Device Identification Method Based on LED Fingerprint for Visible Light Communication System

Dayu Shi, Xun Zhang, Andrei Vladimirescu, Lina Shi, Yanqi Huang, Yourong Liu

A Device Identification Method Based on LED Fingerprint for Visible Light Communication System

Dayu Shi†
Institut supérieur d'électronique de Paris, France
dayu.shi@isep.fr

Xun Zhang
Institut supérieur d'électronique de Paris, France
xun.zhang@isep.fr

Andrei Vladimirescu
Institut supérieur d'électronique de Paris, France
andrei.vladimirescu@isep.fr

Lina Shi
Institut supérieur d'électronique de Paris, France
lina.shi@isep.fr

Yanqi Huang
Institut supérieur d'électronique de Paris, France
yanqi.huang@isep.fr

Yourong Liu
University of Shanghai for Science and Technology, Shanghai, China
yourongliu93@gmail.com

ABSTRACT

In future networks, with the advent of massive machine type communications (mMTC), physical layer security is becoming a significant research area in the fifth generation (5G) and beyond 5G (B5G) communication systems. Device fingerprinting is a widely concerned technology to enhance the security of radio frequency (RF) based wireless systems. Meanwhile, visible light communication (VLC) is developing rapidly due to its remarkably high throughput performance in indoor situation and its security advantages for both privacy and health. In this paper, a VLC device fingerprint extraction and identification method are presented to improve the security of Visible Light Communication (VLC) in the 5G network. This method is based on the fingerprint of Light Emitting Diodes (LEDs) has been investigated theoretically and verified experimentally. Moreover, laboratory demonstration result shows that the fingerprints of five identical white LEDs could be extracted and identified successfully. The best identification accuracy was up to 98.8%.

CCS CONCEPTS

• Security and privacy →Mobile and wireless security.

KEYWORDS

Visible Light Communication, LED Fingerprint, Device Identification.

ACM Reference format:

Dayu Shi, Xun Zhang, Andrei Vladimirescu, Lina Shi, Yanqi Huang, and Yourong Liu. 2020. A Device Identification Method Based on LED Fingerprint for Visible Light Communication System. In *The 15th International Conference on Availability, Reliability and Security (ARES 2020), August 25–28, 2020, Virtual Event, Ireland.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3407023.3409214

ARES 2020, August 25–28, 2020, Virtual Event, Ireland
 ACM ISBN 978-1-4503-8833-7/20/08. . . $15.00
https://doi.org/10.1145/3407023.3409214

1 Introduction

With the enormous growth of wireless devices and the deep integration of information technology into numbers of industrial applications, the 5G network is expected to support massive user connections and exponentially increasing wireless services. In addition, due to a tremendous amount of Internet-of-Things (IoT) featured by the massive Machine-Type Communications (mMTC) extensive application in the 5G network, high data rates, high connection density, ultra-reliable low latency communication (URLLC) and security must be urgently provided by the future 5G network [2]. Hence, traditional radio frequency (RF) networks, which are already crowded, are arduous to satisfy these high demands [20]. One of the new communication technologies that has been proposed as an auspicious solution for the 5G and beyond is visible light communication (VLC) [3]. 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 [19]. These exciting assets generate considerable research and industrial interests for indoor VLC, especially with the approval of the IEEE 802.15.7 standard [10] and 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 [4,17,18]. The advantage of VLC compared to RF communication system [3] and its applications scenarios [1,27] has been discussed widely in the VLC literature. The security capacity of a VLC or Li-Fi network is proved to be at least an order of magnitude higher than a Wireless Fidelity (Wi-Fi) network due to the internet characteristics of the THz band [24]. 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, security of the transmitted signal cannot be guaranteed [13].

Meanwhile, 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 reducing the vulnerability of wireless networks to node forgery or insider attacks [23]. Its low-complexity and difficult or impossible to forge property could be perfectly matched with the security requirements of the 5G net-

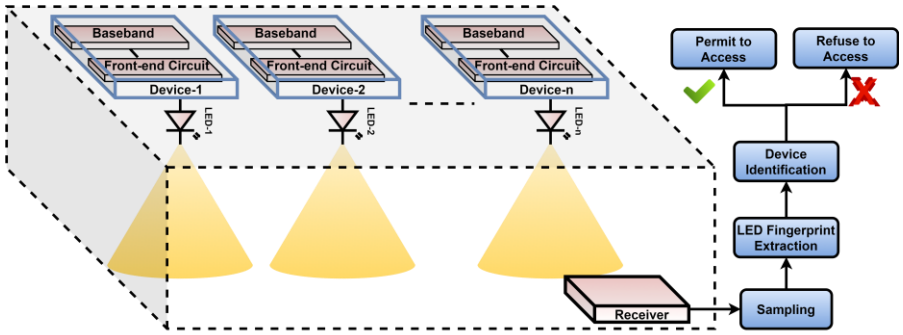


Figure 1: A block diagram of A Typical VLC Multi-access Scenario Using Our proposal

work. Notably, Wireless device identification via Radio Frequency (RF) fingerprint becomes a widely concerned physical layer security mechanism [26] and has been investigated in Wi-Fi, LTE and Zigbee systems. It provides a probability to accomplish the access authentication and 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 [12]. 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) [6] necessitate the development of new device fingerprinting methods specific to VLC systems.

There is little research on VLC device identification. However, drawing lessons from the successful works on device identification via RF fingerprint provides the possibility to propose the appropriate and efficient device identification method for VLC systems. The conception of RF fingerprint was firstly proposed by Hall et al. in 2003 [8]. This device identification method is featured by the detection of the transient signal emitted by the transmitter. Until 2008, Kennedy et al. was the first to introduce the device identification method based on the steady state signal [11]. 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 [14–16,22]. A comprehensive overview of high-level issues in the context of device identification method via RF fingerprint is summarized by Xu et al. [23].

In this paper, an LED fingerprint-based device-identification method is proposed for VLC communication systems. The inherent characteristics of LEDs are used as their fingerprints to identify each of them. Based on the proposed LED fingerprint model, the corresponding extraction method for device identification is designed and experimentally verified. The main contributions of this paper can be summarized as follows:

- The LED fingerprint model is established. Based on an LED equivalent circuit, the parameters, which represent the LED's inherent and stable characteristics are chosen to establish the LED feature vector. The feature vector of each LED is defined as its fingerprint.
- An LED fingerprint extraction and identification method are designed. By fitting the power spectrum of the received signal, the LED feature vector can be extracted. Meanwhile, a K-means clustering based classifier is employed to perform the registration for authorized devices. According to the comparison with the registered fingerprints, an access device can be identified.
- A simulation-based demonstration of the proposed device identification method is employed. The fingerprints of five commercial white LEDs were extracted and identified by the proposed method. The accuracy of the identification can reach maximum 98.8%.

The rest of this paper is organized as follows: section II illustrates the methodology of the proposed approach. The simulation-based demonstration results and analysis are detailed in section III. Finally, discussion and future work are contained in section IV.

2 METHODOLOGY OF DEVICE IDENTIFICATION

A block diagram of a typical VLC multi-access scenario using our proposal is shown in Fig 1. The physical layer of a VLC system c an be simplified by a baseband, a front-end circuit and an LED. B y using our proposal, the received signal from a device will be sam pled and the LED fingerprint will be extracted. If it is positively v erified by the device identification module, this device will get the access permission, otherwise it will be denied.

2.1 LED Fingerprint Model

It is noteworthy that there is little difference between the components of the system except for the LEDs. The nonlinearity and saturation characteristic support the possibility to distinguish LEDs even those from the same batch [25]. Thus, an LED fingerprint model has been established to characterize the distinctive feature of each device.

A small-signal equivalent circuit model of an LED in the VLC system is depicted in Fig 2. According to the equivalent circuit, p_{signal} is the power of 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 [5,21]:

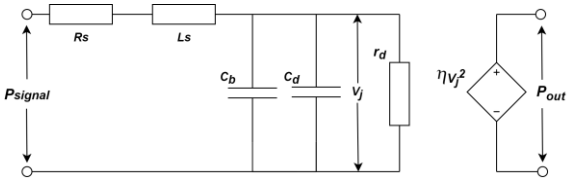


Figure 2: A Small-Signal Equivalent Circuit Model of an LED in the VLC System

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

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

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

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

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

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

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

2.2 Extraction and Identification Mechanism

In this section, the proposed LED fingerprint extraction and identification will be introduced. The extraction and identification Mechanism are illustrated in Fig.3.

The LED fingerprint extraction of device-i will be detailed as an example to illustrate the proposed method. The signal transmitted from device-i 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 results as the LED's fingerprint.

Before the identification, the registration of authorized devices should be processed first. The feature vector of each authorized device will be extracted several times by the above method. All the extracted feature vectors will be stored in a database and automatically classified into different classes by using a K-means

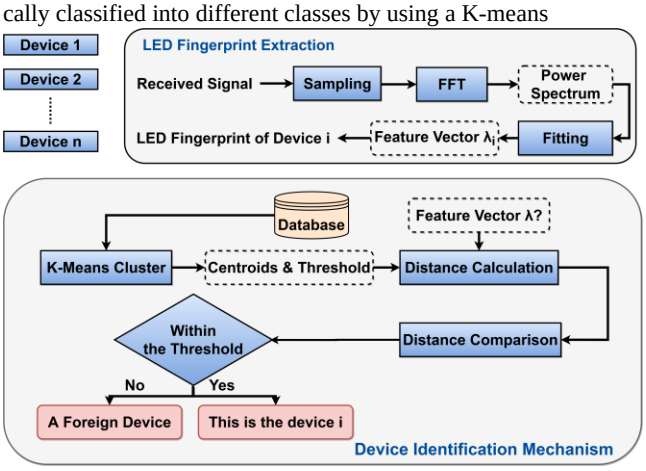


Figure 3: Figure 2: LED Fingerprint Extraction and Identification Mechanism

clustering classifier. All vectors of one class form a cluster representing an authorized device. Meanwhile, the classifier will also calculate a centroid for each cluster as its reference feature vector. However, there random errors can occur during the measurement and extraction. In order to adapt to this reality, a judgment threshold is introduced to avoid an erroneous decision.

When a device requests accessing, its feature vector will be extracted. By comparing the distance between its feature vector $\lambda?$ with each centroid, the nearest centroid-i will be chosen to decide. If this distance is within a prescribed limit, we consider that it is the device corresponding to the centroid i. If not, we consider that it is a foreign device and deny its access.

Although some well-known classifiers can provide excellent performance, for example the artificial neural networks (ANN), support vector machines (SVM), in this paper, we focus on proposing a feasible method of device identification for a VLC system. Hence, a simple minimum-distance-based K-means clustering classifier is employed.

2.3 Implementation of 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:

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

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

$$H_L\mathrm{ED}(j\omega) = \frac{\eta r_d Z_{in}}{\left((j\omega r_d C + 1)(R_s + Z_{in} + j\omega L) + r_d\right)^2} \tag{9}$$

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

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 [7]. 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 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):

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

Afterwards, the authorized devices will be registered. The feature vectors of devices 1 to k will be extracted by the proposed method. The extraction result will be saved into a set δ as an input parameter for the typical K-means clustering classifier employed in this work [9]. By using this classifier, all extracted feature vectors will be classified into different clusters and the centroids μi of each cluster will be computed out. Subsequently, the identification will be carried out by comparing the distance between the feature vector of accessing device with each centroid (12):

$$\Delta = \begin{cases} 0 & arg\,min\, i \sum_{i}^{n}\sum_{j}^{k} D_{ij} > \epsilon \\ n & arg\,min\, i \sum_{i}^{n}\sum_{j}^{k} D_{ij} \le \epsilon \end{cases} \quad (12)$$

where, Δ is the identification result, ϵ is the value of the threshold, and D_{ij} represents the distance between the feature vector i to the centroid j. If the feature vector of an accessing device is nearest to the centroid n and their distance is within the threshold ϵ, the identification result will return n. It represents that the accessing device is the authorized device n, otherwise, it will return 0 which means that this device is a foreign device.

3 DEMONSTRATION RESULTS

In order to evaluate the feasibility and accuracy of the proposed extraction and identification method, an experimental demonstration was implemented. The extraction results and the accuracy of identification are presented below. Moreover, the covariance of each LED's feature vectors was analyzed to evaluate the extraction quality. The identification accuracy under different threshold values has also been simulated to find out the optimum value of the threshold.

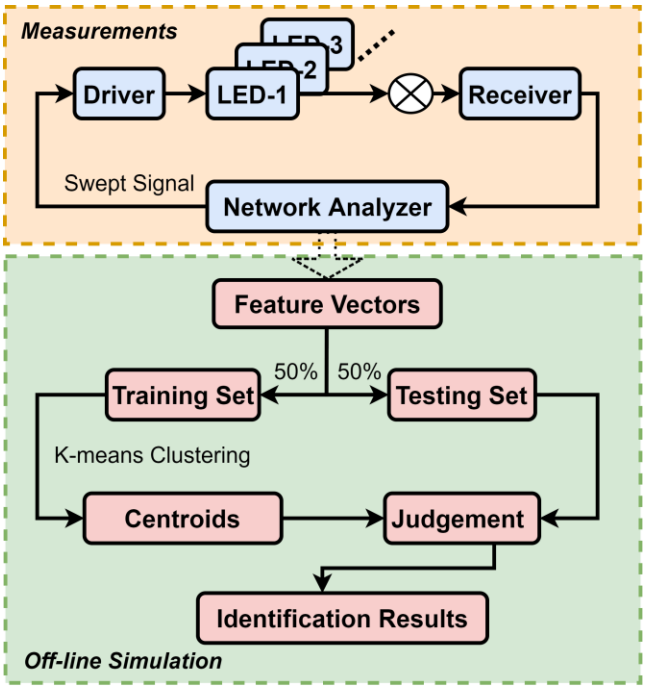
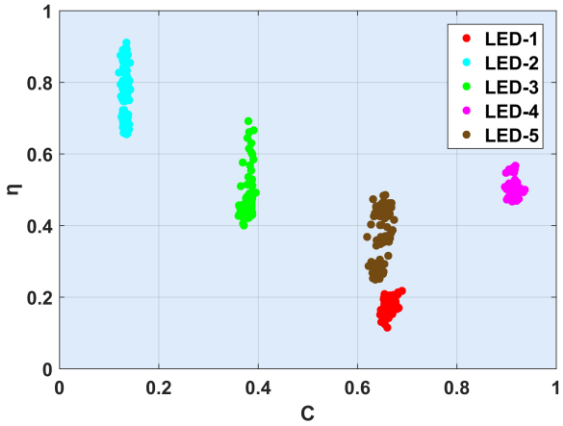


Figure 4: The Experimental Setup

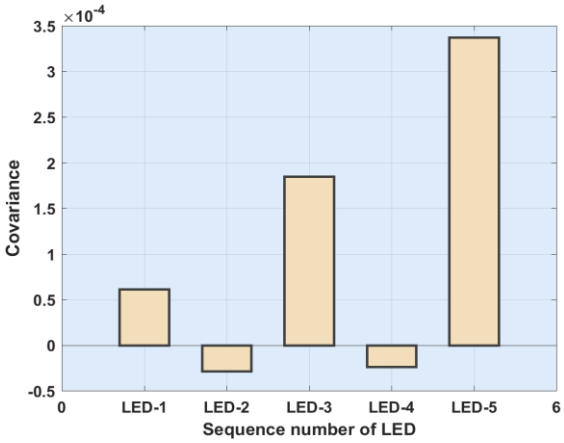
Figure 5: LEDs for Experiment

Table 1: Parameters of the Experiment.

Symbol	Value	Unit
P_{signal}	0	dBm
f	1-30	MHz
r_d	37	**Ω**
R_s	2.8	**Ω**
L_s	10^{-18}	H
D	0.1	m
ϕ	0	rad
$G_{circuit}$	40	dB
m	1.5	None unit
K	5	None unit

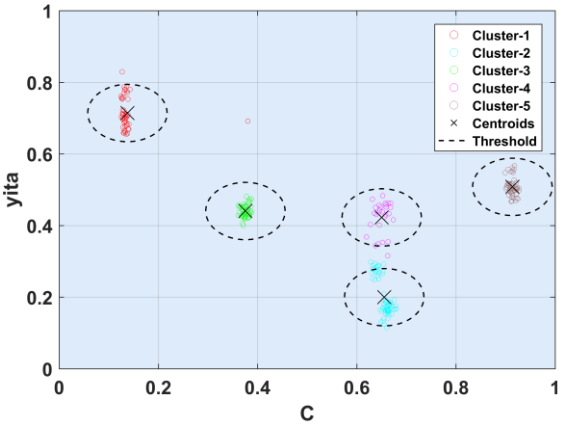


(a) Feature Vectors of the LEDs extracted from 100 times measurements

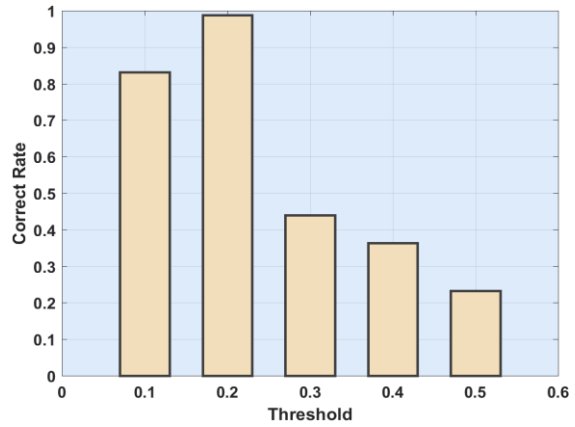


(b) The standard deviation of feature vectors vs. Numbers of measurements

Figure 6: LED Fingerprint Feature Vectors Extraction Results



(a) The trained classification model by k-means clustering classifier



(b) The accuracy rate of device identification in different threshold

Figure 7: The Simulation Results of VLC Device Identification

3.1 Experimental Setups

A block diagram of the experimental setup is shown in Fig.4. It consists of two parts: (i) the LED feature vectors extraction, (ii) the off-line simulation in a computer (security server). Five identical white LEDs (shown in Fig 5) were used to do this demonstration.

A. Extracted the feature vectors of 5 LEDs:

An Agilent E5061b Network Analyzer generated a swept signal passed through a driver, an LED, an optical wireless channel and a commercial receiver to calculate the power spectrum. Each LED was measured 100 times in this way. The feature vectors of the 5 LEDs were extracted from the measurements and did the normalization.

B. Registered the authorized devices:

For each LED, its feature vectors were randomly selected a half to save into the training set. They were regarded as the feature vectors of authorized devices. After the execution of the K-means clustering classifier, the training set were classified into 5 clusters and each cluster was calculated a centroid. The threshold was primarily set as 0.1.

C. Simulated the device identification:

Since the above registration had been accomplished, the rest feature vectors as the testing set was identified. The parameters of this experimental demonstration are shown in Table 1.

3.2 LED Feature Vector Extraction Results

The LED feature vector extraction results of the 5 LEDs are shown in Fig 6 (a). Each point of the diagram represents an extracted feature vector which is normalized and projected to a 2D coordinate system.

According to the extraction results, the feature vectors of each LED are clearly distinguishable. Furthermore, it is evident that for each LED, its theoretically unique and constant feature vector changed for each measurement and associated extraction. These

variation of feature vectors comes from the random error of measurements which are mainly caused by the noise of the VLC communication link such as: thermal and shot noise of devices, background noise of the optical wireless channel, distortion of diodes, etc. Here, the covariance of each LED's feature vectors was used to evaluate the random error of the extraction results (13):

$$\mathrm{cov}(\lambda) = \frac{1}{\mathrm{N}-1}\sum_{\mathrm{i}=1}^{\mathrm{N}}\left(\mathrm{C}^{\mathrm{i}} - \bar{C}\right) * \left(\eta^{\mathrm{i}} - \bar{\eta}\right) \qquad (13)$$

where N represents the extraction numbers, C and η are corresponding to the values of the feature vector. Fig 6 (b) shows the covariance value of each LED's feature vectors. The closer the value is to zero the lower the random error introduced during the measurement and extraction. Thus, LED-2 and LED-4 have the least interference of random error, while, on the contrary, LED-5 suffered the most impact from random errors.

3.3 Simulation of Device Identification

Based on the above extraction results, a simulation of device identification was carried out. The five clusters and the corresponding centroids of the training set obtained from the K-means clustering classifier are shown in Fig 7 (a). By using these centroids to identify the feature vectors in the testing set, the accuracy rate was 83.2% while the threshold was set to 0.1.

Moreover, Fig 7 (b) represents the relation between the accuracy and the threshold values. According to the comparison, it is evident that the best threshold value equals to 0.2. At this threshold value, the accuracy rate reaches 98.8%.

4 DISCUSSION AND FUTURE WORK

In this paper, a device identification method based on a LED's fingerprint specific to VLC systems is proposed. This method extracts the unique LED fingerprint to identify the devices in a multi-access VLC scenario to further strengthen the network security. This proposal provides a potential solution of accessing devices management and avoiding node forgery for VLC system in the 5G network. The development of the LED fingerprint model and the corresponding extraction method are detailed. Additionally, a K-means clustering classifier-based identification method is investigated theoretically and verified experimentally. The extraction results and the accuracy of identification are presented in this paper. Moreover, the covariance of each LED's feature vectors was analyzed to evaluate the extraction quality. The identification accuracy under different threshold values has also been simulated to find out the optimum value of the threshold. The demonstration results show that the proposed method had an up to 98.8% accuracy rate to identify the accessing devices of VLC system. This accuracy indicated that this method has strong potential to strengthen the security for VLC system in the 5G network.

Future work will focus on evaluating and optimizing this method in a more complete system and realistic environment. The proposed LED fingerprint extraction and identification method will be integrated in the SDN-based integrated security framework for the Internet of Radio Light (IoRL) system. To simplify our test and focus on the validation of our proposal, the experimental environment is set as ideal as possible, where only Line-of-Sight light is considered. The illuminance is set as a constant also. In our future work, we are planning to test the reliability of our method under different ambient light environments by changing the transmitter and receiver distance and adding None line-of sight propagation of light. Finally, there is still plenty of room for improvement by using more advanced classifier, such as the artificial neural networks (ANN), support vector machines (SVM), etc.

ACKNOWLEDGMENT

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

REFERENCES

[1] Rahma Abdaoui, Xun Zhang, and Fanfan Xu. 2016. Potentiality of a bi-directional system based on 60GHz and VLC technologies for e-health applications. In *2016 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)*, IEEE, 1–3.

[2] Mohamed Amine Arfaoui, Mohammad Dehghani Soltani, Iman Tavakkolnia, Ali Ghrayeb, Majid Safari, Chadi Assi, and Harald Haas. 2020. Physical layer security for visible light communication systems: A survey. *IEEE Communications Surveys & Tutorials* (2020).

[3] Harald Burchardt, Nikola Serafimovski, Dobroslav Tsonev, Stefan Videv, and Harald Haas. 2014. VLC: Beyond point-to-point communication. *IEEE Communications Magazine* 52, 7 (2014), 98–105.

[4] Krzysztof Cabaj, Marcin Gregorczyk, Wojciech Mazurczyk, Piotr Nowakowski, and Piotr Żórawski. 2019. Network threats mitigation using Software-Defined Networking for the 5G Internet of Radio Light system. *Security and Communication Networks* 2019, (2019).

[5] Peng Deng and Mohsen Kavehrad. 2016. Effect of white LED DC-bias on modulation speed for visible light communications. *arXiv preprint arXiv:1612.08477* (2016).

[6] Sarangi Devasmitha Dissanayake and Jean Armstrong. 2013. Comparison of aco-ofdm, dco-ofdm and ado-ofdm in im/dd systems. *Journal of lightwave technology* 31, 7 (2013), 1063–1072.

[7] Zabih Ghassemlooy, Wasiu Popoola, and Sujan Rajbhandari. 2019. *Optical wireless communications: system and channel modelling with Matlab®*. CRC press.

[8] Jeyanthi Hall, Michel Barbeau, and Evangelos Kranakis. 2003. Detection of transient in radio frequency fingerprinting using signal phase. *Wireless and Optical Communications* (2003), 13–18.

[9] John A Hartigan and Manchek A Wong. 1979. Algorithm AS 136: A k-means clustering algorithm. *Journal of the royal statistical society. series c (applied statistics)* 28, 1 (1979), 100–108.

[10] Steve Hranilovic and Frank R Kschischang. 2004. Short-range wireless optical communication using pixilated transmitters and imaging receivers. In *2004 IEEE International Conference on Communications (IEEE Cat. No. 04CH37577)*, IEEE, 891–895.

[11] Irwin O Kennedy, Patricia Scanlon, Francis J Mullany, Milind M Buddhikot, Keith E Nolan, and Thomas W Rondeau. 2008. Radio transmitter fingerprinting: A steady state frequency domain approach. In *2008 IEEE 68th Vehicular Technology Conference*, IEEE, 1–5.

[12] Kevin Merchant, Shauna Revay, George Stantchev, and Bryan Nousain. 2018. Deep learning for RF device fingerprinting in cognitive communication networks. *IEEE Journal of Selected Topics in Signal Processing* 12, 1 (2018), 160–167.

[13] Ayman Mostafa and Lutz Lampe. 2014. Physical-layer security for indoor visible light communications. In *2014 IEEE International Conference on Communications (ICC)*, IEEE, 3342–3347.

[14] Linning Peng and Aiqun Hu. 2019. A design of deep learning based optical fiber ethernet device fingerprint identification system. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, IEEE, 1–6.

[15] Linning Peng, Aiqun Hu, Yu Jiang, Yan Yan, and Changming Zhu. 2016. A differential constellation trace figure based device identification method for ZigBee nodes. In *2016 8th International Conference on Wireless Communications & Signal Processing (WCSP)*, IEEE, 1–6.

[16] Linning Peng, Aiqun Hu, Junqing Zhang, Yu Jiang, Jiabao Yu, and Yan Yan. 2018. Design of a hybrid RF fingerprint extraction and device classification scheme. *IEEE Internet of Things Journal* 6, 1 (2018), 349–360.

[17] Lina Shi, Wei Li, Xun Zhang, Yue Zhang, Gaojie Chen, and Andrei Vladimirescu. 2018. Experimental 5G new radio integration with VLC. In *2018 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, IEEE, 61–64.

[18] Lina Shi, Xun Zhang, Andrei Vladimirescu, Zhan Wang, Yue Zhang, Jintao Wang, Jorge Garcia, John Cosmas, and Adam Kapovits. 2019. Experimental testbed for VLC-based localization framework in 5G Internet of Radio Light. In *2019 26th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, IEEE, 430–433.

[19] Anagnostis Tsiatmas, Frans MJ Willems, Jean-Paul MG Linnartz, Stan Baggen, and Jan WM Bergmans. 2015. Joint illumination and visible-light communication systems: Data rates and extra power consumption. In *2015 IEEE International Conference on Communication Workshop (ICCW)*, IEEE, 1380–1386.

[20] Dobroslav Tsonev, Stefan Videv, and Harald Haas. 2015. Towards a 100 Gb/s visible light wireless access network. *Optics express* 23, 2 (2015), 1627–1637.

[21] Andrei Vladimirescu. 1994. *The SPICE book*. Wiley New York.

[22] Yuexiu Xing, Aiqun Hu, Jiabao Yu, Guyue Li, Linning Peng, and Fen Zhou. 2019. A Robust Radio Frequency Fingerprint Identification Scheme for LFM Pulse Radars. In *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, IEEE, 1–6.

[23] Qiang Xu, Rong Zheng, Walid Saad, and Zhu Han. 2015. Device fingerprinting in wireless networks: Challenges and opportunities. *IEEE Communications Surveys & Tutorials* 18, 1 (2015), 94–104.

[24] Liang Yin and Harald Haas. 2018. Physical-Layer Security in Multiuser Visible Light Communication Networks. *IEEE J. Select. Areas Commun.* 36, 1 (January 2018), 162–174. DOI:https://doi.org/10.1109/JSAC.2017.2774429

[25] Kai Ying, Zhenhua Yu, Robert J Baxley, Hua Qian, Gee-Kung Chang, and G Tong Zhou. 2015. Nonlinear distortion mitigation in visible light communications. *IEEE Wireless Communications* 22, 2 (2015), 36–45.

[26] J Yu, A Hu, C Zhu, L Peng, and Y Jiang. 2016. Rf fingerprinting extraction and identification of wireless communication devices. *J. Cryptologic Res* 3, 5 (2016), 433–446.

[27] Xun Zhang, John Cosmas, Ben Meunier, Kareem Ali, Nawar Jawad, Mukhald Salih, Hong-Ying Meng, Jian Song, Jintao Wang, Min Tong, and others. 2017. 5G Internet of radio light services for supermarkets.