sensors

MDPI

Communication

On Improving 5G Internet of Radio Light Security Based on LED Fingerprint Identification Method

Dayu Shi [1], Xun Zhang [1,*], Lina Shi [1], Andrei Vladimirescu [1], Wojciech Mazurczyk [2], Krzysztof Cabaj [2], Benjamin Meunier [3], Kareem Ali [3], John Cosmas [3] and Yue Zhang [4]

1 Laboratory LISITE, Institut Supérieur D'électronique de Paris, 75006 Paris, France; dayu.shi@isep.fr (D.S.); lina.shi@isep.fr (L.S.); andrei.vladimirescu@isep.fr (A.V.)
2 Institute of Computer Scence, Warsaw University of Technology, 00-665 Warsaw, Poland; w.mazurczyk@tele.pw.edu.pl (W.M.); k.cabaj@elka.pw.edu.pl (K.C.)
3 Department of Electronic and Computer Engineering, Brunel University, Uxbridge UB8 3PN, UK; benjamin.meunier@brunel.ac.uk (B.M.); kareem.ali2@brunel.ac.uk (K.A.); john.cosmas@brunel.ac.uk (J.C.)
4 School of Engineering, University of Leicester, Leicester LE1 7RH, UK; yue.zhang@leicester.ac.uk
* Correspondence: xun.zhang@isep.fr

Abstract: In this paper, a novel device identification method is proposed to improve the security of Visible Light Communication (VLC) in 5G networks. This method extracts the fingerprints of Light-Emitting Diodes (LEDs) to identify the devices accessing the 5G network. The extraction and identification mechanisms have been investigated from the theoretical perspective as well as verified experimentally. Moreover, a demonstration in a practical indoor VLC-based 5G network has been carried out to evaluate the feasibility and accuracy of this approach. The fingerprints of four identical white LEDs were extracted successfully from the received 5G NR (New Radio) signals. To perform identification, four types of machine-learning-based classifiers were employed and the resulting accuracy was up to 97.1%.

Keywords: visible light communication; LED fingerprint; 5G networks; security

Citation: Shi, D.; Zhang, X.; Shi, L.; Vladimirescu, A.; Mazurczyk, W.; Cabaj, K.; Meunier, B.; Ali, K.; Cosmas, J.; Zhang, Y. On Improving 5G Internet of Radio Light Security Based on LED Fingerprint Identification Method. *Sensors* **2021**, *21*, 1515. https://doi.org/10.3390/s21041515

Academic Editor: Giuseppe Piro

Received: 7 January 2021
Accepted: 16 February 2021
Published: 22 February 2021

1. Introduction

With the enormous growth of wireless devices and the deep integration of information technology into a number of industrial applications [1], the 5G network is expected to support massive user connections and exponentially increase wireless services. In addition, due to a tremendous number of Internet-of-Things (IoT) devices featured by the massive Machine-Type Communication (mMTC) extensive applications in the 5G network, high data rates, high connection density and ultra-reliable low latency communication (URLLC) should be provided. Moreover, security must be urgently assured by the future 5G network [2]. Hence, traditional radio frequency (RF) networks, which are already crowded, are arduous to satisfy these high demands [3]. One of the new communication technologies that has been proposed as an auspicious solution for the 5G and beyond is Visible Light Communication (VLC) [4]. VLC provides the nomadic access in hundreds of terahertz (THz) of unlicensed optical spectrum, immunity to electromagnetic interference, safety and security, simple implementation, and deployment of systems [5–7]. These exciting assets generate considerable research and industrial interests for the indoor VLC, especially with the approval of the IEEE 802.15.7 standard [8]. The research in this topic is conducted in the European H2020 project Internet of Radio Light (IoRL), which was the first to propose a hybrid indoor optical-radio network in convergence with the 5G Era [9–11]. The advantage of the VLC compared to radio [4] and its applications scenarios [12,13] has been widely discussed in the VLC literature. Due to the line-of-sight light propagation and the impermeability for non-transparent objects, the VLC channel exhibits higher security in a single-user or private-room scenario. However, in public areas such as classrooms, libraries, hallways, or planes, the security of the transmitted signal cannot be guaranteed [14].

Device fingerprinting, the process of gathering device information to generate device-specific signatures and using them to identify individual devices, has emerged as a potential solution for the 5G network to reduce the vulnerability of wireless networks to node forgery or insider attacks [15,16]. Its low-complexity and difficult or impossible to forge property could be perfectly matched with the security requirements of the 5G network. Notably, wireless device identification via Radio Frequency (RF) fingerprint becomes a widely concerned physical-layer security mechanism [17] and has been investigated in Wi-Fi, LTE (Long Term Evolution) and ZigBee systems. It provides an opportunity to accomplish the authentication and the target device identification in the physical layer. Recently, a RF fingerprint-based device identification method successfully demonstrated 92.29% identification accuracy on a set of seven 2.4 GHz commercial ZigBee devices [18]. It must be noted that device fingerprinting schemes can also be applied in the same spirit to VLC systems. However, the distinctive transmission protocols and modulation schemes of VLC systems such as intensity-modulation direct detection (IM/DD), direct-current (DC) biased optical orthogonal frequency-division multiplexing (DCO-OFDM) [19] necessitate the development of new device fingerprinting methods specific to VLC systems [20].

Currently, little research on VLC device identification exists. However, drawing on lessons from the successful implementations of device identification via RF fingerprint provides the possibility to propose the appropriate and efficient device identification method also for VLC systems. The concept of RF fingerprinting was firstly proposed by Hall et al. in 2003 [21]. This device identification method is featured by the detection of the transient signal emitted by the transmitter. Kennedy et al. was the first to introduce the device identification method based on the steady-state signal [22]. Afterwards, a large body of literature is dedicated to the general issues of design, implementation and identification algorithm relevant to many kinds of RF identification systems [23–26]. A comprehensive overview of high-level issues in the context of device identification method via RF fingerprint is summarized by Xu et al. [15].

That is why, in this paper, a device identification method is proposed based on the IoRL framework which is a typical indoor solution that integrates VLC-based communication, positioning and illumination systems within the 5G network [27,28]. This proposal aims to improve the security for the VLC-based 5G network under the public areas and broadcasting scenario as mentioned above. In this approach, fingerprints are extracted from the signal emitted by Light-Emitting Diodes (LEDs). These fingerprints are unique for every LED even if they are of the same type. Moreover, by employing a machine-learning-based classifier, the system is able to distinguish these fingerprints, thereby identifying with which device it is communicating. This fundamentally eliminates the threat of rouge base-station. It replaces the traditional encryption by a real-time and OTP (One Time Pad) encryption, which strengthens the overall security of the 5G networks. Moreover, the only prerequisites of this method are the received analog signal and some software modules, which means that this mechanism can be integrated into an existing 5G network physical layer. Considering the above, the main contributions of this paper can be summarized as follows:

- We introduce the LED fingerprint model based on the characteristics of the LED equivalent circuit and design the LED fingerprint extraction and identification mechanisms—by fitting the power spectrum. The parameters which represent the LED's inherent and stable nature are chosen to constitute the LED feature vector. The feature vector of each LED forms its fingerprint. A multi-SVM (Support Vector Machine) classifier is investigated theoretically to illustrate the process of the fingerprint identification.
- We illustrate the conceptual design of a typical 5G VLC multi-access scenario using the proposed security solution. We present how LED fingerprinting could be used in real-life systems. To detail the process, we choose the IoRL project as an exemplary test system.
- We demonstrate the feasibility and accuracy of this method in a practical indoor VLC-based 5G network. During experimental evaluation, four identical LEDs were used

to extract their fingerprints from the emitted 5G NR signals. Four machine-learning-based classifiers, i.e., decision tree, Naïve Bayes, SVM (Support Vector Machine), and KNN (K-Nearest-Neighbor) were employed to identify the extracted LED fingerprints. It turned out that the best results were achieved for the SVM classifier, which reached the accuracy of 97.1%.

The rest of this paper is organized as follows. Section 2 describes the proposed LED fingerprinting method in detail. Then, the experimental methodology and obtained results are detailed in Section 3. Finally, Section 4 concludes our work and outlines potential future directions.

2. LED Fingerprint Verification Mechanism

2.1. LED Fingerprint Model

It is noteworthy that there is little difference between the components of a VLC system except for the LEDs. The nonlinearity and saturation characteristic support the possibility to distinguish LEDs, even those from the same batch [26]. Thus, the LED fingerprint model has been established to characterize the distinctive feature of each device. A small-signal equivalent circuit model of the LED in the VLC system is illustrated in Figure 1 According to the equivalent circuit, p_{signal} is the power of the input signal, and p_{out} is the power of the output optical signal. R_s and L_s are the parasitic resistance and parasitic inductance. C_d and C_b represent the diffusion and the barrier capacitance of the LED, respectively. η is the photoelectric conversion efficiency and r_d is the small-signal diode resistance of an LED. The equations defining these elements using SPICE parameters are the following [29,30]:

$$P_{optical} = \eta P_{electric} \tag{1}$$

$$g_d = \frac{1}{r_d} = \frac{dI_d}{dV_d} = \frac{qI_s}{NkT} e^{qV_D/NkT} \approx \frac{I_D}{NV_{th}} \tag{2}$$

$$C_d = TT \cdot g_d \tag{3}$$

$$C_b = \begin{cases} \frac{C_{J0}}{(1-V_D/V_B)^M} & V_D < FC \cdot V_B \\ \frac{C_{J0}}{(1-FC)^{1+M}} \left[1 - FC(1+M) + \frac{MV_D}{V_B}\right] & V_D \geq FC \cdot V_B \end{cases} \tag{4}$$

$$C = C_b + C_d \tag{5}$$

$$\lambda = [C, \eta] \tag{6}$$

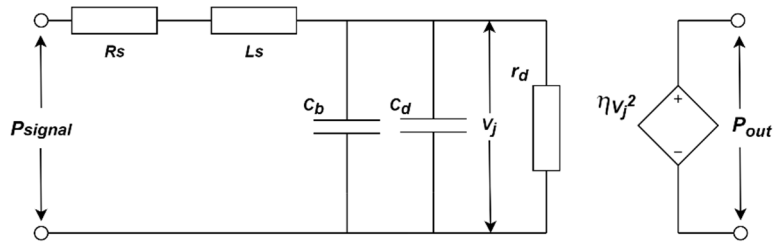


Figure 1. A Small-Signal Equivalent Circuit Model of an LED in the VLC System.

The values of the diffusion capacitance C_d, the barrier capacitance C_b and the photoelectric conversion efficiency η are the inherent and stable values of an LED. Once the fabrication of an LED is accomplished and the quiescent operation point was set, these values are fixed. Due to the industrialized and standardized production of LEDs, the dissimilarity of parasitic resistance and inductance values are too subtle to distinguish between different LEDs. Therefore, the values of η and C constitute a two-dimensional feature vector λ. It can represent the inherent characteristics of the LED and, as a result, we are able to define the feature vector of the LED and thus its fingerprint.

2.2. Extraction and Identification Mechanisms

In this section, introduced LED fingerprint extraction and identification will be explained. The extraction and identification mechanisms are illustrated in Figure 2.

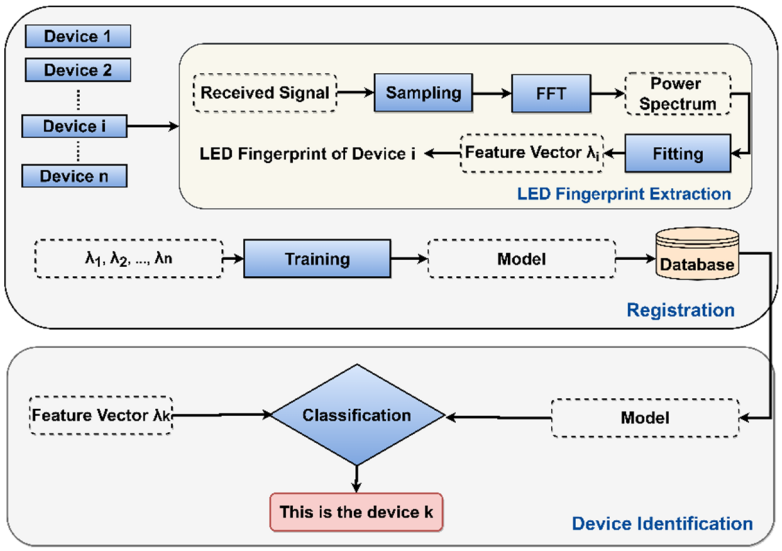


Figure 2. LED Fingerprint Extraction and Identification Mechanism.

The example of the LED fingerprint extraction of the *i*-th device will be described below in order to illustrate the proposed method's functioning. The signal transmitted from the *i*-th device will be sampled by performing a Fast Fourier Transform (FFT) to calculate the power spectrum at the receiver. By fitting this measured power spectrum with its theoretical function, the feature vector becomes the LED's fingerprint.

Before the identification, the registration of the authorized devices should be processed first. The feature vector of each authorized device will be extracted and put into a machine-learning-based classifier to train an identification model. Once the model has been established, it will be stored into a database which is integrated on the judgment module.

When a device k requests accessing, its feature vector λk will be extracted by the receiver. Meanwhile, the classification module will invoke the model stored in the database and perform identification. As the device has been recognized, the judgment module will decide if it permits it to access, based on the demands of the user.

2.3. Implementation of Features for Extraction and Identification

As described above, the signal transmitted by a device will pass through an optical wireless channel and be captured at the receiver. The power spectrum of this received signal will be fitted with its theoretical function to extract the feature vector as its fingerprint. The theoretical power spectrum function at the receiver $p_{Rx}(j\omega)$ is derived as follows:

$$P_{Rx}(j\omega) = H_{LED} * H_{channel} * G_{PD} * G_{circuit} * P_{input}(j\omega) \tag{7}$$

$$\omega = [2\pi f_1,\ 2\pi f_2,\ 2\pi f_3, \ldots, 2\pi f_n] \tag{8}$$

$$H_{LED}(j\omega) = \frac{\eta r_d Z_{in}}{((j\omega r_d C + 1)(R_s + Z_{in} + j\omega L) + r_d)^2} \tag{9}$$

$$H_{channel} = \frac{Adet(m+1)cos^m(\phi)}{2\pi D^2} \tag{10}$$

where H_{LED} is the power transfer function of the LED. It can be derived from the proposed LED equivalent circuit model. $H_{channel}$ is the power-loss function of the wireless optical channel [17]. G_{PD} and $G_{circuit}$ are the power gain of the photodiode and the VLC front-

end circuits, respectively. In this paper, the lights from the transmitter are considered to propagate only through line-of-sight (LOS), the non-line-of-sight (NLOS) propagation of lights is ignored. Based on the theoretical power spectrum function P_{Rx} and the practical measurement P_{rx}, optimization can be employed to fit the feature vector λ as defined by (11):

$$\min_{\lambda} \sum_{\omega=2\pi f_1}^{2\pi f_n} [P_{Rx}(j\omega) - P_{rx}(j\omega)] \tag{11}$$

Afterwards, all the feature vectors of devices from 1 to n will be extracted by the proposed method. The extraction result will be put into a model to train an identification classifier. Here, a multi-SVM classifier [31] is introduced as an example to solve the identification problem of M devices. We supposed that there are N training samples: $\{\lambda_1, LED_1\}, \ldots, \{\lambda_N, LED_N\}$. Here, λ_i is the extracted fingerprint and LED_i is the label that represents the feature vectors extracted from each LED. Subsequently, a one-against-all approach constructs M binary SVM classifiers, each of which separates one LED fingerprint from all the rest. Mathematically, ith SVM solves Equation (12) to yield the decision function (13):

$$\begin{cases} \arg\min L\left(\omega, \xi_j^i\right) = \frac{1}{2}\|\omega_i\|^2 + C\sum\limits_{l=1}^{N} \xi_j^i \\ y_j\left(\omega_i^T \phi\left(\lambda_j\right) + b_i\right) \geq 1 - \xi_j^i,\ \xi_j^i \geq 0 \end{cases} \tag{12}$$

$$f_i(\lambda) = \omega_i^T \phi\left(\lambda_j\right) + b_i \tag{13}$$

where ξ_j^i denotes slack variables that are related to the soft margin, and C is the tuning parameter used to balance the margin and the training error. $\phi\left(\lambda_j\right)$ is the nonlinear mapping of λ_j. It maps the λ_j to a much higher dimensional space in which the optimal hyperplane is found. During the classification phase, an unidentified feature vector λ is classified as LED_k which decision function produces the largest value (14).

$$f_i(\lambda) = \omega_i^T \phi k = \arg\max_{i=1,\ldots,M} f_i(\lambda) = \arg\max_{i=1,\ldots,M} \omega_i^T \phi(\lambda) + b_i\left(\lambda_j\right) + b_i \tag{14}$$

2.4. Envisioned Applications for the IoRL Security Framework

The threat that we would like to mitigate with the proposed LED fingerprinting method is as follows. The rogue device is a device placed by the attacker, which due to, e.g., a stronger signal, can lure users to connect to it and intercept valuable, confidential data send by the tricked users. Further in this paragraph we present how LED fingerprinting could be used in real-life systems. As an exemplary test system, we choose IoRL project [32]. The main subsystems of the IoRL system are optical RAN, UEs (User Equipment) and Intelligent Home IP Gateway (IHIPG). In the IHIPG, there is an OpenStack environment with SDN (Software Defined Network) which hosts various VNFs (Virtual Network Functions), for example, for security purposes. An example of the device that can be susceptible to such kind of attack is a LED device in the IoRL system. In effect, UE (User Equipment) receives data from the attacker's LED, which, for example, could lead to installation of malware on it. Thus, the security system should detect such a situation and react accordingly. As already mentioned in the previous section, in this scenario we assume that during the registration phase before installation each new LED is tested in the laboratory environment. Its fingerprint is extracted to create a sort of "signature" of the LED for further use in the next phases and stored in the security system's database enriched with the information where a given LED is physically installed.

Then, during the rogue LED detection phase, the security system periodically polls UE (using specialized software/firmware at UE) to establish the LED characteristics (i.e., LED fingerprint). The extracted LED fingerprints are sent to the security system for evaluation. Using these fingerprints and localization information security system verifies whether the extracted fingerprint is consistent with the fingerprint registered. In the case when the

attacker placed a rogue LED device, the extracted fingerprint should be inconsistent with the fingerprint of the LED placed in the security system database during the registration phase. As a result, if the attack is detected, the security system can block the traffic directed towards/outgoing from the LED (so exfiltration of the confidential data obtained by the attacker is possible), and the administrators can be notified about this incident.

Figure 3 presents the main components used during the detection of rogue LED attacks. The main steps of the proposed detection mechanism are as follows:

- Step 0: Register LED fingerprint and their localization database (this information is established and inserted to the database before LED installation)—the database is located at the security system.
- Step 1: A heartbeat-like protocol (UE <-> security subsystem) with which the security subsystem would be able to periodically poll the UE to initiate the LED fingerprint extraction process and securely transmit the determined fingerprint back to the security subsystem.
- Step 2: The measurement-based protocol (UE <-> LED) that would operate between the selected UE and the LED which would allow to determine the fingerprint of the LED under investigation.
- Step 3: The mechanism at the security subsystem that would compare the fingerprint of the chosen LED and its location with the corresponding data stored in the database.
- Step 4: In the case of a detected security breach, the security system can install rules on the SDN controller to block incoming/outgoing traffic to the LED and notify the administrators.

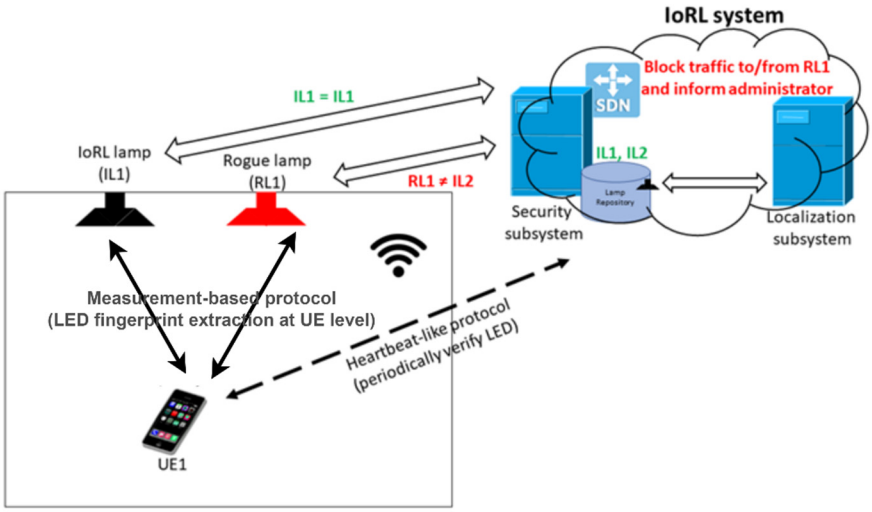


Figure 3. A block diagram of a typical 5G VLC multi-access scenario using the proposed security solution.

3. Demonstration and Evaluation

In this section, the feasibility and accuracy of the proposed method was evaluated by a demonstration implemented in a practical indoor environment.

3.1. Demonstration Setup

A flow chart of the demonstration and its realistic scenario are shown in Figure 4a,b. A server (Dell R740) acts as the 5G NR transmitter-generated 5G baseband signal. It modulates the user data with different modulation schemes which include QPSK, 16-QAM, 64-QAM and 256-QAM. As the modulated symbols were assigned to the 5G NR frame shown in Figure 4c, inverse Fast Fourier Transform (IFFT) processing and IQ modulation were applied to convert the OFDM frame to the time domain and guarantee the signal well matched with the IM/DD VLC system. Subsequently, a digital-analog (D/A) converter (USRP 2944R) and a DC bias transformed this digital signal to analog signal with an

appropriate DC component. This signal is sent to four LEDs (LUXEN 5050). Through an optical wireless channel, the signal from each LED is captured by a commercial receiver (HAM C5331-11) in sequence and digitized by an analog-digital (A/D) converter (USRP 2944R). Finally, the received signal is transferred back to the server to extract fingerprints.

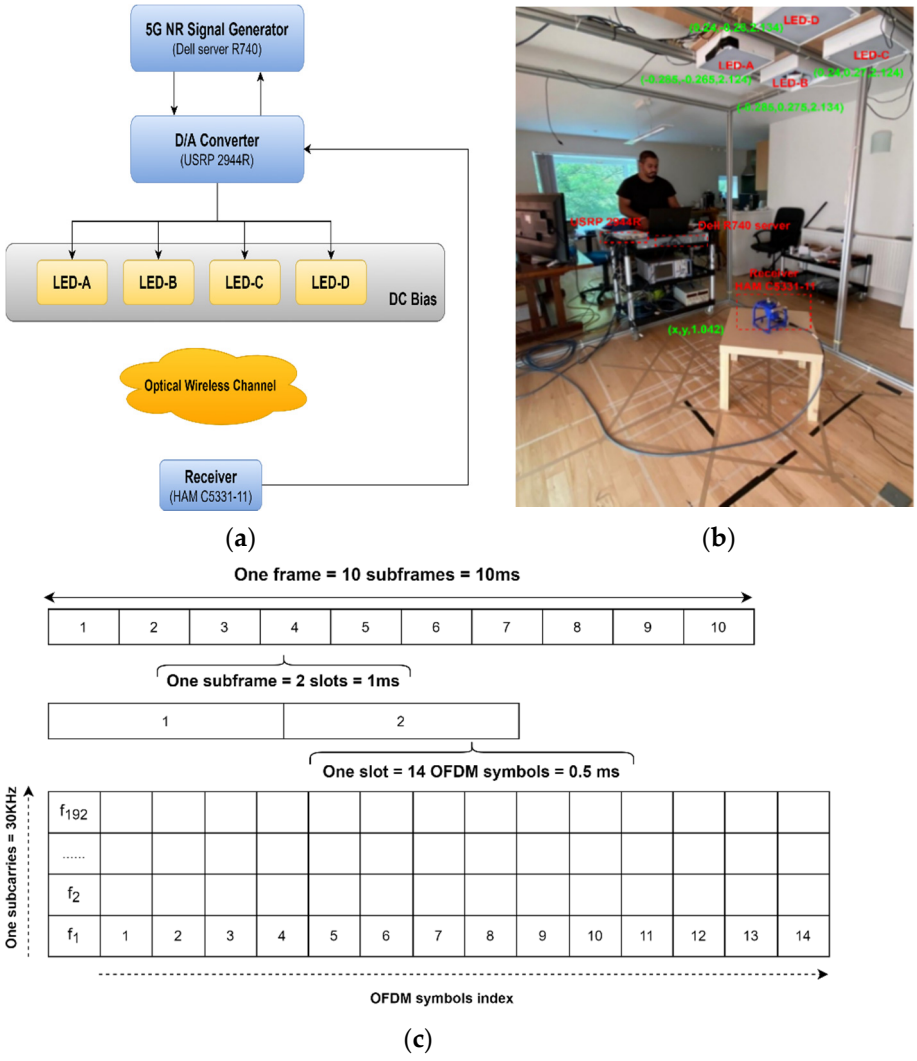


Figure 4. (**a**) A flow chart of the demonstration; (**b**) The realistic scenario; (**c**) The structure of 5G NR signal.

A 3D coordinate system was established to demonstrate the feasibility and accuracy of the proposed method for various distances and environments. According to Figure 4b, four LEDs were fixed on the ceiling in a known location. The receiver kept 1.042 m height and moved on a plane parallel to the ground. The distribution of the EVM (Error Vector Magnitude) of each LED in the whole area was tested to describe the optical wireless channel. Subsequently, signal samples from each LED were collected 10 times by the receiver at 24 different points. By using the proposed method, 960 LED fingerprints were extracted from all the samples and were randomly divided into training set and testing set in a ratio of 6:4. Several types of classifiers were employed to verify the accuracy of the extracted LED fingerprints.

3.2. Results and Analysis

Figure 5 illustrates 4 LEDs' distribution of the EVM in the whole area. According to the results, LED-A and LED-C had the largest and the second-largest coverage of the high-quality communication environment. On the contrary, the channel of the LED-

B and LED-D had limited quality. The phenomenon that the same type of four LEDs has different communication performance was caused by the non-linearity of the optical wireless channel.

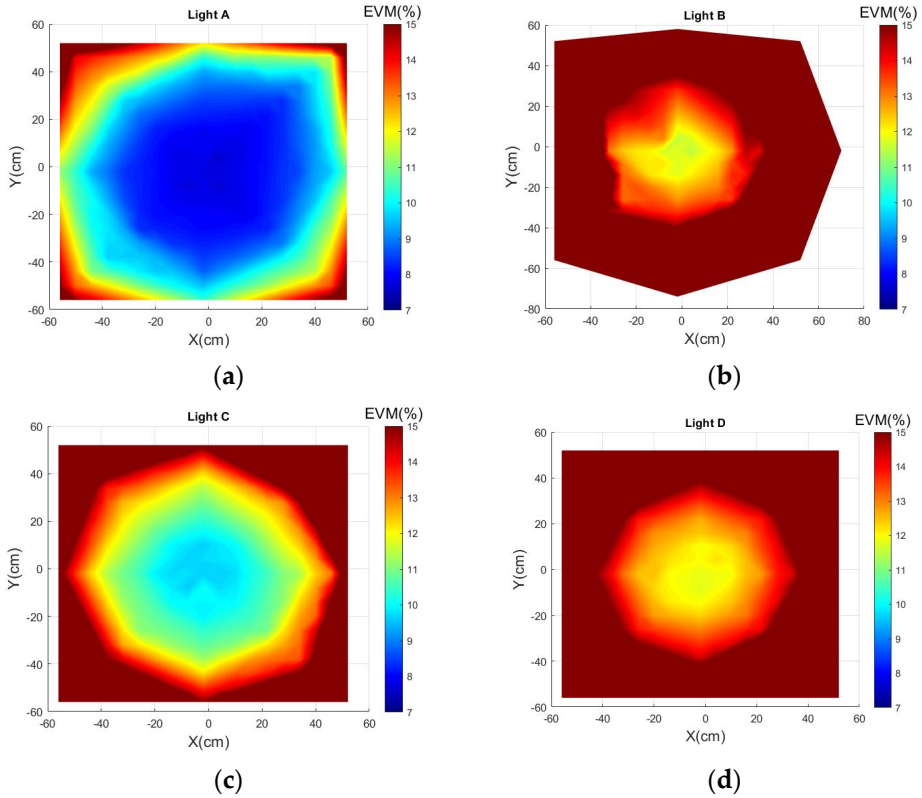


Figure 5. EVM distribution of LED in testbed: (**a**) EVM@LED-A; (**b**) EVM@LED-A; (**c**) EVM@LED-C; (**d**) EVM@LED-D.

Based on this environment, the total of 960 samples were captured by the receiver and, based on them, the LED fingerprints shown in Figure 6a were extracted. The extraction results were put into selected machine-learning algorithms, i.e., Decision Tree, Naive Bayes, SVM and KNN classifiers, respectively. The comparison of the verification accuracy is presented in Figure 6b. According to the obtained results, it is clearly visible that the proposed extraction method successfully extracted the LED fingerprints of four LEDs. Meanwhile, four machine-learning-based classifiers are able to distinguish these fingerprints appropriately.

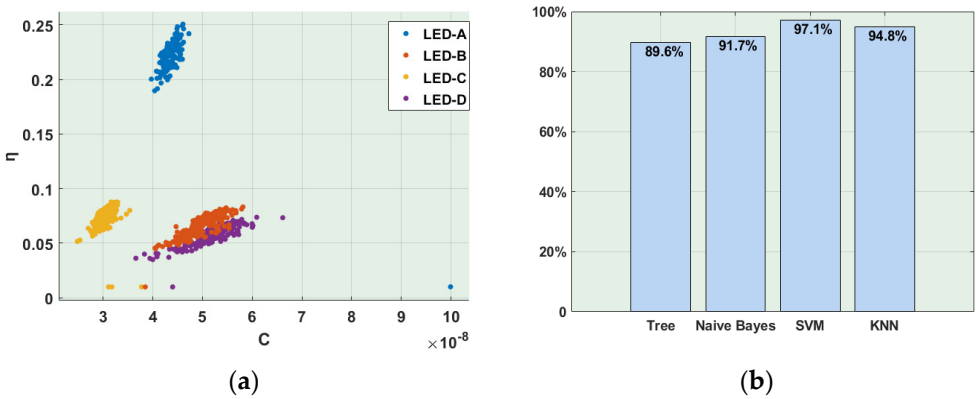
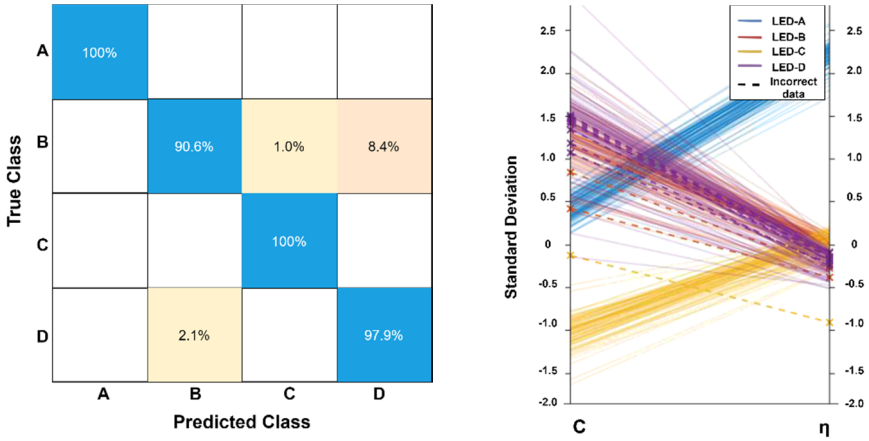


Figure 6. (**a**) Extracted LED fingerprints; (**b**) Comparison of verification accuracy.

Note that further investigation leads to the conclusion that the fingerprints of the LED-B and LED-D overlapped in some regions, which was the primary reason of the classifiers' misjudgment. In this case, the SVM classifier obtained the best performance due to its property of maximum classification margin and its ability of producing accurate and robust classification results for non-monotone and non-linearly separable input data. Moreover, the confusion matrix and parallel coordinate plots of the SVM classifier for the extraction and identification results are presented in Figure 7a,b.



(**a**) (**b**)

Figure 7. (**a**) The confusion matrix of the SVM classifier; (**b**) The parallel coordinate plots of the SVM classifier.

According to the confusion matrix, almost all the misjudgment is caused by the LED-B as 8.4% LED fingerprints of LED-B were regarded as the fingerprints of the LED-D. Meanwhile, 2.1% fingerprints of the LED-D were misclassified as the fingerprints of the LED-B. Additionally, the parallel coordinate plots reflected the distinction of each parameter for all the fingerprints. The LED-A, LED-B and LED-C had distinct convergence on the parameter *C*. On the contrary, the LED-D performed more divergently and overlapped with the LED-B. For the parameter η, all the LEDs were convergent; however, the LED-B, LED-C and LED-D overlapped in a small interval. This phenomenon can be explained as follows. First, the identification quality is influenced by the communication environment. The LED-A has the best EVM and covered almost the whole area, which caused the highest identification accuracy. On the contrary, the LED-B yielded the worst accuracy due to its limited EVM coverage. Secondly, the parameter η is sensitive to the communication environment. According to the theoretical analysis of the extraction, η represents the photoelectric efficiency. Once there is a large attenuation in the channel, then the η will be calculated near the boundary value. Consequently, it will lose the ability to describe the characteristics of the LED.

4. Conclusions and Future Work

In this paper, a novel device identification method was proposed to improve the security of VLC in the 5G network. This method extracts the unique fingerprints of LEDs from their emitted signals. By employing a machine-learning-based classifier to distinguish these LED fingerprints, the devices accessing the 5G network can be reliably identified. The advantage of the proposed method is that it can work in real time and uses OTP (One Time Pad) encryption, which fundamentally avoids the threat of pseudo base-station and KI (Key identifier) disclosure. The feasibility and high accuracy of device identification were verified by using proof-of-concept implementation in a practical indoor VLC-based 5G network. In order to establish the optimal tuning of this approach, the comparison of four types of machine-learning-based classifiers was conducted. The obtained results indicate

that the SVM classifier yields the best performance as it reaches the maximum accuracy of 97.1%. Additionally, the analysis of the confusion matrix and the parallel coordinate plots proved that the identification accuracy relies on the quality of the communication environment.

Our approach extracted the fingerprints of the transmitter in a VLC system to identify accessing devices. In future research, a bilateral identification mechanism which consists of Tx fingerprints and Rx fingerprints will be investigated to enrich the application scenario and further improve the security of the VLC system in the 5G network.

Author Contributions: Conceptualization, D.S., X.Z. and W.M.; methodology, D.S.; software, D.S.; validation, L.S., Y.Z.; formal analysis, D.S., A.V.; investigation, D.S, K.C.; data curation, B.M., K.A., J.C.; writing—original draft preparation, D.S.; writing—review and editing, W.M., K.C.; supervision, A.V.; project administration, X.Z.; funding acquisition, X.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the EU Horizon 2020 program towards the Internet of Radio-Light project H2020-ICT 761992.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Acknowledgments: The authors gratefully acknowledge the financial support of the EU Horizon 2020 program towards the Internet of Radio-Light project H2020-ICT 761992.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wang, J.; Spicher, N.; Warnecke, J.M.; Haghi, M.; Schwartze, J.; Deserno, T.M. Unobtrusive health monitoring in private spaces: The smart home. *Sensors* **2021**, *21*, 864. [CrossRef] [PubMed]
2. Honar Pajooh, H.; Rashid, M.; Alam, F.; Demidenko, S. Multi-layer blockchain-based security architecture for internet of things. *Sensors* **2021**, *21*, 772. [CrossRef] [PubMed]
3. Tsonev, D.; Videv, S.; Haas, H. Towards a 100 Gb/s Visible light wireless access network. *Opt. Express* **2015**, *23*, 1627–1637. [CrossRef] [PubMed]
4. Burchardt, H.; Serafimovski, N.; Tsonev, D.; Videv, S.; Haas, H. VLC: Beyond point-to-point communication. *IEEE Commun. Mag.* **2014**, *52*, 98–105. [CrossRef]
5. Tsiatmas, A.; Willems, F.M.; Linnartz, J.-P.M.; Baggen, S.; Bergmans, J.W. Joint Illumination and Visible-Light Communication Systems: Data Rates and Extra Power Consumption. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), IEEE, London, UK, 8–12 June 2015; pp. 1380–1386.
6. Rahman, A.B.M.M.; Li, T.; Wang, Y. Recent advances in indoor localization via visible lights: A survey. *Sensors* **2020**, *20*, 1382. [CrossRef] [PubMed]
7. Rehman, S.; Ullah, S.; Chong, P.; Yongchareon, S.; Komosny, D. Visible light communication: A system perspective—Overview and challenges. *Sensors* **2019**, *19*, 1153. [CrossRef] [PubMed]
8. *IEEE Standard for Local and Metropolitan Area Networks-Part 15.7: Short-Range Optical Wireless Communications*; IEEE: New York, NY, USA, 2018.
9. Shi, L.; Li, W.; Zhang, X.; Zhang, Y.; Chen, G.; Vladimirescu, A. Experimental 5G New Radio Integration with VLC. In Proceedings of the 2018 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS), Bordeaux, France, 9–12 December 2018; pp. 61–64.
10. Cabaj, K.; Gregorczyk, M.; Mazurczyk, W.; Nowakowski, P.; Żórawski, P. Network threats mitigation using software-defined networking for the 5G internet of radio light system. *Secur. Commun. Netw.* **2019**, *2019*, 1–22. [CrossRef]
11. Shi, L.; Zhang, X.; Vladimirescu, A.; Wang, Z.; Zhang, Y.; Wang, J.; Garcia, J.; Cosmas, J.; Kapovits, A. Experimental Testbed for VLC-Based Localization Framework in 5G Internet of Radio Light. In Proceedings of the 2019 26th IEEE International Conference on Electronics, Circuits and Systems (ICECS), Genova, Italy, 27–30 November 2019; pp. 430–433.
12. Abdaoui, R.; Zhang, X.; Xu, F. Potentiality of a Bi-Directional System Based on 60GHz and VLC Technologies for e-Health Applications. In Proceedings of the 2016 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), Nanjing, China, 16–19 October 2016; pp. 1–3.
13. Zhang, X.; Cosmas, J.; Meunier, B.; Ali, K.; Jawad, N.; Salih, M.; Meng, H.-Y.; Song, J.; Wang, J.; Tong, M.; et al. 5G Internet of Radio Light Services for Supermarkets. In Proceedings of the 2017 14th China International Forum on Solid State Lighting: International Forum on Wide Bandgap Semiconductors China (SSLChina: IFWS), Beijing, China, 1–3 November 2017.

14. Mostafa, A.; Lampe, L. Physical-Layer Security for Indoor Visible Light Communications. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, Australia, 10–14 June 2014; pp. 3342–3347.
15. Xu, Q.; Zheng, R.; Saad, W.; Han, Z. Device fingerprinting in wireless networks: Challenges and opportunities. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 94–104. [CrossRef]
16. Sun, H.; Zhu, X.; Liu, Y.; Liu, W. Construction of hybrid dual radio frequency RSSI (HDRF-RSSI) fingerprint database and indoor location method. *Sensors* **2020**, *20*, 2981. [CrossRef] [PubMed]
17. Yu, J.; Hu, A.; Zhu, C.; Peng, L.; Jiang, Y. Rf Fingerprinting extraction and identification of wireless communication devices. *J. Cryptol. Res* **2016**, *3*, 433–446.
18. Merchant, K.; Revay, S.; Stantchev, G.; Nousain, B. Deep learning for RF device fingerprinting in cognitive communication networks. *IEEE J. Sel. Top. Signal Process.* **2018**, *12*, 160–167. [CrossRef]
19. Dissanayake, S.D.; Armstrong, J. Comparison of Aco-Ofdm, Dco-Ofdm and Ado-Ofdm in Im/Dd systems. *J. Lightwave Technol.* **2013**, *31*, 1063–1072. [CrossRef]
20. Yin, Y.; Qiu, J.; Li, Z.; Cao, M. Research on secure debugging interaction of sensor nodes based on visible light communication. *Sensors* **2021**, *21*, 953. [CrossRef] [PubMed]
21. Hall, J.; Barbeau, M.; Kranakis, E. Detection of transient in radio frequency fingerprinting using signal phase. *Wirel. Opt. Commun.* **2003**, *7*, 13–18.
22. Kennedy, I.O.; Scanlon, P.; Mullany, F.J.; Buddhikot, M.M.; Nolan, K.E.; Rondeau, T.W. Radio Transmitter Fingerprinting: A Steady State Frequency Domain Approach. In Proceedings of the 2008 IEEE 68th Vehicular Technology Conference, Calgary, AB, Canada, 21–24 September 2008; pp. 1–5.
23. Peng, L.; Hu, A. A Design of Deep Learning Based Optical Fiber Ethernet Device Fingerprint Identification System. In Proceedings of the ICC 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 21–23 May 2019; pp. 1–6.
24. Peng, L.; Hu, A.; Jiang, Y.; Yan, Y.; Zhu, C. A Differential Constellation Trace Figure Based Device Identification Method for ZigBee Nodes. In Proceedings of the 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP), Yanghzhou, China, 13–15 October 2016; pp. 1–6.
25. Peng, L.; Hu, A.; Zhang, J.; Jiang, Y.; Yu, J.; Yan, Y. Design of a Hybrid RF Fingerprint Extraction and Device Classification Scheme. *IEEE Internet Things J.* **2018**, *6*, 349–360. [CrossRef]
26. Xing, Y.; Hu, A.; Yu, J.; Li, G.; Peng, L.; Zhou, F. A Robust Radio Frequency Fingerprint Identification Scheme for LFM Pulse Radars. In Proceedings of the 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 21–23 October 2019; pp. 1–6.
27. Yang, H.; Zhong, W.-D.; Chen, C.; Alphones, A.; Du, P.; Zhang, S.; Xie, X. Coordinated resource allocation-based integrated visible light communication and positioning systems for indoor IoT. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 4671–4684. [CrossRef]
28. Yang, H.; Zhong, W.-D.; Chen, C.; Alphones, A. Integration of visible light communication and positioning within 5G networks for internet of things. *IEEE Netw.* **2020**, *34*, 134–140. [CrossRef]
29. Shi, D.; Li, J.; Liu, Y.; Shi, L.; Huang, Y.; Wang, Z.; Zhang, X.; Vladimirescu, A. Effect of Illumination Intensity on LED Based Visible Light Communication System. In Proceedings of the 15th Symposium on Broadband Multimedia Systems and Broadcasting, Paris, France, 27–29 October 2020.
30. Vladimirescu, A. *The SPICE Book*; Wiley: New York, NY, USA, 1994.
31. Liu, Y.; Zheng, Y.F. One-against-All Multi-Class SVM Classification Using Reliability Measures. In Proceedings of the 2005 IEEE International Joint Conference on Neural Networks, Montreal, QC, Canada, 31 July–4 August 2005; Volume 2, pp. 849–854.
32. Cosmas, J.; Meunier, B.; Ali, K.; Jawad, N.; Salih, M.; Zhang, Y.; Hadad, Z.; Globen, B.; Gokmen, H.; Malkos, S. A 5G Radio-Light SDN Architecture for Wireless and Mobile Network Access in Buildings. In Proceedings of the 2018 IEEE 5G World Forum (5GWF), Silicon Valley, CA, USA, 9–11 July 2018; pp. 135–140.