Can Commercial LED Bulbs Pose a Threat to PLC System Security?

Yara Yaacoub, Fabienne Nouvel, Sylvain Haese, Jean-Yves Baudais

Can Commercial LED Bulbs Pose a Threat to PLC System Security?

Yara Yaacoub, F. Nouvel, S. Haese and J.-Y. Baudais

***Abstract*—Techniques that improve interfacing between power-line communication (PLC) systems and LED-based visible light communication (VLC) systems start to gain attention in recent years. Indeed, this hybrid system is able to provide simultaneously power, lighting, and data transmission. Contrariwise, if the integration between PLC and commercial LED bulbs is done unintentionally, the risks of PLC data leakage by commercial LED bulbs must be carefully analyzed. Thus, in this paper, the risks of eavesdropping on the PLC network via commercial LED bulbs are studied. The impact of the LED driver on PLC data leakage through LED bulbs is explained. The electrical-optical channel transfer function for different LED bulbs and the power spectral density of the signal received through the LED bulbs when two commercial powerline modems are plugged into the same power line are measured. Afterwards, pseudo random binary sequence signals are injected into the electrical-optical channel in order to assess quantitatively the possibility to extract information from the received signal. Finally, simple LED driver modifications that foster and increase the leakage are analyzed.**

***Index Terms*—power-line communication; Light-emitting diode; LED drivers; eavesdropping.**

I. Introduction

Recently, lighting industries have adopted LEDs for almost all of their applications. LEDs have proven *i*) to be energy efficient, *ii*) to not dissipate too much heat, *iii*) to have a very long lifetime and *vi*) to have a good color rendering. This great spread of LEDs capabilities prompted researchers to conduct studies on the possibility of using these lamps for communication. Their successful results have led to several visible light communication (VLC) standards like IEEE 802.17.5 [1] and ITU-T G.9991 [2]. However, VLC needs a backbone system that links LEDs to the Internet and extends the VLC range as it is limited due to the inability of light to penetrate through opaque obstacles. Fortunately, powerline communication (PLC) system can solve this problem and simultaneously provide power and data to LEDs.

PLC and VLC integration was firstly proposed by [3], [4], using single carrier phase shift keying. Subsequently, studies began to develop this idea in order to get a faster and more robust PLC-VLC system. In this regard, in [5], orthogonal frequency division modulation (OFDM) is applied in PLC-VLC transmission, reducing the effect of channel fading and frequency selectivity to reach higher throughput and get better spectral efficiency. In [6], a PLC-VLC system based on the use of a DC biased optical OFDM (DCO-OFDM) is proposed in order to exploit its clipping feature to reduce the impulsive noise of the PLC channel. Similarly in [7], asymmetrically clipped optical OFDM (ACO-OFDM) is employed in the hybrid PLC-VLC system, taking advantage of the nulling feature of the ACO-OFDM to mitigate the PLC channel impulsive noise. In [8], low complexity amplify and forward (AF) PLC-VLC system is proposed using spatial optical OFDM to reduce the peak to average power ratio. The AF module allows a direct transmission of the PLC signal through the optical system without making any modification. However in [9], decode and forward (DF) protocol is used in indoor broadcasting PLC-VLC system. Unlike the AF, the DF relay fully recovers the PLC data, re-encodes it to adapt it to the optical system and then re-transmits it via the VLC system. Despite the complexity of the DF relay, it is proven to offer better performance compared to the AF. Finally, in [10], a successful HomePlugAV (HPAV) signal transmission is carried out through a simple optical system without making any modification to the original HPAV signal.

As mentioned in the previous paragraph, all attempts are made to promote and facilitate PLC-VLC integration. However, the risks of PLC data leakage via domestic LED bulbs cannot be neglected. Especially because the LED bulbs are plugged in the powerline network. This aspect has never been discussed in literature up to our knowledge. Usually, when talking about the security threat of a PLC system, attentions are drawn to the electromagnetic radiation of PLC data near the powerline cable. Indeed, the electromagnetic radiation of the PLC signal, when it propagates through an unshielded power cable, can be detected by any wireless communication device operating in the same frequency band [11]. In this case we are talking about a wireless side or auxiliary channel. However, one may wonder if there is another way to eavesdrop on the PLC network through LED luminary. Thus, the idea of eavesdropping to the PLC network through domestic LED bulbs comes after validating the ability of the power LED to transmit HPAV signals without any modification to the original signal before being transmitted to the optical system. It should be mentioned that the power LED are originally intended for lighting [10].

In this paper, the leakage of broadband PLC signals through LED bulbs light is investigated when there is no particular match between the PLC system and the LED bulbs. Several commercial LED bulbs of different brands are tested. Further

Authors are with Univ Rennes, INSA Rennes, CNRS, IETR-UMR 6164, F-35000 Rennes, France. email: yara.yaacoub@insa-rennes.fr

978-1-6654-3540-6/22

analyses of LED drivers are performed to find out technologies that are most prone to leak. In addition, simple modifications are performed on some LED drivers to show that, in a very easy way, the leakage can be fostered even through the least leaking bulbs.

The rest of this paper is organized as follows: in Section II, a brief survey of the most commonly used LED drivers in the domestic lighting industry is carried out. In Section III, the leakage channel is studied taking into account a large number of LED bulbs. In Section III-A, two experimental setups are described, specifying the selected parameters of their instruments. In III-A1, measurement of the transfer function (TF) of the auxiliary electrical-optical channel is performed. In III-A2, measurements of the power spectral density (PSD) of the signal received by the electrical-optical channel are also carried out. In III-A3, a preliminary experiment based on the transmission of the pseudo random binary sequence (PRBS) is used as a channel sounding signal to better analyzed the auxiliary channel, especially when this channel exhibits high attenuation levels. Moreover, the results of the three experiments are interpreted and analyzed in Section III-B. In Section IV leakage enhancement is studied. The modifications made to the LED drivers to facilitate the leak are detailed in IV-A. The tests described in Section III-A are repeated with the modified LED bulbs and the results obtained are presented in IV-B. Finally, the paper ends with concluding remarks in Section V.

II. LED Drivers

As we aim to study the possibility of signal leakage through LED bulbs, it is necessary to analyze the LED drivers that power them because the PLC signal should traverse the drivers before reaching the LED array. The driver circuit is an indispensable component in the LED light bulbs. It provides the necessary amount of voltage and current to ensure the best brightness and the longest lifetime. The driver topology differs depending on the size of the bulb, the environment in which the bulb will be used in, and the available power source [12]. There are two main types of LED drivers: passive and active. The passive LED driver is the simplest and most reliable circuit because it uses only passive components. However, it has a low power factor, bulky components, and inaccurate current control, thus limiting its use to applications that prioritize reliability over efficiency. This kind of drivers is typically used in outdoor lighting systems where they are exposed to harsh environmental conditions [13]. Moving on to active LED drivers, they are divided into linear regulators (LR) and non-linear or switch mode power supplies (SMPS). The LR has slightly lower efficiency than SMPS. However, the LR allows precise current control, does not require electromagnetic interference (EMI) filters, and requires a limited number of surface mounted components (SMC) that can be mounted on the same board with a LED array. Hence, the LR is extensively used in low-power applications [14]. Whereas, in applications where power efficiency and current control are required but the cost does not come in priority, SMPS is chosen.

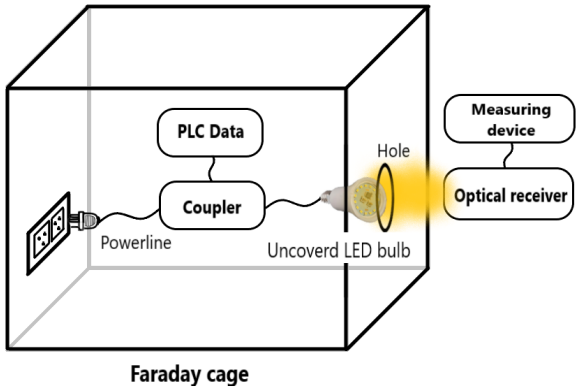

Figure 1. Experimental setup schema.

The main drawback of the SMPS driver is the generation of significant harmonics which can reach hundreds of MHz. These harmonics can easily cause high emissions hence the need for an EMI filter [15]. After examining many LED bulbs in the 6–8 watt power range, we find that most of them use an active LR and some high-end bulbs use a SMPS. So, in the upcoming sections of this paper, only LED bulbs with LR and SMPS drivers are tested.

III. Leakage assessment

A. Experimental setup

In this section, several LED bulbs are tested. The chosen LED bulbs belong to different price ranges and their power consumption varies between 6 W and 9 W (see Table I). As seen in the setup schema of Fig. 1, to prevent the powerline cable radiations from interfering with the optical emissions and disturbing the measurement results, the transmitter elements (the powerline cable, the PLC coupler or the PLC modems, and the LED bulbs) are placed inside a Faraday's cage. The optical receiver and the measuring instrument are placed outside the cage. The LED light is transmitted to the optical receiver through a hole in the cage. The optical receiver is composed of a lens to concentrate the received optical power, a photodiode to transform the received optical power into electric current, and a transimpedance amplifier that amplifies and transforms the received photocurrent into voltage. It should be noted that the LED bulbs are uncapped to maximize the amount of light passing through the hole as illustrated in Fig. 1. The testbed components parameters are detailed in the Table II.

1) Electrical-optical channel response: The TF of the electrical-optical channel is measured in order to evaluate the bandwidth of the commercial bulb. This bandwidth can be limited due to the existence of the driver which filters the high frequencies and the limited bandwidth of the white LED. Thus, the cascaded electrical-optical channel is measured using a network analyzer with a transmitted signal power of 10 dBm. The measured band is 300 kHz–100 MHz, and the step size

Table I
SPECIFICATIONS OF THE TESTED COMMERCIAL LED BULBS.

LED bulb	Driver	Consumed Power (W)	price (€)
Bailey	LR	8	2.5
Aric	LR	9	3.36
LSC	LR	9	1.29
Eurodomest	LR	6	0.99
SLV	SMPS	9.1	11.3
Philips Corepro	SMPS	7.5	5.29

Table II
SPECIFICATIONS OF THE TESTBED.

Index	value
Powerline cable length	1.5 m
PLC coupler cutoff frequency	28 MHz
distance between the bulb and the receiver	25 cm
hole diameter	3 cm
photodiode active area	1 mm^2
photodiode sensitivity	0.46 A/W
transimpedance gain	0.2 MΩ
optical receiver bandwidth	70 MHz
Network analyzer measured bandwidth	300 kHz-100 MHz
spectrum analyzer measured bandwidth	20 kHz-30 MHz

is 400 kHz. The network analyzer's output signals are injected into an isolated PLC network via a PLC coupler. The LED bulb is connected to the same electrical network. The LED driver filters some of the RF signals and the rest traverses the drivers to the LED array where it will be transduced from an electrical to an optical signal. The photodiode receives the optical signal and transforms it into an electrical signal, then it is amplified by the transimpedance amplifier to be reinjected into the network analyzer that will calculate the channel TF.

2) PSD of the HomePlugAV leaked signal: In this experiment, the HPAV is chosen among the various PLC specifications (e.g., HD-PLC, United Powerline Alliance, Open PLC European Research Alliance [16], etc). In fact, HPAV is a specified PLC standard for fast home communication. It has a large physical bandwidth operating in the 2–30 MHz band. The physical layer uses the OFDM modulation technique with an adaptive bit loading scheme to avoid PLC channel impairments [17].

The maximum value of the PSD of the received signal is measured using the "maxhold" function of the spectrum analyzer. In this case, the LED bulb is plugged in the same powerline network with two commercial HPAV modems (Dlan 200 AV from Devolo), that can transmit up to 200 Mbit/s. One modem acts as a client which sends UDP packets to the other modem (server). The spectrum analyzer measures the PSD of the signal received by the electrical-optical channel in a 20 kHz–30 MHz band with a step size of 40 kHz.

3) PRBS transmission through the auxiliary PLC-VLC channel: In this part, a preliminary experiment is performed to check if the level of the leakage can be correctly detected, especially when the auxiliary channel exhibits a high attenuation. Thus, two signals of 10 and 30 Mbit/s, consisting of a series of 10 identical pseudo-random binary sequence (PRBS) of order 11 are coupled to the electrical network where the LED bulb is connected. The signals are generated using a series waveform generator (RIGOL DG952 with 16 bits resolution). The optical receiver signal is acquired and digitized using an oscilloscope (LeCroy 64 MXs-A, 8 bits resolution). It should be emphasized that the PRBS is a maximum length sequence generated using a deterministic algorithm. However, they have random statistical behavior. This sequence has the property of having a very narrow and accentuated correlation peak which facilitates its detection even if it becomes very noisy.The spread factor of the chosen PRSB is $2^{11} - 1$, i.e., 33 dB. Thus, the cross-correlation peaks of the received signal with the already known PRBS sequence are calculated for all LED bulbs to quantitatively assess the ability of LED bulbs to leak.

B. Results and discussion

In this section the results of the three experiments described in Section III are presented. It should be noted that due to the space limitation in this paper, only the most significant results are presented. Fig. 2a gives the electrical-optical TF when the LED bulbs are covered with an opaque screen (dashed red curves) and in the absence of the opaque screen (blue solid curves). It should be noted that the Bailey and LSC bulbs use a LR, whereas the Philips bulb uses a SMPS. It is clear from Fig. 2a that the difference between the dashed blue and red curves in the case of the LSC LED cannot be neglected. The TF shows an attenuation of -48 dB at 30 MHz when the LED is not covered versus an attenuation of -68 dB at the same frequency in the case where it is covered with an opaque screen. However, for the other two LED bulbs (Bailey and Philips), they have very limited bandwidth and the difference between the red and blue curves are barely recognizable.

Moving to the experimental test described in Section III-A2, the results in Fig. 2b show the PSD of the injected HPAV signal (black dotted-dashed curve), the PSD of the received signal through the commercial LED bulbs when the HPAV modems are ON (TX modem connected, transmission of PLC signal, blue solid curve) and OFF (modem connected but no PLC transmission, only noise) (red dashed curve). As seen in Fig. 2b, the PLC signal leakage through commercial LED bulbs seem possible, as is the case of the LSC LED bulb. The received signal PSD at 12 MHz is -39 dBm against a noise PSD of -42 dBm. On the other hand, for the Bailey and Philips bulbs, the HPAV spectrum is not obvious. The results of the previous paragraph show that it may be possible to extract certain information from the signal emitted by the LED bulbs tested. However, for some LEDs, it seems difficult to validate precisely this possibility using the previous measurements.

To check quantitatively the risk of non-intentional PLC leakage, we have transmitted a PRBS signal and measured the cross-correlation peak value of the received PRBS signal as detailed in Section III-A3. Fig. 2c shows the average value of the cross-correlation peaks of the ten sequences sent to each

LED bulb. From Fig. 2c, it can be noticed that the sequences are correctly detected for all the LED bulbs. However, the average cross-correlation peaks vary from LED to LED. By comparing the bulbs having LR to those having SMPS, it can be seen that the bulbs with LR reach higher peak values than those with SMPS. In all cases, the auxiliary channel attenuations are lower than 38 dB with the experimental setup.

IV. LEAKAGE ENHANCEMENT

A. Experimental setup

The existence of a smoothing capacitor at the output of the AC/DC rectifier, of the active linear driver as well as of the EMI filter of the SMPS driver, can block the arrival of PLC data to the LED and reduce data leaks. In order to facilitate the PLC signals transmission through LED bulbs, simple modifications are made to their driver. We chose Bailey and Philips LED bulbs for the modifications because the results in Section III-B show that these bulbs leak less than other tested bulbs with similar drivers. Fig. 3a shows the active LED driver circuit of the Bailey LED bulb before and after modifications and Fig. 3b shows the driver of Philip LED bulb before and after modifications. As it can be seen in these figures, two capacitors have been added to filter out the AC signal and inject the PLC data signal directly into the LED array. A resistor is also added in series with the smoothing capacitor in the LR and in series to LED array in the SMPS to increase the leakage ability of capacitors. It should be mentioned that these modifications.It should be noted that these modifications do not disturb the amount of power delivered to the LED array. Afterwards, the three experiments described in III-A are repeated with these modified bulbs.

B. Results

The TF of the modified LED bulbs are presented in Fig. 4a. In the case of uncovered LED bulb with an opaque screen, the attenuation which was -67 dB at 30 MHz before modifications becomes -52 dB after modification. Whereas, in the case when the LED is covered, the attenuation remains equal to -67 dB. Moving on to the Philips LED bulb, the modifications cannot improve the bandwidth in the same way as in the case of the Bailey, especially for frequencies below 20 MHz. In fact, the SMPS circuit is more complicated than the LR and any further modification may disrupt the main function of this driver. However, the attenuation becomes -51 dB at 30 MHz for uncovered LEDs and -70 dB at the same frequency when it is covered with an opaque screen.

The results of the experiment described in III-A2 using the modified LED bulbs are shown in Fig. 4b. The PSDs of the injected HPAV signal, the received noise, and the received signals after modifying the drivers are presented. It is obvious from Fig. Fig.4b that the modifications have improved the received power in the case of the Bailey LED bulb (-29 dBm at 28 MHz). However the improvement in the case of the Philips LED bulb is not as expected.

The results of the cross-correlation peak value of the received PRBS signal detailed in Section III-A3 are presented in this paragraph. As shown in Fig. 3, when comparing the modified bulbs to the same unmodified bulbs, it can be noticed that for the Bailey LED the peak before modification was 2230 at a rate of 10 Mbit/s (183.2 at a rate of 30 Mbit/s) and after modification, it becomes 7.5×10^4 at 10 Mbit/s (2.7×10^4 at 30 Mbit/s). For the Philips bulb, the peak before modification was 181 at 10 Mbit/s (134 at 30 Mbit/s) instead of 887.9 at 10 Mbit/s (1205 at 30 Mbit/s) after the modification. The obtained results can confirm that a simple modification of the drivers (LR or SMPS) can significantly increase the leakage.

V. CONCLUSION

In this paper, an investigation of the ability of commercial LED bulbs to inadvertently transmit PLC signals is carried out. The PLC signal leakage through LED light when there is no intentional relay between the powerlines and the LED bulbs. The LED driver technologies survey shows that the LR and the SMPS are the most adopted in domestic LED bulbs. Moreover, measurements of the electrical-optical channel TF and the PSD of the signal received through this side channel show that some LED bulbs with a LR are more likely to transmit data than other bulbs. Then, the cross-correlation peak value of the optically received PRBS sequence shows that the quantity of the received power allows the correct detection of the transmitted signals. However, the peak value differs from LED to LED even though they use the same type of driver. Finally, we demonstrated that the obtained results can be remarkably improved if some simple modifications are applied to the drivers of the LED bulbs.

ACKNOWLEDGMENT

This work has been supported by the *Pôle d'excellence cyber* under the project "PEC-Région Bretagne PLC-VLC n° 1208".

REFERENCES

[1] IEEE Std 802.15.7-2018, *IEEE standard for local and metropolitan area networks. part 15.7: Short-range optical wireless communications*, 2019, pp. 1–407.

[2] ITU-T G.9991, *VLC high speed indoor visible light communication transceiver. system architecture, physical layer and data link layer specification.* Mar. 2019, pp. 1–88.

[3] T. Komine and M. Nakagawa, "Integrated system of white LED visible-light communication and power-line communication", *IEEE Transactions on Consumer Electronics*, vol. 49, no. 1, pp. 71–79, 2003.

[4] T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights", *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 100–107, 2004.

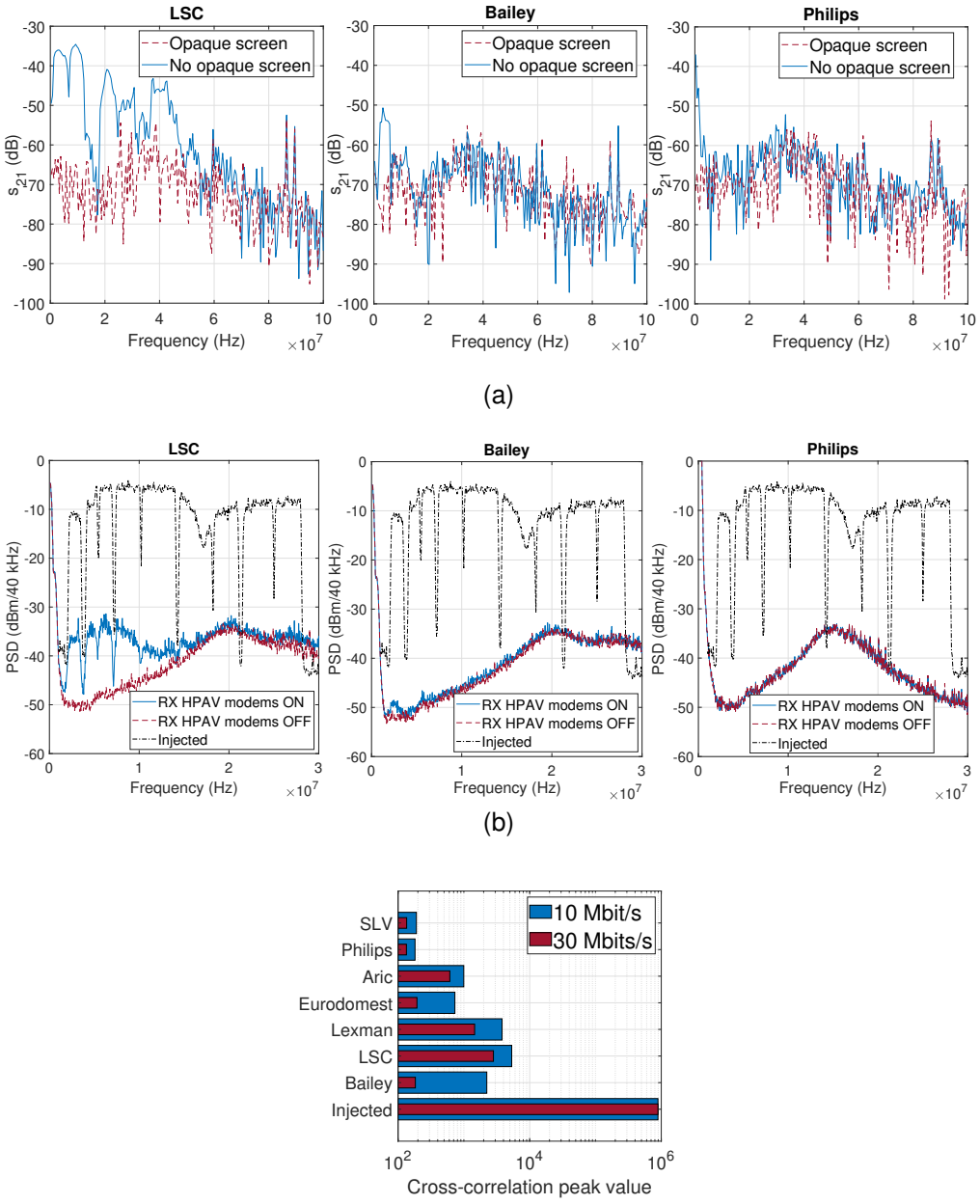

Figure 2. Results of two experimental tests.(a) The TF of the electrical-optical channel for LSC, Bailey and Philips LED bulbs. (b) The PSD of the transmitted HPAV signal using a commercial PLC modem, the optically leaked signal and the received noise. (c) Cross-correlation peak values of received PRBS signal for all LED bulbs tested at 10 Mbit/s and 30 Mbit/s.

[5] T. Komine, S. Haruyama, and M. Nakagawa, "Performance evaluation of narrowband OFDM on integrated system of power line communication and visible light wireless communication", in *International Symposium on Wireless Pervasive Computing*, Phuket, Thailand, Jan. 2006, pp. 1–6.

[6] M. Kubjana, A. Ndjiongue, and T. Shongwe, "Impulsive noise evaluation on PLC-VLC based on DCO-OFDM", in *International Symposium on Communication Systems, Networks Digital Signal Processing*, Budapest, Hungary, Jul. 2018, pp. 1–6.

[7] M. Kubjana, T. Shongwe, and A. Ndjiongue, "Hybrid PLC-VLC based on ACO-OFDM", in *International Conference on Intelligent and Innovative Computing Applications*, Plaine Magnien, Republic of Mauritius, Dec. 2018, pp. 1–5.

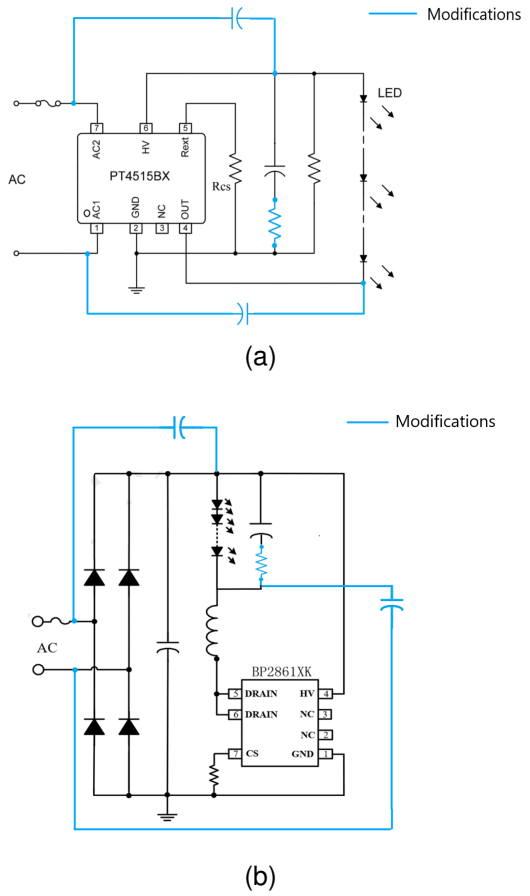

Figure 3. Circuit diagrams of Bailey and Philips LED bulb drivers after modification. (a) Modified active LR of Bailey LED bulb [18]. (b) Modified SMPS of Philips LED bulb [19].

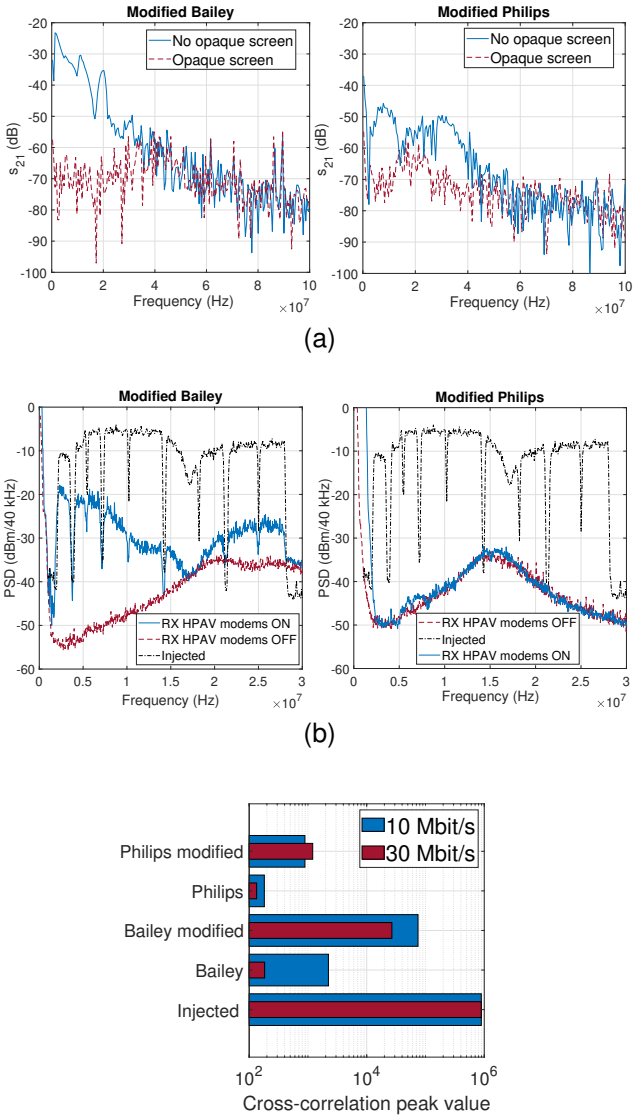

Figure 4. Results of the two experimental test applied on modified LED bulbs. (a) The TF of the electrical-optical channel for modified Bailey and Philips LED bulbs. (b) The PSD of the transmitted HPAV signal using a commercial PLC modem, the optically leaked signal and the received noise. (c) Cross-correlation peak values of received PRBS signal for Bailey and Philips LED bulbs before and after modifications at 10 Mbit/s and 30 Mbit/s.

[8] M. S. A. Mossaad, S. Hranilovic, and L. Lampe, "Amplify-and-forward integration of power line and visible light communications", in *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2015, pp. 1322–1326.

[9] J. Song, W. Ding, F. Yang, *et al.*, "An indoor broadband broadcasting system based on PLC and VLC", *IEEE Transactions on Broadcasting*, vol. 61, no. 2, pp. 299–308, 2015.

[10] Y. Yaacoub, F. Nouvel, S. Haese, *et al.*, "A seamless broadband PLC-VLC transmission: Performance evaluation and dimensioning", in *IEEE International Symposium on Power Line Communications and its Applications (ISPLC)*, 2021, pp. 61–66.

[11] P. Degauque, P. Laly, V. Degardin, *et al.*, "Power line communication and compromising radiated emission", *International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, vol. 7, Jan. 2010.

[12] S. Musumeci, "Passive and active topologies investigation for LED driver circuits", in *Light-Emitting Diodes and Photodetectors*, IntechOpen, Sep. 2021, ch. 3.

[13] I. Castro, A. Vazquez, M. Arias, *et al.*, "A review on flicker-free AC-DC LED drivers for single-phase and three-phase AC power grids", *IEEE Transactions on Power Electronics*, vol. 34, no. 10, pp. 10 035–10 057, 2019.

[14] J. Cosp-Vilella and H. Martínez-García, "Design of an on-chip linear-assisted DC-DC voltage regulator", in

International Conference on Electronics, Circuits, and Systems (ICECS), 2013, pp. 353–356.

[15] J. Shao, "Single stage offline LED driver", in *Applied Power Electronics Conference and Exposition*, Palm Springs, CA, Feb. 2009, pp. 582–586.

[16] S. Galli, M. Koch, H. Latchman, *et al.*, "Industrial and international standards on PLC-based networking technologies", in *Power Line Communications: Theory and Applications for Narrowband and Broadband Communications over Power Lines*, John Wiley & Sons, May 2010, ch. 7, pp. 363–412.

[17] *Homeplug power line aliiance*, Mar. 2010. [Online]. Available: http://www.homeplug.org/.

[18] *PT4515BX single-segment linear LED driver chip with integrated rectifier bridge*, PowerTech Datasheet.

[19] *BP2861XK non-isolated buck offline LED driver*, Bright Power Semiconductor Datasheet.