Study of the combination of PLC and VLC technologies for intra-building communications

Yara Yaacoub

THESE DE DOCTORAT DE

L'INSTITUT NATIONAL DES SCIENCES APPLIQUEES RENNES

ECOLE DOCTORALE N° 601
Mathématiques et Sciences et Technologies de l'Information et de la Communication
Spécialité : *Télécommunications*

Par

« Yara YAACOUB »

« Study of the combination of PLC and VLC technologies for intra-building communications»

Thèse présentée et soutenue à « Rennes », le « 28/10/2022 »
Unité de recherche : Institut d'Electronique et des Technologies du numéRique
Thèse N° : 22ISAR 24 / D22 - 24

Rapporteurs avant soutenance :

Catherine Lepers Professeure, Institut Polytechnique de Paris, Télécom SudParis
Andrea Tonello Professeur, Alpen-Adria-Universität Klagenfurt

Composition du Jury :

Président : Ghaya Rekaya-Ben Othman Professeure, Telecom Paris
Examinateurs : Catherine Lepers Professeure, Institut Polytechnique de Paris, Télécom SudParis
Ghaya Rekaya-Ben Othman Professeure, Telecom Paris
Sébastien Roy Professeur, Université de Sherbrooke
Nicolas Verneuil Expert technique, DGA
Andrea Tonello Professeur, Alpen-Adria-Universität Klagenfurt

Dir. de thèse : Fabienne Nouvel Maîtresse de conférences, HDR, INSA-Rennes
Co-dir. de thèse : Jean-Yves Baudais Chargé de recherche, HDR, CNRS
Encadrant : Sylvain Haese Maître de conférences, INSA-Rennes

Invité(s)
Sébastien Mallier Expert technique, DGA

Study of the combination of PLC and VLC technologies for intra-building communications

Yara YAACOUB

Acknowledgements

First and foremost, I would like to express my most sincere gratitude to my thesis supervisor, Dr. Fabienne Nouvel, for giving me the opportunity to pursue my Doctoral studies at INSA of Rennes, for his exceptional support and guidance throughout my research work. I attribute the level of my Ph.D degree to his permanent encouragement and involvement. I am also very thankful to him for helping me improve my writing and tutoring skills besides. I could just not expect a better supervisor.

I am extremely thankful to my thesis co-supervisors, Dr. Jean-Yves Baudais and Dr. Sylvain Haese, for their support, encouragement and valuable advice over the course of my research.

I would like to thank Pr. Ghaya Rekaya-Ben Othman for having accepted to be the president of the dissertation committee, Pr. Catherine Lepers and Dr. Andrea Tonello for their careful reading and rating of my thesis report. I also thank Pr. Sébastien Roy, Dr. Nicolas Verneuil and M. Erwan Nogues for having accepted to be part of the jury and for their relevant questions after my presentation. I would also like to thank Dr Sébastien Mallier for his follow-up of my thesis work during his three years as well as his presence during the defense.

I would like also to acknowledge the financial supporter of my PhD studies from the DGA-MI pôle cyber sećurite.

I thank my parents and sister for their support throughout all my studies. Your encouragement always gave me the confidence to continue to pursue my goals.

I would like to thank my second half, my husband Dr. Philip, who has been an inspiration to me, for his boundless love, patience and support. Philip always tried to increase my confidence in my skills and always stayed by my side every step of the way.

Finally, I would like to thank all my friends and colleagues, especially Qiong who supported me in every possible way.

At the end, I want to dedicate this thesis to my beautiful princess Nathalia and to my dear niece Maria.

Résumé étendu en français

Le spectre des radiofréquences classiquement utilisé pour la communication est quasiment épuisé. Cependant, la demande de communications sans fil à haut débit connaît une croissance exponentielle, créant un écart important entre les réseaux d'accès sans fil disponibles et la demande d'un débit de données élevé. Heureusement, les chercheurs commencent à étudier la possibilité de migrer vers d'autres parties du spectre électromagnétique comme le spectre des ondes millimétriques et le spectre visible.

Le déploiement rapide des diodes électroluminescentes (DEL) à base de nitrure d'indium et de gallium (InGaN) dans l'industrie de l'éclairage a incité les chercheurs à étudier la possibilité d'exploiter l'éclairage à DEL pour transmettre des signaux de communication. Cependant, le système de communication par lumière visible (VLC) ne peut pas fonctionner seule. Il s'agit d'un système de communication du dernier mètre qui doit être connecté à un autre système de communication nommé dorsale. Le système de communication par courant porteur (PLC) peut être considérée comme l'un des systèmes de dorsale les plus appropriés pour le VLC car ils sont naturellement connectés. D'autre part, le PLC est une technologie très mature et de nombreuses normes sont développées pour différentes bandes comme G3-PLC pour le Narrowband et Homeplug AV (HPAV) pour le Broadband PLC. Il convient de noter que l'intégration PLC-VLC n'est pas aussi simple qu'il y parait, surtout si nous recherchons un système PLC-VLC à large bande passante. Les canaux PLC et VLC souffrent d'une sévère atténuation quand la fréquence augmente. D'où, lors de la mise en cascade de ces deux canaux ensemble, le canal résultant aura une bande passante très limitée. c'est pour cela, peu d'études expérimentales sont menées afin de tester la faisabilité de l'intégration PLC-VLC à large bande, en particulier celles basées sur le relais d'amplification et de retransmission (AR).

La combinaison des deux systèmes de communication peut être une solution prometteuse pour assurer la continuité de la communication à l'intérieur des bâtiments ou des environnements urbains. Mais cela peut aussi être perçu comme un risque, les données PLC peuvent fuir à travers les ampoules LED domestiques lorsqu'elles sont branchées sur le courant porteur. à notre connaissance, les chercheurs n'ont jamais étudié cette menace pour la sécurité. Toutes les tentatives se concentrent sur la facilitation et l'optimisation de l'intégration PLC-VLC. Au contraire, si nous cherchons à isoler le PLC du VLC, les risques d'interception des signaux du PLC à travers les ampoules DEL domestiques doivent être soigneusement mesurés afin

d'assurer une isolation complète.

Ainsi, deux sujets sont abordés dans cette thèse : *i)* la mise en oeuvre d'un système PLC-VLC simple à haut débit et à faible coût qui ne nécessite pas de phase de décodage/réencodage entre les deux sous-systèmes. *ii)* la fuite du signal PLC à travers des ampoules LED domestiques.

Chapitre 1

Le chapitre 1 présente une introduction générale au sujet de la thèse. D'une part, cette introduction montre l'importance de mettre en oeuvre un système CPL-VLC à large bande capable d'assurer simultanément l'éclairage et la communication. D'autre part, elle met en évidence le risque de sécurité qui peut menacer le réseau CPL si l'association entre les ampoules LED et le système VLC est réalisée par inadvertance. Ce chapitre présente également les parcours et les motivations qui nous ont amenés à étudier ces deux sujets. Il décrit aussi la structure de la thèse et nos principales contributions. Enfin, il liste nos publications produites au cours de cette thèse.

Chapitre 2

Le chapitre 2 contient une revue de la littérature sur l'intégration des systèmes PLC et VLC. Il comprend une brève description des systèmes PLC et VLC en tenant compte de leurs standards disponibles, de la caractérisation des canaux, de la modélisation des canaux et de l'analyse du bruit. Les standards du système PLC varient en fonction de la bande de modulation utilisée. Pour le PLC à bande étroite, Les standards G.9901, G.9902, G.9903, G.9904 et IEEE 1901.2 sont développés. Pour le PLC à large bande, deux standards sont élaborés : IEEE 1901 et G.996x. Les concepteurs du système PLC ont rencontré de nombreux obstacles liés aux problèmes du canal PLC. Le canal PLC est affecté par des sévères atténuations qui augmentent avec l'augmentation de la fréquence et avec l'augmentation de la longueur du câble. Pour modéliser le canal PLC, il existe deux approches principales : l'approche descendante qui utilise un modèle multi-trajets et l'approche ascendante qui est basée sur la théorie des lignes de transmission. Le canal PLC est également affecté par de nombreux bruits comme le bruit à bande étroite, le bruit impulsionnel aléatoire et le bruit impulsionnel périodique.

Concernant le système VLC, trois standards principaux sont développés : IEEE 802.15.7, ITU-T G.9991, et IEEE 802.11bb. Similaire au canal PLC, le canal VLC présente de nombreux problèmes tels que la limitation de la bande passante, la non-linéarité et l'atténuation avec la distance. De plus, le gain du canal VLC peut être modélisé comme un rayonnement lambertien inversement proportionnel au carré de la distance séparant l'émetteur du récepteur optique. Ce canal peut être aussi affecté par plusieurs types de bruit comme le bruit de fond, le bruit

thermique et le bruit de grenaille.

Ce chapitre présente également les techniques de modulation les plus utilisées dans le système VLC telles que l'OFDM à écrêtage asymétrique et l'OFDM à polarisation continue. Il couvre aussi les différentes techniques de relais qui permettent l'intégration des systèmes PLC et VLC comme l'amplification et la transmission et le décodage et la transmission. Ce chapitre présente également les résultats de mesure et l'approche de modélisation de la réponse en fréquence du canal PLC-VLC en cascade pour la communication intra-bâtiment sur la base de recherches antérieures.

Une étude rapide est réalisée sur la fuite du signal de communication à travers les canaux secondaires afin de mettre en évidence l'importance de découvrir tous les canaux secondaires existants qui peuvent menacer la sécurité des systèmes de communications. ce chapitre explique les différentes classes d'attaques (passives/actives et intentionnelles/non intentionnelles). Les différents types de canaux latéraux sont répertoriés selon qu'ils sont électromagnétiques ou non électromagnétiques. Les contre-mesures pouvant être prises pour protéger le réseau de communication contre les attaques sont également présentées, telles que le zonage, le blindage des composants, le blindage des installations, le brouillage, etc.

Enfin, le sujet de la sécurité de la couche physique est introduit dans ce chapitre en considérant les principaux types de canaux latéraux (Wyner, Csizàr et Korner, et *keyhole channel*). Les métriques fondamentales utilisées pour évaluer la sécurité de la couche physique sont présentées comme le taux d'équivocation, le taux de secret et la capacité de secret.

Chapitre 3

Le chapitre 3 constitue les premières contributions de cette thèse. Il montre la procédure de mise en oeuvre de notre système PLC-VLC proposé. Un test expérimental est réalisé pour mesurer la bande passante de 3 LED de trois couleurs différentes (rouge, vert et bleu). Les résultats montrent que la LED rouge a la plus grande bande passante (20 MHz à −3 dB) (voir fig. 1). Ainsi, la LED rouge est choisie pour être utilisée dans le banc d'essai PLC-VLC. Ensuite, l'impédance fréquentielle des LED RGB est mesurée afin de trouver un modèle de circuit équivalent pour les LED. Fig. 3 montre que l'impédance fréquentielle du circuit proposé (voir fig.2) correspond bien à celle mesurée pour la LED bleue. Cependant, la phase d'impédance du modèle ne correspond pas aux LED vertes et rouges qui nécessitent un modèle de circuit plus compliqué (voir fig. 3b).

Une expression théorique est développée afin de modéliser avec précision le système VLC. cette expression peut nous aider lors de la conception de l'émetteur et du récepteur optiques. Elle permet de calculer immédiatement le courant ou la tension du signal récupéré à la sortie du récepteur optique I ou V_{TIA} en fonction du courant traversant la LED i (1). La comparaison entre la tension calculé à l'aide de cette expression et la tension mesurée à la

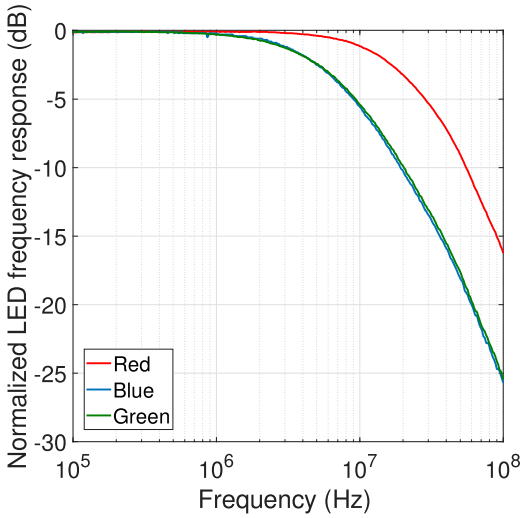


FIGURE 1 : Réponses fréquentielles des LED rouges, vertes et bleues.

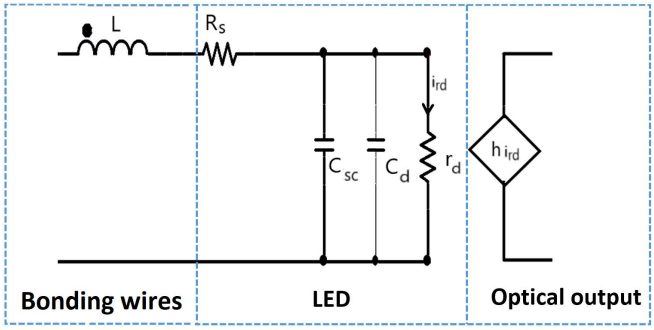
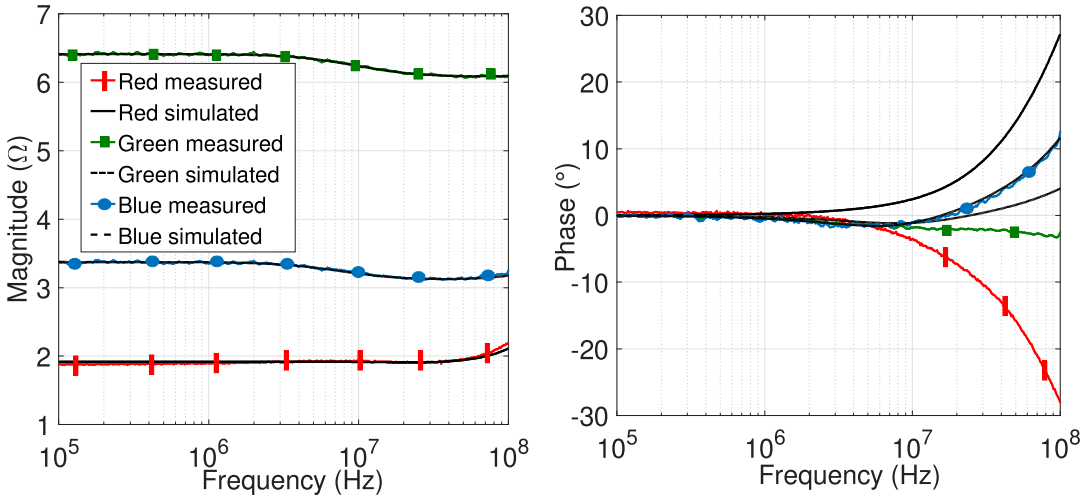


FIGURE 2 : Modèle simplifié du circuit équivalent d'une LED.



(a) (b)

FIGURE 3 : Comparaison entre l'impédance fréquentielle modélisée et mesurée des LED rouges, vertes et bleues. (a) Modules, (b) phases.

sortie du récepteur optique montrent une erreur de 22% qui est acceptable au regard des caractéristiques du banc d'essai.

$$I(i) = PH_B H_V S_{max} L(i) \sqrt{\pi} \left(ca \left(s_1 \left(\frac{c^2}{2} + b^2 \right) + s_2 b + s_3 \right) + df \left(s_1 \left(\frac{f^2}{2} + e^2 \right) + s_2 e + s_3 \right) \right) \quad (1)$$

De plus, le système PLC-VLC est mis en oeuvre à l'aide de modems HPAV commerciaux et de notre émetteur et récepteur optique conçu comme le montre la fig. 4. Les résultats de débit de la transmission de paquets UDP (*User Datagram Protocol*) via notre banc d'essai PLC-VLC montrent une valeur maximale de 66 Mbit/s jusqu'à une distance de 40 cm (voir fig. 5). Ce résultat semble prometteur puisque on a pu atteindre cette distance en utilisant une seule LED. Pour pouvoir atteindre de plus grandes distances, il est nécessaire d'utiliser une matrice de plusieurs LED qui transmettront simultanément le même signal.

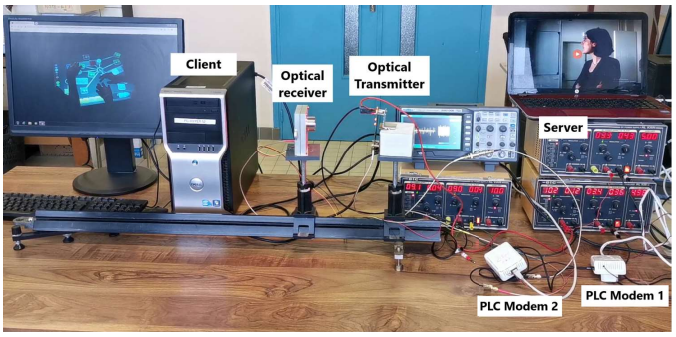


FIGURE 4 : Banc d'essai du system PLC-VLC.

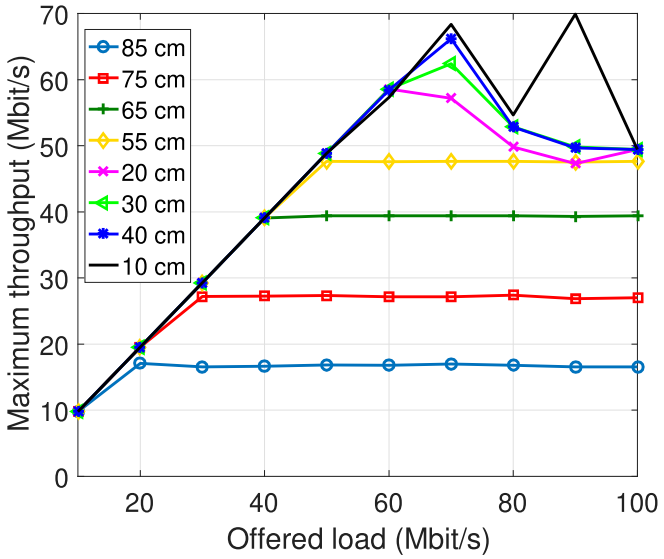


FIGURE 5 : Throughput UDP en fonction du débit offerte pour différentes distances entre la LED et le récepteur optique.

Pour pouvoir extrapoler théoriquement les résultats de mesure à des scénarios à plus grande échelle sans avoir besoin d'effectuer des mesures supplémentaires, une étude théorique est réalisée à l'aide de nos paramètres de banc d'essai. Cette étude permet de calculer le nombre de LED nécessaires pour pouvoir assurer la communication PLC-VLC et l'éclairage dans des scénarios réels. Les résultats montrent qu'il faut au moins 60 LED rouges pour garantir un débit maximum de 66 Mbits/s à l'intérieur d'un bureau typique. Heureusement, cette étude montre également que ce nombre équivaut approximativement au nombre de LED nécessaires pour l'éclairage, ce qui signifie qu'aucune LED supplémentaire n'est nécessaire pour la communication.

Chapitre 4

Le chapitre 4 traite le deuxième aspect de la thèse qui est la fuite du signal PLC à travers les ampoules LED domestiques. Dans ce chapitre, de nombreuses ampoules LED domestiques de différentes marques sont ouvertes pour vérifier leurs types de drivers. On a découvert que les drivers actives linéaire (AL) (fig. 6) sont utilisés dans de nombreuses ampoules LED en plus que les drivers d'alimentation à découpage (SMPS). Les drivers AL étaient généralement utilisés dans des applications à faible puissance car ils étaient considérés comme moins chers, moins encombrants, et moins efficaces que les drivers SMPS s'ils sont adoptés pour l'éclairage intérieur . Cependant, lorsque nous avons comparé l'efficacité énergétique des ampoules SMPS avec celle des ampoules LED AL consommant la même puissance (moins de 10 W), nous avons constaté qu'elles sont très proches. Ce qui explique leur récente utilisation intensive dans l'éclairage intérieur.

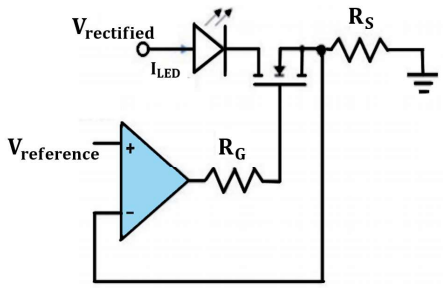
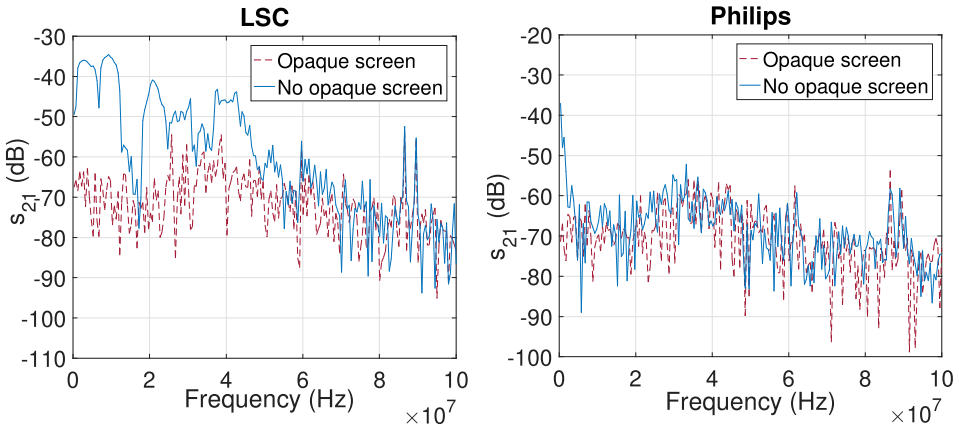


FIGURE 6 : Principe de fonctionnement du driver actif et linéaire.

Ensuite, la caractérisation du canal latéral est effectuée en utilisant toutes les ampoules déjà testées. Cette caractérisation commence par la mesure de la réponse fréquentielle du canal auxiliaire. Fig. 7a montre la réponse fréquentielle du canal dans le cas de l'ampoule LED AL de la marque LSC. On peut remarquer que la réponse du canal lorsque le récepteur optique n'est pas recouvert d'un écran opaque montre une atténuation considérablement plus faible que celle couverte pour les fréquences inférieures à 50 MHz. Cependant, dans le

cas d'une ampoule LED SMPS de la marque philips (voir fig. 7b), les courbes bleue et rouge sont approximativement confondues pour des fréquences supérieures à 5 MHz. Ces résultats prouvent que les ampoules LED AL ont une bande passante plus large que les ampoules SMPS, ce qui signifie que les ampoules AL ont plus de chance de fuir naturellement. Ensuite, la



(a) (b)

FIGURE 7 : La fonction de transfert des canaux latéraux optique-électriques. (a) Ampoule LED LSC. (b) Ampoule LED Philips.

densité spectrale de puissance (PSD) du signal reçu via le canal latéral est mesurée lorsque les ampoules LED sont branchées sur la même ligne électrique avec des modems HPAV. Prenons l'exemple de l'ampoule LED LSC, la PSD du signal reçu à 12 MHz est de -39 dBm lorsque les modems HPAV sont ON contre (bleu continu) une PSD de -42 dBm lorsque les modems sont OFF (courbe rouge en pointillés, fig. 8a). Cependant, dans le cas de l'ampoule LED Philips, la différence entre les courbes rouge et bleue est à peine détectable (fig. 8b). Ces résultats prouvent une autre fois que les ampoules LED AL ont plus de chance de fuir que les ampoules SMPS. De plus, le maximum pic d'intercorrélation est calculé lorsqu'un signal de séquence binaire pseudo-aléatoire (PRBS) est transmis via le canal latéral électrique-optique. Les résultats de fig. 9 montrent que les atténuations des canaux latéraux pour toutes les ampoules LED testées sont inférieures à 38 dB par rapport au signal injecté tenant en compte les conditions du montage expérimental.

Ce chapitre présente également les résultats de la transmission d'un signal *discrete multi-tone* (DMT) qui a presque les mêmes paramètres qu'un signal HPAV via le canal latéral. Fig. 10 montre que dans cette essai, le bit error rate (BER) des ampoules LED AL est inférieur à $0,36$. Dans le cas de l'ampoule LED LSC, le BER est de $0,19$ ce qui signifie que 81 % des bits transmis sont correctement restitués. Cependant, dans le cas des ampoules LED SMPS comme Philips et SLV, presque la moitié des bits transmis (47 %) ne sont pas correctement reçus. Cela signifie que dans le cas des ampoules SMPS, le driver empêche le signal PLC de le traverser pour

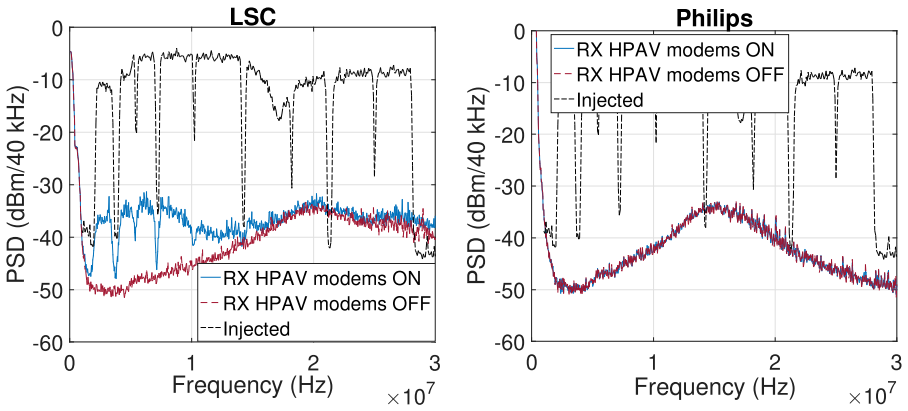


FIGURE 8 : The PSD of the transmitted HPAV signal using a commercial PLC modem, the optically leaked signal when the PLC modems are ON, and when they are OFF. (a) LSC LED bulb. (b) Philips LED bulb.

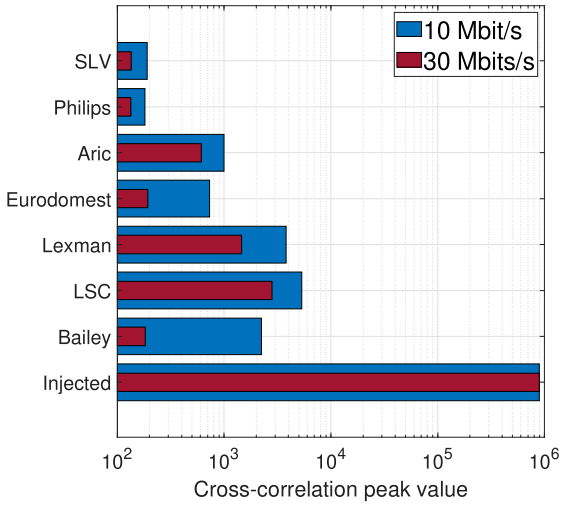


FIGURE 9 : Valeurs des pics d'intercorrélation du signaux PRBS reçu pour toutes les ampoules LED testées à 10 Mbit/s et 30 Mbit/s.

atteindre la matrice de LED.

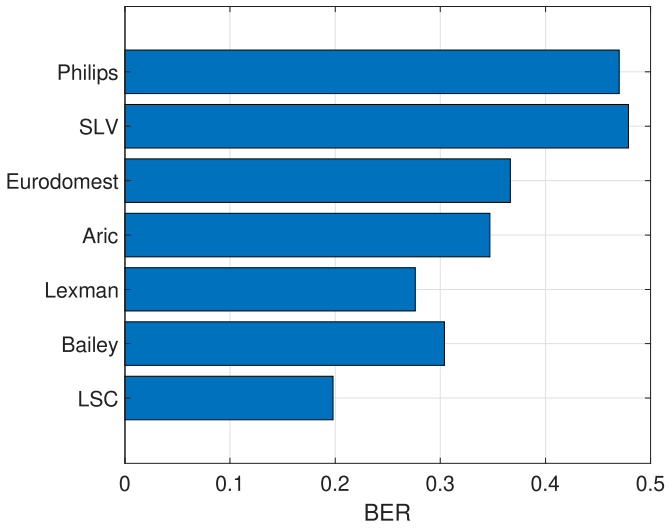


FIGURE 10 : BER en fonction des ampoules LED testées.

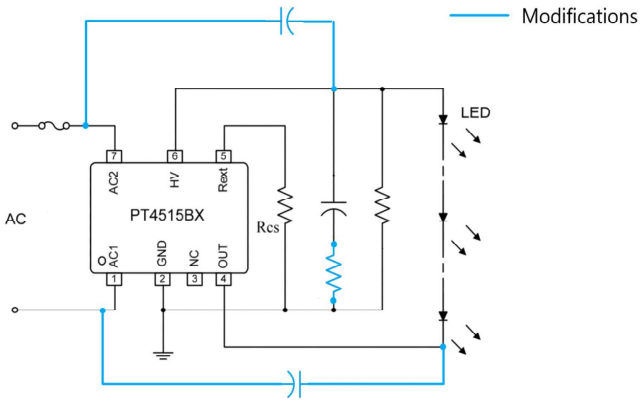
Des simple modifications sont effectuées sur les drivers AL et SMPS des ampoule de marque Bailey et Philips respectivement pour prouver qu'il est possible de favoriser facilement la fuite par une intervention intentionnelle (voir fig. 11). Les essais précités sont répétés après réalisation de ces modifications. Les résultats obtenus montrent une amélioration significative des fuites notamment dans le cas des ampoules LED AL (voir fig. 12, 13, 14 et 15).

Enfin, la sécurité de la couche physique du système PLC est étudiée dans le cas où un émetteur VLC non légitime est connecté au réseau PLC. La capacité moyenne de secret est calculée sur la base d'expressions analytiques. La capacité de secret calculée est ensuite comparée aux résultats de la simulation. Une correspondance parfaite est trouvée (voir fig. 16 et 17). De plus, les résultats obtenus ont révélé que la capacité de secret augmente avec la puissance transmise (fig. 16), avec la longueur du câble électrique du canal non légitime(fig. 16) et avec la distance verticale séparant les LED du récepteur optique (fig. 17).

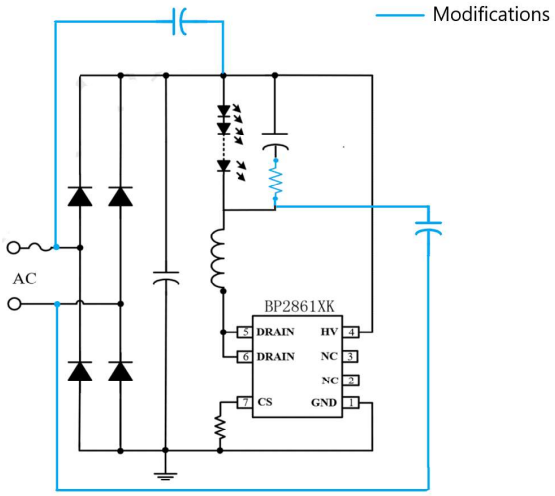
Chapitre 5

Cette thèse se termine par le chapitre 5 qui conclut l'ensemble de nos contributions. Ce chapitre présente également les travaux d'extension qui peuvent être réalisés dans le futur. Par exemple :

- Trouver un modèle de circuit équivalent LED plus précis qui a une amplitude et une phase qui peuvent parfaitement correspondre à celles mesurées ;

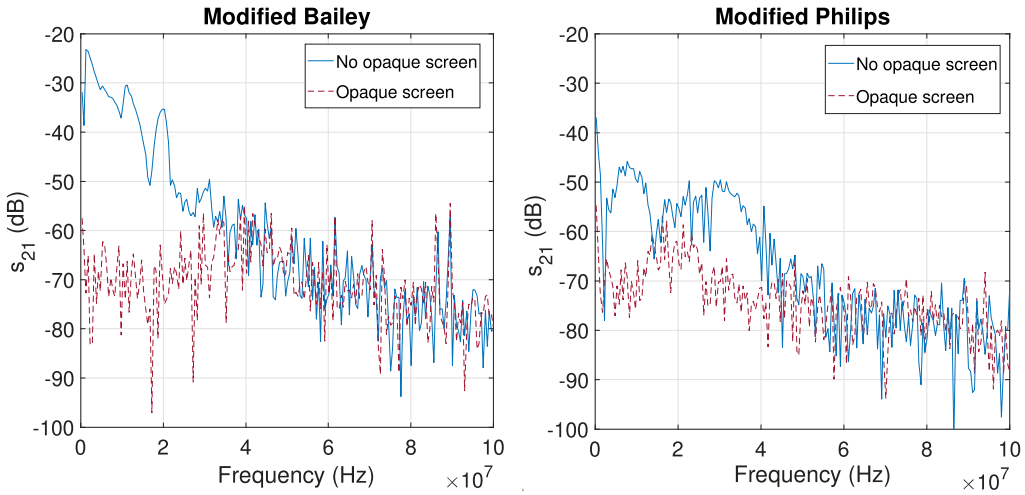


(a)



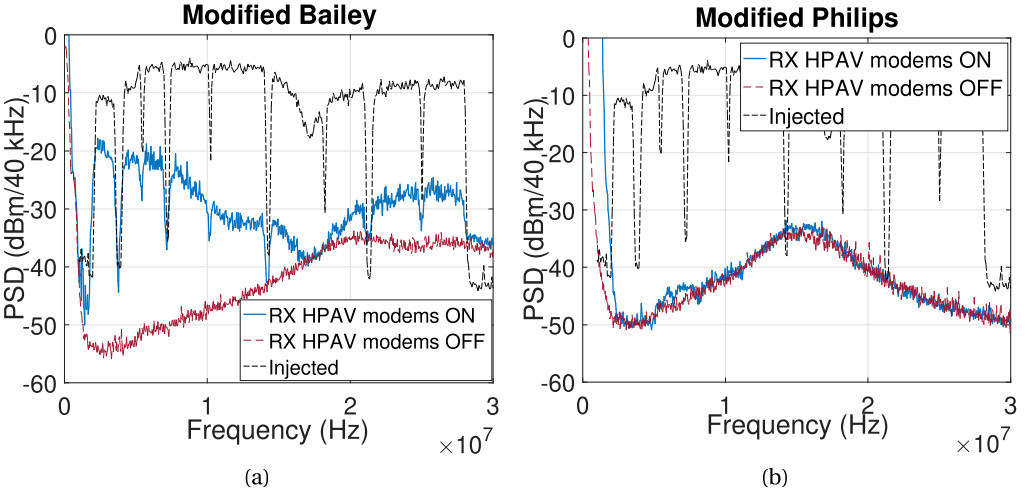
(b)

FIGURE 11 : Schémas de circuits des drivers d'ampoules LED Bailey et Philips après modification. (a) AL modifié de l'ampoule LED Bailey. (b) SMPS modifié de l'ampoule LED Philips.



(a) (b)

FIGURE 12 : La fonction de transfert du canal électrique-optique après modification du driver. (a) Ampoule LED Bailey. (b) Ampoule LED Philips.



(a) (b)

FIGURE 13 : PSD du signal HPAV transmis à l'aide d'un modem PLC commercial, signal reçu optiquement lorsque les modems HPAV sont ON et lorsqu'ils sont OFF. (a) Ampoule LED Bailey. (b) Ampoule LED Philips.

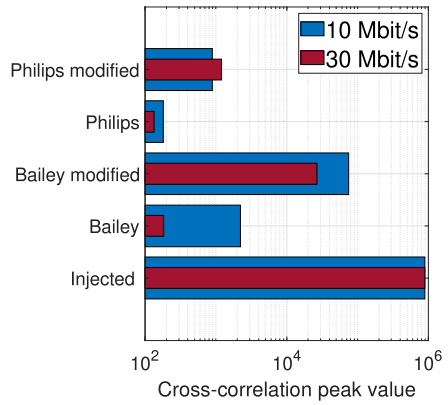


FIGURE 14 : Valeurs des pics d'intercorrélation du signaux PRBS reçu pour les ampoules LED modifiées à 10 Mbit/s et 30 Mbit/s.

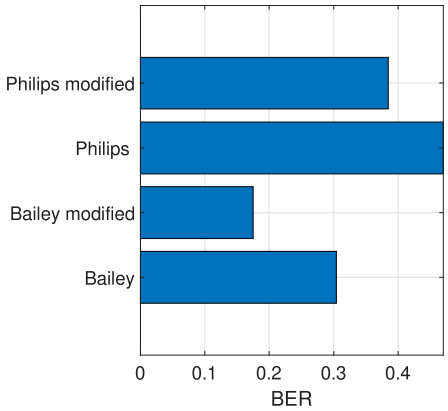


FIGURE 15 : Comparaison du BER avant et après modification des drivers des ampoules LED Bailey et Philips.

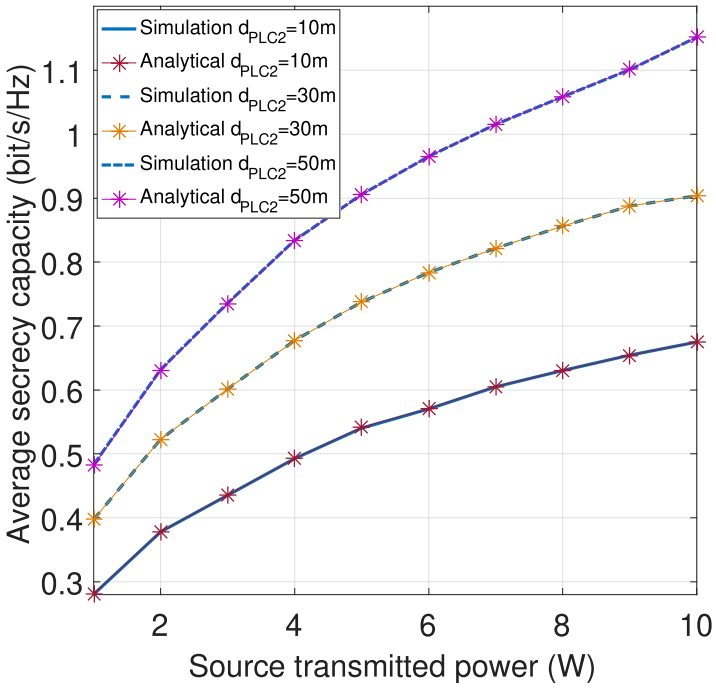


FIGURE 16 : Comparaison entre la capacité moyenne de secret calculée analytiquement et simulée en fonction de la puissance transmise pour différentes longueurs de câble PLC2.

- élaborer une expression modélisant le système VLC prenant en compte l'effet de la température de jonction LED ;
- implémenter un banc d'essai PLC-VLC à grande échelle afin d'effectuer des tests expérimentaux pour évaluer les performances du système proposé au lieu d'études théoriques ;
- tester des marques d'ampoules LED supplémentaire pour voir s'il y a d'autres LED qui fuient plus que les ampoules testées dans cette thèse ;
- étudier la sécurité de la couche physique du système PLC dans le cas d'un régime de longueur de bloc finie.

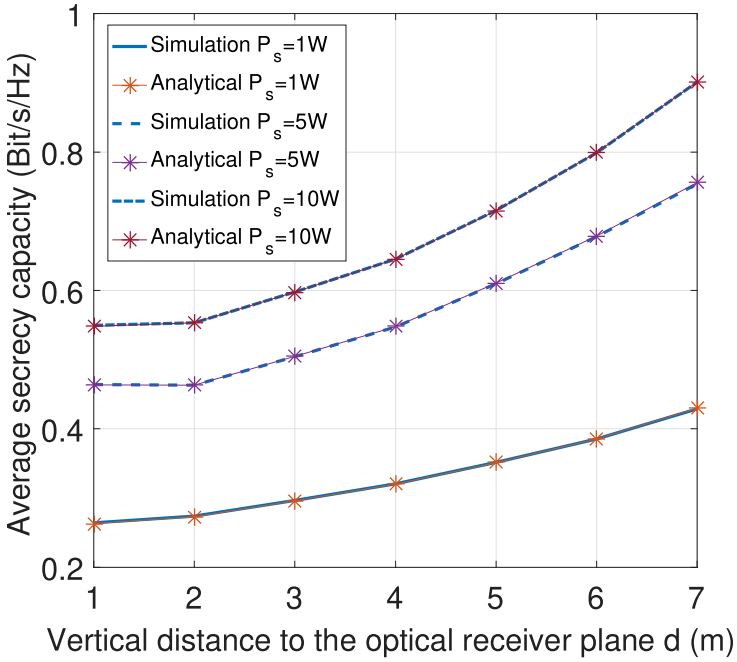


FIGURE 17 : Comparaison entre la capacité de secret moyenne calculée analytiquement et simulée en fonction de la longueur entre la matrice de LED et le récepteur optique pour différentes valeurs de puissance transmise.

Contents

Acknowledgements 3

Résumé étendu en français 5

Contents 19

List of Figures 23

List of Tables 27

List of acronyms 29

1 General introduction 31
- 1.1 Background and motivation . . . 32
- 1.2 Structure of the thesis and contribution . . . 34
- 1.3 Publications . . . 35
  - 1.3.1 Article . . . 35
  - 1.3.2 International conferences . . . 35
  - 1.3.3 Poster . . . 36

2 Literature review 37
- 2.1 Powerline communication . . . 37
  - 2.1.1 PLC standardization . . . 38
    - 2.1.1.1 The narrow-band PLC standards . . . 38
    - 2.1.1.2 The broad-band PLC standards . . . 39
    - 2.1.1.3 Homeplug AV (HPAV) . . . 40
  - 2.1.2 Channel characteristics . . . 41
    - 2.1.2.1 Channel attenuation characteristics . . . 41
    - 2.1.2.2 Channel models . . . 42
  - 2.1.3 Noise characteristics . . . 43
- 2.2 Visible light communication . . . 44
  - 2.2.1 Visible light communication standards . . . 45

2.2.1.1 IEEE 802.15.7 . . . 45
2.2.1.2 ITU-T G.9991 . . . 46
2.2.1.3 IEEE 802.11bb . . . 47
2.2.2 Light-emitting-diodes for visible light communication and lighting . . . 48
2.2.2.1 Blue LED with phosphor coat . . . 48
2.2.2.2 RGB LED . . . 49
2.2.3 Channel characteristics . . . 49
2.2.3.1 Channel model . . . 49
2.2.3.2 LED non-linearity . . . 52
2.2.4 Noise characteristics . . . 52
2.3 PLC and VLC systems integration . . . 53
2.3.1 PLC-VLC relaying techniques . . . 54
2.3.2 Channel characteristics . . . 55
2.4 Side channel attacks . . . 56
2.4.1 Class of attacks . . . 57
2.4.2 Class of side-channel . . . 57
2.4.2.1 Electromagnetic channels . . . 57
2.4.2.2 Non-electromagnetic channels . . . 58
2.4.3 Countermeasures . . . 60
2.5 Physical layer security from an information theoretic perspective . . . 61
2.5.1 Wiretap channel models . . . 62
2.5.2 Secrecy performance evaluation for physical layer security . . . 63
2.5.3 Physical layer security enhancement . . . 64
2.5.3.1 Artificial-Noise-Aided Security . . . 64
2.5.3.2 Security-Oriented Beamforming Techniques . . . 64
2.5.3.3 Diversity-Assisted Security Approaches . . . 65
2.5.4 Physical-Layer Secret Key Generation . . . 65
2.6 Conclusion . . . 66

3 Broadband PLC-VLC system integration 69
3.1 VLC subsystem experimental and theoretical analysis . . . 70
3.1.1 LED frequency characteristics . . . 70
3.1.1.1 LED frequency response . . . 70
3.1.1.2 LED frequency impedance . . . 71
3.1.2 LED equivalent circuit model . . . 71
3.1.2.1 The process of estimating the value of each component . . . 73
3.1.2.2 Results . . . 74
3.1.3 VLC channel modeling taking into account the optical, electrical and frequency behavior . . . 77

3.1.3.1 Proposed model . . . 77
3.1.3.2 Current measurement setup . . . 79
3.1.4 Results . . . 80
3.2 PLC-VLC integration . . . 80
3.2.1 System setup . . . 82
3.2.2 Performance evaluation . . . 83
3.2.3 Optical system dimensionning . . . 86
3.3 Conclusion . . . 89

4 PLC signal leakage through domestic LED bulbs **91**
4.1 Domestic LED bulbs characteristics . . . 92
4.1.1 LED driver . . . 92
4.1.1.1 Active linear driver . . . 93
4.1.2 LED assembly . . . 93
4.2 Optical side channel characterization . . . 95
4.2.1 Experimental setup . . . 95
4.2.1.1 Side channel frequency response . . . 95
4.2.1.2 PSD of the HomePlugAV leaked signal . . . 97
4.2.1.3 PRBS transmission through the side electrical-optical channel . 97
4.2.2 Results and discussion . . . 97
4.2.2.1 Side channel frequency response results . . . 98
4.2.3 PSD of the HomePlugAV leaked signal results . . . 98
4.2.3.1 Side channel sounding using PRBS signal . . . 100
4.3 DMT transmission through the electrical-optical side channel . . . 100
4.3.1 System architecture and experimental setup . . . 103
4.3.2 Results and discussion . . . 104
4.4 LED driver modification to facilitate the leakage . . . 105
4.4.1 Driver modifications and experimental setup . . . 105
4.4.2 Results . . . 106
4.4.2.1 Side channel frequency response . . . 106
4.4.2.2 PSD of the HomePlugAV leaked signal . . . 108
4.4.2.3 PRBS transmission through the side electrical-optical channel . 108
4.4.2.4 DMT signal transmission through the electrical-optical side channel . . . 109
4.5 Physical layer security of PLC system in the presence of a non-legitimate optical system . . . 110
4.5.1 System model . . . 110
4.5.2 Average secrecy capacity . . . 113
4.5.2.1 Average capacity at Bob . . . 114

4.5.2.2 Average capacity at Eve 114
4.5.3 Results and validation 116
4.6 Conclusion 117

5 General conclusion **121**

A Circuit design **125**
A.1 Wide-band bias tee 125
A.1.1 Bias tee design 126
A.1.2 Simulation results 127
A.2 Optical receiver 127
A.2.1 Circuit design 130
A.2.2 Simulation results 131

Bibliography **135**

List of Figures

1 Réponses fréquentielles des LED rouges, vertes et bleues. 8
2 Modèle simplifié du circuit équivalent d'une LED. 8
3 Comparaison entre l'impédance fréquentielle modélisée et mesurée des LED rouges, vertes et bleues. (a) Modules, (b) phases. 8
4 Banc d'essai du system PLC-VLC. 9
5 Throughput UDP en fonction du débit offerte pour différentes distances entre la LED et le récepteur optique. 9
6 Principe de fonctionnement du driver actif et linéaire. 10
7 La fonction de transfert des canaux latéraux optique-électriques. (a) Ampoule LED LSC. (b) Ampoule LED Philips. 11
8 The PSD of the transmitted HPAV signal using a commercial PLC modem, the optically leaked signal when the PLC modems are ON, and when they are OFF. (a) LSC LED bulb. (b) Philips LED bulb. 12
9 Valeurs des pics d'intercorrélation du signaux PRBS reçu pour toutes les ampoules LED testées à 10 Mbit/s et 30 Mbit/s. 12
10 BER en fonction des ampoules LED testées. 13
11 Schémas de circuits des drivers d'ampoules LED Bailey et Philips après modification. (a) AL modifié de l'ampoule LED Bailey. (b) SMPS modifié de l'ampoule LED Philips. 14
12 La fonction de transfert du canal électrique-optique après modification du driver. (a) Ampoule LED Bailey. (b) Ampoule LED Philips. 15
13 PSD du signal HPAV transmis à l'aide d'un modem PLC commercial, signal reçu optiquement lorsque les modems HPAV sont ON et lorsqu'ils sont OFF. (a) Ampoule LED Bailey. (b) Ampoule LED Philips. 15
14 Valeurs des pics d'intercorrélation du signaux PRBS reçu pour les ampoules LED modifiées à 10 Mbit/s et 30 Mbit/s. 16
15 Comparaison du BER avant et après modification des drivers des ampoules LED Bailey et Philips. 16

16 Comparaison entre la capacité moyenne de secret calculée analytiquement et simulée en fonction de la puissance transmise pour différentes longueurs de câble PLC2. 17
17 Comparaison entre la capacité de secret moyenne calculée analytiquement et simulée en fonction de la longueur entre la matrice de LED et le récepteur optique pour différentes valeurs de puissance transmise. 18

2.1 Multipath model [109]. 42
2.2 Transmission line propagation [59]. 43
2.3 Indoor VLC system using LED lighting [21]. 45
2.4 Frequency and time domaine DCO-OFDM signal. 47
2.5 Frequency and time domaine ACO-OFDM signal. 48
2.6 Generating white lights using LEDs [51]: (a) Blue LED with a phosphor layer, (b) RGB LED. 50
2.7 Optical wireless channel DC gain geometry [3]. 51
2.8 The LED E/O characteristic. 52
2.9 Komine PLC-VLC system model [55]. 54
2.10 Amplify and forward PLC-VLC system block diagram 55
2.11 Decode and forward PLC-VLC system block diagram. 55
2.12 The measured channel frquency response (CFR) of the VLC part, the CFR of a typical hybrid PLC and VLC communication system [20]. 56
2.13 Electromagnetic side channels [14]. 58
2.14 Non Electromagnetic side channels[14]. 60
2.15 Communication system with a transmitter (Alice), a legitimate receiver (Bob) and an eavesdropper (Eve) [52]. 62
2.16 The wiretap channel configurations. (a) Wyner [52]. (b) Csizàr and Körner [52]. (c) Keyhole 63

3.1 Bias Tee. (a) explanatory scheme, (b) our manufactured circuit. 71
3.2 Red, green, and blue LED frequency responses. 72
3.3 Frequency impedance of the red, green, and blue LED of luxeon RGB module. (a) Magnitudes, (b) phases. 72
3.4 Simplified equivalent circuit model for a LED. 73
3.5 Comparison between the modeled and the measured frequency impedance of the red, green, and blue LED. (a) Magnitude, (b) phases. 75
3.6 Comparison between the modeled and the measured LED frequency response. (a) Red LED, (b) green LED, (c) blue LED. 76
3.7 VLC testbed. 77
3.8 The normalized eye efficacy v(λ). 78

3.9 LED and photodiode datasheet curves models. (a) The spectral power density of red, green, and blue LEDs compared to their modeled curves, (b) the three LEDs' electrical/optical characteristics compared to our polynomial model, (d) spectral sensitivity response of the photodiode compared to our polynomial model. . . 81
3.10 PLC-VLC system testbed.(a) Diagram of PLC-VLC system, (b) real photo of the testbed. 83
3.11 UDP Throughput versus the offered load for different distance between the LED and the optical receiver. 85
3.12 UDP Throughput comparison between PLC and PLC-VLC system in function of the Transmitted power. 85
3.13 Number of LED needed to receive 706 nA signal as a function of the distance between the LED and the photodiode. 87
3.14 CIE 1931 xy color space with the red, green, blue and white LED chromatic coordinates and the target white light chromatic coordinates [76]. 88
3.15 Received power attenuation as a function of the receiver position in a $5 \times 5 \times 3$ m^3 office. 89

4.1 Taking apart an LED light bulb [92]. 92
4.2 Operation principle of active linear driver. 93
4.3 Two single-junction LED package (upper) and high voltage LED including 3 sub-LEDs (lower) [100]. 94
4.4 Experimental setup schema. 96
4.5 The transfer function of the optical-electrical side channels for the LED bulbs having an AL driver. (a) LSC LED bulb. (b) Lexman LED bulb. (c) Bailey LED bulb. (d) Eurodomdest LED bulb. (e) Aric LED bulb. 99
4.6 The transfer function of the optical-electrical side channels for the LED bulbs having a SMPS driver. (a) Philips LED bulb. (b) SLV LED bulb. 100
4.7 The PSD of the transmitted HPAV signal using a commercial PLC modem, the optically leaked signal when the PLC modems are ON, and when they are OFF. (a) LSC LED bulb. (b) Lexman LED bulb. (c) Bailey LED bulb. (d) Eurodomdest LED bulb. (e) Aric LED bulb. 101
4.8 The PSD of the transmitted HPAV signal using a commercial PLC modem, the optically leaked signal and the received noise via SMPS LED bulbs. (a) Philips LED bulb. (b) SLV LED bulb. 102
4.9 Cross-correlation peak values of received PRBS signal for all the tested LED bulbs at 10 Mbit/s and 30 Mbit/s. 102
4.10 Physical layer frame. 104
4.11 Comparison between the transmitted and received images through the side channel for LSC, Bailey, Lexman, Aric, Eurodomest, SLV, and Philips bulbs. . . . 105

4.12 BER in function of the tested LED bulbs. 106
4.13 Circuit diagrams of Bailey and Philips LED bulb drivers after modification. (a) Modified AL driver of Bailey LED bulb [79]. (b) Modified SMPS driver of Philips LED bulb [7]. 107
4.14 The transfer function of the electrical-optical channel after driver modification. (a) Bailey LED bulb. (b) Philips LED bulb. 108
4.15 The PSD of the transmitted HPAV signal using a commercial PLC modem, the optically leaked signal and the received noise via modified LED bulbs. (a) Bailey LED bulb. (b) Philips LED bulb. 109
4.16 Cross-correlation peak values of received PRBS signal for the modified LED bulbs at 10 Mbit/s and 30 Mbit/s. 110
4.17 Comparison between the received images through the side channel for Bailey and Philips LED bulbs before and after modification. 111
4.18 BER comparison before and after modifying the drivers of Bailey and Philips LED bulbs. 112
4.19 a PLC system in the presence of an optical eavesdropper. 112
4.20 Comparison between the analytically calculated and the simulated average secrecy capacity in function of the transmitted power for different PLC2 cable lengths. 117
4.21 Comparison between the analytically calculated and the simulated average secrecy capacity depending on the length between the LED array and the optical receiver for different transmitted power values. 118

A.1 Simple bias tee schema. 125
A.2 The frequency impedance of an inductor. 126
A.3 The frequency impedance of three inductors having different values. 126
A.4 The designed bias tee circuit 128
A.5 The s parameters of the designed bias tee (a) $S23$. (b) $S21$. 129
A.6 Simple TIA schema 129
A.7 Our designed TIA schema 132
A.8 Time domain simulation results of the signals at the output of each stage of the optical receiver (a) The photodiode current. (b) The Voltage at the output of the first stage. (c) The voltage at the output of the second stage. (d) The voltage at the output of the third stage. 133
A.9 The frequency gain of the optical receiver at each of its stages. (a) The gain after the second stage (b) The gain after the third stage 134

List of Tables

2.1 The ITU and IEEE defined bands for NB-PLC [46]. 39
2.2 HomePlug AV parameters [38]. 41

3.1 Estimated values of the equivalent circuits components of the red, green, and blue LEDs. 75
3.2 comparison of I and V_{TIA} calculated in 3 different cases: considering all the non-linearities, considering $L(i)$ linear, and considering $s(\lambda)$ and $p(\lambda)$ at the dominant wavelength of the LED. 80
3.3 VLC subsystem parameters. 84
3.4 Design of a 4000 K white light system using red, green, blue and white LEDs from Luxeon module [76]. 88

4.1 Specifications of the tested commercial LED bulbs. 96
4.2 Testbed parameters. 96
4.3 Physical layer parameters. 104
4.4 Parameters of the proposed scenario. 116

List of acronyms

ACO	Asymetrically clipped Optical
AF	Amplify and forward
AL	Active linear
BB	Broad-band
BCH	Bose-Chaudhuri-Hocquenghem
BER	Bit error rate
BPSK	Binary phase-shift keying
CP	Cyclic prefix
CSMA/CA	Carrier sense multiple access/Collision avoidance
DCO	Direct current-biased optical
DF	Decode and forward
DMT	Discrete multi-tone
DSO	Distribution system operators
EMC	Electromagnetic Compatibility
EMI	Electromagnetic interference
E/O	Electrical/Optical
FEC	Forward error corrector
FFT	Fast Fourier transform
FSO	Free space optics
HD-PLC	High-Definition Power Line Communication Alliance
HPA	Homeplug Powerline Alliance
HPAV	Homeplug AV
IEEE	Institute of electrical and electronics engineers
IFFT	Inverse Fourier transform
IM/DD	Intensity modulation/Direct detection
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector
IR	Infrared
LDPC	Low-Density Parity-Check
LED	Light emitting diode

LIFI	Light fidelity
LOS	Line of sight
MAC	Medium access control
NB	Narrow-band
NLOS	None line of sight
NSA	National security agency
OFDM	Orthogonal frequency division modulation
O/E	Optical/Electrical
PAM	Pulse amplitude modulation
PCS	Physical Coding Sub-layer
PDF	Probability density function
PPDU	Procedure Protocol Data Unit
PLC	Powerline communication
PMA	Physical media attachment
PMD	Physical medium dependent
PRBS	Pseudorandom binary sequence
PSD	Power spectral density
QAM	Quadrature amplitude modulation
RF	Radio frequency
RLC	Run-length limited codes
SMD	Surface mount device
SMPS	Switch mode power supply
SNR	Signal to noise ratio
TDMA	time domaine multiple access
TEMPEST	Telecommunications and electrical machinery protected from emanations security
TGbb	Task Group bb
TIA	Transimpedance amplifier
UDP	User Data protocol
UPA	Universal Powerline Alliance
VLC	Visible light communication
Wifi	Wireless fidelity

Chapter 1

General introduction

Besides radio frequency and infra-red, visible light communication is an alternative technology for wireless communication. This technology has demonstrated the advantage of of free license, high security, and high immunity to electromagnetic interference [62]. In fact, VLC uses visible light as a physical medium to transmit communication signals.

The rapid deployment of indium gallium nitride (InGaN)-based light emitting diodes (LEDs) in the lighting industry has attracted researchers to investigate the possibility of harnessing LED lighting to transmit communication signals. In fact, VLC can be leveraged in many applications such as vehicular communication for lane departure warnings, pre-collision detection, and traffic light violation warning to avoid accidents [53]. This technology can also be used in places sensitive to electromagnetic radiation such as airplanes and hospitals to prevent electromagnetic waves from interfering with other machines [20]. VLC can also be used for indoor communication thanks to LEDs that are initially installed for lighting [66]. However, in such application visible light communication (VLC) cannot be operated on its own [66]. It is a short-range communication system that must be connected to a backbone. In fact, powerline communication (PLC) network can be considered one of the most suitable backhaul networks for the VLC as they are naturally connected. On the other hand, PLC is a very mature technology and many standards are developed for different bands like G3-PLC for narrowband, and Homeplug AV (HPAV) for broadband PLC [59]. Indeed, PLC is already integrated as a stand-alone communication system in several applications. Using PLCs, electricity providers can remotely monitor and control energy consumption at the customer site. Smart meters can be linked to concentrators on low or medium voltage networks, allowing suppliers to have remote access to each customer, to transmit information such as tariffs, prepaid amounts, current and accumulated metering, etc. PLC can be used also for smart-grid monitoring where electricity generation is decentralized and the flow of electricity must be carefully controlled [59]. Additionally, the PLC can be used for in-vehicle communication where the available space to install equipment is limited (car, boats, airplanes, trains, etc.) [93]. Furthermore, in-home communication may be one of the most important applications of PLC. This type of

communication uses pluggable modems in power sockets and can be extended using Ethernet [59]. Back to PLC-VLC system, the implementation of such system is not easy as it looks, especially if we are looking for a high-bandwidth PLC-VLC system. Both PLC and VLC channels suffer from attenuation with the frequency increase. When cascading these two channels, the resulting channel may have very limited bandwidth. That's why few experimental studies are carried on in order to test the feasibility of broadband PLC-VLC integration, particularly those based on the amplify and forward (AF) relay. This relay amplifies and forward the PLC signal to the VLC system without modifying the original signal.

The combination of the two communication systems can be a promising solution to ensure the continuity of communication inside buildings or urban environments. But it can also be perceived as a risk, the PLC data can leak through the domestic LED bulbs as they are plugged in the powerline and can become an additional possibility of leakage. According to our knowledge, researchers have never studied this security threat. All attempts focus on facilitating and optimizing PLC-VLC integration. On the contrary, if we aim to isolate PLC from VLC, the risks of intercepting PLC signals through domestic LED bulbs should be carefully measured in order to ensure complete isolation.

1.1 Background and motivation

PLC-VLC integration offers the possibility of performing a wired transmission over existing powerline infrastructure and a short-range energy-efficient wireless transmission through pre-installed LEDs for indoor illumination. The first hybrid PLC and VLC system prototype was proposed in [55]. It was based on the use of a single carrier binary phase-shift keying modulation to provide a low rate transmission. Further works studied orthogonal frequency division modulation (OFDM) to compensate for the effect of multipath fading and frequency selectivity to reach higher throughput and get better spectral efficiency [54]. In [57], a PLC-VLC system based on the use of a direct current-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 [58], 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 [71], low complexity amplify and forward (AF) PLC-VLC system is proposed using spatial optical OFDM to reduce the peak to average power ratio. In [88], 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.

In spite of the existence of many studies to optimize the integration of these two systems, the number of experimental trials is quite limited. In [20], a hybrid broadband AF PLC-VLC system is proposed using OFDM modulation for localization and communication within

hospitals. In [102], video was transmitted through a PLC-VLC AF system using an array of three LED lamps. For [20], [102] the PLC-VLC system bandwidth is limited to 8 MHz located from 2 to 10 MHz because a limited frequency response LED lamp is used (white LED with a phosphor coating). In [89], a duplex PLC-VLC system is proposed based on the DF approach. The data rate achieved is 5 Mbit/s and it can be extended to 30 Mbit/s. Thus, to the author's knowledge, there is no report up to date on the feasibility of transmitting HPAV data directly into the optical system without making any modification to the PLC signal before being transmitted by the VLC system because of the mismatch between the phosphor white LED bandwidth and the bandwidth of the HPAV signal. Additionally, if a blue filter is used to suppress the slow response of the phosphor layer, the received optical power will be significantly reduced, which can also limit system performance. These shortcomings will be addressed in this thesis.

As we show in this these thesis, under some conditions the feasibility of transmitting an HPAV signal through an optical system without making any modification to this signal is confirmed, one can wonder if there is a risk of making optical side-channel attacks on PLC networks using LEDs luminaires that are connected to the same electrical network. But, if we look at the security aspect of the PLC system, we see that most research focus on the study of the risk of exploiting the electromagnetic field radiated in the vicinity of a PLC network for espionage. In [17], a preliminary investigation on the possibility of extracting some information from the radiated PLC signal when it propagates on an unshielded power cable has been carried out. Moreover, the authors in [85] show that an attacker can easily use electromagnetic radiation from power cables to eavesdrop or ex-filtrate powerline data using realistic scenarios. They also developed a system that identifies the presence of a hidden electrical network from the analysis of characteristic electromagnetic emissions in the frequency and time domains. Thus, in all the aforementioned studies, no investigation attempts to discover another side-channel that can threaten the PLC network like the visible light channel. The risk of PLC data leakage through domestic LED bulbs cannot be overlooked, especially since LED bulbs are directly connected to the electrical network.

Thus, in this thesis, we are going to fill in the gaps and treat the subject from two different aspects:

1. The first objective is to demonstrate the possibility of implementing a VLC system that it is able to transmit directly a broadband PLC signal (HPAV) without modifying the signal before being transmitted through the optical system. The proposed system resembles a PLC-VLC system with an AF-type relay. The only difference is that our system does not comprise a PLC signal amplification phase. Many optimizations are carried out in the design of the transmitter, the receiver and the choice of components in order to extend the system bandwidth as much as possible to be compatible with the bandwidth of the HPAV signal (2 MHz–28 MHz). Since the LED is the most critical component in the optical system as it has the narrowest bandwidth, a deeper analysis is performed on

3 monochromatic LEDs (red, green and blue) taking into account their optical, electrical and frequency behavior;

2. The second objective is to study the ability of commercial LED bulbs to inadvertently transmit PLC signals. As the PLC signal should cross the LED driver before arriving at the LED, a survey on used LED drivers in the domestic LED bulbs is made. Followed by a characterization of this side-channel using several LED bulbs of different brands and a real eavesdrop demonstration is performed. Simple LED driver modifications that foster and increase the leakage are analyzed. The physical layer security of the PLC networks in presence of a non-legitimate VLC system is also evaluated.

1.2 Structure of the thesis and contribution

The remainder or this thesis consists of three main chapters ended by a conclusion and organized as follows:

Chapter 2 It contains a literature review that presents the background knowledge of the hybrid PLC-VLC system. This includes a brief description of PLC and VLC systems considering their available standards, channel characterization, channel modeling, and noise analysis. In addition, it presents the most used modulation techniques in the VLC system. It also covers the different relaying techniques that allow the integration of the PLC and the VLC system. This chapter shows also the measurement results and modeling approach of cascaded PLC-VLC channel frequency response for indoor communication based on previous research. Moreover, this chapter presents a quick study on signal leakage through side-channel to highlight the importance of discovering all the existing auxiliary channels that can threaten the security of communication system. Finally, the topic of physical layer security is introduced considering the main types of wiretap channels. The fundamental metrics used to assess the physical layer security are presented as the equivocation rate, the secrecy rate, and the secrecy capacity.

Chapter 3 It constitutes the first contributions of this thesis. It shows the implementation procedure of our proposed PLC-VLC system. An experimental test is carried out to measure the bandwidth of 3 LEDs of three different colors (red, green, and blue) in order to choose the one with the largest bandwidth. Then, the frequency impedance of the LED is measured in order to find an equivalent circuit model for LEDs. Next, a theoretical expression is developed in order to accurately model the VLC system which can help us when designing the optical transmitter and receiver. Furthermore, the PLC-VLC system is implemented using commercial HPAV modems and our designed optical transmitter and receiver. This chapter also shows the throughput results of transmitting a User Datagram Protocol (UDP) packets through our manufactured PLC-VLC test-bed. To be able to theoretically extrapolate the measurement

results to larger-scale scenarios without the need to perform extra measurements, a theoretical study is performed using our test-bed parameters.

Chapter 4 It deals with the second aspect of the thesis which is the leakage of the PLC signal through domestic LED bulbs. In this chapter, many domestic LED bulbs of different brands are opened to see their drivers. An important model of the LED driver which has never been mentioned in the literature before is discovered. Afterwards, the side channel characterization is performed using all the already tested bulbs. This characterization starts with the measurement of the channel frequency response. Then, the power spectral density (PSD) of the received signal through the side channel is measured when the LED bulbs are plugged into the same powerline with HPAV modems. In addition, the maximum cross-correlation peak is calculated when a pseudo-random binary sequence (PRBS) signal is transmitted through this electrical-optical channel. This chapter presents also the results of transmitting a discrete multi-tone (DMT) signal that has almost the same parameters as an HPAV signal. Simple modifications of the LED drivers are also performed in this chapter to prove that it is possible to easily foster the leakage. The abovementionned tests are repeated after realizing these modifications. Finally, the physical layer security of the PLC system when a passive VLC eavesdropper is plugged in the same poweline network is investigated.

The thesis ends by a general conclusion of the main results obtained and directions for future works based on the findings.

1.3 Publications

1.3.1 Article

- Y. Yaacoub, F. Nouvel, S. Haese and J.-Y. Baudais, "Do optical side-channel attacks threaten the security of the PLC network?" in preperation.

1.3.2 International conferences

- Y. Yaacoub, F. Nouvel, S. Haese and J.-Y. Baudais, "VLC Modelization for VLC-PLC System: Evaluation of Optical, Electrical, and Frequency Behavior," *International Symposium on Circuits and Systems (ISCAS)*, Daegu, Korea, pp. 1–5, May 2021.

- Y. Yaacoub, F. Nouvel, S. Haese and J.-Y. Baudais, "A Seamless Broadband PLC-VLC Transmission: Performance Evaluation and Dimensioning," *International Symposium on Power Line Communications and its Applications (ISPLC)*, Aachen, Germany, pp. 61–66, October 2021.

- Y. Yaacoub, F. Nouvel, S. Haese and J.-Y. Baudais, "Can Commercial LED Bulbs Pose a Threat to PLC System Security" accepted to: *Global Communications Conference*

(GLOBECOM), Rio de Janeiro, Brazil, December 2022.

1.3.3 Poster

- Y. Yaacoub, F. Nouvel, S. Haese and J.-Y. Baudais, "Relayer directement la transmission de signaux PLC via lumière visible: mythe ou réalité". *Journée de l'innovation DGA maitrise de l'information*, Bruz, France, November 2021.

Chapter 2

Literature review

The PLC-VLC hybrid system is a cost effective communication system. It uses a ubiquitous infrastructure that simultaneously enables wired data transmission and power supply via electric cables as well as wireless data transmission and lighting via LED luminaire. The state of the art of each subsystem is reviewed in this chapter. Indeed, this chapter presents all the standards developed for PLC and VLC systems, their channel characteristics, then the types of noise affecting them, the applied modulation techniques used to improve broadband communication, the common relay techniques for integrating PLC and VLC systems, and the characteristics of PLC-VLC channels. It should be noted that this chapter focuses mainly on the transmitter part of the VLC system (more precisely the LED), as it is the most critical component due to its limited bandwidth. However, the optical receiver is not detailed because it is easier to achieve the desired bandwidth compared to the optical transmitter. In addition, an overview of the existing side channels is displayed followed by a survey on the most used LED drivers in lighting industry, in order to cover all the optical side channels that may exist and threaten the PLC system security. Finally, the physical layer security is covered from an information theoretic view. The main models of wiretap channels, the secrecy performance evaluation methods, and the main countermeasures are taken into account.

2.1 Powerline communication

The origin of PLC dates back to the year 1918 when a Japanese company tried to transmit voice telephony over a power line [69]. However, the ideas were even generated earlier at the end of the 19th century. Until 1950, the application of these technologies was quite limited. It was dedicated to the automation of certain tasks using low frequencies such as the remote control of public lighting. Then, the community lost interest in these communication systems until 1990 when progress in signal processing field led to powerful processing platforms capable of mitigating PLC channel anomalies [59]. In the following years, researchers restarted to extensively study the PLC system for many application such as smart metering, vehicular

communication, Home automation, *etc.* This section is divided as follows: section 2.1.1 presents a detailed overview on the PLC standards. paragraph 2.1.2 provides the PLC channel attenuation characteristics and models. Finally, paragraph 2.1.3 summarizes the various noises that may affect the powerline channel.

2.1.1 PLC standardization

To ensure interoperability between Powerline products from various industries around the world, international standards organizations have chosen a specific technology, defined its parameters, and standardized it. This section is divided into three parts. The first part presents the existing standards for the Narrow-band (NB)-PLC. The second part shows the Broad-band (BB)-PLC standards and the third part highlights in detail the HPAV [38] standard that is adopted throughout this thesis.

2.1.1.1 The narrow-band PLC standards

In this part, the international telecommunication union (ITU)-telecommunication section (T) [46, 48] and the institute of electrical and electronics engineers (IEEE) standards [42] are listed:

- The ITU family for NB-PLC is divided into four parts. The first part is G.9901 [46]. It defines the specifications of the power spectral density (PSD) of the PLC signal that the ITU-T standards must use. It complements the other three parts. The second part is the G.9902 also called Narrowband OFDM Power Line Communication Transceivers for ITU-T G.hnem Networks. It is developed by the ITU-T for smart-metering, vehicle to grid communication and in-home energy management. This standard uses OFDM and supports binary phase shift keying (BPSK) to 8-phase shift keying (PSK) and 16-quadrature amplitude modulation (QAM) mappers. It shares the same method for FEC and interleaving as the G3-PLC [46]. This standard is also defined in 7 frequency bands as listed in table 2.1: the CENELEC-A, the CENELEC-B, and the CENELEC-CD are adopted in Europe. FCC, FCC-1, and FCC-2 are the bands of the united state. Moreover, there exists the ARIB bands which is the defined band in Japan. The third part is the ITU-T G.9903 or the G3-PLC. It is created to meet the requirements of the french distribution system operators (DSO). The main standard features are its robustness through the use of a specific mode for harsh environments, its adaptive tone mapping capable of adapting to varying channel conditions and its specific two-dimensional interleaver (temporal and frequency interleaving) capable of mitigating both deep frequency fading and impulsive noise. It uses also reed Solomon and convolutional encoder. This standard is also defined in 3 frequency bands [48]: the CENELEC-A and the CENELEC-B, and the FCC (see table 2.1). The fourth part is the G.9904 also called Prime. This standard is developped by the Spanish DSO. The typical use-case behind this technology is as

Table 2.1: The ITU and IEEE defined bands for NB-PLC [46].

Band name	Bandwidth (kHz)
CENELEC-A	35.9375-90.625
CENELEC-B	98.4375-120.3125
CENELEC-CD	125-143.75
FCC	34.375- 478.125
FCC-1	34.375-137.5
FCC-2	150-478.125
FCC-above-CENELEC	154.6875-487.5
ARIB	154.7-403.1
ARIB-1	37.5-117.1875
ARIB-2	154.6875-403.125

was the case for G3-PLC: smartmetering. The technology is very similar to the G3-PLC. They are both OFDM based, they use differential BPSK, Quadrature phase shift keying (QPSK) and 8-PSK. This part also uses error correction mechanisms such as a convolutional encoder. However, the correction code can be entirely disabled to increase the throughput as in User Data Protocol (UDP). Furthermore, it uses a block interleaver to spread the information inside an OFDM symbol to overcome the frequency fading. The physical layer is defined in only one frequency band [47] which is the CENELEC-A (Europe) (table 2.1);

- The IEEE provides a single standard for NB-PLC which is IEEE 1901.2. This standard takes into account either indoor PLC networks or outdoor networks. It is mainly based on G3-PLC technology, especially for the physical layer. However, it differs from G3-PLC in the medium access control (MAC) layer. It also provides information on Electromagnetic Compatibility (EMC) requirements and coexistence mechanism with other technologies using the same band. IEEE 1901.2 is defined in 6 frequency bands [42]: the CENELEC-A, the CENELEC-B, FCC-above-CENELEC, the FCC, the ARIB-1, and the ARIB-2 (see table 2.1).

2.1.1.2 The broad-band PLC standards

Initially, the BB-PLC was designed for in-home communication by three main industrial alliances: the Homeplug Powerline Alliance (HPA), the High-Definition Power Line Communication Alliance (HD-PLC) and the Universal Powerline Alliance (UPA). The technologies developed by each alliance cannot interoperate with each others. Consequently, The IEEE and the ITU-T established standard specifications for BB-PLC to unify these technologies:

- The IEEE developed the 1901 standard [41]. As HPAV and HD-PLC have different physical

layers based on OFDM and wavelet transform respectively, the 1901 standard developed a common MAC layer for both technologies and two protocols of physical layer convergence that provide the possibility to use both physical layers. The first physical layer is the OFDM. It uses the same signal processing techniques as in HPAV: same scrambler, turbo forward error corrector (FEC) encoder, channel interleaver, and finally support for the same modulations (BPSK, QPSK and {8, 16, 64, 256, 1024}-QAM). However, IEEE 1901 brought some improvements listed below:

1. IEEE 1901 operates in a frequency band between 2 MHz and 50 MHz with 1974 used subcarriers, while the HPAV operate in a the 2 MHz to 28 MHz with 917 used subcarriers;
2. Shorter guard interval to increase the overall throughput;
3. Support for 4096-QAM for channels presenting high signal to noise ratio (SNR);
4. More efficient code rate for the turbo encoder: 16/18 in addition to 1/2 and 16/21;
5. The data rate is improved from 200 Mbit/s in the case of HPAV to 500 Mbit/s in the case of IEEE 1901.

The second physical layer protocol is based on the Wavelet-OFDM. It supports only pulse amplitude modulation (PAM) up to 32-PAM and uses 512 subcarriers from 0 Hz to 30 MHz. Only 338 of them are used in practice to cover the 2 MHz to 28 MHz band.

- The ITU-T developed the G.996x standard. This standard was not designed specifically for PLCs. It defines a generic windowed OFDM physical layer and a common MAC layer for media present inside a home such as: telephone lines, power lines, coaxial cables, Ethernet cables and even optical fiber. For PLCs, this standard defines 3 frequency bands [45] starting from 0 MHz to 25 MHz, to 50 MHz, and to 100 MHz and having respectively 1024, 2048, and 4096 carriers. In addition, it supports QAM modulation (from BPSK to 4096-QAM) and Low-Density Parity-Check (LDPC) FEC encoder and it uses an optional repetition encoder to increase time diversity. However, this standard does not implement an interleaving block.

2.1.1.3 Homeplug AV (HPAV)

HPAV is one of the most popular high-speed industrial specifications for PLCs. Its physical layer has an operating frequency band from 2 MHz to 28 MHz and a hybrid carrier sense multiple access (CSMA), collision avoidance (CA) and time division multiple access (TDMA) MAC layer. It uses QAM modulation and adaptive bit loading with a modulation order of up to 10 bit/carrier. This protocol also adopts interleaver and turbo convolution encoder. The waveform of the HPAV protocol is of the "Pulse-Shaped OFDM" type. This modulation technique improves the frequency localization by shaping each OFDM symbol using a window

and interleaving it with the previous symbol and the next symbol, which lengthens the duration of the symbol. At the receiver, the signal is recovered using a simple rectangular window, hence the name "windowed OFDM" [38]. Table 2.2 shows the different parameters of the HPAV protocol.

Table 2.2: HomePlug AV parameters [38].

Parameter	Value
Scrambler	Yes
Forward error corrector	Turbo code
Interleaver	Yes
Mapper	QAM 2 to 1024
Modulation	Windowed-OFDM
IFFT/FFT size	3072
Number of total subcarriers	1536
Sampling frequency	75 MHz
Bandwidth	2-28 MHz
Inter-carriers space	24.414 kHz
Symbol time	40.96 µs
Guard interval	5.56 µs or 7.56 µs or 47.12 µs
MAC layer protocol	Hybrid: CSMA/CA & TDMA

2.1.2 Channel characteristics

Power lines are originally designed to carry electrical energy, which means they have poor characteristics when they are used as communication channels. They suffer from impedance mismatch, high noise levels and fading which directly impact communication quality [59]. It is therefore important for the design of an appropriate system to have a realistic model of the PLC channel. This paragraph presents the different attenuation characteristics of the PLC channel and the two main modeling approaches used for PLC channel.

2.1.2.1 Channel attenuation characteristics

Channel attenuation is one of the most crucial problems in PLC and especially for broadband communication systems [99]. When the high frequency signal travels the powerline channel, it will be exposed to impedance mismatch, resonance, reflection, standing waves and many other phenomena that may attenuate it. Thus, two channel attenuation characteristics are listed below [99]:

- The channel attenuation increases with the increase of frequency. Also, there are special frequencies where the signal is more faded compared to other frequencies due to impedance mismatch;

- The distance is another reason for the signal attenuation. In fact, the attenuation increased with the distance separating the transmitter from the receiver.

2.1.2.2 Channel models

Characterizing the powerline channel is very complicated due to the heterogeneity of the networks and the lack of common wiring practices. In addition, the PLC channel is a frequency-selective and a time-varying channel, which makes the modeling process very difficult. Several approaches have been followed for modeling the powerline channel. In this part, we point out the two main approaches proposed to model the PLC channel for broadband communication.

Top down approach The top down approach uses a multipath model as can be seen in fig. 2.1. In fact, the PLC signal will not propagate in a direct line of sight path between the transmitter and the receiver. Indeed, The impedance mismatches and the powerline branches create echos of the original signal leading to the multipath model and frequency selective fading. According to [109], this model can be represented using the following expression:

$$H_P(f) = \sum_{i=0}^{N-1} g_i e^{-(\alpha(f)+j\beta)l_i} \tag{2.1}$$

and

$$\beta = \omega\sqrt{L'C'} \tag{2.2}$$

where N is the number of paths, g_i is the combination of reflection and transmission coeffi-

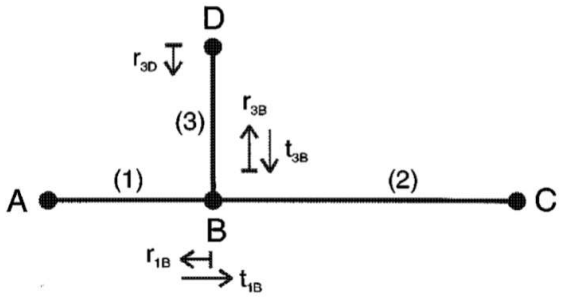


Figure 2.1: Multipath model [109].

cients in the i^{th},α denotes the real part of the frequency dependant propagation coefficient whereas β denotes the imaginary part of the propagation coefficient and it is called the phase constant, l_i represents the cable length, ω is considered as the angular frequency,L' and C' represent the link inductance and capacitance per unit length, respectively.

It should be noted that many researches have performed further statistical analyses for each parameter of this expression (2.1) based on real measurements, in order to extend the above-mentioned model [97].

Bottom-up approach The bottom-up approach models the power line based on transmission line theory (see fig. 2.2). When power lines are used to transmit a high frequency communication signal, they can be treated as transmission lines that guide transverse electromagnetic waves. This model requires a previous knowledge of the powerline cables parameters and characteristics to be able to calculate the intrinsic parameters (the conductance per unit length between two wires G', the resistance per unit length R', the capacitance per unit length C', and the inductance per unit length L') of the transmission line. Then, using these parameters the transfer function is determined based on scattering matrices or transmission matrices [25]. It is worth to mention that despite the computational complexity of the bottom-up approach,

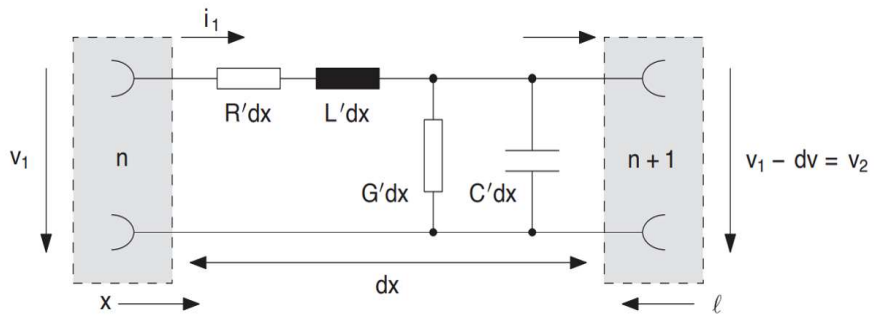


Figure 2.2: Transmission line propagation [59].

a statistical extension is found in [97]. Similarly, many studies have succeeded in creating random channel generators. Additionally, using this approach, the researchers were able to model the time-varying nature of the PLC channel[9].

2.1.3 Noise characteristics

Besides channel attenuation, the noise is a major problem that affects the quality of the communication. In household power lines, the source of noise can be inside or outside the power grid. The internal source of noise comes from the various electrical devices that are plugged into the powerline network while the external source of noise is due to the low electromagnetic shielding performance of the powerline cables. In this part, the various kind of noises are listed [99]:

- *The background noise.* The domestic alliance is the main source of the background noise. It results from the summation of many noise sources of low power. It has a relatively low PSD and can interfere with signals at frequencies below 30 MHz;

- *The Narrowband noise.* It is caused by wireless signal interference having frequencies between 1–22 MHz. This noise occurs as the combination of many amplitude modulated sinusoidal signals;

- *Random impulse noise.* It is caused by switching transients in the power grid. It has a severe impact on the BB-PLC. Its damage is assessed by the pulse amplitude, width and the interval of time. This kind of noise may occur in as a single pulse or a series of pulses. Each pulse has the form of a time decayed sinusoidal signal;

- *Periodic impulsive noise.* There exists two types of periodic impulse noise: asynchronous and synchronous noise. The asynchronous periodic noise occurs with a frequency range that varies between 50–100 Hz. They are usually caused by televisions and computer monitors. The second kind of noise is synchronous to the mains frequency. They are mainly generated by the switching actions of the rectifier diodes existing in many electrical appliance. This kind of noise persists for a long time, has a high power and has a wide frequency range.

2.2 Visible light communication

The idea of transmitting communication signals using optical means is very old. The Archaic Greeks used flares to warn of the existence of enemies. Additionally, ancient Chinese warriors used beacons to indicate an impending threat [3]. In 1810, Carl Friedrich invented the heliograph which is a solar telegraph. The principle of this telegraph is to transmit the signal by interrupting the sunlight using a shutter or a rotating mirror [91]. In 1880, the world's first wireless telephone was developed by Alexander Graham Bell. It was based on the modulation of sunlight by voice messages using a vibrating mirror at the transmitter. The receiver of this system used selenium which is an optical/electrical (O/E) transducer to detect the optical signal [13]. In 1962, an experimental attempt to send a communication signal through a laser diode was carried out by a Hughes group over a range of 30 km [27]. In the following years, other studies are performed in the laser optical communication field. The last studies found that the laser diode is not suitable for communication because the laser has a very large beam divergence [30]. Therefore, the focus has been moved to fiber-based systems where the laser problems are more manageable. In this regards, an infrared (IR)-based system was implemented in 1979 [26], which encouraged many researchers to try to carry out further research on this system. However, eye safety regulations have fixed the amount of IR power that can be emitted, which has created a significant link budget limitation for IR networks [36]. After the rapid spread of LEDs in the lighting industry, researchers became interested in investigating the possibility of incorporating the lighting infrastructure with wireless communication using VLC (see fig. 2.3). In 2002, Komine and Nakagawa came up with the first model of the LED-based VLC system for indoor communication [56]. Later, many other researchers set up real test beds to validate the feasibility of this system. So far, many improvements have been made to these systems in order to achieve high data rates. Therefore in this section, the various achievements in the field of VLC are presented. The different VLC standards are listed.

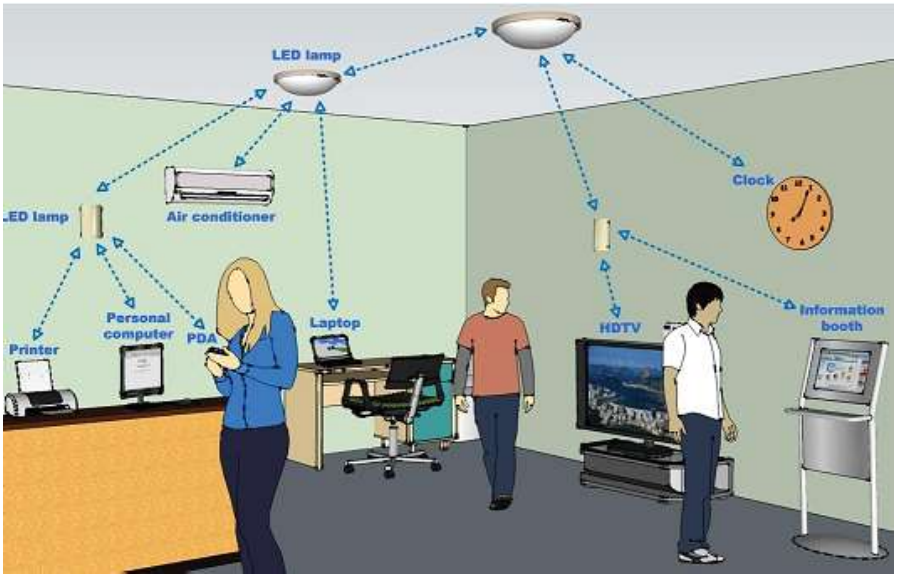


Figure 2.3: Indoor VLC system using LED lighting [21].

In addition, LED lighting technologies that can be used in communication are investigated. Finally, channel characteristics are detailed followed by a summary of the different types of VLC noise.

2.2.1 Visible light communication standards

With academic progress in the field of VLCs, manufacturers start to be more and more attracted by this wireless communication technology, which has prompted standardization bodies to define parameters and standardize the VLC system. In this section, the three VLC standards are described, underlining their physical layer parameters.

2.2.1.1 IEEE 802.15.7

In 2011 the IEEE has published the 802.15.7-2011 standard for VLC. Few years later, a new version has taken an approval in December 2018 [43]. This standard define the physical layer and the MAC layer for the VLC systems and ensure a data rate that allows audio and video transmissions. The physical layer is divided into 6 different types depending on the usage environment and the transmission rate. The first physical layer is dedicated to outdoor communication and operates between 10 to 266s kbit/s, while the second is dedicated for indoor comunication with a data rate of tens of Mbit/s. The third physical layer is created for applications with multiple transceivers with a data rate of tens of Mbit/s. The fourth and the fifth physical layers are respectively used for discrete light sources and for diffused surface light source. Finally, the last physical layer is dedicated for video displays with a rate of up 512 kbit/s [43]. It should be noted that the most used physical layer types are the first three

above-listed types.

The first two physical layer types are defined for a single light source, support on-off keying, and variable pulse position modulation. In fact, the on-off keying modulation is the simplest modulation scheme for VLC, where the LED is turned on and off to send the bits of communication data. The variable pulse position modulation changes the duty cycle of each optical symbol to encode the bits. To avoid a long series of ones or zeros that may cause light flickering, run-length limited codes (RLC) are also defined for these two physical layers like the Manchester code, 4B6B code, and 8B10B code [43].

The third physical layer has multiple optical sources from different colors and supports a particular modulation format called Color shift keying that encodes the bit patterns into color combinations. This type of modulation does not require the RLC [43].

Moreover, the 802.15.7 supports also FEC codes for indoor and outdoor VLC systems. For the indoor case, this standard adopts Reed Solomon code while for the outdoor, it adopts both Reed Solomon and convolutional coding [43].

2.2.1.2 ITU-T G.9991

The ITU-T established as well its own standard for VLC that is called G.9991 or ITU VLC [44]. This standard specified physical layer and MAC layer parameters for high speed indoor VLC. Indeed, it supports two physical layers. The first one is based on DCO-OFDM while the second is based on ACO-OFDM, which are described as follows:

- The DCO-OFDM is a modulation technique first proposed by Carruthers and Kahn [10]. The main purpose of DCO-OFDM is to generate a real and positive OFDM signal. This technique consists in using the property of Hermitian symmetry to obtain a real signal which is done by using half of the sub-carriers of the OFDM symbol of length N to transmit the useful symbol modulated according to different constellations (BPSK, QPSK, QAM...) and the other half of the subcarriers are used to transmit their complex conjugates. Then, an IFFT is applied to obtain the real-valued time signal. A sufficient amount of DC bias is added to convert the resulting bipolar signal to a unipolar signal (see fig. 2.4). Finally, the remaining negative peaks are removed by hard clipping;

- The ACO-OFDM is proposed to avoid the added DC bias used in the case of DCO-OFDM. This approach is initially proposed by Armstrong and Lowery in [49]. It is based on the use of subcarriers having only odd indexes of the OFDM symbol. $N/4$ useful complex symbols are transmitted on the first $N/4$ sub-carriers followed by the application of the Hermitian symmetry. The obtained time domain signal after performing the inverse fast fourier transform (IFFT) is an anti-symmetric real signal, which means that the negative part is the mirror of the positive part and can be eliminated by zero-level clipping (see fig. 2.5).

The two physical layers include three sub-layers which are as follows [44]:

1. Physical Coding Sub-layer (PCS)
2. Physical Media Attachment (PMA) sub-layer
3. Physical Medium Dependent (PMD) sub-layer

The PCS maps the MAC layer data unit into physical frames. Then, the PMA scrambles and encodes these frames. Finally, the PMD sub-layer modulates the PMA frames using DCO-OFDM or ACO-OFDM and transmit them over the optical channel. It should also be noted that besides the payload, the physical frame includes a preamble in its header for synchronization and channel response estimations [44].

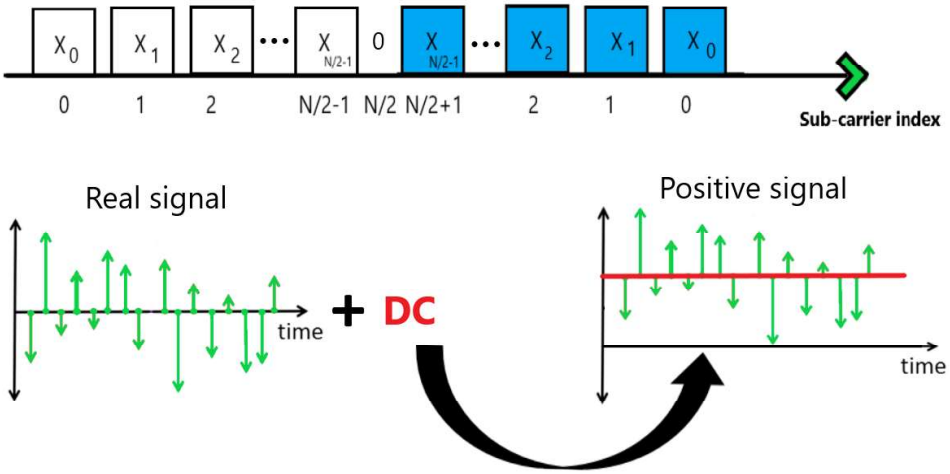


Figure 2.4: Frequency and time domaine DCO-OFDM signal.

2.2.1.3 IEEE 802.11bb

In July 2018 a task group named IEEE 802.11 Light Communications Amendment-Task Group bb (TGbb) was created in order to standardize mobile networked light communication. The main target of TGbb is to enable the coexistence between wireless fidelity (WiFi) and light fidelity (LiFi) [82]. LiFi can profit of the wide spread of Wifi to easily enter the market while improving its capabilities without interfering with it. The TGbb starts setting the physical layer parameters. So far, two main proposals for the structure of the physical layer have been declared.

The first is based on the use of an already existing WiFi chipset and LiFi front ends. However, the signal delivered by the WiFi chipset is not suitable to be transmitted directly by the LiFi system. Therefore, frequency upconversion is performed, followed by the addition of DC

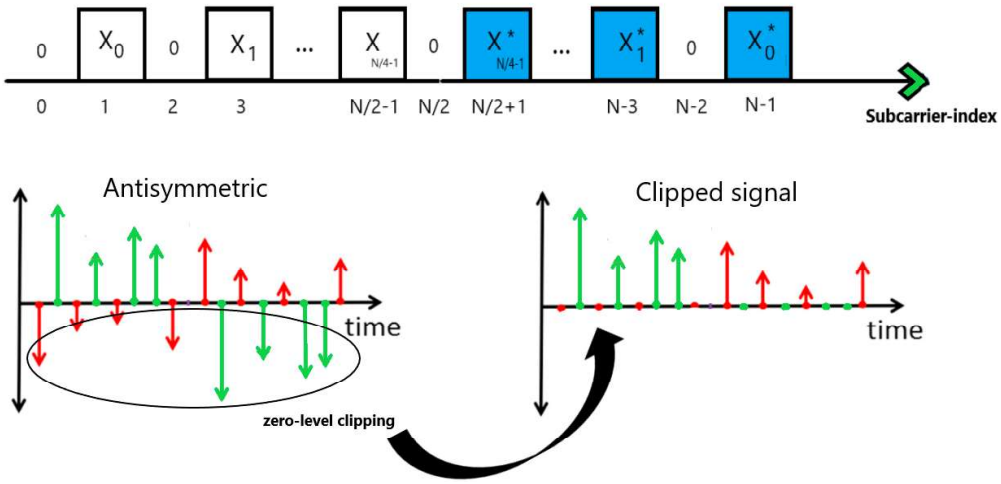


Figure 2.5: Frequency and time domaine ACO-OFDM signal.

bias to enable intensity modulation and direct detection (IM/DD) over the LEDs. The main advantage of this proposal is that no additional modification of the WiFi chipset is required. However, the frequency upconversion reduces the modulation bandwidth by eliminating the frequency spectrum near the DC. The upconversion also leads to having a high center frequency implying higher attenuation due to the limited bandwidth of the LED.

The second approach is based on the use of ACO-OFDM or DCO-OFDM with adaptive bit loading. It is more complicated than the first approach because many modifications in the digital domain must be carried out in order to obtain a Physical Layer Convergence Procedure Protocol Data Unit (PPDU) compatible with that of 802.11 [81].

It should be emphasized that many studies are underway to find other approaches that can guarantee both spectral efficiency and low complexity.

2.2.2 Light-emitting-diodes for visible light communication and lighting

In the lighting industry, there are two main techniques for generating white light. After the great progress in the field of VLCs, many researchers have tried to exploit the white LEDs dedicated to lighting in high-speed communications. In this part, the different methods of generating white light are described, highlighting their main advantages and disadvantages for lighting and communication.

2.2.2.1 Blue LED with phosphor coat

The most adopted technique in the lighting industry is based on the use of a blue LED which excites a yellow inorganic phosphor. The combination of blue emission and broad yellow emission creates white light [36, 77] (see fig. 2.6a). Although this technique is considered

inexpensive and simple, some studies show the evinced between blue light and eye damage and recommend reducing the time of eye exposure to blue light [105]. Regarding the use of this type of LED for VLC, the slow response of the yellow phosphor limits the modulation bandwidth of the white LED to a few MHz. Hence, many techniques have been proposed to overcome the bandwidth limitation such as using a pre- and post-equalizer or placing a filter in front of the optical receiver to get rid of slow yellow light. However, it has been shown that the last solution considerably reduces the received optical power [96].

2.2.2.2 RGB LED

The second techniques uses the combination of three monochromatic RGB LEDs (red, green, and blue LED) to obtain the white light as it shows fig. 2.6b. This technique permits to vary the white tone and the color temperature according to the users preferences. In addition, it provides the possibility to reduce the intensity of the blue light to ensure eye comfort. However, RGB LED is much more expensive and more complicated in manufacturing than the phosphor coated blue LED described in § 2.2.2.1. In terms of communication performance, the RGB LED has a larger modulation bandwidth since it does not require a phosphor coat. It also offers the opportunity to use the wavelength division multiplexing technique that can attain a high data-rate up to 11.28 Gbit/s [36, 77].

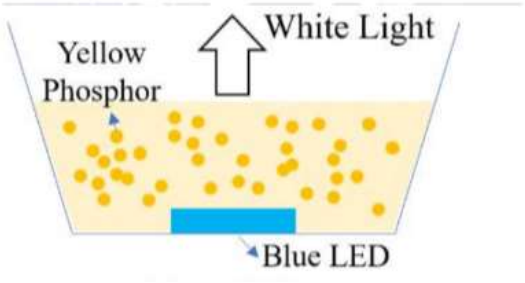
Note that for both techniques, the size of the LED has a major impact on the modulation bandwidth. In fact, as the active area of the LED increases, the space of charge capacity increases, thereby reducing the LED modulation bandwidth. Therefore, micro LEDs are developed to overcome the bandwidth limitation. Micro-LEDs have a very small surface area offering several hundred MHz. However, this type of LED cannot be used for lighting due to the large number of LEDs required to provide the required amount of optical power [3].

2.2.3 Channel characteristics

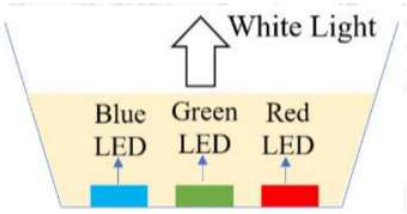
The VLC channel is a very important element that must be carefully studied when designing a VLC system. However, when modeling the VLC channel, the LED frequency response must be considered as it limits the channel modulation. Besides the low-pass filter behavior of the LED, its non-linear behavior must also be taken into account. Hence, this paragraph introduces the frequency response model of the VLC channel (transmission and propagation) and the nonlinear behavior of the LED

2.2.3.1 Channel model

The transfer function of the indoor VLC channel can be modeled by the summation of a line of sight (LOS) and non-line of sight (NLOS) components. The LOS components are the result of the direct reception of the LEDs light. They can be modeled by Dirac pulses. However, the



(a)



(b)

Figure 2.6: Generating white lights using LEDs [51]: (a) Blue LED with a phosphor layer, (b) RGB LED.

NLOS component considers the photodiode reception of lights after being reflected by objects and obstacles inside the room. They are usually modeled by an integrating-sphere model. So, the channel frequency response can be written as [77]:

$$H(f) = \sum_{i=1}^{N_{LED}} H_{LOS,i} \exp(-j2\pi f \Delta\tau_{LOS,i}) + H_{NLOS} \frac{\exp(-j2\pi f \Delta\tau_{NLOS})}{1 + \frac{jf}{f_0}} \tag{2.3}$$

where N_{LED} is the number of LEDs, $H_{LOS,i}$ and H_{NLOS} are respectively LOS and NLOS channel gains, $\Delta\tau_{LOS,i}$ and $\Delta\tau_{NLOS}$ represent the corresponding signal delays, and f_0 is the cut-off frequency of the NLOS channel. According to [56], the NLOS can be neglected as the major amount of optical power is received through the LOS channel. Thus, for the rest of the manuscript, only the LOS component is considered. The LOS channel gain $H_{LOS,i}$ for the i^{th} LED can be modeled by the following equation:

$$H_{LOS,i} = \frac{AGS(m+1)\cos^m(\phi_i)\cos(\psi_i)}{2\pi D^2}, \qquad \psi_i < \psi_{\text{FOV}} \tag{2.4}$$

where A is the active area of the photodiode, G is the gain of the lens that concentrates the light to the photodiode, S represent the sensitivity of the photodiode, m is the is the Lambertian index, ϕ_i and $\psi_i$are the angles of irradiance and incidence respectively, D is the distance between the LED and the photodiode ψ_{FOV} is the irradiance angle of the field of vision of the

receiver, and ψ_{FOV} is the irradiance angle of the field of vision of the receiver, see fig. 2.7.

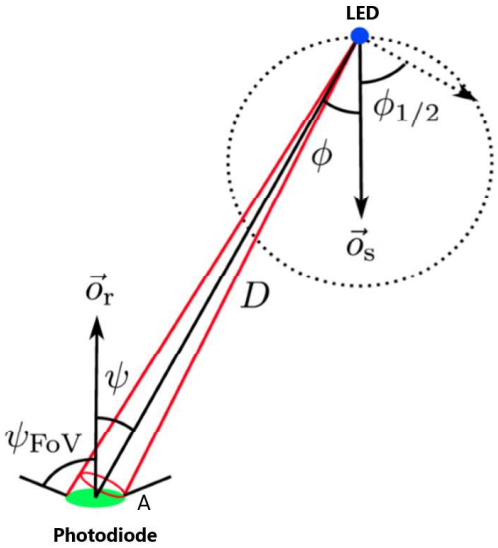


Figure 2.7: Optical wireless channel DC gain geometry [3].

As explained in § 2.2.2, LEDs have a limited modulation bandwidth which varies according to their size. In order to accurately model the VLC channel response, the LED frequency response must be introduced within the model. According to [64], the frequency response of the i^{th} LED can be modeled by a first order low-pass filter as:

$$H_{L,i} = \frac{1}{1 + j\frac{f}{f_{c,i}}} \tag{2.5}$$

where f_c is the -3 dB cut-off frequency of the LED frequency response. Furthermore, when the blue LED with phosphor coat is used, the frequency response of the phosphor can be modeled also by a first order low-pass filter as:

$$H_{phosphor} = \frac{1}{1 + j\frac{f}{f_0}} \tag{2.6}$$

where f_0 is the -3 dB cutoff frequency of the phosphor coat response. Consequently, the LED frequency response can be written as:

$$H_{LED,i} = \begin{cases} H_{L,i} H_{phosphor}, & \text{if blue LED with phosphor coat} \\ H_{L,i}, & \text{if monochromatic LED} \end{cases} \tag{2.7}$$

The total channel frequency response can be represented by the concatenation of the

channel response $H_{LOS,i}$ and the LED frequency response $H_{LED,i}$ as:

$$H_{total} = H_{LOS,i} H_{LED,i} \tag{2.8}$$

2.2.3.2 LED non-linearity

The LED is a transducer that transforms the electrical signal into an optical signal. However, the electrical-to-optical (E/O) conversion is not linear, which introduces distortion into the transmitted signal [36]. The E/O characteristic of a LED in fig. 2.8 shows there is a limited region, for a current value greater than I_{min}, where the LED response (red curve) matches the linear expected response (blue curve). In this region, the response can be considered quasi-linear. Beyond the linear zone, we can notice that the two curves begin to separate which means that the LED enters the saturation zone. This zone is limited by the saturation current I_{max} which cannot be exceeded.

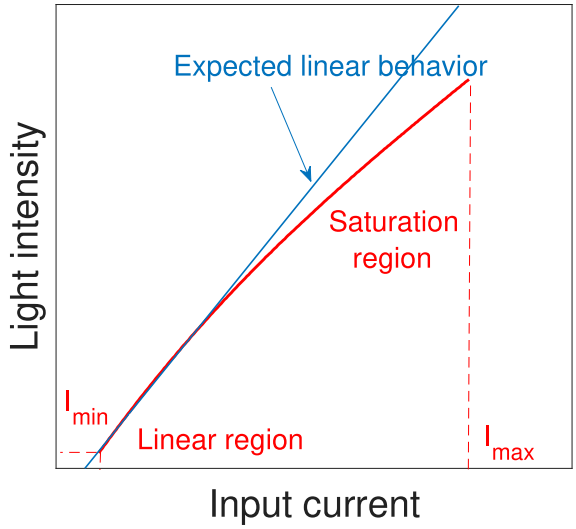


Figure 2.8: The LED E/O characteristic.

When the current amplitude of the communication signal goes out of the linear region, it will be clipped and distorted. This non-linear behavior of the LED degrades the performance of the VLC system which pushes the researchers to find techniques to linearise the E/O relationship like pre-distortions [23] and iterative signal clipping with multiple LEDs [70] .

2.2.4 Noise characteristics

Noise is another impairment source that can affect the VLC system performance. In VLC, noise is classified into two categories: noise from electronic components and noise from parasitic optical sources [77]. In this part, the three main noise sources are depicted:

- *Background noise.* Solar radiation penetrating through doors and windows is the primary background noise source. The modelization of the solar noise is a tedious process as it can change depending on the location inside the room, the time of the day, and the window orientation. Additionally, light bulbs such as incandescent and fluorescent lamps contribute to this type of noise but their effect can be canceled by using an electrical high pass filter at the receiver [3];

- *Shot noise.* The shot noise is induced in the photodetector due to the electron generation when the photodiode is exposed to light. Shot noise increases with increasing light intensity because higher light intensity boosts the number of photon-electron interactions. Besides solar radiation and artificial light, the information signal itself is considered an unavoidable source of shot noise. According to [39], the shot noise can be modeled as a white Gaussian noise (AWGN);

- *Thermal noise.* Trans-impedance amplifier (TIA) is used as the first stage amplifier in the VLC system receiver [39]. It is the main cause of thermal noise which is due to the motion of the thermal electrons in the TIA circuit creating an AWGN [3].

2.3 PLC and VLC systems integration

The PLC system is now a very popular communication system in home networks. To add mobility features to this system, researchers are beginning to integrate it with other wireless communication systems. Since LED lamps are naturally connected to the power line, VLC can be a strong contender as a wireless extension for the PLC. In fact, the direct integration of the PLC and the VLC systems is not as simple as it seems, especially because their channels are not designed for communication. The VLC system has limited bandwidth due to the attenuation of the limited LED frequency response which can be around 10 dB at 50 MHz. This attenuation is acceptable if the VLC is implemented alone. However, when the VLC system is integrated into the PLC system whose channel also suffers from severe attenuations with increasing frequency, the overall channel bandwidth will be significantly reduced, leading in some cases to a non-functional PLC-VLC system [20]. In 2002, Komine demonstrated in [55] the feasibility of a simple PLC-VLC system. As shown in fig. 2.9 this system uses a narrowband signal which is first transmitted by electric cable until it reaches the VLC transmitter. In this phase, the signal coming from the cable is divided into two parts: *i*) the first part is filtered using a band-pass filter to recuperate the communication signal that will be transmitted through the LED; *ii*) the second part is rectified and transformed from alternating current to direct current to power the LEDs. This simple technique was the basis of all subsequent studies. Many achievements are still underway to develop this idea. However, the main step in designing new PLC-VLC systems is to be able to accurately model their channels. But, before moving to the modeling

phase, it is necessary to specify the relaying method adopted to connect the PLC system to the VLC system. Thus, this section explains the existing relaying techniques that are developed to combine the PLC and the VLC system in addition to the hybrid channel characteristics.

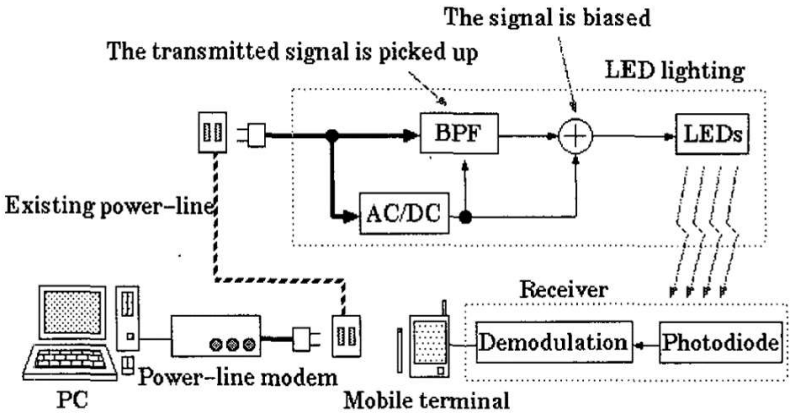


Figure 2.9: Komine PLC-VLC system model [55].

2.3.1 PLC-VLC relaying techniques

The conventional PLC and VLC system integration would apply a complete PLC system with a complete VLC system connected through the application layer. However in [67], an alternative form of integration inspired by cooperative transmission techniques was proposed, namely the use of relays. In fact, a PLC-VLC hybrid system can be thought of as a relay-assisted two-hop communication system with no direct link between source and destination. The PLC and VLC systems act as the first and second hop respectively where the LED is the component that ensure their connection. The relay between the PLC and the VLC systems can be made using two different methods:

- The amplify and forward (AF) relay: The PLC signal is amplified and re-transmitted by the VLC system without modifying the original signal [71] as it is shown in fig. 2.10. Despite the simplicity and the power efficiency of this method, the PLC noise is also amplified and transmitted by the VLC system which can degrade the performance of the hybrid PLC-VLC system [67];

- The decode and forward (DF) relay: The PLC signal arriving at the LED is demodulated and decoded then re-encoded and re-modulated for VLC transmission, see fig. 2.11. Although the DF technique can have better communication performance, it requires significant signal processing thus complicating the communication system and negatively affect the power efficiency of the PLC-VLC system[71, 67].

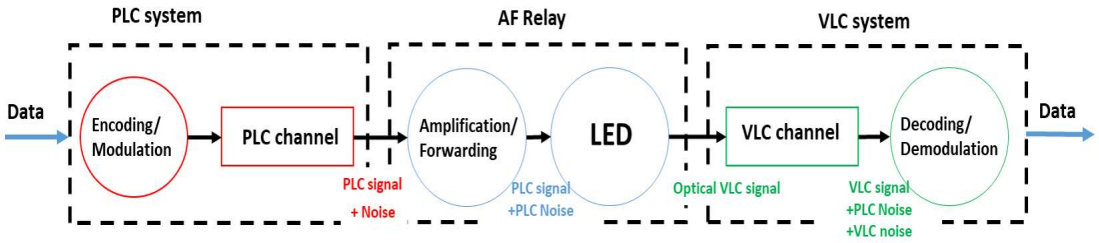


Figure 2.10: Amplify and forward PLC-VLC system block diagram

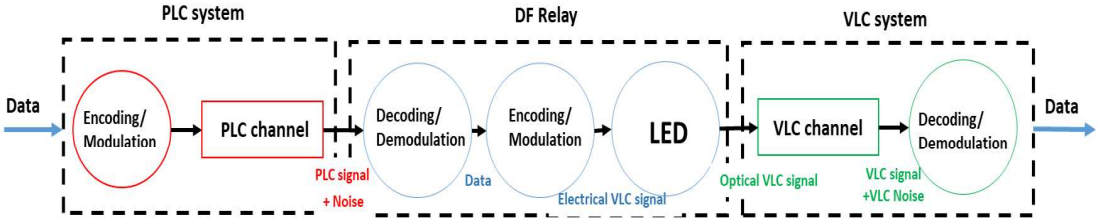


Figure 2.11: Decode and forward PLC-VLC system block diagram.

The implementation of relays in a hybrid communication system is studied for the combination of different communication systems such as PLC-WiFi and free space optics (FSO)-VLC. It is proven that the use of hybrid systems surpasses the use of each system individually. In [19], AF relay is adopted to combine PLC with WiFi. However, in [32], a DF relay is established between the FSO and VLC systems. In [29], the performance of the hybrid AF PLC-VLC system is studied in terms of average capacity. In addition, in [28], a full analysis is performed on the PLC-VLC hybrid system with the presence of a DF relay. Despite the existence of several studies that show that DF has better performance than AF, researchers prefer to use AF relay in the PLC and VLC systems integration because it consumes less power and does not require a very sophisticated VLC transmitter, which are key parameters in the case of the PLC-VLC system.

2.3.2 Channel characteristics

As both PLC and VLC channels are connected, their effects must be considered when modeling the hybrid PLC-VLC channel, especially if they are connected using an AF relay. In the case of AF, the hybrid PLC-VLC system channel can be considered as the cascading of the two PLC and VLC channels. Hence, the channel frequency response of the AF PLC-VLC system can be expressed as it follows [73]:

$$H_{PLC/VLC}(f) = H_{PLC} H_{VLC} \tag{2.9}$$

where H_{PLC} and H_{VLC} are respectively the PLC and the VLC channel frequency responses. H_{PLC} can be expressed by the expression (2.1) based on the top down approach. The VLC channel frequency response can be expressed using the equation (2.8). Accordingly, the

PLC-VLC channel frequency model can be written as the following expression:

$$H_{PLC/VLC}(f) = H_{LED} \sum_{i=0}^{N-1} g_i exp(-(\alpha(f) + j\beta) l_i \sum_{i=0}^{N_{LED}} \frac{AGS(m+1)\cos^m(\phi_i)\cos(\psi_i)}{2\pi D^2} \quad (2.10)$$

where H_{LED} is the LED frequency response model formulated in (2.7).

In [20], Ding and al. compares the cascaded PLC-VLC channel to the solely VLC channel. It is found that the measured VLC attenuation at −12 dB at 30 MHz which is acceptable for the standalone VLC system. However, the hybrid PLC-VLC channel response shows an attenuation of −35 dB at 30 MHz (see fig 2.12). Thus, the cascading of the VLC to PLC channel leads to a sever attenuation at high frequencies which limits the modulated bandwidth [20] It should be

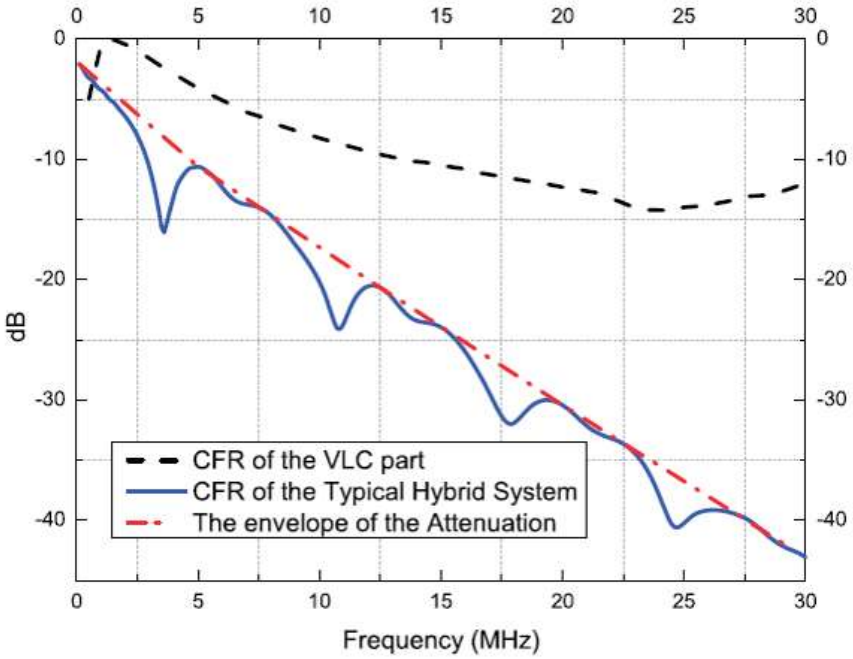


Figure 2.12: The measured channel frquency response (CFR) of the VLC part, the CFR of a typical hybrid PLC and VLC communication system [20].

mentioned that the hybrid PLC-VLC system is subject to all types of noise encountered in PLC system (see § 2.1.3 and 2.2.4).

2.4 Side channel attacks

Communication systems may diffuse signals along channels not intended for these signals. Such channels are called side channels. The side channels can be intercepted and illegally exploited to extract information resulting in a high-risk security threat. Existing side channels can be classified into two categories depending on the nature of the leak. The first category

includes software side channels that exist in the device and are created due to hardware or firmware weaknesses. Emanation side channels constitute the second category that is created due to physical phenomena that divert information from its original path to reach an undesired path. Emanation side channels can have different forms: electromagnetic, optical, and electrical. As this thesis deals in its fourth chapter with power line signal leakage through LED domestic lighting, the focus will be on emanation side channel only. This section presents the different kinds of security attacks, the existing physical propagation side channels, and the different countermeasures that can be taken to improve the security.

2.4.1 Class of attacks

Attacks can be classified according to two main criteria: active or passive and intentional or unintentional, which can be distinguished as follows: [14]

- Active/passive: An active attack is performed by transmitting a carrier signal from an active system to a specific device in order to disrupt its normal functions, such as inducing computational errors to force the device to behave unconventionally or force the device to leak a signal by emitting a wave capable of modulating a secure signal to facilitate its leak. Contrariwise, passive attacks are executed in order to only eavesdrop on the signal without modifying it;

- Intentional/unintentional: The unintentional leakage is emitted through naturally existing side channels like electromagnetic radiations through a powerline channel transmitting PLC signals. In contrast, attackers can access a target device to force it to leak. This kind of attack usually happens in an air-gapped channel where this is the only way to exfiltrate data. The intentional attack is studied in [33] in order to exfiltrate data from an isolated computer by installing software capable of transmitting the information via the electric cable which supplies the target computer.

2.4.2 Class of side-channel

Emanation side channels can be distinguished into electromagnetic and non-electromagnetic channels.

2.4.2.1 Electromagnetic channels

The electronic devices may be the initial sources of electromagnetic side channels. The signals can easily travel the side channel as it is usually used as a legitimate communication path. The side-channels may be generated due to different origins. The main three origins of this type of channel can be classified as following (see fig. 2.13) [14]:

- Illumination: In this case, the attacker intentionally transmits an electromagnetic beam towards the target device. This beam can be considered as a side-channel carrier enforcing the information leak through electromagnetic means. The attacker is always listening to the side channel to receive back the radio beam that carries the information;
- Mixing: The difference between the mixing and the illumination case is that in the mixing case, the radio beam comes from a legitimate source and not from the attacker;
- Radiation: This case occurs when an electric current induces an electromagnetic field as it passes through an electronic device. This field modulates the information signal crossing the device leading it to leak;
- Coupling: It is similar to the radiation case. The only difference is that the signal propagates at the vicinity of a conductor and not in the air.

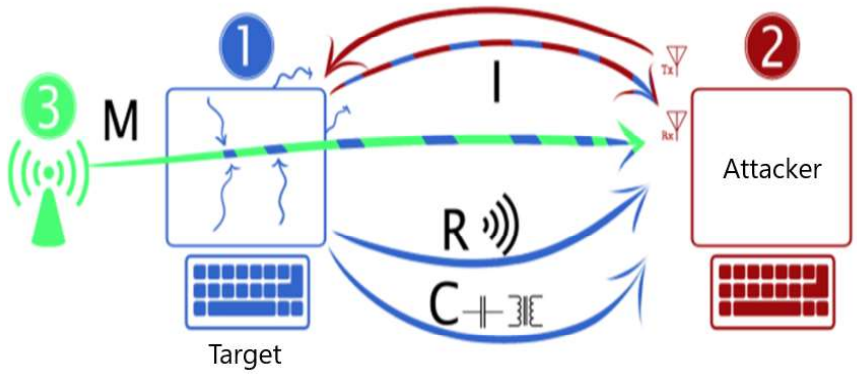


Figure 2.13: Electromagnetic side channels [14].

2.4.2.2 Non-electromagnetic channels

There are 3 types of non-electromagnetic physical channels that can also be considered a security threats (see fig. 2.14):

- Powerline: Electrical cables supplying a communication system can be considered as a side-channel. Whichever component of the system consumes the most energy, its trace will prevail and dominate the traces of the other components, making their detection more complex. It was revealed in [22], that a letter typed on the keyboard can be recognized by measuring the energy consumed by the keyboard during a key press and the consumption of other components. In [90], a method for exfiltrating data from Universal Serial Bus (USB) cable using the power supply provided by the USB

cable. It have been proven also the possibility to eavesdrop on cryptography devices by analyzing its power consumption. In fact, there are several algorithms that help to make power consumption analyses like simple power analyses, differential power analysis, correlation power analysis, etc.;

- Sound: the mechanical components present inside a communication device can generate another type of emanation that can be exploited to collect data which is the sound. In addition to mechanical components, electronic components can also create acoustic noise that is highly correlated to the electrical signal that caused it, and subsequently the information signal. The main difficulty in sound channel attacks is that the attacker system should be trained before to be able to identify signals. An acoustic side channel attack on a printer was demonstrated in [5]. The attacker recovered up to 72% of the printed words using a record of the sound that the printer makes when it was processing an English text. In [1], it was shown to detect typed letters on a PC keyboard using the sound generated by each key-press. A neural network was used to classify the sound of each key when it is clicked;

- Light: The last studied information leakage channel is the light. This kind of leakage can have different sources. It can be attained by exploiting the surface of a computer screen using a telescope or by using the screen's reflection on eyeglasses, teapots, and even user eyes. Moreover, LED is another source of side-channel. In fact, LEDs are used in every electronic device that requires a visible indicator. In some network equipment, the LED flashes at the same rate as the transmitted information, indicating a strong correlation between flash and the transmitted data. In 2002, an eavesdropping technique was demonstrated to remotely read cathode ray tube. screens. It is shown that the intensity of the light emitted by the screen in the time domain is equal to the convolution of the video displayed on this screen and the impulse response of the phosphor. In [6] more modern screens are used to check the possibility of data leakage through them. In addition, this study confirms the possibility of correctly recovering screen images using their reflections on metal or plastic surfaces. Later this work is extended to incorporate the reflections on walls and clothing as well[4]. The authors in [63], find that some LEDs used in some equipment are directly connected to the data bus, which facilitates full data recovery in the optical domain. In 2017, a successful exfiltration of data was achieved from an isolated computer via the small hard drive LEDs[35]. In the following year, a lack of security was found in an Air-Gapped network. It is shown the possibility of exfiltrating data via the LED present on the routers [34].

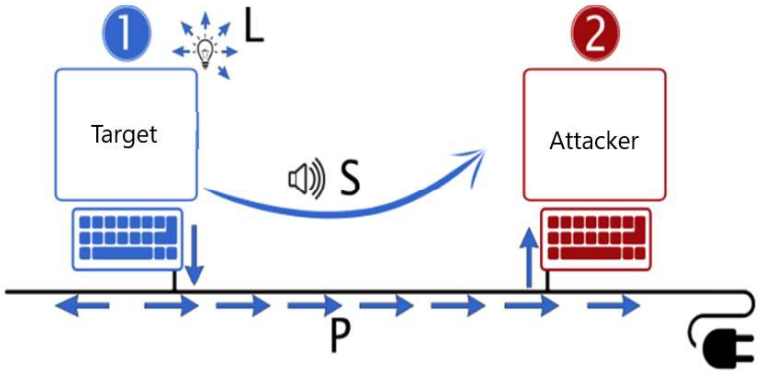


Figure 2.14: Non Electromagnetic side channels[14].

2.4.3 Countermeasures

The National Security Agency (NSA) developed the TEMPEST (Telecommunications and Electrical Machinery Protected from Emanations Security) specification to address the risk of unintentional emanations. TEMPEST first tries to act as an attacker to see how information can be intercepted and secondly tries to develop a protection solution to prevent this studied attack. After detecting the origin of a leak, the appropriate countermeasures can be chosen from the method proposed in TEMPEST or from the classic EMC method in the case of electromagnetic emanation. In this part, the main countermeasures are listed explaining their effectiveness and shortcomings in certain scenarios[74]:

1. Zoning: The NSA proposed zoning to measure the maximum space area where the emanation of a device containing sensitive information remains detectable to keep it completely empty. This recommendation considers that the leaked signal cannot propagate for long distances. However, the generalization of this idea was dismissed after demonstrating that some side channels can transmit the signal to very long ranges [2]. In contrast, when the leaked information is an acoustic signal, zoning can be a very important solution. In fact, these signals cannot travel long distances and keeping any equipment at a sufficient distance from the sensitive device can overcome this type of attack;

2. Component Shielding: In order to reduce electromagnetic emanation, a conductive or magnetic shield is used to isolate the security-sensitive device[2]. However, in some cases, the presence of shielding can complicate the use of the device. For example, if the device that should be protected is a screen or a touch screen, the presence of a metallic shield will make the usage of this screen impossible. Hence, in [103], it was suggested to

use a conductive mesh allowing the user to see the screen. Moreover, a thick polarizing filter that is able to reduce the electrical coupling between the shield and the screen without obstructing the legitimate user from using it is introduced;

3. Facility Shielding: This method is best suited for high-security protection. Instead of using a small shield for each device, which is very costly, a single installation shield having a very large volume can be used, making it possible to house several devices therein [2, 14];

4. PCB and Equipment Rack Designing: when designing printed circuits, it is always necessary to solve the emanations of each stage separately by adopting grounding, bonding, shielding, filtering, and insulation [2];

5. Jamming: When it is difficult to reduce emanation and prevent leakage, jamming can be one of the best solutions. This method is based on covering the leaks by noisy signals that operates in the same frequency-band [14]. Jamming can be used also in the case of non-electromagnetic emanation. For example, in the case of optical emanation, a natural jamming system which is sunlight can be used [6]. Additionally, sound leaks can also be jammed using an acoustic white noise source near the sensitive device [1].

Countermeasures are developed to reduce the security risks of side channels. However, when applying one of the protections listed above, it is necessary to properly adapt it to the communication device so as not to disturb its proper operation.

2.5 Physical layer security from an information theoretic perspective

In broadcast communication systems, the information confidentiality can be threatened as the channels are shared by the network users. Traditionally to ensure network security, the upper layers of the network are employed to apply different cryptography techniques [37]. In contrast, the physical layer security exploits the randomness behavior of the physical channel witch is due to multipath propagation and unpredictable fluctuations in the signal strength, Doppler and delay domains [78]. The cryptography techniques consider that the attacker has a limited computational resources that makes it unable decode the encrypted message. Contrariwise, the physical layer security assumes that the attacker has unlimited resources which implies to ensure that no information is leaked to him [87]. In fact, physical layer security is not a new concept. It dates back to 1975 when Wyner introduced the wiretap system model [101]. Wyner's concept was based on Shannon's original work founded on the basis of information theory [87]. It starts to get more attention in recent years as researchers are intending the application of quantum computers with high-speed computing power, which

can reduce the efficiency of cryptography. Hence, an overview about the physical layer security is provided in this section. In section this section, the concept of wiretap channel is introduced. the main wiretap models are also listed and explained. moreover, this section provides the methods used to assess the secrecy performance of the network. Finally, the approaches that can be used to enhance the physical layer security are presented.

2.5.1 Wiretap channel models

A communication system is represented in fig. 2.15 where Alice wants to send a private message to Bob while keeping it perfectly secrete from Eve. The channel separating Alice from Eve is called a wiretap channel. The wiretap channel has three main configurations:

- The first configuration is offered by Wyner [101]. He considers that Eve receives a noisier and more degraded version of the information than that received by Bob. This means that Bob receives the signal transmitted via channel 1. However, Eve receives the signal which is additionally conveyed via channel 2. Thus, this model is later referred to as a degraded wiretap channel (see fig. 2.16a);

- The second configuration is proposed by Csizàr and Körner [16]. It assumes that the legitimate and the non-legitimate channels are independent and Eve may receive the information in the same quality as Bob. As can be seen in fig. 2.16b, this model is very close to a broadcast scenario that can be suitable in the case of wireless, PLC, and VLC networks. In this case, the non-legitimate channel is called a non-degraded wiretap channel;

- The last configuration is called the keyhole channel [12, 78]. In this case, the legitimate and non-legitimate channels start from the same pinhole (k) which is the output of an ideal channel (channel 0) (see fig. 2.16c). This model corresponds to a tree configuration or bus structure which can also be common in PLC networks.

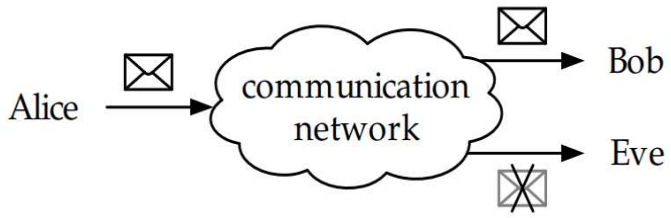


Figure 2.15: Communication system with a transmitter (Alice), a legitimate receiver (Bob) and an eavesdropper (Eve) [52].

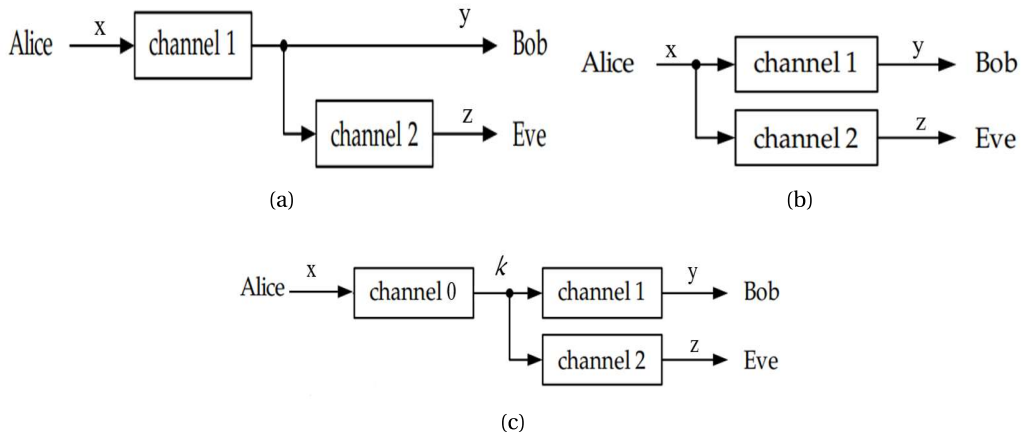


Figure 2.16: The wiretap channel configurations. (a) Wyner [52]. (b) Csizàr and Körner [52]. (c) Keyhole

2.5.2 Secrecy performance evaluation for physical layer security

From an information-theoretic point of view, the signal x transmitted by Alice and the signal y received by Bob and z received by Eve are modeled as random variables. Alice transmits a message from the message set $S = \{1,2,...M\}$ with $M = 2^{nR_s}$ over n channel uses while ensuring the information-theoretic security. R_s denotes the secrecy rate in bit per channel use. The secret message s is encoded at the transmitter into a codeword $x^{(n)}$. The received codeword $y^{(n)}$ at Bob is decoded into a message S_B taking the channel state information at the receiver into account. An (M,n) code includes the message set S, the encoding and the decoding functions. Eve eavesdrops the signal $z^{(n)}$ at the output of the non-legitimate channel. The secrecy is assessed through the uncertainty of Eve about the message s sent by Alice under the condition that Eve receives $z^{(n)}$. The measure of the uncertainty is called the equivocation rate which is expressed by the following expression [52, 31]:

$$R_e = \frac{1}{n} H(s|z^{(n)}) \tag{2.11}$$

where $H(\cdot)$ denotes the entropy. We aim to obtain a secure transmission with a achievable secrecy rate R_s. A secrecy rate R_s is said to be achievable over the wiretap channel if for any $\epsilon > 0$, there exists a sequence $(2^{nR_s}, n)$ code such that for any $n \geq n(\epsilon)$, the average decoding error probability becomes arbitrary small[31]. The equivocation rate fulfilled the following security constraint[52, 78] :

$$R_e \geq R_s - \epsilon \tag{2.12}$$

A perfect secrecy means that ϵ should be equal to zero. Hence, the secrecy capacity is the maximum secrecy rate R_s such that the secrecy of the transmitted data is ensured. In other

words, it is the maximum secrecy rate that the equivocation rate that guarantee $R_e = R_s$. For a general none degraded Gaussian wiretap channel, the secrecy capacity is given by [52]:

$$C_s = \max_{f_x \in F} [I(x;y) - I(x;z)]^+ \tag{2.13}$$

where F is the set of all the probability density functions (PDF) at the channel input under power constraint at the transmitter, f_x is the PDF of the channel input x, $[m]^+$ is equal $\max(m,0)$ which means if m is negative then $[m]^+ = 0$, $I(X;Y)$ and $I(X;Z)$ are the mutual information terms that are convex in f_x. This will allow us to formulate the lower bound R_s for the secrecy capacity C_S [52]:

$$R_s = [\max_{f_x \in F} [I(x;y)] - \max_{f_x \in F} [I(x;z)]]^+ \tag{2.14}$$

The secrecy rate R_s is defined as the difference of the channel capacities from Alice to Bob and from Alice to Eve. This lower bound R_s is often used because it allows a simple calculation of the secrecy capacity due to the knowledge of how to maximize the mutual information terms [52].

2.5.3 Physical layer security enhancement

To limit physical layer attacks, several countermeasures can be adopted. This section lists some solutions that help improve the physical layer security based on information theory.

2.5.3.1 Artificial-Noise-Aided Security

In this solution, the transmitter Alice generates specific interfering signals also called artificial noise [111]. This signal only disturbs the eavesdropper Eve as the artificial noise must already be known to the legitimate user Bob so that he can separate it easily from the useful signal. This technique reduces the wiretap channel capacity while keeping the capacity of the legitimate channel unaffected, thereby increasing the privacy capacity [111, 108]. Although this technique seems very effective in improving the security of the physical layer, however, it is not power efficient as the transmitter needs additional power to generate the artificial noise [108].

2.5.3.2 Security-Oriented Beamforming Techniques

This solution allows Alice to transmit the information signal in only the direction of the legitimate receiver so the the signal received by Eve becomes very week [104]. Hence, Bob's received power becomes much higher than that of Eve leading to an increase in the secrecy capacity. This technique can be applied in wireless networks like VLC. Furthermore, The beamforming technique can be combined with the artificial noise techniques to further enhance the physical layer security [111].

2.5.3.3 Diversity-Assisted Security Approaches

This technique can be also adopted to enhance the physical layer security. Contrariwise to artificial noise technique, this method is capable to improve the security without consuming additional power [111]. In this section three diversity based approaches are distinguished:

- Multi-antenna-assisted transmission diversity has proven effective in improving physical layer security [106]. Indeed, several antennas should be present on the transmitter side. The transmitter chooses to transmit the information signal using the antenna that guarantees the highest secrecy capacity. It should be noted that computing the secrecy capacity requires knowledge of the channel state information of the legitimate and wiretap channels. However, this technique can also be used in the case where the state information of the eavesdropping channel is unknown to the transmitter. This can be done by simply choosing the antenna which provides the optimum capacity of the legitimate channel while keeping the capacity of the wiretap channel unchanged. Thus, this will also increase the security capability [111];

- Multi-user diversity can also be seen as a way to improve physical layer security [111, 110]. In the case where a transmitter serves multiple users, a multiple access mechanism must be followed. Considering the case of orthogonal frequency division multiple access in a cellular network, the user is allowed to access a sub-band and start its signal transmission using a multiuser schedule [110]. However, since the signal is broadcast in nature, the eavesdropper can easily intercept the transmitted signal. Therefore, in the diversity approach, scheduling must be designed to minimize the capacity of the wiretap channel and maximize that of the legitimate channel if their information states are available to the transmitter. In the absence of wiretap channel state information, the schedule should be designed to maximize the capacity of the legitimate channel while keeping the wiretap channel capacity intact .

- Cooperative diversity can also protect the communication system from eavesdropping attacks [111]. This technique depends on the presence of several relays between the transmitter and the receiver. The sender elects to send the information signal to the legitimate receiver via the relay that provides the highest secrecy capacity or the highest legitimate channel capability [86].

2.5.4 Physical-Layer Secret Key Generation

A secret key is generated by exploiting the physical layer characteristics of the legitimate channel [111]. This technique can be adopted for reciprocal channels. More precisely, the channel separating Alice from bob has the same characteristics and values as the channel separating Bob from Alice. Thus, using classical channel estimation methods, they can exploit

the state information of their estimated channels to generate a secret key while keeping it completely secret from Eve because the channels separating Eve from Bob and Alice are not correlated to the legitimate channel [84].

2.6 Conclusion

This chapter provides a brief overview of PLC and VLC systems. It shows how these ancient ideas have developed over the years until having international standards and regulations that unify and organize their use worldwide. In this chapter, almost all existing standards for PLC and VLC systems are reported highlighting the physical layer parameters of each standard. PLC and VLC channel characteristics are also detailed showing their different modeling approaches. In addition, the different types of noise that can disturb the signal are listed for both the PLC system and the VLC system. Moreover, this chapter emphasizes on the different techniques used in lighting industries to generate white light and shows their advantages and drawbacks if adopted for VLC.

An investigation about the integration of PLC and VLC systems is made. The AF and DF relaying techniques are presented and compared in terms of complexity, efficiency and performance. The full system channel model is addressed along with a comparison between the frequency response of the PLC only channel and the hybrid PLC-VLC channel indicating the LED attenuation effect of the hybrid channel.

Another subject is introduced also in this chapter which is the side-channel attack. Literally, it is quick snapshot about the possible attacks that can be divided considering two main criteria: active/passive and intentional/unintentional. Electromagnetic and non-electromagnetic side channels are also discussed in addition to the possible countermeasures that can be taken to prevent these kind of attacks.

Eventually, the physical layer security based on the information-theoretic context is presented. The wiretap channel is explained in addition to its main types: the degraded wiretap channel, the non-degraded wiretap channel, and the keyhole channel. The equivocation rate, the secrecy rate, and the secrecy capacity metrics are introduced in order to how the secrecy performance in a communication system can be evaluated. Finally, the primary methods used to improve physical layer security are listed and explained.

With a comprehensive overview of PLC, VLC, their combination, and side-channel attacks, it will be easy now to understand the importance of this thesis contributions that fill the gaps found in the literature. It has been shown that the VLC channel frequency response can be modeled by multiplying the LED frequency responses by the channel frequency response. However, to the knowledge of the author, there is no explicit expression allowing to precisely model the VLC channel and taking into account the E/O characteristics of the LED and the O/E characteristics of the photodiode. Moreover, even if several studies focus on the integration

of PLC-VLC systems, the number of real test benches used to measure the performance of the broadband PLC-VLC system is quite limited. Besides, all the studies aim to optimize the integration of PLC-VLC systems. But no studies are showing the optical side-channel security threats for powerline systems, although LED bulbs and power lines are naturally connected. Finally, the physical layer security of a PLC network in the presence of a non-legitimate VLC system connected to the same powerline network has never been covered. All the fore-mentioned shortcomings are addressed in this thesis.

Chapter 3

Broadband PLC-VLC system integration

PLC has been extensively studied by researchers over the past few years. NB-PLC and BB-PLC have been standardized to offer a reliable communication system for emerging applications such as the Internet of Things in the case of NB-PLC and the in-home communication network in the case of BB-PLC. However, mobility is a fundamental characteristic of indoor communication systems which is unfortunately not available in PLC. Integrating VLC with PLC comes as one of the simplest solutions to provide an indoor wireless communication experience to users, thus completing the missing feature in PLC.

The idea behind this chapter is to create a simple AF PLC-VLC system using commercial PLC modems based on the existing BB-PLC standard (HPAV) and power LEDs dedicated to lighting without applying any modifications to the signal before crossing the VLC system. Implementing a VLC system capable of transmitting HPAV signals requires a careful choice of VLC system components. Since LEDs are the most critical components of the VLC system, a thorough analysis should be done considering their transmission bandwidth, impedance, electrical to optical conversions, etc. Then, the performance of the proposed PLC-VLC system should be evaluated to determine its ability to be employed for large-scale applications.

In this chapter, we evaluate the characteristics of red, green, and blue LEDs in terms of modulation bandwidth and frequency impedance. In addition, a LED equivalent electric circuit model is proposed based on the frequency response and impedance measurements. This chapter also presents a meticulous VLC channel model taking into account the electrical, optical, and frequency behavior of the system components. The PLC-VLC system setup is also described showing the parameters of the different components. Moreover, an online UDP packet transmission is carried out using our PLC-VLC testbed to assess it performance. Finally, a theoretical study is carried out to dimension the proposed PLC-VLC system for typical indoor applications.

3.1 VLC subsystem experimental and theoretical analysis

The LED is the transducer that converts the PLC electrical signal into an optical signal. As discussed in chapter 2, the LED has a limited frequency response which is narrower when a blue LED and a phosphor layer is used to generate white light. Thus, in section 3.1.1, the modulation bandwidth of each LED of an RGB module is measured in order to find the one that has the largest bandwidth that matches the HPAV band. The frequency impedance measurement results of each LED are also depicted in section 3.1.1. A LED equivalent circuit model is worked out in section 3.1.2 which can help when designing an efficient driver or an equalizer to extend the LED bandwidth. Finally, section 3.1.3 presents an explicit expression of the VLC channel allowing a direct calculation of the received signal as a function of the transmitted one.

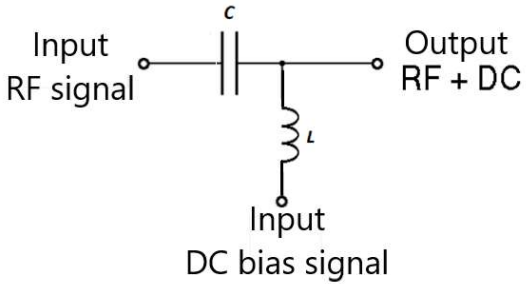
3.1.1 LED frequency characteristics

As the phosphor layer reduces the LED bandwidth, we decided to use an RGB LED module dedicated to lighting called LUXEON MultiColor LED Module 2.5 W [65]. This module has a red, green, and blue LEDs in addition to a white LED which can be used to adjust the temperature of the resulting white light. The bandwidth and the frequency impedance of the three LEDs are measured using a network analyzer (Hewlett Packard 4195A) with an impedance test adapter (Hewlett Packard 41951-69001) for the impedance measurements. Note that these measurements are made when the LEDs are biased by their typical current.

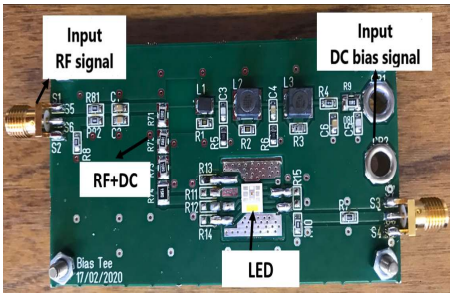
3.1.1.1 LED frequency response

To be able to measure the bandwidth of the LED, a bias tee circuit must be used to simultaneously power the LED and inject the signal that we want to transmit from the network analyzer. Indeed, a bias tee is a three-port network used to bias the device using the low-frequency port and to pass the high-frequency signal through the second port. The third or the combo port (output) is connected to the LED and receives both bias signals and high-frequency signals (see fig. 3.1a). We designed the bias tee with a bandwidth of 100 MHz (fig. 3.1b), which means that its bandwidth is large enough not to affect the measurement results we are going to see later (see section A.1 in the appendix).

As shown in fig. 3.2, the red LED when biased at 120 mA has a wide modulation bandwidth with a −3 dB cutoff frequency of 20 MHz. However, the green and blue LEDs when biased at 120 mA have approximately the same response with a cutoff frequency of 6 MHz. It can also be noticed that the LED response slowly decreases as a first order low pass filter. For example, the red LED has an attenuation of −3.8 dB at 30 MHz. This slow attenuation behavior with increasing frequency can be exploited to transmit a signal having a modulation bandwidth larger than the measured LED modulation bandwidth. As the red LED has the greatest cutoff



(a)



(b)

Figure 3.1: Bias Tee. (a) explanatory scheme, (b) our manufactured circuit.

frequency, we decide to be used in our PLC-VLC testbed.

3.1.1.2 LED frequency impedance

Although Xicong Li [60] has investigated the frequency impedance of power LED with a typical bias current greater than 100 mA, the measurements are carried out with a much lower polarization current (35 mA). Hence, in this section, the measurements are performed when the LEDs are biased with their typical current (120 mA) in order to accurately examine their behavior when they are used in real applications.

Fig. 3.3 shows the frequency impedance of the red, green, and blue LED of the RGB Luxeon module. It can be noticed that the resistor behavior dominates in the low-frequency domain. The impedance can be considered flat for frequencies under 5 MHz for the green and blue LEDs and under 20 MHz in the case of the red LED. Then the capacitor effect starts to appear as the impedance starts decreasing with increasing frequency. Finally, for frequencies above 60 MHz, the impedance begins increasing with the frequency which means that an inductive behavior starts to appears [60].

3.1.2 LED equivalent circuit model

As fig. 3.4 shows, the LED can be modeled by a parallel RC circuit with a series resistor. The resistor (r_d) is the differential resistance of the intrinsic p-n junction of the LED. The capacitor

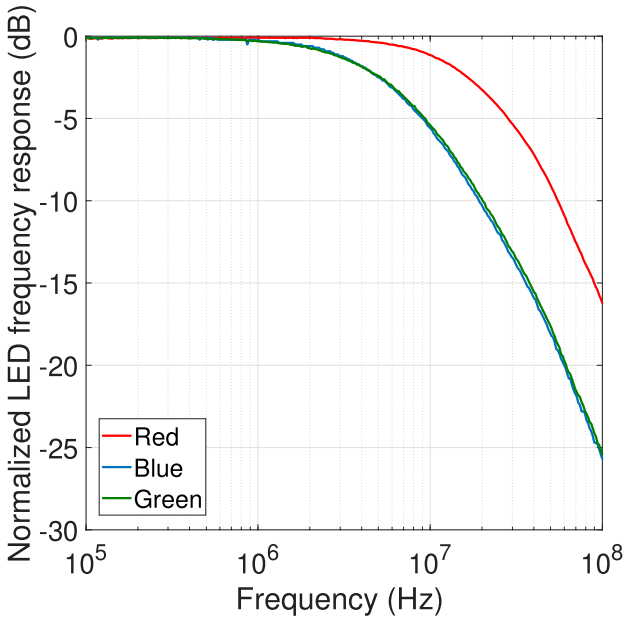
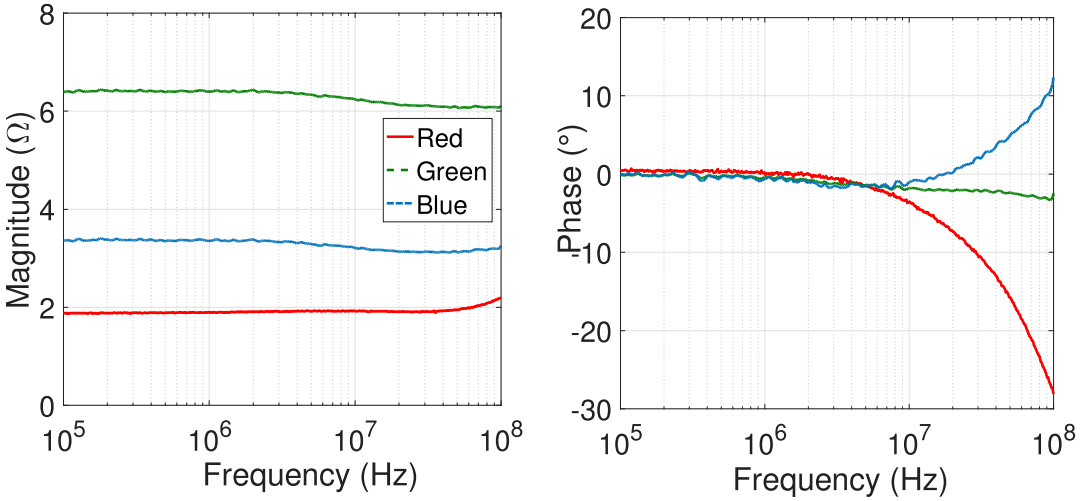


Figure 3.2: Red, green, and blue LED frequency responses.



(a) (b)

Figure 3.3: Frequency impedance of the red, green, and blue LED of luxeon RGB module. (a) Magnitudes, (b) phases.

is the sum of the diffusion capacitance (C_d) and the charge space capacitance (C_{sc}). The space of charge capacitor is a parasitic capacitance that occurs due to carrier injection delay in the p-n junction. In addition, the current crowding under the electrodes and the ohmic contacts inside a LED chip create a series resistance effect with the RC model (R_s). Finally, the bonding wire can be modeled as a simple inductor in series with the circuit model LEDs (L).

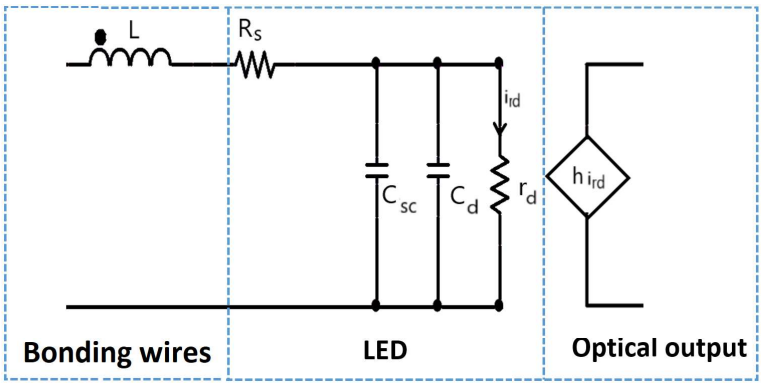


Figure 3.4: Simplified equivalent circuit model for a LED.

3.1.2.1 The process of estimating the value of each component

This section estimates the value of each components based on measurments obtained in the two previous sections (section 3.1.1 and 3.1.2). The circuit value is estimated by comparing the measured LED frequency response and the frequency impedance depicted in section 3.1.1 to their expressions calculated based on the equivalent circuit model described in section 3.1.2. Thus, since the LED frequency response is the ratio of the LED optical power to LED injected current and the relationship between the optical power and the current passing through r_d can be considered linear with a gain h, the frequency response of the LED can be expressed as follows:

$$H_e = \frac{h}{1 + jcr_d\omega} \tag{3.1}$$

where c is the sum of c_d and c_{sc}, and ω is the angular frequency (rad/s). It should be noted that the measured LED impedances are very small compared to that of our bias tee (50 Ω) which allows us to use the expression (3.1) while ensuring accurate results. According to the model shown in fig 3.4, the total LED impedance can be written as:

$$Z = jL\omega + R_s + \frac{r_d}{1 + jcr_d\omega} \tag{3.2}$$

The real part of the impedance can be expressed as:

$$R = R_s + \frac{r_d}{1 + (cr_d\omega)^2} \tag{3.3}$$

an the imaginary part:

$$X = L\omega - \frac{c{r_d}^2\omega}{1+(cr_d\omega)^2} \tag{3.4}$$

After finding the LED frequency response and the impedance expressions, the values of each component can be estimated according to the following procedure:

1. At high frequency, R tends to be equal to R_s. By using the real part of the measured impedance at high frequency, the value of R_s can be easily estimated;

2. At low frequency, R is approximately equal to $R_s + r_d$. Knowing the value of R_s, r_d can be deduced from the real part of the measured impedance at low frequency;

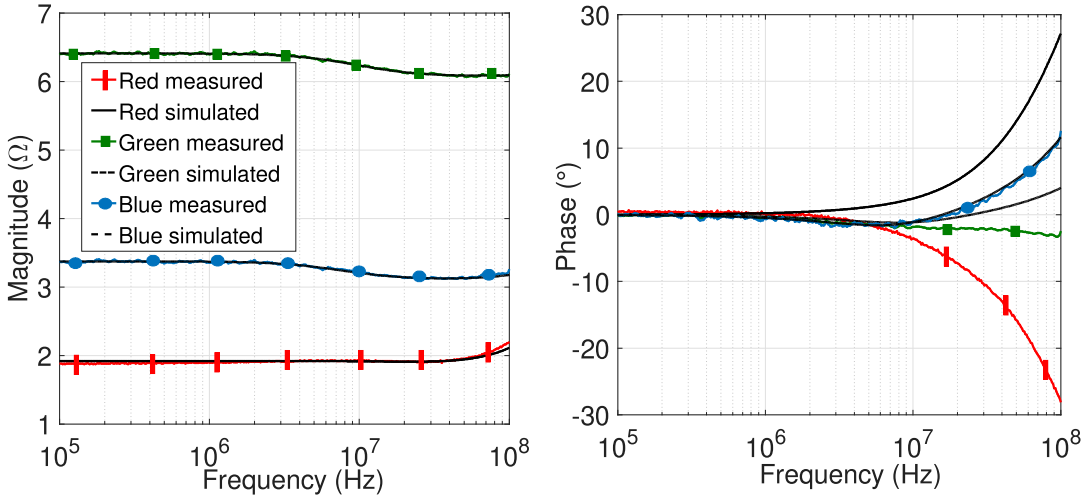
3. The -3 dB cutoff frequency of the LED frequency response is equal to $\frac{1}{2\pi r_d c}$. Using the LED frequency response measurement results and the already estimated value of r_d, c can be inferred;

4. L is deducted from X at high frequency because X tends to be equal to $L\omega - \frac{1}{c\omega}$ and c is estimated in the previous step.

3.1.2.2 Results

Fig. 3.5 compares the modeled and the measured frequency impedances for the three existing LEDs in the RGB module. As shown in fig. 3.5a, the magnitude of the modeled impedance fits perfectly with that measured for the red, green, and blue LEDs in the entire measured frequency band (500 kHz-100 MHz). Also, the modeled phase impedance of the blue LED matches the measured one. However, the modeled phases of the red and green LED impedances do not correspond to those measured, particularly for frequencies above 2 MHz (see fig. 3.5b). This discrepancy is due to the existence of many parasitic elements which are not considered in this model. Additional studies should be carried out in the future in order to extend this model to take into account the rest of the parasitic elements. The estimated circuits parameters of the red, green, and blue LEDs when they are biased by a current of 120 mA are listed in table 3.1.

To further verify the accuracy of the proposed model, a comparison between the measured (see section 3.1.1.1) and modeled LED frequency responses for red, green, and blue LEDs is performed. As seen in fig. 3.6, there is a good matching between the measured frequency response and the simulated one for the three LEDs, which also proves that the monochromatic frequency response of LEDs can be modeled as a first order low-pass filter, see § 2.2.3.1 in chapter 2.



(a) (b)

Figure 3.5: Comparison between the modeled and the measured frequency impedance of the red, green, and blue LED. (a) Magnitude, (b) phases.

Table 3.1: Estimated values of the equivalent circuits components of the red, green, and blue LEDs.

LED color	L (nH)	R_s (Ω)	r_d (Ω)	c_d (nF)
Red	15.5	1.88	0.04	162
Green	7.3	6.07	0.34	50
Blue	10.5	3.11	0.26	80

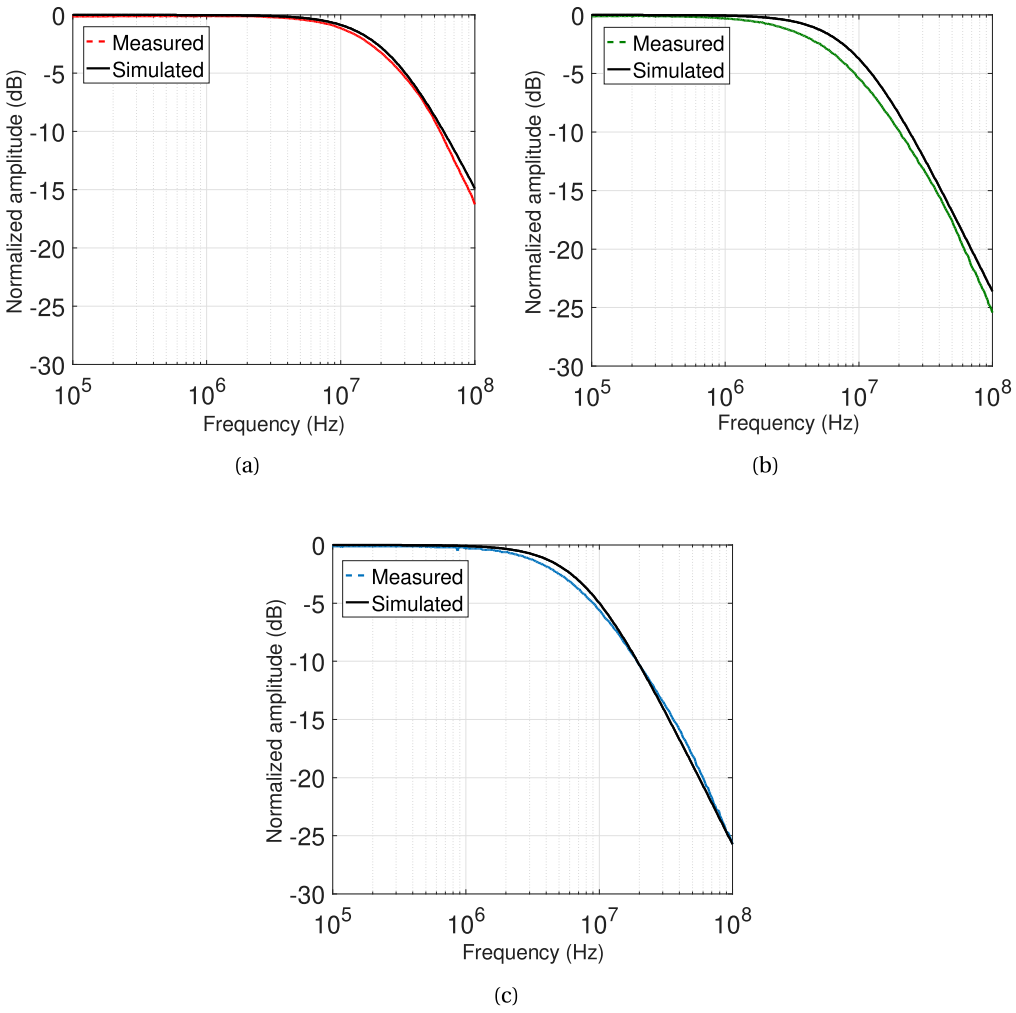


Figure 3.6: Comparison between the modeled and the measured LED frequency response. (a) Red LED, (b) green LED, (c) blue LED.

3.1.3 VLC channel modeling taking into account the optical, electrical and frequency behavior

As seen in section 3.1.1, the LED frequency response has an explicit influence on the bandwidth of the VLC channel, hence we need to take it into account when modeling the LED. Moreover, in order to obtain a model which faithfully copies the real behavior of the VLC channel, additional parameters must be considered in the model such as E/O and O/E conversions which have non-linear forms. In this section, a VLC channel model expressing the relationship between the current flowing through the LED and the voltage at the output of the optical receiver is proposed.

3.1.3.1 Proposed model

The VLC transmitter consists of a bias tee responsible for biasing and transmitting the communication signal to the LED as an electrical current. The LED transforms the electric current into an optical power that travels through the medium. The photodiode (BPW34) receives and converts the optical signal to the electrical aspect (current). The trans-impedance amplifier (TIA) amplifies and transforms the photo-generated electric current into an electric voltage. The photodiode, and the TIA constitutes the components of the VLC receiver. At this point, the data will be demodulated and decoded (see fig. 3.7).

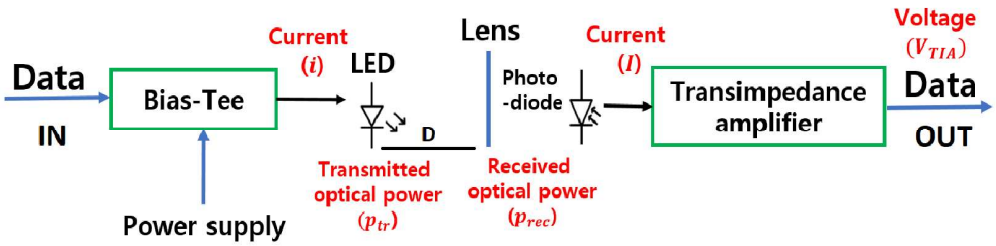


Figure 3.7: VLC testbed.

The LED's E/O conversion is calculated based on the information and curves usually given in the LED datasheet (Luxeon multicolor 2.5 W [65]). However, in the used RGB module datasheet, the typical transmitted power density at the LED's dominant wavelength P is not given explicitly even though all the given curves are normalized to this value. Nevertheless, it can be calculated using the luminous flux expression φ [50] as follows:

$$P = \frac{\varphi}{V_{max} \int_{380}^{780} v(\lambda) p(\lambda)\, d\lambda} \tag{3.5}$$

where $v(\lambda)$ is normalized to its maximum eye efficacy V_{max} (V_{max} = 683 lm/W at λ = 555 nm) and $p(\lambda)$ is the optical power density normalized to P, which is given with the value of φ in the LED datasheet. To be able to calculate the integral, $p(\lambda)$ and $v(\lambda)$ are modeled by the sum

of two Gaussian functions as shown in fig. 3.8 [107]:

$$p(\lambda) = ae^{-(\frac{\lambda-b}{c})^2} + de^{-(\frac{\lambda-e}{f})^2} \tag{3.6}$$

and

$$v(\lambda) = a_1 e^{-(\frac{\lambda-b_1}{c_1})^2} + d_1 e^{-(\frac{\lambda-e_1}{f_1})^2} \tag{3.7}$$

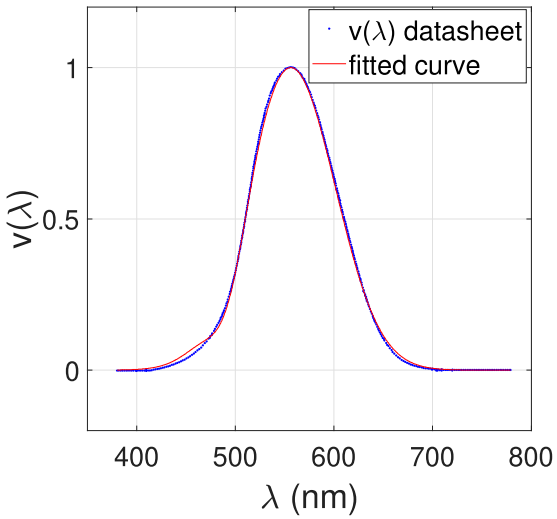


Figure 3.8: The normalized eye efficacy v(λ).

Moving to the relationship between the light output (L) and the current crossing the LED (i), it is also given in the datasheet normalized to its typical and it could be expressed by a polynomial function as following:

$$L(i) = k_1 i^3 + k_2 i^2 + k_3 i + k_4 \tag{3.8}$$

So, the LED transmitted power density in function of wavelength (λ) at a determined current (i) can be described by:

$$P_{tr}(\lambda, i) = Pp(\lambda)L(i) \tag{3.9}$$

However, this transmitted power is affected by the total channel attenuation and the LED frequency response described by (2.8) in chapter 2:

$$H_v = \frac{AG(m+1)\cos^m(\phi_i)\cos(\psi_i)}{2\pi D^2} \frac{1}{1+j\frac{f}{f_c}}, \tag{3.10}$$

where m is the Lambertian index, A is the active area of the photodiode, ϕ and ψ are the angles of irradiance and incidence respectively, D is the distance between the LED and the photodiode, G is the gain of the lens that concentrates the light to the photodiode and f_c is the

−3 dB cutoff frequency of the LED frequency response. Hence, the received power density is written as follows:

$$p_{rec}(\lambda, i) = P_{tr} H_v \tag{3.11}$$

The photodiode receives the light and generates the photo-current depending on its sensitivity. The following equation shows the current spectral density as a function of the received optical power density:

$$i_P(\lambda, i) = S_{max} s(\lambda) p_{rec}(\lambda, i) \tag{3.12}$$

where S_{max} is the maximum sensitivity of the photodiode, $s(\lambda)$ is the normalized sensitivity given in the photodiode's datasheet. In order to reduce the complexity of calculation in the following steps, we modeled only $s(\lambda)$ in the part of the spectrum where the RGB LEDs radiate, as follows:

$$s(\lambda) = s_1 \lambda^2 + s_2 \lambda + s_3 \tag{3.13}$$

Hence, the overall generated current is the integral of the current density over the all spectrum:

$$I(i) = \int_{380}^{780} i_P(\lambda, i) d\lambda \tag{3.14}$$

The final expression of the generated current is:

$$I(i) = P H_B H_V S_{max} L(i) \sqrt{\pi} \left(ca \left(s_1 \left(\frac{c^2}{2} + b^2 \right) + s_2 b + s_3 \right) + df \left(s_1 \left(\frac{f^2}{2} + e^2 \right) + s_2 e + s_3 \right) \right) \tag{3.15}$$

where H_B is the bias tee frequency attenuation. P, H_V and $L(i)$ are respectively the typical power, the VLC channel, and the light output described in (3.5), (3.10), and (3.8). If an array of N_{LED} identical LEDs is used, the total generated current can be expressed as follows:

$$I_{total}(i) = N_{LED} I(i) \tag{3.16}$$

3.1.3.2 Current measurement setup

In this section, measurements are carried out to validate the proposed model expressed by (3.15). The test bench is set up according to the diagram shown in fig. 3.7. The bias tee presented in section 3.1.1.1 is used to polarize the red LED at 120 mA and to inject a 50 kHz sinusoidal signal of 10 mA using the RF port. The used optical receiver involves a photodiode called BPW34 having an active surface of 7.5 mm^2 and a sensitivity of 0.62 A/W [98] and a TIA with a gain of 50 kΩ. The transmitter and the receiver are aligned and separated by a distance of 13 cm. The bias tee has an attenuation of 0.6 at 50 kHz. As the TIA transforms the photocurrent to a voltage signal, the measured signal at the output of the TIA has a peak amplitude of 10 mV which corresponds to a photo-current of 200 nA.

3.1.4 Results

As figs. 3.9a to 3.9c show, the proposed models of $p(\lambda)$ (3.6), $L(i)$ (3.8) and $s(\lambda)$ (3.13) fit properly the curves of the LED and photodiode datasheets. The improvement brought by this model when it takes into account the optical nonlinearity $L(i)$ and the LED spectral power width $p(\lambda)$ with the spectral sensitivity of the photodiode $s(\lambda)$ is also highlighted. Hence, the maximum generated photocurrent I and the TIA's output voltage V_{TIA} is calculated based on the test-bed parameters described in section 3.1.3.2 for a bias current of 120 mA and a sinusoidal signal of 10 mA at 50 kHz at three different cases:

(i) when all nonlinearities are considered (our proposed model);

(ii) when the light output $L(i)$ is considered linear;

(iii) when the photodiode sensitivity $s(\lambda)$ and $p(\lambda)$ are considered only at the dominant wavelength ($\lambda_{dominant}$ = 625 nm in the case of the LED red).

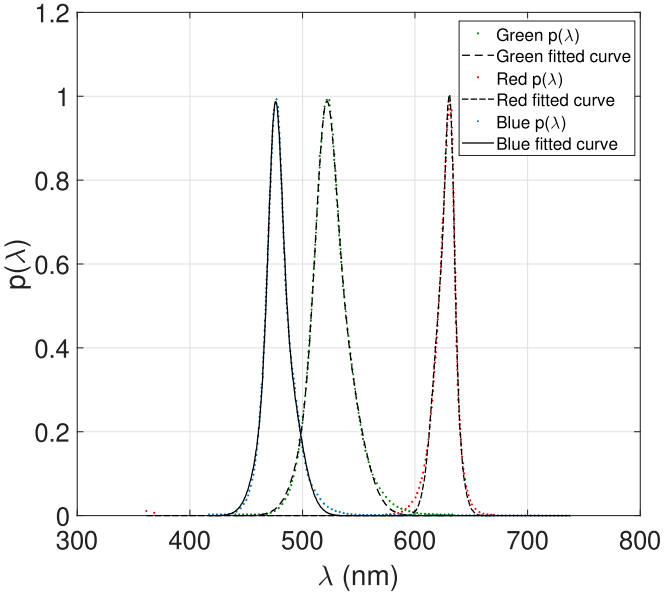
The results in table 3.2 show the precision enhancement in calculation that our model provides in comparison to the results obtained in the last two cases. The calculated V_{TIA} is compared to the measurement (10 mV), resulting in the relative error ERR. It has decreased from 41 % in case *ii*) and 27 % in case *iii*) to 22 % in case *i*). The 22 % error obtained in our model is acceptable regarding the test-bed characteristics. In fact, during measurements, the junction temperature cannot be controlled despite the great influence of the junction temperature on LED characteristics. Especially on the red LED which seems the most affected by the increase in junction temperature [65]. In fact, high power LEDs used for illumination run at high drive current leading to high junction temperature which cause signal power degradation over the time [95]. However, the thermal effect is not treated in this chapter. Thus, this simple expression provides a good estimate of the maximum current amplitude that a photodiode could generate.

Table 3.2: comparison of I and V_{TIA} calculated in 3 different cases: considering all the non-linearities, considering $L(i)$ linear, and considering $s(\lambda)$ and $p(\lambda)$ at the dominant wavelength of the LED.

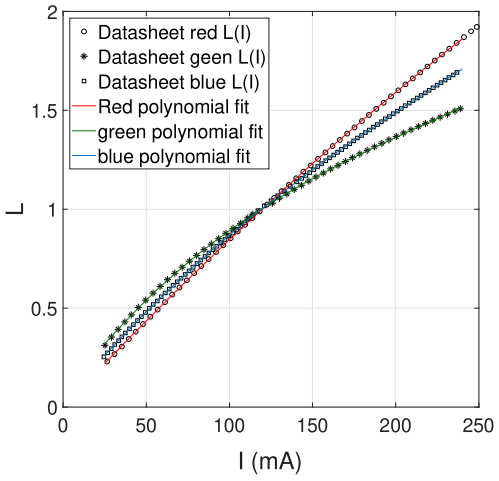
Assumption	I (nA)	V_{TIA} (mV)	ERR(%)
i) proposed model	244	12.2	22
ii) $L(i)$ linear	281	14.1	41
iii) $p(\lambda)$ and $s(\lambda)$ at $\lambda_{dominant}$	254	12.7	27

3.2 PLC-VLC integration

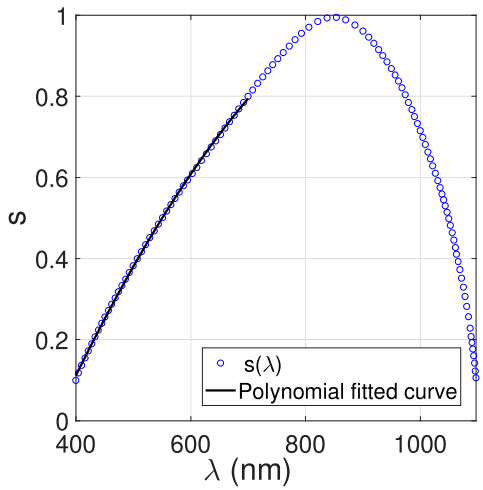
The main objective of this chapter is to test the possibility of transmitting a broadband PLC signal through a power LED without the need to modify the PLC signal and to add too much



(a)



(b)



(c)

Figure 3.9: LED and photodiode datasheet curves models. (a) The spectral power density of red, green, and blue LEDs compared to their modeled curves, (b) the three LEDs' electrical/optical characteristics compared to our polynomial model, (d) spectral sensitivity response of the photodiode compared to our polynomial model.

electronic devices between the PLC and the VLC subsystems. As seen in the previous section, the red LED of the tested RGB module has the largest modulation bandwidth among all the existing LEDs, which is 20 MHz at −3 dB, which may be compatible with the HPAV modulation bandwidth (2 MHz–28 MHz). Therefore, a broadband PLC-VLC system is proposed using commercial HPAV modems and the red LED of a power RGB module. In section 3.2.1, the proposed PLC-VLC system is detailed and the choice of each component is discussed. A brief explanation of the modification made to commercial HPAV modems in order to be able to use them in our system is also given. The performance of the implemented system is evaluated in section 3.2.2. UDP packets are transmitted through our PLC-VLC system. The throughput of the system is measured as a function of the offered load according to the distance between the optical transmitter and the receiver. In addition, a throughput comparison between the PLC and the PLC-VLC system is made as a function of the transmitted power to highlight the effect of the VLC channel attenuation on the PLC system. In section 3.2.3, a theoretical study is carried out to extrapolate the results obtained on our small-scale PLC-VLC testbed to a typical indoor application.

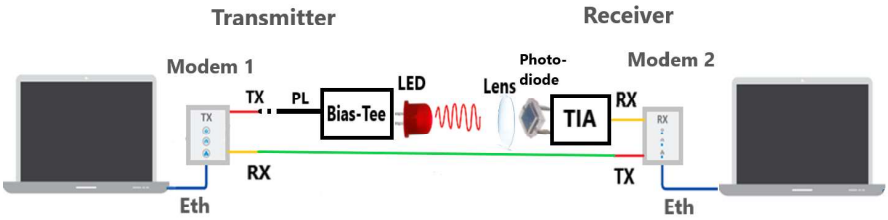
3.2.1 System setup

The PLC subsystem is based on two commercial half-duplex HPAV modems (DLAN 200 AV from Devolo [18]). To be able to use them in our simplex PLC-VLC system, a simple modification is made to separate the transmission part (Tx) from the reception part (Rx). This modification consists of simply removing the coupling transformer present inside each modem. After validating the proper functioning of the modified modems, the implementation of the PLC-VLC system is launched. The signal transmitted by the first PLC modem (modem 1) is injected into the LED via the bias tee as shown in fig. 3.10. Then, the LED retransmits the original PLC signal to the optical receiver consisting of a photodiode and a TIA. In order to perform fast real time decoding and to ensure the continuity of the system, the received optical signal is sent back to the second powerline modem (modem 2), which plays the role of the decoder. The downlink is simply connected using a wire.

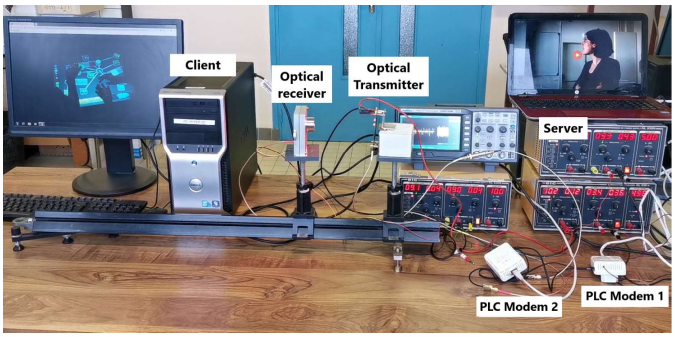
PLC subsystem It consists of two PLC modems having a theoretical bitrate of 200 Mbit/s. However, after measuring the maximum throughput, it is found that the actual throughput is limited to 68 Mbit/s. Moreover, the delivered signal has an amplitude of 8 V peak-peak which correspond to a current of 160 mA at 50 Ω. Since the LED supports a maximum current of 240 mA [65], the signal delivered by the PLC modem can be injected directly into the LED through the bias tee.

VLC subsystem It consists of an optical transmitter and an optical receiver. The optical transmitter is composed of our manufacture bias tee described in section 3.1.1.1 and the

red LED of the tested RGB module [65]. Our manufactured optical receiver consists of a photodiode (SFH2400 [75]) and a TIA that have a bandwidth large enough to not affect the PLC signal. Besides the trans-impedance amplifier circuit, the TIA comprises a high pass filter and a voltage amplifier. The TIA transforms the received optical signal into an electrical voltage. The high pass filter eliminates the DC component obtained by the DC signal used to bias the LED in order to keep only the communication signal. The voltage amplifier further amplifies the recovered signal (see section A.2 in the appendix). It should be mentioned that although our system uses the red led only for communication because, the use of green, blue and white LEDs can be dedicated to generating the desired white color for the indoor lighting. Note that their use is still possible for signal transmission, but they do not increase the transmission bandwidth. The VLC subsystem parameters are listed in table 3.3



(a)



(b)

Figure 3.10: PLC-VLC system testbed.(a) Diagram of PLC-VLC system, (b) real photo of the testbed.

3.2.2 Performance evaluation

In this section, the possibility to directly transmit a HPAV signal through a VLC system is proven by experiments. Fig. 3.11 shows the maximum throughput as a function of the offered load for several distances between the LED and the optical receiver. Obviously, the greatest value of the maximum throughput is reached (between 58 Mbit/s and 68 Mbit/s) for distances

Table 3.3: VLC subsystem parameters.

Index	Value
LED luminous flux	18 lm
Dominant wavelength of the LED	618 nm
LED half intensity beam angle	85 °
Input bias current	120 mA
Bias-tee bandwidth	20 kHz–100 MHz
Photodiode sensitivity	0.44 A/W
Photodiode active area	1 mm^2
TIA total gain	0.2 MΩ
TIA total bandwidth	70 MHz
Distance between the LED and the photodiode	10 – 85 cm
HPAV PLC signal amplitude	10 V peak-peak
HPAV transmission bandwidth	2 – 28 MHz

less than 40 cm. Beyond this distance, the maximum throughput begins to decrease until it reaches 17.06 Mbit/s at a distance of 85 cm. As it can be remarked, the distances seams to be short. In fact, the distances are normal as we are using a single small LED. It should be noted that the PLC topology used in the testbed is very simple (only two nodes) and has almost no effect on the signal.

To illustrate the impact of integrating the VLC system into the PLC system, a UDP throughput comparison is carried out between the PLC system and the PLC-VLC system as a function of the transmitted power by the modem 1. To be able to vary the modem 1 transmitted power, a variable gain power attenuator is placed at modem 1's output. In the PLC-VLC system, the distance between the LED and the optical receiver is fixed at 10 cm. As shown in fig. 3.12, the maximum PLC throughput is almost constant (maximum) for these power values. However, in the PLC-VLC system, additional power is required to maintain the maximum throughput of 66 Mbit/s. In fact PLC modems support high attenuation values since they are designed to sustain extremely faded channels. However, in the PLC-VLC case, the additional power required to reach the maximum throughput of 66 Mbit/s is due to the lower signal-to-noise ratio (SNR) in the case of PLC-VLC in comparison to the standalone PLC system. This is caused by the additional VLC noise and the VLC channel's limited bandwidth.

To further highlight the effect of limited LED bandwidth and VLC noise, the UDP throughput of both systems (full PLC and PLC-VLC) are compared when modem 2 receives the same amount of power. Considering the case where the PLC-VLC system transmits a signal of power −8 dBm, modem 2 receives a power of −20 dBm. In this case, the maximum throughput reached is about 27 Mbit/s. However in the case of the full PLC system, when modem 2 receives a power of −20 dBm, the maximum throughout achieved is approximately 67 Mbit/s.

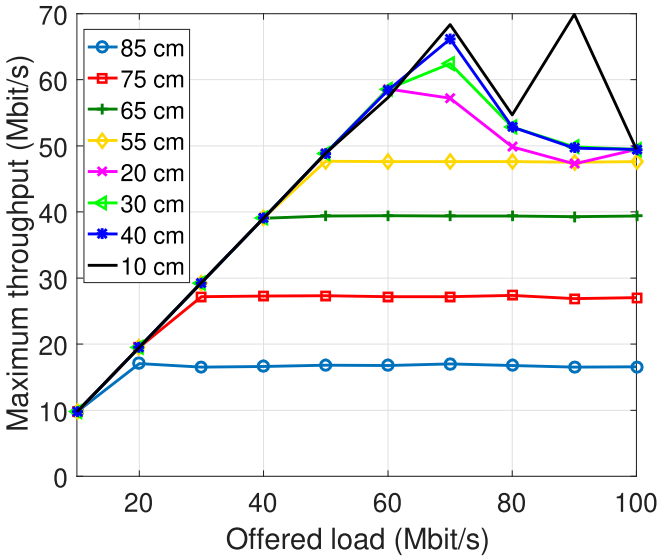


Figure 3.11: UDP Throughput versus the offered load for different distance between the LED and the optical receiver.

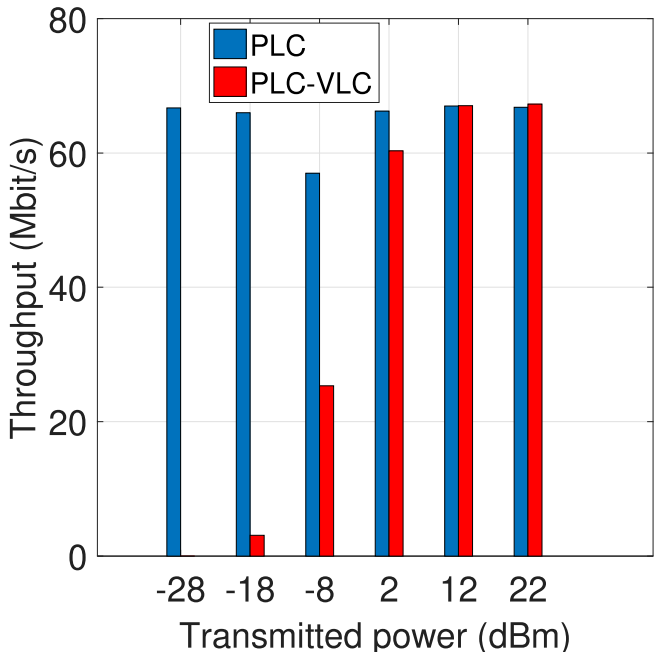


Figure 3.12: UDP Throughput comparison between PLC and PLC-VLC system in function of the Transmitted power.

So even though the modem 2 receives the same amount of power in both systems, the SNR in the case of PLC-VLC is much lower than that of the PLC system, which substantially reduces the maximum throughput.

3.2.3 Optical system dimensionning

As seen in the previous section, 40 cm is the maximum distance between the transmitter and the optical receiver for which a maximum throughput is maintained (66 Mb/s). The measurement shows that at this distance, the received electrical current is 706 nA. Hence, it can be predicted that this value is the minimum current that guarantees the maximum throughput of the PLC-VLC system when a signal of 160 mA peak to peak is transmitted by modem 1. To reach greater distances, the transmitted power must be increased. In fact, there are two ways to increase the transmitted power: *i)* increase the transmitted power per LED, which is not always possible because the transmitted power is limited to a certain level, *ii)* or use several LEDs which is the most suitable solution. Therefore, an analysis is performed in this section to calculate the minimum number of red LEDs needed to achieve the maximum throughput in the function of distance while considering that they are synchronized and they transmit the same signal. Also, the minimum number of LEDs required for implementing a VLC system inside a typical room is estimated and compared to the number of red LEDs needed to illuminate the same room. This comparison demonstrates that the LEDs used for lighting are sufficient for VLC.

The received signal is inversely proportional to the square of the distance separating the optical transmitter and the optical transmitter. Using (3.16), our VLC system parameters and a fixed transmitted signal value (160 mA), the minimum number of LEDs required to maintain 706 nA at the optical receiver is calculated in function of the distance. Considering a typical room of 3 m in height, the distance between the LED and a receiver located on a work area for work purposes, typically 0.75 m above the ground, is approximately 2.25 m. At this distance of 2.25 m, the minimum number of red LED is 60 (see fig. 3.13). This number should be compared to the number of LED required to illuminate the room to validate that no additional LED are needed to maintain good communication performance. It should be noted that in this part the vertical distance is only considered. However, in the last paragraph the mobility of the mobility of the user is taken into account.

Based on the Deutsche Institut fur Normung (DIN) standard, the required illuminance of a normal office room is 500 lux [50]. The total luminous flux can be calculated as a function of the horizontal illuminance (E_h) by the following expression [50]:

$$E_h = \sum_{n=1}^{N_{LED}} \frac{(m+1)\,A\cos^m(\phi)\cos(\psi)}{2\pi D^2}\phi_n \tag{3.17}$$

where ϕ_n is the luminous flux of the nth LED. The target luminous flux at a distance of 2.25 m

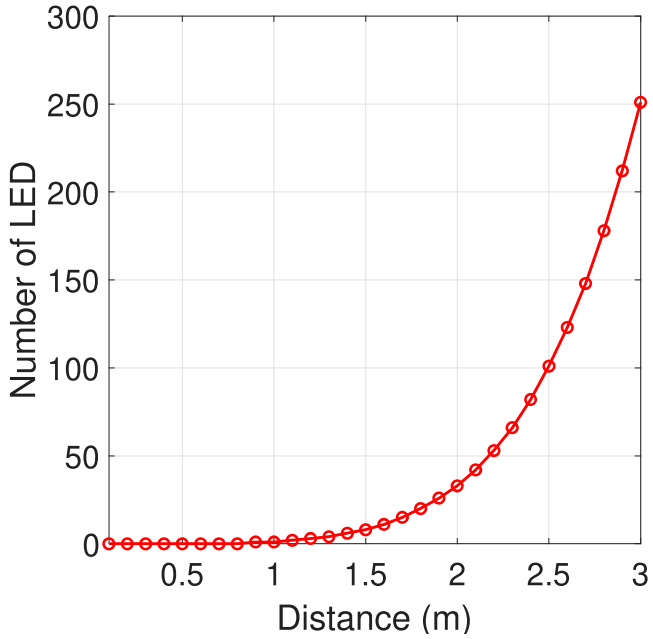


Figure 3.13: Number of LED needed to receive 706 nA signal as a function of the distance between the LED and the photodiode.

should be 7078 lm. This value cannot be achieved by using only a single RGB module because their LED are very small. As mentioned in [65], the red, green, blue and the extra white LED of the module provide respectively 18, 38, 12 and 53 lm which can't suffice for lighting the room. Thus, an array of multi-LED should be used. The minimum number of red, green, blue and white LEDs needed to get a white light of 7078 lm with a color temperature of 4000 K (cool white) are derived using of ColorCalculator software developed by OSRAM [76] via the following procedure: at first the target luminous flux, the luminous flux and the wavelength of each LED color should be known. Then, using the ColorCalculator software, the chromatic coordinates of each of the LED color and the target light color is extracted from the CIE 1931 xy color space (see fig. 3.14). By exhaustive trials using the same software, the total luminous flux of each of the four colors is found such that the sum of the luminous flux of these four colors is equal to the target luminous flux and that their proportions reach the chromatic coordinates of the desired color as shown in fig. 3.14. Finally, the number of LED for each color is obtained by dividing the total required luminous flux by the luminous flux emitted by a single LED. Table 3.4 shows the total luminous flux and the number of LED needed for each color. As seen in table 3.4, the minimum number of red LED needed for lighting is 71 LED, which is greater than that required for data transmission (60 LED). Hence, this total number of LED needed for lighting can easily transmit the UDP packets at a rate of 66 Mbit/s.

Indeed, the numbers of LEDs for VLC and lighting are calculated by considering that the user is immobile inside the room and that the LED luminaire is directly vertical to him. How-

Table 3.4: Design of a 4000 K white light system using red, green, blue and white LEDs from Luxeon module [76].

LED	Red	Green	Blue	White
Required total luminous flux (lm)	1278	2584	696	3127
Required number of LED	71	68	58	59

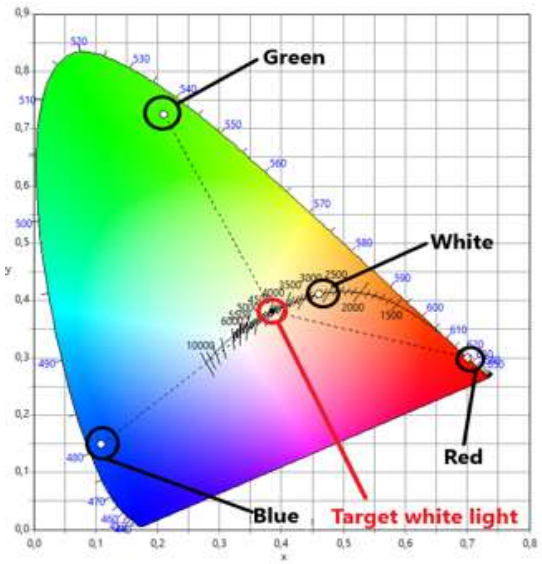


Figure 3.14: CIE 1931 xy color space with the red, green, blue and white LED chromatic coordinates and the target white light chromatic coordinates [76].

ever, the user may be mobile, so the amount of the received power may decrease depending on his position in the room. Using a matrix of 64 red LEDs separated by 1 cm from each other and set in the middle of a typical room ($5 \times 5 \times 3$ m^3), the normalized received electrical power is calculated based on the expression (3.16) in the function of the user position inside the room. The origin of the x, y, and z axes is considered in the middle of the LED matrix and the distance between the user and the LED matrix (D) is calculated in function of x, y, and z according to this expression: $D = \sqrt{x^2 + y^2 + z^2}$. As shown in fig. 3.15, the power attenuation increases as the receiver moves away from the LED array until it reaches −26.81 dB at the corners of the room. This simple analysis highlights the importance of finding the right number and optimal distribution of LEDs in order to obtain uniform lighting and communication signal power inside the entire room.

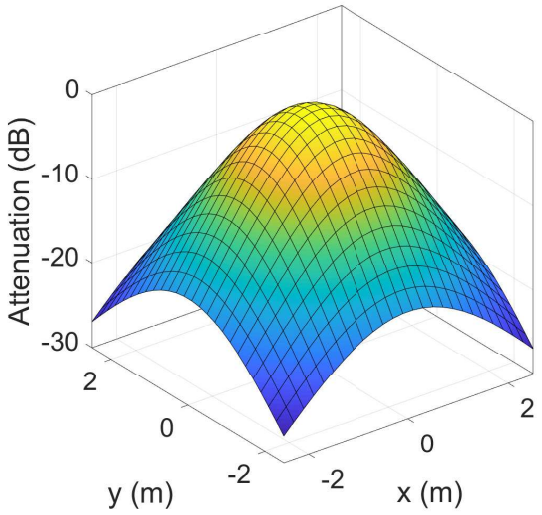


Figure 3.15: Received power attenuation as a function of the receiver position in a $5 \times 5 \times 3$ m^3 office.

3.3 Conclusion

This chapter provides our first contribution is this thesis. It presents a new broadband PLC-VLC system that directly uses an already existing PLC standard without making any changes to the signal before passing through the VLC system. First, the frequency characteristics of monochromatic LEDs (red, green, and blue) are measured. The measurement results show that the red LED has larger bandwidth (20 MHz) compared to the blue and green LED (5 MHz) of the same RGB module. And we also notice that above the cut-off frequency the attenuation decreases slowly which makes it possible to transmit signals having a modulation bandwidth greater than that of the LED. Therefore, the red LED is chosen to transmit the HPAV signal because as it can support the modulation bandwidth of the HPAV signal (2–28 MHz). The

impedance of the LED is also measured in order to check the LED behavior according to increasing frequency. It is shown that at low frequencies, the LED impedance acts as a simple resistor until reaching a certain frequency when capacitive behavior begins to appear and at high frequencies, the inductance components starts to arise as the impedance begin to increase with the increase of the frequency.

Based on [60], an equivalent electrical circuit is proposed to model power LEDs. Circuit parameters are estimated for each LED in the RGB module using the frequency response and impedance measurement results. The accuracy of this model is validated for the blue LED. The estimated frequency impedance and frequency responses of the LED match perfectly those measured in the case of the blue LED. However, for the red and green LEDs, the simulated impedance phases do not match those measured. Therefore, a more accurate model must be found, especially to model power LEDs when they are biased by their typical current value.

When designing the optical receiver, we needed a meticulous method that allowed us to directly calculate the current generated by the photodiode based on the current injected by the LED. Therefore, an expression is constructed taking into account the E/O and O/E conversions, LED frequency attenuation, and channel behavior to calculate the photo-generated current as a function of the LED injected current. This expression can also help to avoid repeating measurements each time the transmitted signal power is adjusted. The reliability of this expression is validated by measurements.

Finally, the proposed PLC-VLC system is implemented. The possibility of directly transmitting the HPAV signal through the optical system is demonstrated. An experimental test shows that it is possible to obtain a maximum throughput of 66 Mbit/s using a single red LED at a distance of 40 cm from the photodiode. Additionally, a maximum throughput comparison is performed between the PLC and the PLC-VLC system to highlight the effect of VLC channel attenuation and noise on system performance when both systems transmit the same amount of power. As this test bench is a small-scale communication system, a theoretical study is also made to extrapolate the obtained results to real applications like PLC-VLC communication in a typical room. The results show that to apply the PLC-VLC system inside a typical room, 60 red LEDs are needed to guarantee a maximum throughput of 66 Mbit/s. It is also revealed that in order to light the same room using RGB white LED technology, 71 LEDs is the minimum number of red LEDs to be used, which is greater than the number required for communication. This result proves that no additional LEDs are needed to apply optical communication alongside with the lighting.

Chapter 4

PLC signal leakage through domestic LED bulbs

After having successfully transmitted HPAV signals through a power LED, we begin to examine this integration from a different point of view: The PLC signal leakage through LED bulbs. Domestic LED bulbs are always connected to powerline that can carry PLC signal. So, the risk of eavesdropping on PLC network via LED bulb should be carefully studied. Hence, passive attacks through domestic LED bulbs are discussed in this chapter. First, unintentional leaks are studied to assess the ability of LED bulbs to naturally leak PLC signals. Later, intentional modifications are applied to domestic LED bulbs to observe if it is possible to promote leaks.

The LED driver is the link between the powerline and the LEDs existing inside the bulb. Thus, an in-depth investigation of the common LED driver technologies adopted to power domestic LED bulbs is carried out. In fact, the driver circuit is an indispensable component in LED bulbs. It provides the necessary amount of DC voltage and current after transforming and matching the power signal from the original AC to DC. The driver is the first component in the LED bulb that governs the amount of PLC signal that leaks to the LEDs. Thus, several LED bulbs with different driver technologies are tested in this chapter in order to verify which one is the most prone to leaks. In addition, the optical side channel is characterized for each bulb by measuring *i*) the frequency response of the channel, *ii*) the power spectral density (PSD) of the optically received signal when the PLC modems are connected to the same PLC network, *iii*) and the cross-correlation value of the optically received signal when transmitting a pseudo-random binary sequence (PRBS) over powerlines. On the other hand, a DMT signal is injected into the power line where the LED bulb is connected in order to check if the data from the PLC can be optically retrieved. In addition, the intentional attack is also studied in this chapter. Indeed, simple modifications are made to the drivers of the LED bulbs to verify if it is possible to increase the leak. Finally, the physical layer security for indoor PLCs is studied in the existance of a non-legitmate optical system.

4.1 Domestic LED bulbs characteristics

The LED bulb is mainly composed of a LED driver and a LED matrix (see fig. 4.1). These two components play a major role in the amount of energy that can leak from the PLC system. So, in section 4.1.1, an overview of existing LED drivers that can power the LEDs is provided, especially the active linear driver. To the author's knowledge, this type of driver is not frequently mentioned in reference In section 4.1.2, the LEDs inside the bulbs are also investigated. The advantage of using high voltage LED assembly instead of single LED is explained .

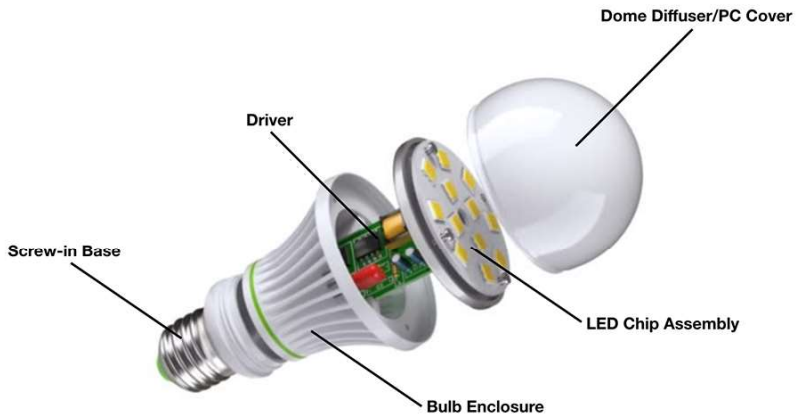


Figure 4.1: Taking apart an LED light bulb [92].

4.1.1 LED driver

There exists several types of drivers and their typologies depend on the power of the bulb, the environment the bulb will be used in, and the available power source [72]. 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, large components, and an inaccurate current control, thus limiting its use to applications that prioritize reliability over efficiency. This type of driver is typically used in outdoor lighting systems where they are exposed to harsh environmental conditions [11].

The growing demand for high-brightness and energy-efficient LED bulbs has led LED designers to introduce an active non-linear current driver called a switch-mode power supply (SMPS). Multiple topologies are available depending on power range, need for galvanic isolation, size and cost-effectiveness, easy dimming capability, modular approach availability, and efficiency goal [72]. In this type of driver, current and voltage are controlled using pulse width modulation signals. These drivers are widely used for indoor lighting. The main disadvantage of the SMPS driver is the generation of significant harmonics that can reach hundreds of

MHz. These harmonics can easily cause high emissions hence the need for an electromagnetic interference (EMI) filter [61].

4.1.1.1 Active linear driver

Through experimental testing, we have found that Active Linear (AL) drivers are also used in many LED bulbs, especially those having power less than 10 W. The AL provides precise current control, does not require EMI filters, and requires a limited number of surface mount devices (SMD) that can be mounted on the same board with a LED array. AL drivers are very cheap in comparison to SMPS drivers. These drivers were typically used in low-power applications such as smart home devices and LED displays as they were considered less efficient than SMPS drivers if they are adopted for indoor lighting [15]. However, when we compared the power efficiency of SMPS bulbs with that of LED AL bulbs consuming the same power (less than 10 W), we found that they are very close, which may explain their recent extensive use in indoor lighting.

After rectifying the AC signal using the diode bridge, the AL driver establishes the necessary constant current by means of feedback through a sensing resistor and a Differential amplifier circuit which compares a reference voltage ($V_{reference}$) with the actual voltage ($V_{rectified}$) on the sensing resistor (R_S) as can be seen in fig. 4.2. The necessary LED current is established by the relation [72] [80]:

$$I_{LED} = \frac{V_{reference}}{R_s} \tag{4.1}$$

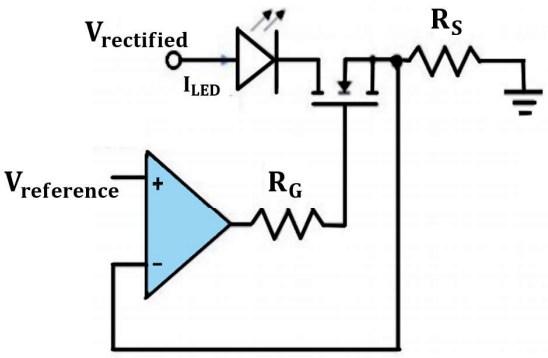


Figure 4.2: Operation principle of active linear driver.

4.1.2 LED assembly

While examining LED bulbs from different brands, we discovered that almost all the bulbs contain a LED array made up of high voltage LEDs. In fact, the high voltage LEDs are DC-driven LEDs with a turn-on voltage greater than the 2–3 V turn-on voltage of conventional LEDs [68].

In order to satisfy power efficiency, the LED designer should directly connect the LEDs to the high output voltage [100]. This means, the voltage drop in the Mosfet transistor of the driver must remain low compared to the voltage present on the LEDs. Hence, has to choose between using a large number of low-voltage LEDs connected in series to form a high voltage string or using a few high voltage LEDs. Besides the bulkiness of the low voltage LED string, the lifetime of this LED string is directly correlated to the degradation of the solder interconnecting the LEDs over time. Thus, most designers prefer to use high voltage LEDs as they are compact in size, cheaper, and have a long lifetime. Actually, each high voltage LED comprises a large number of junctions or sub-LEDs mounted on a submount. The sub-LEDs are interconnected in series which means that the forward voltage required to drive the high voltage LED depends on the number of sub-LEDs and their individual drive voltage. This technology allows for the custom design of the LED in order to obtain the desired voltage and current [40]. Fig. 4.3 shows the difference between two single-junction LEDs and three sub-LEDs mounted on the same submount.

As seen in the previous paragraph, power efficiency is one of the reasons of using a large number of LEDs with a low drive current for obtaining the desired light output instead of using a small number with a high drive current. However, avoiding efficiency droop is another reason that pushes the LED bulbs manufacturer to use LED assembly. Efficiency droop refers to the reduction of the luminous efficacy with increasing current densities or operating temperatures [24].

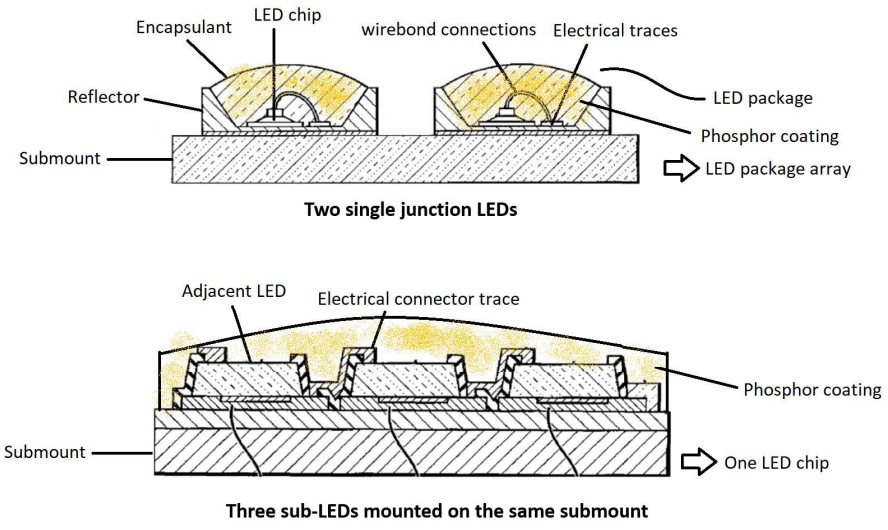


Figure 4.3: Two single-junction LED package (upper) and high voltage LED including 3 sub-LEDs (lower) [100].

4.2 Optical side channel characterization

Side channel characterization is an indispensable step when assessing the risks of PLC data leakage through commercial LED bulbs. Hence, in this section channel characterization is performed according to three different approaches: *i*) measuring the side channel frequency response, *ii*) measuring the frequency power received through the side channel when the LED bulb is plugged in the same powerline with two PLC modems, and *iii*) calculating the maximum cross correlation peak value after transmitting a PRBS signal through the side channel. Section 4.2.1, lists all the tested LED bulbs and compares them according to their parameters. In addition, section 4.2.1 describes the experimental setups adopted when characterizing the side channel. In section 4.2.1.1, the measurement of the transfer function of the side channel is performed. In section 4.2.1.2, the PSD of the received signal through the side channel is measured when two PLC modems are exchanging information on the same powerline network. In section 4.2.1.3, the channel sounding is performed using PRBS signal in order to increase the detection capability especially when the optical side channel exhibits high attenuation levels. Finally, the results of the three experiments are presented and analysed in section 4.2.2.

4.2.1 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 as presented in table 4.1. As seen in the setup schema of fig. 4.4, 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.It should be noted that we removed the diffuser (plastic cover) of the LED bulb to maximize the amount of light passing through the hole as illustrated in fig. 4.4. 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. The optical receiver used in this testbed is the same as the one used in section 3.2 where its parameters are listed in the table 3.3. The rest of the testbed components parameters are detailed in the table 4.2.

4.2.1.1 Side channel frequency response

The transfer function of the side channel is measured in order to evaluate the bandwidth limitation of the commercial LED bulb, which is due to the existence of the LED driver and the white LED. The side channel is composed of the powerline channel and the optical channel. Thus, the cascaded electrical-optical channel is measured using a network analyzer with a

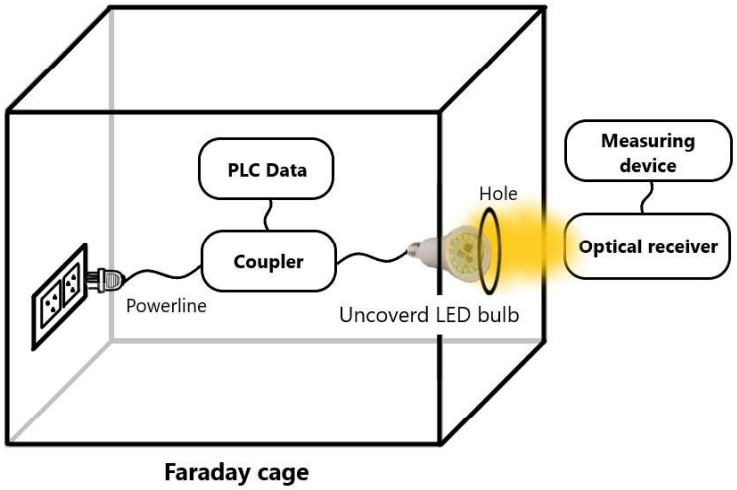


Figure 4.4: Experimental setup schema.

Table 4.1: Specifications of the tested commercial LED bulbs.

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

Table 4.2: Testbed parameters.

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
Network analyzer measured bandwidth	300 kHz–100 MHz
spectrum analyzer measured bandwidth	20 kHz–30 MHz

transmitted signal power of 10 dBm. The band of analysis is 300 kHz–100 MHz, and the step size is 400 kHz. The network analyzer's output signal is 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 signal and the rest goes through the drivers to the LED array where it will be transduced from an electrical to an optical signal. The optical receiver transforms and amplifies the signal before being reinjected into the network analyzer that will calculate the channel transfer function.

4.2.1.2 PSD of the HomePlugAV leaked signal

The objective of this chapter is to study the risks of PLC signal leakage through domestic LED bulbs. Therefrom, the HPAV standard is chosen in this experiment because, as seen in section 2.1.1.3, HPAV is one of the most popular PLC standards for indoor communication.

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 (the same modems used in chapter 3. 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.

4.2.1.3 PRBS transmission through the side electrical-optical channel

In this section, channel sounding is performed to precisely characterize the side channel, 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 size $2^{11}-1$ 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. 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. These impulse-like cross-correlation functions can give an estimate of the channel impulse response.

4.2.2 Results and discussion

In this section the results of the three experiments described in section 4.2.1 are presented.

4.2.2.1 Side channel frequency response results

Figures 4.5 and 4.6 show the side channel frequency responses for LED bulbs having AL drivers and SMPS drivers respectively. They describe the results when the LED bulb is covered with an opaque screen (dotted red curves) and in the absence of the opaque screen (solid blue curves). This comparision is made in order to estimate the reliability of the measurement by comparing the signal received when through RF leaks (the optical channel is masked) with that observed when the optical signal is directed to the photodiode of the receiver. It is clear from figs. 4.5a and 4.5b that the difference between the blue and red curves in the case of LSC and Lexman LED bulbs cannot be overlooked. The transfer function in the case of LSC bulbs shows an attenuation of −48 dB at 30 MHz when the LED is not covered against an attenuation of −68 dB at the same frequency in the case where it is covered with an opaque screen. Additionally, Lexman's frequency response has higher attenuation than LSC's. Fig. 4.5b shows −70 dB attenuation at 30 MHz when the LED bulb is uncovered compared to −72 dB attenuation at the same frequency when the bulb is covered with the opaque screen. The bandwidth of Eurodomest bulb is perceptible for frequencies lower than 1 MHz. However, Bailey and Aric bulbs have very limited bandwidth and the difference between the red and blue curves is barely recognizable. Let us now turn to the results obtained in the case of the SMPS pilots. As shown in fig. 4.6, the red and blue curves in the case of Philips and SLV LED bulbs are quite similar, which means that the attenuation in these cases is very severe.

4.2.3 PSD of the HomePlugAV leaked signal results

The results of the experiment described in section 4.2.1.2 are depicted in this section. Figs. 4.7 and 4.8 show respectively 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 the PSD of the received signal when the HPAV modems are OFF (red dashed curve), respectively in the case of AL and SMPS LED bulbs. It seems form figs. 4.7a, 4.7b, and 4.7e that the PLC signal leakage through commercial AL LED bulbs looks possible, as is the case of LSC, Lexman, and Aric LED bulbs. The received signal PSD at 12 MHz is −39 dBm against a PSD of −42 dBm when the modems are OFF. In addition, the PSD of the signal received through the Lexman LED bulb is −40 dB at 10 Hz against a PSD of −45 dB at the same frequency when the HPAV modems are OFF. Also, in the case of Aric LED bulb, the received signal PSD at 8 MHz is −42 dB against a −45 dB when modems are OFF. However, for the rest of the AL LED bulbs (Bailey and Eurodomest), it is difficult to notice the received HPAV spectrum because of the severe attenuation. On the other hand, the SMPS LED bulbs attenuate intensively the HPAV power making leakage detection through this experiment impossible. Hence, further experiments should be made to be able to assess precisely the leakage.

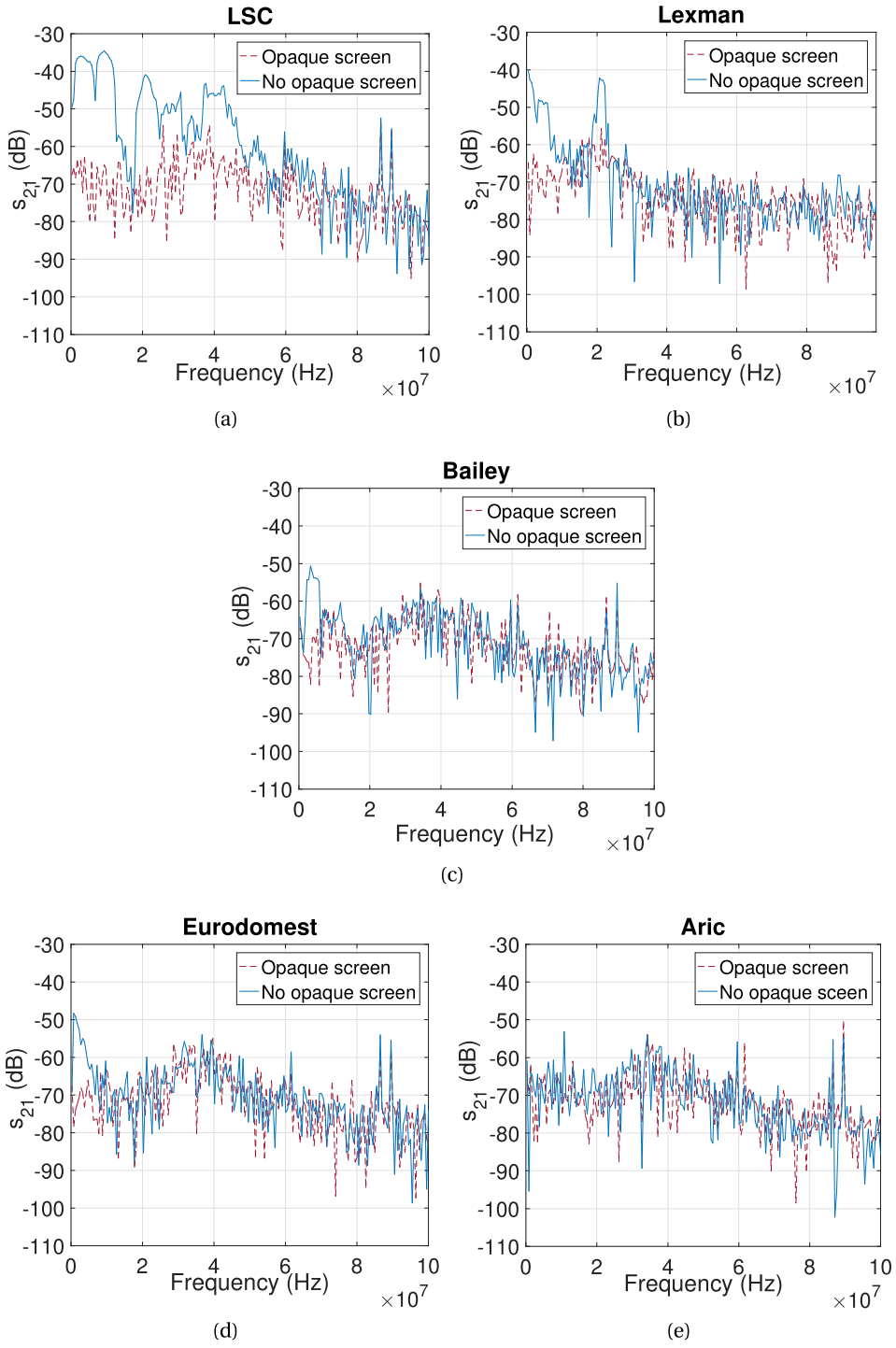
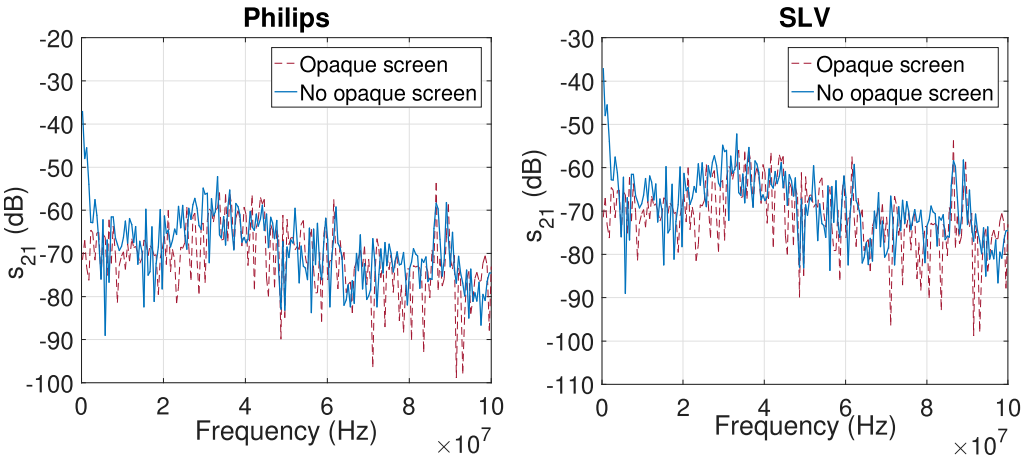


Figure 4.5: The transfer function of the optical-electrical side channels for the LED bulbs having an AL driver. (a) LSC LED bulb. (b) Lexman LED bulb. (c) Bailey LED bulb. (d) Eurodomdest LED bulb. (e) Aric LED bulb.



(a) (b)

Figure 4.6: The transfer function of the optical-electrical side channels for the LED bulbs having a SMPS driver. (a) Philips LED bulb. (b) SLV LED bulb.

4.2.3.1 Side channel sounding using PRBS signal

The cross-correlation between the transmitted and the received PRBS signal is calculated in this section. Fig. 4.9 shows the average value of the cross-correlation peaks of the ten transmitted signal through the optical-electrical side channel. 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. For example, the cross-correlation peak value in the case of the LED bailey that has an AL driver is 2230 and 183.2 at rates of 10 Mbits/s and 30 Mbits/s respectively. Also, in the case of the Philip LED bulbs, the the cross-correlation peak value is respectively 181 and 141 when the PRBS signal has a rate of 10 Mbits/s and 30 Mbits/s. However, in all cases, the auxiliary channel attenuations are lower than 38 dB compared to the injected signal with the experimental setup.

4.3 DMT transmission through the electrical-optical side channel

In order to verify the possibility of correctly detecting the PLC signal leakage through the domestic LED bulbs, a DMT signal is injected into the electrical network where the LED bulbs are plugged. The side channel received signal is recorded to be decoded and interpreted offline. Thus, section 4.3.1 outlines the architecture of this experience taking into account the equipment parameters and the physical layer adopted to perform the experiment. Section 4.3.2 exhibits and interprets the obtained results based on the computation of the bit error rate

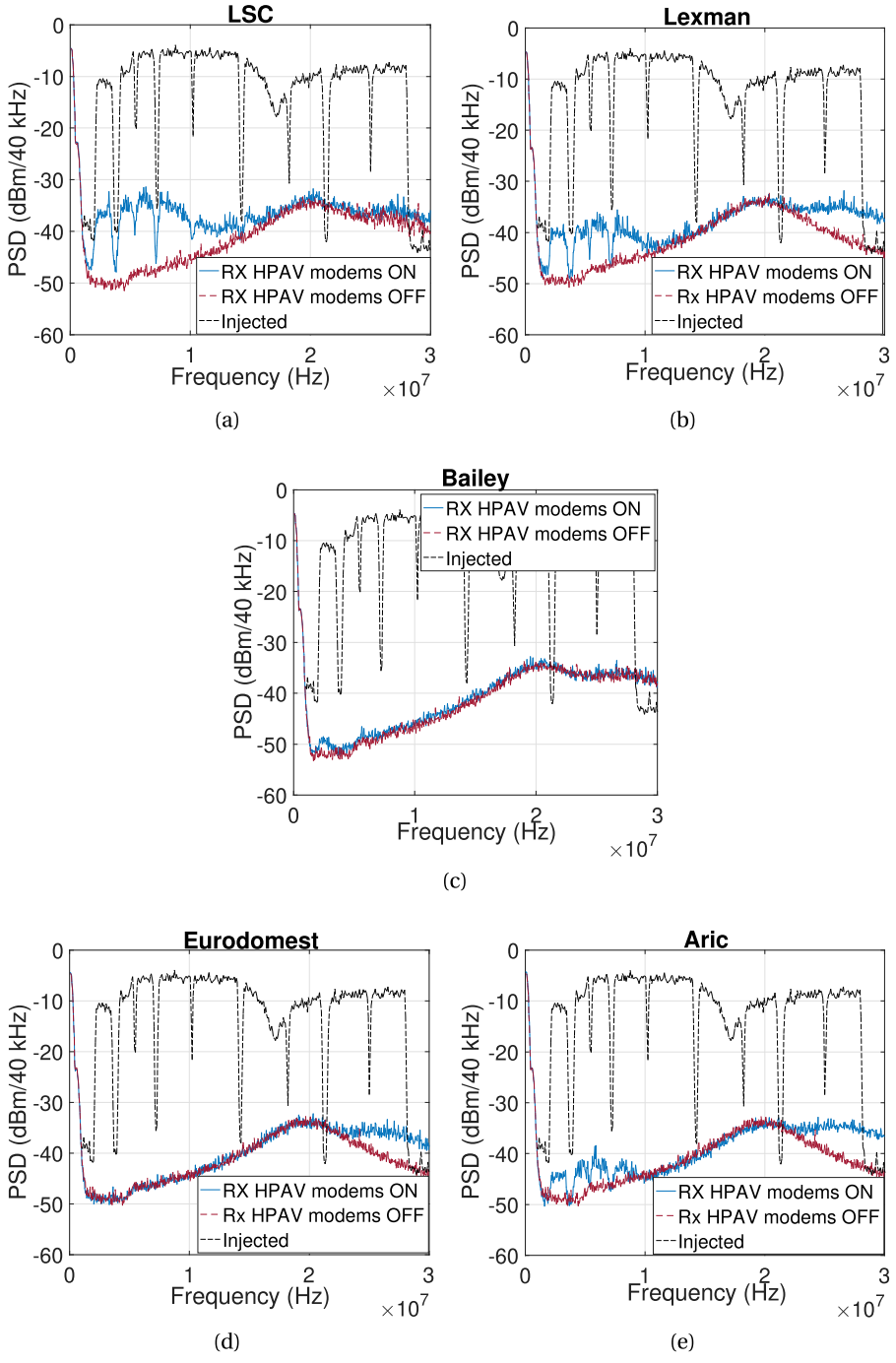
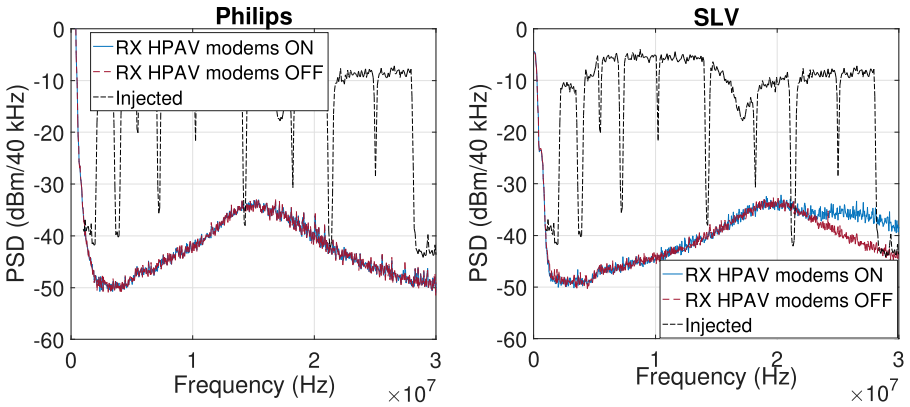


Figure 4.7: The PSD of the transmitted HPAV signal using a commercial PLC modem, the optically leaked signal when the PLC modems are ON, and when they are OFF. (a) LSC LED bulb. (b) Lexman LED bulb. (c) Bailey LED bulb. (d) Eurodomdest LED bulb. (e) Aric LED bulb.



(a) (b)

Figure 4.8: The PSD of the transmitted HPAV signal using a commercial PLC modem, the optically leaked signal and the received noise via SMPS LED bulbs. (a) Philips LED bulb. (b) SLV LED bulb.

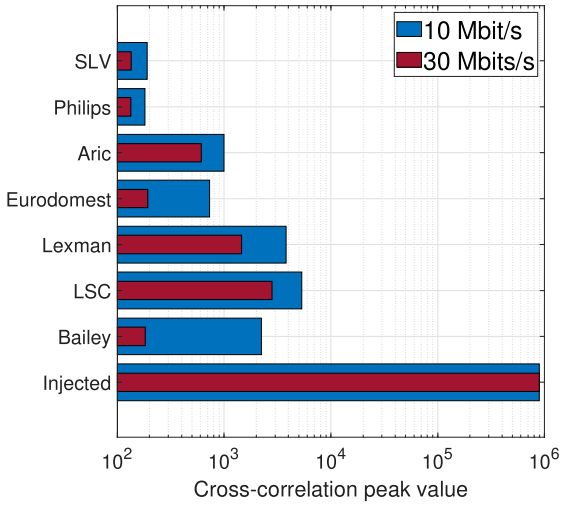


Figure 4.9: Cross-correlation peak values of received PRBS signal for all the tested LED bulbs at 10 Mbit/s and 30 Mbit/s.

(BER).

4.3.1 System architecture and experimental setup

In this trial, the experimental setup described in section 4.2.1 is also adopted with the same parameters listed in table 4.2. A digital image is first encoded and modulated offline using Matlab. Then the digital data is fed to an arbitrary waveform generator to be converted into an analog signal. As the maximum amplitude of the delivered signal at the output of the waveform generator is limited to 2 V peak-to-peak which does not correspond to the amplitude of the signal produced by commercial HPAV modems (8 V peak-to-peak), Texas Instrument's THS6222RHF evaluation module [94] is used to amplify the signal to the desired level. We fixed the gain to $V_{OUT}/V_{IN} = 4$ in order to get an output signal of 8 V peak-to-peak. As seen in [94], this module is dedicated to broadband PLC applications. Then, the amplified signal is injected into the power line via the PLC coupler used in the previous experiments (see section 4.2.1). The optical receiver collects the light delivered by the LED bulb connected to the same powerline. Finally, an oscilloscope (LeCroy 6 MXs-A, 8-bit resolution) is used to sample and save the received signal in order to be processed offline using Matlab.

The DMT is chosen in this experiment in order to perform a real base-band transmission. The physical layer frame generated using Matlab is composed of a header and a payload. The header includes a preamble that is used to detect the frame and to perform time synchronization. The preamble is based on the algorithm of Minn & Bhargava [93]. This algorithm exploits a particular preamble in the frequency domain which is the concatenation of a vector A as follows:

$$[A, A, -A, -A] \tag{4.2}$$

where A is the IFFT of a pseudo noise sequence of length four time smaller than the length of the DMT symbol ($L = N/4$). The cross-correlation of the L first samples and the L following samples is expressed by the following equation:

$$P(n) = \sum_{k=0}^{1} \sum_{m=0}^{L-1} r(n+2Lk+m)\, r(n+2Lk+m+L) \tag{4.3}$$

where r represents the normalized received signal. $P(n)$ is normalized to the sum of energy of the L following samples which is calculated as follows:

$$R(n) = \sum_{k=0}^{1} \sum_{m=0}^{L-1} |r(n+2Lk+m+L)|^2 \tag{4.4}$$

The metric used to detect the beginning of the frame is calculated following this expression:

$$M(n) = \frac{|P(n)|^2}{R^2(n)} \tag{4.5}$$

The header includes also pilot symbols that can be exploited to estimate the channel for channel equalization. A zero-forcing equalizer is applied to each sub-carrier. Moving to the payload, it contains the useful data that are QAM mapped and DMT modulated. A FEC based on Bose-Chaudhuri-Hocquenghem (BCH) code is also employed. Table 4.3 shows the different parameters of the physical layer.

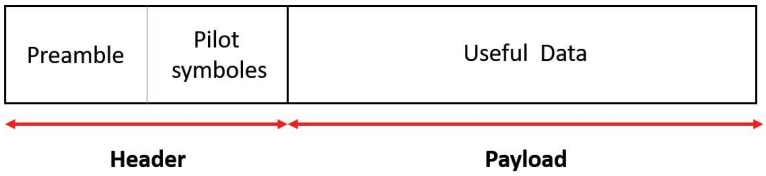


Figure 4.10: Physical layer frame.

Table 4.3: Physical layer parameters.

Useful bandwidth	[2-28 MHz]
FFT length	2288
Useful sub-carriers number	1058
Total sub-carriers number	1140
Sampling frequency	75 MHz
Oversampling frequency	120 MHz
Number of samples of cyclic prefix (CP) (5.56 us)	417
Symbol time without CP	40.67 us
Inter-carrier space	24.45 kHz
Mapping	16 QAM
FEC	BCH (8,4)
Transmitted image	Cameraman.tif (128 × 128)

4.3.2 Results and discussion

This section evaluates the ability to retrieve useful information from the leaked signal. At first, we will qualitatively compare the image transmitted with the image received through the various tested domestic LED bulbs. Afterward, the BER is calculated to try to quantitatively assess the existence of unintentional optical leaks.

Fig. 4.11 shows the images received through all tested LED bulbs connected to the power line where the image is initially injected. As we can see, some LED bulbs can naturally leak certain information without intervening on the LED bulbs to foster their ability to leak. It is obvious that AL LED bulbs (LSC, Bailey, Lexman, Aric, and Eurodomest) are more prone to leaking PLC signals than SMPS LED bulbs (SLV, and Philip).

The results of BER calculations after the application of FEC are presented in fig. 4.12. It can be noticed that the BER varies between 0.19 to 0.48. In this experiment, the BER of the AL

LED bulbs is less than 0.36. In the case of the LSC LED bulb, the BER is 0.19 which means that 81 % of the transmitted bits are correctly restored. However, in the case of SMPS LED bulbs like Philips and SLV, almost half of the transmitted bits (47 %) are not correctly received. This means that in the case of SMPS bulbs, the driver obstructs the PLC signal to cross it to reach the LED array.

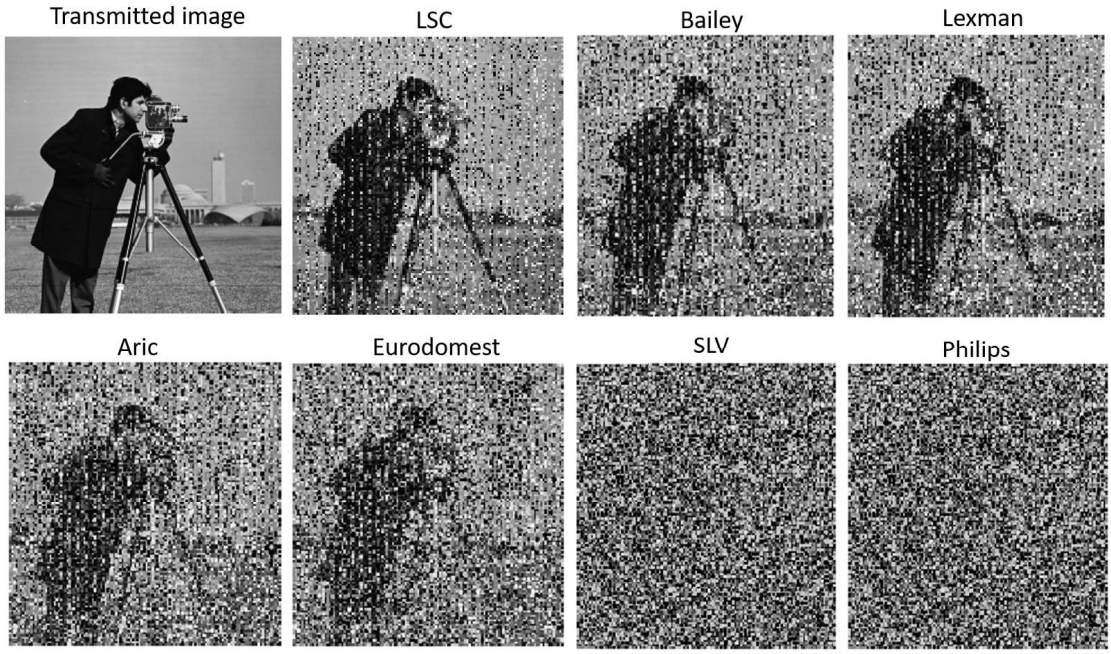


Figure 4.11: Comparison between the transmitted and received images through the side channel for LSC, Bailey, Lexman, Aric, Eurodomest, SLV, and Philips bulbs.

4.4 LED driver modification to facilitate the leakage

After testing the natural leakage ability of the LED bulbs, intentional modifications are performed to the LED drivers to verify the possibility of improving leakage. Two LED bulbs are chosen to be modified: Bailey and Philips. These LED bulbs have an AL and SMPS driver respectively. It should be mentioned that these modifications are very simple and do not disturb the operation of the driver. Section 4.4.1 describes the modifications brought to LED drivers. The tests presented in section 4.2.1 and 4.3.1 are repeated with the modified LED bulbs and the results obtained are interpreted in section 4.4.2.

4.4.1 Driver modifications and 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

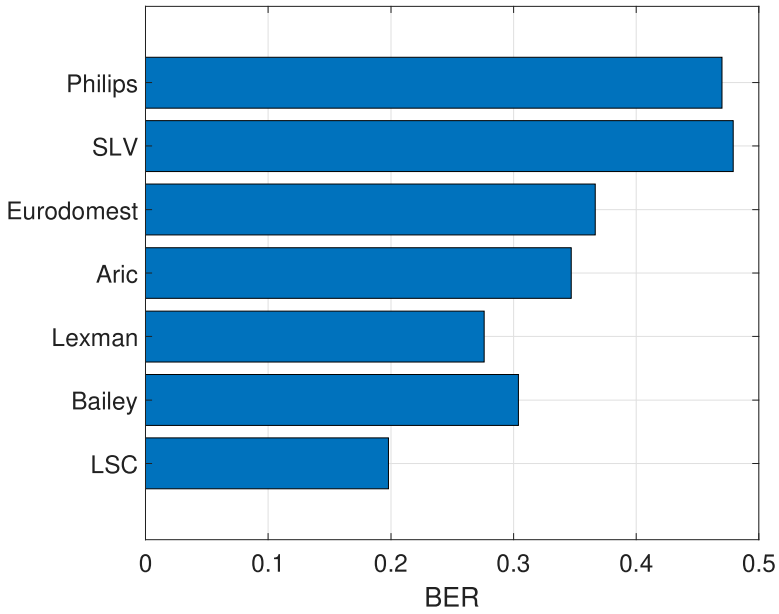


Figure 4.12: BER in function of the tested LED bulbs.

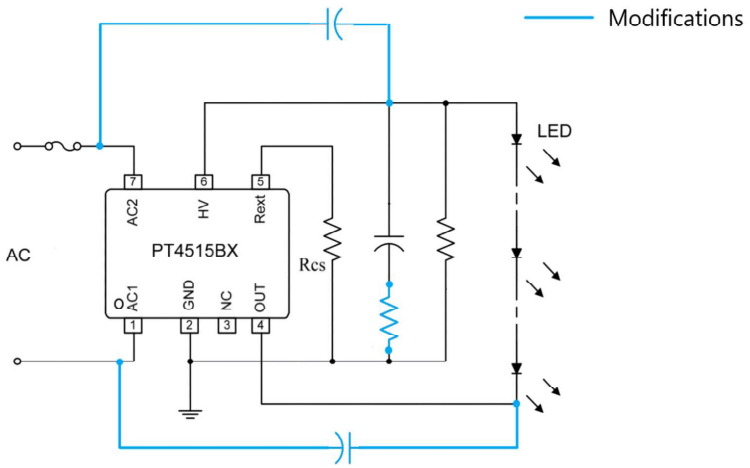
LED and reduce data leaks. In order to facilitate the PLC signals transmission through LED bulbs, simple modifications are made to their driver. These modifications is considered as an intentional attack to the powerline network. It should be noted that after modifications, the SMPS LED bulbs will probably no longer satisfy the EMC tests. Fig. 4.13a shows the active LED driver circuit of the Bailey LED bulb before and after modifications, and fig. 4.13b 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 to increase the leakage ability of capacitors. It should be noted that these modifications do not disturb the amount of power delivered to the LED array. Then, the three experiments described in section 4.2.1 in addition to the experiment presented in section 4.3.1 are repeated with these modified bulbs.

4.4.2 Results

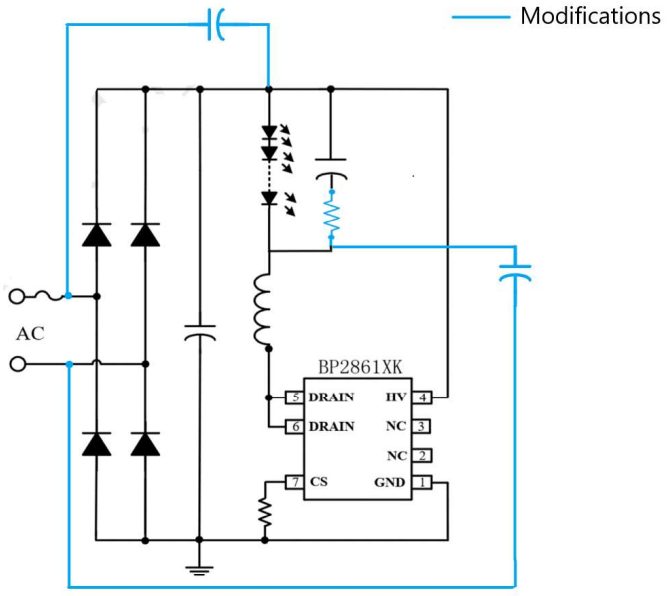
In this section, the results obtained before and after the drivers modification are compared in order to check if this modification can improve the leakage.

4.4.2.1 Side channel frequency response

The transfer function of the modified LED bulbs are presented in fig. 4.14. In the case of Bailey LED bulb (fig. 4.14a), the attenuation for uncovered LED with opaque screen was −67 dB at



(a)



(b)

Figure 4.13: Circuit diagrams of Bailey and Philips LED bulb drivers after modification. (a) Modified AL driver of Bailey LED bulb [79]. (b) Modified SMPS driver of Philips LED bulb [7].

30 MHz, before modifications. It 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 (see fig. 4.14b). In fact, the SMPS circuit is more complicated than the LR one, and any further modification may disrupt the main function of this driver. However, the attenuation becomes −51 dB at 30 MHz.

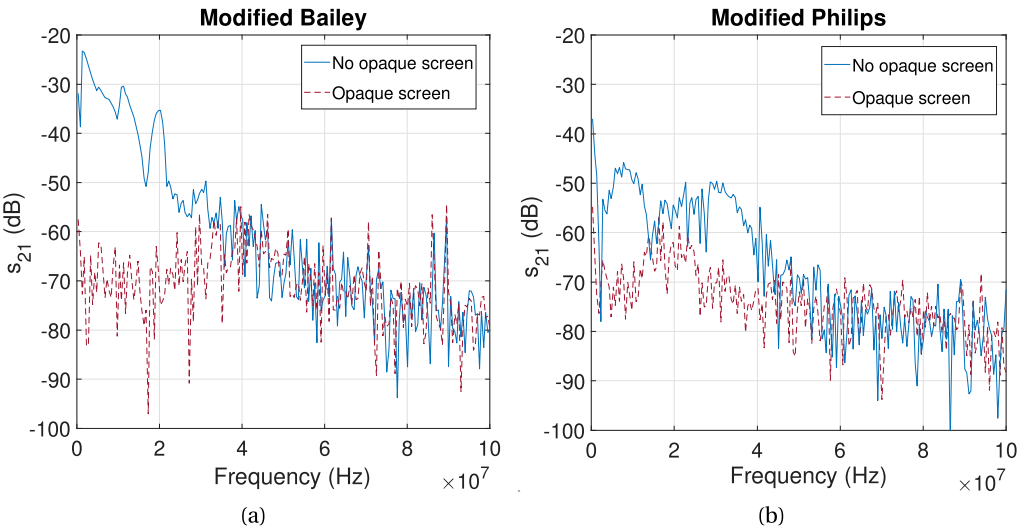


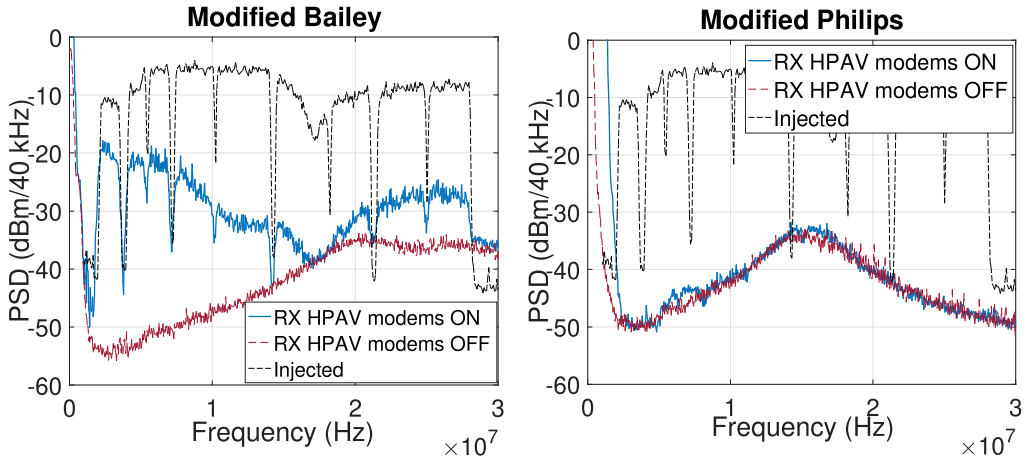
Figure 4.14: The transfer function of the electrical-optical channel after driver modification. (a) Bailey LED bulb. (b) Philips LED bulb.

4.4.2.2 PSD of the HomePlugAV leaked signal

The results of the experiment described in section 4.2.1.2 using the modified LED bulbs are shown in fig. 4.15. 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. 4.15a 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 (see fig. 4.15b). This is because the leakage enhancement procedure is limited by the complexity of the SMPS driver.

4.4.2.3 PRBS transmission through the side electrical-optical channel

The results of the cross-correlation peak value of the received PRBS signal detailed in section 4.2.1.3 are presented in this section. As shown in fig. 4.16, when comparing the modified bulbs to the same unmodified bulbs, it can be noticed that for the Bailey LED the peak before



(a) (b)

Figure 4.15: The PSD of the transmitted HPAV signal using a commercial PLC modem, the optically leaked signal and the received noise via modified LED bulbs. (a) Bailey LED bulb. (b) Philips LED bulb.

modification was 2230 at a rate of 10 Mbit/s (180 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 180 at 10 Mbit/s (134 at 30 Mbit/s) instead of 890 at 10 Mbit/s (1200 at 30 Mbit/s) after the modification. The obtained results can confirm that a simple modification of the drivers (AL or SMPS) can significantly increase the leakage.

4.4.2.4 DMT signal transmission through the electrical-optical side channel

After repeating the same experiment described in section 4.3.1, the results presented in fig. 4.17 show the significant improvement brought by the drivers' modifications. In fact, in the case of Bailey LED bulbs, we can see that the received image after driver modification is less noisy than that before modifications. However, in the case of Philips LED bulbs, we can see that the received image after driver modification is barely recognizable.

Moving on to fig. 4.18, this figure compares the received BER signal for Bailey and Philips LED bulbs before and after driver modifications. The BER in the case of the Bailey LED bulb was 0.3 before modification and it becomes 0.17 after modification. In addition, the BER in the case of the Philips LED bulb is reduced from 0.47 before modification to 0.38 after modification. This means that this simple modification of the driver considerably favors the signal leading to detecting correctly an additional 13 % of the transmitted bits in the case of the Bailey LED and 9 % in the case of the Philips LED bulb.

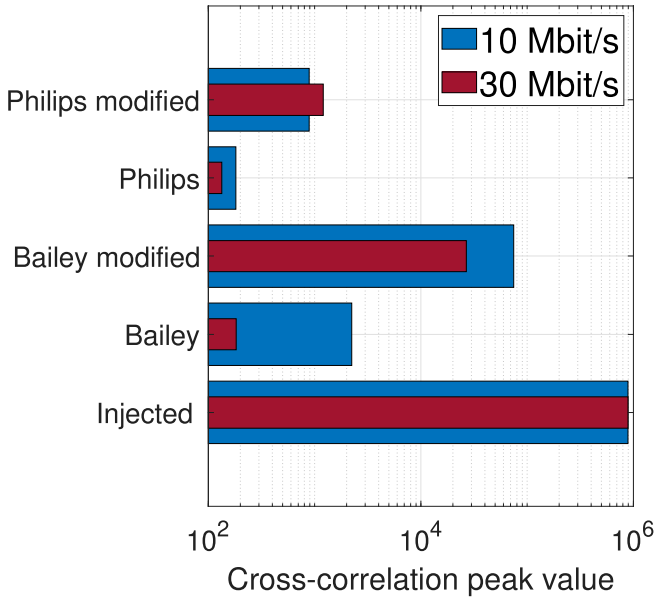


Figure 4.16: Cross-correlation peak values of received PRBS signal for the modified LED bulbs at 10 Mbit/s and 30 Mbit/s.

4.5 Physical layer security of PLC system in the presence of a non-legitimate optical system

In the previous sections of this chapter, we validate that a LED bulb can be considered as a security risk to PLC network. The attacker can easily exploit the natural presence of domestic LED bulbs that are connected to powerline to eavesdrop on PLC data. In this section, another scenario is studied. The physical layer security of PLC system in the presence of non-legitimate VLC system is studied taking into account the mobility of the optical receiver. This is a preliminary study based on information theory. Hence, in section 4.5.1, the system model is described. The average secrecy capacity is derived using numerical simulation and an analytical expression in section 4.5.2. Finally in section 4.5.3 the results are presented and discussed.

4.5.1 System model

In this model, we considered that the wiretap is of type Csiszar and Korner channel [16]. This type of channel considers that the legitimate and the non legitimate channels are independent as seen in Section 2.5 in Chapter 2. It has a star configuration (see section 2.5.1 as the broadcast scenario. Fig. 4.19 shows the system configuration. As it can be seen, the legitimate PLC system is composed of two nodes: the source node (Alice) and the legitimate receiver (Bob). The

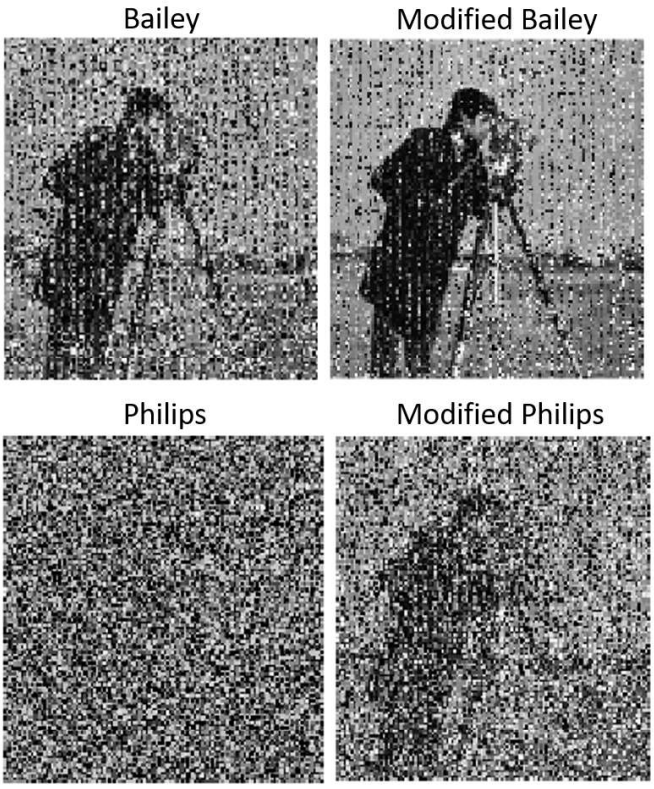


Figure 4.17: Comparison between the received images through the side channel for Bailey and Philips LED bulbs before and after modification.

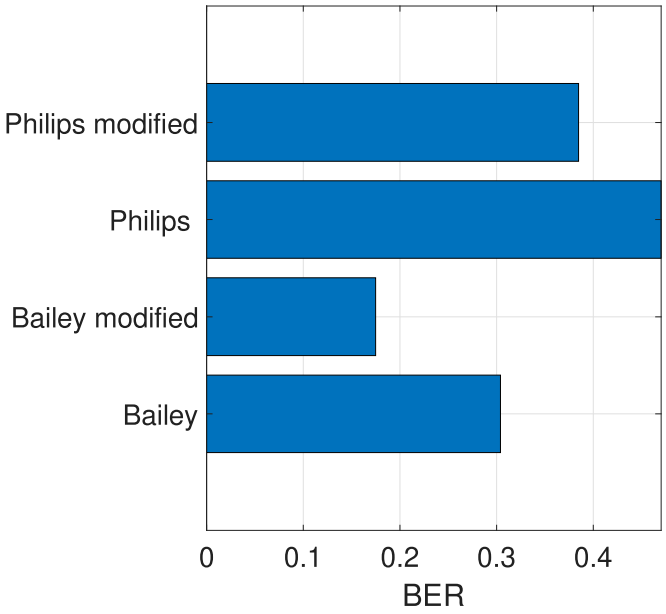


Figure 4.18: BER comparison before and after modifying the drivers of Bailey and Philips LED bulbs.

eavesdropper is a VLC subsystem connected to the powerline which can be the same VLC subsystem described in chapter 3. Alice should transmit a private message to Bob keeping it

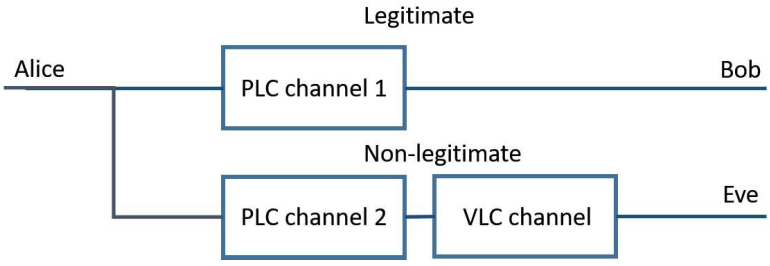


Figure 4.19: a PLC system in the presence of an optical eavesdropper.

totally secret from Eve. The received signal at the legitimate destination (Bob) can be expressed by the following expression [29]:

$$y_{Bob} = \sqrt{P_s} e^{-\alpha_1 d_{PLC1}} h_{PLC1} s + n_{PLC1} \tag{4.6}$$

where P_s is the source transmitted power, d_{PLC1} is the PLC link length, h_{PLC1} is the PLC complex channel gain. The magnitude of the channel coefficients of the PLC channel is considered log-normal having a mean μ and a variance σ, s is the transmitted signal normalized to its average power, α_1 denotes the PLC channel attenuation factor and is given by $\alpha_1 = a_0 + a_1 f^k$,

where a_0 and a_1 are constants determined by measurements, f is the system operating frequency and k is the exponent of the attenuation factor, and n_{PLC1} is the PLC noise at the legitimate destination which can be considered complex Gaussian with a zero mean and a variance σ^2_{PLC1}. For a given channel coefficient, the SNR at the legitimate receiver side can be expressed based on expression (4.6) as:

$$\gamma_{Bob} = \frac{P_s e^{-2\alpha_1 d_{PLC1}} |h_{PLC1}|^2}{\sigma^2_{PLC1}} \tag{4.7}$$

The signal received at the non-legitimate node (Eve) crosses the PLC channel then the VLC channel from where it can be expressed as follows [29]:

$$y_{Eve} = h_{VLC}\left(\sqrt{P_s} e^{-\alpha_2 d_{PLC2}} h_{PLC2} s + n_{PLC2}\right) + n_{VLC} \tag{4.8}$$

where h_{VLC} is the VLC channel gain taking into account only the LOS. The VLC channel is randomly distributed according to the receiver location which follows a uniform distribution, n_{VLC} represents noise that is assumed to be a additive white Gaussian noise with zero mean and variance σ^2_{VLC}, h_{PLC2} represents the PLC channel gain which is similar to h_{PLC1}. This channel follows also a log-normal distribution with a mean μ_{PLC2} and a variance σ^2_{PLC2}, n_{PLC2} is the PLC noise at the end of the PLC2 node which is considered complex Gaussian with a zero mean and a variance σ^2_{PLC1}. The SNR at Eve can be calculated as for given channels coefficient (h_{PLC2} and and h_{VLC}):

$$\gamma_{Eve} = \frac{P_s e^{-2\alpha_2 d_{PLC2}} |h_{PLC2}|^2 |h_{VLC}|^2}{|h_{VLC}|^2 \sigma^2_{PLC2} + \sigma^2_{VLC}} = \frac{P_s e^{-2\alpha_2 d_{PLC2}} |h_{PLC2}|^2}{\sigma^2_{PLC2} + \frac{\sigma^2_{VLC}}{|h_{VLC}|^2}} \tag{4.9}$$

4.5.2 Average secrecy capacity

In our scenario we assumed that the channel state information is unknown at the source. Therefore, the average secrecy capacity which is given for a bandwidth of 1 MHz, can be written as [31]:

$$\bar{C_s} = [E[C_{Bob}] - E[C_{Eve}]]^+ \tag{4.10}$$

where C_{Bob} and C_{Eve} are the destination and the eavesdropper capacity for given channel coefficients that can be expressed as follows:

$$C_{Bob} = \log_2(1 + \gamma_{Bob}) \tag{4.11}$$

and

$$C_{Eve} = \log_2(1 + \gamma_{Eve}) \tag{4.12}$$

In order to elaborate an analytical expression of the average secrecy capacity, we refer to [83] and [29] that calculate the analytical expression of the mean capacity of PLC and PLC-VLC systems.

4.5.2.1 Average capacity at Bob

The average capacity at Bob is calculated as:

$$\bar{C}_{Bob} = \int \log_2(1+\gamma_{Bob}) f_{\gamma_{Bob}}(\gamma_{Bob}) d\gamma_{Bob} \tag{4.13}$$

where $f_{\gamma_{Bob}}$ is the probability density function of γ_{Bob} which can be written as [83] [29]:

$$f_{\gamma_{Bob}}(\gamma_{Bob}) = \frac{\delta}{\sigma\sqrt{8\pi}\sigma} \exp\left(-\frac{\left(\delta \log_2 \gamma_{Bob} - 2(\mu + \delta \log_2 a_1)\right)^2}{8\sigma^2}\right) \tag{4.14}$$

where δ is the scaling constant and it is equal to $\frac{10}{\log_2(10)}$ and $a_1 = \frac{P_s e^{-2\alpha_1 d_{PLC1}}}{\sigma^2_{PLC1}}$. In [83] (4.13) is approximated by the Hermite Gauss quadrature. Considering that:

$$x = \frac{\delta \log_2 \gamma_{Bob} - 2\mu + \gamma_{Bob} \log_n(a_1)}{8\sigma^2} \tag{4.15}$$

Applying the change of variable on the expression (4.13):

$$\bar{C}_{Bob} = \int_{-\infty}^{\infty} \frac{1}{\pi} h_{PLC1}(x) \exp(-x^2) dx \tag{4.16}$$

Using Hermite-Gauss quadrature C_{Bob} can be approximated as following:

$$\bar{C}_{Bob} = \sum_{n=1}^{N_p} \frac{1}{\sqrt{\pi}} H_{x_n} h_{PLC1}(x_n) \tag{4.17}$$

where H_{x_n} and x_n are the weight factors and zeros of the Np-order Hermite polynomial $h_{PLC1}(x_n)$ is expressed as follows:

$$h_{PLC1}(x_n) = \log_2\left(1 + \exp\frac{\sqrt{8\sigma x_n + 2\mu + \delta \log_2 a_1}}{\sigma}\right) \tag{4.18}$$

4.5.2.2 Average capacity at Eve

The average capacity at Eve can be written as:

$$\bar{C}_{Eve} = \int \log_2(1+\gamma_{Eve}) f_{\gamma_{Eve}}(\gamma_{Eve}) d\gamma_{Eve} \tag{4.19}$$

where γ_{Eve} in (4.9) can be expressed as:

$$\gamma_{Eve} = \frac{A}{b+C} \tag{4.20}$$

So the average secrecy capacity can be rewritten as:

$$\bar{C}_{Eve} = E\left(\log_2(1+\frac{A}{b+C})\right) = \int_0^\infty \frac{1}{z}(1-M_A(z))M_{C+b}(z)dz \tag{4.21}$$

where $M_A(z)$ and $M_{b+C}(z)$ denote the moment generation function of random variables A and $C+b$. $M_A(z)$ is given by:

$$M_A(z) = M_{|h_{PLC2}|^2 P_s e^{2\alpha d_{PLC2}}} \tag{4.22}$$

where $M_{|h_{PLC2}|^2}$ is the moment generation function of $|h_{PLC2}|^2$. As h_{PLC2} follows a log-normal distribution, $M_{|h_{PLC2}|^2}$ can be estimated based on Hermite polynomial [29]. Hence $M_A(z)$ is expressed as:

$$M_A(z) = \frac{1}{\pi}\sum_{n=1}^{N_p} H_{x_n} \exp(10^{\frac{-\sqrt{22}\sigma_{h_{PLC2}} x_n + 2\mu_{h_{PLC2}}}{10}} P_s e^{-2\alpha d_{PLC2}} z) \tag{4.23}$$

Moving now to the VLC channel, it can be modeled using the expression (2.8) presented in chapter 2. However, in our scenario, we considered that the optical receiver is mobile inside a room. Thus, D can be written:

$$D = \sqrt{d^2+r^2} \tag{4.24}$$

where d is the vertical distance between the LEDs and the optical receiver plane and r is the position of the optical receiver in the horizontal plane. We assume that the position of the optical receiver is uniform on a circle of radius R and the probability density function of the distance r is [29]:

$$f_R(r) = \frac{2r}{R^2} \tag{4.25}$$

where R is the maximum radius of the LOS. Hence, $\cos^m(\phi)$ and $\cos(\psi)$ that are described in (2.4) in Chapter 2 are now equal to $\frac{D}{\sqrt{d^2+r^2}}$. To simplify the expression, it is assumed that $Q = \frac{m+1}{2\pi} AGSH_{LED}N_{LED}$ detailed in (2.8) and (2.4). In order to calculate the moment generation function of C which is equal to $\frac{\sigma^2_{PLC2}}{|h_{VLC}|^2}$, [29] expressed the moment generation function of $\frac{1}{|h_{VLC}|^2}$ as following:

$$M_{\frac{1}{|h_{VLC}|^2}} = \frac{(Q(m+1)L^{m+1})^{\frac{2}{m+3}}}{(m+3)r^2} \times \cdots \left(z^{\frac{-1}{m+3}}\Gamma\left(\frac{1}{m+3}, \frac{d^4 z}{Q^2(1+m)^2}\right) z^{\frac{-1}{m+3}}\Gamma\left(\frac{1}{m+3}, \frac{d^{-2(m+1)}(L^2+r^2)^{m+3}z}{Q^2(1+m)^2}\right)\right) \tag{4.26}$$

where $\Gamma(\cdot)$ is the upper incomplete gamma function. The moment generation function of $b+C$ can now be written as:

$$M_{b+C} = \frac{\left(\frac{\sigma_d^2}{G^2}z\right)^{\frac{-1}{m+3}}}{(m+3)r^2}\left(Q(m+1)L^{m+1}\right)^{\frac{2}{m+3}} \times \cdots \\ \left(\Gamma\left(\frac{1}{m+3}, \frac{d^4\sigma_{PLC2}^2 z}{Q^2(1+m)^2G^2}\right) - \Gamma\left(\frac{1}{m+3}, \frac{d^{-2(m+1)}(d^2+r^2)^{m+3}\sigma_{PLC2}^2 z}{Q^2(1+m)^2G^2}\right)\right) \tag{4.27}$$

C_{Eve} can be calculated using the expressions of M_A and M_{b+C}. After finding the expressions of C_{Bob} and C_{Eve}, the average secrecy capacity can be calculated according to (4.10).

4.5.3 Results and validation

In this section, a comparison is made between the secrecy capacity obtained using Monte-Carlo simulation of (4.7) and (4.9) and that obtained using the analytical developments. The parameters of the considered scenario are unless indicated, otherwise listed in table 4.4. It should be noted that the rest of the VLC system parameters are taken following table 3.3 in chapter 3 Fig. 4.20 shows the secrecy capacity obtained using the analytical expressions and

Parameters	Value
a_0	2×10^{-3}
a_1	3.57×10^{-7}
k	0.7
d_1 and d_2	30 cm
$h_{PLC1}$and h_{PLC1}	log-normal(0,1)
σ_{PLC1} and σ_{PLC1}	1
R	7 m
d	2.25 m
N_{LED}	60 red LED
P_s	1 W
f	2 MHz

Table 4.4: Parameters of the proposed scenario.

using Monte-Carlo simulation according to the transmitted power. A perfect match can be noticed between the calculated and the simulated values. It can be perceived also that the average secrecy capacity increases with the transmitted power. For example, when the length of the powerline cable separating Alice from the VLC transmitter is d_{PLC2} = 10 m, the average secrecy capacity increases from 0.3 bit/s/Hz at 1 W to 1.15 bit/s/Hz at 10 W. In addition, the position of the VLC system on the PLC network can affect the average secrecy capacity. Fig. 4.20 presents also the average secrecy capacity according to the transmitted power in three different conditions: *i*) the length of the PLC2 cable is shorter than that of PLC1 d_{PLC2} = 10 m, *ii*) the length of the PLC2 cable is equal to that of PLC1 d_{PLC2} = 30 m, *iii*) the length of PLC2

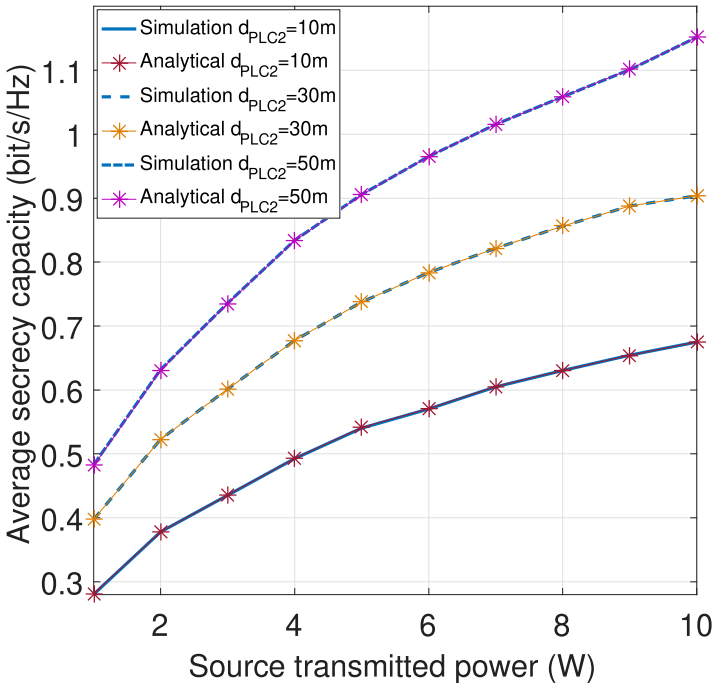


Figure 4.20: Comparison between the analytically calculated and the simulated average secrecy capacity in function of the transmitted power for different PLC2 cable lengths.

cable is longer than that of PLC1 $d_{PLC2} = 50$ m. The average secrecy capacity increases with the distance increase. For example, for a transmitted power of 10 W the secrecy capacity increases from 0.78 bit/s/Hz in the case *i*) to 0.9 bit/s/Hz in the case *ii*) and 1.15 bit/s/Hz in the case *iii*). Moreover, the vertical distance d between the LED array and the optical receiver influences the secrecy capacity. Fig. 4.21 shows the simulated and the analytically calculated average secrecy capacity according the distance d. It is obvious that the average secrecy capacity increases with the distance d increase. The average secrecy capacity at $P_s = 1$ increases from 0.28 bit/s/Hz at a distance of 1 m to 0.42 bit/s/Hz at when the distance becomes 7 m.

4.6 Conclusion

This chapter investigates a new side channel that may threaten the PLC network. The leakage of the PLC signal through domestic LED bulbs is studied based on experimental trials. In addition, a theoretical study based on physical layer security is made in order to assess the secrecy capacity of a PLC network in the presence of non legitimate VLC system.

The electrical-optical side channel is characterized by measuring the side channel frequency response. Furthermore the power spectral density of the received signal through the side channel when two PLC modems are connected to the same powerline that power the domestic LED bulbs. In addition, the cross-correlation of the received signal through the side

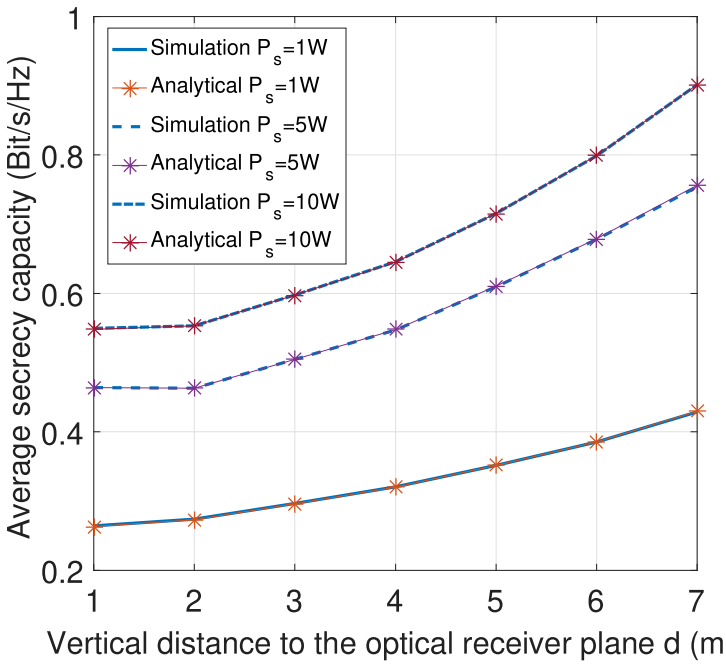


Figure 4.21: Comparison between the analytically calculated and the simulated average secrecy capacity depending on the length between the LED array and the optical receiver for different transmitted power values.

channel is calculated after transmitting a PRBS signal through the powerline network in order to precisely characterize the channel. The results show that LED bulbs with AL drivers have larger bandwidth and are more capable of naturally leaking PLC signals than LED bulbs with SMPS drivers. A DMT signal is transmitted through the powerline network where the LED bulbs are connected. The BER of the received signal through the side channel are calculated. The results show that the LSC LED bulb with AL driver is the most leaky bulb among all bulbs tested with a BER of 0.2. However, the LED bulbs having SMPS drivers cannot be transmit DMT signal.

After testing the natural leakage of the PLC signals through domestic LED bulbs, intentional modifications are made to the LED driver to check if it is possible to increase the leakage. These changes are simple and do not affect the original function of the driver. The channel characteristics are determined in addition to the BER. The results prove that these simple modifications are capable of significantly increasing the leakage, especially in the case of AL drivers.

Physical layer security of the PLC system is studied in the case where a non-legitimate VLC transmitter is connected to the PLC network. The average secrecy capacity is calculated based on analytical expressions. The calculated secrecy capacity is later compared to simulation results when a perfect match is found. Moreover, the obtained results revealed that the secrecy

capacity increases with transmitted power, with the length of the powerline cable of the non legitimate channel, and with the vertical distance separating the LEDs from the optical receiver.

Chapter 5

General conclusion

This thesis studies the possibility of directly integrating the PLC and the VLC broadband systems without the need to have a stage that demodulates and remodulates the PLC signal before transmitting it to the VLC system. It tests also the ability of domestic LED bulbs to leak PLC signals and threaten the security of the in-home PLC network.

Hence, an overview of the VLC and the PLC systems is provided in the literature review. The main PLC and VLC physical layer parameters that are specified in each of their standards are presented. The characteristics of PLC and VLC channels and modeling approaches are also given. Additionally, the different types of noise that can affect PLC and VLC signals are listed. The most commonly used techniques for generating white light are also interpreted to highlight techniques that can facilitate the employment of the VLC in indoor LED lighting. The state of the art of the PLC-VLC system is presented. The most common relay techniques that can be used to combine PLC and VLC systems are described. The PLC-VLC hybrid channel model is also provided. Additionally, side channel attacks are covered, followed by a brief survey of the existing side channel classes and the countermeasures that can be applied. Finally, the topic of physical layer security is introduced considering the main types of wiretap channels. The fundamental metrics used to assess the physical layer security are presented as the equivocation rate, the secrecy rate, and the secrecy capacity.

As mentioned above, two topics are addressed in this thesis: (i) the implementation of a simple high-bandwidth and low-cost PLC-VLC system that does not require a decoding/re-encoding phase between the two subsystems. (ii) The in-home PLC signal leakage through domestic LED bulbs. Thus, the main attainments in the first topic can be summarized as follow:

1. The frequency characteristics of monochromatic LEDs (red, green, and blue) are measured. The obtained results show that the red LED has the largest bandwidth (20 MHz). It is noticed that the LEDs have a frequency response that matches a first order low pass filter. In addition the frequency impedance measurements show that at low frequen-

cies, the LED impedance acts as a simple resistor until reaching a certain frequency when a capacitive behavior begins to appear, and at high frequencies, the inductance components starts to arise as the impedance begin to increase with the increase of the frequency;

2. an equivalent circuit model of the LEDs is elaborated. The components' values are estimated based on the measurements of the LED frequency characteristics. This method showed good accuracy when modeling the blue LEDs. However, the green and red LEDs need a more complicated circuit in order to obtain an impedance that matches the measured one;

3. an explicit expression is developed to accurately model the VLC system taking into account its optical, electrical, and frequency behavior. This expression describes the relationship between the current flowing through the LED and the voltage at the output of the optical receiver. The comparison between the results obtained using this expression and those measured shows an error of 22% which is acceptable regarding the testbed characteristics and can help when designing an optical receiver;

4. a simple PLC-VLC system is implemented using commercial HPAV modems and a monochromatic VLC system. The possibility of transmitting the HPAV signal through the VLC system without modifying the signal is demonstrated with a maximum bit rate of 66 Mbit/s;

5. The test bed results based on the use of a single red LED are extrapolated to real scenarios based on a theoretical study. The results show that 60 red LEDs are needed to ensure a maximum throughput of 66 Mbps inside a typical room. This number is lower than the number required to light the room with an RGB LED array (71 red LEDs). These results verify that it is possible to provide lighting and communication simultaneously without increasing the number of LEDs.

The most significant findings of the second topic are recapped as follows:

1. The natural leakage of the PLC signal through domestic LED bulbs is studied. The frequency response of the electrical-optical side channel is measured. In addition, the power spectral density of the received signal through LED bulbs when two PLC modems are connected to the same powerline that power the bulbs is also measured. Moreover, the cross-correlation of the received signal through the side channel is calculated after transmitting a PRBS signal through the powerline network in order to precisely characterize the channel. These channel characterization methods show that there are some AL LED bulbs that can naturally leak PLC signal (LSC, Lexman, LSC, etc.). However, SMPS LED bulbs have a narrower bandwidth which can obstruct leakage;

2. a DMT signal with a modulation bandwidth of 2-30 MHz is transmitted through the electrical-optical side channel. The BER of the received signal is calculated for each of the tested LED bulbs. The results show that in the case of AL LED bulbs, the BER varies between 0.2 and 0.36. However, the BER in the case of SMPS LED bulbs is approximately 0.4. These results validate again that AL LED bulbs are more prone to leak naturally;

3. intentional modifications are performed to two LED bulbs having AL and SMPS drivers in order to check the possibility of enhancing the leakage. After the drivers modifications, the channel characteristics and the BER are determined. The results reveal that these modifications can significantly increase the leakage especially in the case of AL LED bulbs;

4. the physical layer security of the PLC system, when a malicious VLC transmitter is plugged into the same powerline network with the PLC modems, is studied. The average secrecy capacity is calculated using an analytical expression and using Monte-Carlo simulations. The results show a perfect match betwen the calculated and the simulated secrecy capacity. It shows also that the average secrecy capacity increases with the transmitted power, with the powerline cable length of the wiretap channel, and with the vertical distance separating the LEDs from the optical receiver.

Based on the obtained findings, the following directions for future research work can be suggested:

1. Find a more accurate LED equivalent circuit model that has a magnitude and a phase that can perfectly match the measured ones;

2. elaborate an expression that models the VLC system and takes into account the effect of the LED junction temperature;

3. implement a large scale PLC-VLC test bed in order to perform experimental tests to evaluate the performance of the proposed system instead of theoretical studies (increase the number of LEDs, increase the distance between the optical transmitted and receiver, environment, etc.);

4. test more brands of LED bulbs to see if there are other LEDs that leak more than the LEDs tested in this thesis;

5. study the physical layer security of the PLC system in the case of a finite blocklength regime.

Appendix A

Circuit design

A.1 Wide-band bias tee

The bias Tee for VLC is a circuit that allows the injection of a DC signal in order to determine the operating point of LED on the basis of the LI curve and an AC signal containing the information to be transmitted. A bias tee can be thought of as a diplexer with an ideal capacitor that allows AC through but blocks the DC bias and an ideal inductor that blocks AC but allows DC. Conceptually, the simplest bias tee is just a coupling capacitor and an inductor (fig. A.1).

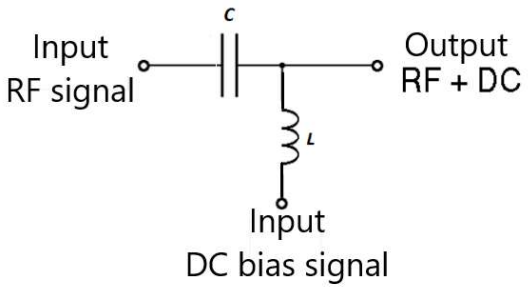


Figure A.1: Simple bias tee schema.

The major obstacle one may face when designing a wide-band bias tee is achieving high DC side performance while ensuring the desired bandwidth on the AC side. Indeed, obtaining a wide bnadwidth on the AC side requires a bias tee capable of blocking the AC component on the DC side over several decades of frequency and at a cut-off frequency lower than the lowest frequency that we want to inject into the AC part. However, these two conditions are difficult to be achieved simultaneously a using a single inductor due to its self resonance at high frequencies. This is because the inductor after a certain frequency called the resonant frequency starts behaving like a capacitor (fig. A.2) which can ruin the desired function of the designed circuit at frequencies higher than the resonant frequency.

One of the best solutions is to design a series of damped lowpass filter sections where

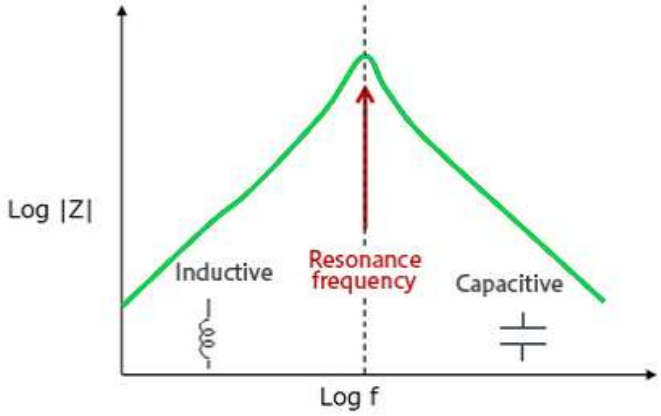


Figure A.2: The frequency impedance of an inductor.

each inductor is only required to operate over a little more than one decade of frequency. This technique guarantees a low-pass behavior over the entire bandwidth as can be seen in fig. A.3.

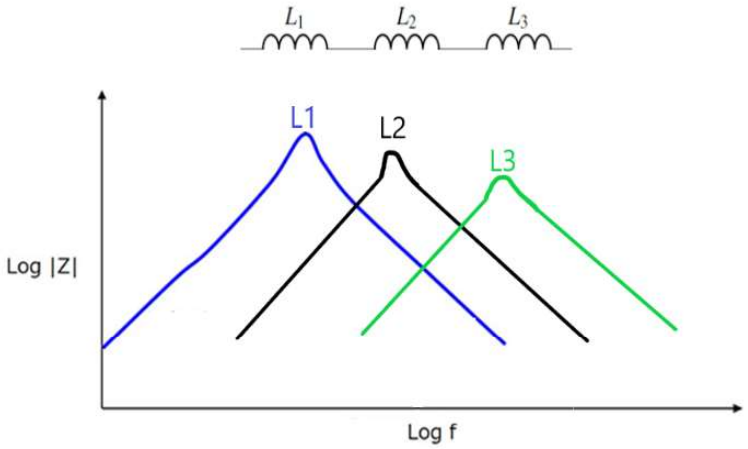


Figure A.3: The frequency impedance of three inductors having different values.

A.1.1 Bias tee design

We designed a bias tee of a bandwidth of 20 kHz-100 MHz which is able to bias the LED by a 120 mA DC current. The value of the capacitor can be calculated using the following expression:

$$C = \frac{1}{2\pi f_c R} \tag{A.1}$$

where f_c is the cutoff frequency for the AC side and R is the sum of source and load impedance. In our case, we consider that we have a load impedance of 50 Ω. It should be noted that to

avoid the self-resonance of capacitors, two parallel capacitors are used. The two capacitors are of different ranges. The first is of the order of a hundreds of nF and the second is of the order of tens of nF. The inductance value can be calculated using the following expression:

$$L = \frac{R}{2\pi f_l} \tag{A.2}$$

where f_l is the cutoff frequency for the DC side. To avoid the self resonance frequency, we used three inductors in series that are also of different ranges. The two cutoff frequencies f_c and f_l should verify the following in-equation:

$$f_l < f_c \tag{A.3}$$

A.1.2 Simulation results

After some experimentation using Orcad, the bias tee design is designed as shown in fig. A.4. As can be seen, the resistors $R3$, $R4$, $R5$, and $R6$ are used in series instead of using a single resistor of 45 Ω in order to reduce the effects of the parasitic elements that can exist in a large resistor and that can have a significant influence on circuit performance. The zero resistors $R12$, $R13$, $R14$, and $R15$ are used in order to be able to chose the LED a single LED from the used RGB module [65]. The SMA output (2) is designed to be able to measure the current flowing through the LED. The results of the simulated circuit that takes into account the resonance effect are shown in fig. A.5. The fig. A.5a shows that the low pass filter on the DC side has a cutoff frequency at −3 dB from 19 kHz. The curve of fig. A.5b shows that the AC side high pass filter has a cutoff frequency of 18.6 kHz at −3 dB and has a flat response up to 100 MHz. This means that the designed bias tee can easily operate between 20 kHz and 100 MHz. It worth to mention that the simulated results are validated by measurements after the circuit implementation.

A.2 Optical receiver

The optical receiver is mainly composed of a TIA, a high pass filter, and voltage amplifier. The TIA is a circuit used to amplify and transform the light-dependant current of photodiodes to voltage. The design of a transimpedance amplifier should take into account many considerations like the stability of the circuit, the bandwidth, input and output voltage range limitations, etc. The most simple TIA is composed of a operational amplifier (op-amp) and a feedback resistor R_{ref} (see fig. A.6). In the fig. A.6 the photodiode operates in the photoconductive mode: an external reverse bias (V_r) is applied to the photodiode. The photodiode is connected in a way that its current increases the output voltage of the op-amp. In order to ensure the stability of the TIA a feedback capacitor C_F should be used. This capacitor compensates for

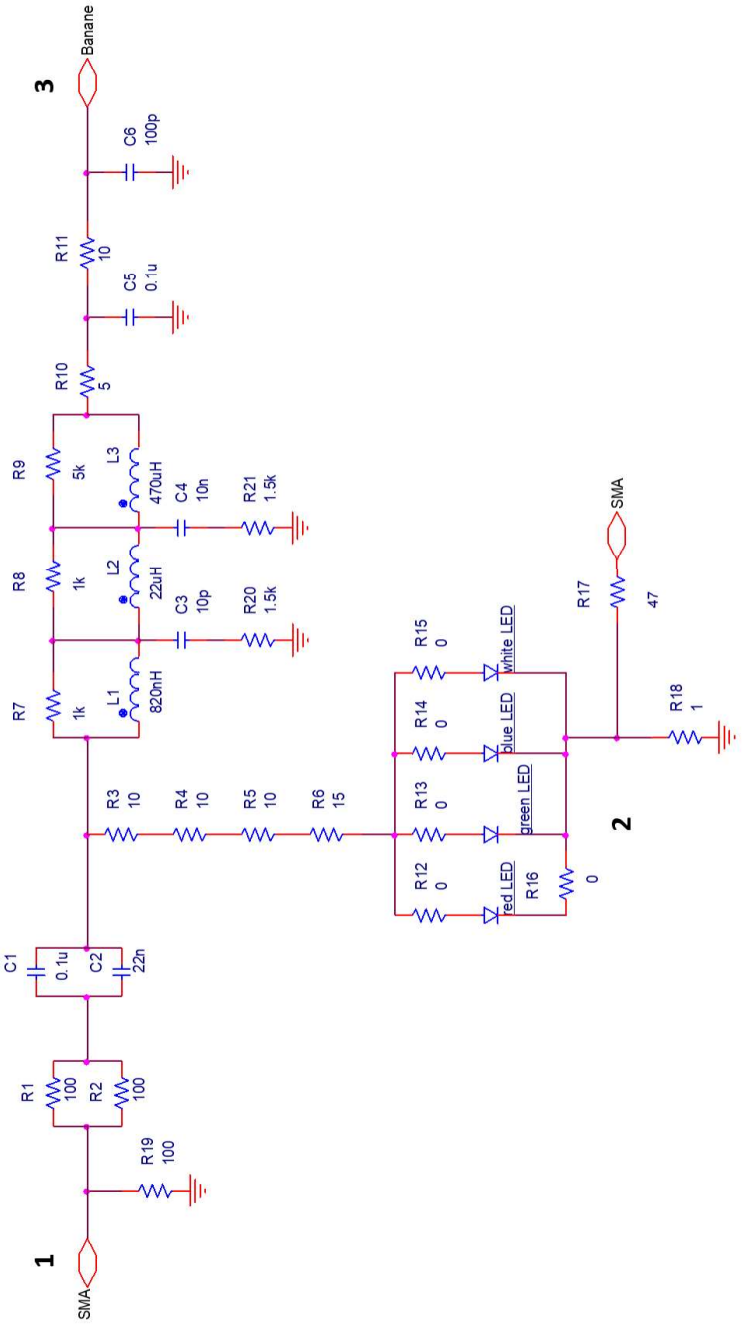


Figure A.4: The designed bias tee circuit

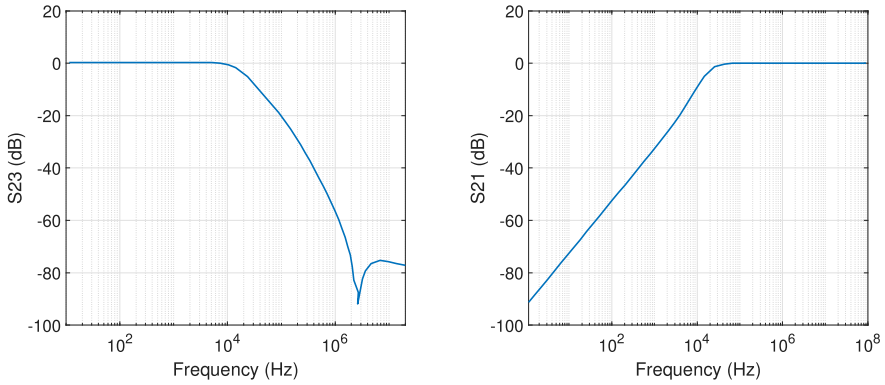


Figure A.5: The s parameters of the designed bias tee (a) $S23$. (b) $S21$.

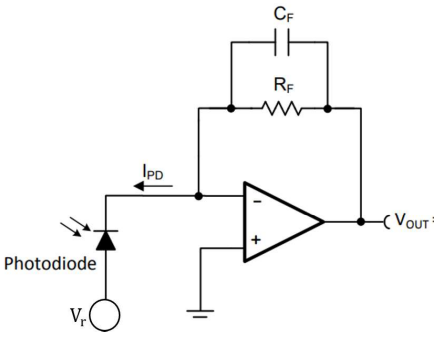


Figure A.6: Simple TIA schema

the photodiode capacitance at the inverting input of the op-amp.

A.2.1 Circuit design

Before starting the TIA design, the photodiode should be chosen. In our case, we chooses the SFHSFH2400-Z [75] that has a maximum sensitivity of 0.65 A/W and a photocourrent of 10 uA at a reverse voltage of 5 V and a illuminace of 1000 lx.

The gain of the TIA is calculated after setting the maximum desired output voltage and following this equation [8]:

$$R_F = \frac{V_{out}}{I_{PD}} \tag{A.4}$$

where I_{PD} is the maximum current generated by the photodiode when it is exposed to light. The feedback capacitor, in combination with the feedback resistor, forms a pole in the frequency response of the amplifier [8]:

$$f_p = \frac{1}{2\pi R_F C_F} \tag{A.5}$$

Above this pole frequency, the amplification of the circuit will decline. The maximum feedback capacitor value can be determined using the feedback resistor value and the desired bandwidth [8]:

$$C_F < \frac{1}{2\pi R_F f_p} \tag{A.6}$$

a compromise between bandwidth and gain must be found otherwise additional stages must be added. To validate the stability of the op-amp, the intersection frequency between the open loop gain of the amplifier and the inverse feedback factor f_I should be greater than f_p [8]. f_I can be expressed by the following expression:

$$f_I = \frac{C_F}{C_{IN} + C_F} f_{GBW} \tag{A.7}$$

where C_{IN} is the sum of the junction capacitance of the photodiode, the differential and common-mode input capacitances of the amplifier. f_{GBW} is the unity gain bandwidth of the op-amp. Thus, to ensure the stability of the amplifier f_{GBW} must obey the following in-equation [8]:

$$f_I > f_p \tag{A.8}$$

if we replace f_p and f_I by their expressions (A.5) and (A.7) respectively, we arrive at the useful in-equation that allow us to chose the right op-amp [8]:

$$f_{GBW} > \frac{C_{IN} + C_F}{2\pi R_F C_F^2} \tag{A.9}$$

A.2.2 Simulation results

In our case, we need a bandwidth of at least 30 MHz and a gain of at least 0.2 MΩ. These two conditions are difficult to be reached using a single stage TIA. Hence, we propose a three stages circuit in which the first stage is a typical TIA, the second and the third are voltage amplifiers with high pass filters (see fig. A.7). It can be seen from fig. A.7 that the third stage can be connected or not depending on the desired bandwidth and gain. It should also be mentioned that some additional components are added to the circuit after simulation on orcad in order to guarantee a stable system with the desired behavior.

A time and a frequency domain simulations are performed using Orcad. The signals at the output of each stage are visualized in order to ensure that the amplifiers are stable (fig. A.8). A rectangular current of 5 MHz is set at the input of the TIA (fig. A.8a). Figs. A.8b, A.8c, and A.8d show the voltage signal at the output of each stage of the amplifier. It is noticed that the amplified signals retain the same shape as the injected current and the overshoot at the transition phases between the two extremums is acceptable. Moreover, this simulation can give a prior validation of the stability of the circuit. Fig. A.9 depicts the frequency gain of the optical receiver at the second (fig A.9a) and the third stages (fig. A.9b). These figures show that our circuit has a bandwidth of 70 MHz at −3 dB. It should be noted that in our testbed we used only the first and the second stages of the circuit.

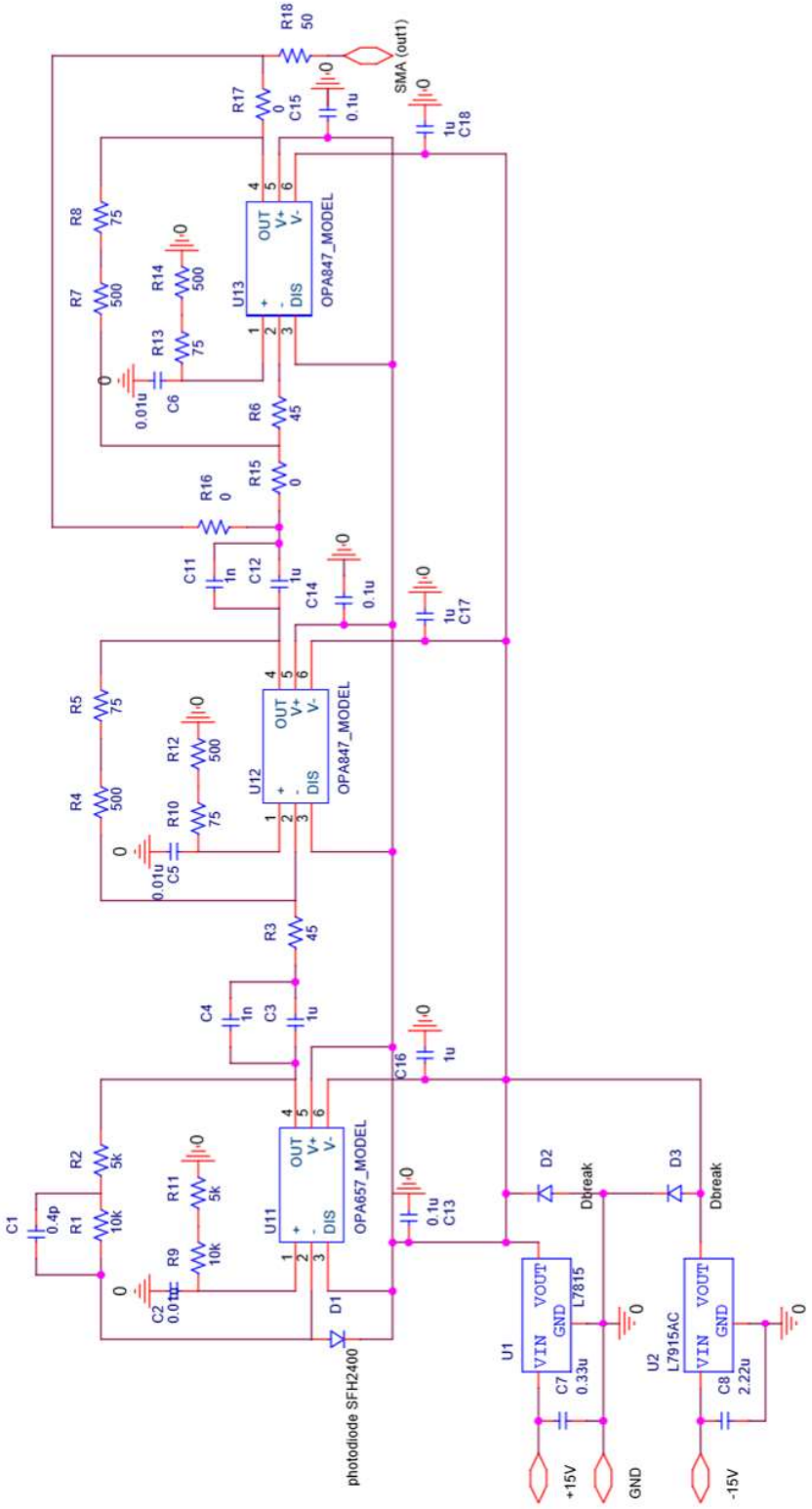
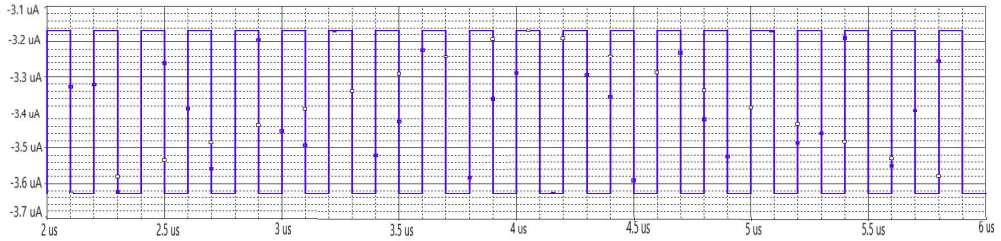
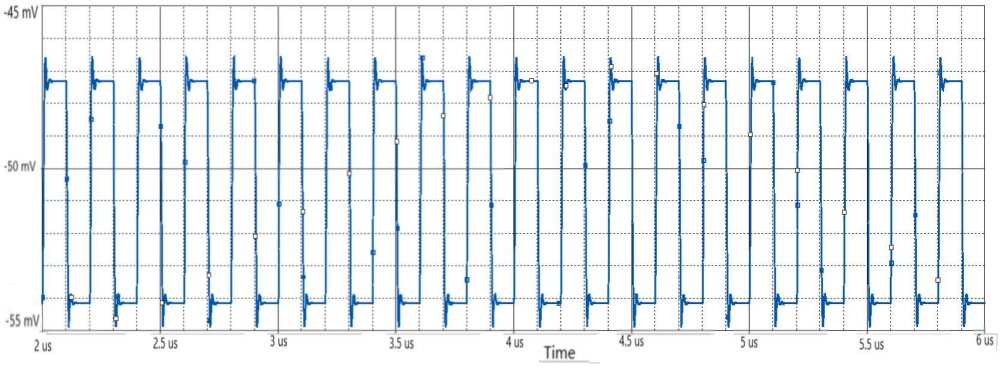


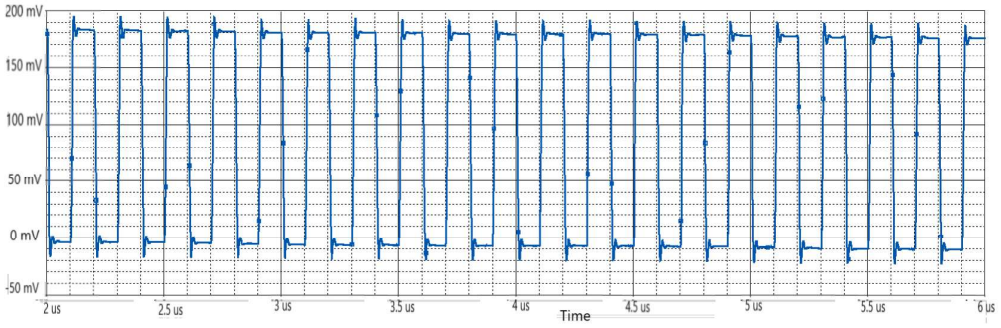
Figure A.7: Our designed TIA schema



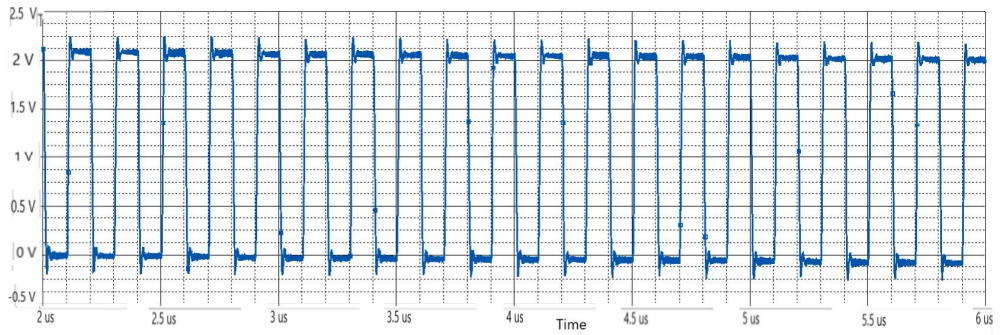
(a)



(b)

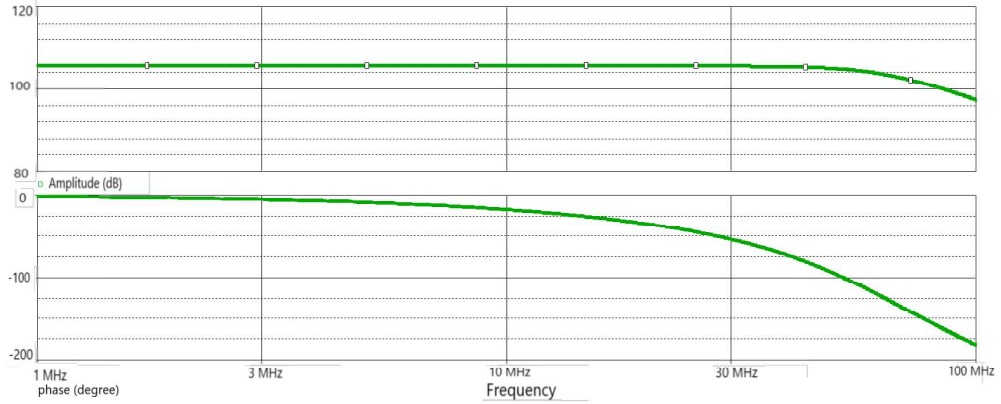


(c)

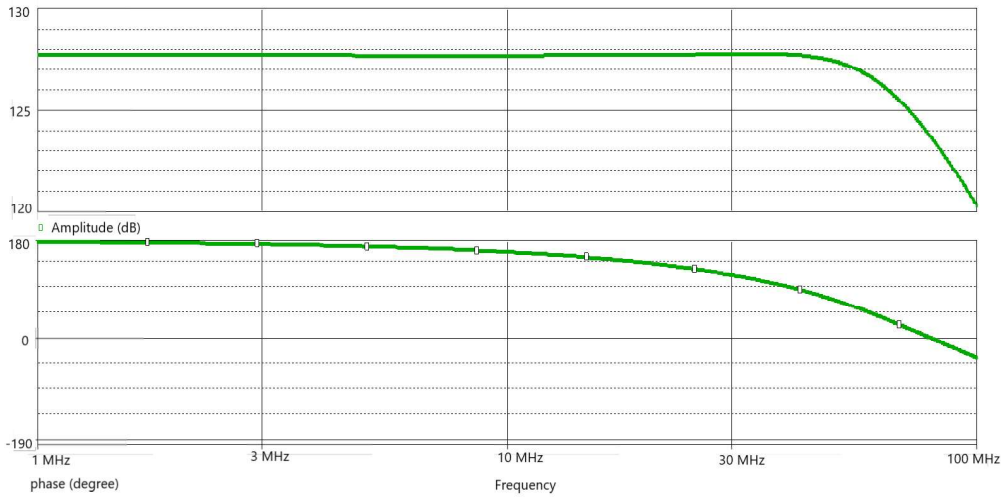


(d)

Figure A.8: Time domain simulation results of the signals at the output of each stage of the optical receiver (a) The photodiode current. (b) The Voltage at the output of the first stage. (c) The voltage at the output of the second stage. (d) The voltage at the output of the third stage.



(a)



(b)

Figure A.9: The frequency gain of the optical receiver at each of its stages. (a) The gain after the second stage (b) The gain after the third stage

Bibliography

[1] D. Asonov and R. Agrawal. Keyboard acoustic emanations. In *IEEE Symposium on Security and Privacy*, pages 3–11, 2004.

[2] Anindya Auddy and Sapnesh Sahu. Tempest: Magnitude of threat and mitigation techniques. In *10th International Conference on Electromagnetic Interference & Compatibility*, pages 603–611, 2008.

[3] Ali Waqar Azim. *Signal Processing Techniques for Optical Wireless Communication Systems*. Theses, Université Grenoble Alpes, September 2018.

[4] Michael Backes, Tongbo Chen, Markus Duermuth, Hendrik P.A. Lensch, and Martin Welk. Tempest in a teapot: Compromising reflections revisited. In *30th IEEE Symposium on Security and Privacy*, pages 315–327, 2009.

[5] Michael Backes, Markus Dürmuth, Sebastian Gerling, Manfred Pinkal, and Caroline Sporleder. Acoustic side-channel attacks on printers. In *USENIX Security Symposium*, 2010.

[6] Michael Backes, Markus Dürmuth, and Dominique Unruh. Compromising reflections-or-how to read lcd monitors around the corner. In *IEEE Symposium on Security and Privacy*, pages 158–169, 2008.

[7] Bright Power Semiconductor. *BP2861XK Non-isolated Buck Offline LED Driver*.

[8] John Caldwell. *1 MHz, Single-Supply, Photodiode Amplifier ReferenceDesign*. Texas Instruments, November 2014.

[9] Francisco J. Canete, Jose A. Cortés, Luis Diez, and Jose T. Entrambasaguas. A channel model proposal for indoor power line communications. *IEEE Communications Magazine*, 49(12):166–174, 2011.

[10] Jeffrey B. Carruthers and Joseph M. Kahn. Multiple-subcarrier modulation for nondirected wireless infrared communication. *IEEE J. Sel. Areas Commun.*, 14:538–546, 1996.

[11] Ignacio Castro, Aitor Vazquez, Manuel Arias, Diego G. Lamar, Marta M. Hernando, and Javier Sebastian. A review on flicker-free ac-dc led drivers for single-phase and three-phase ac power grids. *IEEE Transactions on Power Electronics*, 34(10):10035–10057, 2019.

[12] Dmitry Chizhik, Gerard J. Foschini, and Reinaldo A. Valenzuela. Capacities of multi-element transmit and receive antennas: Correlations and keyholes. *Electronics Letters*, 36:1099–1100, 2000.

[13] J. Clark. An introduction to communications with optical carriers. *IEEE Students' Quarterly Journal*, 36:218–222, June 1966.

[14] Lavaud Corentin, Gerzaguet Robin, Gautier Matthieu, Berder Olivier, Nogues Erwan, and al. Whispering devices: A survey on how side-channels lead to compromised information. *Journal Hardware and Systems Security*, 2021.

[15] Jordi Cosp-Vilella and Herminio Martínez-Garcia. Design of an on-chip linear-assisted dc-dc voltage regulator. In *20th International Conference on Electronics, Circuits, and Systems (ICECS)*, pages 353–356, 2013.

[16] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.

[17] Pierre Degauque, P. Laly, Virginie Degardin, and Martine Lienard. Power line communication and compromising radiated emission. *Proceedings of 18th International Conference on Software, Telecommunications and Computer Networks, SoftCOM*, 7, 01 2010.

[18] devolo AG, Germany. *DLAN 200 AV*, November 2006.

[19] Leonardo de M. B. A. Dib, Victor Fernandes, Mateus de L. Filomeno, and Moises V. Ribeiro. Hybrid plc/wireless communication for smart grids and internet of things applications. *IEEE Internet of Things Journal*, 5(2):655–667, 2018.

[20] Wenbo Ding, Fang Yang, Hui Yang, Jintao Wang, Xiaofei Wang, Xun Zhang, and Jian Song. A hybrid power line and visible light communication system for indoor hospital applications. *Computers in Industry*, 68:170 – 178, 2015.

[21] Deirdre O Donnell. The visible light communication market may exceed us$100 billion in value by 2024.

[22] Yu-Lei Du, Ying-Hua Lu, and Zhang Ling. Novel method to detect and recover the keystrokes of ps/2 keyboard. *Progress In Electromagnetics Research C*, 41:151–161, 01 2013.

[23] Hany Elgala, Raed Mesleh, and Harald Haas. Non-linearity effects and predistortion in optical ofdm wireless transmission using leds. *Int. J. Ultra Wideband Commun. Syst.*, 1:143–150, 2009.

[24] Houqiang Fu and Yuji Zhao. 9 - efficiency droop in gainn/gan leds. In JianJang Huang, Hao-Chung Kuo, and Shyh-Chiang Shen, editors, *Nitride Semiconductor Light-Emitting Diodes (LEDs)*, Woodhead Publishing Series in Electronic and Optical Materials, pages 299–325. Woodhead Publishing, second edition, 2018.

[25] S. Galli and T.C. Banwell. A deterministic frequency-domain model for the indoor power line transfer function. *IEEE Journal on Selected Areas in Communications*, 24(7):1304–1316, 2006.

[26] F. R. Gfeller and U. Bapst. Wireless in-house data communication via diffuse infrared radiation. In *IEEE 67.11*, pages 1474–1486, 1979.

[27] Zabih Ghassemlooy, Murat Uysal, Mohammad Ali Khalighi, Vitor Viterbo, Florian Moll, Stanislav Zvanovec, and Aviceto Belmonte. Overview of Optical Wireless Communications. In *OPTICAL WIRELESS COMMUNICATIONS, AN EMERGING TECHNOLOGY*. Springer International Publishing, August 2016.

[28] Waled Gheth, Khaled Rabie, Bamidele Adebisi, Muhammad Ijaz, and Georgina Harris. On the performance of df-based power/line visible-light communication systems. In *International Conference on Signal Processing and Information Security (ICSPIS)*, pages 1–4, 11 2018.

[29] Waled Gheth, Khaled M. Rabie, Bamidele Adebisi, Muhammad Ijaz, and Georgina Harris. Performance analysis of integrated power-line/visible-light communication systems with af relaying. In *IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, 2018.

[30] F. E. Goodwin. A review of operational laser communication systems. *SPIE milestone series 30*, pages 3–9, 1991.

[31] Praveen Kumar Gopala, Lifeng Lai, and Hesham El Gamal. On the secrecy capacity of fading channels. *IEEE Transactions on Information Theory*, 54(10):4687–4698, 2008.

[32] Akash Gupta, Nikhil Sharma, Parul Garg, and Mohamed-Slim Alouini. Cascaded fso-vlc communication system. *IEEE Wireless Communications Letters*, 6(6):810–813, 2017.

[33] Mordechai Guri, Boris Zadov, Dima Bykhovsky, and Yuval Elovici. Powerhammer: Exfiltrating data from air-gapped computers through power lines. *IEEE Transactions on Information Forensics and Security*, 15:1879–1890, 2020.

[34] Mordechai Guri, Boris Zadov, Andrey Daidakulov, and Yuval Elovici. xled: Covert data exfiltration from air-gapped networks via switch and router leds. In *16th Annual Conference on Privacy, Security and Trust (PST)*, pages 1–12, 2018.

[35] Mordechai Guri, Boris Zadov, and Yuval Elovici. Led-it-go: Leaking (a lot of) data from air-gapped computers via the (small) hard drive led. In *LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED*, pages 161–184, 06 2017.

[36] H. Haas. A guide to wireless networking by light. *Quantum Electronics 55*, pages 88–111, 2017.

[37] Jehad M. Hamamreh, Haji M. Furqan, and Huseyin Arslan. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 21(2):1773–1828, 2019.

[38] HPAV. *HomePlug Power line Aliance*, March 2010.

[39] Luchi Hua, Yuan Zhuang, Longning Qi, Jun Yang, and Longxing Shi. Noise analysis and modeling in visible light communication using allan variance. *IEEE Access*, 6:74320–74327, 2018.

[40] James Ibbetson and Sten Heikman. High voltage low current surface-emitting led. *U.S. Patent 7 985 970 B2*, July 2011.

[41] IEEE. *IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications*, 2010.

[42] IEEE. *IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications*, 2013.

[43] IEEE. *IEEE Standard for Local and metropolitan area networks–Part 15.7: Short-Range Optical Wireless Communications - Redline*, 2019.

[44] ITU. *VLC high speed indoor visible light communication transceiver-system architecture, physical layer and data link layer specification*, 2019.

[45] ITU-T. *Unified high-speed wireline-based home networking transceivers - Power spectral density specification*, 2011.

[46] ITU-T. *Narrowband orthogonal frequency division multiplexing power line communication transceivers for ITU-T G.hnem networks*, 2012.

[47] ITU-T. *Narrowband orthogonal frequency division multiplexing power line communication transceivers for PRIME networks*, 2012.

[48] ITU-T. *Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks*, 2014.

[49] Armstrong J. and Lowery A.J. Power efficient optical ofdm. *Electronic Letters 42(6)*, pages 370–372, 2006.

[50] Ahmad Jabban, Sylvain Haese, and Maryline Helard. Theoretical and experimental optimization of dmt-based visible light communication under lighting constraints. *EURASIP Journal on Wireless Communications and Networking*, 99, 12 2020.

[51] Ruonan Ji, S.-W Wang, Qingquan Liu, and Wei Lu. High-speed visible light communications: Enabling technologies and state of the art. *Applied Sciences*, 8:589, 04 2018.

[52] Eduard Jorswieck, Anne Wolf, and Sabrina Gerbracht. *Secrecy on the Physical Layer in Wireless Networks*, pages 413–436. InTech, 03 2010.

[53] Latif U. Khan. Visible light communication: Applications, architecture, standardization and research challenges. *Digital Communications and Networks*, 3, 05 2017.

[54] 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 *2006 1st International Symposium on Wireless Pervasive Computing*, pages 6 pp.–6, 2006.

[55] T. Komine and M. Nakagawa. Integrated system of white led visible-light communication and power-line communication. *IEEE Transactions on Consumer Electronics*, 49(1):71–79, 2003.

[56] T. Komine and M. Nakagawa. Fundamental analysis for visible-light communication system using led lights. *IEEE Transactions on Consumer Electronics*, 50(1):100–107, 2004.

[57] M. D. Kubjana, A. R. Ndjiongue, and T. Shongwe. Impulsive noise evaluation on plc-vlc based on dco-ofdm. In *11th International Symposium on Communication Systems, Networks Digital Signal Processing (CSNDSP)*, pages 1–6, 2018.

[58] M. D. Kubjana, T. Shongwe, and A. R. Ndjiongue. Hybrid plc-vlc based on aco-ofdm. In *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, pages 1–5, 2018.

[59] Aurélien Van Laere. *Powerline Communication transmission performance study in field conditions: cases of G3-PLC for smart metering and Homeplug AV2 for railway signaling*. PhD thesis, Université de Mons, 2019.

[60] Xicong Li, Zabih Ghassemlooy, Stanislav Zvanovec, Min Zhang, and Andrew Burton. Equivalent circuit model of high power leds for vlc systems. In *2nd West Asian Colloquium on Optical Wireless Communications (WACOWC)*, pages 90–95, 2019.

[61] D.H. Liu and J.G. Jiang. High frequency characteristic analysis of emi filter in switch mode power supply (smps). In *33rd Annual IEEE Power Electronics Specialists Conference. Proceedings (Cat. No.02CH37289)*, pages 2039 – 2043, 02 2002.

[62] Xiaoyan Liu, Pengfei Tian, Zixian Wei, Suyu Yi, Yuxin Huang, Xiaolin Zhou, Zhi-Jun Qiu, Laigui Hu, Zhilai Fang, Chunxiao Cong, Lirong Zheng, and Ran Liu. Gbps long-distance real-time visible light communications using a high-bandwidth gan-based micro-led. *IEEE Photonics Journal*, 9(6):1–9, 2017.

[63] Joe Loughry and David Umphress. Information leakage from optical emanations. *ACM Transactions on Information and System Security*, 5, 08 2002.

[64] Tianyu Luan and Keyuan Qian. Research on influencing factors of led frequency response. In *GREEN ENERGY AND SUSTAINABLE DEVELOPMENT I: Proceedings of the International Conference on Green Energy and Sustainable Development (GESD)*, volume 1864, page 020008, 08 2017.

[65] Lumileds. *LUXEON MultiColor Module 2.5W*, 4 2020.

[66] Hao Ma, Lutz Lampe, and Steve Hranilovic. Integration of indoor visible light and power line communication systems. In *IEEE 17th International Symposium on Power Line Communications and Its Applications*, pages 291–296, 2013.

[67] Hao Ma, Lutz Lampe, and Steve Hranilovic. Integration of indoor visible light and power line communication systems. In *IEEE 17th International Symposium on Power Line Communications and Its Applications*, pages 291–296, 2013.

[68] LED Magazine. High-voltage leds offer optimum solution for indoor retrofit lamps. LED Magazine, April 2011.

[69] Nagayuki Marumo. Simultaneous transmission and reception in radio telephony. *Proceedings of the Institute of Radio Engineers*, 8:199–219, 1920.

[70] Raed Mesleh, Hany Elgala, and Harald Haas. Led nonlinearity mitigation techniques in optical wireless ofdm communication systems. *Journal of Optical Communications and Networking*, 4(11):865–875, 2012.

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

[72] Salvatore Musumeci. Passive and active topologies investigation for led driver circuits. In *IntechOpen*, 2021.

[73] Stephane M. Nlom, Alain R. Ndjiongue, and Khmaies Ouahada. Cascaded plc-vlc channel: An indoor measurements campaign. *IEEE Access*, 6:25230–25239, 2018.

[74] NSA and 5000 NACSIM. Tempest fundamentals. Technical report, National Communications Security, 1982.

[75] OSRAM. *Silicon PIN Photodiode SFH2400-Z*, 4 2016.

[76] OSRAM Sylvania, Inc. *ColorCalculator User Guide*, September 2019.

[77] Parth H. Pathak, Xiaotao Feng, Pengfei Hu, and Prasant Mohapatra. Visible light communication, networking, and sensing: A survey, potential and challenges. *IEEE Communications Surveys and Tutorials*, 17(4):2047–2077, 2015.

[78] Alberto Pittolo and Andrea Tonello. Physical layer security in power line communication networks: An emerging scenario, other than wireless. *Communications, IET*, 8:1239–1247, 05 2014.

[79] PowerTech. *PT4515BX Single-segment linear LED driver chip with integrated rectifier bridge*.

[80] PowerTech. *PT4515BX Single-segment linear LED driver chip with integrated rectifier bridge*.

[81] Ardimas Andi Purwita and Harald Haas. Iq-wdm for ieee 802.11bb-based lifi. In *Wireless Communications and Networking Conference (WCNC)*, pages 1–6, 2020.

[82] Ardimas Andi Purwita and Harald Haas. Studies of flatness of lifi channel for ieee 802.11bb. In *IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6, 2020.

[83] Khaled M. Rabie, Bamidele Adebisi, Andrea M. Tonello, and Galymzhan Nauryzbayev. For more energy-efficient dual-hop df relaying power-line communication systems. *IEEE Systems Journal*, 12(2):2005–2016, 2018.

[84] Kui Ren, Hai Su, and Qian Wang. Secret key generation exploiting channel characteristics in wireless communications. *IEEE Wireless Communications*, 18(4):6–12, 2011.

[85] Ivan Martinovic Richard Baker. Empower: Detecting malicious power line networks from em emissions. In *33th IFIP International Conference on ICT Systems Security and Privacy Protection (SEC)*, 2018.

[86] A. Sendonaris, E. Erkip, and B. Aazhang. User cooperation diversity. part i. system description. *IEEE Transactions on Communications*, 51(11):1927–1938, 2003.

[87] Claude E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 28:656–715, 1949.

[88] Jian Song, Wenbo Ding, Fang Yang, Hui Yang, Bingyan Yu, and Hongming Zhang. An indoor broadband broadcasting system based on plc and vlc. *IEEE Transactions on Broadcasting*, 61(2):299–308, 2015.

[89] Jian Song, Sicong Liu, Guangxin Zhou, Bingyan Yu, Wenbo Ding, Fang Yang, Hongming Zhang, Xun Zhang, and Amara Amara. A cost-effective approach for ubiquitous broadband access based on hybrid plc-vlc system. In *International Symposium on Circuits and Systems (ISCAS)*, pages 2815–2818, 2016.

[90] Riccardo Spolaor, Laila Abudahi, Veelasha Moonsamy, Mauro Conti, and Radha Poovendran. No free charge theorem: A covert channel via usb charging cable on mobile devices. In *International Conference on Applied Cryptography and Network Security*, pages 83–102, 06 2017.

[91] Christopher H Sterling. *Military communications : from ancient times to the 21st century*. ABC-CLIO, California, USA, 2008.

[92] Vincent Tabora. Led-lighting the way and saving energy. Online, January 2020.

[93] Philippe Tanguy. *Étude et optimisations d'une communication à haut débit par courant porteur en ligne pour l'automobile*. PhD thesis, INSA de Rennes, 2012.

[94] Texas Instruments. *THS6222RHF Evaluation Module*, 2019.

[95] Amrutha Thomas. Experimental study on the effect of junction temperature on power leds. In *19th International Conference on Instrumentation, Electrical and Electronics Engineering (ICIEEE)*, 08 2015.

[96] Sezer Tokgoz, Noha Anous, Serhan Yarkan, Diaa Khalil, and Khalid Qaraqe. Performance improvement of white led-based vlc systems using blue and flattening filters. In *International Conference on Advanced Communication Technologies and Networking (CommNet)*, pages 1–6, 04 2019.

[97] A. M. Tonello and F. Versolatto. Bottom-up statistical plc channel modeling part i: Random topology model and efficient transfer function computation. *IEEE Transactions on Power Delivery*, 26(2):891–898, 2011.

[98] Vishay. *Silicon PIN Photodiode*, 1 2019.

[99] Dongshan Wang, Yanbin Song, and Xianhui Wang. Channel modeling of broadband powerline communications. In *9th International Conference on Communication Software and Networks (ICCSN)*, pages 427–430, 2017.

[100] C. S. Wong, K. H. Loo, Y. M. Lai, Martin H. L. Chow, and Chi K. Tse. An alternative approach to led driver design based on high-voltage driving. *IEEE Transactions on Power Electronics*, 31(3):2465–2475, 2016.

[101] Aaron D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54:1355–1387, 1975.

[102] Yangtian Yan, Wenbo Ding, Hui Yang, and Jian Song. The video transmission platform for the plc and vlc integrated system. In *International Symposium on Broadband Multimedia Systems and Broadcasting*, pages 1–5, 2015.

[103] Wenhan Yang, Yinghua Lu, and Jun Xu. Video information recovery from em leakage of computers based on storage oscilloscope. *Frontiers of Electrical and Electronic Engineering in China*, 5:143–146, 06 2010.

[104] Junwei Zhang and M. Cenk Gursoy. Collaborative relay beamforming for secrecy. *arXiv*, pages 1–5, 10 2009.

[105] Yunhong Zhang, Na Liu, and Hong Chen. Evaluation of fatigue and comfort of blue light under general condition and low blue light condition. In *AHFE*, 2019.

[106] Lizhong Zheng and D.N.C. Tse. Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels. *IEEE Transactions on Information Theory*, 49(5):1073–1096, 2003.

[107] Li Zhou, Cheng-Xiang Wang, Ahmed Al-Kinani, and Wen-Sheng Zhang. Visible light communication system evaluations with integrated hardware and optical parameters. *IEEE Transactions on Communications*, 66(9):4059–4073, 2018.

[108] Xiangyun Zhou and Matthew R. McKay. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. *IEEE Transactions on Vehicular Technology*, 59(8):3831–3842, 2010.

[109] M. Zimmermann and K. Dostert. A multipath model for the powerline channel. *IEEE Transactions on Communications*, 50(4):553–559, 2002.

[110] Yulong Zou, Xianbin Wang, and Weiming Shen. Physical-layer security with multiuser scheduling in cognitive radio networks. *IEEE Transactions on Communications*, 61(12):5103–5113, 2013.

[111] Yulong Zou, Jia Zhu, Xianbin Wang, and Lajos Hanzo. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9):1727–1765, 2016.

Titre : Etude de la combinaison des technologies PLC et VLC pour les communications intra-bâtiment.

Mots clés : PLC, VLC, fuite du signal, canal auxiliaire, LED, sécurité de la couche physique.

Résumé : Comme les lampes à LED sont naturellement connectées aux lignes électriques, l'intégration des systèmes de communication par courant porteur (PLC) et par lumière visible (VLC) peut être un sujet intéressant à inspecter.
Ainsi, le premier objectif est de mettre en œuvre un système PLC-VLC large bande à bas coût qui ne nécessite pas l'existence d'un relais qui décode et ré-encode le signal PLC avant de le transmettre au système VLC. Mais avant, une étude approfondie est menée pour évaluer le sous-système VLC, en particulier les LED. Ensuite, le banc d'essai PLC-VLC est mis en œuvre à l'aide de modems PLC commerciaux, d'un émetteur et récepteur VLC. Après avoir validé la faisabilité de notre banc d'essai à petite échelle, une étude théorique est réalisée pour extrapoler les résultats obtenus à des applications réelles.
Le deuxième objectif est d'étudier le risque de sécurité apporté par les ampoules LED au réseau PLC. La fuite de données PLC à travers les ampoules LED domestiques est examinée. Les caractéristiques du canal auxiliaire sont étudiées. De plus, le taux d'erreur binaire est calculé. Toutes ces mesures ont montré qu'il existe certaines ampoules LED susceptibles de fuir naturellement le signal PLC. De plus, des modifications intentionnelles sont apportées aux drivers des ampoules afin d'etudier la possibilité de favoriser la fuite. Après la modification des drivers, toutes les mesures susmentionnéees sont répétés, il est remarqué que ces modifications ont considérablement amélioré la fuite. Enfin, la sécurité de la couche physique du système PLC est étudiée en présence d'un système VLC non légitime pour evaluer theoriquement ce risque de securité.

Title: Study of the combination of PLC and VLC technologies for intra-building communications

Keywords: PLC, VLC, signal leakage, side channel, LED, physical layer security.

Abstract: As LED lamps are naturally connected to powerline, the integration of Powerline Communication (PLC) and Visible Light Communication (VLC) systems can be an interesting topic to be investigated.
Hence, the first objective of this thesis is to implement a low-cost broadband PLC-VLC system that does not require the existence of a relay that decodes a re-encode the PLC signal before transmitting it to the VLC. But before that, an in-depth study is carried out to evaluate the VLC subsystem. Then, the PLC-VLC testbed is implemented using commercial PLC modems, VLC transmitter, and receiver. After validating the feasibility of our small-scale testbed, a theoretical study is carried out to extrapolate the obtained results to real applications.
The second objective is to study the security risk brought by LED bulbs to the PLC network. The PLC data leakage through the domestic LED bulbs is investigated. The characteristics of the electrical-optical side channel are inspected. Moreover, the bit error rate is calculated. All these measurements have shown that there exist some LED bulbs that are prone to leak naturally PLC signal. Moreover, intentional modifications are made to the LED bulbs drivers to study the possibility of fostering the leakage. After driver modifications, the aforementioned experiments are repeated. It is noticed that these modifications enhance considerably the PLC data leakage. Finally, the physical layer security of the PLC system is studied in the presence of a non-legitimate VLC system in order to theoretically assess this security risk.