Universidade Federal de Juiz de Fora
Programa de Pós-Graduação em Engenharia Elétrica
Doutorado em Engenharia Elétrica

Ândrei Camponogara

Physical Layer Security Analyses for Low-Bit-Rate Hybrid PLC/WLC and Broadband PLC Systems

Juiz de Fora
2020

Ândrei Camponogara

Physical Layer Security Analyses for Low-Bit-Rate Hybrid PLC/WLC and Broadband PLC Systems

Tese de doutorado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Juiz de Fora, na área de concentração em sistemas eletrônicos, como requisito parcial para obtenção do título de Doutor em Engenharia Elétrica.

Orientador: Moisés Vidal Ribeiro

Juiz de Fora
2020

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF com os dados fornecidos pelo(a) autor(a)

Camponogara, Â.

Physical Layer Security Analyses for Low-Bit-Rate Hybrid PLC/WLC and Broadband PLC Systems / Ândrei Camponogara. – 2020.

117 f. : il.

Orientador: Moisés Vidal Ribeiro

Tese de Doutorado – Universidade Federal de Juiz de Fora, Doutorado em Engenharia Elétrica. Programa de Pós-Graduação em Engenharia Elétrica, 2020.

Ândrei Camponogara

Physical Layer Security Analyses for Low-Bit-Rate Hybrid PLC/WLC and Broadband PLC Systems

Tese de doutorado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Juiz de Fora, na área de concentração em sistemas eletrônicos, como requisito parcial para obtenção do título de Doutor em Engenharia Elétrica.

Aprovada em: 21 de agosto de 2020

BANCA EXAMINADORA

Moisés Vidal Ribeiro

Prof. Dr. Moisés Vidal Ribeiro - Orientador
Universidade Federal de Juiz de Fora

Richard Demo Souza

Prof. Dr. Richard Demo Souza
Universidade Federal de Santa Catarina

Rausley A. A. de Souza

Prof. Dr. Rausley A. A. de Souza
Instituto Nacional de Telecomunicações

Luciano M. de A. Filho

Prof. Dr. Luciano Manhães de Andrade Filho
Universidade Federal de Juiz de Fora

Alvaro A. M. de Medeiros

Prof. Dr. Álvaro Augusto Machado de Medeiros
Universidade Federal de Juiz de Fora

To my mother Ivani
To my father Luiz
To my brothers Gláuber and Douglas
To my girlfriend Tatiane

AGRADECIMENTOS

Eu agradeço primeiramente a Deus, porque sem Ele nada seria possível. Agradeço, também, aos meus pais, Luiz Francisco Camponogara e Ivani Teresinha Camponogara, pelo apoio incondicional e exemplo que sempre deram em minha vida. Aos meus irmãos, Gláuber Camponogara e Douglas Camponogara, que sempre estiveram ao meu lado, mesmo fisicamente distantes, dando-me força para seguir o meu caminho. A minha amada namorada, Tatiane Ribeiro, por todo amor, carinho, e companheirismo, estando ao meu lado mesmo nos momentos mais difíceis. Aos meus amigos Paulo Carabajal, Lucas Meneses e Cinthia Lopes, cuja amizade e conselhos foram essenciais para me dar forças e passar pelas dificuldades do Doutorado e da vida.

Agradeço ao professor Moisés Vidal Ribeiro pelos conselhos e orientações, os quais foram imprescindíveis para a realização do Doutorado. Aos meus amigos e colegas de laboratório, Mateus Filomeno, Leonardo Dib, Lucas Giroto, Victor Fernandes, Roberto M. de Oliveria, Túlio Fernandes, entre outros, cujas conversas, seja de forma direta ou indireta, ajudaram na realização do meu trabalho de Doutorado.

Por fim, agradeço a todos os brasileiros que, diretamente ou indiretamente, financiaram esse trabalho através do CNPq, CAPES, INERGE e FAPEMIG.

RESUMO

Nesta tese de doutorado, investiga-se a segurança na camada física (do inglês, *physical layer security*) (PLS) de sistemas de comunicação via rede de energia elétrica (do inglês, *power line communication*) (PLC). Para tanto, discute-se como sinais privados, trafegando ou radiando através da rede de energia elétrica, podem ser obtidos por meio de uma escuta. Além disso, aborda-se questões de PLS relativas à combinação de sistemas PLC e de comunicação sem fio (do inglês, *wireless communication*) (WLC) em paralelo para a realização de transmissão *one-hop*. Para apresentar de forma adequada os problemas investigados, discute-se o que é PLS em termos de níveis de tensão em sistemas elétricos de potência e como o processo de escuta e, consequentemente, violação da informação dá-se em sistemas PLC. Considerando PLS de sistemas PLC banda larga residenciais, investiga-se até que ponto uma escuta passiva composta por dispositivos PLC ou WLC pode ser capaz de ameaçar a segurança de sistemas PLC no nível da camada física. Com este fim, a probabilidade de indisponibilidade de sigilo, a vazão eficaz de sigilo, e as taxas de código de escuta são numericamente analisadas por meio do uso de dados reais constituídos por estimativas de canal e medidas de ruído aditivo. Esses conjuntos de dados foram obtidos por meio de duas campanhas de medição distintas realizadas em algumas residências brasileiras. Através de resultados numéricos, mostra-se, de forma quantitativa, o nível de vulnerabilidade de sistemas PLC banda larga residenciais em termos de PLS e fornece-se as taxas de código de escuta para lidar com a presença de escutas PLC e WLC. Além disso, investiga-se os benefícios da existente diversidade relacionada ao uso em paralelo dos canais PLC e WLC pelo sistema híbrido PLC/WLC de baixas taxas para melhorar a PLS. A esse respeito, formulações matemáticas da taxa de sigilo alcançável ergódica e da probabilidade de indisponibilidade de sigilo são desenvolvidas para o modelo de canal de escuta híbrido PLC/WLC e suas versões incompletas. Por meio dos resultados numéricos, mostra-se que os sistemas híbridos PLC/WLC podem fornecer benefícios notáveis em termos de PLS para aplicações de baixas taxas quando a escuta é composta por uma única interface de comunicação.

Palavras-chave: Comunicação via rede de energia elétrica. Comunicação sem fio. Segurança na camada física.

ABSTRACT

This Doctoral thesis focuses on the physical layer security (PLS) aspects of power line communication (PLC) systems. In this way, it addresses how a malicious device can overhear private signals traveling over and radiating from electric power grids. Also, it discusses the PLS issues related to the parallel combination of PLC and wireless communication (WLC) systems for accomplishing one-hop transmission. Given these aims, a general discussion on important issues related to PLC systems is presented. First, PLS issues associated to the distinct voltage levels in electric power systems are detailed. Second, the types of eavesdroppers that can breach the security of PLC systems are listed. Focusing on the PLS of in-home broadband PLC systems, this thesis investigates to which extent malicious and passive PLC or WLC devices can be capable of breaching the security of PLC systems in the physical layer level. To this end, secrecy outage probability, effective secrecy throughput, and wiretap code rates are numerically evaluated with the use of real data sets composed of channel estimates and measured additive noises. These data sets were obtained from distinct measurement campaigns carried out in several Brazilian houses. The numerical results quantitatively show, in practice, the level of vulnerability of in-home broadband PLC systems in terms of PLS and offer the wiretap code rates to deal with the presence of PLC and WLC eavesdroppers. Furthermore, the investigation of the benefits of the existing diversity in the parallel use of both PLC and WLC channels by low-bit-rate hybrid PLC/WLC systems to improve PLS is provided. In this regard, mathematical formulations of the ergodic achievable secrecy rate and the secrecy outage probability are developed for the hybrid PLC/WLC wiretap channel model and its incomplete versions. The numerical results show that the hybrid PLC/WLC systems can provide remarkable benefits in terms of PLS for low-bit-rate applications when the eavesdropper makes use of only one data communication interface.

Key-words: Power line communications. Wireless communications. Physical layer security.

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

AC	alternating current
ACA	average channel attenuation
ANATEL	Brazilian telecommunication regulation authority (*Agência Nacional de Telecomunicações* in Portuguese)
AMI	advanced metering infrastructure
AMR	automatic meter reading
ARIB	Association of Radio Industries and Businesses
ASK	amplitude shift keying
AWGN	additive white Gaussian noise
BER	bit error rate
BPSK	binary phase shift keying
CDF	cumulative distribution function
CFR	channel frequency response
CENELEC	European Committee for Electrotechnical Standardization (*Comité Européen de Normalisation Électrotechnique* in French)
CGRC	circular Gaussian relay channel
CIR	channel impulse response
CSI	channel state information
DC	direct current
DFT	discrete-time Fourier transform
DR	demand response
FCC	Federal Communications Commission
FSK	frequency shift keying
GE	General Electric Corporation
HV	high voltage
IoT	Internet of Things
LGRC	linear Gaussian relay channel
LP-RF	low-power radio-frequency
LV	low voltage
MIMO	multiple-input multiple-output
MV	medium voltage

NB-PLC	narrowband PLC
nSNR	normalized signal-to-noise ratio
PLC	power line communication
PLS	physical layer security
PSD	power spectral density
OA	optimal power allocation
SISO	single-input single-output
RCS	ripple carrier signaling
RMS-DS	root mean squared delay spread
TWACS	two-way automatic communications system
UA	uniform power allocation
WLC	wireless communication

CONTENTS

1 INTRODUCTION

The increasing demand for connectivity fuels the astonishing widespread use of the Internet of Things (IoT), smart grids, industry 4.0, and smart city concepts. It has been pushing forward worldwide efforts to design new generation of effective, reliable, flexible, energy-efficiency, and low-energy consumption telecommunication infrastructures [1]. In this context, multiple-input multiple-output (MIMO) and cooperative concepts have been investigated for improving data communication through wireless and wireline media [2, 3]. Moreover, cognitive concepts have being studied to deal with the scarcity of the available spectrum for data communication [4]. Lately, 5G and visible light communication are attracting the interest of many researchers [5, 6]. Also, the usefulness of electric power grids [7, 8] for data communication purposes is being revitalized because of the increased need for connectivity among things and people and the availability of underutilized resources of these grids for data communications.

The power line communication (PLC) technology has been widely studied by both academic and business sectors since electric power systems are pervasive and connections to them are ubiquitous. Also, electric power systems support well-established data communication technology for indoor (residential and commercial buildings) and outdoor (medium voltage (MV) and low voltage (LV)) electric power grids [3, 9, 10]. Currently, transportation systems (e.g., car, ship, train, spacecraft, and aircraft) [11–15] have been constituted a new frontier for designing and introducing novel PLC technologies and usages of them. Despite the well-known advantages, such as ubiquitousness, low-cost implementation, and easy installation for LV levels (i.e., below 1 kV), electric power systems (generation, transmission, and distribution) were initially designed for energy delivery rather than data communications. Therefore, data-carrying signals traveling through electric power grids suffer severe degradation and attenuation due to the increases in distance and/or frequency, multipath effect due to impedance mismatching, dynamic of loads (i.e., consumers and utilities) connected to the grids [3, 8, 16–21], coupling losses for injecting and extracting data-carrying signals [10, 22], and interference with other telecommunication systems operating in the same frequency band because power cables are usually unshielded (i.e., electromagnetically unprotected).

Recently, the existing diversity among distinct communication media has been investigated in order to increase the reliability and coverage of telecommunication infrastructures in indoor and outdoor environments. In this way, the combined use of power line, wireless, and visible light media has drawn attention. According to [23], PLC and wireless communication (WLC) show more advantages than disadvantages and, as a consequence, it defines an appealing motivation for studying their combinations. Among the possibilities, the parallel use of the narrowband PLC and low-power radio-frequency[1] channels, which has been termed *low-bit-rate hybrid PLC/WLC channel*, and the cascade combination of broadband PLC and

[1] The low-power radio-frequency channel is a type of WLC channel that occupies a narrow frequency bandwidth and is typically used by low-energy consumption devices.

WLC channels, which has been termed *hybrid PLC-WLC channel*, deserve attention.

Notably, several works have shown that PLC systems can improve the performance of WLC systems or vice-versa even using very low transmission power [24–26]. For instance, [27] proposed a scheme for data communication through the hybrid PLC/WLC channel model and analyzed its performance in terms of bit error rate (BER) when binary phase shift keying (BPSK) digital modulation is adopted. This work also showed that the use of a saturated additive white Gaussian noise (AWGN) metric for diversity combining results in good performance when the PLC noise is highly impulsive. Furthermore, [28] presented two receiver diversity combining techniques that take into account the asymmetric impulsiveness nature of the noise on both PLC and unlicensed WLC links and the interference on both links. Also, [25] and [29] verified that the hybrid PLC/WLC interface at a relay node can improve the data communication system performance. Furthermore, [30,31] discussed the achievable data rate and the outage probability of the hybrid PLC/WLC single-relay channel model whereas the performance of its incomplete versions was addressed in [32]. Finally, [33] proposed the hardware of a hybrid PLC/WLC device.

In a pioneering study [7], the authors investigated the use of broadband PLC and WLC channels in cascade. Basically, PLC signals (i.e., data-carrying signals) flowing to unshielded power cables radiate an electromagnetic field that can be sensed by a WLC device operating in the same frequency band and located in the vicinity of the electric power circuit. In this regard, a comprehensive characterization and statistical analysis of the hybrid PLC-WLC channel considering the frequency band 1.7 – 100 MHz were discussed [7]. Soon after, statistical modeling of average channel attenuation (ACA), root mean squared delay spread (RMS-DS), coherence bandwidth, and coherence time were proposed [34].

The broadcast nature of WLC and PLC systems and the fact that electric power grids are mainly constituted of unshielded power cables can potentially turn both systems vulnerable to malicious users [7,34,35]. In particular, PLC signals radiated from the power cable into the air may be accessed by a malicious WLC device. To circumvent malicious attacks, the use of physical layer security (PLS) in PLC systems becomes an interesting approach to prevent security breaches. Generally speaking, PLS exploits the characteristics of the data communication medium to increase security using appropriate codes and signal processing. The idea of security at the physical layer level stems from studies of information-theoretic security back to the 1970s [36–38]. In particular, [36] introduced the degraded wiretap channel. Soon after, the secrecy capacity was analyzed for the Gaussian wiretap channel [37] and a more general model known as non-degraded wiretap channel was proposed in [38]. Recently, PLS has been investigated for fading wiretap channels [39–41] and for MIMO wiretap channels [6,42–45], among others. For a review of this area, see [35].

According to the literature, few studies have analyzed PLS for PLC systems. In [46–48], the authors assumed that the transmitter has full channel state information (CSI) of the intended receiver and the eavesdropper, while the assumption of passive eavesdropping was made in

[49–51]. Note that [50] considered both PLC and hybrid PLC/WLC systems, whereas [51] taken into account the hybrid PLC/WLC system under the presence of a WLC or PLC eavesdropper. Furthermore, it is important to point out that real data was considered only in [48], where the authors provided achievable secrecy rate results for broadband PLC systems in the frequency band 2 – 28 MHz. Observe that none of those studies have considered PLC signals radiating into the air and sensed by a malicious WLC device. Further, they have not taken into account a real data set to quantify, in a practical perspective, the PLS in narrowband or broadband PLC systems except [48]. This type of analysis is of the utmost importance because, in the end, security evaluation carried out from realistic scenarios can precisely point out to which extent the security breach countermeasure needs to be taken into account. Therefore, this Doctoral thesis aims at extending the PLS analysis of both PLC and hybrid PLC/WLC systems in order to provide import insights.

1.1 OBJECTIVES

Based on the aforementioned motivations, the objectives of this Doctoral thesis are as follows:

- To provide a comprehensive and practical discussion on the PLS related to the PLC and hybrid PLC/WLC systems covering the following issues: the accessing of PLC signals traveling over high voltage (HV), MV, and LV electric power grids by malicious devices; types of eavesdroppers (malicious devices); and the access conditions that allow malicious devices overhear private information in both PLC and hybrid PLC/WLC systems.

- To analyze the PLS of an in-home and broadband PLC system when a malicious WLC device tries to overhear private information exchanged between two PLC devices. Then a hybrid wiretap channel model is proposed and the ergodic achievable secrecy rate, secrecy outage probability, effective secrecy throughput, and wiretap code rates are numerically computed considering the presence of a passive eavesdropper. Also, the frequency band 1.7 – 86 MHz is adopted and the data set obtained from the measurement campaign addressed in [7, 52] is considered to represent the hybrid wiretap channel model.

- To investigate the security at the physical layer of an in-home and broadband PLC system when a malicious PLC device eavesdrops private information sent by a PLC transmitter to an intended PLC receiver. Such a scenario is represented by the PLC wiretap channel model. Moreover, considering passive eavesdropping, numerical results regarding the ergodic achievable secrecy rate, secrecy outage probability, effective secrecy throughput, and wiretap code rates are provided and discussed for the frequency bands 1.7 – 30 MHz, 1.7 – 50 MHz, and 1.7 – 86 MHz. To do so, the data set obtained from the measurement campaign presented in [3] is taken into account.

- To assess the data communication security of the low-bit-rate hybrid PLC/WLC system and its incomplete versions under the PLS perspective by adopting the so-called low-bit-rate hybrid PLC/WLC wiretap channel model. In this investigation, theoretical models proposed in [53] for the narrowband PLC channel and in [54] for the WLC channel are taken into account so that the frequency bands $0-500$ kHz and $5,799,750-5,800,250$ kHz are adopted, respectively. In this regard, considering that the eavesdropper belongs to the hybrid PLC/WLC system, i.e., the transmitter knows the CSI of the eavesdropper, the ergodic achievable secrecy rate and secrecy outage probability results are provided and discussed.

1.2 DOCTORAL THESIS OUTLINE

The reminder of this Doctoral thesis is organized as follows:

- Chapter 2 presents a comprehensive and practical discussion on the PLS of PLC and hybrid PLC/WLC systems. In this sense, aspects related to the accessing of PLC signals traveling over distinct electric power grids and the types of eavesdroppers as well as their respective access conditions to private information in PLC and hybrid PLC/WLC systems are covered.
- Chapter 3 assesses the performance of the hybrid wiretap channel model in terms of PLS for the frequency band 1.7 – 86 MHz. In this regard, mathematical expressions and numerical results covering the ergodic achievable secrecy rate, secrecy outage probability, effective secrecy throughput, and wiretap code rates are provided.
- Chapter 4 analyzes the PLS of the PLC wiretap channel model considering the frequency bands 1.7 – 30 MHz, 1.7 – 50 MHz, and 1.7 – 86 MHz. To this end, it addresses mathematical expressions and numerical results regarding the ergodic achievable secrecy rate, secrecy outage probability, effective secrecy throughput, and wiretap code rates.
- Chapter 5 evaluates the low-bit-rate hybrid PLC/WLC wiretap channel model and its incomplete versions in terms of PLS. To do so, mathematical expressions regarding the ergodic achievable secrecy rate and secrecy outage probability as well as the respective numerical results are presented.
- Chapter 6 states the concluding remarks of this Doctoral thesis.

2 PHYSICAL LAYER SECURITY IN PLC AND HYBRID PLC/WLC SYSTEMS

A huge amount of research efforts towards WLC systems is justifiable because they are the main data communication technology for assisting the widespread deployment of smart grids, smart cities, IoT, and industry 4.0 solutions. However, other media, such as electric power grids, also deserve research efforts due to several reasons. Among them, the spectrum scarcity together with the necessity of feasible, flexible, and energy-efficient technologies emerges. It is worth mentioning that electric power systems are the most pervasive artificial systems built by human beings with a remarkable potential for data communications. As a result, they show a great potential for supporting the needs and demands related to the interconnections among IoT, smart grids, smart cities, and industry 4.0 devices. Recently, the parallel combination of both WLC and PLC channels for data communication purposes has drawn the attention of many researchers because it allows to take advantage of the benefits of both data communication media for smart grids, smart cities, IoT, and industry 4.0 applications.

However, it is well-known that electric power systems were not conceived, designed, and deployed for data communication purposes. Actually, their aims are the transmission and the delivery of a high amount of energy in the electric form from power generation plants to consumers. It means that electric power systems may not be the best medium for data communications. Despite that, several narrowband and broadband technologies are in the market to exploit the existing data communication potential in electric power systems. Additionally, the existing limitations in electric power systems for data communication purposes and the diversity among these media and wireless media have motivated the combined use of PLC and WLC systems (e.g., hybrid PLC/WLC system). It has been recognized that such a combination is a new frontier for introducing new telecommunication technologies that are capable of fulfilling several needs and demands related to IoT, smart cities, smart grids, and industry 4.0.

Nowadays, an important issue is the security of information exchanged among devices through the PLC and WLC channels. Considering the security aspects at the physical layer level, the problem is more challenging since the broadcast nature of both PLC and WLC channels as well as the fact that power cables used in most electric power grids are mainly unshielded turn the security at this level a relevant issue to be pursued. In this context, the investigation of physical layer characteristics to improve security, i.e., PLS, has drawn the attention of many researchers of the academic sector. Due to this novelty, a detailed discussion on potential, limitation, and scenarios related to PLS in PLC systems deserve careful attention to offer guidelines for pushing forward research efforts in this challenging topic.

Given such perspective, this chapter provides a historical overview about the PLC technology covering the emergence of PLC at the early 1900s to these days as well as the main standards and technologies available in the market. Also, considering the PLS of PLC and hybrid systems based on PLC and WLC technologies, this chapter describes the types of eavesdroppers that can threaten the PLS in these systems as well as the conditions in which these eavesdroppers can access private information.

The rest of this chapter is organized as follows: Section 2.1 presents a historical overview regarding PLC from the beginning of the technology to these days; Section 2.2 describes some important standards and technologies of PLC; Section 2.3 presents a comprehensive discussion on PLS in PLC systems so that the influence of the voltage levels in the electric power grids, types of eavesdroppers, and access conditions where the private information can be eavesdropped are covered; Section 2.4 extends the PLS discussion for hybrid PLC/WLC systems; and, finally, Section 2.5 states the summary of this chapter.

2.1 POWER LINE COMMUNICATIONS

The idea of using power lines for data communication is not new. In 1838, a remote electricity supply metering was proposed in order to check voltage levels of batteries at unmanned sites on the London-Liverpool telegraph system [55]. Moreover, the first patent on data communication over power lines dates back to 1898, in the United Kingdom. In this regard, a power line signaling system was proposed in order to read meters at remote locations [55, 56]. Next, in 1905, a similar system was patented in the United States [55,57] and, in 1913, it started the first commercial production of automatic electromechanical meter repeaters [58].

Soon after, investigations on the use of power lines as medium for analogic voice communications have started. The first test and commercial operation of carrier-current telephony over power lines reported in the literature refers the year 1918 in Japan. Such a system was successfully tested over 144 km long MV power lines [59, 60]. Two years later, a similar system was first tested in the United States over 19.2 km long aerial MV power lines and over 33 km long underground MV power lines with transformers [60, 61]. Next, in 1921, the carrier-current system was first commercialized in the United States by the General Electric Corporation (GE) company. This system made use of amplitude modulation, simplex transmission, and antenna coupling. They operated over HV and MV electric power grids considering the range of frequencies $50-150$ kHz, in the United States, and frequency bandwidths of few kHz [60, 62]. The main applications of carrier-current systems were handling operations management of power supplies [58]. In the end 1920s, there were around 1000 carrier-current systems spread across the United States and Europe. Also, from that time, capacitive coupling has substituted the antenna coupling [60]. Note that only voice was transmitted in those systems; however, after 1940, telemetering and telecontrol began to be implemented by carrier-current systems with initial data-rate of 50 bps and then increased to 100 bps and 200 bps [58].

In the 1930s, the ripple carrier signaling (RCS) technology emerged in order to manage operations in MV and LV electric power grids. Next, in the 1950s, they began to be developed on large scale [62]. The RCS systems operated in low frequencies, between 125 Hz and 3 kHz, which allowed the signal to pass through MV/LV transformers [58]. Also, these systems made use of amplitude shift keying (ASK) and frequency shift keying (FSK) modulation techniques with data-rates reaching a few bits per second [63]. Management of street lights and load control were among the applications related to RCS systems [58].

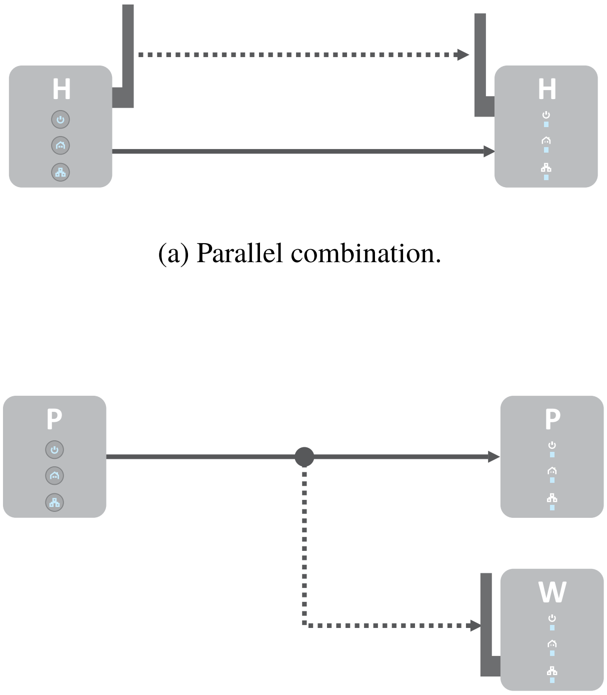
The emergence of sophisticated signal modulation techniques and error control coding, the advance of digital signal processing, and the invention of integrated circuits pushed forward the development of a bi-directional and low-cost PLC technology with higher data-rates in the end 1980s [58, 63]. The main applications of this new technology were automatic meter reading (AMR) and automation in MV and LV electric power grids as well as industry and home automation [62]. Note that all these PLC technologies can be categorized as ultra-narrowband and low-bit-rate narrowband. The former considers frequencies below 3 kHz and offers data-rates lower than 100 bps. The latter operates in the frequency band 3 − 500 kHz and provides data-rates of a few kilobits per second [62, 64].

In the 1990s, the deregulation of the telecommunication and energy markets in Europe attracted the interest of electric utilities in providing broadband Internet access to residential customers [62, 64]. As consequence, considering the advances aforementioned regarding modulation techniques, error control coding, and digital signal processing as well as the low-cost microelectronic, it arose the broadband PLC technology offering high-data-rates, around 200 Mbps in the physical layer, and using the frequency band 2 − 30 MHz. Soon after, in the 2000s, the concept of smart grid has emerged and it has attracted the interest of many research groups and electric utilities. In this regard, PLC has became a natural candidate for smart grid since the use of the pre-existent electric power infrastructure is quite attractive due to the low-costs involved. Consequently, the high-data-rate narrowband PLC has emerged since sophisticated techniques applied to broadband PLC systems, such as multi-carrier modulations, start to be used in narrowband PLC systems allowing data-rates between tens of kbps to about 500 kbps [62, 64].

Nowadays, PLC systems make use of the most advanced signal processing techniques, multi-carrier schemes with adaptive notching, MIMO, and so on [62, 63]. Furthermore, recent investigations have considered the combined use of PLC systems with WLC ones. Among the possibilities, the parallel and concatenate combinations stand out, which are termed hybrid PLC/WLC and hybrid PLC-WLC, respectively, see Figure 1. In the parallel combination of these media, transmitter and receiver use both power line and wireless media together to communicate. In the literature, many investigations have shown the benefits that one data communication medium can bring to another because of the potential behind the existing diversity between them. [23–32]. Regarding the cascade combination, transmitter and receiver use distinct media to communicate. Basically, PLC signals traveling over unshielded power lines radiate an electromagnetic field that can be sensed by a WLC device closes enough and operating in the same frequency band as the PLC system. A complete characterization of the hybrid PLC-WLC channels as well as their advantages were introduced in [7, 34].

PLC systems have achieved notable advances in terms of reliability and data-rate since the beginning of 1900s. Consequently, the number of applications related to PLC technology have increased significantly covering the outdoor (HV, MV, and LV) and indoor (in-home, building, and in-vehicle) electric power grids. In contrast, the broadcast nature of PLC systems

Figure 1 – Illustration of two types of hybridism related to PLC and WLC



(a) Parallel combination.

(b) Cascade combination.

Source: Personal collection.
Note: The continuous and dashed lines represent the power line and wireless media, respectively.

poses a security threat during the data transmission. The well-established strategy to circumvent this issue is the use of sophisticated cryptography techniques [65]. Recently, the urgency of ensuring privacy for the transmitted information in novel scenarios (e.g., IoT, smart grid, smart cities, and industry 4.0) have pushed forward research efforts toward the physical layer of the aforementioned PLC and hybrid systems [43,46–50]. However, the investigations related to PLS in those systems are in the infancy and, as a consequence, there is a lack of a comprehensive characterization of what is PLS in PLS systems. Also, significant research efforts are demanded to make feasible the introduction of PLS in the novel generation of PLC systems.

2.2 STANDARDS AND TECHNOLOGIES OF POWER LINE COMMUNICATIONS

Standards are of utmost importance for the deployment of new telecommunication technologies since they may provide the co-existence and/or interconnection among them and pre-existent technologies [66]. In particular, established PLC standards focus their specifications on physical and link layers and usually support the development of narrowband and broadband PLC technologies. According to the literature, the PLC technology may fall in the following categories: ultra-narrowband, narrowband, and broadband.

Following [64], ultra-narrowband PLC systems cover the frequency bands 0.3 – 3 kHz and 30 – 300 Hz and can offer data-rates of a few bits per second (around 100 bps). Among the systems that operate in these low-frequencies, the turtle system and the two-way automatic communications system (TWACS) stand out. The turtle system is mainly used for AMR applications achieving data-rates around 0.001 bps. Regarding the TWACS, they are more used for advanced metering infrastructure (AMI), distribution automation, and demand response (DR) applications. This system may provide maximum data-rates of 100 bps and 120 bps in Europe and in North America, respectively. Despite the low-data-rates, ultra-narrowband PLC systems may cover distances of 150 km or more allowing access to electric power meters in remote locations. Additionally, the TWACS uses higher power transmission than turtle systems and it operates with several levels of parallelization, which allows to handle with tens or hundreds of thousand electric power meters. Finally, it is noteworthy that both turtle system and TWACS are proprietary. Nowadays, only TWACS is available on the market being commercialized by ESCO Technologies [67] and Aclara [68].

The so-called narrowband PLC comprises all PLC systems that operate in the frequency range from 3 kHz up to 500 kHz. In this regard, distinct frequency bands are used around the world, such as the European Committee for Electrotechnical Standardization (*Comité Européen de Normalisation Électrotechnique* in French) (CENELEC) band (3 – 148.5 kHz), the United States Federal Communications Commission (FCC) band (10 – 490 kHz), the Japanese Association of Radio Industries and Businesses (ARIB) band (10 – 450 kHz), and the Chinese band (3 – 500 kHz) [64]. Furthermore, narrowband PLC can be categorized as low-data-rate or high-data-rate systems. The former is related to single carrier systems that provide data-rates of few kilobits per second, while the latter is related to multi-carrier systems capable of achieving data rates about 500 kbps. Among many standards available, the following ones can be highlighted: PRIME [69], G3-PLC (ITU-T G.9903) [70], IEEE 1901.2 [71], ITU-T G.hnem [72], and IEEE 1901a [73]. The main applications of these standards are summarized in Table 1.

Table 1 – Narrowband PLC Standards

Standards	**Main Applications**
PRIME [69]	smart things*
G3-PLC [70]	smart things, in-vehicular
IEEE 1901.2 [71]	smart things, in-vehicular
ITU-T G.hnem [72]	smart things, in-vehicular
IEEE 1901.a [73]	IoT

Source: [66].
Note: **Smart things* is a generic term related to smart grids, smart cities, industry 4.0, and so on.

Broadband PLC systems are defined as those which operate in the frequency range from 1.8 MHz up to 250 MHz [62, 64]. Such systems may offer data-rates ranging from several megabits per second to more than 1 Gbps [64]. Clearly, broadband PLC systems can offer much higher data-rates than narrowband PLC ones due to the higher used frequencies. However, this issue has a drawback since the PLC signal attenuation increases exponentially with the frequency, i.e., the distances achieved by a broadband PLC signal (below 500 meters) are much shorter than a narrowband PLC signal (more than 20 km). The main applications of broadband PLC technology are Internet access, in-home multimedia, indoor data network, and smart grid [66]. Among several standards developed for broadband PLC systems, one can mention HomePlug 1.0 [74], HomePlug AV [75], HomePlug AV2 [76], HomePlug GP [77], IEEE 1901 [78], IEEE 1901.1 [79], HD-PLC [80], ITU-T G.hn [81], ITU-T G.hn-MIMO [82], and so on. The main applications of such standards are summarized in Table 2.

Table 2 – Broadband PLC Standards

Standards	**Main Applications**
HomePlug 1.0 [74]	home area networks
HomePlug AV [75]	multimedia
HomePlug AV2 [76]	multimedia
HomePlug GP [77]	smart things, in-vehicular, multimedia
IEEE 1901 [78]	smart things, in-vehicular, multimedia
IEEE 1901.1 [79]	smart grids
HD-PLC [80]	smart home
ITU-T G.hn [81]	smart things, in-vehicular
ITU-T G.hn-MIMO [82]	home networks

Source: [66].

Moreover, the growing demand for connectivity imposed by IoT, smart grids, smart cities, and industry 4.0 solutions has attracted the interest of many companies worldwide in the development and commercialization of narrowband and broadband technologies. Regarding the companies that manufacture narrowband PLC chipsets, some can be mentioned, such as Texas Instruments [83] and Atmel [84], which support the PRIME, G3-PLC, and IEEE 1901.2 standards; and Maxim Integrated [85], which supports the PRIME, G3-PLC, IEEE 1901.2, and ITU-T G.hnem standards. Regarding the broadband PLC chipsets manufacturing, one can mention Qualcomm [86], supporting HomePlug standards and IEEE 1901; MegaChips [87] and Panasonic [88], which comply with HD-PLC technology; and Marvell, supporting ITU-T G.hn [89].

All the aforementioned standards and technologies ensure or suggest the use of encryption techniques in the upper layers for maintaining confidentiality of the transmitted data, preventing corruption of the transmitted information and verifying authenticity. With an astonishing increase in computing power, the use of encryption may no longer prevent information leakage to adversaries that can eventually be physically connected to the electric power system to overhear private information or can wirelessly overhear private information in the signal radiated from unshielded power cables. At the moment, none of the existing PLC technologies and standards are capable of dealing with eavesdroppers that can either overhear the PLC signals propagating through the electric power grids or radiating into the air. The fact that PLC systems can be threatened by malicious PLC and/or WLC devices operating in the same frequency band constitutes a serious and challenging security breach that must be addressed in the near future.

2.3 PHYSICAL LAYER SECURITY IN POWER LINE COMMUNICATIONS

First of all, PLC is a well-establish data communication technology for many applications in outdoor (HV, MV, and LV levels) and indoor (in-home, building, and in-vehicle) electric power grids. Different from other wireline media (e.g., coaxial, twisted-pair, and fiber-optic), electric power grids present a broadcast nature, which may turn private information vulnerable to malicious PLC devices connected to the electric power grid in which a PLC system operates.

The recent identification of the significance of this problem has motivated the investigation of PLS for PLC systems. In [46–48], the authors evaluated the PLS of PLC systems assuming that the transmitter has full CSI of the intended receiver and the eavesdropper (i.e., the receiver and the eavesdropper belong to the PLC system). In this regard, [46] assessed the secrecy achievable rate for quasi-static flat PLC channels and compared them with WLC ones. Further, [48] extended that analysis to frequency selective PLC channels, in which a real data set obtained from several houses is considered. Also, single- and multi-user scenarios for the frequency band 2 – 28 MHz were taken into account. Last, [47] investigated the secrecy capacity for MIMO-PLC channels and compared the obtained results with the ones from WLC channels. The authors considered frequency selective channels in the frequency band 2 – 28 MHz. Moreover, several studies made a more realistic assumption, i.e., the eavesdropper is a passive device, meaning the transmitter does not know the CSI of the eavesdropper [49–51]. According to [49], an artificial noise scheme can be applied to improve the average secrecy capacity for cooperative relaying PLC systems if the PLC channels are quasi-static and flat fading ones. Next, [50] analyzed the average secrecy capacity and secrecy outage probability for PLC and hybrid PLC/WLC single relay channels. Finally, [51] introduced an artificial noise scheme to improve the security of the hybrid PLC/WLC channel.

Nevertheless, PLC signals spreading over the electric power circuit is not the only security concern related to PLC systems. In [7], the authors characterized the hybrid PLC-WLC channel, which consists of the cascade combination of the PLC and WLC channels. They showed that part of the PLC signal traveling over unshielded power cables radiates a relevant electromagnetic field that can be sensed by any WLC device located at the vicinity of these cables and operating in the same frequency band as the PLC signal. Since electric power circuits are mainly composed of unshielded power cables, it constitutes a relevant and challenging security breach that may turn PLC systems even more vulnerable to offensive maneuvers that target private information transmitted in PLC systems.

2.3.1 Physical Layer Security in Terms of Voltage Levels

Electric power grids are the most complex systems developed by human beings for energy transmission and distribution from long-distance sources of energy to customers localized in urban and rural areas. Broadly speaking, they consist of three distinct networks that are classified according to the voltage level of the mains frequency: HV, MV, and LV. It is well-know that power transmission and distribution systems are very different in terms of construction and purpose. As a result, it is expected that each of them faces distinct problems related to PLS. Therefore, it is important to highlight the challenges that an eavesdropper may impose on HV, MV, and LV electric power systems because each of them are differently used by PLC systems. In this regard, Subsections *2.3.1.1*, *2.3.1.2*, and *2.3.1.3* discuss PLS issues of PLC systems related to HV, MV, and LV electric power systems, respectively.

2.3.1.1 High-voltage electric power systems

HV electric power grids typically work at alternating current (AC) voltage levels from 69 kV up to 230 kV. They are responsible for transmitting electric energy from the power stations to the distribution stations located in the consumption areas. They cover distances from several tens up to several hundreds of kilometers [58]. Usually, HV electric power grids are constituted of aerial and unshielded power lines. Figure 2 shows a picture of an electric power transmission system. The height of the towers used to support the power cables and the use of HV levels make the physical access by third parties to steal energy extremely dangerous. The same problem arises if a malicious third party tries to physically connect a device to overhear the signal transmitted by a PLC system that is operating over the power cable.

PLC systems operating in HV power lines use very low frequencies because power cables are non ideal conductors, signal attenuation is low at low frequencies, coupling with HV power cables is very expensive, and the point-to-point communication needs to cover long distances. Consequently, sensing the electromagnetic field yielded by the PLC signal traveling over these power lines can be a hard task to be accomplished by a malicious WLC device because the required antenna length is very long. It is noteworthy that at the beginning of XX century the antenna was used to inject/extract PLC signals into/from HV power lines by the electric utility. To this end, a very long cable was installed in parallel to the HV power line. Note that this kind of approach is costly, complex, and difficult to be hidden by an eavesdropper, which is supposed to operate in the shadows.

Moreover, signals traveling over HV power lines can radiate to the MV and LV power lines operating near the HV ones. Then, theoretically, a malicious PLC device connected to the MV or LV electric grid may be able to overhear the private PLC signal traveling over HV power lines. Also, a physical connection of a malicious PLC device to HV power lines deserve attention; however, it is a big challenge to be accomplished due to the high costs related to the acquisition and installation of capacitive coupler[1]. In fact, the installation of a capacitive coupler in HV power lines is a total nonsense initiative because these power lines are very well monitored and the physical installation of a capacitive coupler must be performed when these power lines are not transmitting energy, which requires the consent of the transmission company. Also, it is a high-risk of life without the consent of the owner of the HV transmission system. Regarding the use of the inductive coupling, it is important mentioning that it is not technical and feasible approach to be adopted by a malicious device due to the same reason posed to capacitive coupling.

It is important to highlight that the use of PLC systems in power transmission systems has control and monitoring purposes. As a consequence, the owners of the transmission assets may be impacted by the presence of an eavesdropper. However, this eavesdropper can face remarkable technical and operational challenges to wired and/or wirelessly overhear the transmitted PLC signal through HV electric power systems.

Figure 2 – HV power transmission lines

Source: [90].

[1] The capacitive coupler is a circuit used to physically connect the PLC device to the electric power grid. Basically, it works as passband analog filter because it blocks the main frequency (50 or 60 Hz) and limits the frequency band.

2.3.1.2 Medium-voltage electric power systems

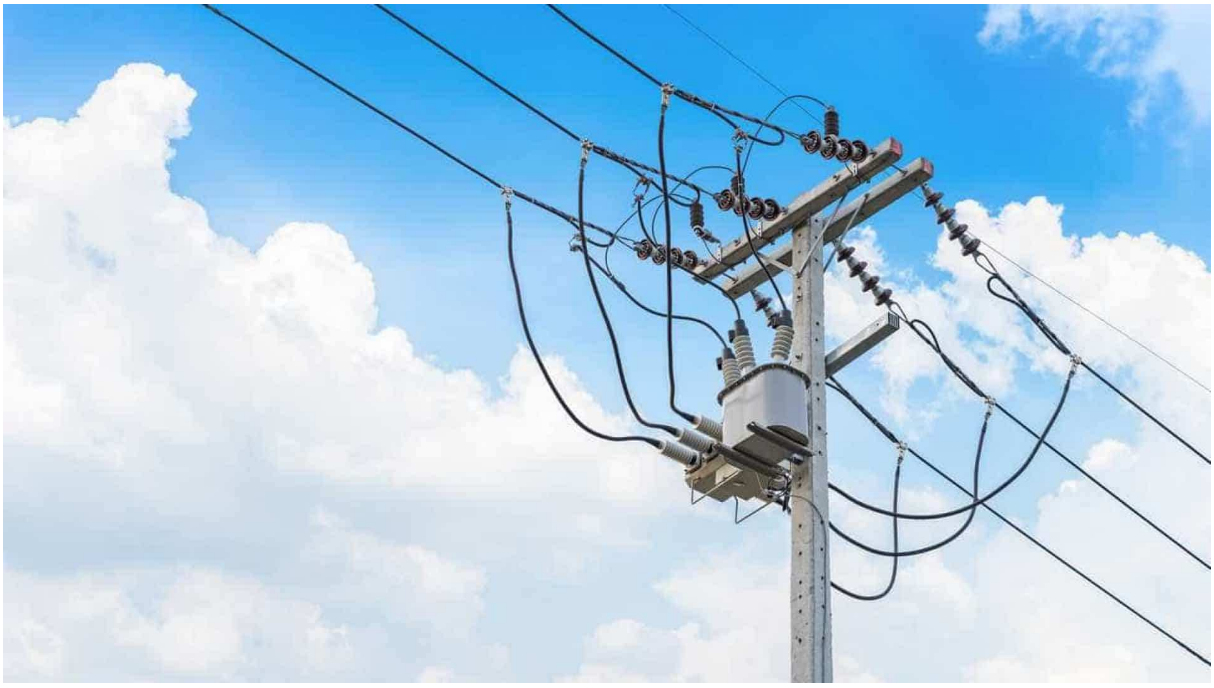
MV electric power grids operate at AC voltage levels from 1 kV up to 69 kV and deliver electric energy from the distribution stations to the pole-mounted transformers, covering distances of few kilometers [58]. This type of electric power grid makes use of aerial and underground power lines. Note that aerial power lines are usually unshielded and widely deployed while the underground power lines are typically shielded for being used in high density downtown areas. Figure 2 shows a picture of the aerial and unshielded MV power lines.

Well-established PLC technologies applied to MV electric power grids usually consider narrowband applications [83–85]; however, there are some solutions for broadband applications as well [91]. While narrowband PLC signals can travel distances greater than 20 km in rural areas (e.g., turtle technologies used for long distance metering), broadband PLC signals can reach distances ranging from hundreds of meters to a few kilometers [58]. These distances indicate how far a malicious PLC device can be located from the PLC transmitter and be considered a threat to the security of PLC systems operating in MV electric power grids. However, a physical connection to MV power lines is still dangerous and the costs of PLC couplers are high, which represent a barrier for physically accessing MV power lines by a malicious PLC device. Note that the connection of inductive couplers to MV power lines can be accomplished without the knowledge of the electric utility because their connection can be carried out without interrupting the energy delivery. On the other hand, the use of capacitive coupling for allowing a malicious device overhear the transmitted PLC signal is more complicated and necessarily demands a coordination with the electric utility.

Regarding the electromagnetic field yielded by narrowband and broadband PLC signals flowing into MV power lines, only the broadband PLC signal is a concern if a WLC malicious device is located close to the MV power line and operates in same frequency band as the PLC system. In fact, the antenna length needed by a malicious WLC device to sense the radiation of the narrowband PLC signal is not feasible. Nonetheless, it is noteworthy that, theoretically, these signals can radiate to the LV electric power grid and, as a consequence, the induced PLC signal in this grid can be overheard by a malicious PLC device connected to the LV power lines. Furthermore, note that the PLC signal radiation do not represent a security problem for PLC systems working on underground MV electric power grids since the power cables are shielded, i.e., they block the electromagnetic field generated by the PLC signal traveling over these lines.

Given the topology of MV power distribution systems and the used voltage levels, access to private information by a malicious device is still dangerous and complex, but less than in HV power transmission systems. On the other hand, as the access to MV power lines is less complicated than HV ones and more users make use of MV power distribution systems, such as metering and public lighting companies, PLS becomes a more relevant issue in these systems than in HV power transmission ones.

Figure 3 – MV power distribution lines



Source: [90].

2.3.1.3 Low-voltage electric power systems

LV electric power grids operate at AC voltage levels below 1 kV and use unshielded power cables. They connect the pole-mounted transformers to the electric utility users. From each pole-mounted transformer, a LV electric power grid delivers energy to tens of users (i.e., between 20 and 80 users) [58]. Regarding PLC systems, LV electric power grids can be classified as indoor or outdoor. The former is related to the power lines that connect the electric power meter to power outlets inside a house or commercial building and usually belongs to the users. Also, indoor and LV power lines cover in-vehicular electric power grids for delivering energy in AC and direct current (DC) forms. The latter corresponds to the electric power grid that connects the pole-mounted transformer to electric power meters and is owned by the electric utility.

Indoor and outdoor LV electric power grids pose a serious security concern in PLC systems because different from HV and MV electric power grids, it is usually easy for physically connecting to LV power lines by using an inductive or capacitive coupler and, as a consequence, for accessing private PLC signals. In particular, the indoor electric power circuit is the easiest one since a malicious PLC device can overhear the private PLC signal through a power outlet. An important aspect of these grids is that the majority of PLC systems operating over them are devoted to broadband applications. This issue may turn private PLC signals related to broadband PLC systems more vulnerable than others associated with narrowband PLC systems to malicious attacks from WLC devices locating near the electric power circuit and operating in the same frequency band as the broadband PLC system. The reason is that the radiated PLC signal can be wirelessly sensed in the vicinity of the power lines by a WLC device with feasible and small-size antennas.

LV power distribution systems constitute the most challenging scenario for ensuring PLS in PLC systems because it is cheap and easy to physically access these systems by a malicious device. Another issue is that a malicious device can be physically connected to the electric power circuit in a hidden way. Overall, the large use of broadband PLC technology in indoor facilities constitutes a security breach because power cables are unshielded and the broadband PLC signal can be more easily sensed by a WLC eavesdropper.

2.3.2 Types of Eavesdroppers

From the point of view of PLS, the broadcast nature and the large use of unshielded power cables turn PLC systems vulnerable to malicious attacks perpetrated by malicious PLC and/or WLC devices. In fact, these characteristics result in the spreading of PLC signals over the electrical power system and their radiation into the air. Then these signals can be overheard by PLC devices, which are physically connected to the power cables, and/or WLC devices, which locate near the electric power grid. Hence, a PLS breach, similar to WLC systems, may occur in PLC systems if PLC and WLC devices are used separated or together. In this regard, it is important to precisely define the types of eavesdroppers that can threaten the PLS of PLC systems. They may be defined as follows:

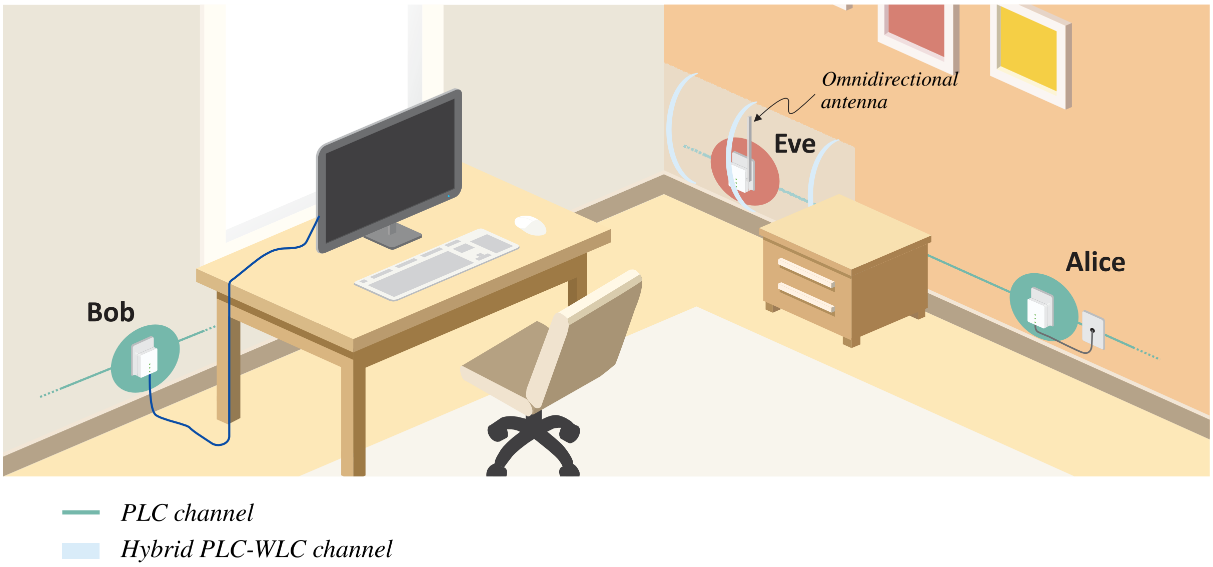
- *PLC eavesdropper*: It is a malicious PLC device that is able to overhear private information exchanged in PLC systems, at the physical layer level, through a physical connection to the electric power circuit over which such systems operate (e.g., the eavesdropper is connected to a power outlet). It can be categorized as narrowband or broadband. The former may be located far from the PLC system (e.g., up to several kilometers) because the attenuation introduced by the communication medium reduces when the used frequencies decreases. The latter must be located near the PLC system (e.g., up to hundreds of meters) because the attenuation in power cables remarkably increases with distance and frequency.

- *WLC eavesdropper*: It is a malicious WLC device that is capable of wirelessly overhearing private information exchanged in a PLC system at the physical layer level. To do so, this eavesdropper must be located near the electric power circuit, in which the PLC system works, and must operate in the same frequency band as the PLC system. This type of eavesdropping occurs due to the inherent characteristic of unshielded power cables: they radiate part of the PLC signal flowing through them. Consequently, a malicious WLC device can sense this radiation. It is worth mentioning that this type of eavesdropping is feasible when the PLC system is broadband (e.g., the frequency band start in 1.7 MHz and can reach hundreds of mega Hertz) because the length of the antenna, which is applied by a malicious WLC device to sense the radiated PLC signal, is relatively small (e.g., less than 1 meter). In narrowband applications, the length of the needed antenna constitutes a technical and practical problem for wirelessly overhearing the private PLC signal since the spectrum content is in low frequencies, i.e., lower than hundreds of kilohertz and, as a consequence, long-size antennas are demanded.

- *Hybrid PLC/WLC eavesdropper*: This malicious device is the result of the parallel combination of both aforementioned eavesdroppers and, as a consequence, it can threaten both narrowband and broadband PLC systems. It is the powerful eavesdropper because it can exploit the existing diversity between both PLC and hybrid PLC-WLC channels to better overhear the transmitted signal and, as a consequence, it is the most dangerous eavesdropper.

Figure 4 depicts a broadband PLC system, where a PLC transmitter (Alice) sends private information to an intended PLC receiver (Bob), while the hybrid PLC/WLC eavesdropper (Eve) overhears this private information through both PLC and hybrid PLC-WLC channels.

Figure 4 – Illustration of broadband data communication between two PLC devices (Alice and Bob) under the presence of a hybrid PLC/WLC eavesdropper (Eve)



Source: Personal collection.

It is noteworthy that a WLC eavesdropper capable of wirelessly overhearing PLC signals can be built by replacing the PLC coupling circuit of a PLC device with an antenna (e.g., an omnidirectional antenna that is designed to operate in the frequency band of interest, such as between 1 MHz and 1 GHz). In addition, the hybrid PLC/WLC device can be built taking into account the discussion presented in [33]. In this study, the authors provided a detailed description of a prototype of the low-bit-rate hybrid PLC/WLC transceiver covering signal processing and PLC- and WLC- analog front-ends.

Moreover, an eavesdropper can overhear the transmitted signal by a node belonging to a PLC system by adopting (consciously or unconsciously) one of the two distinct conditions[2]:

[2] It is important to highlight that the discussion of legal or illegal is related to the way the eavesdropper

- *Legal*: Eve is the owner of an electric power circuit physically connected to another electric power circuit. The latter is used by a PLC system to perform data communication. For instance, a neighbor connected to the outdoor and LV electric power grid inside his home can sense the transmitted signal from a PLC network operating within another home. Also, Eve overhearing the radiated PLC signal constitutes another form of legal access to the PLC signal because power cables are unshielded and, as a consequence, work as antennas. Figure 5 illustrates those types of legal access, where Eve overhears private PLC signals sent by Alice to Bob in a broadband in-home PLC system through both power line and wireless media.

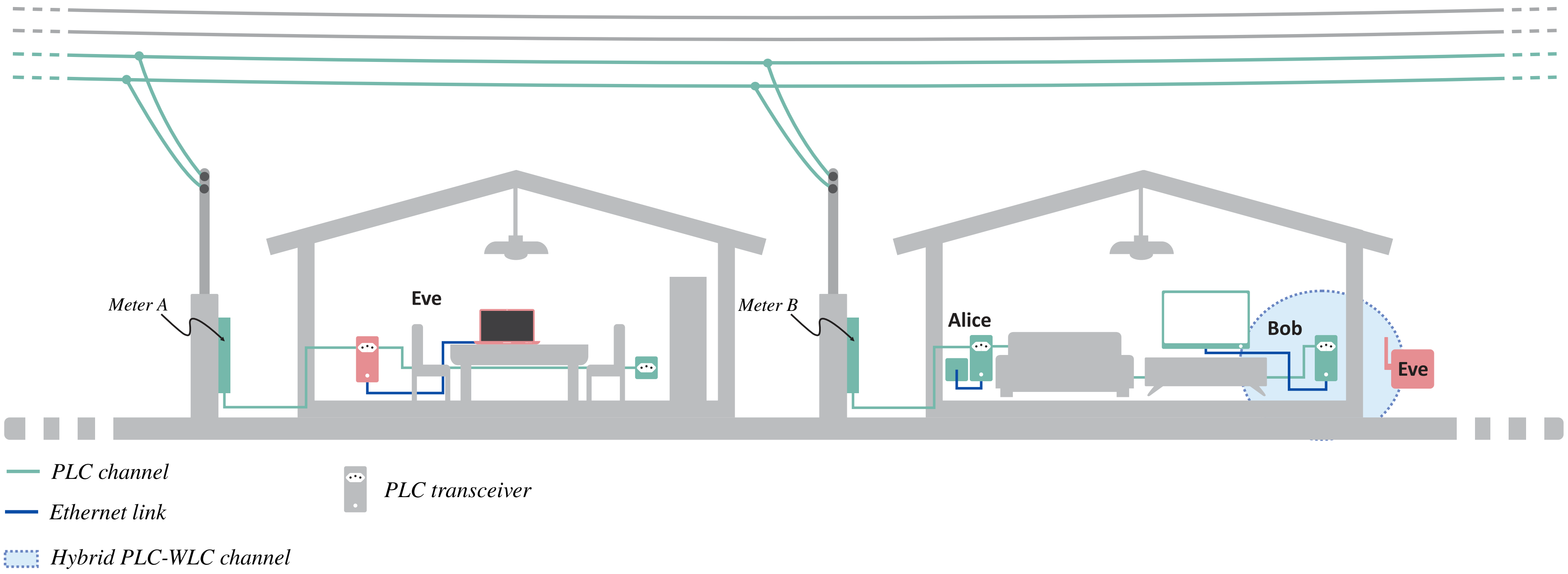
- *Illegal*: Eve performs a non-authorized physical connection to the electric power circuit, which is used by a PLC system to perform data communication. For instance, Eve connects her PLC device to an outlet inside the house in which a PLC system is operating, or to the outdoor and LV electric power grid belonging to the electric utility. In both cases, Eve does not have authorization of the owner of the electric power circuit to be physically connected to it. Figure 6 depicts the situation where Eve illegally overhears the private information sent by Alice to Bob in an in-home broadband PLC system employing a physical connection to outdoor and in-home LV power lines.

It is important to highlight that there are some countermeasures against a few types of legal and illegal access to PLC systems carried out by Eve. For instance, the installation of a PLC signal blocking circuit[3] at the output of the electric power meter connected to the in-home electric power circuit in which the PLC system operates can prevent PLC signals from leaking to the outdoor LV electric power grid. In this way, malicious PLC devices connected to the outdoor LV power grid or to a neighboring indoor LV power grid cannot overhear any private signal transmitted by a PLC system. Furthermore, regarding the WLC eavesdropping, an efficient countermeasure against malicious WLC devices is the use of shielded power cables, as they preclude PLC signals radiate in the air.

can access private information and not the eavesdropper's use of that information.

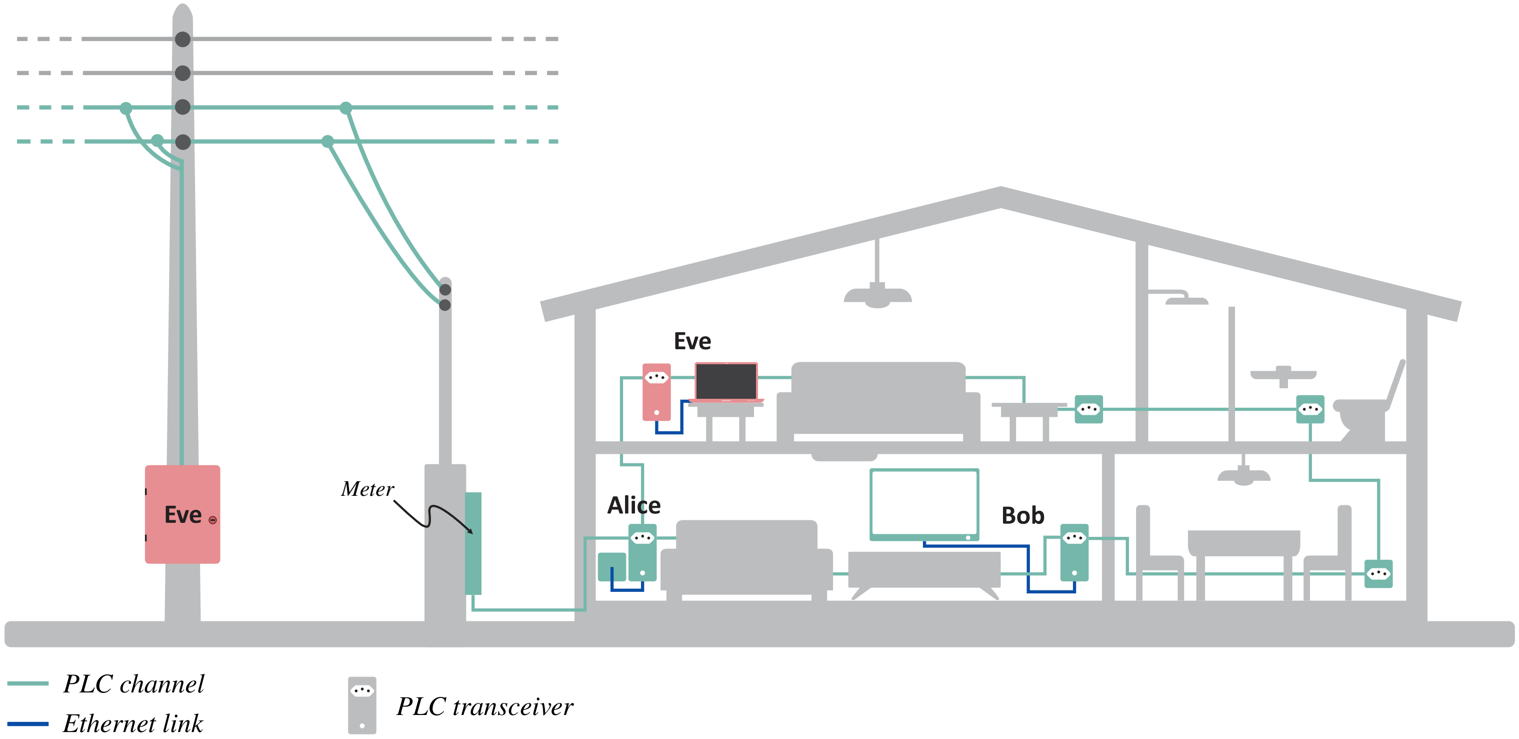
[3] Blocker circuits are band-stop filters designed to block signals whose spectrum is located in a given frequency band.

Figure 5 – Illustration of two types of *legal access* of Eve to private information exchanged between Alice and Bob in a broadband in-home PLC system



Source: Personal collection.

Figure 6 – Illustration of two kinds of *illegal access* of Eve to private information exchanged between Alice and Bob in a broadband in-home PLC system



Source: Personal collection.

2.4 PHYSICAL LAYER SECURITY IN HYBRID PLC/WLC SYSTEMS

The hybrid PLC/WLC system makes use of the parallel combination of both PLC and WLC channels in distinct frequency bands to perform data communication. In other words, it constitutes an augmented scenario in comparison to the discussion carried out in Subsection 2.3. The motivation for addressing this kind of parallel combination is the fact that the use of the existent diversity between PLC and WLC environments turns the data communication system more reliable and flexible. In the context of PLS, the ways and conditions that the eavesdroppers can access private information in a hybrid PLC/WLC system present similarities and differences from the ones related to PLC systems, which were discussed in Subsection 2.3. In this regard, the security at the physical layer level of the hybrid PLC/WLC system can be threaten by the following types of eavesdroppers:

- *PLC eavesdropper*: It is the same malicious device as the one that eavesdrops private information in PLC systems. It overhears private information exchanged between two hybrid PLC/WLC devices through a physical connection to the electric power grid in which the hybrid PLC/WLC system works.

- *WLC eavesdropper*: It is a malicious WLC device that is able to overhear private information from both hybrid PLC-WLC and WLC channels if the hybrid PLC/WLC system is devoted to broadband applications. To this end, this eavesdropper needs to operate with two antennas that cover the frequency ranges for receiving the PLC (baseband) and WLC (baseband or passband) signals. Note that two malicious WLC devices equipped with one antenna each can cooperate to eavesdrop both PLC and WLC signals. In addition, to wirelessly overhear the PLC signal, the WLC eavesdropper needs to be located in the vicinity of the electric power circuit in which the hybrid PLC/WLC system works. As aforementioned, if only frequencies in the baseband are used by the PLC device, then a WLC eavesdropper may wirelessly sense only the broadband PLC signal since the size of the antenna is small and its construction is feasible.

- *Hybrid PLC/WLC eavesdropper*: This malicious device makes use of the parallel combination of both WLC and PLC eavesdroppers. In the context of broadband applications, this powerful eavesdropper may overhear private information exchanged in a hybrid PLC/WLC system through the PLC, WLC, and hybrid PLC-WLC channels. Regarding narrowband applications, the hybrid PLC/WLC eavesdropper is capable of overhearing private information in the hybrid PLC/WLC system only through the WLC and PLC channels.

It is clear that the hybrid system discussed in the current subsection is different from the one addressed in Subsection 2.3. Therefore, it is important mentioning that, in the hybrid PLC/WLC system, Eve can overhear private information sent by Alice to Bob according to the following conditions:

- *Legal*: Eve is connected to her own electric power circuit, which is located close enough to the electric power circuit over which a hybrid PLC/WLC system operates. Then she is able to eavesdrop the PLC signal, which belongs to the hybrid PLC/WLC system, through a PLC device connect to her electric power circuit. Also, Eve can overhear part of the PLC signal that radiates into the air and the WLC signal using WLC devices.
- *Illegal*: Eve makes use of a PLC device connected to the outdoor and LV electric power circuit where the hybrid PLC/WLC system is operating or inside a house that belongs to another person and is located close enough. In both cases the physical access to electric power systems is non-authorized. As well-known, any existing electric power circuit between the electric power meter and the transformer owns to the electric utility and, as a consequence, any kind of non-authorized connection is illegal as well as the use the in-home electric power circuit that belongs to another owner.

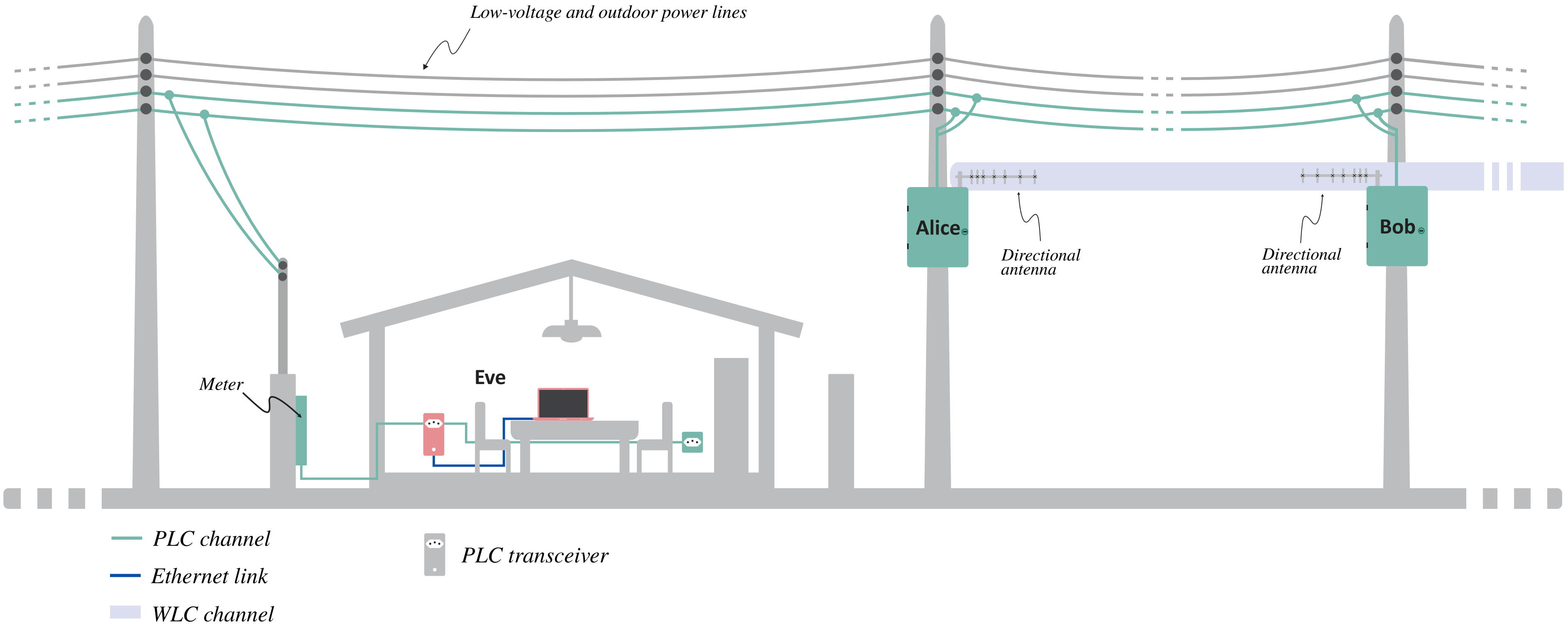
Figure 7 depicts the situation in which Eve overhears private PLC signals of a hybrid PLC/WLC system through an in-home electric power grid. Note that the hybrid PLC/WLC system is operating in an outdoor and LV electric power grid. Also, one states that this situation can either categorize legal access if the house is owned by Eve or illegal access if the house does not belong to Eve and she is not authorized by the owner to access it.

2.5 SUMMARY

This chapter has presented a comprehensive discussion on PLS in PLC systems and then has extended it to hybrid PLC/WLC systems. In this sense, the PLS was addressed taking into account the voltage levels in which electric power grids operate and the types of eavesdroppers that can threaten data communication security as well as their access conditions to private information.

Based on the aforementioned discussion, Chapter 3 and 4 will investigate the PLS of a broadband PLC system under the presence of WLC and PLC eavesdroppers, respectively. Next, in Chapter 5, the PLS of a low-bit-rate hybrid PLC/WLC system will be evaluated considering the threat of WLC, PLC, and hybrid PLC/WLC eavesdroppers under several configurations.

Figure 7 – Illustration of *legal* or *illegal* access of Eve to private information exchanged between Alice and Bob in a low-bit-hybrid PLC/WLC system



Source: Personal collection.

3 THE HYBRID WIRETAP CHANNEL MODEL

The broadband PLC system is a well-established and available technology in the market, mainly used in in-home environments. Nonetheless, the broadcast nature of electric power grids and the fact that they are mainly composed of unshielded power cables may threaten data communication security through these media. It means that a malicious PLC device connected to an existing LV electric power grid inside or outside a residence can overhear private messages exchanged between the transmitter and the legitimate receiver. Furthermore, a malicious WLC device close to the electric power grid and operating in the same frequency band as the PLC system may also overhear private messages exchanged between the transmitter and the legitimate receiver.

Few studies have discussed the PLS in PLC systems for narrowband [46, 49, 50] and broadband [47, 48] applications in the literature. However, those studies have considered the presence of a PLC eavesdropper only. Hence, they have not addressed the potential impact of information leakage, in terms of PLS, from the PLC signal radiating into the air to a malicious WLC device located near the electric power grid and operating in the same frequency band as the PLC system. In this regard, in order to analyze such a scenario in the PLS perspective, the hybrid wiretap channel model is introduced, see Figure 8. Basically, the PLC transmitter (Alice) sends private messages to the legitimate PLC receiver (Bob) whereas a malicious WLC device (Eve) eavesdrops the PLC signal radiated by the power line. In this kind of wiretap channel, Alice can not realize that Eve is overhearing private messages sent to Bob.

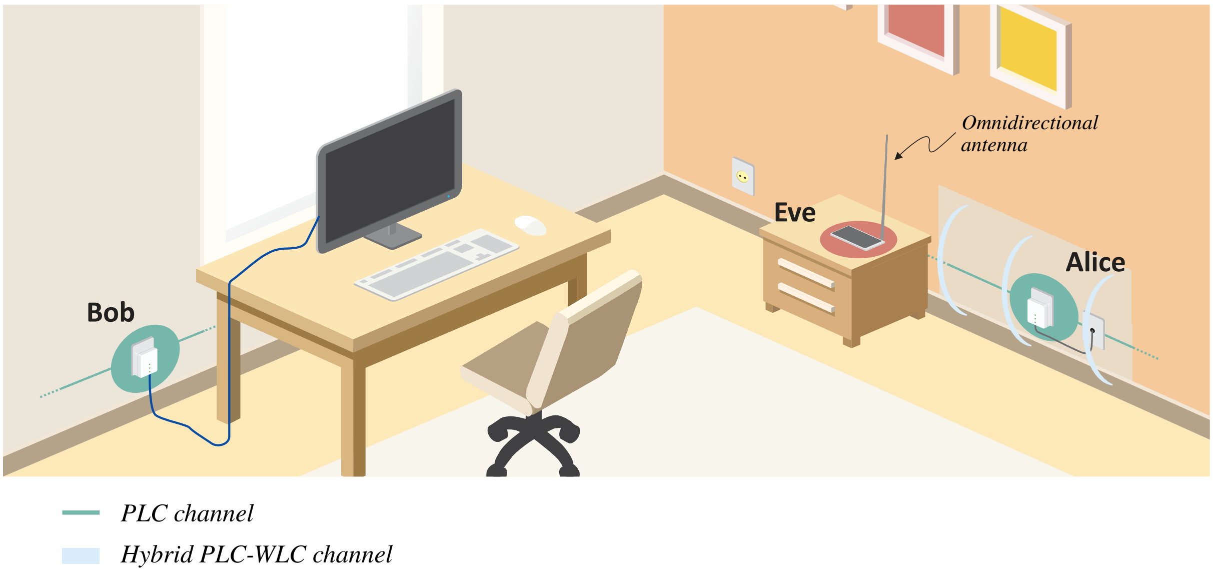
Based on the fact that the widespread use of in-home broadband PLC systems is a reality, this chapter aims to quantitatively discuss PLS when the hybrid wiretap channel model is taking into account and the frequency band 1.7 – 86 MHz (in agreement with ITU-T G.hn [81] and HomePlug AV2 [76]) is covered. The main contributions of this chapter are stated below:

- Introductions of the hybrid wiretap channel model and mathematical formulations of the secrecy outage probability and effective secrecy throughput. Also, discussion on numerical results related to the ergodic achievable secrecy, secrecy outage probability, effective secrecy throughput, and wiretap code rates considering passive eavesdropping (i.e., the CSI of Eve is not available at Alice). Numerical results make use of a real data set obtained from the measurement campaign carried out in Brazilian in-home facilities (see Appendix A) [7, 52].

- Performance analysis considering the following issues: distinct distances between Alice and Bob; different positions of Eve in relation to Alice and Bob; distinct levels of the total transmission power; and two types of resource allocation technique (optimal and uniform). Such an analysis allows to quantify how much a WLC device can threaten the security of a broadband PLC system in practice.

The reminder of this chapter is organized as follows: Section 3.1 introduces the hybrid wiretap channel model; Section 3.2 describes mathematical formulations of the secrecy outage probability and effective secrecy throughput; and, finally, Section 3.3 shows the numerical results.

Figure 8 – Illustration of broadband data communication between two PLC devices (Alice and Bob) under the presence of a WLC eavesdropper (Eve)



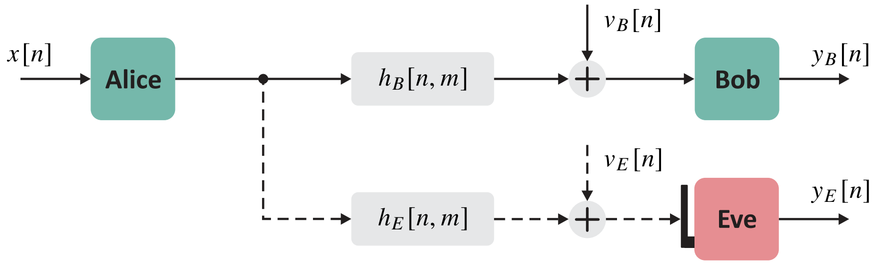
Source: Personal collection.

3.1 PROBLEM FORMULATION

This section is devoted to the PLS problem formulation related to a broadband PLC system when a WLC eavesdropper is located nearby and, as a consequence, it is capable of overhearing private messages exchanged between two PLC devices. It represents a typical situation that can occur in MV and LV electric power grids because both narrowband and broadband PLC systems are used over these grids. In this regard, the block diagram in Figure 9 illustrates the hybrid wiretap channel model. According to this model, a PLC transmitter Alice (A) sends private messages to the legitimate PLC receiver Bob (B). Meanwhile, a malicious WLC device Eve (E) overhears the private messages. Based on [7, 52], the hybrid PLC-WLC channels can completely characterize the wireless propagation of the radiated PLC signal (i.e., the link between Alice and Eve) whereas the channel estimates discussed in [52] can represent the PLC channels regarding Alice-Bob and Alice-Eve links, if the hybrid wiretap channel model refers to broadband and in-home PLC systems.

Considering that both PLC and hybrid PLC-WLC channels are linear time-varying systems, then $\{h_l[n, m]\}$, where $l \in \{B, E\}$, denotes the discrete-time version of the time-varying channels associated with Alice-Bob and Alice-Eve links. Based on this assumption, the

Figure 9 – Block diagrams that represents the hybrid wiretap channel model



Source: Personal collection.
Note: The continuous and dashed lines represent the PLC and hybrid PLC-WLC links, respectively.

discrete-time representation of the received signal at the input of the l^{th} receiver is given by

$$y_l[n] = \sum_{m=-\infty}^{\infty} Ax[m]h_l[n,m] + v_l[n], \tag{3.1}$$

where $\{x[n]\}$ is constituted of an infinite number of N-length symbols (N-block symbols) and refers to the transmitted sequence; $A \in \mathbb{R}_+$ is the amplitude of the transmitted sequence; $h_l[n,m]$ denotes a causal channel impulse response (CIR) seen by the l^{th} receiver in the n^{th} sample when an impulse is injected in the m^{th} sample by Alice so that $h_l[n,m] = 0$ with $n < m$; and $\{v_l[n]\}$ denotes the additive noise sequence. The assumption that both $\{x[n]\}$ and $\{v_l[n]\}$ are independent and wide-sense stationary random processes applies to this formulation.

Whether the time interval associated with an N-block symbol is shorter than the coherence time of the PLC and hybrid PLC-WLC channels in the continuous time-domain, then these channels can be considered linear and time-invariant during a time interval corresponding to an N-block symbol. In this regard, the discrete-time CIR over a time interval corresponding to an N-block symbol is time-invariant and, as a consequence, $h_l[n,m] = h_l[n-m]$, such that finite-length CIRs denoted by $\{\mathrm{h}_l[n]\}_{n=0}^{L_l-1}$, where L_l is the length of the CIR associated with the link between Alice and the l^{th} receiver, is adopted. The vector representation of the discrete-time version of such channels during one N-block symbol duration is $\mathbf{h}_l = [\mathrm{h}_l[0], \mathrm{h}_l[1], \ldots, \mathrm{h}_l[L_l - 1]]^T$, in which $\{\cdot\}^T$ is the transpose operator, whereas $\mathbf{H}_l = [H_l[0], H_l[1], \ldots, H_l[N-1]]^T$ denotes its vector representation in the discrete-frequency domain, where $\mathbf{H}_l = \mathcal{F}[\mathbf{h}_l^T, \mathbf{0}_{N-L_l}^T]^T$, $\mathcal{F} = \frac{1}{\sqrt{N}}\mathbf{W}$, $\mathbf{W} \in \mathbb{C}^{N\times N}$ is the $N \times N$ discrete-time Fourier transform (DFT) matrix, and N denotes the number of sub-channels (see appendix C for more details). Hereafter, the diagonal matrices $\mathbf{\Lambda}_{\mathcal{H}_l} = \mathbf{diag}\{H_l[0], H_l[1], \ldots, H_l[N-1]\}$ and $\mathbf{\Lambda}_{|\mathcal{H}_l|^2} = \mathbf{diag}\{|H_l[0]|^2, |H_l[1]|^2, \cdots, |H_l[N-1]|^2\}$, where $|\cdot|$ denotes the modulus operator, will be considered.

Moreover, the vector representation of the N-block symbol, which is defined in the frequency domain for performing data transmission, is $\mathbf{X} \in \mathbb{C}^{N\times 1}$ so that $\mathbb{E}[\mathbf{X}] = \mathbf{0}_{N\times 1}$, in which $\mathbb{E}[\cdot]$ is the expectation operator and $\mathbf{0}_{N\times 1}$ is the N-length column vector of zeros, and $\mathbf{R}_{\mathbf{XX}} = \mathbb{E}[\mathbf{X}\mathbf{X}^\dagger] = N\mathbf{\Lambda}_P$, where $\{\cdot\}^\dagger$ denotes the Hermitian operator,

$\mathbf{\Lambda}_P = \mathbf{diag}\{P[0],\ P[1],\ \ldots,\ P[N-1]\}$ is the matrix representation of the allocated power, $\mathbf{tr}(\mathbf{\Lambda}_P) = P_T$ is the total transmission power, and $\mathbf{tr}(\cdot)$ is the trace operator. Also, $\mathbf{V}_l \in \mathbb{C}^{N\times 1}$ is the frequency domain vector representation of the zero mean additive noise, such that $\mathbf{R}_{\mathbf{VV},l} = \mathbb{E}[\mathbf{V}_l\mathbf{V}_l^{\dagger}] = N\mathbf{\Lambda}_{P_{V_l}}$, $\mathbf{\Lambda}_{P_{V_l}} = \mathbf{diag}\left\{P_{V_l}[0],\ P_{V_l}[1],\ \ldots, P_{V_l}[N-1]\right\}$, and $P_{V_l}[k]$ is the additive noise power in the k^{th} sub-channel.

Given the aforementioned formulation, the following questions arise: *How secure is a broadband PLC system at the physical layer level, from a practical perspective, when Eve is a WLC device operating in the same frequency band and is near Alice or Bob? In other words, how much information is leaked from the radiated PLC signal to Eve and what is its impact on the secrecy outage probability and the effective secrecy throughput on broadband PLC systems? Furthermore, how is the behavior of the wiretap codes R_B and R_E?* Aiming to answer these questions, Section 3.2 deduces the secrecy outage probability and effective secrecy throughput for the hybrid wiretap channel model and Section 3.3 discusses numerical results that support important findings related to PLS in PLC systems.

3.2 PHYSICAL LAYER SECURITY METRICS AND WIRETAP CODE RATES

This section deduces mathematical expressions to compute the secrecy outage probability and effective secrecy throughput for the hybrid wiretap channel model. To do so, similar to the linear Gaussian relay channel (LGRC) addressed in [92], PLC and hybrid PLC-WLC channels are assumed to be N-block linear Gaussian channels with finite memory and, as a consequence, $L_{\max} = \max\limits_{l} L_l$. Based on this channel model, the inter-block interference caused by the memory of CIRs and the correlated noises make difficult to evaluate the achievable data rate [93]. On the other hand, the proposal in [93] can overcome this drawback since it states that the N-block circular Gaussian relay channel (CGRC) eliminates the inter-block interference when $N \gg L_{\max}$. Besides, the LGRC tends to N-CGRC as $N \to \infty$. Hence, N-CGRC channel model applies to PLC and hybrid PLC-WLC channels when $N \to \infty$ applies to deal with dispersive channels.

Assuming perfect synchronization, the vector representation, in the frequency domain, of the received N-block symbol at the l^{th} receiver is given by

$$\mathbf{Y}_l = \mathbf{\Lambda}_{\mathcal{H}_l}\mathbf{X} + \mathbf{V}_l. \tag{3.2}$$

Then the mutual information between Alice and the l^{th} receiver can be expressed as [94, pp. 92]

$$\begin{aligned} I(\mathbf{X};\mathbf{Y}_l) &= \hbar(\mathbf{Y}_l) - \hbar(\mathbf{Y}_l|\mathbf{X}) \\ &= \hbar(\mathbf{Y}_l) - \left[\hbar(\mathbf{\Lambda}_{\mathcal{H}_l}\mathbf{X}|\mathbf{X}) + \hbar(\mathbf{V}_l|\mathbf{X})\right] \\ &= \hbar(\mathbf{Y}_l) - \hbar(\mathbf{V}_l), \end{aligned} \tag{3.3}$$

Considering the additive noise and transmitted symbols as Gaussian random processes, the entropy of $\mathbf{Y}_l$ and $\mathbf{V}_l$ are given by

$$\hbar(\mathbf{Y}_l) = \frac{1}{2}\log_2\left[(2\pi e)^N \det(\mathbf{R}_{\mathbf{YY},l})\right] \tag{3.4}$$

and

$$\hbar(\mathbf{V}_l) = \frac{1}{2}\log_2\left[(2\pi e)^N \det(\mathbf{R}_{\mathbf{VV},l})\right], \tag{3.5}$$

respectively, in which $\hbar(\cdot)$ refers to the differential entropy function, $\det(\mathbf{\Lambda}_D)$ is the determinant of the matrix $\mathbf{\Lambda}_D$, and $\mathbf{R}_{\mathbf{YY},l} = \mathbf{\Lambda}_{\mathcal{H}_l}\mathbf{R}_{\mathbf{XX}}\mathbf{\Lambda}_{\mathcal{H}_l}^{\dagger} + \mathbf{R}_{\mathbf{VV},l}$ (see Appendix D for more details). Thus, the capacity between Alice and the l^{th} receiver can be expressed as

$$\begin{aligned} C_l &= \max_{f_{\mathbf{X}}(\mathbf{x}):\mathbf{tr}(\mathbf{R}_{\mathbf{XX}})\leq NP_T} I(\mathbf{X};\mathbf{Y}_l) \\ &= \max_{\mathbf{\Lambda}_P} \log_2\left[\det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_l}\right)\right] \text{ [bps/Hz]}, \end{aligned} \tag{3.6}$$

where $f_{\mathbf{X}}(\mathbf{x})$ is the joint density function of $\mathbf{X}$ and

$$\begin{aligned} \mathbf{\Lambda}_{\gamma_l} &= \frac{\mathbf{\Lambda}_{\mathcal{H}_l}\mathbf{R}_{\mathbf{XX}}\mathbf{\Lambda}_{\mathcal{H}_l}^{\dagger}}{\mathbf{R}_{\mathbf{VV},l}} \\ &= \mathbf{\Lambda}_P\mathbf{\Lambda}_{|\mathcal{H}_l|^2}\mathbf{\Lambda}_{P_{V_l}}^{-1}. \end{aligned} \tag{3.7}$$

Hence, the secrecy capacity is given by [95]

$$C_S = \max_{f_{\mathbf{X}}(\mathbf{x}):\mathbf{tr}(\mathbf{R}_{\mathbf{XX}})\leq NP_T} \left[I(\mathbf{X};\mathbf{Y}_B) - I(\mathbf{X};\mathbf{Y}_E)\right]^+, \tag{3.8}$$

in which $\max[b]^+ = \max(0, b)$. Notice that (3.8) is difficult to calculate. By using [95], this difficulty can be handled. Basically, it suggests the use of a lower bound that can be applied to the hybrid wiretap channel model as follows:

$$\begin{aligned} C_S &\geq \left[\max_{f_{\mathbf{X}}(\mathbf{x}):\mathbf{tr}(\mathbf{R}_{\mathbf{XX}})\leq NP_T} I(\mathbf{X};\mathbf{Y}_B) - \max_{f_{\mathbf{X}}(\mathbf{x}):\mathbf{tr}(\mathbf{R}_{\mathbf{XX}})\leq NP_T} I(\mathbf{X};\mathbf{Y}_E)\right]^+ \\ &= \left[C_B - C_E\right]^+, \end{aligned} \tag{3.9}$$

where C_B and C_E denote the capacities related to Alice-Bob and Alice-Eve links, respectively. Based on the aforementioned formulations and discussions, the achievable secrecy rate of the hybrid wiretap channel model is given by

$$R_S = \frac{1}{N}\left[\log_2\left[\det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_B}\right)\right] - \log_2\left[\det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_E}\right)\right]\right]^+ \text{ [bps/Hz]}. \tag{3.10}$$

As discussed in [96], a wiretap code is necessary to obtain the secrecy capacity. Further, for having a reliable and secure data communication, such codes have to fulfill the following requirements [96]:

- *Reliability constraint*: The error probability of Bob must decrease as the code length increases.
- *Secrecy constraint*: The rate of information leakage to Eve must decrease as the code length increases.

In this sense, the wiretap code can be designed based on the following rates:

- Rate of transmitted codewords, $R_B \in \mathbb{R}_+$;
- Rate of transmitted confidential information (i.e., target secrecy rate), $R \in \mathbb{R}_+$.

Notice that $R_B \leq C_B$ is chosen to ensure the reliability constraint whereas $R_E > C_E$ fulfills the secrecy constraint, in which $R_E = R_B - R$ is the rate of redundancy used to confuse Eve. Also, to achieve the maximum R, the complete CSIs of Bob and Eve have to be available at Alice.

3.2.1 Secrecy Outage Probability

In a more practical scenario, Eve is a passive device, i.e., she does not transmit any information to Alice. Consequently, the knowledge of Eve's CSI is unavailable at Alice and then $R_E > C_E$ can not be guaranteed, where $R_E \in \mathbb{R}_+$ is the redundancy rate. In this context, the secrecy outage probability can be an useful parameter to measure secrecy at the physical layer level. Therefore, the secrecy outage probability is expressed as

$$\begin{aligned} P_S(R) &= \mathbb{P}\left\{R_S < R\right\} \\ &= \mathbb{P}\left\{\det\left(\frac{\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_B}}{\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_E}}\right) < 2^{RN}\right\}, \end{aligned} \tag{3.11}$$

in which $\mathbb{P}\{c > d\}|(c, d) \in \mathbb{R}^2$ denotes the probability that c is greater than d. Notice that perfect secrecy is achieved when $R_S > R$ whereas $R_S < R$ means that perfect secrecy is not guaranteed.

3.2.2 Effective Secrecy Throughput

Despite of the secrecy outage probability, $P_S(R)$, be a useful parameter to measure secrecy, it does not separate reliability and secrecy requirements. In this regard, [96] proposed a new framework to estimate R_B and R_E based on the effective secrecy throughput. Then, following [96], the secrecy outage probability can be rewritten as

$$\begin{aligned} O_s(R_E) &= \mathbb{P}\left\{R_E < C_E\right\} \\ &= \mathbb{P}\left\{2^{R_E N} < \det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_E}\right)\right\}, \end{aligned} \tag{3.12}$$

whereas the reliability outage probability is given by

$$\begin{aligned} O_r(R_B) &= \mathbb{P}\left\{R_B > C_B\right\} \\ &= \mathbb{P}\left\{2^{R_B N} > \det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_B}\right)\right\}. \end{aligned} \tag{3.13}$$

Therefore, the effective secrecy throughput can obtained from

$$\Psi(R_E, R_B) = (R_B - R_E)[1 - \mathcal{O}_r(R_B)][1 - \mathcal{O}_s(R_E)], \tag{3.14}$$

where $(R_B - R_E)$ represents the target secrecy rate R whereas $[1 - \mathcal{O}_r(R_B)][1 - \mathcal{O}_s(R_E))]$ quantifies the probability that the information is securely transmitted from Alice to Bob. Thus, $\Psi(R_E, R_B)$ quantifies the average secrecy rate at which the messages are transmitted from Alice to Bob without being leaked to Eve. Finally, as stated in [96], the constraints $R_B > 0$ and $0 < R_E < R_B$ apply to (3.14). Such constraints result in $\Psi(R_E, R_B) \geq 0$.

The computation of the effective secrecy throughput is relevant in the following situations:

- *Situation #1*: Alice knows C_B (i.e., the complete CSI of Bob is available at Alice) and does not know C_E. In this case, $R_B = C_B$ and, as a consequence, $\mathcal{O}_r(R_B) = 0$ and the effective secrecy throughput can be expressed as

$$\Psi_1(R_E) = (C_B - R_E)[1 - \mathcal{O}_s(R_E)]. \tag{3.15}$$

In this regard, the redundancy rate that maximizes (3.15) is given by

$$R_E^* = \underset{0<R_E<C_B}{\arg\max}\ \Psi_1(R_E) \tag{3.16}$$

and then the maximum effective secrecy throughput is $\Psi_1^* = \Psi_1(R_E^*)$.

- *Situation #2*: Alice does not know the complete CSI of Bob and Eve and, as a consequence, C_B and C_E. In this case, the effective secrecy throughput is given by

$$\Psi_2(R_E, R_B) = (R_B - R_E)[1 - \mathcal{O}_r(R_B)][1 - \mathcal{O}_s(R_E)]. \tag{3.17}$$

The codeword and redundancy rates which maximize (3.17) are defined as

$$(R_B^\star, R_E^\star) = \underset{0<R_B, 0<R_E<R_B}{\arg\max}\ \Psi_2(R_B, R_E) \tag{3.18}$$

and, as a consequence, the maximum effective secrecy throughput is $\Psi_2^* = \Psi_2(R_B^\star, R_E^\star)$.

3.3 NUMERICAL RESULTS

This section numerically assesses the secrecy outage probability, effective secrecy throughput, and wiretap code rates for the hybrid wiretap channel model when Eve is a passive device. Also, the situations where Alice has and does not have the complete knowledge of Bob's CSI are considered. Moreover, the ergodic achievable secrecy rate $\bar{R}_S = B_w \mathbb{E}_{\mathcal{H}_B, \mathcal{H}_E}[R_S]$ is also evaluated, where $\mathbb{E}[\cdot]$ is the expectation operator and B_w is the frequency bandwidth. Although theoretical, $\bar{R}_S$ is an interesting parameter to quantify the information leakage to Eve when data communication is carried out between Alice and Bob. The frequency band 1.7 – 86 MHz (in compliance with ITU-T G.hn [81] and HomePlug AV2 [76]) and $N = 1727$ are taken into account. Note that the resulting frequency bandwidth of the sub-channels, $\Delta f = B_w/N = 47.8$ kHz, does not exceed the coherence bandwidth of the normalized signal-to-noise ratios (nSNRs) related to the PLC and hybrid PLC-WLC channels [7, 8, 52]. The optimal power allocation (OA) based on the water-filling algorithm [97] and uniform power allocation (UA)[1] techniques are considered for analyzing ergodic achievable rate and secrecy outage probability. Regarding effective secrecy throughput and wiretap code rates, only UA technique is taken into account because the numerical results related to ergodic achievable rate and secrecy outage probability do not show a significant difference between OA and UA techniques. The total transmission power (P_T) ranges from -30 to 30 dBm. Note that $P_T \in [0, 30]$ dBm refers to the practical values.

The data set obtained from a measurement campaign carried out in Brazilian houses is used to represent the hybrid wiretap channel model [7, 8, 52]. This data set comprises estimates of PLC and hybrid PLC-WLC channel frequency responses (CFRs) (for more details, see Appendix A), which are used to represent, respectively, Alice-Bob and Alice-Eve links. Even though the adopted data set is from a measurement campaign carried out in Brazilian houses, their results may be extended to other environments, such as commercial buildings and even MV and LV outdoor electric power grids, since they point out under what conditions PLS can be compromised adopting a practical perspective. Also, the estimates of hybrid PLC-WLC CFRs allow to assess the following two types of situations that can be addressed by the hybrid wiretap channel model:

- *Eve is close to Alice*: This situation is represented by the hybrid PLC-WLC short-path (SP) channels (see Appendix A for details).
- *Eve is far from Alice*: This situation is represented by the hybrid PLC-WLC long-path (LP) channels (see Appendix A for details).

For the sake of brevity, the hybrid PLC-WLC SP and hybrid PLC-WLC LP channels are named SP and LP channels, respectively.

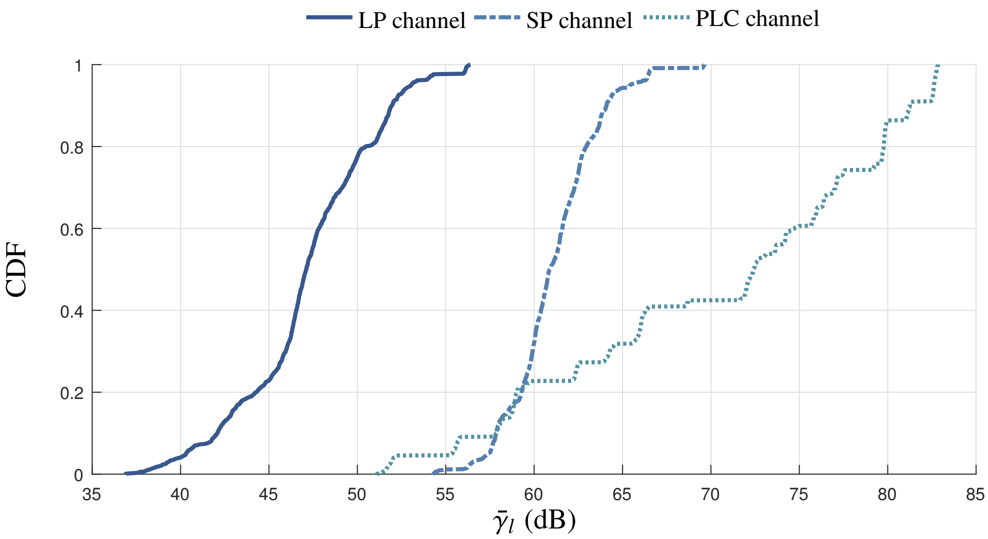
Figure 10 shows the cumulative distribution functions (CDFs) of the multi-channel nSNR, $\bar{\gamma}_l$, regarding PLC and hybrid PLC-WLC channels. According to [97], the mathematical definition of the multi-channel nSNR is

$$\bar{\gamma}_l \triangleq \det\left(\mathbf{I}_N + \mathbf{\Lambda}_{|\boldsymbol{\mathcal{H}}_l|^2}\mathbf{\Lambda}^{-1}_{P_{\mathrm{V}_l}}\right)^{1/N} - 1. \tag{3.19}$$

From Figure 10, note that the maximum values of $\bar{\gamma}_l$ found for LP, SP, and PLC channels are, respectively, 56.4, 69.6, and 82.8 dB whereas the minimum values of $\bar{\gamma}_l$ are, respectively, 36.9, 54.3, and 51.1 dB. In addition, for a probability less than or equal to 0.9, $\bar{\gamma}_l$ can reach, respectively, 51.9, 64.1, and 81.2 dB for the LP, SP, and PLC channels. On the other hand,

[1] In the UA technique, P_T is equally distributed over N sub-carriers, i.e., the power P_T/N is allocated to each sub-carrier.

Figure 10 – Cumulative distribution function of $\bar{\gamma}_l$ in dB



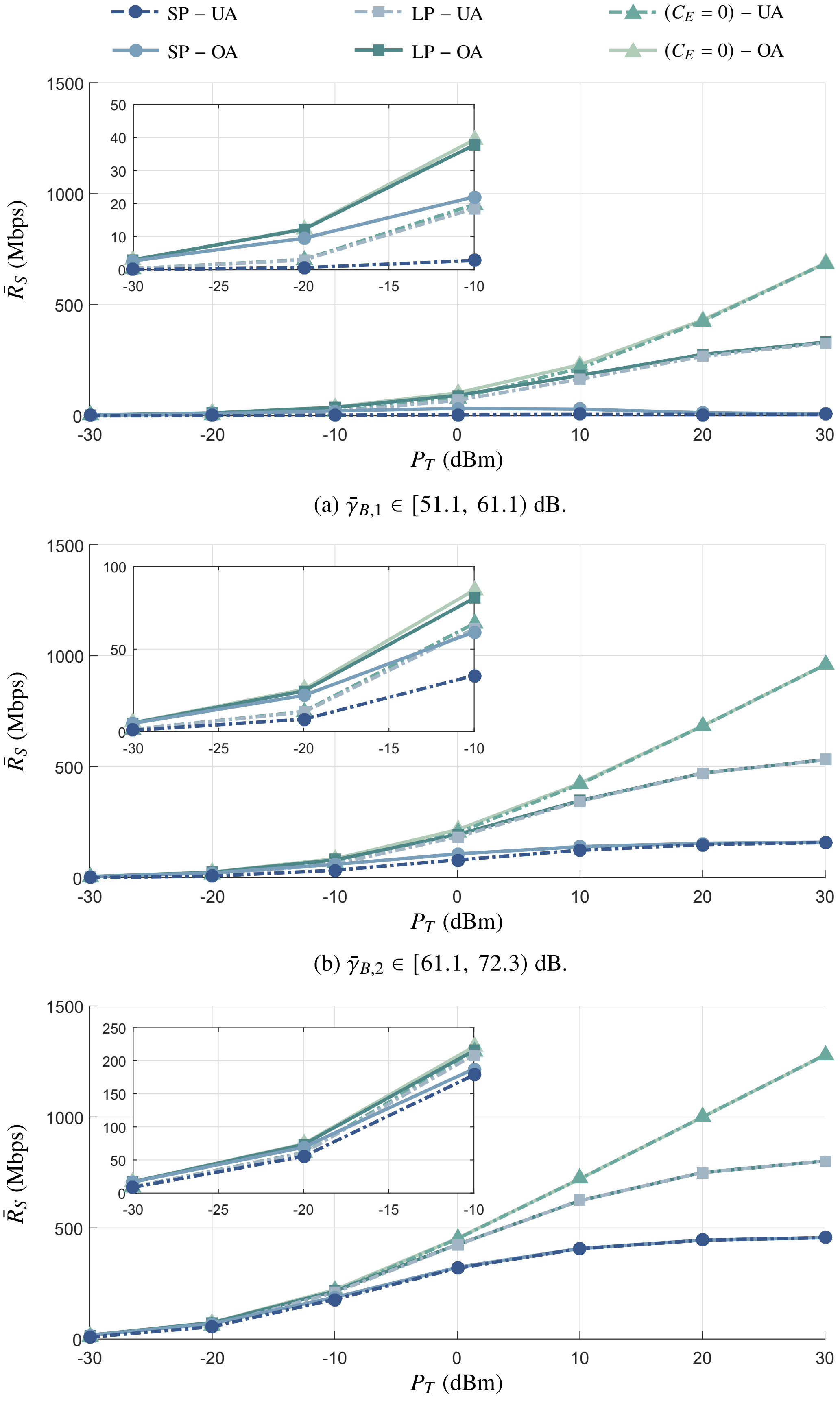
Source: Personal collection.

if a probability less than or equal to 0.5 is considered, then $\bar{\gamma}_l$ can reach, respectively, 47.1, 60.9, and 72.4 dB. Moreover, observe that as Bob moves away from Alice, $\bar{\gamma}_B$ decreases and, as a consequence, PLS may be impaired. On the other hand, if Bob is close to Alice, high values of $\bar{\gamma}_B$ are observed, making the decoding of the information exchanged between Alice and Bob a hard task to be accomplished by Eve. In this regard, unless stated otherwise, the assessment of numerical results considers three distinct ranges of $\bar{\gamma}_B$: $\bar{\gamma}_{B,1} \in [51.1,\ 61.1)$ dB, $\bar{\gamma}_{B,2} \in [61.1,\ 72.3)$ dB, and $\bar{\gamma}_{B,3} \in [72.3,\ 82.9]$ dB.

3.3.1 Analysis of Ergodic Achievable Secrecy Rate

Figures 11(a), (b), and (c) show $\bar{R}_S \times P_T$ for the hybrid wiretap channel model under the adoption of OA and UA together with $\bar{\gamma}_{B,1}$, $\bar{\gamma}_{B,2}$, and $\bar{\gamma}_{B,3}$, respectively. In addition, the scenario in which Eve is far away from Alice and Bob (i.e., $C_E = 0$) is used as a reference to analyze the information leakage from Alice-Bob link to Eve. Figures 11(a), (b), and (c) show that the difference between OA and UA is minimal regardless of the values of P_T and the distance between Alice and Bob. Also, notice that as Bob moves away from Alice, R_S decreases in both SP and LP scenarios. In particular, for $\bar{\gamma}_{B,1}$ (see Figure 11(a)), the SP scenario has the lowest values of $\bar{R}_S$ when UA is adopted, regardless of the values of P_T. For instance, $\bar{R}_S$ achieves only 22 Mbps when $P_T = -10$ dBm and OA are adopted. Also, the differences between SP and LP scenarios, in terms of $\bar{R}_S$, are almost the same in Figures 11(a), (b), and (c), achieving 322.9, 355.2, and 353.7 Mbps, respectively, for $P_T = 30$ dBm. Lastly, when $P_T = 30$ dBm, the values of $\bar{R}_S$ regarding SP, LP, and $C_E = 0$ scenarios are equal to, respectively, 5.8, 328.7, and 685.8 Mbps in Figure 11(a); 187.6, 542.8, and 987.9 Mbps in Figure 11(b); and 471.0, 824.7, and 1,296.0 Mbps in Figure 11(c). Note that Table 3 summarizes those values of $\bar{R}_S$ obtained when $P_T = 30$ dBm and OA are taken into account.

Figure 11 – Hybrid wiretap channel model: $\bar{R}_S \times P_T$ under the adoption of OA and UA techniques



(a) $\bar{\gamma}_{B,1} \in [51.1,\ 61.1)$ dB.

(b) $\bar{\gamma}_{B,2} \in [61.1,\ 72.3)$ dB.

(c) $\bar{\gamma}_{B,3} \in [72.3,\ 82.9]$ dB.

Source: Personal collection.

Table 3 – $\bar{R}_S$ for the hybrid wiretap channel model considering $P_T = 30$ dBm and OA technique

Ergodic achievable secrecy rate (Mbps)			
	$\bar{\gamma}_{B,1}$	$\bar{\gamma}_{B,2}$	$\bar{\gamma}_{B,3}$
SP	5.8	187.6	471.0
LP	328.7	542.8	824.7
$C_E = 0$	685.8	987.9	1,296.0

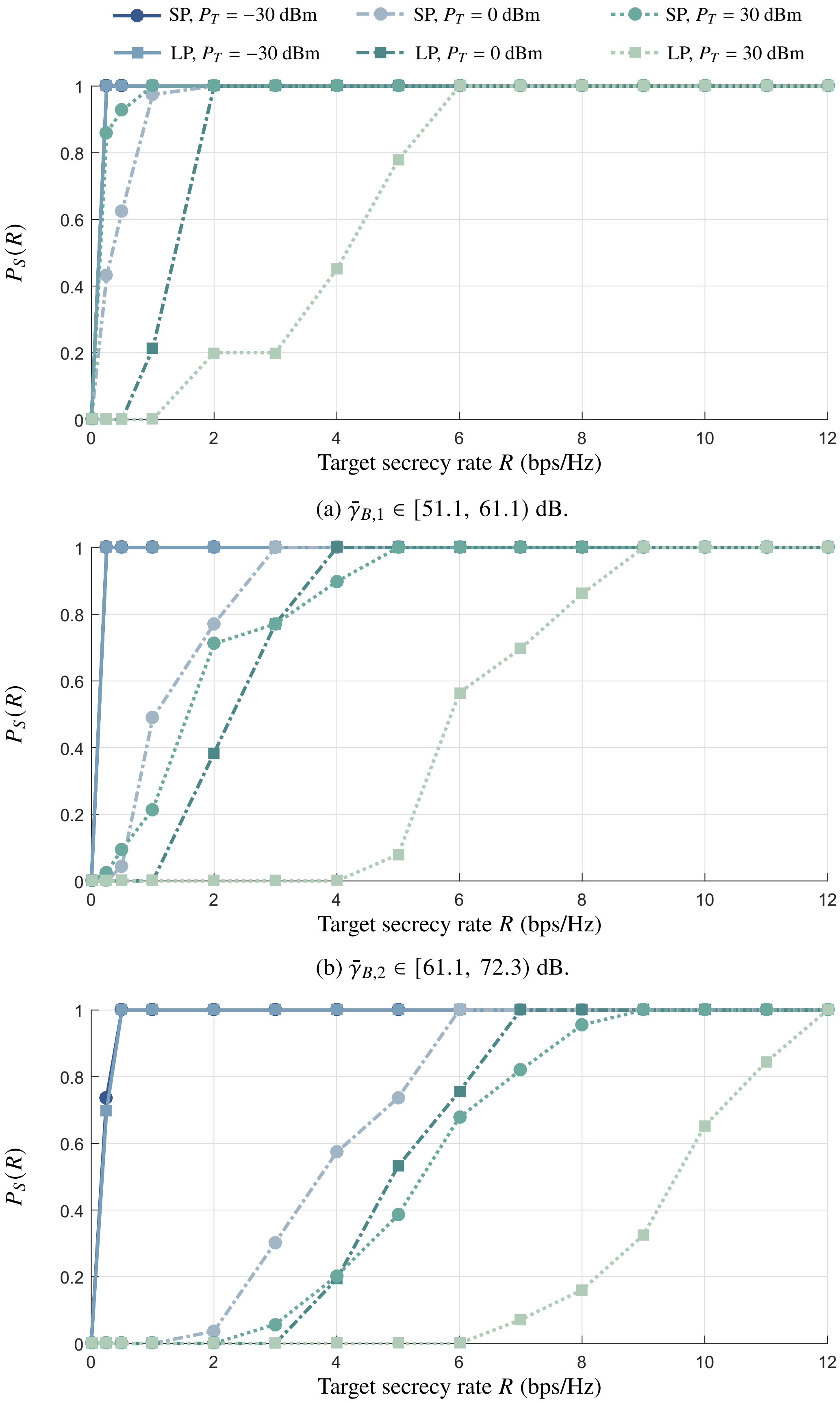
Source: Personal collection.

3.3.2 Analysis of Secrecy Outage Probability

Figures 12 and 13 depict $P_S \times R$ for the hybrid wiretap channel model considering OA and UA, respectively, as well as $P_T \in \{-30, 0, 30\}$ dBm. Also, $\bar{\gamma}_{B,1}$, $\bar{\gamma}_{B,2}$, and $\bar{\gamma}_{B,3}$ are considered in Figures 12(a), (b), and (c), respectively, and in Figures 13(a), (b), and (c), respectively. The figures show a minimal difference between OA and UA so that a small advantage in favor of OA can be observed in $\bar{\gamma}_{B,1}$ and $\bar{\gamma}_{B,2}$ cases when P_T is equal to -30 and 0 dBm. Furthermore, notice that as Bob moves away from Alice, $P_S(R)$ increases significantly. In particular, considering OA, $P_T = 30$ dBm, and $R = 6.00$ bps/Hz, SP and LP scenarios present $P_S(R)$ equal to 1 for $\bar{\gamma}_{B,1}$. Also, SP and LP scenarios show $P_S(R)$ around 0.64 and equal to 0, respectively, for $\bar{\gamma}_{B,3}$ and $P_S(R)$ equal to 1 and around 0.47, respectively, for $\bar{\gamma}_{B,2}$. Finally, observe that when $P_T = -30$ dBm and $R \geq 1.00$ bps/Hz, $P_S(R)$ is equal to 1 in both SP and LP scenarios regardless of the distance between Alice and Bob and the used power allocation technique. Finally, as shown in Figures 12(a) and 13(a), the practical values of total transmission power (i.e., 0 and 30 dBm) result in high values of $P_S(R)$ for the SP scenario.

Figures 14 and 15 show $P_S(R) \times P_T$ for the hybrid wiretap channel model considering OA and UA, respectively, as well as $R \in \{0.25, 0.50, 1.00\}$ bps/Hz. In addition, $\bar{\gamma}_{B,1}$, $\bar{\gamma}_{B,2}$, and $\bar{\gamma}_{B,3}$ are adopted in Figures 14(a), (b), and (c), respectively, and in Figures 15(a), (b), and (c), respectively. Note that, as P_T increases the difference between OA and UA tends to zero. On the other hand, if P_T decreases, a small improvement in favor of OA occurs. Considering the LP scenario, OA, and practical values of total transmission power, i.e., $0 \leq P_T \leq 30$ dBm, $P_S(R)$ is close to zero for $\bar{\gamma}_{B,1}$, $\bar{\gamma}_{B,2}$, and $\bar{\gamma}_{B,3}$ regardless of R, except when $P_T = 0$ dBm in the $\bar{\gamma}_{B,1}$ case, in which $P_S(R)$ is around 0.2. Concerning the SP scenario, if OA and $0 \leq P_T \leq 30$ dBm are taken into account, $P_S(R)$ is close to zero for $\bar{\gamma}_{B,3}$ regardless of R and for $\bar{\gamma}_{B,2}$ when R is equal to 0.25 bps/Hz. Besides, $R = 0.50$ and 1.00 bps/Hz provide $P_S(R) < 0.1$ and $P_S(R) < 0.5$, respectively, for $\bar{\gamma}_{B,2}$. Lastly, observe that $P_S(R)$ values higher than 0.40, 0.60 and 0.90 are found when R is equal to 0.25, 0.50, and 1.00 bps/Hz, respectively, for $\bar{\gamma}_{B,1}$.

Figure 12 – Hybrid wiretap channel model: $P_S(R) \times R$ for $P_T \in \{-30, 0, 30\}$ dBm under the adoption of OA technique



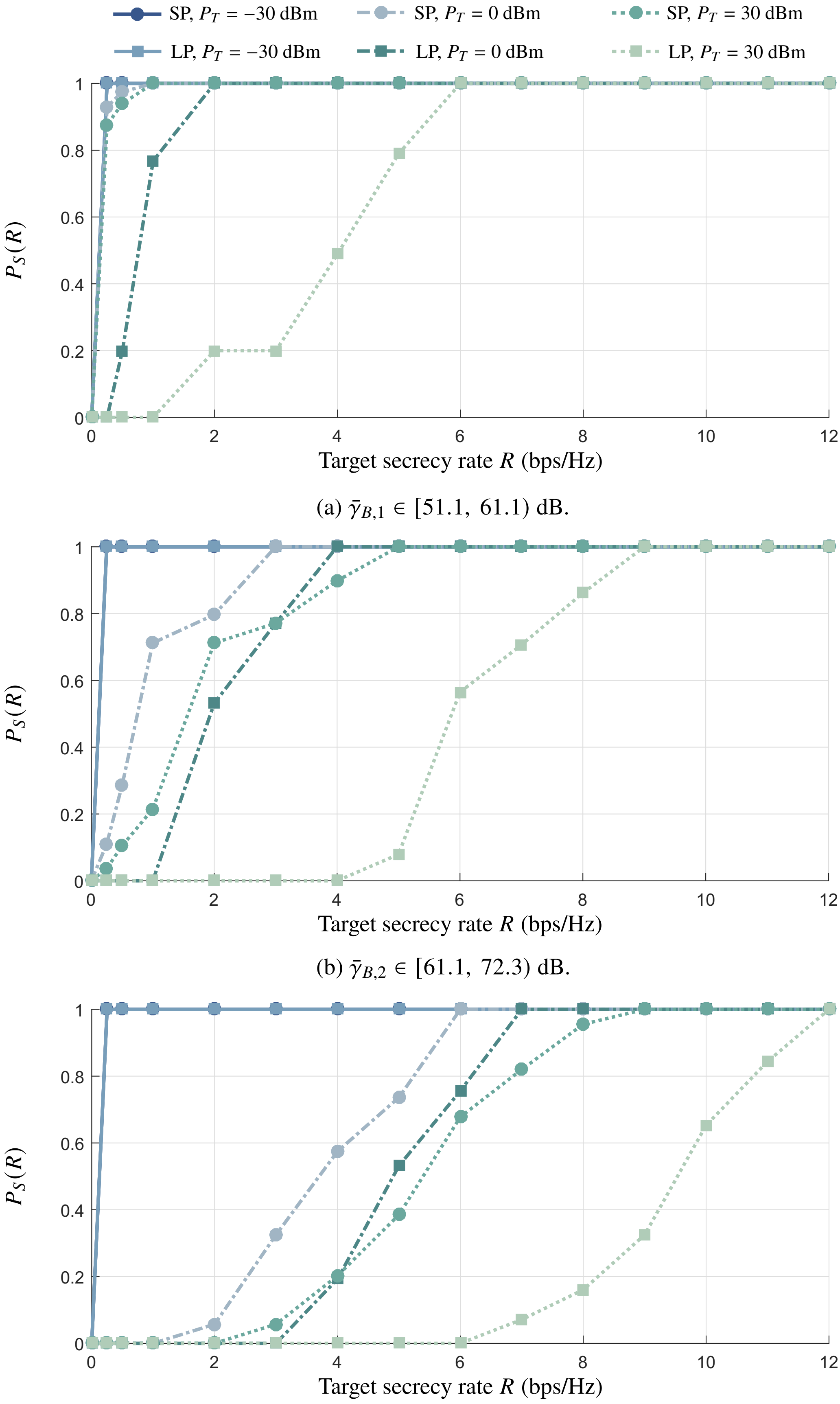
(a) $\bar{\gamma}_{B,1} \in [51.1,\ 61.1)$ dB.

(b) $\bar{\gamma}_{B,2} \in [61.1,\ 72.3)$ dB.

(c) $\bar{\gamma}_{B,3} \in [72.3,\ 82.9]$ dB.

Source: Personal collection.

Figure 13 – Hybrid wiretap channel model: $P_S(R) \times R$ for $P_T \in \{-30, 0, 30\}$ dBm under the adoption of UA technique



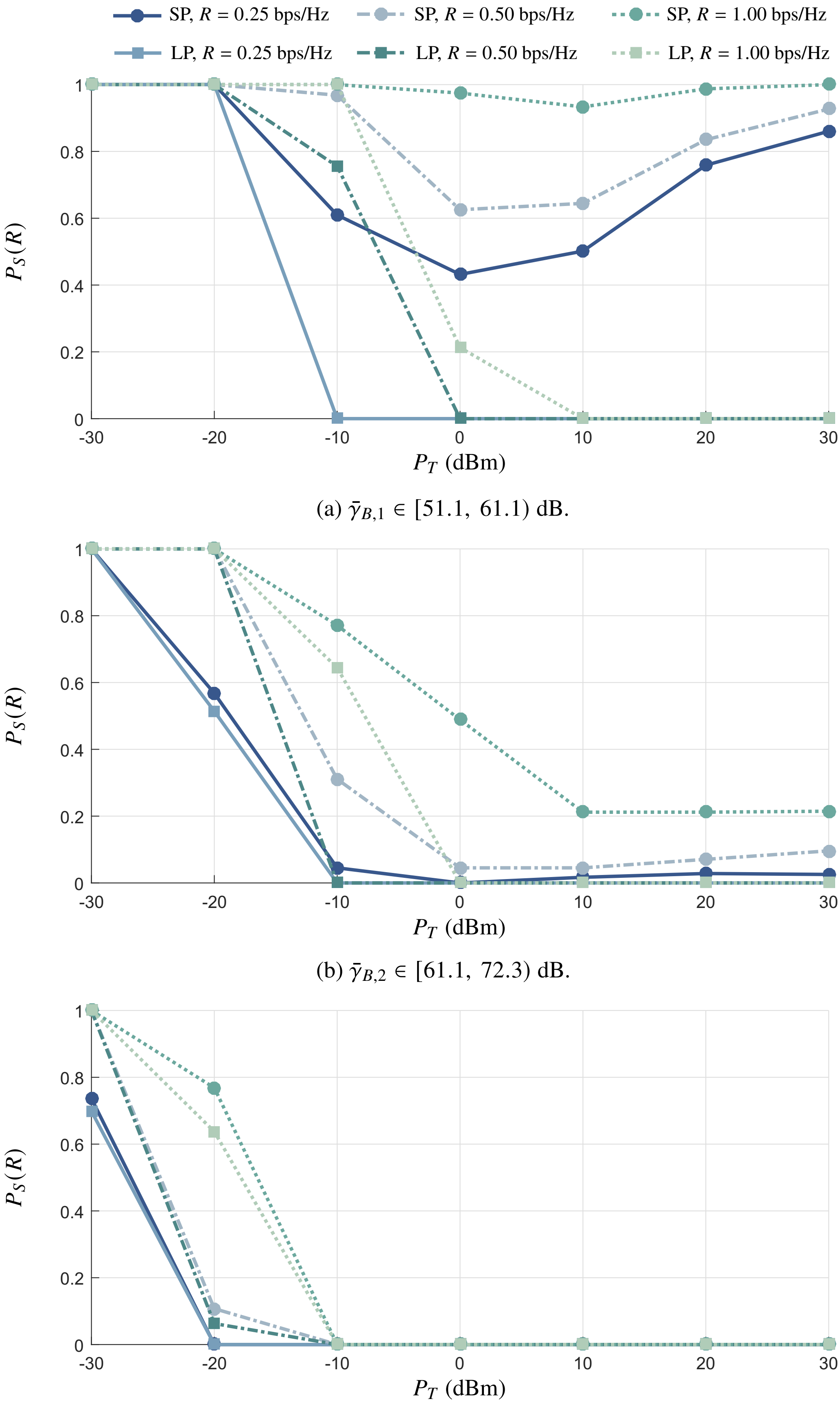
(a) $\bar{\gamma}_{B,1} \in [51.1,\ 61.1)$ dB.

(b) $\bar{\gamma}_{B,2} \in [61.1,\ 72.3)$ dB.

(c) $\bar{\gamma}_{B,3} \in [72.3,\ 82.9]$ dB.

Source: Personal collection.

Figure 14 – Hybrid wiretap channel model: $P_S(R) \times P_T$ for $R \in \{0.25, 0.50, 1.00\}$ bps/Hz under the adoption of OA technique



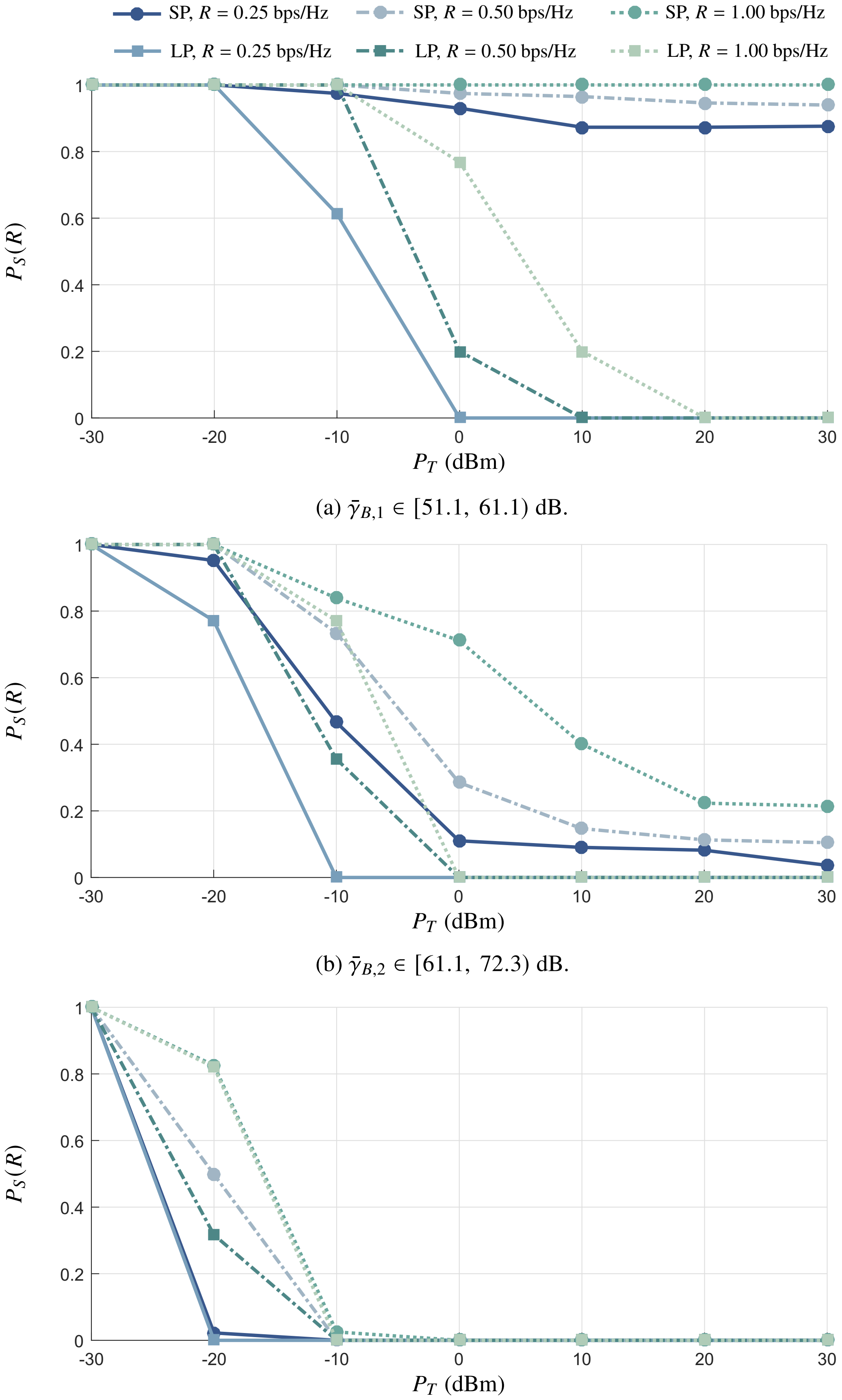
(a) $\bar{\gamma}_{B,1} \in [51.1,\ 61.1)$ dB.

(b) $\bar{\gamma}_{B,2} \in [61.1,\ 72.3)$ dB.

(c) $\bar{\gamma}_{B,3} \in [72.3,\ 82.9]$ dB.

Source: Personal collection.

Figure 15 – Hybrid wiretap channel model: $P_S(R) \times P_T$ for $R \in \{0.25, 0.50, 1.00\}$ bps/Hz under the adoption of UA technique



(a) $\bar{\gamma}_{B,1} \in [51.1,\ 61.1)$ dB.

(b) $\bar{\gamma}_{B,2} \in [61.1,\ 72.3)$ dB.

(c) $\bar{\gamma}_{B,3} \in [72.3,\ 82.9]$ dB.

Source: Personal collection.

3.3.3 Analysis of Effective Secrecy Throughput

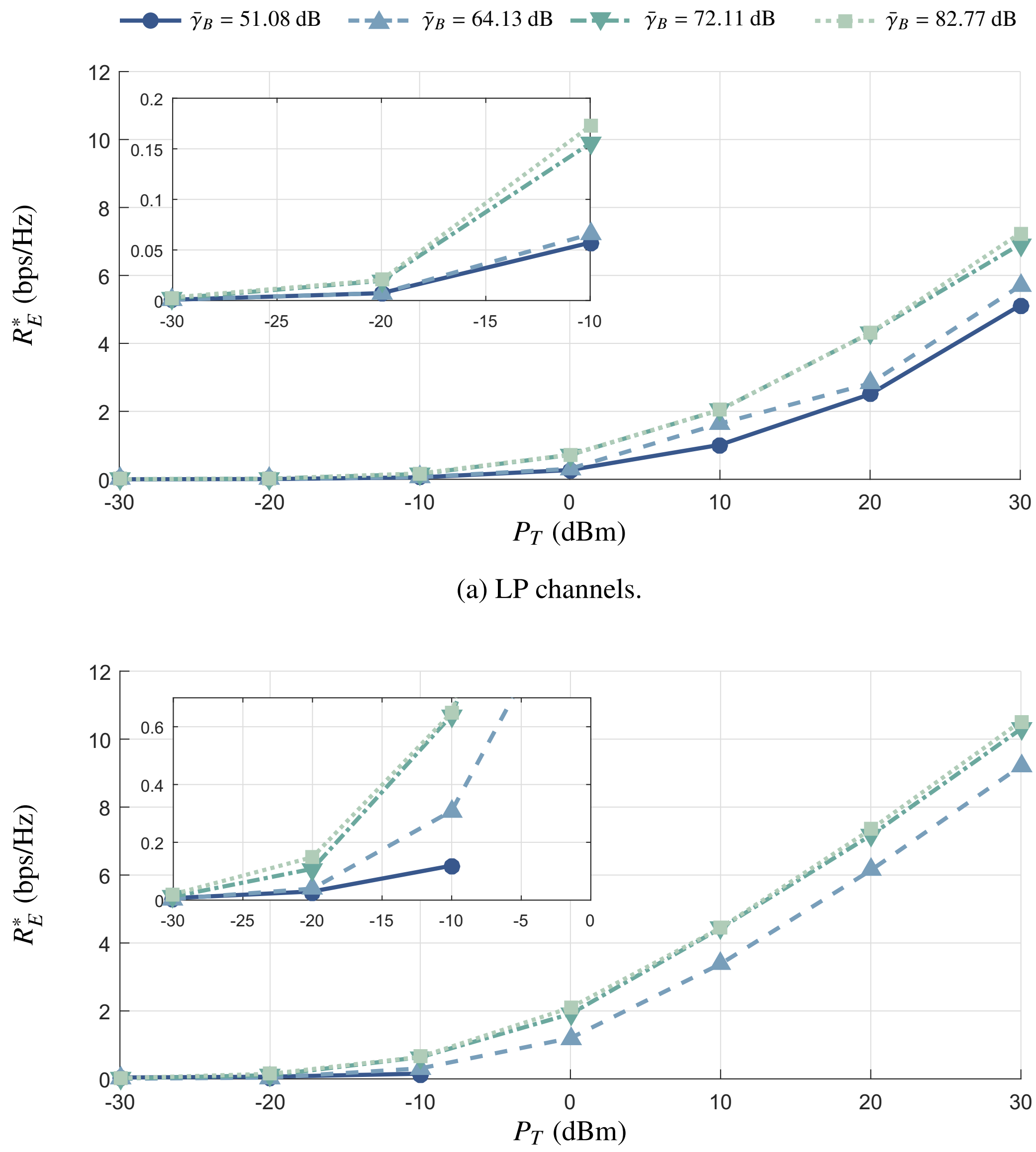
Figures 16(a) and (b) show $R_E^* \times P_T$ for the hybrid wiretap channel model considering the LP and SP channels, respectively. Also, $\bar{\gamma}_B = 51.08$, 64.13, 72.11, and 82.77 dB are taken into account. Notice that values of R_E^* higher than the ones found in LP channels are necessary for achieving Ψ_1^* in the SP channels. It is noteworthy that Figure 16(b) does not plot R_E^* when $\bar{\gamma}_B = 51.08$ and $P_T \geq 0$ since $\Psi_1^* = 0$ (see Figure 17(b)). In addition, one sees that R_E^* increases as $\bar{\gamma}_B$ rises and similar values of R_E^* are found when $\bar{\gamma}_B = 72.11$ and 82.77 dB for both LP and SP channels regardless of P_T. For instance, considering practical values of P_T, observe that if $P_T = 0$ dBm and $\bar{\gamma}_B = 64.13$, 72.11, and 82.77 dB are considered, then R_E^* equal to 0.31, 0.72, and 0.72 bps/Hz are found, respectively, for LP channels whereas R_E^* equal to 1.20, 1.91, and 2.10 bps/Hz are observed, respectively, for SP channels. Taking into account $P_T = 30$ dBm, R_E^* equal to, 6.70, 5.92, and 7.24 bps/Hz are noted for LP channels whereas R_E^* equal to 9.21, 10.30, and 10.52 bps/Hz are found for SP channels.

Figures 17(a) and (b) show $\Psi_1^* \times P_T$ for the hybrid wiretap channel model considering the LP and SP channels, respectively. In addition, $\bar{\gamma}_B = 51.08$, 64.13, 72.11, and 82.77 dB are considered. Observing Figure 17, one can see that Ψ_1^* is higher for LP channels than SP ones. Also, Ψ_1^* increases as P_T rises except when $\bar{\gamma}_B = 51.08$ and $P_T \geq 0$ for SP channels. Considering practical values of P_T, notice that when $P_T = 0$ dBm and $\bar{\gamma}_B = 51.08$, 64.13, 72.11, and 82.77 dB, Ψ_1^* is equal to 0.22, 1.11, 2.82, and 5.95 bps/Hz, respectively, for LP channels whereas Ψ_1^* is equal to 0, 0.22, 1.47, and 4.57 bps/Hz, respectively, for SP channels. Now, for $P_T = 30$ dBm, Ψ_1^* equal to 0.63, 3.47, 5.74, and 9.17 bps/Hz are found for LP channels and Ψ_1^* equal to 0, 0.56, 2.48, and 5.89 bps/Hz are observed for SP channels.

Figures 18(a), (b), and (c) show $(R_B^\star, R_E^\star) \times P_T$ for the hybrid wiretap channel model considering $\bar{\gamma}_{B,1}$, $\bar{\gamma}_{B,2}$, and $\bar{\gamma}_{B,3}$, respectively. Notice that as Bob moves away from Alice, $R_B^\star$ and $R_E^\star$ decrease. Also, observe that the difference between them, (i.e., the target secrecy rate) increases as P_T rises and Bob comes close to Alice. In this regard, one sees that, when $P_T = 30$ dBm and $\bar{\gamma}_{B,1}$ are adopted, Figure 18(a) shows $R_B^\star = 8.63$ bps/Hz and $R_E^\star = 8.39$ bps/Hz for SP channels and $R_B^\star = 8.31$ bps/Hz and $R_E^\star = 5.48$ bps/Hz for LP channels. Now, considering $\bar{\gamma}_{B,2}$, Figure 18(b) shows $R_B^\star = 10.95$ bps/Hz and $R_E^\star = 9.28$ bps/Hz for SP channels and $R_B^\star = 9.72$ bps/Hz and $R_E^\star = 5.70$ bps/Hz for LP channels. Lastly, taken into account $\bar{\gamma}_{B,3}$, Figure 18(c) shows $R_B^\star = 14.13$ bps/Hz and $R_E^\star = 10.51$ bps/Hz for SP channels and $R_B^\star = 12.99$ bps/Hz and $R_E^\star = 6.92$ bps/Hz for LP channels.

Figures 19(a), (b), and (c) show $\bar{\Psi}_1^* = \mathbb{E}\left[\Psi_1^*\right]$ and Ψ_2^* versus P_T for the hybrid wiretap channel model considering $\bar{\gamma}_{B,1}$, $\bar{\gamma}_{B,2}$, and $\bar{\gamma}_{B,3}$, respectively. Following Figure 19, one can see that both $\bar{\Psi}_1^*$ and Ψ_2^* as well as the difference between them rise as P_T increases and Bob moves closer to Alice. Furthermore, $\bar{\Psi}_1^*$ is higher than Ψ_2^* regardless of P_T and $\bar{\gamma}_B$. For instance, when $P_T = 30$ dBm is considered, Figure 19(a) shows $\bar{\Psi}_1^* = 0.03$ bps/Hz and $\Psi_2^* = 0.01$ bps/Hz for SP channels and $\bar{\Psi}_1^* = 1.77$ ad $\Psi_2^* = 1.19$ for LP channels. In addition, Figure 19(b) shows $\bar{\Psi}_1^* = 0.87$ bps/Hz and $\Psi_2^* = 0.8$ bps/Hz for SP channels and $\bar{\Psi}_1^* = 3.86$ bps/Hz and

Figure 16 – Hybrid wiretap channel model: Redundancy rate for the situation #1, R_E^*, versus P_T



(a) LP channels.

(b) SP channels.

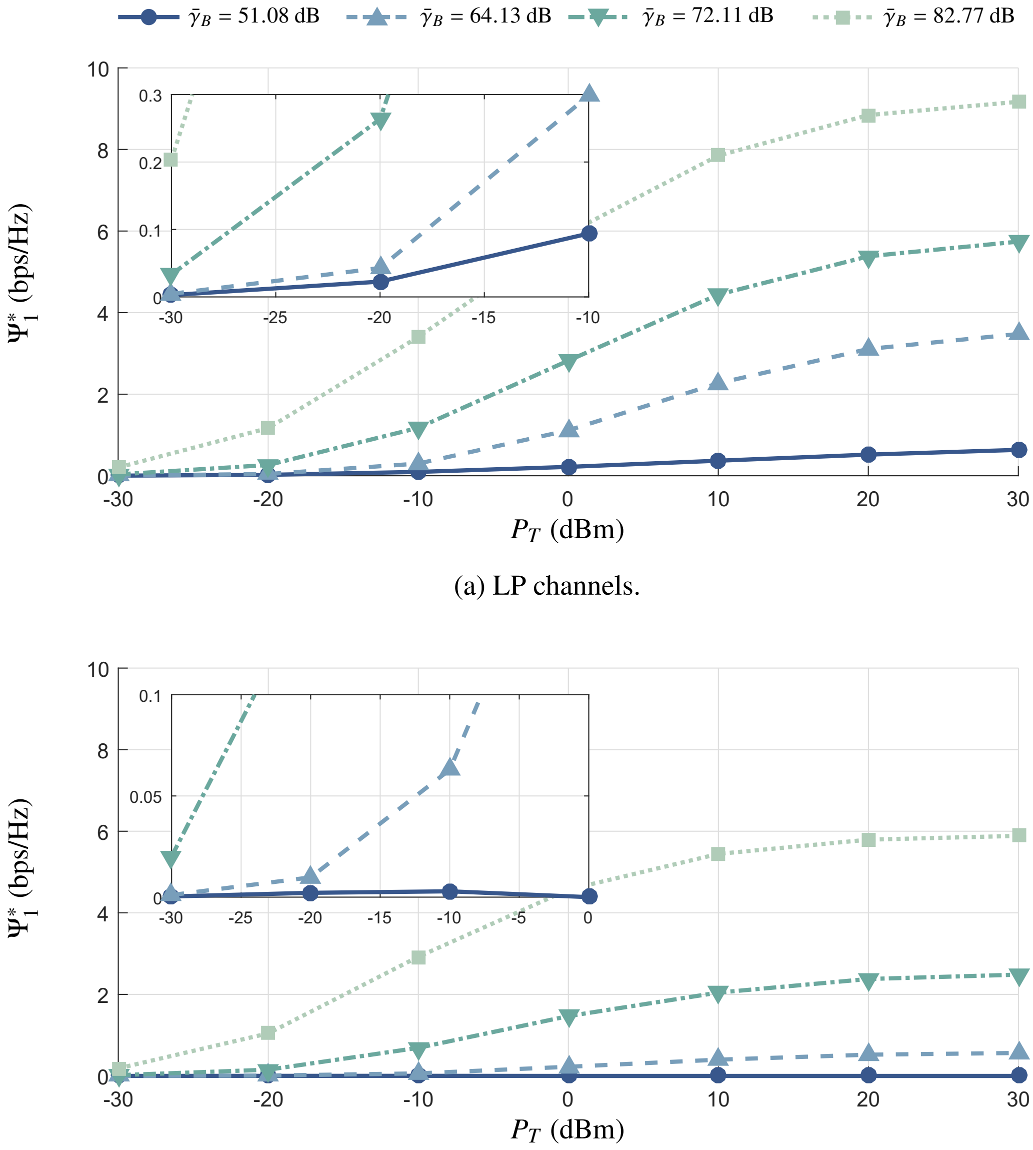
Source: Personal collection.

Ψ_2^* = 3.00 bps/Hz for LP channels. Finally, Figure 19(c) shows SP $\bar{\Psi}_1^*$ = 4.25 bps/Hz and Ψ_2^* = 2.58 bps/Hz for SP channels and $\bar{\Psi}_1^*$ = 7.52 bps/Hz and Ψ_2^* = 5.77 bps/Hz for LP channels.

3.3.4 General Comments

First of all, note that the values of $\bar{R}_S$, R_E^*, and Ψ_1^* related to SP scenario in Figures 11(a), 16(b), and 17(b), respectively, increase until a given value of P_T and after that, as $P_T \to \infty$, they decrease. The same happens with the values of $P_S(R)$ in Figure 12(a) and (b), but in opposite. The reason is that when P_T is low, if a given Bob's CFR presents few sub-channels much better than the respective sub-channels of Eve's CFR in terms of nSNR, which is defined

Figure 17 – Hybrid wiretap channel model: Effective secrecy throughput for the situation #1, Ψ_1^*, versus P_T



(a) LP channels.

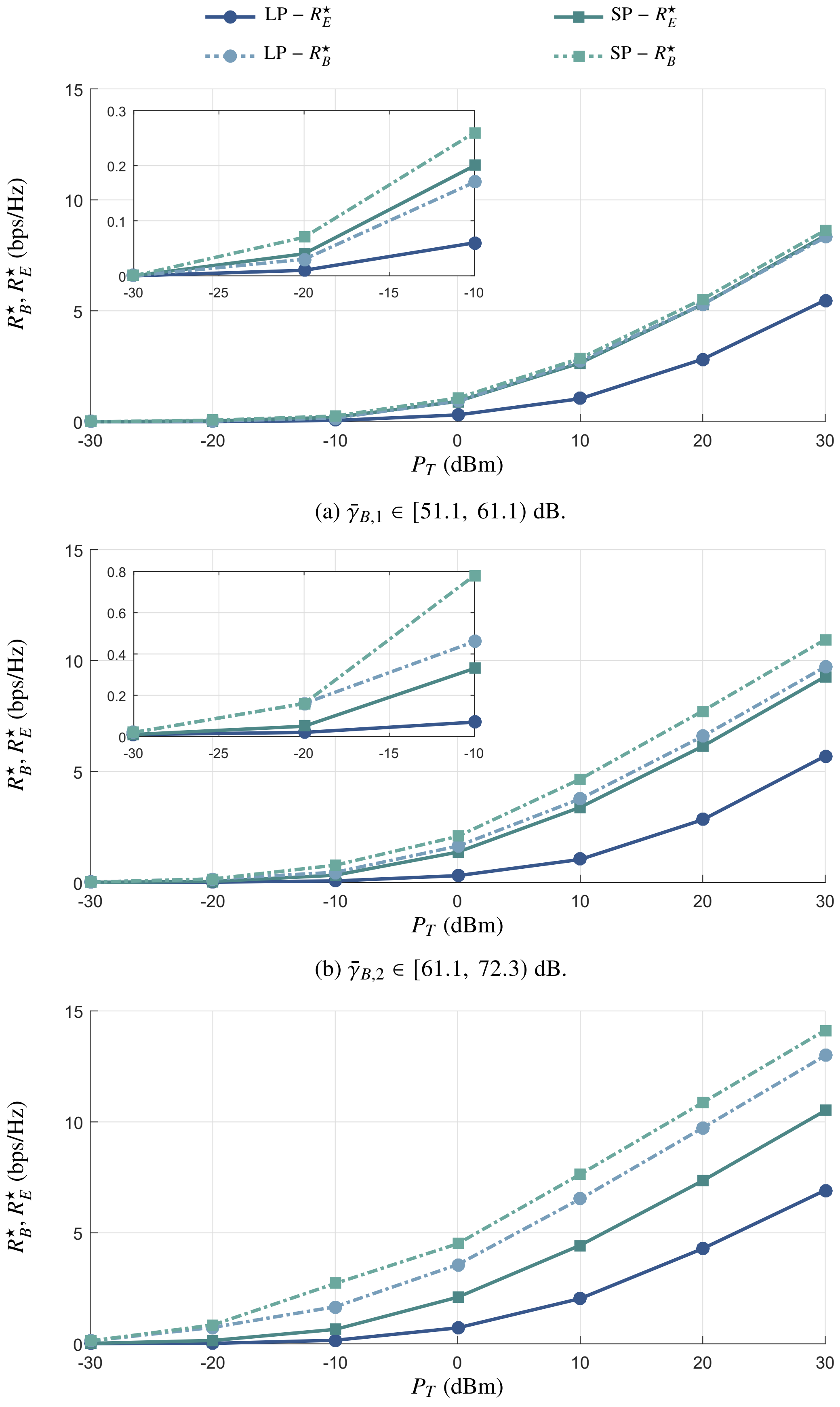
(b) SP channels.

Source: Personal collection.

as the ratio between $|H_l[k]|^2$ and $P_{V_l}[k]$, then $C_B > C_E$ may hold, despite that Eve's CFR has a greater number of sub-channels better than the ones of Bob's CFR. However, as $P_T \to \infty$, the fact that Eve's CFR has a greater number of sub-channels plays a more relevant role and, as a consequence, $C_B < C_E$ holds.

Overall, the numerical results regarding $P_S(R)$ have shown that Eve may be able to eavesdrop confidential information exchanged between Alice and Bob in the SP scenario when $\bar{\gamma}_{B,1}$ is observed, which corresponds to the situation where Eve is less than 2 meters away from Alice and Bob is around 6 meters away from Alice. In fact, high values of $P_S(R)$ have been found regardless of R and P_T, mainly with the use of UA. In contrast, despite that $\Psi_1^* = 0$ has been observed for $\bar{\gamma}_B = 51.08$ dB and $P_T \geq 0$ in the SP channel, $\Psi_1^* > 0$ and $\Psi_2^* > 0$ have been found in the SP channels for the others values of $\bar{\gamma}_B$ and P_T as well as in the LP channels. Consequently, the respective wiretap code rates that can ensure PLS for those simulated scenarios have been provided. Although $P_S(R)$ values have shown that the radiation from PLC signals compromise PLS if Eve is a WLC device operating in the same frequency band and located less than 2 meters from Alice, the analysis of effective secrecy throughput has shown that the wiretap code rates are able to ensure PLS in almost all practical scenarios considered.

Figure 18 – Hybrid wiretap channel model: Wiretap code rates for the situation #2, $R_B^\star$ and $R_E^\star$, versus P_T considering $\bar{\gamma}_{B,1}$, $\bar{\gamma}_{B,2}$, and $\bar{\gamma}_{B,3}$



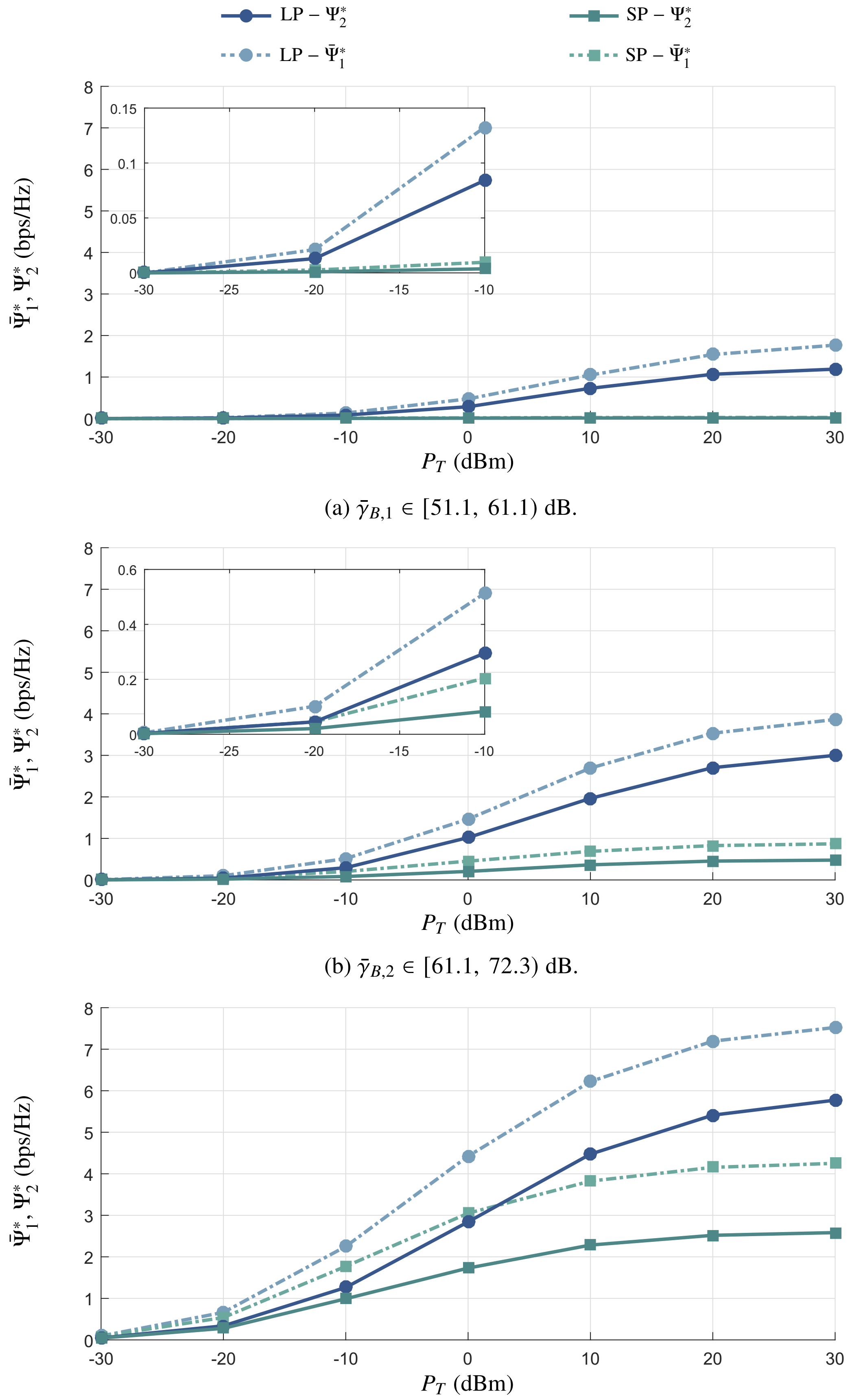
(a) $\bar{\gamma}_{B,1} \in [51.1,\ 61.1)$ dB.

(b) $\bar{\gamma}_{B,2} \in [61.1,\ 72.3)$ dB.

(c) $\bar{\gamma}_{B,3} \in [72.3,\ 82.9]$ dB.

Source: Personal collection.

Figure 19 – Hybrid wiretap channel model: $\bar{\Psi}_1^*$ and Ψ_2^* versus P_T considering $\bar{\gamma}_{B,1}$, $\bar{\gamma}_{B,2}$, and $\bar{\gamma}_{B,3}$



(a) $\bar{\gamma}_{B,1} \in [51.1,\ 61.1)$ dB.

(b) $\bar{\gamma}_{B,2} \in [61.1,\ 72.3)$ dB.

(c) $\bar{\gamma}_{B,3} \in [72.3,\ 82.9]$ dB.

Source: Personal collection.

4 PLC WIRETAP CHANNEL MODEL

The broadcast nature of PLC systems may jeopardize data communication security since any PLC device connected to the same electric power grid in which a PLC system operates can access messages exchanged among PLC devices, which belong to this PLC system. One way to circumvent that problem is the use of the PLS approach. In this way, Fig. 20 shows the PLC wiretap channel model, where a PLC transmitter (Alice) sends private information to an intended PLC receiver (Bob) whereas a malicious PLC device (Eve) eavesdrops such information.

The PLC wiretap channel model has been addressed in some studies in the literature for narrowband [46,49,50] and broadband [47,48] applications. Note that [46–48] considered that Alice has complete knowledge of the CSIs of Bob and Eve whereas, in [49,50], the authors made a more realistic assumption, they assume that Eve is a passive device. Furthermore, considering the broadband applications, [47] and [48] provided some secrecy capacity results for MIMO and single-input single-output (SISO) broadband PLC systems, respectively, in the frequency band $2 - 28$ MHz. It is important mentioning that only [48] considered the use of a real data to analyze the PLS in PLC systems. In this regard, one can see the necessity of providing a further investigation about the presence of a malicious PLC device. From the author's perspective, this kind of investigation can offer, together with the one presented in Chapter 3, a better picture of the threat of non-authorized access by a malicious device (e.g., PLC or WLC) in a PLC system.

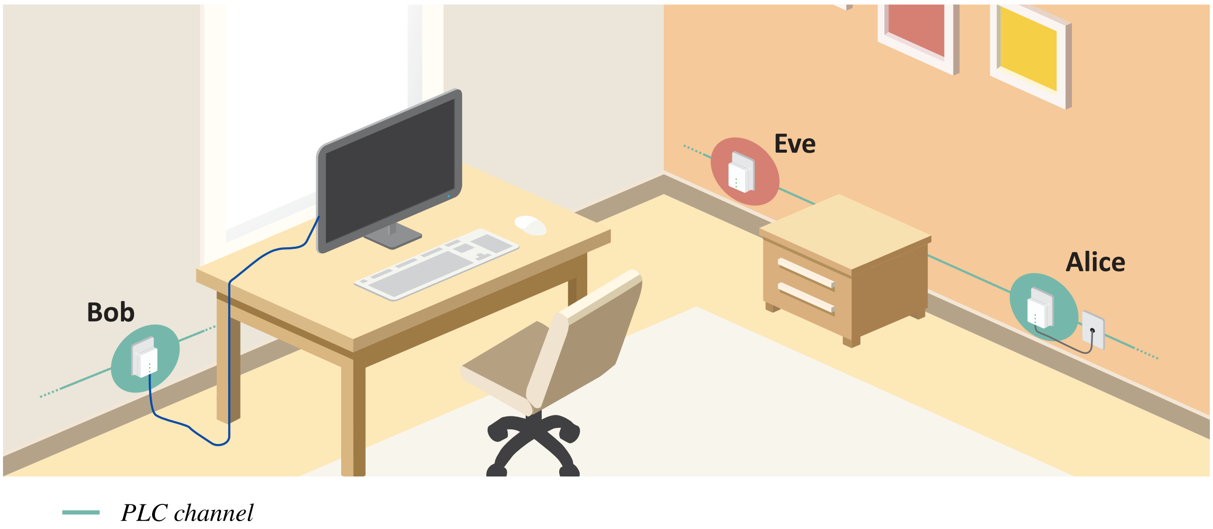
This chapter investigates the PLS of the PLC wiretap channel model represented by PLC channel estimates and measured additive noises obtained from the measurement campaign carried out in several Brazilian houses (see Appendix B) [3]. Different from [48], four distinct sets of PLC transmitter, legitimate PLC receiver, and PLC eavesdropper positions are assessed. Such sets of positions define typical and realistic situations faced by in-home broadband PLC systems. Also, this chapter analyzes three distinct frequency bands: (i) $1.7 - 30$ MHz, to comply with CENELEC; $1.7 - 50$ MHz, to address Brazilian telecommunication regulation authority (*Agência Nacional de Telecomunicações* in Portuguese) (ANATEL); and $1.7 - 86$ MHz, in agreement with ITU-T G.hn [81] and HomePlug AV2 [76]. In this regard, the main contributions are stated as follows:

- Analysis of the ergodic achievable secrecy rate, secrecy outage probability, effective secrecy throughput, and wiretap code rates of an in-home broadband PLC system when a passive and malicious PLC device eavesdrops private information sent by the transmitter to the legitimate receiver. To do so, a real data set constituted of PLC channel estimates and measured additive noises is taken into account [3].

- Performance comparisons considering the following situations: four distinct sets of positions for transmitter, legitimate receiver, and eavesdropper; three well-established frequency bands for broadband PLC systems; different levels of the total transmission power (practical and theoretical); and two types of resource allocation techniques (optimal and uniform).

The rest of this chapter is organized as follows: Section 4.1 presents the problem formulation; Section 4.2 describes mathematical expressions for the secrecy outage probability and effective secrecy throughput; and, finally, Section 4.3 shows the numerical results.

Figure 20 – Illustration of broadband data communication between two PLC devices (Alice and Bob) under the presence of a PLC eavesdropper (Eve)



Source: Personal collection.

4.1 PROBLEM FORMULATION

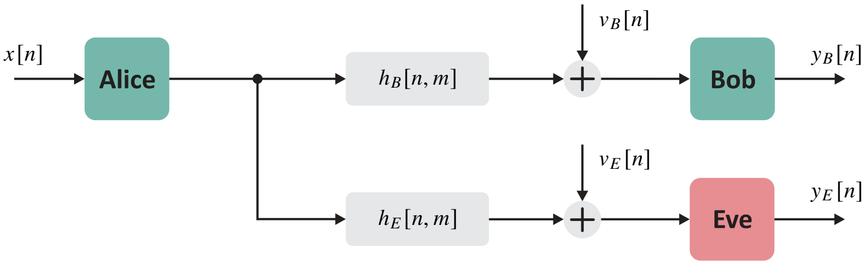
Let the block diagram shown in Fig. 21 represent the PLC wiretap channel model. A transmitter Alice (A) sends private messages to the legitimate receiver Bob (B), while a malicious device Eve (E) eavesdrops the private messages. $\{h_l[n,m]\}$, where $l \in \{B,\ E\}$, denotes the discrete-time version of the time-varying channels associated with Alice-Bob and Alice-Eve links, respectively. Then the discrete-time representation of the received signal at the input of the l^{th} receiver is given by

$$y_l[n] = \sum_{m=-\infty}^{\infty} x[m]h_l[n,m] + v_l[n], \tag{4.1}$$

where $\{x[n]\}$ is the transmitted sequence constituted of an infinite number of N-length symbols (N-block symbols); $h_l[n,m]$ is the CIR seen by the l^{th} receiver in the n^{th} sample when an impulse is injected in the m^{th} sample by Alice; and $\{v_l[n]\}$ denotes the additive noise sequence. Also, $\{x[n]\}$ and $\{v_l[n]\}$ are independent and wide-sense stationary random processes.

In practical terms, the dynamic of loads connected to the electric power system imposes to the PLC channels a time-varying behavior. However, it is possible to assume that PLC channels are linear and time-invariant during a time interval corresponding to an N-block symbol. In this regard, the discrete-time CIR is represented by $\{\mathrm{h}_l[n]\}_{n=0}^{L_l-1}$, where L_l is the length of CIR associated with the link between Alice and the l^{th} receiver. The vector representation of the discrete-time

Figure 21 – Block diagram of the PLC wiretap channel model



Source: Personal collection.

version of such channels during one N-block symbol is $\mathbf{h}_l = [\mathrm{h}_l[0],\ \mathrm{h}_l[1],\ \ldots,\ \mathrm{h}_l[L_l-1]]^T$ whereas $\mathbf{H}_l = [H_l[0],\ H_l[1],\ \ldots,\ H_l[N-1]]^T$ denotes its vector representation in the frequency domain and $\{\cdot\}^T$ is the transpose operator. Also, $\mathbf{H}_l = \boldsymbol{\mathcal{F}}[\mathbf{h}_l^T,\ \mathbf{0}_{N-L_l}^T]^T$, $\boldsymbol{\mathcal{F}} = \frac{1}{\sqrt{N}}\mathbf{W}$, $\mathbf{W} \in \mathbb{C}^{N\times N}$ denotes the $N \times N$ DFT matrix, and N is the number of sub-channels (see Appendix C). From now on, the diagonal matrices $\boldsymbol{\Lambda}_{\mathcal{H}_l} = \mathbf{diag}\{H_l[0],\ H_l[1],\ \ldots,\ H_l[N-1]\}$ and $\boldsymbol{\Lambda}_{|\mathcal{H}_l|^2} = \mathbf{diag}\{|H_l[0]|^2,\ |H_l[1]|^2,\ \cdots,|H_l[N-1]|^2\}$, in which $|\cdot|$ is the modulus operator, will be used.

Moreover, the vector representation of the N-block symbol, in the frequency domain, is $\mathbf{X} \in \mathbb{C}^{N\times 1}$ so that $\mathbb{E}[\mathbf{X}] = \mathbf{0}_{N\times 1}$, where $\mathbb{E}[\cdot]$ denotes the expectation operator and $\mathbf{0}_{N\times 1}$ is an N-length column vector of zeros, and $\mathbf{R}_{\mathbf{XX}} = \mathbb{E}[\mathbf{XX}^\dagger] = N\boldsymbol{\Lambda}_P$, in which $\{\cdot\}^\dagger$ is the Hermitian operator, $\boldsymbol{\Lambda}_P = \mathbf{diag}\{P[0],\ P[1],\ \ldots,\ P[N-1]\}$ is the matrix representation of the power allocated in the frequency domain, $\mathbf{tr}(\boldsymbol{\Lambda}_P) = P_T$ is the total transmission power, and $\mathbf{tr}(\cdot)$ denotes the trace operator. Furthermore, $\mathbf{V}_l \in \mathbb{C}^{N\times 1}$ is the vector representation, in the frequency domain, of the zero mean additive noise, such that $\mathbf{R}_{\mathbf{VV},l} = \mathbb{E}[\mathbf{V}_l\mathbf{V}_l^\dagger] = N\boldsymbol{\Lambda}_{P_{\mathrm{V}_l}}$, where $\boldsymbol{\Lambda}_{P_{\mathrm{V}_l}} = \mathbf{diag}\left\{P_{\mathrm{V}_l}[0],\ P_{\mathrm{V}_l}[1],\ \ldots, P_{\mathrm{V}_l}[N-1]\right\}$ and $P_{\mathrm{V}_l}[k]$ is the additive noise power in the k^{th} sub-channel.

Based on the aforementioned formulation, the following two questions arise: *How secure is a broadband PLC system at the physical layer level, from a practical perspective, when Eve is a PLC device? In other words, how much information is leaked to Eve and how does it impact the secrecy outage probability and effective secrecy throughput? Moreover, what is the behavior of the wiretap code rates?* Aiming to answer these questions, Section 4.2 deduces the secrecy outage probability and effective secrecy throughput for the PLC wiretap channel model while Section 4.3 shows numerical results that provide important insights regarding the PLS of PLC systems.

Finally, it is worth emphasizing that the problem formulation stated in this section and the mathematical deductions for secrecy outage probability and effective secrecy throughput addressed in next section present many similarities to the ones discussed in Sections 3.1 and 3.2, respectively. These similarities are preserved to facilitate the understanding and to highlight that the same mathematical tools are adopted in both Chapters 3 and 4.

4.2 PHYSICAL LAYER SECURITY METRICS AND WIRETAP CODE RATES

In this section, mathematical expressions to calculate the secrecy outage probability and effective secrecy throughput are deduced for the PLC wiretap channel. In this regard, following [92], we assume that the PLC channels are N-block linear Gaussian channels with finite memory (i.e., $L_{\max} = \max_{l} L_l$). Unfortunately, the inter-block interference caused by the memory of CIRs and the correlated noises make the assessment of the achievable data rate a difficult task to be accomplished [93]. A feasible and effective way to circumvent this problem was introduced in [93]. Essentially, it states that the N-block CGRC completely remove the inter-block interference if $N \gg L_{\max}$. Therefore, as the LGRC tends to N-CGRC as $N \rightarrow \infty$, N-CGRC channels model PLC ones since $N \rightarrow \infty$.

The vector representation, in the discrete-frequency domain, of the received N-block symbol at the l^{th} receiver can be expressed as

$$\mathbf{Y}_l = \mathbf{\Lambda}_{\mathcal{H}_l}\mathbf{X} + \mathbf{V}_l. \tag{4.2}$$

Then the mutual information between Alice and the l^{th} receiver is given by [94, pp. 92]

$$\begin{aligned} I(\mathbf{X};\mathbf{Y}_l) &= \hbar(\mathbf{Y}_l) - \hbar(\mathbf{Y}_l|\mathbf{X}) \\ &= \hbar(\mathbf{Y}_l) - \left[\hbar(\mathbf{\Lambda}_{\mathcal{H}_l}\mathbf{X}|\mathbf{X}) + \hbar(\mathbf{V}_l|\mathbf{X})\right] \\ &= \hbar(\mathbf{Y}_l) - \hbar(\mathbf{V}_l), \end{aligned} \tag{4.3}$$

in which $\hbar(\cdot)$ is the differential entropy function. If the transmitted symbols and the additive noise are Gaussian random process and colored Gaussian random process, respectively, then the entropy of $\mathbf{Y}_l$ and $\mathbf{V}_l$ can be expressed as

$$\hbar(\mathbf{Y}_l) = \frac{1}{2}\log_2\left[(2\pi e)^N \det(\mathbf{R}_{\mathbf{YY},l})\right] \tag{4.4}$$

and

$$\hbar(\mathbf{V}_l) = \frac{1}{2}\log_2\left[(2\pi e)^N \det(\mathbf{R}_{\mathbf{VV},l})\right], \tag{4.5}$$

respectively, where $\det(\mathbf{\Lambda}_D)$ is the determinant of the matrix $\mathbf{\Lambda}_D$ and $\mathbf{R}_{\mathbf{YY},l} = \mathbf{\Lambda}_{\mathcal{H}_l}\mathbf{R}_{\mathbf{XX}}\mathbf{\Lambda}_{\mathcal{H}_l}^{\dagger} + \mathbf{R}_{\mathbf{VV},l}$ (see Appendix D). Hence, the capacity between Alice and the l^{th} receiver is given by

$$\begin{aligned} C_l &= \max_{f_{\mathbf{X}}(\mathbf{x}):\mathbf{tr}(\mathbf{R}_{\mathbf{XX}})\le NP_T} I(\mathbf{X};\mathbf{Y}_l) \\ &= \max_{\mathbf{\Lambda}_P} \log_2\left[\det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_l}\right)\right], \end{aligned} \tag{4.6}$$

where $f_{\mathbf{X}}(\mathbf{x})$ is the joint probability density function of $\mathbf{X}$ and

$$\begin{aligned} \mathbf{\Lambda}_{\gamma_l} &= \frac{\mathbf{\Lambda}_{\mathcal{H}_l}\mathbf{R}_{\mathbf{XX}}\mathbf{\Lambda}_{\mathcal{H}_l}^{\dagger}}{\mathbf{R}_{\mathbf{VV},l}} \\ &= \mathbf{\Lambda}_P\mathbf{\Lambda}_{|\mathcal{H}_l|^2}\mathbf{\Lambda}_{P_{V_l}}^{-1}. \end{aligned} \tag{4.7}$$

Therefore, the secrecy capacity is given by [95]

$$C_S = \max_{f_{\mathbf{X}}(\mathbf{x}):\mathbf{tr}(\mathbf{R}_{\mathbf{XX}})\leq NP_T} \left[I(\mathbf{X};\mathbf{Y}_B) - I(\mathbf{X};\mathbf{Y}_E)\right]^+ . \tag{4.8}$$

However, calculating (4.8) is a hard task to be accomplished. In order to circumvent this problem, [95] addressed the following lower bound:

$$\begin{aligned} C_S &\geq \left[\max_{f_{\mathbf{X}}(\mathbf{x}):\mathbf{tr}(\mathbf{R}_{\mathbf{XX}})\leq NP_T} I(\mathbf{X};\mathbf{Y}_B) - \max_{f_{\mathbf{X}}(\mathbf{x}):\mathbf{tr}(\mathbf{R}_{\mathbf{XX}})\leq NP_T} I(\mathbf{X};\mathbf{Y}_E)\right]^+ \\ &= \left[C_B - C_E\right]^+ , \end{aligned} \tag{4.9}$$

in which C_B and C_E represent the capacities of Alice-Bob and Alice-Eve links, respectively.

4.2.1 Secrecy Outage Probability

As aforementioned in Chapter 3, for achieving C_S, i.e., the maximum target secrecy rate $R \in \mathbb{R}_+$, complete knowledge of CSIs of Bob and Eve have to be available at Alice. However, it is challenging for Alice to obtain CSI of Eve since, in practice, Eve is passive and then $R_E > C_E$ may not always be fulfilled (i.e., secrecy is not guaranteed), in which $R_E \in \mathbb{R}_+$ is the redundancy rate. In this case, Alice may choose a fixed R and the secrecy outage probability becomes a reasonable parameter to quantify PLS [98]. In this regard, the achievable secrecy rate can be expressed as

$$R_S = \frac{1}{N}\left[\log_2\left[\det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_B}\right)\right] - \log_2\left[\det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_E}\right)\right]\right]^+ \text{ [bps/Hz]} \tag{4.10}$$

and then the expression for the secrecy outage probability is

$$\begin{aligned} P_S(R) &= \mathbb{P}\left\{R_S < R\right\} \\ &= \mathbb{P}\left\{\det\left(\frac{\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_B}}{\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_E}}\right) < 2^{RN}\right\}, \end{aligned} \tag{4.11}$$

where $\mathbb{P}\{c > d\}|(c, d) \in \mathbb{R}^2$ is the probability that c is greater than d. Observe that perfect secrecy is achieved when $R_S > R$ whereas $R_S < R$ means that the perfect secrecy is not guaranteed.

4.2.2 Effective Secrecy Throughput

The problem with using $P_S(R)$ is that it is not possible to separate reliability and secrecy constraints. However, the effective secrecy throughput proposed in [96] can provide the wiretap code rates, R_B and R_E, in which $R_B \in \mathbb{R}_+$ denotes the rate of transmitted codewords. In this regard, the secrecy outage probability can be rewritten as

$$\begin{aligned} O_s(R_E) &= \mathbb{P}\left\{R_E < C_E\right\} \\ &= \mathbb{P}\left\{2^{R_E N} < \det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_E}\right)\right\}, \end{aligned} \tag{4.12}$$

and the reliability outage probability is given by

$$\begin{aligned} O_r(R_B) &= \mathbb{P}\{R_B > C_B\} \\ &= \mathbb{P}\left\{2^{R_B N} > \det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_B}\right)\right\}. \end{aligned} \tag{4.13}$$

Hence, the effective secrecy throughput can be expressed as

$$\Psi(R_E, R_B) = (R_B - R_E)[1 - O_r(R_B)][1 - O_s(R_E)], \tag{4.14}$$

where $(R_B - R_E)$ is the target secrecy rate R, i.e. $R = R_B - R_E$, and $[1 - O_r(R_B)][1 - O_s(R_E))]$ expresses the probability in which the private information sent by Alice to Bob is securely transmitted. In summary, $\Psi(R_E, R_B)$ measures the average secrecy rate at which the information transmitted from Alice to Bob is not leaked to Eve. In accordance with [96], the constraints $R_B > 0$ and $0 < R_E < R_B$ must be satisfied to guarantee $\Psi(R_E, R_B) \geq 0$.

The effective secrecy throughput metric is relevant in the following situations:

- *Situation #1*: Alice knows C_B (i.e., she has Bob's CSI) and does not know C_E. In this scenario, $R_B = C_B$ and then $O_r(R_B) = 0$ and the effective secrecy throughput is computed as

$$\Psi_1(R_E) = (C_B - R_E)[1 - O_s(R_E)]. \tag{4.15}$$

  In this way, the redundancy rate that maximizes (4.15) can be obtained through

$$R_E^* = \underset{0<R_E<C_B}{\arg\max}\, \Psi_1(R_E). \tag{4.16}$$

  Consequently, the maximum effective throughput is $\Psi_1^* = \Psi_1(R_E^*)$.

- *Situation #2*: Alice does not know C_B and C_E. In this situation, the effective secrecy throughput can be expressed as

$$\Psi_2(R_E, R_B) = (R_B - R_E)[1 - O_r(R_B)][1 - O_s(R_E)]. \tag{4.17}$$

  The codeword and redundancy rates that maximize (4.17) are given by

$$(R_B^\star, R_E^\star) = \underset{0<R_B, 0<R_E<R_B}{\arg\max}\, \Psi_2(R_B, R_E) \tag{4.18}$$

  and then the maximum effective throughput is $\Psi_2^* = \Psi_2(R_B^\star, R_E^\star)$.

4.3 NUMERICAL RESULTS

This section covers the numerical analysis of the secrecy outage probability, effective secrecy throughput, and wiretap code rates for the investigated PLC wiretap channel model. In this regard, one assumes Alice has only the CSI of Bob, i.e., Eve is passive, and Bob and Eve have only access to their own CSI. Besides, the ergodic achievable secrecy rate $\bar{R}_S = B_w \mathbb{E}_{\mathcal{H}_B, \mathcal{H}_E}[R_S]$

is evaluated to quantify the amount of information that is leaked to Eve when data communication takes place between Alice and Bob, where B_w is the frequency bandwidth. The OA, based on the water-filling algorithm [97], and UA[1] techniques are taken into account for evaluating the ergodic achievable secrecy rate and outage probability. On the other hand, for the sake of simplicity, only UA is considered for assessing the effective secrecy throughput since the results related to ergodic achievable secrecy rate and secrecy outage probability will show that there is no significant difference between OA and UA. Also, P_T ranges from -30 dBm to 30 dBm, in which the intervals $[-30, 0)$ dBm and $[0, 30]$ dBm cover theoretical and practical values of the total transmission power, respectively. Furthermore, one adopts the following three distinct frequency bands: 1.7 – 30 MHz (to comply with CENELEC), labeled as F_{30}; 1.7 – 50 MHz (in compliance with ANATEL), labeled as F_{50}; and 1.7 – 86 MHz (in agreement with ITU-T G.hn [81] and HomePlug AV2 [76]), labeled as F_{86}. Also, the adopted numbers of sub-channels for F_{30}, F_{50}, and F_{86} are $N = 580$, 990, and 1727, respectively, because the resulting frequency bandwidth of the sub-channels, $\Delta_f = B_w/N = 48.8$ kHz, related to those frequency bands does not exceed the coherence bandwidth of the in-home PLC channels [8, 52].

Alice-Bob and Alice-Eve links are represented by PLC channel estimates and measured additive noises obtained from the measurement campaign carried out in several Brazilian residences and discussed in [3]. More details about the measurement campaign addressed in [3] can be seen in Appendix B. Considering distinct sets of transmitters and receivers positions that can be found in a house, the following cases are analyzed (see Figure 22):

- *Case #1*: Eve is positioned in the middle between Alice and Bob.
- *Case #2*: Eve locates near Bob and far from Alice.
- *Case #3*: Eve locates near Alice and far from Bob.
- *Case #4*: Eve locates far from both Alice and Bob.

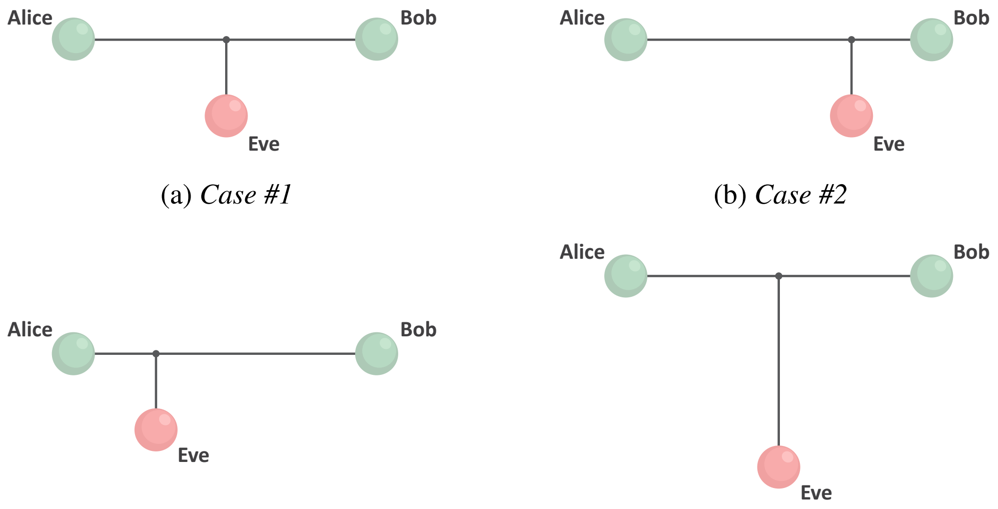
Figures 23(a)-(d) show the CDFs of $\bar{\gamma}_l$ for cases #1, #2, #3, and #4, respectively, in all adopted frequency bands. According to [97], the mathematical definition of the multi-channel nSNR is given by

$$\bar{\gamma}_l \triangleq \det\left(\mathbf{I}_N + \mathbf{\Lambda}_{|\mathcal{H}_l|^2}\mathbf{\Lambda}^{-1}_{P_{V_l}}\right)^{1/N} - 1. \tag{4.19}$$

As aforementioned, $\bar{\gamma}_l$ is related to the distance between Alice and the l^{th} receiver, i.e., the higher $\bar{\gamma}_l$ is, the closer the l^{th} receiver is to Alice. For instance, taking into account F_{86} and a probability less than or equal to 0.9, one observes $\bar{\gamma}_B = 60.4$ dB and $\bar{\gamma}_E = 69.1$ dB for case #1, $\bar{\gamma}_B = 67.0$ dB and $\bar{\gamma}_E = 82.6$ dB for case #3, $\bar{\gamma}_B = 67$ dB and $\bar{\gamma}_E = 67.5$ dB for case #2, and $\bar{\gamma}_B = 84.0$ dB and $\bar{\gamma}_E = 72.8$ dB for case #4. Now, when the probability is less than or equal to

[1] Since Eve is assumed passive, the UA technique is calculated by allocating the power P_T/N for each sub-carrier.

Figure 22 – Eve’s locations based on power line distances



(a) *Case #1*

(b) *Case #2*

(c) *Case #3*

(d) *Case #4*

Source: Personal collection.

0.2, one notes $\bar{\gamma}_B = 45.1$ dB and $\bar{\gamma}_E = 58.9$ dB for case #1, $\bar{\gamma}_B = 53.1$ dB and $\bar{\gamma}_E = 73.2$ dB for case #3, $\bar{\gamma}_B = 53.3$ dB and $\bar{\gamma}_E = 56.4$ dB for case #2, and $\bar{\gamma}_B = 73.4$ dB and $\bar{\gamma}_E = 54.2$ dB for case #4.

4.3.1 Analysis of Ergodic Achievable Secrecy Rate

Figures 24(a)-(d) show $\bar{R}_S \times P_T$ considering OA and UA techniques for cases #1, #2, #3, and #4, respectively. Also, F_{30}, F_{50}, and F_{86} are evaluated. Notice that the difference between OA and UA is not significant and it reduces as the frequency band decreases. Observing Figures 24(a) and (b), we note that cases #1 and #3 show the lowest $\bar{R}_S$ values, which are below 3 Mbps. For instance, adopting OA and $P_T = 30$ dBm, one finds $\bar{R}_S$ equal to zero in the chosen frequency bands for case #3 and in F_{30} and F_{50} for case #1 whereas $\bar{R}_S = 0.1$ Mbps is observed in F_{86} for case #1. Moreover, for OA and $P_T = 30$ dBm, case #2 (see Figure 24(c)) yields $\bar{R}_S = 17.6$, 33.1, and 46.6 Mbps when F_{30}, F_{50}, and F_{86} are taken into account, respectively, whereas case #4 (see Figure 24(d)) shows $\bar{R}_S = 158.6$, 280.7, and 452.9 Mbps, which are the highest values regarding the four cases. For practical values of P_T (i.e., $0 \leq P_T \leq 30$ dBm), $\bar{R}_S$ is equal to zero for case #3 in all frequency bands whereas, for case #1, $\bar{R}_S$ is equal to zero in F_{30} and F_{50} and equal to 0.1 Mbps in F_{86}. In order to facilitate understanding, Table 4 summarizes the values of $\bar{R}_S$ for all cases taken into account when $P_T = 30$ dB and OA are adopted.

4.3.2 Analysis of Secrecy Outage Probability

Figures 25(a)-(d) and 26(a)-(d) show $P_S(R) \times R$ taking into account the frequency bands F_{30}, F_{50}, and F_{86} and the practical values of the total transmission power $P_T = 0$ and 30 dBm. Figures 25(a)-(d) depict cases #1, #3, #2, and #4, respectively, with OA and Figures

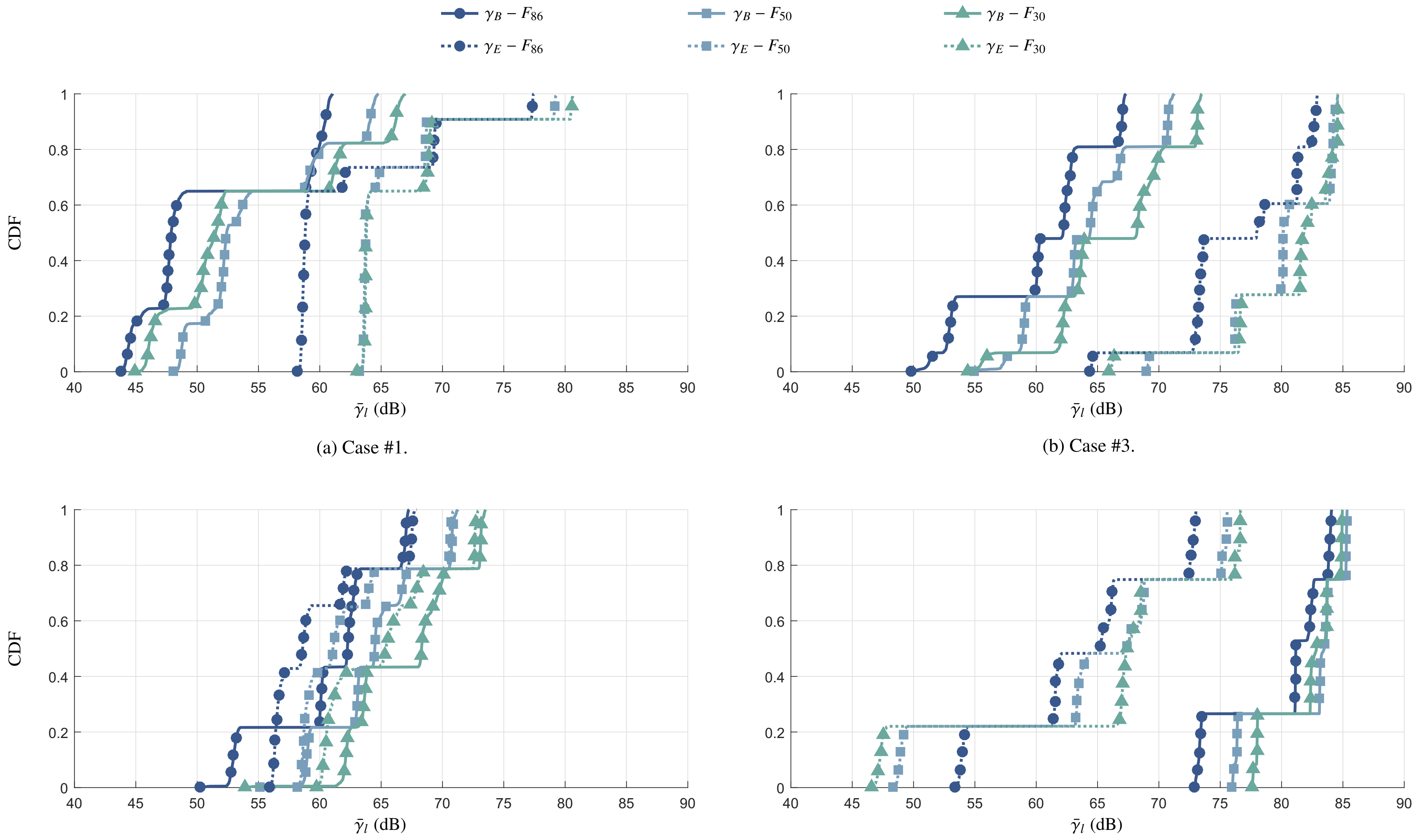
Table 4 – $\bar{R}_S$ for the PLC wiretap channel model considering $P_T = 30$ dB and OA technique

Ergodic achievable secrecy rate (Mbps)				
	Case #1	Case #3	Case #2	Case #4
F_{30}	0	0	17.6	158.6
F_{50}	0	0	33.1	280.7
F_{86}	0.1	0	46.6	452.9

Source: Personal collection.

26(a)-(d) illustrate cases #1, #3, #2, and #4, respectively, with UA. Observe that there is no significant difference between OA and UA techniques in terms of $P_S(R)$ for all analyzed cases and frequency bands. Case #1 (see Figures 25(a) and Figures 26(a)) presents $P_S(R) > 0.9$ for $R \geq 0.05$ bps/Hz whereas case #3 (see Figures 25(b) and 26(b)) shows $P_S(R) = 1$ regardless of the power allocation technique and frequency band adopted. Further, $P_S(R) = 1$ is found for case #2 (see Figures 25(c) and 26(c)) in all frequency bands when $R \geq 2$ bps/Hz regardless of P_T whereas $P_S(R) = 0.05$, 0.29, and 0.46 bps/Hz are found in F_{30}, F_{50}, and F_{86}, respectively, when $R = 0.1$ bps/Hz, $P_T = 30$ dBm, and OA are considered. Regarding case #4 (see Figure 25(d)), when OA and $P_T = 30$ dBm are adopted, one notes that $P_S(R) > 0.8$ for $R \geq 12$ bps/Hz in F_{30} and F_{50} and for $R \geq 10$ bps/Hz in F_{86}. Also, considering $R \leq 2$ bps/Hz, $P_S(R) = 0$ is observed in F_{30} and F_{50} whereas $P_S(R) < 0.2$ is found in F_{86}.

Figure 23 – Cumulative distribution function of $\bar{\gamma}_l$ in dB



(a) Case #1.

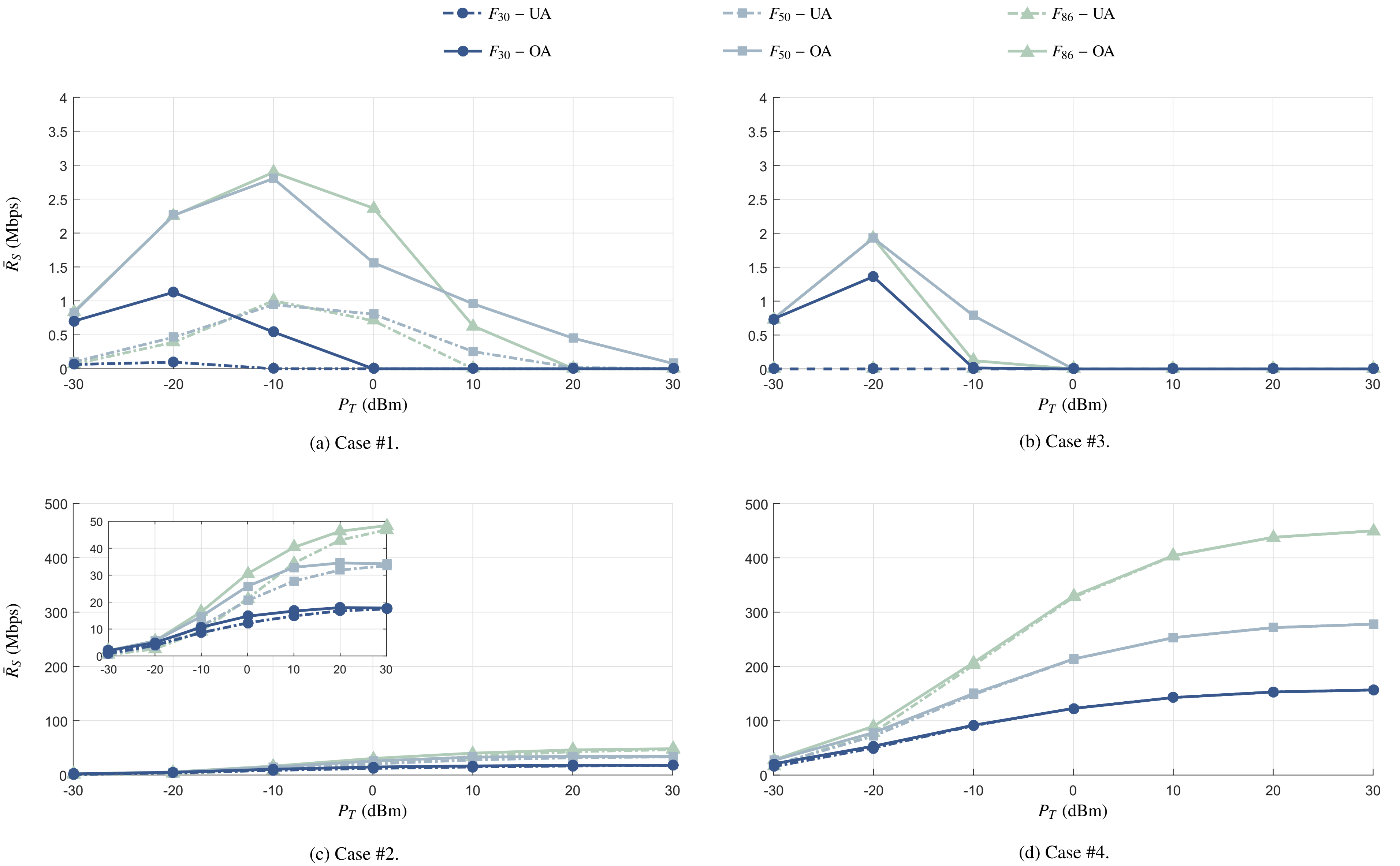
(b) Case #3.

(c) Case #2.

(d) Case #4.

Source: Personal collection.

Figure 24 – PLC wiretap channel model: $\bar{R}_S \times P_T$ under the adoption of both OA and UA techniques



(a) Case #1.

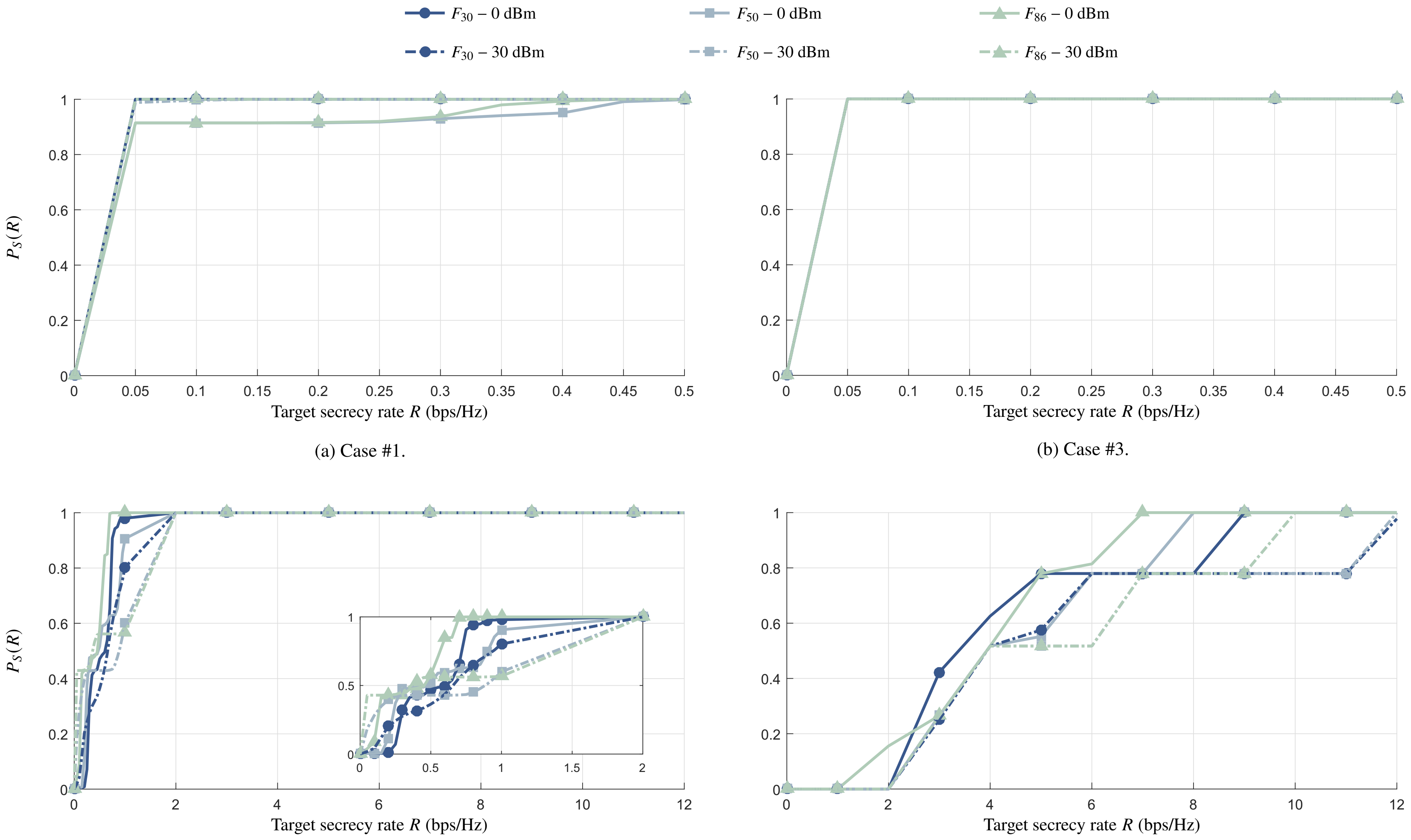
(b) Case #3.

(c) Case #2.

(d) Case #4.

Source: Personal collection.

Figure 25 – PLC wiretap channel model: $P_S(R) \times R$ for $P_T = 0$ and 30 dBm under the adoption of OA



(a) Case #1.

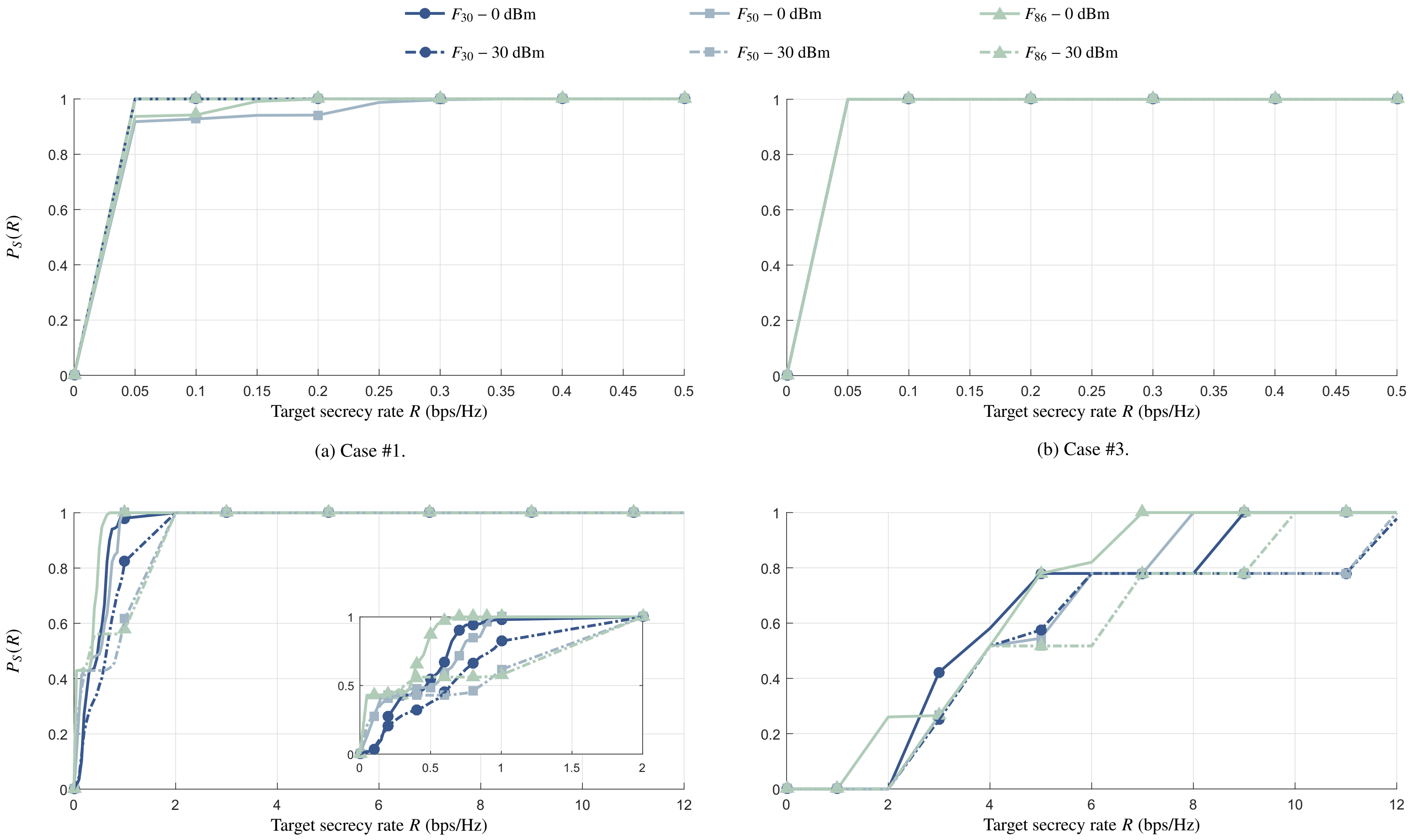
(b) Case #3.

(c) Case #2.

(d) Case #4.

Source: Personal collection.

Figure 26 – PLC wiretap channel model: $P_S(R) \times R$ for $P_T = 0$ and 30 dBm under the adoption of UA



(a) Case #1.

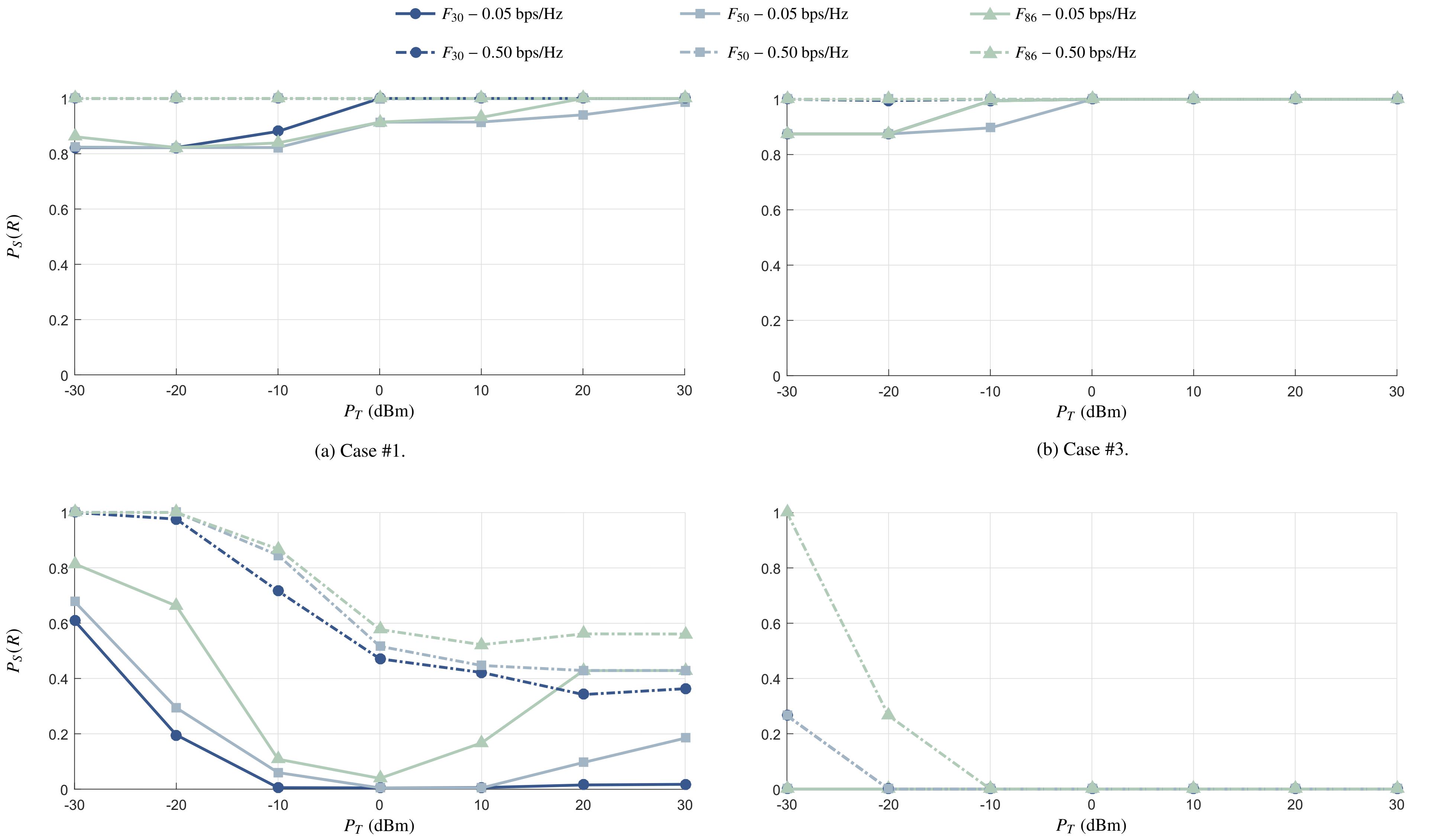
(b) Case #3.

(c) Case #2.

(d) Case #4.

Source: Personal collection.

Figure 27 – PLC wiretap channel model: $P_S(R) \times P_T$ for $R = 0.05$ and 0.50 bps/Hz under the adoption of OA



(a) Case #1.

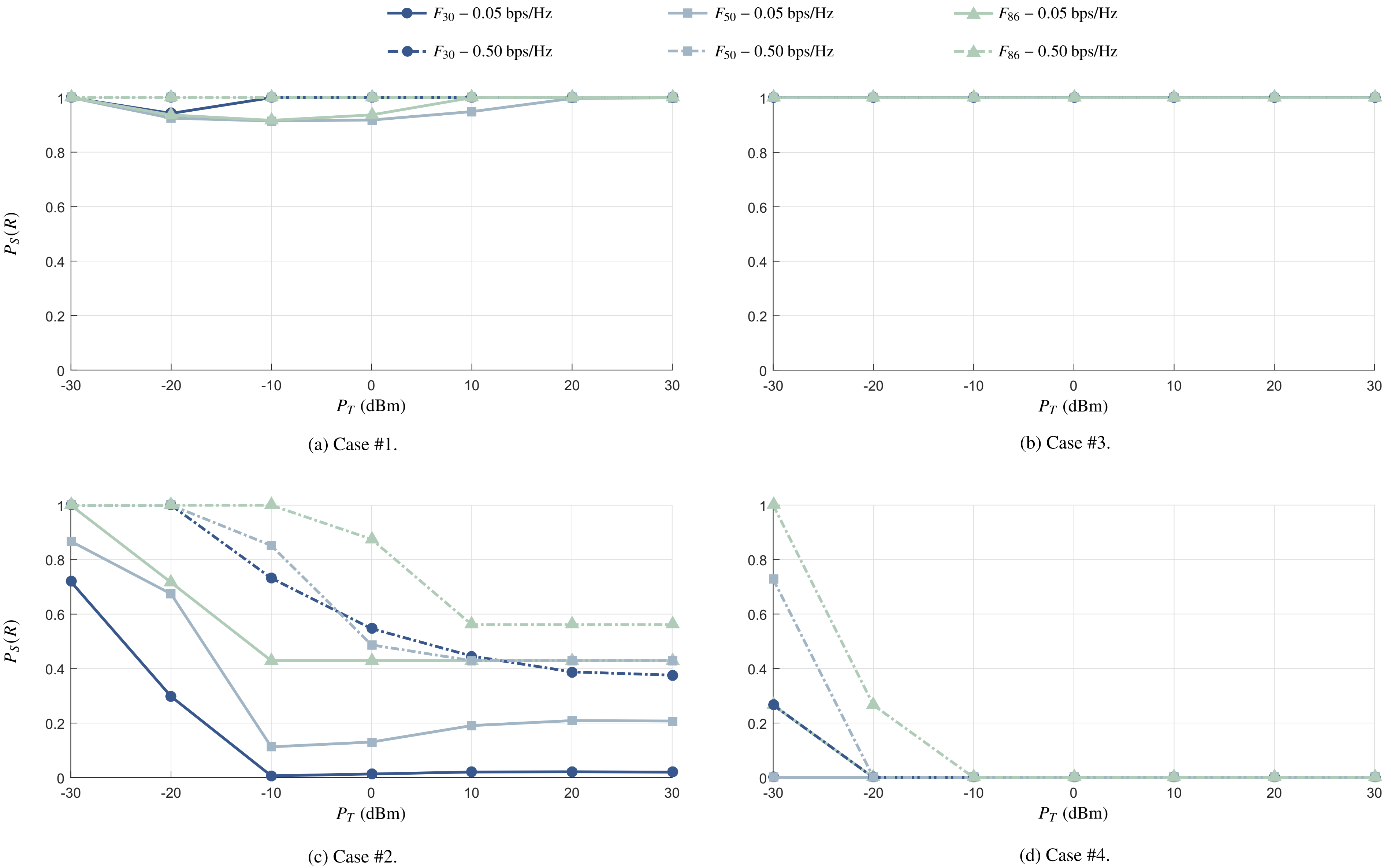
(b) Case #3.

(c) Case #2.

(d) Case #4.

Source: Personal collection.

Figure 28 – PLC wiretap channel model: $P_S(R) \times P_T$ for $R = 0.05$ and 0.50 bps/Hz under the adoption of UA



(a) Case #1.

(b) Case #3.

(c) Case #2.

(d) Case #4.

Source: Personal collection.

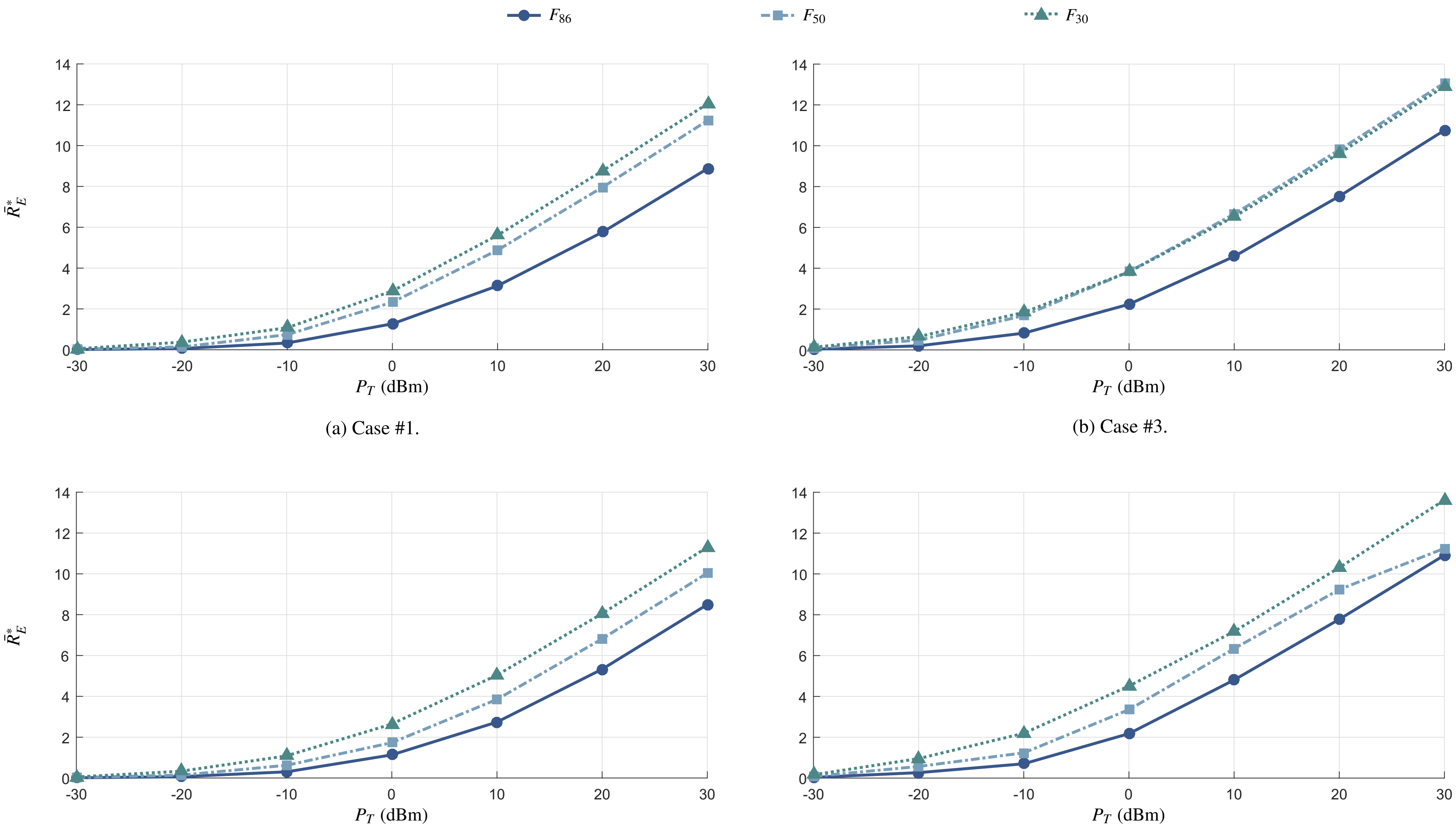
Figures 27(a)-(d) and 28(a)-(d) show $P_S(R) \times P_T$ taking into account the frequency bands F_{30}, F_{50}, and F_{86} and the target secrecy rates $R = 0.05$ and 0.50 bps/Hz. Additionally, Figures 27(a)-(d) depict cases #1, #3, #2, and #4, respectively, with OA and Figures 28(a)-(d) show cases #1, #3, #2, and #4, respectively, with UA. Notice that there is no significant difference between OA and UA. Moreover, cases #1 (see Figures 27(a) and 28(a)) and #3 (see Figures 27(b) and 28(b)) show $P_S(R) > 0.8$ for all values of P_T and the chosen frequency bands. Considering practical values of P_T (i.e., $0 \leq P_T \leq 30$ dBm), case #4 shows $P_S(R) = 0$ in the adopted frequency bands regardless of the value of R. Now, in case #2, one sees significant differences in $P_S(R)$ values for $R = 0.50$ and 0.05 bps/Hz in the adopted frequency bands. For instance, when $P_T \in [0, 30]$ dBm and OA are adopted, the differences reach 0.48, 0.53, and 0.55 in F_{30}, F_{50}, and F_{86}, respectively. Finally, when $P_T = 30$ dBm and $R = 0.05$ bps/Hz, $P_S(R) = 0.02$, 0.19, and 0.46 are found in F_{30}, F_{50}, and F_{86}, respectively.

4.3.3 Analysis of Effective Secrecy Throughput

Figures 29(a)-(d) show $\bar{R}_E^* = \mathbb{E}[R_E^*]$ versus P_T for the PLC wiretap channel model considering cases #1, #3, #2, and #4, respectively. Also, the frequency bands F_{30}, F_{50}, and F_{86} are taken into account. Observe that $\bar{R}_E^*$ increases as P_T rises and the frequency band decreases in all cases, except in case #3 where the $\bar{R}_E^*$ values obtained in F_{30} and F_{50} are close to each other. Moreover, case #4 shows the highest values of $\bar{R}_E^*$ when F_{30} and F_{86} are considered whereas case #3 is better in F_{50}. Also, the smallest values of $\bar{R}_E^*$ are found regarding case #2. For instance, when $P_T = 30$ dBm and F_{86} are adopted, $\bar{R}_E^* = 8.88$, 10.76, 8.50, and 10.92 bps/Hz are observed for cases #1, #3, #2, and #4, respectively.

Figures 30(a)-(d) show $R_B^\star$ and $R_E^\star$ versus P_T for the PLC wiretap channel model taking into account cases #1, #3, #2, and #4, respectively. In addition, the frequency bands F_{30}, F_{50}, and F_{86} are considered. One can see that case #4 show the highest values of $R_B^\star$ and $R_E^\star$ as well as the highest difference between them. On the other hand, case #3 present the smallest difference between $R_B^\star$ and $R_E^\star$, i.e, the smallest target secrecy rate R. For instance, when $P_T = 30$ dBm and F_{86} are taken into account, $R_B^\star = 9.36$ bps/Hz and $R_E^\star = 8.92$ bps/Hz are found for case #1, $R_B^\star = 11.39$ bps/Hz and $R_E^\star = 10.76$ bps/Hz are observed for case #3, $R_B^\star = 9.91$ bps/Hz and $R_E^\star = 8.26$ bps/Hz are seen for case #2, and $R_B^\star = 16.18$ bps/Hz and $R_E^\star = 11.29$ bps/Hz are found for case #4.

Figure 29 – PLC wiretap channel model: $\bar{R}_E^* \times P_T$



(a) Case #1.

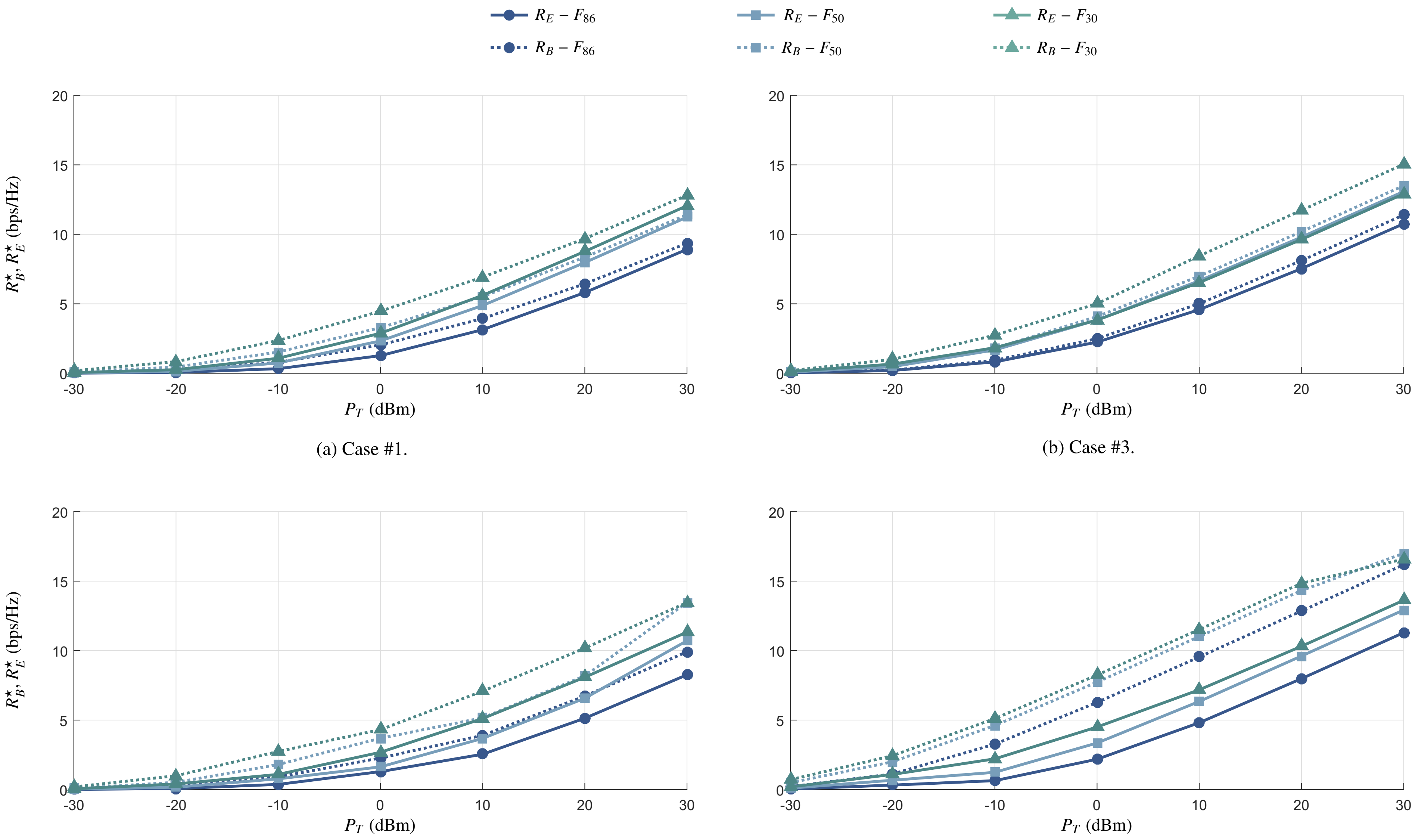
(b) Case #3.

(c) Case #2.

(d) Case #4.

Source: Personal collection.

Figure 30 – PLC wiretap channel model: $R_B^\star$ and $R_E^\star$ versus P_T



(a) Case #1.

(b) Case #3.

(c) Case #2.

(d) Case #4.

Source: Personal collection.

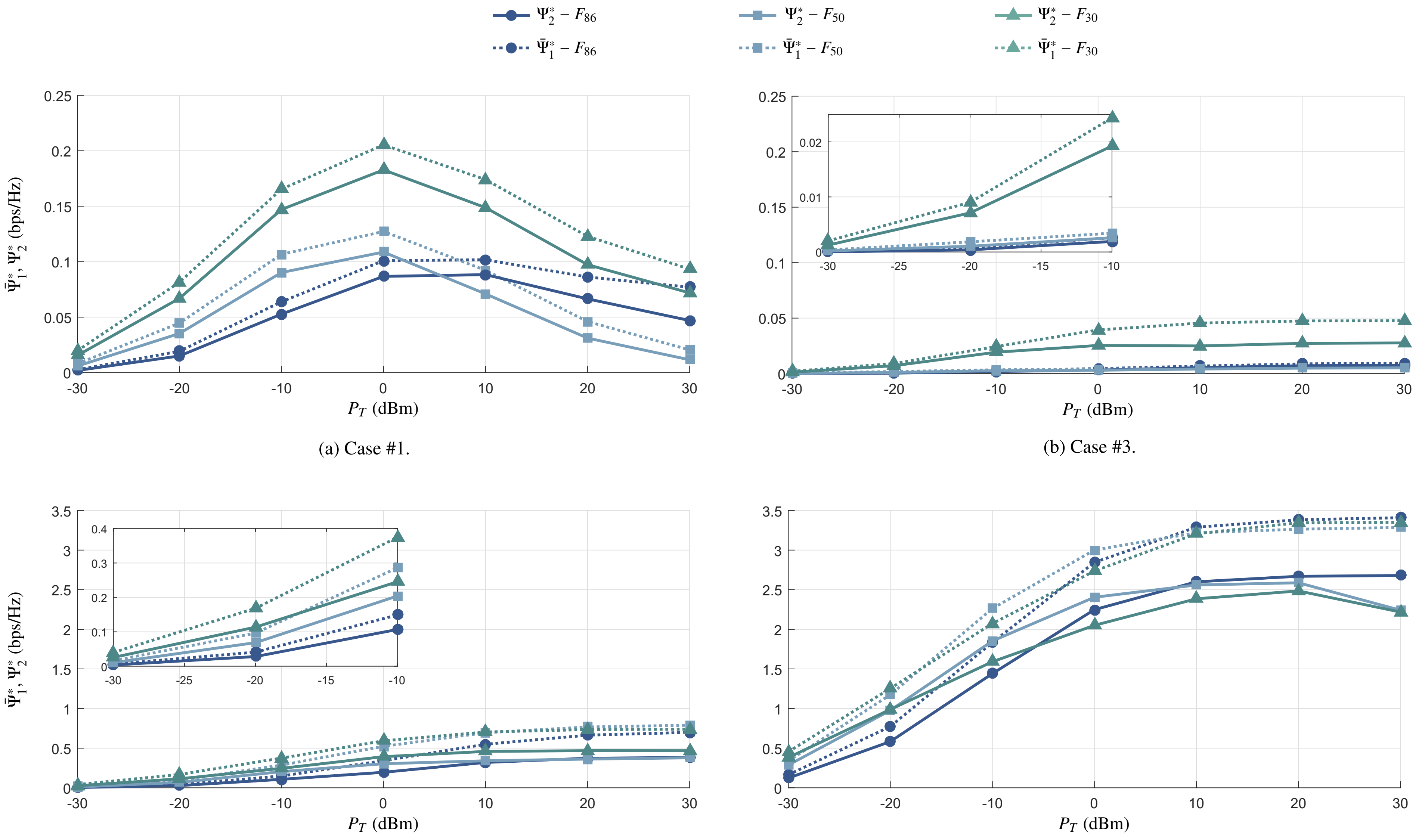
Figures 31(a)-(d) show $\bar{\Psi}_1^* = \mathbb{E}[\Psi_1^*]$ and Ψ_2^* versus P_T for the PLC wiretap channel model considering cases #1, #3, #2, and #4, respectively. Also, the frequency bands F_{30}, F_{50}, and F_{86} are adopted. First, as expected, $\bar{\Psi}_1^*$ is higher than Ψ_2^* regardless of P_T, frequency band, and the analyzed case. Furthermore, for low levels of P_T, the best values of $\bar{\Psi}_1^*$ and Ψ_2^* are found in F_{30} whereas the worst are found in F_{86}, in most cases. However, as P_T increases $\bar{\Psi}_1^*$ and Ψ_2^* in F_{86} tends to be higher than in other frequency bands. The reason is that the magnitude of PLC CFRs may severally attenuate with increasing frequency. However, for high values of P_T this attenuation is not significant. Moreover, case #4 presents the best results whereas case #2 shows the worst ones. For instance, considering $P_T = 30$ dBm and F_{86}, one sees $\bar{\Psi}_1^* = 0.08$, 0.01, 0.70, and 3.41 bps/Hz for cases #1, #3, #2, and #4, respectively, and $\Psi_2^* = 0.05, 0.01, 0.40$, and 2.68 bps/Hz for cases #1, #3, #2, and #4, respectively.

4.3.4 General Comments

First, observe that $\bar{R}_S \times P_T$ and $P_S(R) \times P_T$ curves related to some cases have shown non-typical behaviors. For instance $\bar{R}_S$ increases until a given value of P_T and after that $\bar{R}_S$ decreases. The reason is that, when P_T is low, the fact that Bob's CFR has few sub-channels with nSNR much higher than the ones of Eve's CFR yields $C_B > C_E$, where nSNR denotes the ratio $|H_l[k]|^2/P_{V_l}[k]$, even though Eve's CFR has a greater number of sub-channels better than the ones of Bob's CFR. Conversely, as $P_T \to \infty$, the greater number of sub-channels of Eve's CFR plays a more important role and, as a consequence, $C_E > C_B$ holds.

The discussed numerical results have quantified the PLS in terms of ergodic achievable data rates, secrecy outage probabilities, and effective secrecy throughputs of a broadband PLC system operating in Brazilian in-home facilities. In this scenario, an eavesdropper connected to same electric power grid tries to access private information exchanged between two PLC devices. Such results have shown that cases #1 and #3 are the worst, providing $P_S(R)$ values close to 1 regardless of R, P_T, and the frequency band. Moreover, even for case #2, high values of $P_S(R)$ have been found when $R \geq 0.5$ bps/Hz regardless of P_T. On the other hand, values of $P_S(R)$ around zero and 0.2 have been found in F_{30} and F_{50}, respectively, when $P_T \in [0, 30]$ dBm and a target secrecy rate equal to 0.05 bps/Hz were considered. Further, as expected, case #4 has shown the better performance, in which $P_S(R) = 0$ has been found in all simulated frequency bands when practical values of P_T and $R \leq 1$ have been taken into account. Finally, numerical results regarding the effective secrecy throughput have shown that even in cases #1 and #3, where Alice-Eve links have presented better multi-channel nSNR than Alice-Bob links, PLS is possible if the provided wiretap code rates are used. Also, notice that the difference in security based on the chosen frequency bands is not relevant in terms of secrecy outage probability and effective secrecy throughput.

Figure 31 – PLC wiretap channel model: $\bar{\Psi}_1^*$ and Ψ_2^* versus P_T



(a) Case #1.

(b) Case #3.

(c) Case #2.

(d) Case #4.

Source: Personal collection.

5 THE COMPLETE AND INCOMPLETE LOW-BIT-RATE HYBRID PLC/WLC WIRETAP CHANNEL MODELS

A hybrid PLC/WLC system is an emerging data communication technology for low-bit-rate applications in IoT, smart grids, smart cities, and industry 4.0 scenarios if reliability, flexibility, and availability become a major concern [27–29, 31, 32]. Notice that such a hybrid system uses the parallel combination of both narrowband PLC (NB-PLC) and low-power radio-frequency (LP-RF) channels for providing data communication. However, the broadcast nature of PLC and WLC systems may jeopardize data communication security since malicious users may eavesdrop private messages exchanged between the transmitter and the legitimate receiver. To deal with such a drawback, few studies considered the PLS approach in order to improve the data communication security [49, 51]. In [49], the authors provided secrecy capacity results for both PLC and hybrid PLC/WLC systems whereas in [51] an artificial noise scheme was discussed for the hybrid PLC/WLC system. In this study, secure throughput results were provided for the situations where a PLC or WLC device tries to overhear private messages exchanged between the hybrid PLC/WLC transmitter and the legitimate hybrid PLC/WLC receiver.

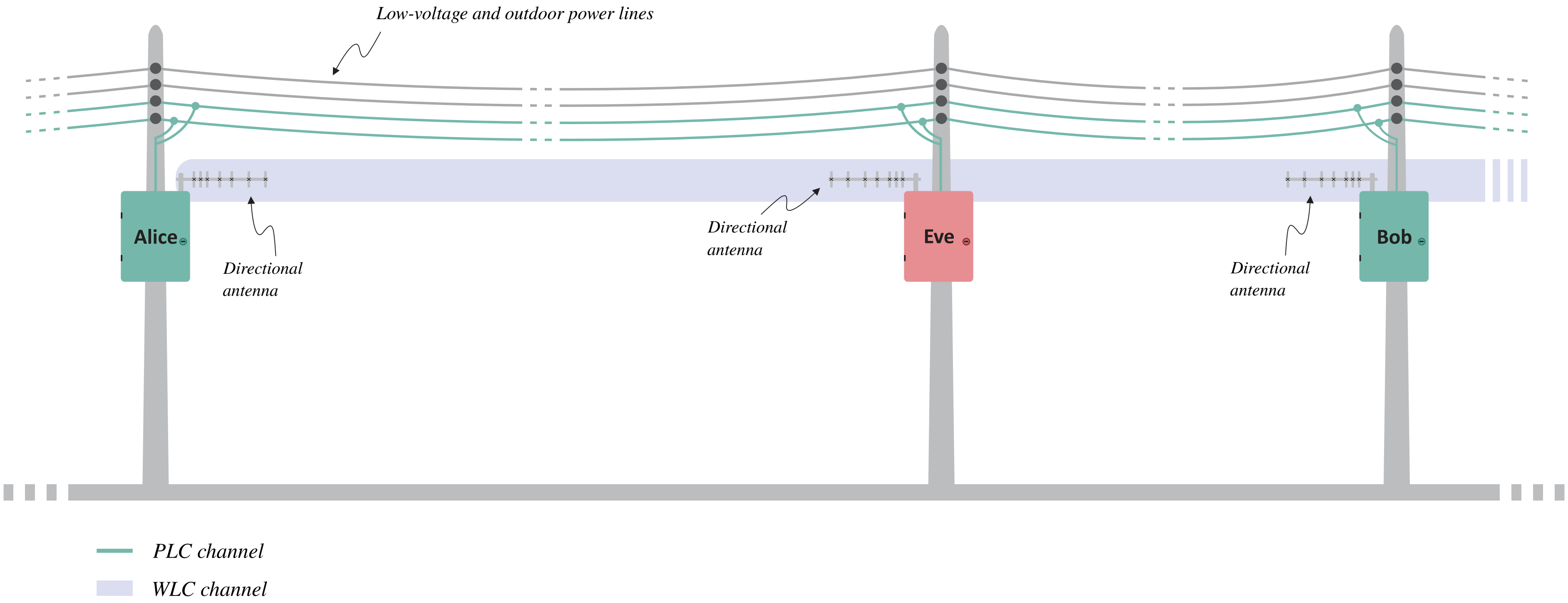
Figure 32 shows a low-bit-rate hybrid PLC/WLC system operating in an outdoor LV electric power grid where the transmitter (Alice) sends private messages to the intended receiver (Bob) through both NB-PLC and LP-RF channels. Meanwhile, a malicious hybrid PLC/WLC device (Eve) overhears those private messages. This scenario is termed hybrid PLC/WLC wiretap channel model. Aiming to offer a better understanding of the hybrid systems under the PLS perspective, this chapter provides comprehensive performance analyses of the low-bit-rate hybrid PLC/WLC wiretap channel model and its incomplete versions by adopting the ergodic achievable secrecy rate and the secrecy outage probability. The incomplete hybrid PLC/WLC wiretap channel models refer to the hybrid PLC/WLC wiretap channel model under the following constraints: (i) one LP-RF or NB-PLC interface is missing and, as a consequence, only a SISO channel model is established and (ii) the NB-PLC or LP-RF link is lost at the legitimate receiver and/or at the eavesdropper, which can give rise to different and very interesting and real scenarios for analyzing secrecy rate at the physical layer level. The main contributions of this chapter are listed as follows:

- The formulation of the hybrid PLC/WLC wiretap channel model as well as of its incomplete versions and the deduction of their ergodic achievable secrecy rates and secrecy outage probabilities when the sum power constraint applies. A detailed discussion of the types of incompleteness that may be associated with the hybrid PLC/WLC wiretap channel model regarding the situations in which an interface (NB-PLC or LP-RF) or a link is missing at the legitimate receiver and/or the eavesdropper.
- Comprehensive performance analyses of the hybrid PLC/WLC and the incomplete hybrid PLC/WLC wiretap channel models from the PLS perspective by considering the OA and the UA (bit and power allocation).

- Performance comparisons among the hybrid PLC/WLC, the incomplete hybrid PLC/WLC, 2×2 parallel MIMO WLC, SISO PLC, and SISO WLC wiretap channel models by considering the NB-PLC and WLC frequency bands, which are intended to assist low-data-rate applications such as IoT, Industry 4.0, and smart grid applications.

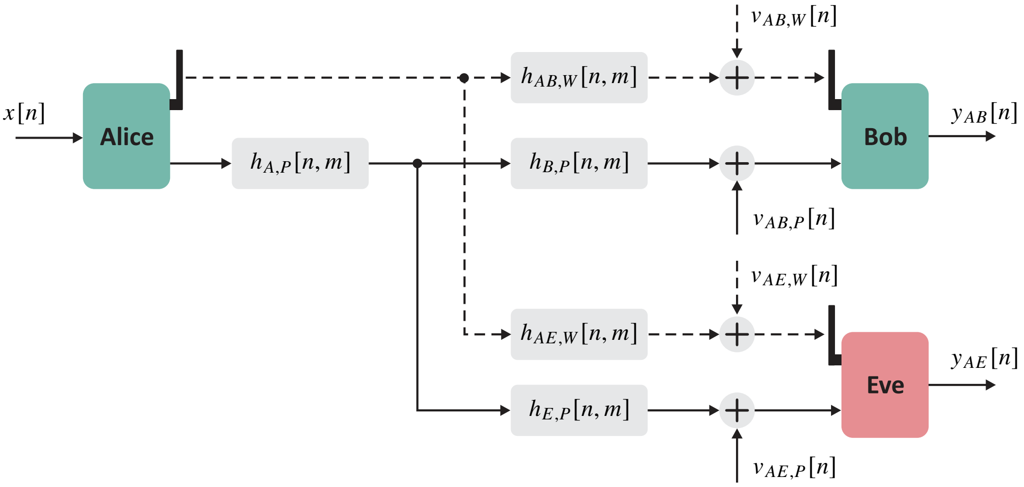
The reminder of this chapter is organized as follows: Section 5.1 introduces the adopted hybrid PLC/WLC wiretap channel model and its incomplete version as well; Section 5.2 deduces the ergodic achievable secrecy rate and secrecy outage probability, which are the performance parameters used in the numerical analyses; and, finally, Section 5.3 shows the numerical results and their discussions.

Figure 32 – Illustration of Eve overhearing private information exchanged between Alice and Bob in a low-bit-rate hybrid PLC/WLC system



Source: Personal collection.

Figure 33 – The (complete) hybrid PLC/WLC wiretap channel model



Source: Personal collection.

The block diagram in Figure 33 illustrates the investigated hybrid PLC/WLC wiretap channel model, in which data are transmitted in parallel through both NB-PLC and LP-RF channels. In this wiretap channel model, PLC and WLC devices operate in the baseband and passband, respectively. Basically, the transmitter Alice (A) sends a message to the legitimate receiver Bob (B) that wants keeping secret from the eavesdropper Eve (E). In Figure 33, dashed and continuous lines denote the wireless and power line links, respectively, whereas the letters W and P denote wireless and power line media, respectively. Note that $\{h_{l,q}[n,m]\}$, where $l \in \{AB,\ AE\}$ and $q \in \{P, W\}$, represents the time-varying channel from Alice to Bob ($l = AB$) or Alice to Eve ($l = AE$) through the PLC ($q = P$) or WLC ($q = W$) medium. Nevertheless, different from the LP-RF channels that are independent, the PLC channels are spatially correlated and, as a consequence, their discrete-time representation can be denoted as $h_{AB,P}[n,m] = h_{A,P}[n,m] \star h_{B,P}[n,m]$ and $h_{AE,P}[n,m] = h_{A,P}[n,m] \star h_{E,P}[n,m]$, where $\star$ denotes the convolution operator [46, 48]. Moreover, it is worth pointing out that the discrete-time signal received by the l^{th} receiver through the q^{th} medium is given by

$$y_{l,q}[n] = \sum_{m=-\infty}^{\infty} A_q x[m] h_{l,q}[n,m] + v_{l,q}[n], \tag{5.1}$$

where $A_q \in \mathbb{R}^+$ is the amplitude of the transmitted sequence and $\{x[n]\}$ and $\{v_{l,q}[n]\}$ are the transmitted symbol and additive noise sequences, respectively, which are assumed to be stationary random processes. Note that $y_l[n] = f(y_{l,P}[n], y_{l,W}[n])$, where $f(\cdot)$ denotes an operator responsible for the combination of the signals received through the wireless and power line interfaces.

It is well-established that NB-PLC and LP-RF channels can be well modeled as linear and time-varying (random) systems. However, if one assumes that the time interval associated with an N-length symbol (N-block symbol) is shorter than the coherence time of the channel, then the channel may be modeled as a linear and time-invariant system during a time interval corresponding to one N-block symbol time interval. In this regard, assume that the discrete-time CIR associated with a given N-block symbol, which is supposed to be transmitted through the existing q^{th} medium between the transmitter (Alice) and the receivers (Bob and Eve), is given by $\{\mathrm{h}_{l,q}[n]\}_{n=0}^{L_{l,q}-1}$, where $L_{l,q}$ denotes the length of CIR.

In this context, the vector representation of such channels during one N-block symbol duration in the discrete-time domain is $\mathbf{h}_{l,q} = [\mathrm{h}_{l,q}[0],\ \mathrm{h}_{l,q}[1],\ \ldots,\ \mathrm{h}_{l,q}[L_{l,q}-1]]^T$ whereas $\mathbf{H}_{l,q} = [H_{l,q}[0],\ H_{l,q}[1],\ \ldots,\ H_{l,q}[N-1]]^T$ denotes its frequency domain vector representation, which is given by $\mathbf{H}_{l,q} = \boldsymbol{\mathcal{F}}[\mathbf{h}_{l,q}^T,\ \mathbf{0}_{N-L_{l,q}}^T]^T$, where $\{\cdot\}^T$ denotes the transpose operator, $\boldsymbol{\mathcal{F}} = \frac{1}{\sqrt{N}}\mathbf{W}$, $\mathbf{W} \in \mathbb{C}^{N\times N}$ is the $N \times N$ DFT matrix, and N represents the number of sub-channels (for more details, see Appendix C). Furthermore, the diagonal matrices $\boldsymbol{\Lambda}_{\mathcal{H}_{l,q}} = \mathbf{diag}\left\{H_{l,q}[0],\ H_{l,q}[1],\ \ldots,\ H_{l,q}[N-1]\right\}$ and $\boldsymbol{\Lambda}_{|\mathcal{H}_{l,q}|^2} = \mathbf{diag}\{|H_{l,q}[0]|^2,\ |H_{l,q}[1]|^2,\ \cdots,|H_{l,q}[N-1]|^2\}$ will be used, where $|\cdot|$ is the modulus operator.

The vector representation of the N-block symbol transmitted through the q^{th} medium in the frequency domain is $\mathbf{X}_q \in \mathbb{C}^{N\times 1}$ so that $\mathbb{E}[\mathbf{X}_q] = \mathbf{0}_{N\times 1}$ and $\mathbb{E}[\mathbf{X}_q\mathbf{X}_q^\dagger] = N\mathbf{I}_N$, in which $\mathbf{I}_N$ denotes the $N \times N$ identity matrix, $\mathbf{0}_{N\times 1}$ represents the N-length column vector of zeros, $\mathbb{E}[\cdot]$ is the expectation operator, and $\{\cdot\}^\dagger$ denotes Hermitian operator. Also, $\mathbf{V}_{l,q} \in \mathbb{C}^{N\times 1}$ is the frequency domain vector representation of the additive noise such that $\mathbb{E}[\mathbf{V}_{l,q}] = \mathbf{0}_{N\times 1}$, $\mathbb{E}[\mathbf{V}_{l,q}\mathbf{V}_{l,q}^\dagger] = N\boldsymbol{\Lambda}_{P_{V_{l,q}}}$, where $\boldsymbol{\Lambda}_{P_{V_{l,q}}} = \mathbf{diag}\left\{P_{V_{l,q}}[0],\ P_{V_{l,q}}[1],\ \ldots,P_{V_{l,q}}[N-1]\right\}$ and $P_{V_{l,q}}[k]$ is the additive noise power in the k^{th} sub-channel. Furthermore, $\boldsymbol{\Lambda}_{P_q} = \mathbf{diag}\left\{P_q[0],\ P_q[1],\ \ldots,\ P_q[N-1]\right\}$ is the matrix representation of the power allocated to the sub-channels in the frequency domain, such that $\mathbf{tr}(\boldsymbol{\Lambda}_{P_q}) = P_q$, where $\mathbf{tr}(\cdot)$ is the trace operator, and $\boldsymbol{\Lambda}_{\sqrt{P_q}} = \mathbf{diag}\left\{\sqrt{P_q[0]},\ \sqrt{P_q[1]},\ \ldots,\ \sqrt{P_q[N-1]}\right\}$ denotes the amplitude of $\mathbf{X}_q$. The total transmission power used by Alice to perform data communication is $P_T = P_P + P_W$, where P_P and P_W are the transmission powers allocated to perform data communication through NB-PLC and LP-RF channels, respectively.

Furthermore, according to [23], the hybrid PLC/WLC wiretap channel model is incomplete when either LP-RF or NB-PLC interface is lost at Alice or either LP-RF or NB-PLC link is missing between Alice and Bob and/or Eve. The former results in a SISO channel model (PLC or WLC) whereas the latter may generate a SISO channel model or a different kind of incompleteness. As well-discussed in [23], the incompleteness of the hybrid PLC/WLC wiretap channel model may be generated by human being and/or natural sources. The main underlying sources of incompleteness in the hybrid PLC/WLC wiretap channel model are as follows:

- High attenuation of the WLC signal due to rain or snow events.
- WLC path interruption because of tree growth or building construction that impairs the

line-of-sight signal propagation.

- Interruption of the power line due to a high impedance fault, fall of a pole, fall of a tree over the power line, or a cable breaking.
- Power cable aging that may severely attenuate the PLC signal over time.
- Hardware failure of the front-end of the transceiver belonging to Alice, Bob or Eve.

Bearing that in mind, the scenarios in which a link is missing at the l^{th} receiver are shown in Figure 34. Each of them and their corresponding acronyms may be shortly described as follows:

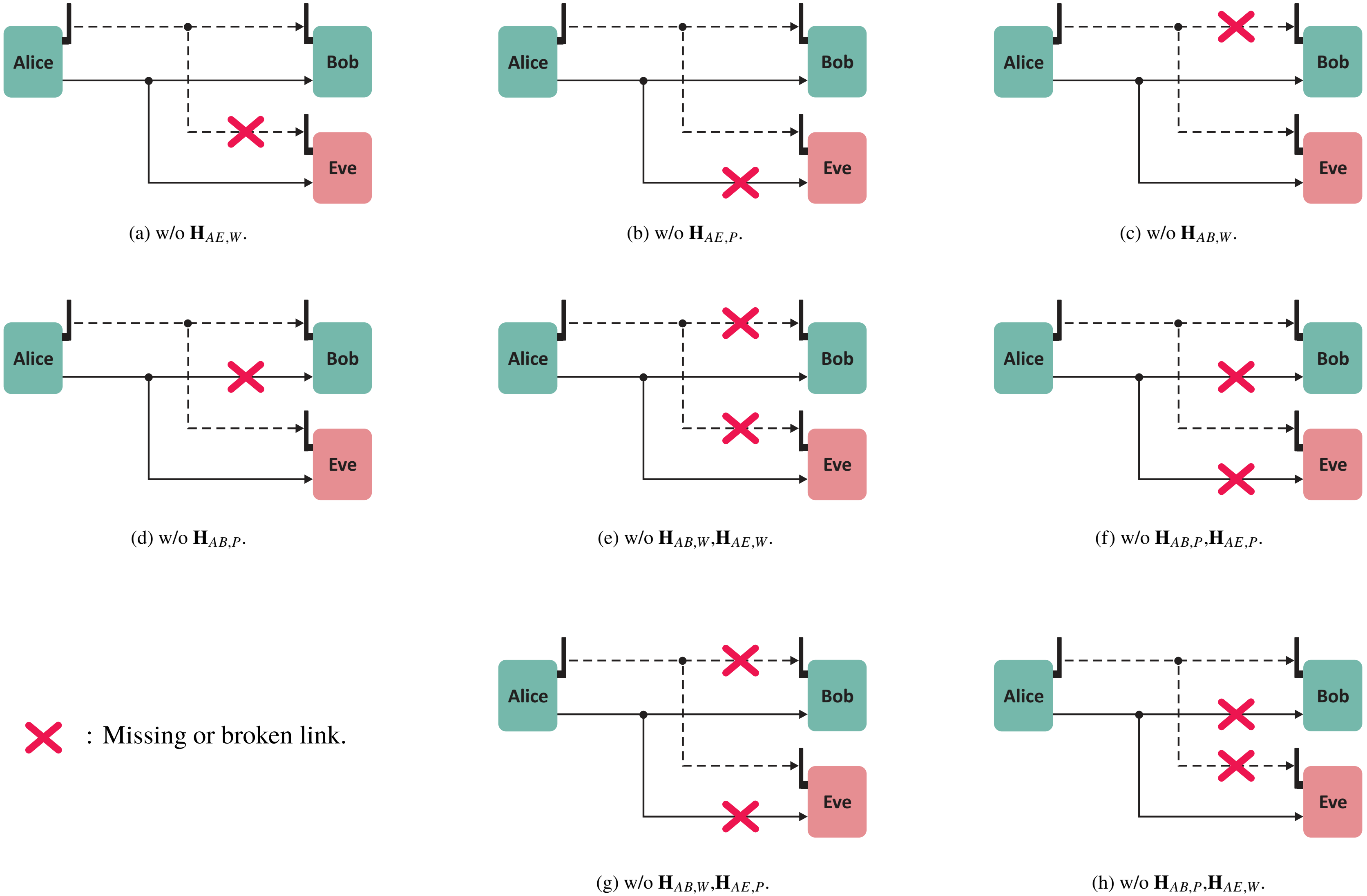
- w/o $\mathbf{H}_{AE,W}$ (Figure 34a): This situation occurs when Eve misses the LP-RF link.
- w/o $\mathbf{H}_{AE,P}$ (Figure 34b): This scenario happens when Eve misses the NB-PLC link.
- w/o $\mathbf{H}_{AB,W}$ (Figure 34c): It occurs when Bob loses the LP-RF link.
- w/o $\mathbf{H}_{AB,P}$ (Figure 34d): This condition happens when Bob misses the NB-PLC link.
- w/o $\mathbf{H}_{AB,W}$, $\mathbf{H}_{AE,W}$ (Figure 34e): It happens if both Bob and Eve miss the LP-RF link.
- w/o $\mathbf{H}_{AB,P}$,$\mathbf{H}_{AE,P}$ (Figure 34f): It is the case where both Bob and Eve lose the NB-PLC link.
- w/o $\mathbf{H}_{AB,W}$,$\mathbf{H}_{AE,P}$ (Figure 34g): This scenario occurs when Bob misses the LP-RF link and Eve misses the NB-PLC link.
- w/o $\mathbf{H}_{AB,P}$,$\mathbf{H}_{AE,W}$ (Figure 34h): This situation happens when Bob misses the NB-PLC link and Eve misses the LP-RF one.

Note that for the scenarios w/o $\mathbf{H}_{AB,W}$, w/o $\mathbf{H}_{AB,P}$, w/o $\mathbf{H}_{AB,W}$,$\mathbf{H}_{AE,W}$, and w/o $\mathbf{H}_{AB,P}$,$\mathbf{H}_{AE,P}$ the hybrid PLC/WLC wiretap channel model becomes a SISO wiretap channel model since one assumes that Alice completely knows Bob's CSI. Furthermore, for the situations portrayed by w/o $\mathbf{H}_{AB,W}$,$\mathbf{H}_{AE,P}$ and w/o $\mathbf{H}_{AB,P}$,$\mathbf{H}_{AE,W}$, one can recognize that Eve is no more capable of overhearing any information from Alice when Bob misses a link. In fact, it is clear that Alice immediately knows what is happening and promptly stops transmitting information because the assumption of the complete CSI availability. Based on that, only SISO PLC, SISO WLC, w/o $\mathbf{H}_{AE,W}$, and w/o $\mathbf{H}_{AE,P}$ scenarios shall be considered as valuable for evaluation since they correctly characterize the behavior of the incomplete hybrid PLC/WLC wiretap channel model under the PLS perspective.

Given the aforementioned formulation, the following research questions arise: *Can the hybrid PLC/WLC wiretap channel model offers higher security at physical layer level than SISO PLC and SISO WLC wiretap channels, or even the* 2×2 *MIMO WLC wiretap channel, under the sum power constraint assumption?*

How is the behavior of the achievable secrecy rate of the hybrid PLC/WLC wiretap channel model when a data communication path is missing at Eve? In other words, are there benefits by exploiting the diversity between PLC and WLC media in terms of secrecy rate? Aiming to answer these questions, Section 5.2 deduces the ergodic achievable secrecy rate and the secrecy outage probability for the hybrid PLC/WLC wiretap channel model and its incomplete versions while Section 5.3 provides important findings related to the PLS of hybrid PLC/WLC systems based on numerical results.

Figure 34 – Types of incompleteness of the hybrid PLC/WLC wiretap channel model: link(s) is (are) missing at the l^{th} receiver



(a) w/o $\mathbf{H}_{AE,W}$.

(b) w/o $\mathbf{H}_{AE,P}$.

(c) w/o $\mathbf{H}_{AB,W}$.

(d) w/o $\mathbf{H}_{AB,P}$.

(e) w/o $\mathbf{H}_{AB,W}$,$\mathbf{H}_{AE,W}$.

(f) w/o $\mathbf{H}_{AB,P}$,$\mathbf{H}_{AE,P}$.

(g) w/o $\mathbf{H}_{AB,W}$,$\mathbf{H}_{AE,P}$.

(h) w/o $\mathbf{H}_{AB,P}$,$\mathbf{H}_{AE,W}$.

Source: Personal collection.

5.2 ERGODIC ACHIEVABLE SECRECY RATES AND SECRECY OUTAGE PROBABILITIES

First of all, note that this section presents many similarities with Sections 3.2 and 4.2. In order to facilitate understanding, these similarities are preserved. In this regard, mathematical expressions to compute the ergodic achievable secrecy rates and outage probabilities for the (complete) hybrid PLC/WLC wiretap channel model as well as for its incomplete versions are deduced. To do so, similar to the LGRC addressed in [92], one assumes that the PLC and WLC channels within the hybrid PLC/WLC wiretap channel model are an N-block linear Gaussian channels with finite memory (i.e., $L_{\max} = \max_{l,q} L_{l,q}$). However, the inter-block interference caused by the memory of CIRs and the correlated noises make difficult to evaluate the achievable data rate [93]. To overcome this situation, one uses the same idea proposed in [93], which states that the N-block CGRC eliminates the inter-block interference when $N \geq L_{\max}$. Also, the LGRC tends to N-CGRC as $N \longrightarrow \infty$. As a result, the hybrid PLC/WLC channel model is modeled as N-CGRC because $N \longrightarrow \infty$ is taken into account.

Assuming that the synchronization is perfect and CSI is available at Alice, Bob, and Eve and they can access their own CSI, the frequency domain vectorial representation of the received symbol associated with the q^{th} medium at the l^{th} receiver is given by

$$\mathbf{Y}_{l,q} = \mathbf{\Lambda}_{\sqrt{P_q}} \mathbf{\Lambda}_{\mathcal{H}_{l,q}} \mathbf{X}_q + \mathbf{V}_{l,q}. \tag{5.2}$$

Consequently, the mutual information between Alice and the l^{th} receiver can be expressed as

$$\begin{aligned} I(\mathbf{X};\mathbf{Y}_l) &= \hbar(\mathbf{Y}_l) - \hbar(\mathbf{Y}_l|\mathbf{X}) \\ &= \hbar(\mathbf{Y}_l) - [\hbar(\mathbf{G}_l\mathbf{X}|\mathbf{X}) + \hbar(\mathbf{V}_l|\mathbf{X})] \\ &= \hbar(\mathbf{Y}_l) - \hbar(\mathbf{V}_l), \end{aligned} \tag{5.3}$$

where $\hbar(\cdot)$ is the differential entropy function,

$$\begin{aligned} \mathbf{Y}_l &= \left[\mathbf{Y}_{l,P}{}^T,\ \mathbf{Y}_{l,W}{}^T\right]^T \\ &= \begin{pmatrix} \mathbf{\Lambda}_{\sqrt{P_P}}\, \mathbf{\Lambda}_{\mathcal{H}_{l,P}} & 0 \\ 0 & \mathbf{\Lambda}_{\sqrt{P_W}}\, \mathbf{\Lambda}_{\mathcal{H}_{l,W}} \end{pmatrix} \mathbf{X} + \mathbf{V}_l \\ &= \mathbf{G}_l\mathbf{X} + \mathbf{V}_l, \end{aligned} \tag{5.4}$$

$\mathbf{X} = [\mathbf{X}_P{}^T,\ \mathbf{X}_W{}^T]^T$, and $\mathbf{V}_l = [\mathbf{V}_{l,P}{}^T,\ \mathbf{V}_{l,W}{}^T]^T$. Assuming that the additive noise and transmitted symbols are Gaussian random processes, then the entropies of $\mathbf{Y}_l$ and $\mathbf{V}_l$ are given by

$$\hbar(\mathbf{Y}_l) = \frac{1}{2}\log_2\left[(2\pi e)^{2N}\det(\mathbf{R}_{\mathbf{YY},l})\right] \tag{5.5}$$

and

$$\hbar(\mathbf{V}_l) = \frac{1}{2}\log_2\left[(2\pi e)^{2N}\det(\mathbf{R}_{\mathbf{VV},l})\right], \tag{5.6}$$

respectively, in which $\det(\mathbf{\Lambda}_D)$ is the determinant of the matrix $\mathbf{\Lambda}_D$, $\mathbf{R}_{\mathbf{YY},l} = \mathbb{E}[\mathbf{Y}_l\mathbf{Y}_l^\dagger] = \mathbf{G}_l\mathbf{R}_{\mathbf{XX}}\mathbf{G}_l^\dagger + \mathbf{R}_{\mathbf{VV},l}$, $\mathbf{R}_{\mathbf{XX}} = \mathbb{E}[\mathbf{XX}^\dagger] = 2N\mathbf{I}_{2N}$, $\mathbf{R}_{\mathbf{VV},l} = \mathbb{E}[\mathbf{V}_l\mathbf{V}_l^\dagger] = 2N\mathbf{\Lambda}_{P_{V_l}}$, and $\mathbf{\Lambda}_{P_{V_l}} = \mathbf{diag}\{\mathbf{\Lambda}_{P_{V_{l,P}}},\ \mathbf{\Lambda}_{P_{V_{l,W}}}\}$. The complete deduction of (5.5) and (5.6) are addressed in Appendix D. Thus, the capacity between Alice and the l^{th} receiver can be expressed as

$$\begin{aligned} C_l &= \max_{f_{\mathbf{X}}(\mathbf{x}):\mathbf{tr}(\mathbf{R}_{\mathbf{XX}})\leq NP_T} I(\mathbf{X};\mathbf{Y}_l) \\ &= \max_{\mathbf{tr}(\mathbf{\Lambda}_P)\leq P_T} \log_2\left[\det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_l}\right)\right] \text{ [bps/Hz]}, \end{aligned} \tag{5.7}$$

in which $f_{\mathbf{X}}(\mathbf{x})$ is the joint density function of $\mathbf{X}$,

$$\begin{aligned} \mathbf{\Lambda}_{\gamma_l} &= \mathbb{E}\left[\mathbf{G}_l\mathbf{X}\left(\mathbf{G}_l\mathbf{X}\right)^\dagger\right]\left\{\mathbb{E}\left[\mathbf{V}_l\mathbf{V}_l^\dagger\right]\right\}^{-1} \\ &= \mathbf{G}_l\mathbf{R}_{\mathbf{XX}}\mathbf{G}_l^\dagger\mathbf{R}_{\mathbf{VV},l}^{-1} \\ &= \mathbf{\Lambda}_{P_\Pi}\mathbf{\Lambda}_{|\mathcal{H}_l|^2}\mathbf{\Lambda}_{P_{V_l}}^{-1}, \end{aligned} \tag{5.8}$$

$\mathbf{\Lambda}_{P_\Pi} = \mathbf{diag}\{\mathbf{\Lambda}_{P_P},\ \mathbf{\Lambda}_{P_W}\}$ and $\mathbf{tr}(\mathbf{\Lambda}_{P_\Pi}) = P_T$, and $\mathbf{\Lambda}_{|\mathcal{H}_l|^2} = \mathbf{diag}\{\mathbf{\Lambda}_{|\mathcal{H}_{l,P}|^2},\ \mathbf{\Lambda}_{|\mathcal{H}_{l,W}|^2}\}$. For the sake of simplicity, the subscript q can be disregarded and then $\mathbf{\Lambda}_{P_\Pi} = \mathbf{diag}\{P_\Pi[0],\ P_\Pi[1],\ \ldots,\ P_\Pi[2N-1]\}$ and $\mathbf{\Lambda}_{|\mathcal{H}_l|^2} = \mathbf{diag}\{|H_l[0]|^2, |H_l[1]|^2,\ \ldots,\ |H_l[2N-1]|^2\}$.

The secrecy capacity is given by [95]

$$C_S = \max_{f_{\mathbf{X}}(\mathbf{x}):\mathbf{tr}(\mathbf{R}_{\mathbf{XX}})\leq 2NP_T} \left[I(\mathbf{X};\mathbf{Y}_{AB}) - I(\mathbf{X};\mathbf{Y}_{AE})\right]^+. \tag{5.9}$$

where $\max[b]^+ = \max(0, b)$. The hardness to compute (5.9) motivates the use of following lower bound

$$C_S \geq \left[\max_{f_{\mathbf{X}}(\mathbf{x}):\mathbf{tr}(\mathbf{R}_{\mathbf{XX}})\leq 2NP_T} I(\mathbf{X};\mathbf{Y}_{AB}) - \max_{f_{\mathbf{X}}(\mathbf{x}):\mathbf{tr}(\mathbf{R}_{\mathbf{XX}})\leq 2NP_T} I(\mathbf{X};\mathbf{Y}_{AE})\right]^+, \tag{5.10}$$

In this way, the achievable secrecy rate for the hybrid PLC/WLC wiretap channel model can be expressed as

$$\begin{aligned} R_S = \frac{B_w}{N}\Bigg[&\max_{\mathbf{\Lambda}_{P_\Pi}} \log_2\left[\det\left(\mathbf{I}_{2N} + \mathbf{\Lambda}_{\gamma_{AB}}\right)\right] - \\ &\max_{\mathbf{\Lambda}_{P_\Pi}} \log_2\left[\det\left(\mathbf{I}_{2N} + \mathbf{\Lambda}_{\gamma_{AE}}\right)\right]\Bigg]^+ \text{ [bps]}, \end{aligned} \tag{5.11}$$

where B_w is the frequency bandwidth. In order to maximize (5.11), the following optimization problem has to be solved:

$$\max_{\mathbf{\Lambda}_{P_\Pi}} R_S \quad \text{subject to} \quad \mathbf{tr}(\mathbf{\Lambda}_{P_\Pi}) \leq P_T \quad \text{and} \quad P_\Pi[k] \geq 0,$$

in which $P_\Pi[k]$ is the k^{th} element of the main diagonal of the matrix $\mathbf{\Lambda}_{P_\Pi}$ and $0 \leq k \leq 2N-1$. However, that problem is non-convex. Then, from [95] and [99], making $P_\Pi[k] = 0$ for the sub-channels where $\dot{\gamma}_{AB}[k] \leq \dot{\gamma}_{AE}[k]$, such that $\dot{\gamma}_l[k] = |H_l[k]|^2/P_{V_l}$ is the nSNR of the k^{th} sub-channel, the remaining problem is convex and its solution is given by

$$P_{\Pi}[k] = \begin{cases} 0 & \text{, if } \dot{\gamma}_{AB}[k] \leq \dot{\gamma}_{AE}[k] \\ \left[-\alpha[k] + \sqrt{\frac{1}{4}\beta^2[k] + \frac{1}{\lambda \ln(2)}\beta[k]} \right]^+ & \text{, otherwise} \end{cases} \tag{5.12}$$

and $\lambda > 0$ such that $\mathbf{tr}(\mathbf{\Lambda}_{P_{\Pi}}) = P_T$. Note that $\alpha[k]$ and $\beta[k]$ can be expressed as

$$\alpha[k] = \frac{P_{V_{AE}}[k]|H_{AB}[k]|^2 + P_{V_{AB}}[k]|H_{AE}[k]|^2}{2|H_{AB}[k]|^2|H_{AE}[k]|^2} \tag{5.13}$$

and

$$\beta[k] = \frac{P_{V_{AE}}[k]|H_{AB}[k]|^2 - P_{V_{AB}}[k]|H_{AE}[k]|^2}{2|H_{AB}[k]|^2|H_{AE}[k]|^2}, \tag{5.14}$$

respectively. Then the ergodic achievable secrecy rate is given by

$$\begin{aligned} \bar{R}_S = \mathbb{E}_{\mathcal{H}_{AB},\mathcal{H}_{AE}} \Bigg\{ \frac{B_w}{N} \Bigg[& \max_{\mathbf{\Lambda}_{P_{\Pi}}} \log_2 \left[\det\left(\mathbf{I}_{2N} + \mathbf{\Lambda}_{\gamma_{AB}}\right)\right] - \\ & \max_{\mathbf{\Lambda}_{P_{\Pi}}} \log_2 \left[\det\left(\mathbf{I}_{2N} + \mathbf{\Lambda}_{\gamma_{AE}}\right)\right] \Bigg]^+ \Bigg\} \text{ [bps]}. \end{aligned} \tag{5.15}$$

From (5.15), note that $\lim\limits_{P_{\Pi} \to \infty} R_S = \log_2 \left[\det\left(\mathbf{\Lambda}_{|\mathcal{H}_{AB}|^2} \mathbf{\Lambda}_{|\mathcal{H}_{AE}|^2}^{-1} \right) \right]$, which means that when $P_{\Pi} \longrightarrow \infty$ the achievable secrecy rate only depends on the relation $\mathbf{\Lambda}_{|\mathcal{H}_{AB}|^2} \mathbf{\Lambda}_{|\mathcal{H}_{AE}|^2}^{-1}$.

Finally, an outage event occurs when Alice-Bob link is in outage or Eve is capable of decoding the private message transmitted through the Alice-Bob link. However, as only the sub-bands in which Alice-Bob is better than Alice-Eve is considered in this study, the outage probability can be calculated by using

$$\begin{aligned} P_S(R) &= \mathbb{P}\left\{ \frac{R_S}{B_w} < R \right\} \\ &= \mathbb{P}\left\{ \det\left(\frac{\mathbf{I}_{2N} + \mathbf{\Lambda}_{\gamma_{AB}}}{\mathbf{I}_{2N} + \mathbf{\Lambda}_{\gamma_{AE}}} \right) < 2^{RN} \right\}, \end{aligned} \tag{5.16}$$

where $R \in \mathbb{R}^+$ is the target secrecy rate and $\mathbb{P}\{c < d\}|(c, d) \in \mathbb{R}^2$ denotes the probability that c is less than d.

5.2.1 Incomplete Hybrid PLC/WLC Wiretap Channel Model

Based on the hybrid PLC/WLC wiretap channel model, the ergodic achievable secrecy rate for its incomplete versions is computed. In this context, note that both SISO PLC and WLC wiretap channel models can be considered as incomplete versions of the hybrid PLC/WLC wiretap channel model (i.e., the PLC or WLC interface of Alice does not work or Bob misses

Table 5 – The list of channel models and their respective symbols (ζ)

ζ	**Description**
M	In parallel 2 × 2 MIMO WLC (2 × 2 MIMO WLC)
Π	Hybrid PLC/WLC
W	SISO WLC
P	SISO PLC
$\bar{P}_E$	w/o $\mathbf{H}_{AE,P}$
$\bar{W}_E$	w/o $\mathbf{H}_{AE,W}$

Source: Personal collection.

a link). As a consequence, the ergodic achievable secrecy rate of both SISO wiretap channel models can be obtained from (5.15) as follows:

$$\begin{aligned}\bar{R}_{S,\zeta} = \mathbb{E}_{\boldsymbol{\mathcal{H}}_{AB},\boldsymbol{\mathcal{H}}_{AE}} \Bigg\{ \frac{B_w}{N} \Bigg[\max_{\boldsymbol{\Lambda}_{P_\Pi}} \log_2 \left[\det\left(\mathbf{I}_N + \boldsymbol{\Lambda}_{\gamma_{AB}}\right)\right] - \\ \max_{\boldsymbol{\Lambda}_{P_\Pi}} \log_2 \left[\det\left(\mathbf{I}_N + \boldsymbol{\Lambda}_{\gamma_{AE}}\right)\right] \Bigg]^+ \Bigg\} \text{ [bps]}, \end{aligned} \tag{5.17}$$

in which $\zeta \in \{W, P\}$ is in accord with Table 5. For the SISO PLC and WLC scenarios, one assumes that $\boldsymbol{\Lambda}_{\gamma_l} = \boldsymbol{\Lambda}_{P_\Pi}\boldsymbol{\Lambda}_{|\boldsymbol{\mathcal{H}}_l|^2}\boldsymbol{\Lambda}_{P_{V_l}}^{-1}$ because the adopted assumptions for mathematically representing the hybrid PLC/WLC wiretap channel models consider that both PLC and WLC channels work in parallel. Note that in (5.17), $\boldsymbol{\Lambda}_{P_\Pi} \in \mathbb{R}^{N\times N}$, $\boldsymbol{\Lambda}_{|\boldsymbol{\mathcal{H}}_l|^2} \in \mathbb{R}^{N\times N}$, and $\boldsymbol{\Lambda}_{P_{V_l}} \in \mathbb{R}^{N\times N}$ are taken into account since only one channel (PLC or WLC) is used. Similar to (5.16), the secrecy outage probability of the incomplete hybrid PLC/WLC wiretap channel model is given by

$$\begin{aligned} P_{S,\zeta}(R) &= \mathbb{P}\left\{\frac{R_{S,\zeta}}{Bw} < R\right\} \\ &= \mathbb{P}\left\{\det\left(\frac{\mathbf{I}_N + \boldsymbol{\Lambda}_{\gamma_{AB}}}{\mathbf{I}_N + \boldsymbol{\Lambda}_{\gamma_{AE}}}\right) < 2^{RN}\right\}. \end{aligned} \tag{5.18}$$

Moreover, the ergodic achievable secrecy rates for w/o $\mathbf{H}_{AE,P}$ and w/o $\mathbf{H}_{AE,W}$ incomplete versions of the hybrid PLC/WLC wiretap channel model are given by

$$\begin{aligned}\bar{R}_{S,\bar{P}_E} = \mathbb{E}_{\boldsymbol{\mathcal{H}}_{AB},\boldsymbol{\mathcal{H}}_{AE}} \Bigg\{ \frac{B_w}{N} \Bigg[\max_{\boldsymbol{\Lambda}_{P_\Pi}} \log_2 \left[\det\left(\mathbf{I}_{2N} + \boldsymbol{\Lambda}_{\gamma_{AB}}\right)\right] - \\ \max_{\boldsymbol{\Lambda}_{P_\Pi}} \log_2 \left[\det\left(\mathbf{I}_{2N} + \boldsymbol{\Lambda}_{\bar{P}_E}\boldsymbol{\Lambda}_{\gamma_{AE}}\right)\right] \Bigg]^+ \Bigg\} \text{ [bps]}. \end{aligned} \tag{5.19}$$

and

$$\begin{aligned}\bar{R}_{S,\bar{W}_E} = \mathbb{E}_{\boldsymbol{\mathcal{H}}_{AB},\boldsymbol{\mathcal{H}}_{AE}} \Bigg\{ \frac{B_w}{N} \Bigg[\max_{\boldsymbol{\Lambda}_{P_\Pi}} \log_2 \left[\det\left(\mathbf{I}_{2N} + \boldsymbol{\Lambda}_{\gamma_{AB}}\right)\right] - \\ \max_{\boldsymbol{\Lambda}_{P_\Pi}} \log_2 \left[\det\left(\mathbf{I}_{2N} + \boldsymbol{\Lambda}_{\bar{W}_E}\boldsymbol{\Lambda}_{\gamma_{AE}}\right)\right] \Bigg]^+ \Bigg\} \text{ [bps]}, \end{aligned} \tag{5.20}$$

respectively, where $\boldsymbol{\Lambda}_{\bar{P}_E} = \mathbf{diag}\{\mathbf{1}^T_{N\times 1},\ \mathbf{0}^T_{N\times 1}\}$, $\boldsymbol{\Lambda}_{\bar{W}_E} = \mathbf{diag}\{\mathbf{0}^T_{N\times 1},\ \mathbf{1}^T_{N\times 1}\}$, and $\mathbf{1}_{N\times 1}$ is the N-length column vector of ones. Finally, it is important to point out that $\boldsymbol{\Lambda}_{P_{\Pi}} \in \mathbb{R}^{2N\times 2N}$ in (5.19) and (5.20).

Lastly, the secrecy outage probability for w/o $\mathbf{H}_{AE,P}$ and w/o $\mathbf{H}_{AE,W}$ can be expressed as

$$\begin{aligned} P_{S,\bar{P}_E}(R) &= \mathbb{P}\left\{\frac{R_{S,\bar{P}_E}}{Bw} < R\right\} \\ &= \mathbb{P}\left\{\det\left(\frac{\mathbf{I}_{2N} + \boldsymbol{\Lambda}_{\gamma_{AB}}}{\mathbf{I}_{2N} + \boldsymbol{\Lambda}_{\bar{P}_E}\boldsymbol{\Lambda}_{\gamma_{AE}}}\right) < 2^{RN}\right\} \end{aligned} \tag{5.21}$$

and

$$\begin{aligned} P_{S,\bar{W}_E}(R) &= \mathbb{P}\left\{\frac{R_{S,\bar{W}_E}}{Bw} < R\right\} \\ &= \mathbb{P}\left\{\det\left(\frac{\mathbf{I}_{2N} + \boldsymbol{\Lambda}_{\gamma_{AB}}}{\mathbf{I}_{2N} + \boldsymbol{\Lambda}_{\bar{W}_E}\boldsymbol{\Lambda}_{\gamma_{AE}}}\right) < 2^{RN}\right\}, \end{aligned} \tag{5.22}$$

respectively.

5.3 NUMERICAL RESULTS

To carry out numerical analyses, the frequency bandwidth is $B_w = 500$ kHz and the carrier frequencies of 5.800 and 5.801 GHz are used by the 2×2 MIMO WLC wiretap channel model because these frequencies are unlicensed WLC frequencies. Regarding the hybrid PLC/WLC wiretap channel model, one takes into account the carrier frequency equal to 5.800 GHz for the LP-RF signal transmission and the low frequency band 0 – 500 kHz for the NB-PLC signal transmission. For the sake of simplicity, $N = 128$ since the squared magnitude of the CFR and the power spectral density (PSD) of the additive noise result in a coherence bandwidth of the nSNR wider than the frequency bandwidth of each sub-channel. Furthermore, aiming to yield fairness analyses, one assumes that $||\mathbf{h}_{AB,P}||^2 = ||\mathbf{h}_{AB,W}||^2 = ||\mathbf{h}_{AE,P}||^2 = ||\mathbf{h}_{AE,W}||^2$ and $P_{V_{AB,P}} = P_{V_{AB,W}} = P_{V_{AE,P}} = P_{V_{AE,W}}$, where $||\mathbf{h}_{l,q}||^2$ is the energy of the q^{th} channel at the l^{th} receiver and $P_{V_{l,q}} = \mathbf{tr}(\boldsymbol{\Lambda}_{P_{V_{l,q}}})$ is the additive noise energy associated with the q^{th} medium at the l^{th} receiver. In other words, this section performs numerical analyses that correctly analyze the benefits of using hybridism (i.e., diversity) regarding the PLS purpose. Furthermore, $P_T \in \{-20, -10, 0, 10, 20, 30\}$ dBm is taken into account.

The NB-PLC channels are in accord with the channel model proposed in [53] with the parameters listed in [71, Annex D] since they are generated by using a well-established NB-PLC channel model. This kind of NB-PLC channel is frequency selective because of impedances mismatching associated with the electric power grids. Moreover, one assumes that $\{h_{AB,P}[n]\}$ and $\{h_{AE,P}[n]\}$ are correlated to agree with Section 5.1. The additive noise is modeled as a zero mean and colored Gaussian random process. From [100], PSD of the colored Gaussian random process is given by $S_P(f) = \eta/2\exp(-\nu|f|)$, where $\nu,\ \eta \in \mathbb{R}_+$ are constants equal to 1.2×10^{-5} and 1.0×10^{-15}, respectively, and $f \in \mathbb{R}$ is the frequency in Hertz (Hz). As a consequence, $\boldsymbol{\Lambda}_{V_P} = \Delta f\mathbf{diag}\{S_P(0),\ S_P(\Delta f),\ \cdots, S_P([N-1]\Delta f)\}$, in which $\Delta f = B_w/N$.

For the LP-RF channels, the channel model for outdoor scenario without line-of-sight suggested in [54] is adopted. Also, a digital filter is applied to select the chosen frequency band. It is important to emphasize that for the adopted frequency bandwidth, the WLC channel is almost frequency flat. Note that $\{h_{AB,W}[n]\}$ and $\{h_{AE,W}[n]\}$ are independent random processes. Moreover, following [101], the additive noise in the wireless channel is zero mean circularly symmetric complex Gaussian random process with PSD $S_W(f) = -173.8 + NF$ dBm/Hz, in which the receiver noise figure NF is equal to 7 dB. As a result, $\mathbf{\Lambda}_{V_W} = \Delta f \mathbf{diag}\{S_W(0),\ S_W(\Delta f),\ \cdots, S_W([N-1]\Delta f)\}$.

The numerical results are obtained by using both OA and UA. $\bar{R}_S$ with OA is calculated using (5.12), whereas $\bar{R}_S$ with UA is achieved by distributing uniformly P_T over all sub-carriers in which $\dot{\gamma}_{AB}[k] > \dot{\gamma}_{AE}$ holds. In order to facilitate comparison, the values $\bar{R}_S$ of all simulated channel models are normalized by the ergodic achievable secrecy rate of the hybrid PLC/WLC wiretap channel model, which is obtained with the use of OA. The normalized ergodic achievable secrecy rate of the hybrid PLC/WLC wiretap channel model is expressed as

$$\rho_{\zeta}^{\delta} = \bar{R}_{S,\zeta}^{\delta} / \bar{R}_{S,\Pi}^{OA}, \tag{5.23}$$

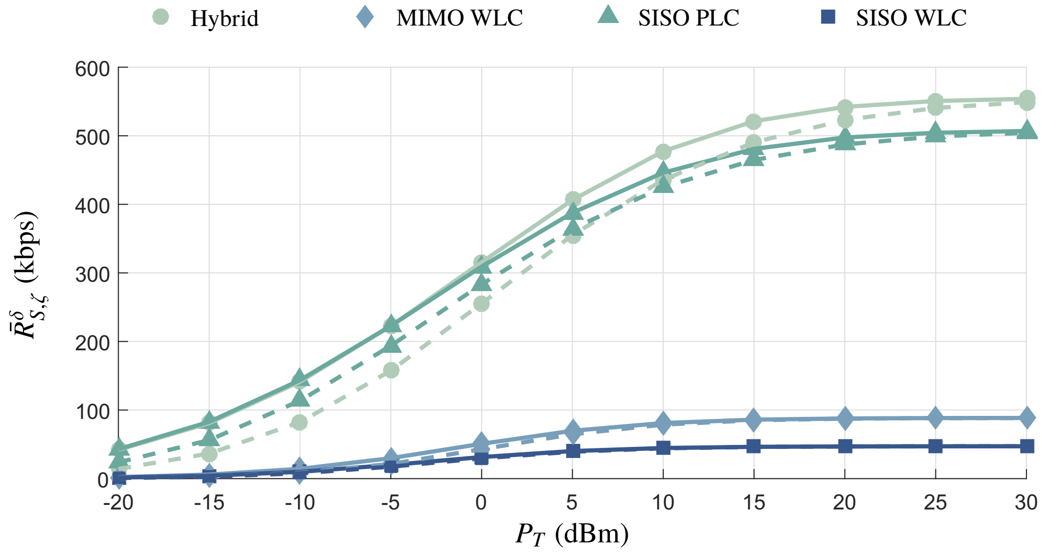
where $\delta \in \{OA, UA\}$ and ζ is according to Table 5. Note that $\bar{R}_{S,\Pi}^{OA} = \bar{R}_S$.

5.3.1 Analysis of Ergodic Achievable Secrecy Rate

Figures 35 and 36 compare the hybrid PLC/WLC, 2 × 2 MIMO WLC, SISO PLC, and SISO WLC wiretap channel models considering both OA and UA in terms of $\bar{R}_{S,\zeta}^{\delta}$. Figure 35 shows $\bar{R}_{S,\zeta}^{\delta} \times P_T$ curves, whereas Figure 36 depicts $\rho_{\zeta}^{\delta} \times P_T$ ones. In both figures, the hybrid PLC/WLC wiretap channel model outperforms all the other ones as $P_T \longrightarrow \infty$ regardless of the adopted power allocation technique. Conversely, when $P_T \leq -5$ dBm and $P_T \leq 8$ dBm the SISO PLC wiretap channel model presents higher $\bar{R}_{S,\zeta}^{\delta}$ than the hybrid PLC/WLC one for the use of OA and UA, respectively. Such a result is more expressive when UA is taken into account. Furthermore, note that the SISO PLC wiretap channel model also outperforms both 2 × 2 MIMO WLC and SISO WLC ones for all simulated values of P_T regardless of the power allocation technique. That result can be explained by the coherence bandwidth of the nSNR parameters of the SISO PLC wiretap channel model and 2×2 MIMO WLC and SISO WLC ones be quite different. In particular, the NB-PLC channel presents a highly frequency selectivity nSNR whereas the LP-RF channel shows an nSNR almost flat in the chosen frequency band and, as a consequence, the former channel is better than the latter one.

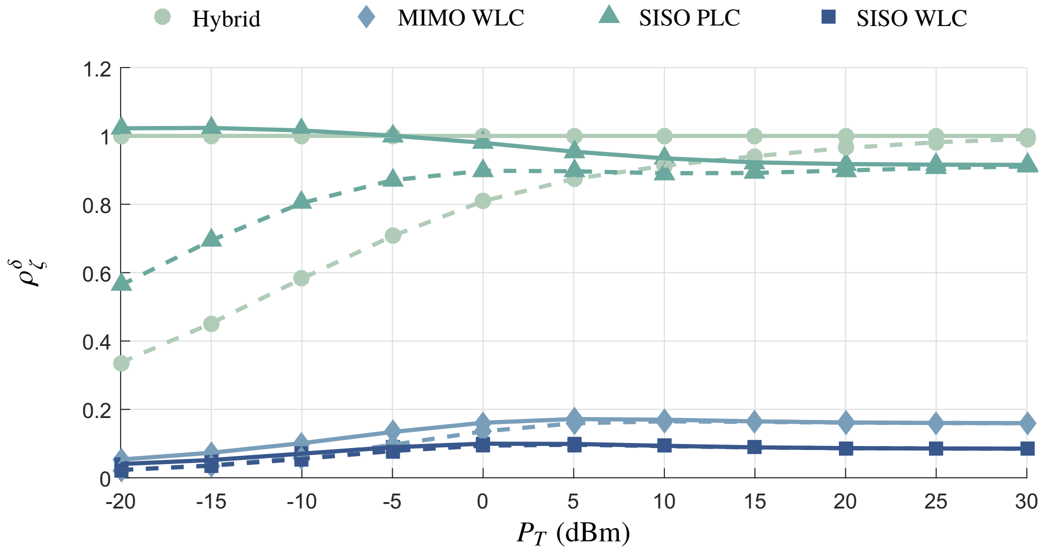
Besides, comparing both 2 × 2 MIMO WLC and SISO WLC wiretap channel models one can note that the former outperforms the latter as depicted in Figures 35 and 36. Also, the use of OA results in a remarkable difference, in terms of ergodic achievable secrecy rate, in comparison to UA when $P_T \longrightarrow 0$ and the hybrid PLC/WLC and SISO PLC wiretap channel models are considered. However, if $P_T \longrightarrow \infty$ then the curves obtained by using UA approximate the corresponding ones associated with OA. Regarding the 2 × 2 MIMO WLC and SISO WLC wiretap channel models, it is evident that the difference between OA and UA is not too much relevant for the chosen values of P_T. Overall, based on the fact that $P_T \geq 10$ dBm is applied in real data communication systems, it is clear that the hybrid PLC/WLC wiretap channel model can offer the highest ergodic achievable secrecy rate.

Figure 35 – Ergodic achievable secrecy rates under the adoption of OA (-) and UA (- -).



Source: Personal collection.

Figure 36 – ρ^{δ}_{ζ} under the adoption of OA (-) and UA (- -).

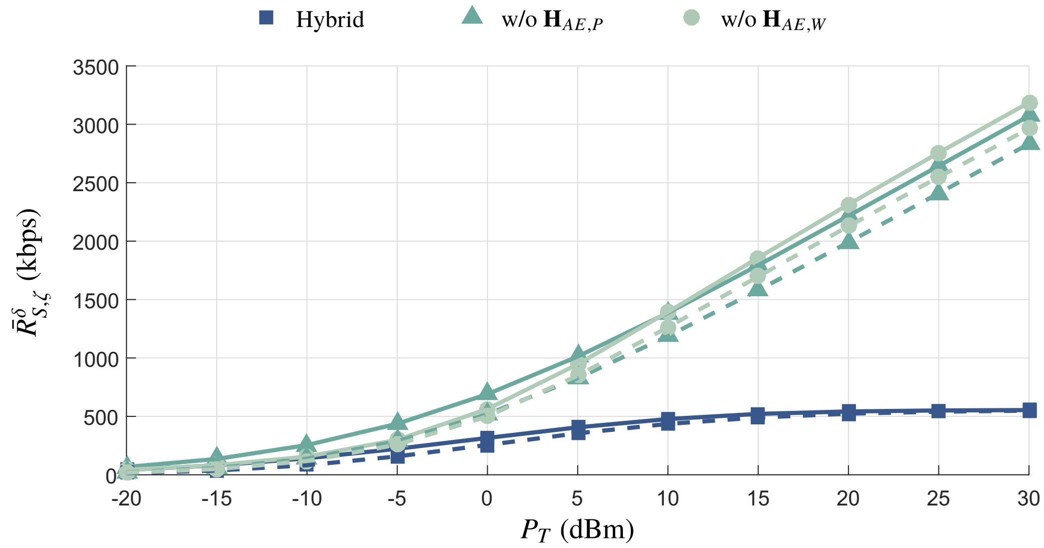


Source: Personal collection.

Figures 37 and 38 show the performance comparison among the hybrid PLC/WLC wiretap channel model and two of its incomplete versions, which are denoted by w/o $\mathbf{H}_{AE,P}$ and w/o $\mathbf{H}_{AE,W}$ incomplete versions, in terms of $\bar{R}^{\delta}_{S,\zeta}$ and adopting both OA and UA. It is interesting to see that Figure 37 shows $\bar{R}^{\delta}_{S,\zeta} \times P_T$ curves whereas Figure 38 highlights $\rho_{\zeta} \times P_T$ curves. According to both figures, w/o $\mathbf{H}_{AE,P}$ and w/o $\mathbf{H}_{AE,W}$ incomplete versions result in significant increase of $\bar{R}^{\delta}_{S,\zeta}$ when $P_T \to \infty$, regardless of the use of the power allocation technique. That interesting result means that the hybrid PLC/wireless channel model can considerably increase the ergodic achievable secrecy rate when Eve only uses one data communication interface. In other words, diversity not only increase PLS, but also can result in a astonishing secrecy rates improvement if Eve does not hear the transmitted signal in both media. For instance, when OA and $P_T = 30$ dBm are taken into account $\bar{R}^{\delta}_{S,\zeta}$ can reach approximately 3.17 and 3.07 Mbps for w/o $\mathbf{H}_{AE,W}$ and w/o $\mathbf{H}_{AE,P}$ incomplete versions, respectively, whereas the complete hybrid PLC/WLC wiretap channel model reaches 550 kbps.

Moreover, Figures 37 and 38 show that for $P_T \leq -10$ dBm the (complete) hybrid PLC/WLC wiretap channel model is better than both the w/o $\mathbf{H}_{AE,W}$ and w/o $\mathbf{H}_{AE,P}$ incomplete versions if UA is adopted. In addition, w/o $\mathbf{H}_{AE,W}$ outperforms w/o $\mathbf{H}_{AE,P}$ for $P_T \geq 10$ dBm and $P_T \geq 3$ dBm regarding the use of OA and UA, respectively. The higher difference between the curves when $P_T \leq 0$ dBm is because the coherence bandwidth of the nSNR parameters associated with both PLC and WLC channels are different. Actually, in terms of secrecy rate improvement, the frequency selectivity of nSNR related to the NB-PLC channel is more relevant when $P_T \to 0$. Also, if $P_T \to 0$, then the secrecy rates maximizations are more dependent on the type of the resource allocation technique since it can exploit the selectivity of nSNR. On the other hand, the frequency flatness of nSNR related to the LP-RF channel is more interesting for maximizing secrecy rates when $P_T \to \infty$.

Figure 37 – Ergodic achievable secrecy rates for OA (-) and UA (- -)

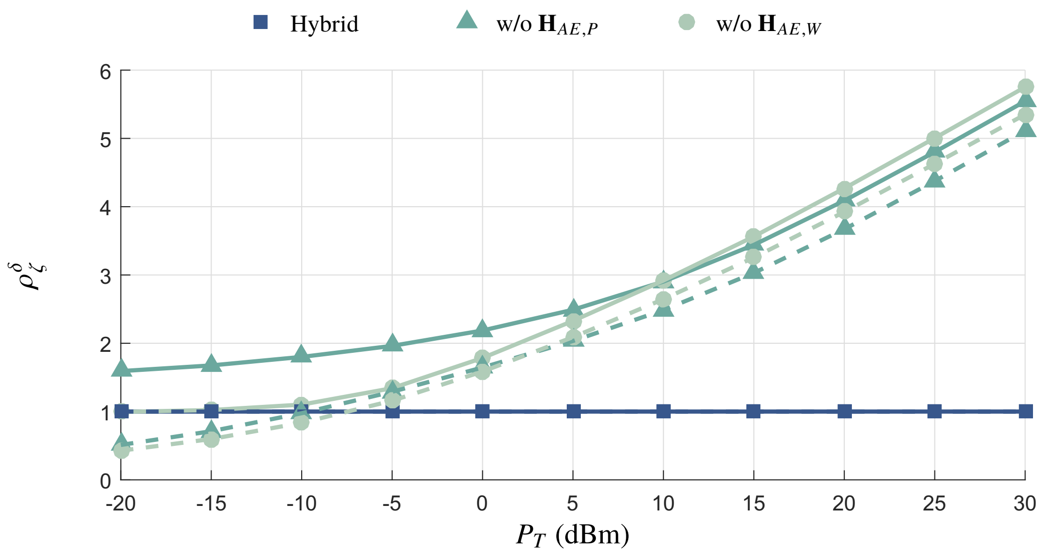


Source: Personal collection.

5.3.2 Analysis of Secrecy Outage Probability

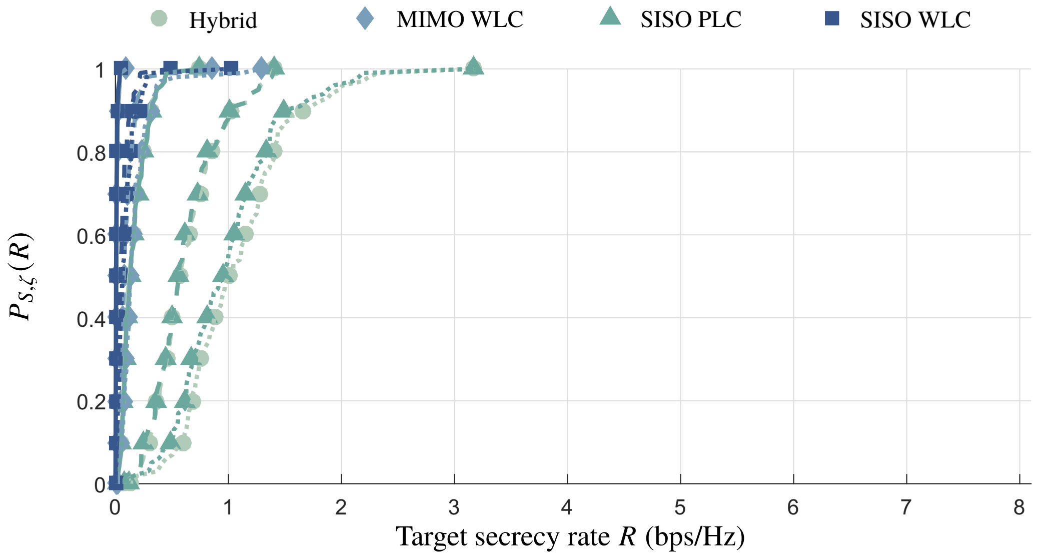
Figures 39 and 40 show comparisons among hybrid PLC/WLC, 2 × 2 MIMO WLC, SISO PLC, and SISO WLC wiretap channel models in terms of $P_{S,\zeta}$ considering OA and UA, respectively. To do so, $P_T \in \{-15, 0, 20\}$ dBm is taken into account. Observing both

Figure 38 – ρ_ζ^δ under the adoption of OA (-) and UA (- -)



Source: Personal collection.

Figure 39 – $P_{S,\zeta}(R)$ under the adoption of OA for P_T equal to -15 (-), 0 (- -), and 20 dBm (· ·)

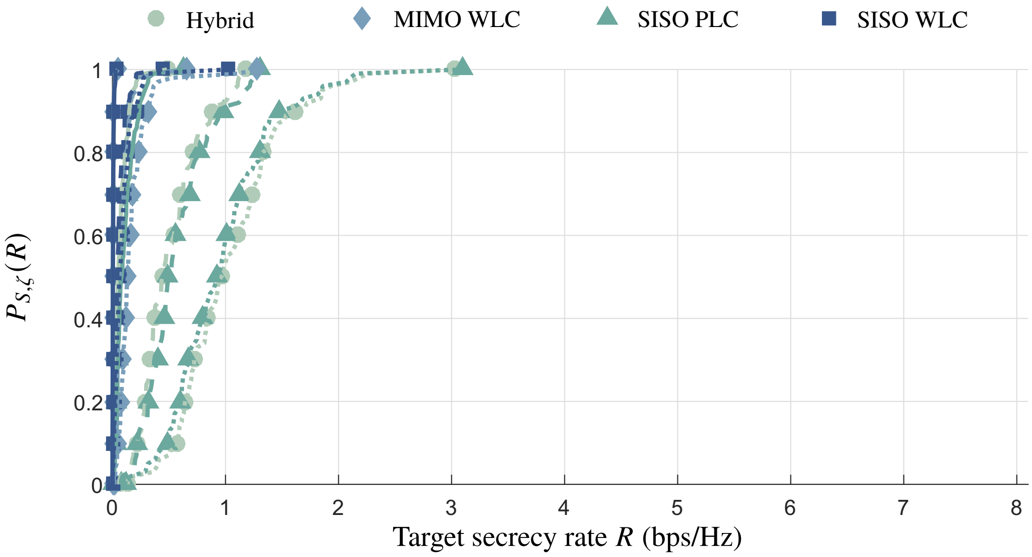


Source: Personal collection.

figures, a minimal difference between OA and UA curves can be observed. Also, secrecy outage probability results seem to corroborate the results shown in Figures 35 and 36. For instance, when $P_T = 20$ dBm and $P_{S,\zeta} = 0.2$, Figure 39 shows target secrecy rates, R, equal to 0.68, 0.61, 0.08, and 0.03 bps/Hz for hybrid PLC/WLC, SISO PLC, 2×2 MIMO WLC, and SISO WLC wiretap channel models, respectively. Similarly, Figure 40 shows R equal to 0.65, 0.60, 0.08, and 0.03 bps/Hz for those channel models.

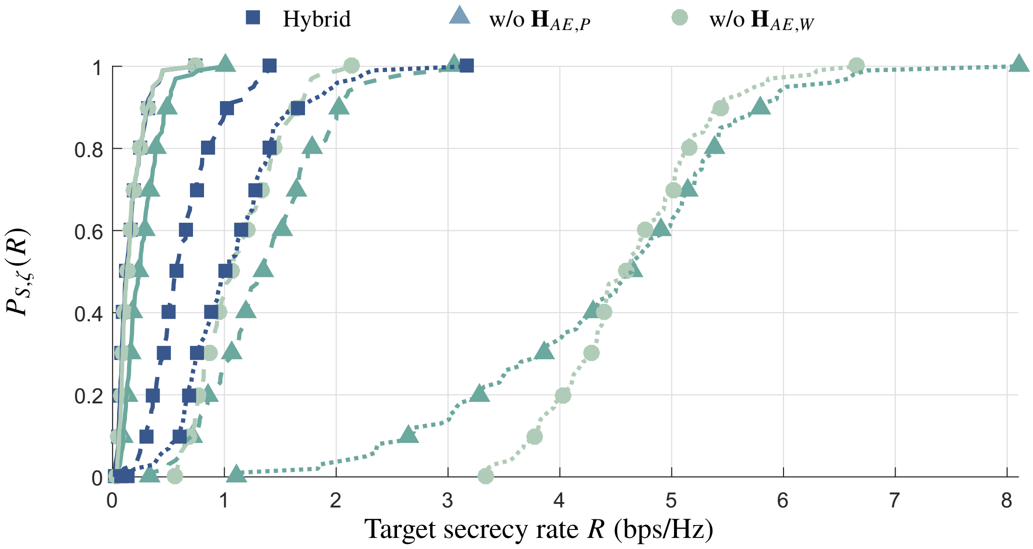
Figures 41 and 42 show the performance comparison among the hybrid PLC/WLC, w/o $\mathbf{H}_{AE,P}$, and w/o $\mathbf{H}_{AE,W}$ wiretap channel models in terms of $P_{S,\zeta}$ adopting both OA and UA, respectively. In this way, $P_T \in \{-15, 0, 20\}$ dBm is chosen. Note that, when $P_T = 20$ dBm and

Figure 40 – $P_{S,\zeta}(R)$ under the adoption of UA for P_T equal to -15 (-), 0 (- -), and 20 dBm (· ·)



Source: Personal collection.

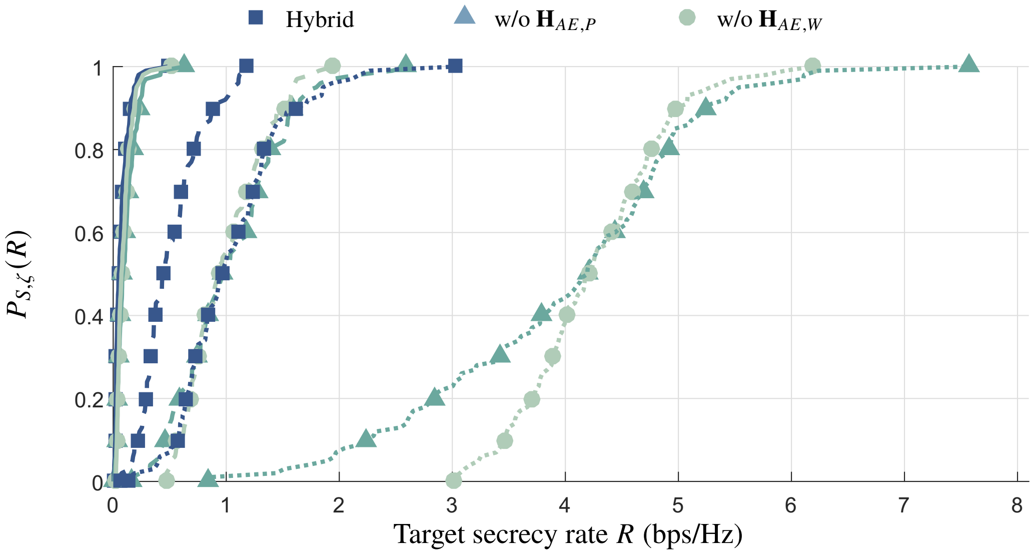
Figure 41 – $P_{S,\zeta}(R)$ under the adoption of OA for P_T equal to -15 (-), 0 (- -), and 20 dBm (· ·)



Source: Personal collection.

$P_{S,\zeta} = 0.2$, Figure 41 shows R equal to 4.03, 3.28, and 0.68 bps/Hz for the w/o $\mathbf{H}_{AE,W}$, w/o $\mathbf{H}_{AE,P}$, and hybrid PLC/WLC wiretap channel models, respectively. On the other hand, such wiretap channel models present values of R equal to 5.02, 5.15, and 1.28 bps/Hz, respectively, when $P_{S,\zeta} = 0.7$. Similarly, Figure 42 shows R equal to 3.70, 2.84, and 0.64 bps/Hz for the w/o $\mathbf{H}_{AE,W}$, w/o $\mathbf{H}_{AE,P}$, and hybrid PLC/WLC wiretap channel models, respectively, when $P_{S,\zeta} = 0.2$. Finally, if $P_{S,\zeta} = 0.7$ is taken into account, those channel models achieve values of R equal to 4.59, 4.69, 1.23 bps/Hz.

Figure 42 – $P_{S,\zeta}(R)$ under the adoption of UA for P_T equal to -15 (-), 0 (- -), and 20 dBm (· ·)



Source: Personal collection.

5.3.3 General Comments

Overall, the attained results show, under the formulated problem perspective and given assumptions, the NB-PLC channel is better than the LP-RF one under the PLS point of view. Besides, the hybrid PLC/WLC wiretap channel model shows higher $\bar{R}^{\delta}_{S,\zeta}$ than 2×2 MIMO WLC one. Regarding the power allocation, one pointed out that UA yields a behavior similar to OA, if $P_T \to \infty$. On the other hand, if $P_T \to 0$, then OA remarkably outperforms UA. Also, numerical results show that it is possible to notably increase $\bar{R}^{\delta}_{S,\zeta}$ when Eve makes use of only NB-PLC or LP-RF interface. In other words, secrecy rates associated with the hybrid PLC/WLC wiretap channel model can be significantly improved if Eve is incomplete (i.e., Eve is a SISO PLC or a SISO WLC device).

6 CONCLUSIONS

This Doctoral thesis has investigated the security at the physical layer level for in-home broadband PLC and low-bit-rate hybrid PLC/WLC systems. In this regard, a comprehensive discussion on PLS in these systems has been provided. Also, numerical results in order to quantify the PLS and then to show the situations where data communication security can be compromised have been addressed.

Chapter 2 has discussed timely and relevant issues regarding the security at the physical layer level in PLC and hybrid PLC/WLC systems. The barriers imposed by the HV, MV, and LV electric power grids, in which the PLC system operates, to an eavesdropper that wishes to wired and wirelessly overhear the PLC signal have been addressed. Also, the types of eavesdroppers that can threaten the PLS of both PLC and hybrid PLC/WLC systems as well as the conditions that these eavesdroppers can access private information in these data communication systems have been covered. In summary, this chapter has addressed important aspects related to PLS in PLC and hybrid PLC/WLC systems in order to highlight the opportunities and challenges necessary for introducing security at the physical layer level in a novel generation of PLC standards and technologies.

Chapter 3 has quantitatively investigated with real data how secure a broadband PLC system can be when a passive WLC device, operating in the vicinity of power cables, overhears private messages exchanged between two PLC devices. In this sense, the introduction of the hybrid wiretap channel to model this scenario has allowed the deduction of mathematical formulations of the secrecy outage probability and effective secrecy throughput as well as the PLS performance evaluation of PLC systems regarding those metrics and the wiretap code rates. The numerical results have shown how vulnerable a broadband in-home PLC system can be when unshielded power cables constitute electric power grids and a malicious WLC device is located in the vicinity of them. In the worst scenario, where Bob is around 6 meters away from Alice whereas Eve is less than 2 meters away from Alice, high values of secrecy outage probability arise for all analyzed values of target secrecy rate and total transmission power. Also, the values found for effective secrecy throughput are close to zero even when Alice completely knows Bob's CSI. Overall, the discussed results have reinforced the importance and necessity of introducing novelties in the design of PLC devices or the use of shielded power cables in electrical power grids when the discussion related to the physical layer of PLC systems involves security issues. Also, the wiretap code rates have been provided to be applied in in-home and broadband PLC systems in order to deal with malicious WLC devices located at the vicinity of the electric power circuit in which the PLC system operates. These wiretap code rates may assist the design of a novel generation of PLC systems with security functionalities at the physical layer level.

Chapter 4 has investigated the PLS of an in-home broadband PLC system when a malicious PLC device, which is connected to the same electric power grid as the PLC system, tries to eavesdrop private messages exchanged between a transmitter and an intended receiver.

To do so, a data set obtained from a measurement campaign carried out in several Brazilian in-home facilities has been taken into account. Also, assuming the realistic situation in which the eavesdropper is passive, the ergodic achievable data rate, secrecy outage probability, effective secrecy throughput, and wiretap code rates have been analyzed by considering four sets of the transmitter, receiver, and eavesdropper positions and the frequency bands $1.7-30$ MHz, $1.7-50$ MHz, and $1.7-86$ MHz. Numerical results have shown the vulnerability of an in-home broadband PLC system when Eve is close to Alice or in the middle between Alice and Bob. Also, the four relative positions of Eve, between Alice and Bob, show high values of secrecy outage probability regardless of the adopted target secrecy rate, the total transmission power, and the chosen frequency band. Besides that, if Eve is close to Bob, then high values of the secrecy outage probability are found for target secrecy rates higher than 1 bps/Hz regardless of the frequency band and the total transmission power. On the other hand, values of secrecy outage probability around zero and 0.2 can be found in the frequency bands $1.7-30$ MHz and $1.7-50$ MHz, respectively, when practical values of the total transmission power (i.e., $[0, 30]$ dBm) and the target secrecy rate equal to 0.05 bps/Hz are adopted. Finally, taken into account the effective secrecy throughput, the attained results have shown that even in cases where Eve is close to Alice or in the middle between Alice and Bob, PLS is possible if the provided wiretap code rates are used. Also, notice that the difference in security based on the chosen frequency bands was not relevant in terms of secrecy outage probability and effective secrecy throughput. In summary, this chapter has yielded detailed information about security issues at the physical layer level and has brought attention to the importance of the appropriate design of PLC devices for improving data communication security in PLC systems when the eavesdropper is a PLC device.

Chapter 5 has analyzed the ergodic achievable secrecy rates and secrecy outage probabilities of the hybrid PLC/WLC wiretap channel model and of its incomplete versions. To do so, OA and UA techniques have been applied. Moreover, by considering low-bit-rate applications one has compared their performances against the performance of 2×2 MIMO WLC, SISO PLC, and SISO WLC wiretap channel models. Based on numerical results, one can state that the hybrid PLC/WLC wiretap channel model provides higher ergodic achievable secrecy rate than the 2×2 MIMO WLC, SISO PLC, and SISO WLC wiretap channel models. Furthermore, the attained results have shown that the SISO PLC wiretap channel model overcomes the 2×2 MIMO and SISO WLC ones in terms of secrecy rate. Regarding the power allocation, UA has yielded ergodic achievable secrecy rates close to OA when $P_T \rightarrow \infty$. On the other hand, if $P_T \rightarrow 0$, then OA is remarkably better than UA. Finally, numerical results have shown that the hybrid PLC/WLC wiretap channel model can notably increase the ergodic achievable secrecy rate if the eavesdropper uses only one data communication interface (NB-PLC or LP-RF). That result shows the usefulness and effectiveness of the hybridism concept within the data communication system for increasing secrecy rate at the physical layer level when low-bit-rate applications are considered.

In order to continue the investigations presented in this Doctoral thesis, the following research issues deserve attention:

- To analyze the effective secrecy throughput as well as the respective wiretap code rates for the low-bit-rate hybrid PLC/WLC wiretap channel model.
- To propose schemes for increasing PLS for low-bit-rate hybrid PLC/WLC systems making use of the existing diversity between LP-RF and NB-PLC channels.
- To investigate the PLS for the hybrid wiretap channel model considering the frequency bands $1.7 - 30$ MHz and $1.7 - 50$ MHz and for PLC wiretap channel model considering the frequency band $3 - 500$ kHz.
- To provide novel techniques to improve PLS in PLC systems under the presence of passive PLC and/or WLC eavesdroppers.
- To investigate the PLC/WLC eavesdropper in PLC systems.

REFERENCES

[1] J. A. Stankovic, “Research directions for the Internet of Things,” *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, Feb. 2014.

[2] Y. Huang, Y. Li, H. Ren, J. Lu, and W. Zhang, “Multi-panel MIMO in 5G,” *IEEE Communications Magazine*, vol. 56, no. 3, pp. 56–61, Mar. 2018.

[3] M. S. P. Facina, H. A. Latchman, H. V. Poor, and M. V. Ribeiro, “Cooperative in-home power line communication: Analyses based on a measurement campaign,” *IEEE Transactions on Communications*, vol. 64, no. 2, pp. 778–789, Feb. 2016.

[4] J. Ploennings, A. Ba, and M. Barry, “Materializing the promises of cognitive IoT: How cognitive buildings are shaping the way,” *IEEE Internet of Things Journal*, Sep. 2017, accepted for publication.

[5] L. Xu, R. Collier, and G. M. P. O’Hare, “A survey of clustering techniques in WSNs and consideration of the challenges of applying such to 5G IoT scenarios,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1229–4662, Jul. 2017.

[6] Z. Yang, W. Xu, Y. Pan, C. Pan, and M. Chen, “Energy efficient resource allocation in machine-to-machine communications with multiple access and energy harvesting for IoT,” *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 229–245, Feb. 2018.

[7] T. R. Oliveira, F. J. A. Andrade, A. M. Picorone, H. A. Latchman, S. L. Netto, and M. V. Ribeiro, “Characterization of hybrid communication channel in indoor scenario,” *Journal of Communication and Information Systems*, vol. 31, no. 1, pp. 224–235, Sep. 2016.

[8] T. R. Oliveira, A. A. M. Picorone, S. L. Netto, and M. V. Ribeiro, “Characterization of Brazilian in-home power line channels for data communication,” *Electric Power Systems Research*, vol. 150, pp. 188–197, 2017.

[9] M. V. Ribeiro, G. R. Colen, F. V. P. Campos, Z. Quan, and H. V. Poor, “Clustered-OFDM for power line communication: When can it be beneficial?” *IET Communications*, vol. 8, no. 13, pp. 2336–2347, Sept. 2014.

[10] L. G. S. Costa, A. C. M. Queiroz, B. Adebisi, V. L. R. Costa, and M. V. Ribeiro, “Coupling for power line communications: A survey,” *Journal of Communication and Information Systems*, vol. 32, no. 1, pp. 8–22, 2017.

[11] M. Mohammadi, L. Lampe, M. Lok, S. Mirabbasi, M. Mirvakili, R. Rosales, and P. Van Veen, “Measurement study and transmission for in-vehicle power line communication,” in *Proc. IEEE International Symposium on Power Line Communications and Its Applications*, Mar. 2009, pp. 73–78.

[12] S. Barmada, L. Bellanti, M. Raugi, and M. Tucci, “Analysis of powerline communication channels in ships,” *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3161–3170, Sep. 2010.

[13] S. Barmada, A. Gaggeli, A. Musolino, R. Rizzo, M. Raugi, and M. Tucci, “Design of PLC system onboard trains: selection and analysis of the PLC channel,” in *Proc. IEEE International Symposium on Power Line Communications and Its Applications*, Apr. 2008, pp. 13–17.

[14] F. Grassi, S. A. Pignari, and J. Wolf, “Channel characterization and EMC assessment of a PLC system of spacecraft DC differential power buses,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 53, no. 3, pp. 664–675, Aug. 2011.

[15] A. Camponogara, T. R. Oliveira, R. Machado, and M. V. Finamore, W. A. Ribeiro, “Measurement and characterization of power lines of aircraft flight test instrumentation,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 3, pp. 1550–1560, Apr. 2019.

[16] J. A. Cortés, F. J. Canete, L. Díez, and J. T. Entrambasaguas, “Characterization of the cyclic short-time variation of indoor power-line channels response,” in *Proc. IEEE International Symposium on Power Line Communications and Its Applications*, Apr. 2005, pp. 326–330.

[17] J. A. Cortés, F. J. Canete, L. Díez, and J. L. G. Moreno, “On the statistical properties of indoor power line channels: Measurements and models,” in *Proc. IEEE International Symposium on Power Line Communications and Its Applications*, Apr. 2011, pp. 271–276.

[18] A. Cataliotti, V. Cosentino, and G. Di Cara, D. Tinè, “Measurement issues for the characterization of medium voltage grids communications,” *IEEE Transactions on Instrumentation and Measurement*, vol. 62, no. 8, pp. 2185–2196, Jun. 2013.

[19] G. Huang, D. Akopian, and C. L. P. Chen, “Measurement and characterization of channel delays for broadband power line communications,” *IEEE Transactions on Instrumentation and Measurement*, vol. 63, no. 11, pp. 2583–2590, May 2014.

[20] A. A. M. Picorone, R. Sampaio-Neto, and M. V. Ribeiro, “Coherence time and sparsity of brazilian outdoor PLC channels: a preliminary analysis,” in *Proc. IEEE International Symposium on Power Line Communications and Its Applications*, Mar. 2014, pp. 1–5.

[21] G. R. Colen, C. A. G. Marques, T. R. Oliveira, F. P. V. de Campos, and M. V. Ribeiro, “Measurement setup for characterizing low-voltage and outdoor electric distribution grids for PLC systems,” in *Proc. Conference on Innovative Smart Grid Technologies Latin America*, Apr. 2013, pp. 1–5.

[22] P. A. Janse van Rensburg and H. C. Ferreira, “Coupler winding ratio selection for effective narrowband power-line communication,” *IEEE Transactions on Power Delivery*, vol. 23, no. 1, pp. 140–149, 2008.

[23] L. de M. B. A. Dib, V. Fernandes, M. de L. Filomeno, and M. V. Ribeiro, “Hybrid PLC/wireless communication for smart grids and Internet of Things applications,” *IEEE Internet Things Journal*, vol. 5, no. 2, pp. 655–667, Apr. 2018.

[24] M. Kuhn and A. Wittneben, “PLC enhanced wireless access networks: a link level capacity consideration,” in *IEEE Vehicular Technology Conference*, May 2002, pp. 125–129.

[25] M. Kuhn, S. Berger, I. Hammerström, and A. Wittneben, “Power line enhanced cooperative wireless communications,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 7, pp. 1401–1410, Jul. 2006.

[26] S. Güzelgöz, H. B. Çelebi, and H. Arslan, “Analysis of a multi-channel receiver: Wireless and PLC reception,” in *Signal Processing Conference*, Aug. 2010, pp. 1106–1110.

[27] S. W. Lai and G. G. Messier, “Using the wireless and PLC channels for diversity,” *IEEE Transactions on Communications*, vol. 60, no. 12, pp. 3865–3875, Dec. 2012.

[28] M. Sayed, T. A. Tsiftsis, and N. Al-Dhahir, “On the diversity of hybrid narrowband-PLC/wireless communications for smart grids,” *IEEE Transactions on Wireless Communications*, vol. 16, no. 7, pp. 4344–4360, Apr. 2017.

[29] Y. Qian, J. Yan, H. Guan, J. Li, X. Zhou, Shengjie, and D. N. K. Jayakody, “Design of hybrid wireless and power line sensor networks with dual-interface relay in IoT,” *IEEE Internet of Things Journal*, Jul. 2017, accepted for publication.

[30] V. Fernandes, M. L. Filomeno, W. A. Finamore, and M. V. Ribeiro, “An investigation on narrow band PLC-wireless parallel channel capacity,” in *Brazilian Symposium on Telecommunications*, Sep. 2016, pp. 834–838.

[31] V. Fernandes, W. A. Finamore, H. V. Poor, and M. V. Ribeiro, “The low-bit-rate hybrid PLC-wireless single relay channel,” *IEEE Systems Journal*, vol. 13, no. 1, pp. 98–109, Mar. 2019.

[32] V. Fernandes, H. V. Poor, and M. V. Ribeiro, “Analyses of the incomplete low-bit-rate hybrid PLC-wireless single-relay channel,” *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 917–929, Apr. 2018.

[33] V. L. R. da Costa, V. Fernandes, and M. V. Ribeiro, “Narrowband hybrid PLC/wireless: Transceiver prototype, hardware resource usage and energy consumption,” *Ad Hoc Networks*, vol. 94, pp. 1–11, Jun. 2019.

[34] T. R. Oliveira, A. A. Picorone, C. B. Zeller, S. L. Netto, and M. V. Ribeiro, “On the statistical characterization of hybrid PLC-wireless channels,” *Electric Power Systems Research*, vol. 163, pp. 329–337, 2018.

[35] H. V. Poor and R. F. Schaefer, “Wireless physical layer security,” *Proceedings of the National Academy of Sciences of the USA*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[36] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[37] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wiretap channel,” *IEEE Transactions on Information Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[38] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[39] P. Parada and R. Blahut, “Secrecy capacity of SIMO and slow fading channels,” in *Proc. International Symposium on Information Theory*, Sep. 2005, pp. 2152–2155.

[40] Y. Liang and H. V. Poor, “Secure communication over fading channels,” in *Proc. 44th Annual Allerton Conference on Communication, Control and Computing*, Sep. 2006, pp. 817–823.

[41] Y. Liang, H. V. Poor, and S. Shamai, “Secure communication over fading channels,” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[42] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” in *Proc. IEEE International Symposium on Information Theory*, Aug. 2008, pp. 524–528.

[43] S. Shafiee, N. Liu, and S. Ulukus, “Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel,” *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4033–4039, Aug. 2009.

[44] A. Mukherjee and A. Swindlehurst, “Robust beamforming for security in MIMO wiretap channels with imperfect CSI,” *IEEE Transactions on Information Theory*, vol. 59, no. 1, pp. 351–361, Sep. 2011.

[45] N. Shlezinger, D. Zhavi, Y. Murin, and R. Dabora, “The secrecy capacity of Gaussian MIMO channels with finite memory,” *IEEE Transactions on Information Theory*, vol. 63, no. 3, pp. 1874–1897, Mar. 2017.

[46] A. Pittolo and A. M. Tonello, “Physical layer security in plc networks: Achievable secrecy rate and channel effects,” in *Proc. IEEE International Symposium on Power Line Communications and Its Applications*, Mar. 2013, pp. 273–278.

[47] Y. Zhuang and L. Lampe, “Physical layer security in MIMO power line communication networks,” in *Proc. IEEE International Symposium on Power Line Communications and Its Applications*, Mar. 2014, pp. 272–277.

[48] A. Pittolo and A. M. Tonello, “Physical layer security in power line communication networks: An emerging scenario, other than wireless,” *IET Communications*, vol. 8, no. 8, pp. 1239–1247, 2014.

[49] A. Salem, K. M. Rabie, K. A. Hamdi, E. Alsusa, and A. M. Tonello, “Physical layer security of cooperative relaying power-line communication systems,” in *Proc. IEEE International Symposium on Power Line Communications and Its Applications*, Mar. 2016, pp. 185–189.

[50] A. Salem, K. A. Hamdi, and E. Alsusa, “Physical layer security over correlated log-normal cooperative power line communication channels,” *IEEE Access*, vol. 5, pp. 13 909–13 921, Jan. 2017.

[51] A. E. Shafie, M. F. Marzban, R. C. Chabaan, and N. Al-Dhahir, “An artificial-noise-aided secure scheme for hybrid parallel PLC/wireless OFDM systems,” in *Proc. IEEE International Conference on Communications*, May 2018, pp. 1–6.

[52] T. R. Oliveira, “The characterization of hybrid PLC-wireless and PLC channels in the frequency band between 1.7 and 100 MHz for data communication,” Ph.D. dissertation, Universidade Federal de Juiz de Fora, Juiz de Fora, MG, 2015.

[53] M. Zimmerman and K. Dostert, “A multipath model for the power line channel,” *IEEE Transactions on Communications*, vol. 50, no. 4, pp. 553–559, Apr. 2002.

[54] A. F. Molisch *et al.*, “IEEE 802.15.4a channel model - final report,” IEEE 802.15 WPAM Low Rate Alternative PHY Task Group, Tech. Rep., 2004.

[55] P. A. Brown, “Power line communications - Past present and future,” in *Proc. IEEE International Symposium on Power Line Communications and Its Applications*, Mar. 1999, pp. 1–8.

[56] J. Routin and C. E. L. Brown, “Improvements in and relating to electricity meters,” British Patent GB 724 833, Oct., 1898.

[57] C. H. Thordarson, “Electric central station recoding mechanism for meters,” U.S. Patent US 784 712, Mar., 1905.

[58] M. V. Ribeiro, “Power line communications: A promising communication system’s paradigm for last miles and last meters applications,” in *Telecommunications: Advances and Trends in Transmission, Networking and Applications*, C. C. Cavalcante, R. F. Colares, and P. C. Barbosa, Eds. Fortaleza, CE: Fundação Edson Queiroz, 2006, ch. 6, pp. 133–152.

[59] N. Marumi, “Simultaneous transmission and reception in radio telephony,” *Proceedings of the Institute of Radio Engineers*, vol. 8, no. 3, pp. 199–219, Jun. 1920.

[60] M. Schwartz, “Carrier-wave telephony over power lines: Early history,” *IEEE Communications Magazine*, vol. 47, no. 1, pp. 14–18, Jan. 2009.

[61] “Interplant telephonic communications established over high-tension lines,” *Electric World*, vol. 76, p. 141, Jul. 1920.

[62] L. Lampe, A. M. Tonello, and T. G. Swart, *Power line communications: Principles, standards and applications from multimedia to smart grid*, 2nd ed. Hoboken, NJ: John Wiley & Sons, 2016.

[63] A. Schwager, “Powerline communications: Significant technologies to become ready for integration,” Ph.D. dissertation, University of Duisburg-Essen, Germany, 2010.

[64] S. Galli, A. Scaglione, and Z. Wang, “For the grid and through the grid: The role of power line communications in the smart grid,” *Proceedings of IEEE*, vol. 99, no. 6, pp. 998–1027, Jun. 2011.

[65] B. Shneier, *Applied Cryptography*. John Wiley & Sons, 1996.

[66] R. M. de Oliveira, A. B. Vieira, H. A. Latchman, and M. V. Ribeiro, “Medium access control protocols for power line communication: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 920–939, Firstquarter. 2019.

[67] “ESCO Technologies.” [Online]. Available: https://www.escotechnologies.com/

[68] “Aclara Technologies.” [Online]. Available: https://www.aclara.com/

[69] *Technology Whitepaper: PHY, MAC and Convergence layers*, PRIME Std., Jul. 2008. [Online]. Available: https://www.prime-alliance.org/wp-content/uploads/2013/03/MAC_Spec_white_paper_1_0_080721.pdf

[70] *Narrowband Orthogonal Frequency Division Multiplexing Power Line Communication Transceivers for G3-PLC Networks*, ITU-T Std. G.9903, Aug. 2017. [Online]. Available: https://www.itu.int/rec/T-REC-G.9903-201708-I/en

[71] *IEEE Standard for Low Frequency (less than 500 kHz) Narrow Band Power Line Communication for Smart Grid Application*, IEEE Std. 1901.2, Dec. 2013. [Online]. Available: https://standards.ieee.org/standard/1901_2-2013.html

[72] *Narrowband Orthogonal Frequency Division Multiplexing Power Line Communication Transceivers for ITU-T G.hnem Networks*, ITU-T Std. G.9902, Oct. 2012. [Online]. Available: https://www.itu.int/rec/T-REC-G.9903-201708-I/en

[73] *IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications*, IEEE Std. 1901a, Mar. 2019. [Online]. Available: https://standards.ieee.org/standard/1901a-2019.html

[74] *HomePlug 1.0 Technology White Paper*, HomePlug Std. 1.0, Oct. 2015. [Online]. Available: http://www.solwise.co.uk/downloads/files/hp_1.0_technicalwhitepaper_final.pdf

[75] *HomePlug AV White Paper*, HomePlug Std. AV, 2005. [Online]. Available: https://www.solwise.co.uk/downloads/files/hpav-white-paper_050818.pdf

[76] *HomePlug AV2 Technology*, HomePlug Std. AV2, 2012. [Online]. Available: https://cdn.shopify.com/s/files/1/0101/1335/1737/files/HomePlug_AV2_Whitepaper.pdf?507196998416574505

[77] *HomePlug Green PHY*, HomePlug Std. GP, 2012. [Online]. Available: https://www.codico.com/fxdata/codico/prod/media/Datenblaetter/AKT/HomePlug_Green_PHY_whitepaper_100614%5B1%5D.pdf

[78] *IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications*, IEEE Std. 1901, Sep. 2010. [Online]. Available: http://standards.ieee.org/findstds/standard/1901-2010.html

[79] *IEEE Standard for Medium Frequency (less than 12 MHz) Power Line Communication for Smart Grid Applications*, IEEE Std. 1901.1, May 2018. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8360785

[80] *IEEE 1901 HD-PLC (High Definition Power Line Communication)*, HD-PLC Std., Feb. 2018. [Online]. Available: https://www.hd-plc.org

[81] *Unified High-Speed Wireline-Based Home Networking Transceivers: System Architecture and Physical Layer Specification*, ITU-T Std. G.9960, Nov. 2018. [Online]. Available: https://www.itu.int/rec/T-REC-G.9960

[82] *Unified High-Speed Wireline-Based Home Networking Transceivers: Multiple Input/Multiple Output Specification*, ITU-T Std. G.9963, Nov. 2018. [Online]. Available: https://www.itu.int/rec/T-REC-G.9963/en

[83] “Texas Instruments.” [Online]. Available: http://www.ti.com/

[84] “Atmel.” [Online]. Available: http://www.atmel.com/

[85] “Maxim Integrated.” [Online]. Available: http://www.maximintegrated.com/

[86] “Qualcomm.” [Online]. Available: http://www.qualcomm.com/

[87] “MegaChips.” [Online]. Available: http://www.megachips.com/

[88] “Panasonic.” [Online]. Available: https://www.panasonic.com/global/corporate/technology-design/technology/hd-plc.html

[89] "Marvell." [Online]. Available: https://www.marvell.com/

[90] M. Casal, "Linhas de transmissão de energia elétrica," *Agência Brasil*, Aug. 2019. [Online]. Available: http://agenciabrasil.ebc.com.br/economia/noticia/2018-12/aneel-leiloa-16-lotes-de-linhas-de-transmissao-e-subestacoes

[91] "Ppc." [Online]. Available: https://www.ppc-ag.com/wp-content/uploads//2019/03/PPC-Flyer-Medium-Voltage-Solutions-16-2100-1E.pdf

[92] C. Choudhuri and U. Mitra, "Capacity bound for relay channels with intersymbol interference and colored Gaussian noise," *IEEE Transactions on Information Theory*, vol. 60, no. 9, pp. 5639–5652, Sep. 2014.

[93] A. J. Goldsmith and M. Effros, "The capacity region of broadcast channels with intersymbol interference and colored noise," *IEEE Transactions on Information Theory*, vol. 47, no. 1, pp. 219–240, Sep. 2001.

[94] R. S. Kshetrimayum, *Fundamentals of MIMO Wireless Communications*. New York: Cambridge University Press, 2017.

[95] A. Jorswieck, Eduard, A. Wolf, and S. Gerbracht, "Secrecy on the physical layer in wireless networks, trends in telecommunications technologies," pp. 413–435, 2010. [Online]. Available: http://www.intechopen.com/books/trends-in-telecommunications-technologies/secrecy-on-the-physical-layer-in-wireless-networks.

[96] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of code rates in SISOME wiretap channels," *IEEE Internet on Wireless Communications*, vol. 14, no. 11, pp. 6377–6388, Nov. 2015.

[97] J. M. Cioffi, *Chapter 4: Multi-channel modulation*, acessed in Jul. 2018. [Online]. Available: http://web.stanford.edu/group/cioffi/book/chap4.pdf

[98] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE International Symposium on Information Theory*, Jul 2006, pp. 356–360.

[99] A. Jorswieck, Eduard and A. Wolf, "Resource allocation for the wire-tap multi-carrier broadcast channel," in *International Conference on Telecommunications*, Jun. 2008, pp. 1–6.

[100] M. Katayama, T. Yamazato, and H. Okada, "A mathematical model of noise in narrowband power line communication systems," *IEEE Journal on Selected Areas in Communication*, vol. 24, no. 7, pp. 1267–1276, Jul. 2006.

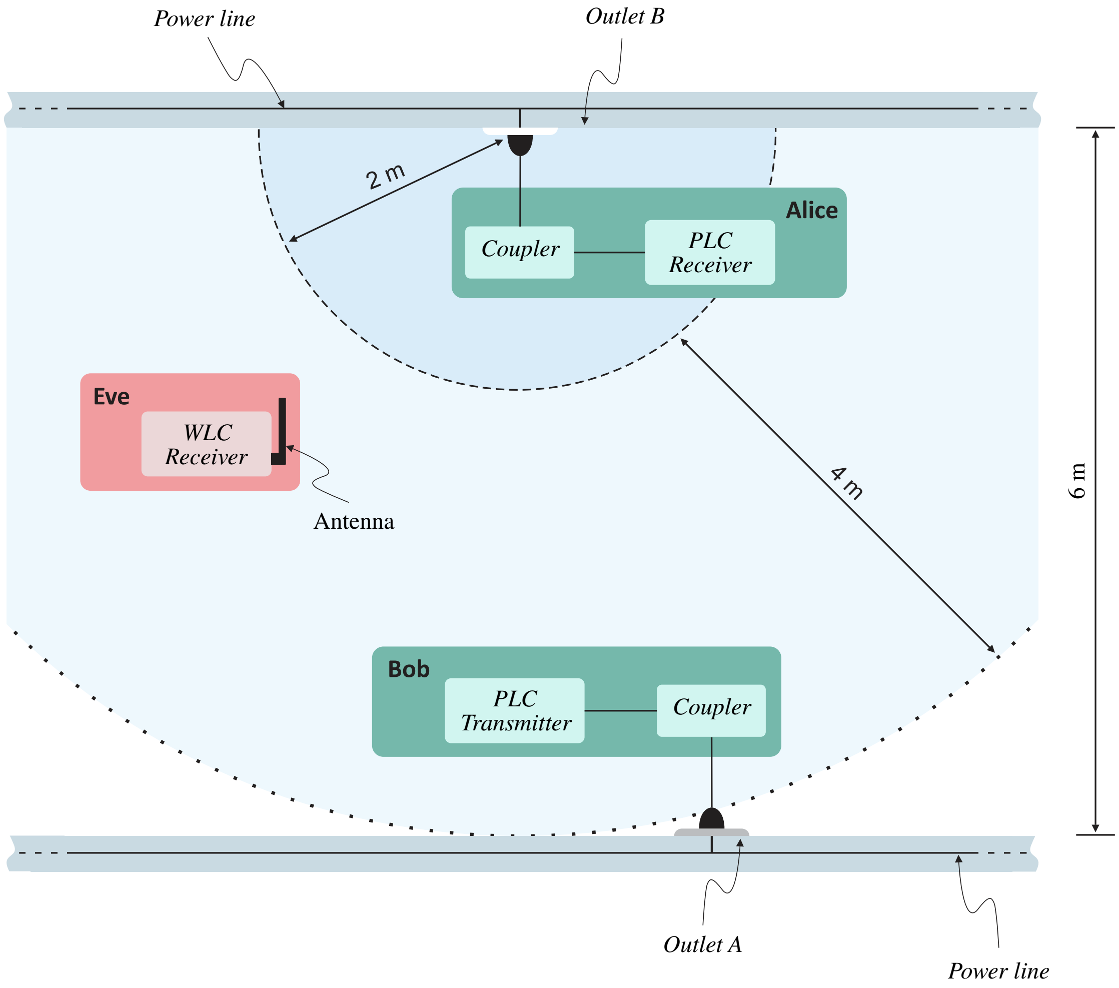
[101] J.-H. Lee and Y.-H. Kim, "Diversity relaying for parallel use of power-line and wireless communication networks," *IEEE Transactions on Power Delivery*, vol. 29, no. 3, pp. 1301–1310, Jun. 2014.

APPENDIX A – In-Home Hybrid PLC-WLC Channels: Measurement Campaign and Setup

This appendix outlines the measurement campaign addressed in [7, 52], in which the data set used to numerically analyze the hybrid wiretap channel model was collected. Such a data set is composed of in-home PLC and hybrid PLC-WLC CFR estimates as well as measured additive noises.

The measurement campaign was carried out in seven middle-class houses in an urban area of Juiz de Fora, Brazil. In this regard, Figure 43 illustrates the measurement setup adopted using the PLS terms considered in this Doctoral thesis. Hence, it consists of the following components:

Figure 43 – Representation of the measurement setup



Source: Based on [7, 52].

- *PLC transmitter*: This equipment generates the sounding signal, which is injected into the electric power grid through a coupler connected to the outlet A.

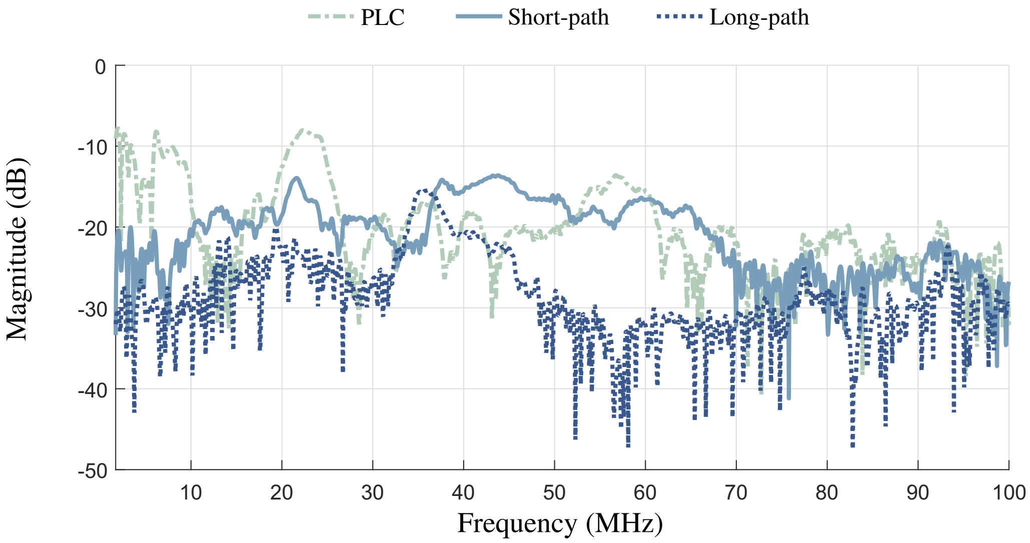
- *PLC receiver*: This equipment acquires the sounding signal from the electric power grid through a coupler connected to the outlet B.
- *Coupler*: This circuit is an interface used to inject/receive the sounding signal into/from the electric power grid. Its main functions are to block the main frequency in order to prevent equipment damage and to limit the PLC signal frequency band, avoiding aliasing [10].
- *WLC receiver*: This equipment acquires through an antenna, the portion of the sounding signal injected into the PLC channel that is irradiated in the air.
- *Antenna*: This transducer acts as an interface in which signals can be inject/receive into/from the wireless medium.

Following the PLS terms, the PLC transmitter and coupler set is named Alice, the PLC receiver and coupler set is named Bob, and the WLC receiver and antenna set is named Eve. It is important to emphasize that the hybrid PLC-WLC channel covers the concatenation of PLC and WLC channels. It means that devices physically and wirelessly connected to a power cable can communicate with each other by operating in the same frequency band. Additionally, Figure 43 shows the maximum distances between Alice and Bob, Alice and Eve, and Bob and Eve adopted in the measurement campaign. As illustrated in Figure 43, the longest distance in which the estimates of PLC CFRs were collected is around 6 meters. In accord with [7, 52], the hybrid PLC-WLC channels may be classified as:

- *Short-path (SP)* : Eve is randomly placed within a 2-m radius circle centered in the outlet A where Alice is connected.
- *Long-path (LP)* : Eve is randomly placed within as a swept circle with an outer and inner radius of 6 and 2 meters, respectively, centered in the outlet where Alice is connected.

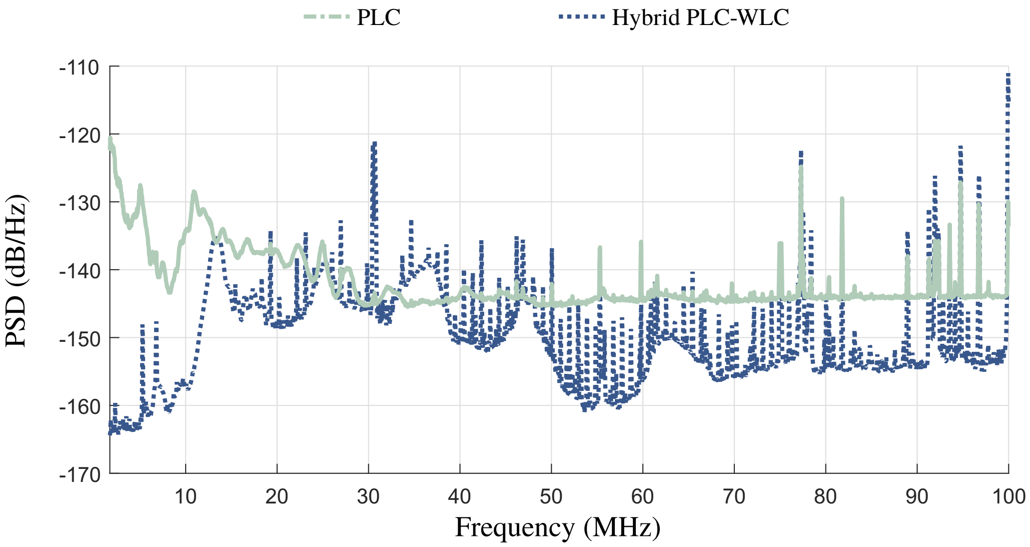
By applying some signal processing techniques (see [8] for details) between the injected sounding signal and the signal measured from the outlet or the air, CFRs are estimated for PLC and hybrid PLC-WLC channels, respectively. In this sense, a total of 216 different combinations of pairs of outlet (PLC channels) were measured. Regarding the hybrid PLC-wireless, Eve was positioned close to Alice (SP channel) in 200 combinations while Eve was placed close to Bob (LP channel) in 93 combinations. Each measure resulted in 600 consecutive CFR estimates, resulting in $175,800$ and $129,600$ CFR estimates for the hybrid PLC-wireless and PLC channels, respectively. An example of a single CFR estimate of each channel is depicted in Figure 44. Furthermore, Figure 45 shows the PSDs of the additive noises measured in both PLC and hybrid PLC-WLC receivers.

Figure 44 – Magnitude of an estimate of PLC and hybrid PLC-WLC CFRs



Source: Personal collection.

Figure 45 – PSD of the measured additive noises related to the PLC and hybrid PLC-WLC channels



Source: Personal collection.

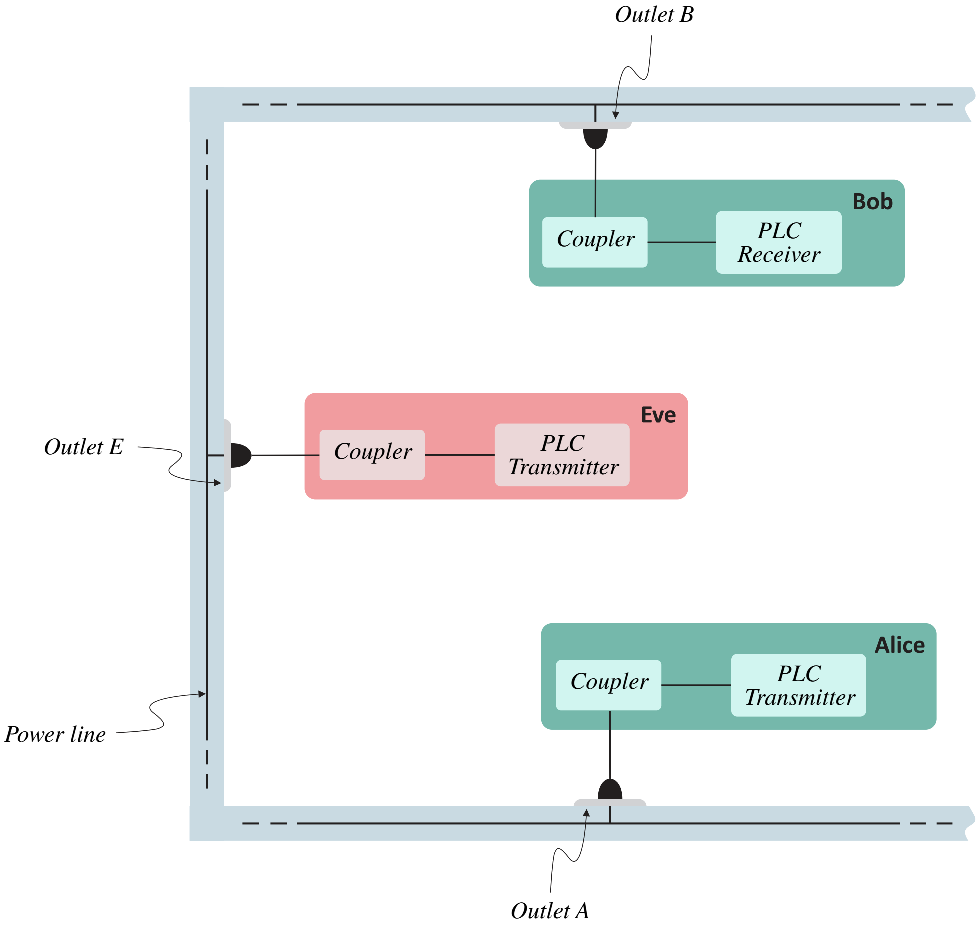
APPENDIX B – In-Home PLC Channels: Measurement Campaign and Setup

This appendix briefly discusses the measurement campaign addressed in [3], through which PLC CFR estimates and measured additive noises considered to represent the PLC wiretap channel model were collected.

The measurement campaign discussed in [3] was carried out in seven middle class residences in a urban area at Juiz de Fora, Brazil, to obtained estimates of in-home PLC channels. In this way, more than $36,000$ CFRs estimates were obtained. The chosen frequency band was $1.7 - 100$ MHz and the selected electric circuits cover distances between 2 to 10 meters within a home.

Figure 46 shows the block diagram of the adopted measurement setup. Note that it is constituted by one PLC transmitter, one PLC receiver, and two couplers. Their functions are the same described in Appendix A. See [3, 15] for more details.

Figure 46 – Block diagram of the measurement setup

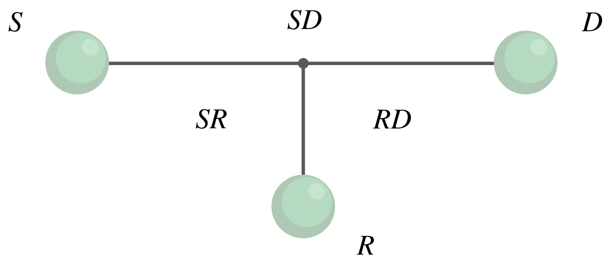


Source: Personal collection.

CFR estimates were measured in order to represent the single-relay channel model shown in Figure 47. Such a channel model is made up by one source (S) node, one relay node (R), and one destination (D) node. Then CFR estimates covered SD, SR or RD links. SD denotes the link between source and destination nodes, SR represents the link between source and relay nodes, and RD is the link between relay and destination nodes. To use the CFR estimates from this measurement campaign to represent the hybrid wiretap channel model, the source, relay, and destination nodes are assumed to be Alice, Bob, and Eve, respectively. Consequently, CFR estimates from SD and SR links are considered to represent Alice-Bob and Alice-Eve links, respectively. With this regard, using the PLS terms, the following cases were investigated in this measurement campaign (see Fig 48):

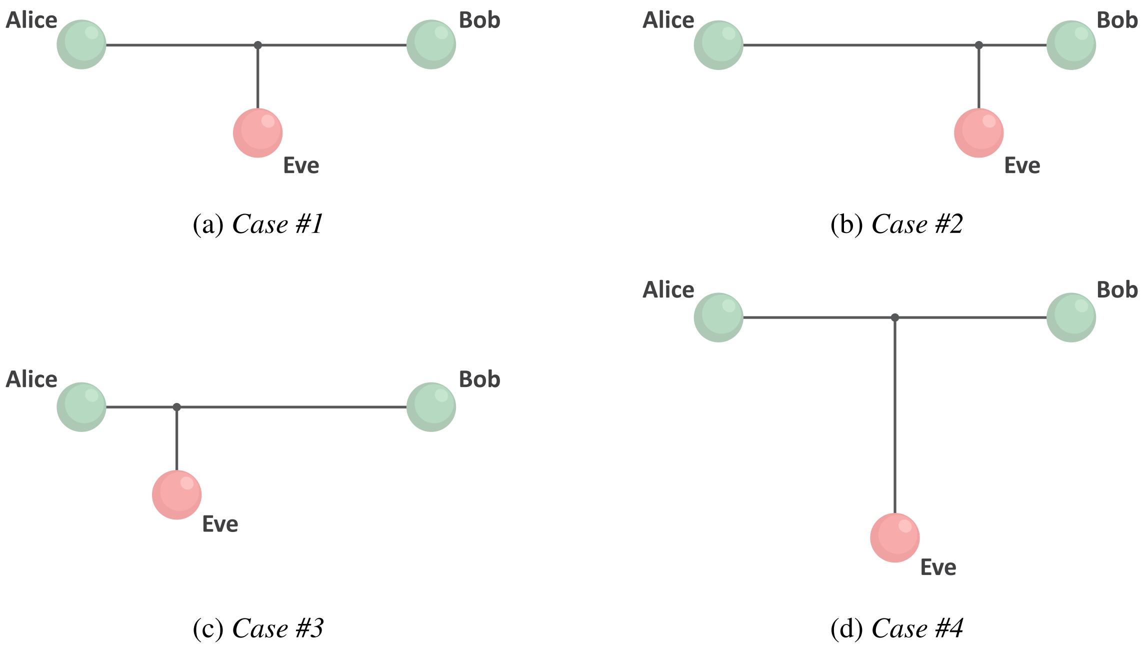
- *Case #1*: Eve locates in the middle between Alice and Bob.
- *Case #2*: Eve locates near Bob and far from Alice.
- *Case #3*: Eve locates near Alice and far from Bob.
- *Case #4*: Eve locates far from both Alice and Bob.

Figure 47 – Single-relay channel model



Source: Personal collection.

Figure 48 – The relative positions of Eve in terms of distances from Alice and Bob



(a) *Case #1*

(b) *Case #2*

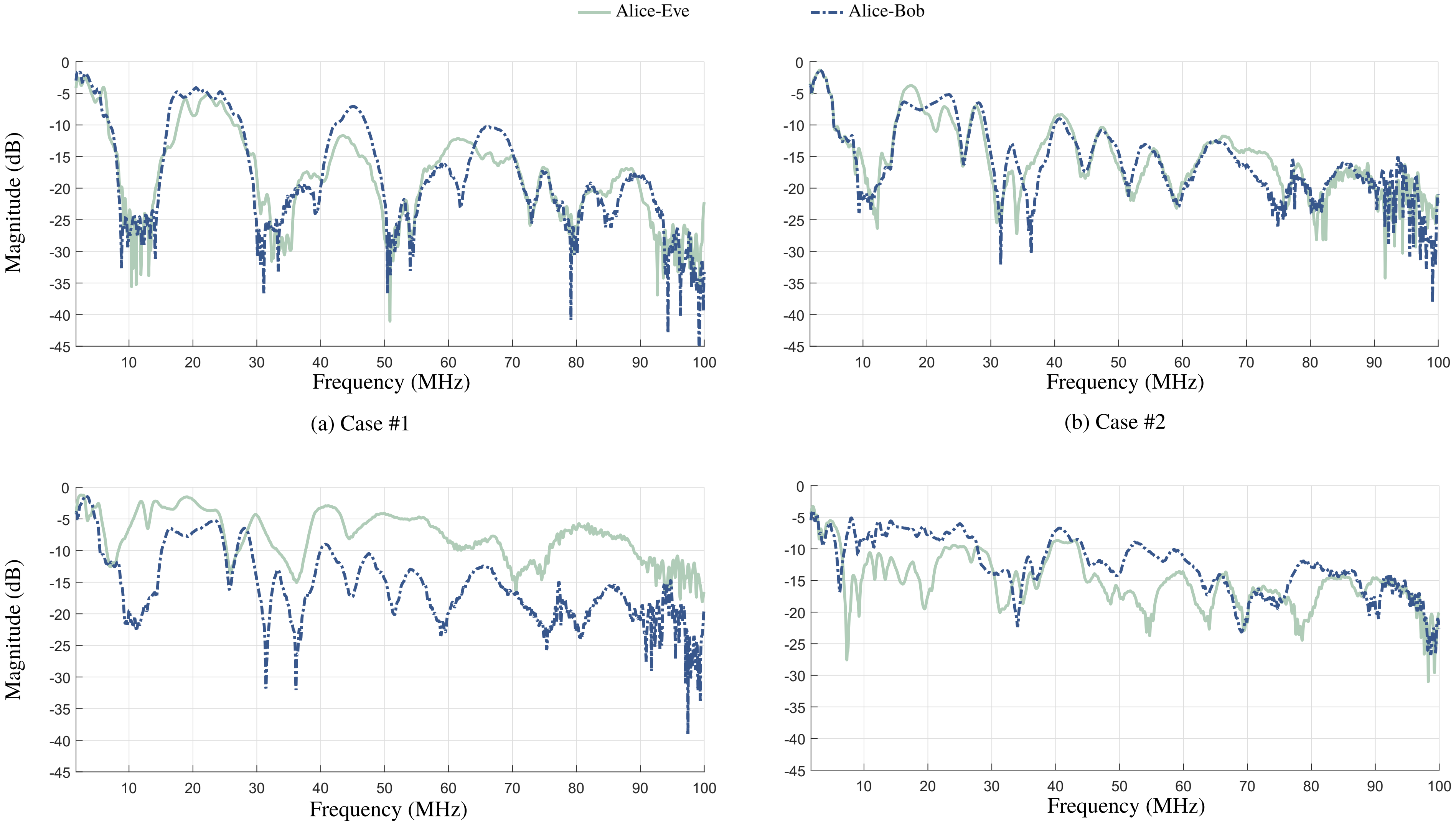
(c) *Case #3*

(d) *Case #4*

Source: Personal collection.

Figures 49(a), (b), (c), and (d) show an example of the magnitude a single CFR estimate of Alice-Bob and Alice-Eve links for case #1, case #2, case #3, and case #4, respectively. In addition, Figures 50(a), (b), (c), and (d) depict the PSDs of the measured additive noises of Alice-Bob and Alice-Eve links considering case #1, case #2, case #3, and case #4, respectively.

Figure 49 – Magnitude of CFR estimates of Alice-Bob and Alice-Eve links



(a) Case #1

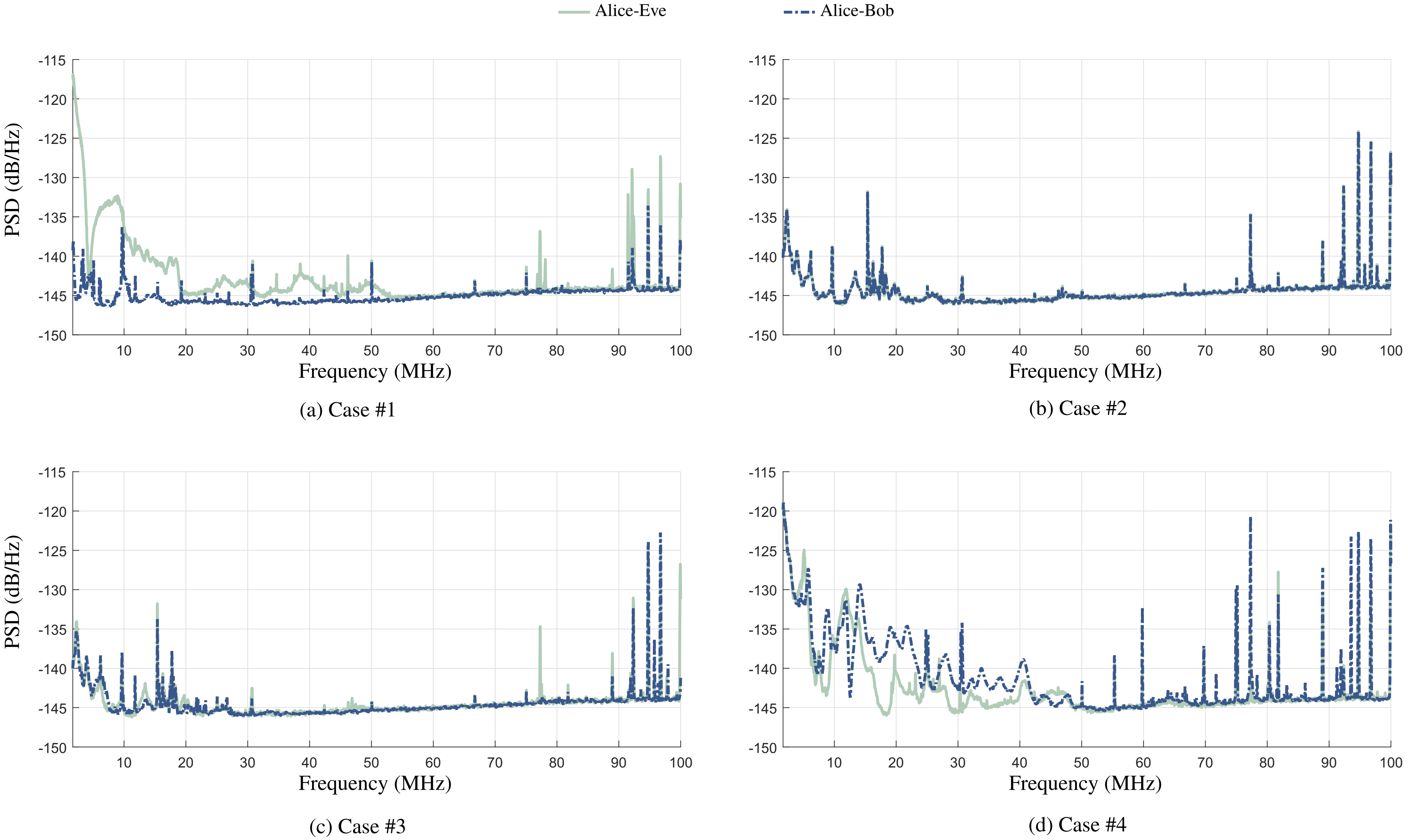
(b) Case #2

(c) Case #3

(d) Case #4

Source: Personal collection.

Figure 50 – PSDs of the measured noises of Alice-Bob and Alice-Eve links



(a) Case #1

(b) Case #2

(c) Case #3

(d) Case #4

Source: Personal collection.

APPENDIX C – Normalized Discrete Fourier Transform Matrix

Let $\{x[n]\}_{n=0}^{N-1}$ be a finite-length sequence in the discrete-time domain and

$$X[k] = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x[n] e^{-\frac{j2\pi}{N}kn}, \quad k = 0, 1, \cdots N-1, \tag{C.1}$$

be its DFT. To make use of the matrix-vector form of (C.1), let $\mathbf{x} \in \mathbb{R}^{N\times 1}$ and $\mathbf{X} \in \mathbb{C}^{N\times 1}$ be the vector representations of $\{x[n]\}_{n=0}^{N-1}$ in the discrete-time and -frequency domains, respectively. Hence, (C.1) can be rewritten as

$$\begin{aligned} \mathbf{X} &= \mathcal{F}\mathbf{x} \\ &= \frac{1}{\sqrt{N}}\mathbf{W}\mathbf{x}, \end{aligned} \tag{C.2}$$

where the DFT matrix $\mathbf{W}$ is given by

$$\mathbf{W} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & e^{-\frac{j2\pi}{N}} & \cdots & e^{-\frac{j2\pi(N-1)}{N}} \\ 1 & e^{-\frac{j4\pi}{N}} & \cdots & e^{-\frac{j4\pi(N-1)}{N}} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & e^{-\frac{j2\pi(N-1)}{N}} & \cdots & e^{-\frac{j2\pi(N-1)(N-1)}{N}} \end{pmatrix}. \tag{C.3}$$

It is worth mentioning that the normalization factor $1/\sqrt{N}$ is adopted in order to ensure the agreement with the Parceval's theorem and, as a consequence, to write $\mathbb{E}\left[\mathbf{x}^{\dagger}\mathbf{x}\right] = \mathbb{E}\left[\mathbf{X}^{\dagger}\mathbf{X}\right]$.

APPENDIX D – Entropy of a Gaussian Random Process

The joint density function of a zero mean Gaussian random vector $\mathbf{V} \in \mathbb{C}^{N\times 1}$, with $\mathbf{R}_{\mathbf{VV}} = \mathbf{I}_N \sigma_{\mathbf{V}}^2$ is given by

$$f_{\mathbf{V}}(\mathbf{v}) = \frac{1}{(2\pi)^{\frac{N}{2}} \det\left(\mathbf{R}_{\mathbf{VV}}\right)^{\frac{1}{2}}} \exp\left(-\frac{\mathbf{V}\mathbf{R}_{\mathbf{VV}}\mathbf{V}^{\dagger}}{2}\right). \tag{D.1}$$

Then the differential entropy of $\mathbf{V} \in \mathbb{C}^{N\times 1}$ can be expressed as

$$\begin{aligned} \hbar(\mathbf{V}) &= -\int f_{\mathbf{V}}(\mathbf{v}) \log_2\left[f_{\mathbf{V}}(\mathbf{v})\right] d\mathbf{v} \\ &= -\int f_{\mathbf{V}}(\mathbf{v}) \left\{-\frac{1}{2}\log_2\left[(2\pi)^N \det(\mathbf{R}_{\mathbf{VV}})\right] - \right. \\ &\quad \left. \frac{1}{2}\mathbf{V}\mathbf{R}_{\mathbf{VV}}\ \mathbf{V}^{\dagger} \log_2[e]\right\} d\mathbf{v} \\ &= \frac{1}{2}\log_2\left[(2\pi)^N \det(\mathbf{R}_{\mathbf{VV}})\right] + \\ &\quad \frac{\log_2[e]}{2}\mathbb{E}\left\{\mathbf{V}\mathbf{R}_{\mathbf{VV}}\ \mathbf{V}^{\dagger}\right\}\ . \end{aligned} \tag{D.2}$$

Using $\mathbb{E}\left\{\mathbf{V}\mathbf{R}_{\mathbf{VV}}\mathbf{V}^{\dagger}\right\} = N$, the differential entropy of $\mathbf{V}$ becomes

$$\begin{aligned} \hbar(\mathbf{V}) &= \frac{1}{2}\log_2\left[(2\pi)^N \det(\mathbf{R}_{\mathbf{VV}})\right] + \frac{N\log_2[e]}{2} \\ &= \frac{1}{2}\log_2\left[(2\pi e)^N \det(\mathbf{R}_{\mathbf{VV}})\right]. \end{aligned} \tag{D.3}$$

APPENDIX E – Publications

The list of papers published during the doctoral period are as follows:

- **Â. Camponogara**, H. V. Poor, and M. V. Ribeiro, "Physical layer security of in-home PLC systems: Analysis based on a measurement campaign," *IEEE Systems Journal*, 2019, *Accepted for publication*.
- **Â. Camponogara**, H. V. Poor, and M. V. Ribeiro, "Broadband PLC system under the presence of a malicious wireless device: Physical layer security analyses", *IEEE Systems Journal*, 2020, *Accepted for publication*.
- **Â. Camponogara**, H. V. Poor, and M. V. Ribeiro, "The complete and incomplete low-bit-rate hybrid PLC/wireless channel models: Physical layer security analyses", *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2760-2729, Apr. 2019.
- **Â. Camponogara**, T. R. Oliveira, R. Machado, W. A. Finamore, and M. V. Ribeiro, "Measurement and characterization of power lines of aircraft flight test instrumentation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 3, pp. 1550-1560, Jun. 2019.
- V. L. R. da Costa, H. V. Schettino, **Â. Camponogara**, F. P. V. de Campos, and M. V. Ribeiro, "Digital filters for clustered-OFDM-based PLC systems: Design and implementation", *Digital Signal Processing*, vol. 70, pp. 166-177, Nov. 2017.

The list of conference papers published during the doctoral period are as follows:

- **Â. Camponogara**, M. L. Filomeno, T. R. Oliveira, L. G. Oliveira, T. F. A. Nogueira, A. A. M. Picorone, S. A. Souza, and M. V. Ribeiro, "Measurement and characterization of a MV distribution network for data communication," in *Proc. Brazilian Symposium on Telecommunications and Signal Processing*, Oct. 2019, pp. 1-6.
- M. V. Ribeiro, F. P. V. de Campos, S. A. Souza, **Â. Camponogara**, E. S. B. Castro, L. M. C. S. Evangelista, and S. D. Penna, "Power Line Communication Applied to Flight Test Instrumentation," in *Proc. 31st Congress of the International Council of the Aeronautical Sciences (ICAS)*, Sep. 2018, pp. 1-7.

The list of expanded summary published during the doctoral period are as follows:

- T. F. Moreira, L. M. de Andrade Filho, **Â. Camponogara**, and M. V. Ribeiro, "Equalização por pseudo-inversa em canais PLC," in *Proc. Brazilian Symposium on Telecommunications and Signal Processing*, Oct. 2019, pp. 1-2.