channel response  $H_C$  is considered to be a constant loss when only considering the line of sight (LoS) component, which can be calculated as

$$H_C = \frac{(m+1)A_r}{2\pi d^2} \cos^m(\phi)g(\psi)\cos(\psi), \quad (2)$$

where  $m = -\ln 2 / \ln(\cos \phi_{1/2})$  is the Lambertian emission order and  $\phi_{1/2}$  is the emission semi-angle of LED.  $A_r$  is the physical detection area of the receiver front-end. The channel loss is related to the distance  $d$  (between the LED and the receiver front-end) and the irradiance angle  $\phi$  of the light [21].

Thus, amplifier, driver, and channel impulse responses can all be considered linear parameters. Therefore, modeling the nonlinearity of LEDs is key to characterizing the distinc-

tive feature of each device. Numerous generic mathematical modeling methods have been proposed to characterize the modulation nonlinearity of LEDs, such as the memory polynomial model, Volterra model, and Hammerstein model [22]. However, these modeling methods typically exhibit high implementation complexity and fail to capture the inherent common modulation nonlinearity of LEDs, which are strongly correlated with the physical structure of the LED. Our previous work modeled the GaN LED from the physics aspect, through the analysis of carrier concentrations in each LED layer, the carrier diffusion, capture, thermal escape, and recombination are formulated by carrier rate equations [23]. Based on the previous work, the physics-based LED model is improved to completely characterize the high-frequency characteristics in this paper, and a novel OF model is proposed.

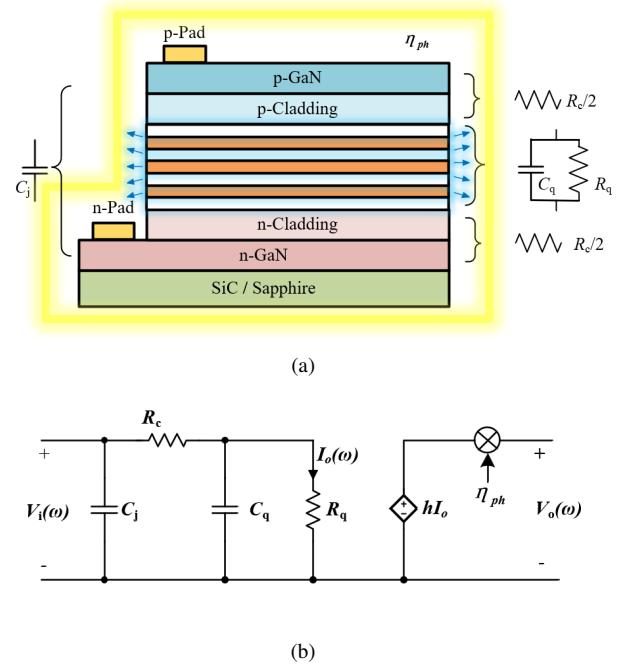


Fig. 2: (a) The physical structure and (b) the equivalent circuit model of the MQW LED.

As shown in Fig. 2(a), silicon carbide (SiC) and sapphire are the common substrates used in the LED. Due to the MQW being wrapped by a cladding layer, it is necessary to consider the capacitance and resistance effects of the quantum well in the LED model. Thus,  $R_q$  and  $C_q$  represent the equivalent resistance and capacitance of MQW, respectively. Specifically, the current through  $R_q$  represents the recombination of electrons, and  $C_q$  reflects the charge storage effect in the quantum well [24]. Moreover,  $R_c$  is the equivalent resistance distributed in p- and n-Cladding layers.  $C_j$  is the sum of the barrier capacitance and the parasitic capacitance. Thus, the corresponding equivalent circuit model is schematically illustrated in Fig. 2(b). It is worth noting that  $h$  represents the external quantum efficiency.  $\eta_{ph}$  is the response of phosphor. The blue wavelength photons emitted by the LED are excited

by the phosphor to produce yellow light and are mixed into white light to provide white lighting services to users. The analytical expression of the LED's impedance  $Z_{\text{LED}}(w)$  can be written as follows.

$$\begin{aligned} Z_{\text{LED}}(w) &= \frac{1}{jwC_j} // (R_c + R_q // \frac{1}{jwC_q}) \\ &= \frac{R_c + R_q + jwR_cR_qC_q}{1 - w^2R_cR_qC_qC_j + jw(R_qC_q + R_cC_j + R_qC_j)}, \end{aligned} \quad (3)$$

where  $w$  is the angular frequency and  $j$  is the imaginary unit. The operator  $//$  denotes the parallel calculation in the circuit. Thus, the parameters of the LED equivalent model can be extracted from the measured impedance curve. However, this method is less practical, as it necessitates additional and complex experiments to obtain device impedance features. In this context, the frequency response of the LED is exploited to extract model features, allowing the utilization of existing communication data for obtaining the transmission response without additional experiments. Specifically, the transfer function of the LED-based VLC system can be expressed as

$$\begin{aligned} H_{\text{VLC}}(w) &= G_{\text{PA}}G_{\text{D}}H_{\text{C}}G_{\text{Re}}H_{\text{LED}}(w) \\ &= \frac{G_{\text{PA}}G_{\text{D}}H_{\text{C}}G_{\text{Re}}h}{1 - w^2R_cR_qC_qC_j + jw(R_qC_q + R_cC_j + R_qC_j)}. \end{aligned} \quad (4)$$

As  $G_{\text{PA}}$ ,  $G_{\text{D}}$ ,  $H_{\text{C}}$ ,  $G_{\text{Re}}$ , and  $h$  remain constant at a specific measurement point, a uniform  $\zeta$  is employed to represent these parameters, simplifying the transmission formulation. Therefore, the feature parameters of the proposed LED model are summarized as a five-dimensional vector  $R_c$ ,  $C_j$ ,  $R_q$ ,  $C_q$ , and  $\zeta$ , which can be derived from the VLC system response  $H_{\text{VLC}}$ . Additionally,  $H_{\text{C}}$  excludes the phosphor response component, as the receiver typically employs a blue light filter to eliminate signal transmission delays. Therefore, the feature parameters  $R_c$ ,  $C_j$ ,  $R_q$ ,  $C_q$ , and  $\zeta$  of the proposed LED model can be derived from the VLC system response  $H_{\text{VLC}}(w)$ .

$$\lambda = [R_c, C_j, R_q]. \quad (5)$$

The values of  $R_c$ ,  $C_j$ , and  $R_q$  form the OF model represented by the three-dimensional feature vector  $\lambda$ . It is important to note that the factors  $\zeta$  and  $C_q$  are omitted from the OF model. This exclusion is justified by the fact that  $\zeta$  primarily relies on the testing equipment types and specific positions, rather than the intrinsic characteristics of the LED. Additionally, Section IV provides further evidence that  $C_q$  lacks distinct characteristics among different LED devices.  $\lambda$  depends on the inherent non-linearity characteristic of each LED, which indicates its unique fingerprints.

### III. EXTRACTION AND IDENTIFICATION

#### A. Optic Fingerprint Extraction

Fig. 3 illustrates the OF feature extraction process. The LED is the device for the proposed OF feature extraction, which acts as the access point within the VLC system. The test signal, encompassing options such as a swept, baseband, or modulated signal, undergoes LED-induced nonlinearity and is

captured by the VLC receiver. The system response data S21, derived from processing the received signal, is utilized for parameter extraction in the proposed OF model. The extraction algorithm employs the nonlinear least squares method. Specifically, given an initial fingerprint value, the fingerprint feature value continuously updates to minimize the residual  $\sum_{i=1}^n e^2(f_i)$  between the fitted system response data and the measured data. Note that  $n$  denotes the frequency points of S21 data. The optimal extraction result is then recorded as the LED's fingerprint feature. Subsequently, numerous LEDs are incorporated into the OF database after feature extraction, facilitating device security authentication.

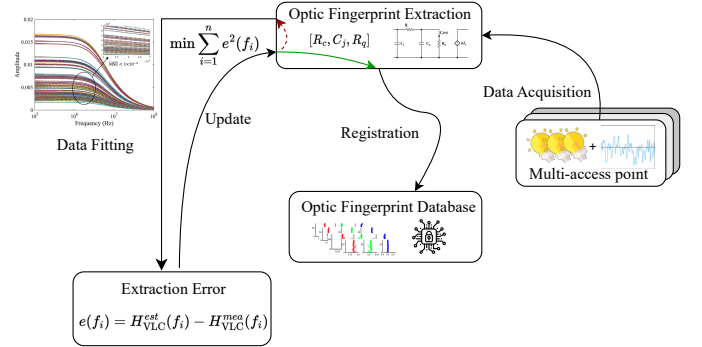


Fig. 3: The extraction scheme of the proposed OF model.

#### B. Security Identification Scheme

Fig. 4 presents an intricate security identification architecture predicated on our OF identification methodology. This system is engineered to preemptively negate network security breaches perpetrated by eavesdroppers (Eve) through identity falsification and unauthorized data acquisition. In the edge network, OF data for registered devices are meticulously cataloged within the OF database. The Security Validation Server (SVS) engages in conjunction with the VLC Access Point to periodically solicit OF data from user equipment (UE). The SVS rigorously evaluates the OF against the established registry of the authenticated user (RegU) fingerprints within the database, subsequently conveying the verification results to the Network Management System (NMS) housed within the Internet Cloud to complete the security validation process. The NMS, predicated on the analysis, orchestrates access authorization via the Access Control Server (ACS) or initiates preemptive alerts through the Identity Services Engine (ISE). The detection mechanism's protocol unfolds as follows:

- 1) The VLC Access Point periodically retrieves OF data from UEs.
- 2) The extracted data are then transmitted to the SVS within the edge network.
- 3) The SVS concurrently retrieves and analyzes corresponding OF data from the database.
- 4) The SVS's verdicts are dispatched to the NMS to facilitate security services.
- 5) The NMS adjudicates network access or restricts it through the ACS based on the analysis.

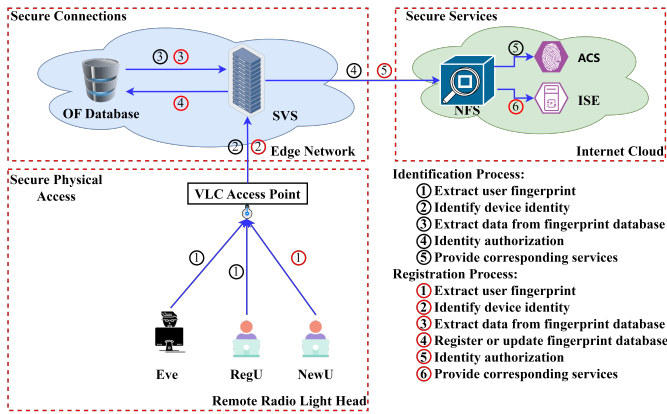


Fig. 4: Security identification scheme based on OF model.

Further, the framework accommodates the registration of new users (NewU), integrating them seamlessly into the network. The registration process entails:

- 1) Upon a NewU's registration request, the VLC Access Point captures pertinent user data and transmutes it into OF data.
- 2) This data is relayed to the SVS for processing.
- 3) The SVS concurrently retrieves and analyzes corresponding OF data from the database.
- 4) The SVS updates the OF database with new entries to the OF database
- 5) The SVS concurrently communicates with the NMS.
- 6) The NMS, leveraging the ISE, disseminates new registration details and provisions services accordingly.

This meticulously orchestrated sequence of operations fortifies the network's defense mechanisms against illicit access while contemporaneously ensuring the OF database remains current, thus fostering a secure and adaptable network milieu for both extant and nascent users.

#### IV. EXPERIMENT SETUP AND RESULTS

##### A. Experiment Setup

The experiment test-bed for acquiring the OF is shown in Fig. 5. Specifically, the vector network analyzer (VNA, Rohde&Schwarz, ZNB20) is employed to measure the frequency responses of the LED. The measurements utilize a continuous wave (CW) frequency-sweep technique. Four LED samples (Cree, XPE2-White) are exploited to establish the OF database. Here, the VNA injects a CW signal with an electrical power of -5 dBm into the power amplifier (Mini-circuits, ZHL-6A-S+), sweeping the modulation frequency from 100 KHz to 100 MHz. Bias-T (Mini-Circuits, ZX85-12G-S+) is exploited to drive the LED with the amplified signal. The VNA then assesses the amplitude and phase variations between the transmitted and received signals, providing the frequency response of the test setup, which includes the wireless link and the optical front ends. The measurements are taken at 15 distinct positions, with each position measured 10 times, totaling 150 measurements per LED. It is worth noting that the longest test distance is 60 cm due to the limited power of a

single LED. These measurements form the basis for extracting the normalized feature vectors of each LED.

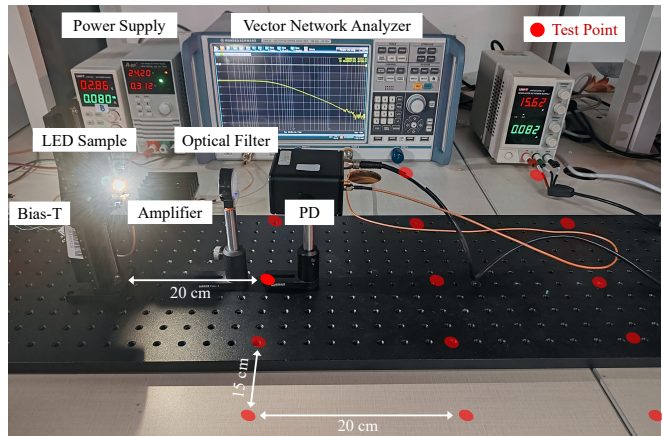


Fig. 5: Schematic diagram of the experiment setup.

Moreover, for each LED, 50% of the dataset was randomly allocated as the training set, with the feature vectors serving as signatures for authenticated devices. A range of machine learning algorithms—Fine Tree (F-Tree), Kernel Naive Bayes (KNB), Quadratic Support Vector Machine (Q-SVM), Fine K Nearest Neighbor (F-KNN), Ensemble Bagged Trees (EB-Trees), Ensemble Subspace K Nearest Neighbor (ES-KNN), and Narrow Neural Network (NN-Network)—was applied to stratify the training data into four clusters. Following this registration, the remaining data constituted the test set. Alongside, the original, unprocessed S21 parameter data were subjected to the same machine learning classification to provide a baseline for performance comparison.

To rigorously evaluate the identification process, noise disturbances were superimposed onto the test dataset and the unprocessed S21 data. These disturbances ranged from 0 dBm to 90 dBm in 5 dBm increments, resulting in a total of 2550 sets of data, emulating various channel conditions, and testing the robustness of the machine learning models. The analysis compared the performance of the models on both the noise-augmented dataset and the original S21 data, highlighting the efficacy of the OF features in maintaining high identification accuracy despite the presence of environmental noise.

##### B. Results and Analysis

The training OF database comprises 300 samples from 4 LED samples. OF extraction is accomplished by fitting S21 to the objective function Eq. (4). Fig. 6 illustrates the fitting results, compared to 300 S21 measured samples. The frequency response of four LEDs shows different amplitudes due to the various test locations. Moreover, it can be seen from the subfigure in Fig. 6 that fitted dots show good coincidence with the measured lines, yielding an average Mean Squared Error (MSE) of less than  $1e-4$ .

Furthermore, Fig. 7 presents the five extracted parameters of the equivalent circuit model based on the aforementioned curve fitting. It can be seen that the circuit model parameters

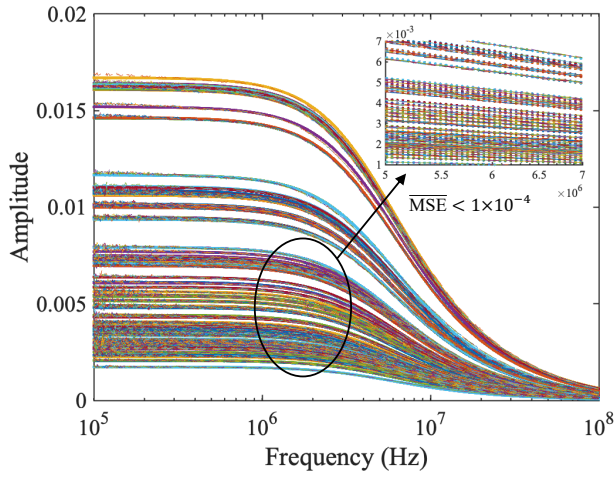


Fig. 6: The fitting results of four LEDs in different positions.

$C_q$  and  $\zeta$  of four LED samples are difficult to distinguish. This is because the impact of different test points on  $\zeta$  blurs its individual, and  $C_q$  is in the nF range making its characteristics challenging to distinguish between LEDs. Thus, the feature vectors  $[R_c, C_j, R_q]$  are chosen as the proposed OF model. Fig. 8 shows the clustering result of the proposed OF for four LED samples, which are clearly clustering at different locations in the space.

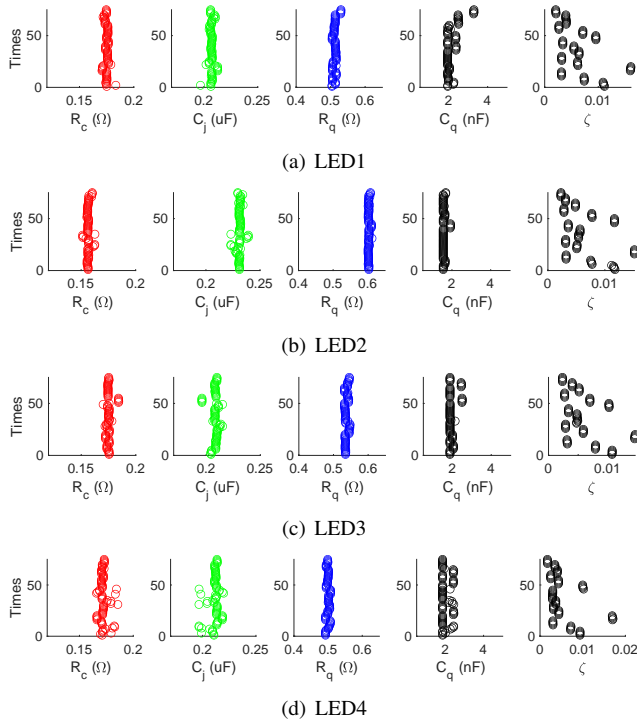


Fig. 7: The extracted features of four LED samples.

In the subsequent analysis, various machine-learning algorithms are employed to assess the classification accuracies and validate the efficacy of the proposed OF model. As depicted in

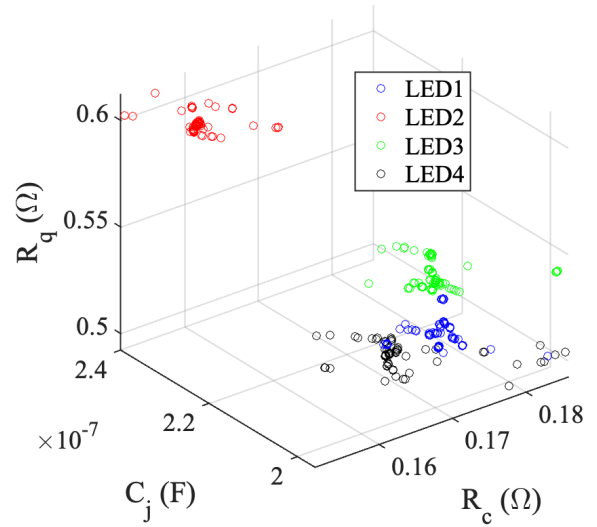


Fig. 8: The clustering of the proposed OF model  $[R_c, C_j, R_q]$ .

Fig. 9, the OF model consistently achieves remarkable accuracy ranging from 99.3% to 95.0% with different algorithms. In contrast, the S21 fingerprint model [18], under the same machine-learning evaluations, exhibits a broader spectrum of accuracy rates, peaking at 93.7% and dropping to as low as 42.0%. Notably, the OF model requires only three features, whereas the S21 fingerprint model relies on 750 features. This substantial reduction in feature count, combined with superior accuracy and stability, highlights the advantages of our proposed OF model over the conventional S21 model, offering improved efficiency and reduced data complexity.

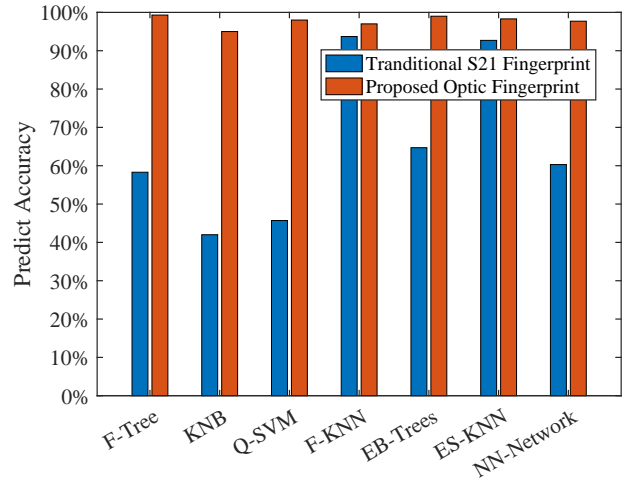


Fig. 9: The accuracy comparison of different algorithms using traditional S21 fingerprint and OF models.

Finally, the reliability of the OF model is analyzed by adding Gaussian white noise of varying powers to both the OF and the traditional S21 fingerprint models. Fig. 10 illustrates that the proposed OF model consistently achieves accuracies exceeding 80% across a noise power range from -90 dBm to -20 dBm. In contrast, the S21 fingerprint model

demonstrates inferior noise immunity, with accuracy declining to below 62%. Furthermore, while the performance of the OF model begins to degrade for noise levels surpassing -20 dBm, it remains superior to the S21 fingerprint model. This indicates that fingerprint feature vectors extracted from LED models inherently capture the LED's characteristics, exhibiting robustness against changes in external channel conditions.

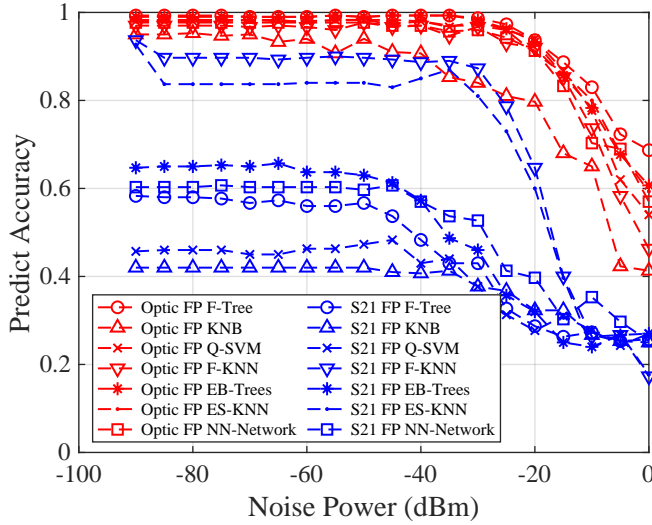


Fig. 10: The comparison of anti-noise performance between traditional S21 fingerprint and proposed OF models.

## V. CONCLUSION

This paper introduces a novel Optic Fingerprint (OF) to apply for enhancing the physical layer security of the sixth-generation network. Four LED samples were exploited to verify the mechanism of the proposed OF model. High classification accuracies were achieved based on the generic machine learning algorithms, which up to 99.3%. Moreover, the OF model was compared with the traditional S21 fingerprint model, showcasing a lower complexity with better performance of anti-environmental interference. It is worth noting that the LED samples with more different types and manufacturers will be discussed in future work. The effects introduced by the different receivers will be considered as well, ensuring its effectiveness in the sixth-generation security framework.

## REFERENCES

- [1] 3rd Generation Partnership Project (3GPP), "Study on 5g security enhancements against false base stations," Tech. Rep. Tech. Report 33.809, 3GPP, Sophia Antipolis, France, 2018.
- [2] P. Porambage, G. Gür, D. P. M. Osorio, M. Livanage, and M. Ylianttila, "6g security challenges and potential solutions," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, pp. 622–627, IEEE, 2021.
- [3] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and challenges of software-defined mobile networks in network security," *IEEE security & privacy*, vol. 14, no. 4, pp. 34–44, 2016.
- [4] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2019.

- [5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge University Press, 2011.
- [6] B. Aazhang *et al.*, "Key drivers and research challenges for 6g ubiquitous wireless intelligence," tech. rep., White Paper, Sep 2019.
- [7] V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, and A. Rezaki, "Security and trust in the 6g era," *IEEE Access*, vol. 9, pp. 142314–142327, 2021.
- [8] B. Khorsandi *et al.*, "D1.3, targets and requirements for 6g - initial e2e architecture, hexa-x," tech. rep., Feb 2022.
- [9] IEEE International Network Generations Roadmap, "Security and privacy," 2022. Available: <https://futurenetworks.ieee.org/roadmap>.
- [10] L. Xie, L. Peng, J. Zhang, and A. Hu, "Radio frequency fingerprint identification for internet of things: A survey," *Security and Safety*, vol. 3, p. 2023022, 2024.
- [11] J. Zhang, G. Shen, W. Saad, and K. Chowdhury, "Radio frequency fingerprint identification for device authentication in the internet of things," *IEEE Communications Magazine*, 2023.
- [12] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 18, pp. 94–104, 2015.
- [13] H. Sun, X. Zhu, Y. Liu, and W. Liu, "Construction of hybrid dual radio frequency rssi (hdrf-rssi) fingerprint database and indoor location method," *Sensors*, vol. 20, p. 2981, 2020.
- [14] J. Yu, A. Hu, C. Zhu, L. Peng, and Y. Jiang, "Rf fingerprinting extraction and identification of wireless communication devices," *Journal of Cryptologic Research*, vol. 3, pp. 433–446, 2016.
- [15] K. Merchant, S. Revay, G. Stantchev, and B. Noursain, "Deep learning for rf device fingerprinting in cognitive communication networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, pp. 160–167, 2018.
- [16] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6g: A comprehensive survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 334–366, 2021.
- [17] N. Chi, Y. Zhou, Y. Wei, and F. Hu, "Visible light communication in 6g: Advances, challenges, and prospects," *IEEE Vehicular Technology Magazine*, vol. 15, no. 4, pp. 93–102, 2020.
- [18] D. Shi, X. Zhang, A. Vladimirescu, L. Shi, Y. Huang, and Y. Liu, "A device identification method based on led fingerprint for visible light communication system," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pp. 1–7, 2020.
- [19] D. Shi, X. Zhang, L. Shi, A. Vladimirescu, W. Mazurczyk, K. Cabaj, B. Meunier, K. Ali, J. Cosmas, and Y. Zhang, "On improving 5g internet of radio light security based on led fingerprint identification method," *Sensors*, vol. 21, no. 4, p. 1515, 2021.
- [20] Z. Liu, D. Shi, S. Oukemeni, and X. Zhang, "Alexnet-based visible light communication devices fingerprint extraction and authentication in broadcast systems," in *2022 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, pp. 01–05, IEEE, 2022.
- [21] M. Zhu, Y. Wang, X. Liu, Z. Qi, X. Chen, and J.-Y. Wang, "Physical layer security performance analysis for relay-aided visible light communication system," *IEEE Photonics Journal*, vol. 15, no. 3, pp. 1–9, 2023.
- [22] X. Deng, S. Mardankorani, Y. Wu, K. Arulandu, B. Chen, A. M. Khalid, and J.-P. M. G. Linnartz, "Mitigating led nonlinearity to enhance visible light communications," *IEEE Transactions on Communications*, vol. 66, no. 11, pp. 5593–5607, 2018.
- [23] D. Shi, X. Zhang, Z. Liu, X. Chen, X. Liu, J. Wang, J. Song, and A. Vladimirescu, "Physics-based modeling of gan mqw led for visible light communication systems," *IEEE Transactions on Electron Devices*, vol. 71, no. 1, pp. 337–342, 2024.
- [24] A. Rashidi, M. Nami, M. Monavarian, A. Aragon, K. DaVico, F. Ayoub, S. Mishkat-Ul-Masabih, A. Rishinaramangalam, and D. Feezell, "Differential carrier lifetime and transport effects in electrically injected iii-nitride light-emitting diodes," *Journal of Applied Physics*, vol. 122, no. 3, 2017.

## REFERENCES

- [1] 3rd Generation Partnership Project (3GPP), "Study on 5g security enhancements against false base stations," Tech. Rep. Tech. Report 33.809, 3GPP, Sophia Antipolis, France, 2018.

- [2] P. Porambage, G. Gür, D. P. M. Osorio, M. Livanage, and M. Ylianttila, "6g security challenges and potential solutions," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, pp. 622–627, IEEE, 2021.
- [3] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and challenges of software-defined mobile networks in network security," *IEEE security & privacy*, vol. 14, no. 4, pp. 34–44, 2016.
- [4] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2019.
- [5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge University Press, 2011.
- [6] B. Aazhang *et al.*, "Key drivers and research challenges for 6g ubiquitous wireless intelligence," tech. rep., White Paper, Sep 2019.
- [7] V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, and A. Rezaki, "Security and trust in the 6g era," *IEEE Access*, vol. 9, pp. 142314–142327, 2021.
- [8] B. Khorsandi *et al.*, "D1.3, targets and requirements for 6g - initial e2e architecture, hexa-x," tech. rep., Feb 2022.
- [9] IEEE International Network Generations Roadmap, "Security and privacy," 2022. Available: <https://futurenetworks.ieee.org/roadmap>.
- [10] L. Xie, L. Peng, J. Zhang, and A. Hu, "Radio frequency fingerprint identification for internet of things: A survey," *Security and Safety*, vol. 3, p. 2023022, 2024.
- [11] J. Zhang, G. Shen, W. Saad, and K. Chowdhury, "Radio frequency fingerprint identification for device authentication in the internet of things," *IEEE Communications Magazine*, 2023.
- [12] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 18, pp. 94–104, 2015.
- [13] H. Sun, X. Zhu, Y. Liu, and W. Liu, "Construction of hybrid dual radio frequency rssi (hdrf-rssi) fingerprint database and indoor location method," *Sensors*, vol. 20, p. 2981, 2020.
- [14] J. Yu, A. Hu, C. Zhu, L. Peng, and Y. Jiang, "Rf fingerprinting extraction and identification of wireless communication devices," *Journal of Cryptologic Research*, vol. 3, pp. 433–446, 2016.
- [15] K. Merchant, S. Revay, G. Stantchev, and B. Nossain, "Deep learning for rf device fingerprinting in cognitive communication networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, pp. 160–167, 2018.
- [16] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6g: A comprehensive survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 334–366, 2021.
- [17] N. Chi, Y. Zhou, Y. Wei, and F. Hu, "Visible light communication in 6g: Advances, challenges, and prospects," *IEEE Vehicular Technology Magazine*, vol. 15, no. 4, pp. 93–102, 2020.
- [18] D. Shi, X. Zhang, A. Vladimirescu, L. Shi, Y. Huang, and Y. Liu, "A device identification method based on led fingerprint for visible light communication system," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pp. 1–7, 2020.
- [19] D. Shi, X. Zhang, L. Shi, A. Vladimirescu, W. Mazurczyk, K. Cabaj, B. Meunier, K. Ali, J. Cosmas, and Y. Zhang, "On improving 5g internet of radio light security based on led fingerprint identification method," *Sensors*, vol. 21, no. 4, p. 1515, 2021.
- [20] Z. Liu, D. Shi, S. Oukemeni, and X. Zhang, "Alexnet-based visible light communication devices fingerprint extraction and authentication in broadcast systems," in *2022 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, pp. 01–05, IEEE, 2022.
- [21] M. Zhu, Y. Wang, X. Liu, Z. Qi, X. Chen, and J.-Y. Wang, "Physical layer security performance analysis for relay-aided visible light communication system," *IEEE Photonics Journal*, vol. 15, no. 3, pp. 1–9, 2023.
- [22] X. Deng, S. Mardankorani, Y. Wu, K. Arulandu, B. Chen, A. M. Khalid, and J.-P. M. G. Linnartz, "Mitigating led nonlinearity to enhance visible light communications," *IEEE Transactions on Communications*, vol. 66, no. 11, pp. 5593–5607, 2018.
- [23] D. Shi, X. Zhang, Z. Liu, X. Chen, X. Liu, J. Wang, J. Song, and A. Vladimirescu, "Physics-based modeling of gan mqw led for visible light communication systems," *IEEE Transactions on Electron Devices*, vol. 71, no. 1, pp. 337–342, 2024.
- [24] A. Rashidi, M. Nami, M. Monavarian, A. Aragon, K. DaVico, F. Ayoub, S. Mishkat-Ul-Masabih, A. Rishinaramangalam, and D. Feezell, "Differential carrier lifetime and transport effects in electrically injected iii-nitride light-emitting diodes," *Journal of Applied Physics*, vol. 122, no. 3, 2017.