

Introduction

1.1 Overview of PLC

Power line communication (PLC) has existed since the early years of the 20th century and is utilized for the purpose of voice and data communications over high voltage power lines [Schwartz, 2009]. In the mid-to-late 1990s, due to significant technological advancements in the field of very large-scale integration (VLSI), digital signal processing (DSP), and communication technologies, PLC emerged as an information and communication technology (ICT) that enabled full duplex digital communication over an electrical wire or power distribution network [Majumder and Caffery J, 2004].

The basic architecture of a PLC network is given in Fig. 1.1. It consists of two units, as follows:

1. **Power distribution network:** It is made up of power lines and transformers.
2. **PLC application device:** It is further classified into the following sub units:
 - a) **Coupling module:** It couples high frequency data signal onto power line and filters low frequency (50Hz or 60Hz) signal. It provides protection from noise disturbance. Various coupling circuits are used in the coupling module such as, capacitive coupling, inductive coupling, and transformer coupling.
 - b) **PLC modem:** It consists of protocol chip and analog front end. The basic function of a PLC modem is to modulate and demodulate the data signal. Additionally, it provides interfaces with application devices.

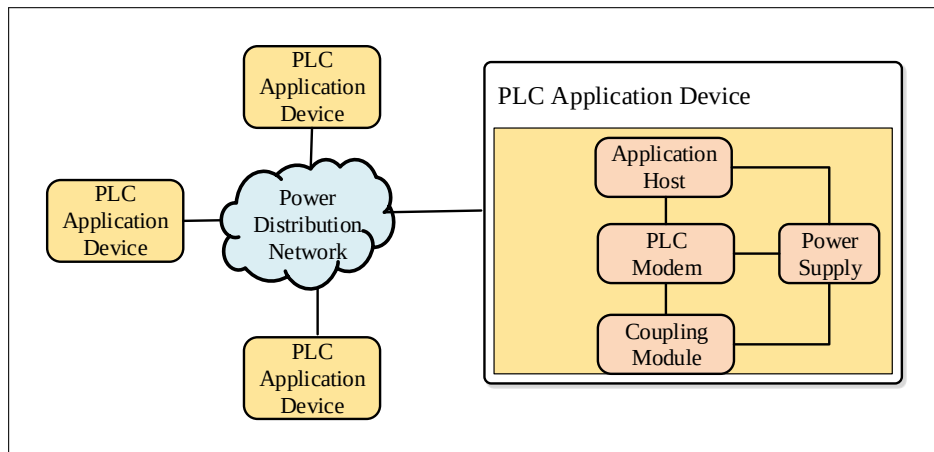


Figure 1.1: Basic architecture of PLC systems.

Based on the frequency range of operation, PLC technology can be classified into three categories as follows [Galli *et al.*, 2011a], [Sendin *et al.*, 2014]:

1. **Ultra-narrow band (UNB) PLC:** These PLC systems typically operate in two frequency ranges: super-low (30–300 Hz) and ultra-low (0.3–3 kHz). This technique is used in ripple control systems for one-way communications. The UNB system offers very low data rates, up to 100 bits per second (bps) at ten to hundreds of kilometres.
2. **Narrow-band (NB) PLC:** NB-PLC systems usually function in the frequency range of 3-500 kHz, which includes the Chinese band (3-500 kHz), the Federal Communications Commission (FCC) band (USA, 10-490 kHz), the European Committee for Electrotechnical Standardization (CENELEC) A band (Europe, 3-148.5 kHz), and the ARIB band (Japan, 10-450 kHz). These technologies have a range that can extend from hundreds of meters to several kilometers, depending on the power lines. NB PLC technologies can be further divided as:
 - *Low Data Rate (LDR) NB-PLC:* It utilizes single carrier modulation schemes and is capable of offering data rates upto a few kilobits per second (kbps).
 - *High Data Rate (HDR) NB-PLC:* This technology employs multi-carrier modulation schemes and can yield data rates upto hundreds of kbps.

Several international standards have been developed for NB-PLC such as Powerline Intelligent Metering Evolution (PRIME), G3, IEEE 1901.2, and ITU-T G.hnem. NB-PLC is considered for outdoor communications or last-mile access, including smart grid communications.

3. **Broad-band (BB) PLC:** This type of PLC has a frequency range of 1.8-250 MHz, which allows it to support data rates ranging from several Megabits per second (Mbps) to hundreds of Mbps over distances of hundreds of meters to kilometers. Some worldwide standards, such as IEEE 1901, ITU-T G.hn, HomePlug AV, HomePlug AV2, and HomePlug Green PHY, have been established for BB PLC. Specifically, these standard specifications are designed for the purpose of indoor communications or last-inch access, including home area networking (HAN).

1.2 Advantages of PLC

PLC has several benefits that establish it as a promising and appropriate contender compared to other communication technologies, as listed below [Cano *et al.*, 2016]:

1. **High networking coverage:** The omnipresence of existing wired infrastructure from urban to rural or remote areas makes PLC ubiquitous. Owing to this, PLC can offer substantial geographical network coverage.
2. **Cost-effective:** Since electricity lines are already in place, there is no need to install additional cables for communication. Therefore, PLC possesses low installation and maintenance costs, which makes PLC cost-effective technology.
3. **High data rates:** Worldwide, several industrial bodies and international standards have been consolidated to achieve high data rates using BB-PLC technology. It has been found that PLC can offer data rates up to several hundred Mbps.
4. **Easy connectivity:** PLC facilitates connection with nodes that are difficult to access due to significant signal weakening in wireless transmission, such as in subterranean structures,

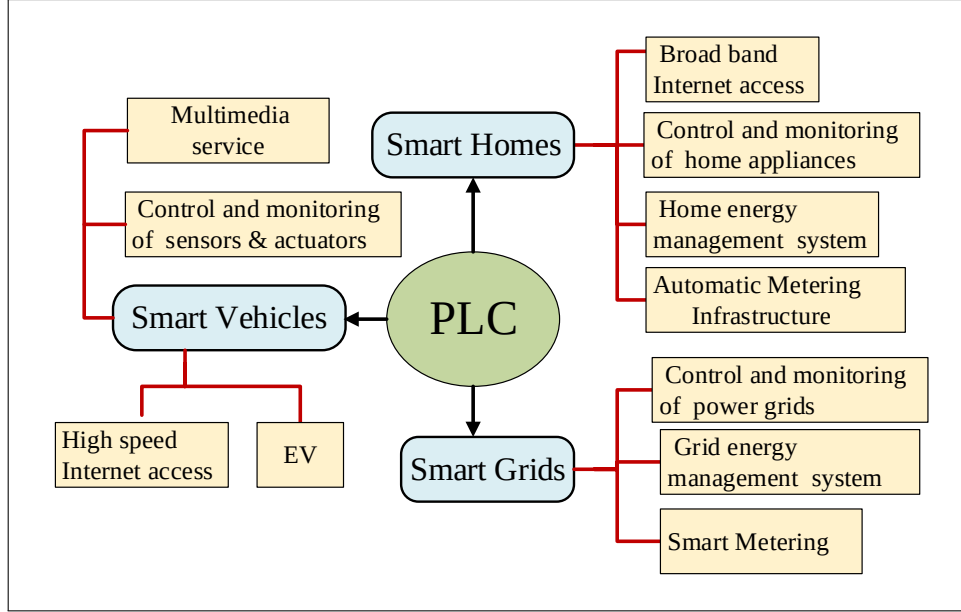


Figure 1.2: Application scenario of PLC systems.

obstructed buildings with metal and bulky cemented walls, or situations where the wireless signal is unwanted due to electromagnetic interference (EMI) concerns. Additionally, it can reduce a significant amount of wiring weight, volume, and complexity in the communication systems.

1.3 PLC Applications

Due to the benefits mentioned above, PLC is widely recognized as an appropriate technology for many engineering applications in the realm of the Internet of Things (IoT) and the fourth industrial revolution, commonly referred to as Industry 4.0, as shown in Fig. 1.2. Some of the PLC applications are discussed in the following [Lampe *et al.*, 2016]:

1. **Smart grid:** PLC is an inherent communication technique for smart grids since it utilizes pre-existing power connections wherein the role of PLC is as a backbone technology to communicate with substations to meet operational requirements. PLC can be deployed to monitor and control power grids in fault detection, power quality, and islanding effect. PLC can also offer services in grid energy management and smart metering.
2. **Smart home and industry:** PLC is well-suited for household and industrial applications because of its cost-effectiveness. PLC leverages the pre-existing infrastructure in residential and industrial buildings, obviating the need for expensive and complex installation of new wires. In this context, PLC can be utilized in home, building, and industry automation, where it can control and monitor the home and building appliances and industry devices. PLC also can be deployed to provide high-speed Internet in HAN.
3. **Smart vehicle:** The use of additional wires for communication in vehicles adds complexity to the wiring harness, resulting in increased manufacturing and installation costs and additional weight and space requirements. Therefore, utilizing power cables for data transfers through PLC minimizes the need for extra wiring, resulting in cost, weight, and space advantages. In addition, PLC can be employed to control and monitor the sensors and actuators of vehicles.

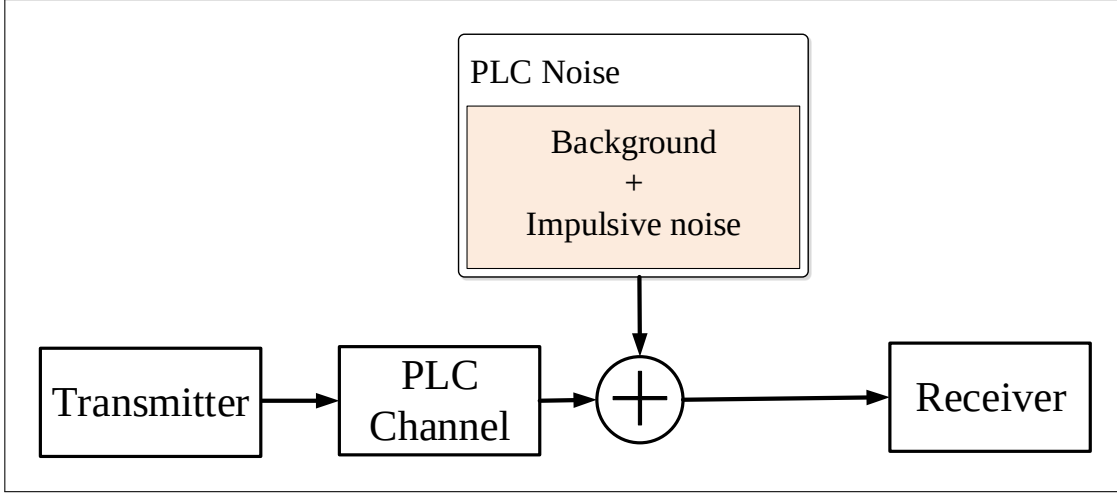


Figure 1.3: Basic communication scenario in PLC.

PLC can also offer multimedia services to the vehicle.

4. **Other Applications:** Besides the aforementioned applications, PLC has been proposed for some other novel applications, including electric vehicles (EVs), robotics, mining security, and wireless power transfer [Cano *et al.*, 2016].

1.4 PLC Channel Modeling

The schematic diagram of a PLC system is demonstrated in Fig. 1.3, where a signal is transmitted by the transmitter to the receiver through a PLC channel in the presence of additive background and impulsive noise. When the signal is propagated via a PLC channel, it severely suffers from the indeterministic characteristics of the channel. Consequently, the signal undergoes multipath propagation due to impedance mismatch and signal reflection. Therefore, signal parameters such as amplitude and phase fluctuate with frequency and time. This process is called signal fading which is characterized by a parameter called channel fading coefficient or channel gain. In literature, several mathematical models have been proposed to model the PLC channel gain as follows [Güzelgöz *et al.*, 2011]:

1. **Rician distribution:** The PLC channel gain was expressed using the Rician distribution in [Lutz and Huber, 2000]. In [Lee *et al.*, 2001], the authors experimentally investigated the channel impulse response of PLC by employing an empirical multipath model, where it was shown that the amplitude of multipath signal components was Rician and Rayleigh distributed over a time period. Further, the authors in [Kim *et al.*, 2002], measured the channel impulse response in an in-house PLC system at 10-30 MHz, where it was reported that the signal amplitude follows the Rician distribution over an average time interval. The probability density function (PDF) of Rician distribution is written as [Lutz and Huber, 2000, Eq. (12)]

$$f(h) = \frac{h}{\sigma^2} \exp\left(-\frac{h^2 + \mu^2 + \mu'^2}{2\sigma^2}\right) I_0\left(\frac{\sqrt{h(\mu^2 + \mu'^2)}}{\sigma^2}\right). \quad (1.1)$$

In (1.1), μ and μ' are the means, σ^2 is the variance, and $I_0(\cdot)$ is the modified Bessel function of zeroth order and first kind [Gradshteyn and Ryzhik, 2014, Eq. (8.402)].

2. **Rayleigh distribution:** The Rayleigh distribution is the special case of the Rician distribution when the Rice factor, $(\mu^2 + \mu'^2)/\sigma^2$ becomes zero in (1.1). The authors in [Lee *et al.*, 2001] performed measurements and simulations for an indoor high-speed multipath power line channel where it was confirmed that the over a time period the statistics of the normalized amplitude fits the Rayleigh distribution curve. Likewise, in [Liu *et al.*, 2008], the authors analyzed and modeled an indoor power line channel over a multipath channel where it was demonstrated that the PLC channel obeys the Rayleigh distribution. The PDF of Rayleigh distribution is expressed as [Liu *et al.*, 2008, Eq. (7)]

$$f(h) = \frac{h}{\sigma^2} \exp\left(-\frac{h^2}{2\sigma^2}\right). \quad (1.2)$$

3. **Log-normal distribution:** The PLC channel gain is very popularly modeled by the Log-normal distribution [Papaleonidopoulos *et al.*, 2003], [Güzelgöz *et al.*, 2011], [Galli, 2011]. In [Papaleonidopoulos *et al.*, 2003], the authors studied indoor PLC channels in the high-frequency range for single-phase low-voltage (LV) networks. They assumed a multipath propagation model and it was shown that the amplitude of these paths follows the Log-normal distribution. The authors in [Güzelgöz *et al.*, 2011] investigated the multipath PLC channels where it was demonstrated that the PLC channel gain could be approximated by the Log-normal distribution. Similarly, in [Galli, 2011], the measurements were conducted on LV/medium voltage (MV) power line channels in sub-urban, urban in-home, and underground MV PLC in the United States (US) across the frequency range of 1.8 MHz to 30 MHz. It was found that the power line channel gain follows the Log-normal distribution. The PDF of the PLC channel gain is given as [Papaleonidopoulos *et al.*, 2003, Eq. (56)]

$$f(h) = \frac{1}{h\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(\ln h - \mu)^2}{2\sigma^2}\right). \quad (1.3)$$

In (1.3), μ and σ^2 are mean and variance, respectively, of the random variable (RV) h and $h \geq 0$.

1.5 Classification and Modeling of PLC Noise

Unlike most other communication channels, the nature of noise present in a powerline environment is severe and exhibits time-varying and non-white characteristics [Katayama *et al.*, 2006]. The non-Gaussian and non-white nature of PLC noise is an important aspect causing the poor performance of PLC systems. The noise in PLC systems can be classified into two different categories as follows [Zimmermann and Dostert, 2002a], [Gotz *et al.*, 2004]:

1. Background Noise

- a) **Colored background noise:** This noise arises from the accumulation of multiple low-power noise sources, including home appliances and fluctuates with frequency and has a comparatively low power spectral density (PSD). This noise slowly changes over time, but in terms of minutes or even hours, it stays relatively constant. This disturbance occurs within the frequency range of 30 MHz.
- b) **Narrow-band noise:** This noise is generated by broadcast stations and primarily comprises modulated amplitude sinusoidal signals. This narrow-band noise occurs in the typical frequency range of 1-22 MHz.

2. **Impulsive Noise:** This noise can be described as either periodic or aperiodic. Periodic

impulsive noise can be categorized further as interference that is synchronous or asynchronous with the main frequency.

- a) **Periodic impulsive noise asynchronous to the mains frequency:** This noise occurs due to the various power supplies present in the networks. The line spectrum of this noise is discontinuous and spaced by the impulse repetition rate; the repetition rate ranges from 50 to 200 kHz.
- b) **Periodic impulsive noise synchronous to the mains frequency:** This type of noise has a brief duration with a repetition rate of 50 or 100 Hz (in Europe). The impulse occurs for just a few microseconds and their PSD decreases as the frequency increases. These impulses are generated by the power supply, due to the switching of rectifier diodes.
- c) **Asynchronous impulsive noise:** This form of noise is caused by network switching transients. The impulses fluctuate randomly, ranging in duration from microseconds to several milliseconds. The magnitude of PSD can exceed 50 dB above the background noise.

Similar to PLC channel modeling, in literature, several mathematical models have been documented to simulate the behavior of both background and impulsive PLC noise as follows:

1. **Nakagami- m distribution:** The authors examined the frequency-domain approach in [Meng *et al.*, 2005], wherein they determined that the amplitude spectrum of the background noise ranging from 1 to 30 MHz adheres to the Nakagami distribution. In [Tao *et al.*, 2007], the authors modeled and statistically analyzed the noise in 10-kV MV power networks using empirical data collected from two representative substations. The measured data showed that the Nakagami distribution is an ideal fit for simulating the colored background noise. The PDF of the Nakagami- m distribution is written as [Tao *et al.*, 2007, Eq. (2)]

$$f(n|m, \Omega) = \frac{2m^m}{\Gamma(m)\Omega^m} n^{2m-1} \exp\left(-\frac{mn^2}{\Omega}\right). \quad (1.4)$$

In (1.4), $\Gamma(\cdot)$ denotes the Gamma function, $\Omega = \mathbb{E}[n^2]$ represents the average power, and m indicates ratio of moments defined as $m = \Omega^2/\mathbb{E}[(n^2 - \Omega)^2]$ with $m \geq 0.5$.

2. **Middleton class-A noise model:** Firstly, the behavior of both the background and impulsive noise was investigated and modeled in [Middleton, 1972], [Spaulding and Middleton, 1977] and was named the Middleton class-A noise model. Thereafter, this noise model has been adopted as a basic model to characterize the behavior of noise in PLC channels [Balakirsky and Vinck, 2003], [Ferreira *et al.*, 2011], [Matanza *et al.*, 2013], [Rabie and Alsusae, 2015]. The PDF of the Middleton class-A noise model is expressed as [Rabie and Alsusae, 2015, Eq. (4)]

$$f(n) = \sum_{m=0}^{\infty} \frac{e^{-A} A^m}{m!} \cdot \frac{1}{\sqrt{2\pi\sigma_m^2}} \exp\left(-\frac{|n|^2}{2\sigma_m^2}\right). \quad (1.5)$$

In (1.5), $\sigma_m^2 = \sigma_u^2 \left(\frac{m+\Upsilon}{1+\Upsilon}\right)$ denotes the variance of the m th arriving impulsive noise components, $\sigma_u^2 = \sigma_G^2 + \sigma_I^2$ shows the total noise power, $\Upsilon = \sigma_G^2/\sigma_I^2$ represents the Gaussian-to-impulsive noise power ratio, and $A = \mathbb{E}[m]$.

3. **Two-mixture Gaussian noise model:** In [Ghosh, 1996] the study examined the combined impact of background and impulsive noise. Herein it was shown that the occurrence of impulsive noise can be modeled using the Bernoulli-Gaussian random process.

The total noise in PLC systems can be expressed as [Ghosh, 1996, Eq. (1)]

$$n = b + i = b + P_B \cdot g. \quad (1.6)$$

In (1.6), b and i indicate the background and impulsive noise components, respectively, where $i = P_B \cdot g$, P_B is the Bernoulli process with $\Pr(P_B = 1) = p$ and $\Pr(P_B = 0) = (1 - p)$. Here, p indicates the probability of arrival of the impulsive noise and g is white Gaussian process with mean zero and variance σ^2 . Hence, the PDF of the noise can be written as [Ma *et al.*, 2005a, Eq. (4)]

$$f(n) = (1 - p)\mathcal{N}(0, \sigma_b^2) + p \mathcal{N}(0, \sigma_b^2 + \sigma_i^2). \quad (1.7)$$

In (1.7), $\mathcal{N}(\cdot, \cdot)$ stands for Gaussian distribution. Here, σ_b^2 and σ_i^2 are the variances of the background and impulsive noises, respectively.

Similarly, the authors in [Ma *et al.*, 2005a, 2008] modeled the arrival of the impulsive noise by Poisson distribution. Therefore, the total noise in this case is written as [Ma *et al.*, 2005a, Eq. (6)]

$$n = b + i = b + P_s \cdot g. \quad (1.8)$$

In (1.8), $i = P_s \cdot g$ and P_s is the Poisson process. Here, probability distribution of arrival of the k^{th} impulsive noise component with time interval t and arrival rate λ is defined as $P_k(t) = \exp(-\lambda t)(\lambda t)^k/k!$. Thus, the PDF of the total PLC noise can be written as [Ma *et al.*, 2005a, Eq. (8)]

$$f(n) = (\lambda t) \mathcal{N}(0, \sigma_b^2) + (1 - \lambda t) \mathcal{N}(0, \sigma_b^2 + \sigma_i^2). \quad (1.9)$$

1.6 PLC Challenges

Despite the numerous benefits and applications of PLC, it also suffers from several technical challenges, similar to other communication technologies. These challenges are described as follows [Lampe *et al.*, 2016]:

1. **Harsh medium:** Power lines, originally not intended for communication, exhibit significant variations in channel characteristics with time and frequency, resulting in frequency and spatial correlation. Furthermore, the presence of different wire topologies and varying impedances results in pronounced branching effects and multipath propagation. Therefore, PLC are very hostile medium for the transmission of data.
2. **Noise and interferences:** Unlike other communication channels, PLC channels are not additive white Gaussian noise (AWGN) channels. These exhibit non-Gaussian characteristics and are susceptible to many types of noise and interference, including colored noise, narrow-band interference, and impulsive noise. Thus, coping with noise is a significant challenge in PLC.
3. **High data rates:** Offering data rates comparable to other communication technologies in PLC is a prominent challenge due to the harsh communication environment. Specifically, power lines are not designed to yield high data rates. Hence, delivering a high data rate through PLC is an important challenge.
4. **Data security:** The PLC channels are broadcast and ubiquitous in nature; thus the channels are shared among the users in the network. Owing to this, an intruder easily connects with them and is capable of eavesdropping and jamming them. In this scenario, data security can be breached. Therefore, providing security in PLC is an important challenge in PLC systems.

1.7 Strategies to Mitigate PLC Security Challenges

Let us now discuss some techniques that have been used in PLC systems to compensate for PLC security challenges in the following subsections. In this thesis, we employ and delve into these techniques for the proposed system.

1.7.1 Physical Layer Security Technique

The significance of privacy and security issues in communication networks has notably escalated with the development in ICT networks and advancements in hacking technology. Typically, security is often seen as a separate aspect addressed above the physical layer. Thereupon, the most common cryptographic algorithms, such as Rivest, Shamir, Adleman (RSA), Advanced Encryption Standard (AES), and key management mechanisms have been developed and executed on the assumption that the physical layer is self-sufficient and offers an error-free connection. However, because of the progress and advancement in computer technology, these cryptographic algorithms and key management systems could not guarantee perfect network security [Bloch *et al.*, 2008]. Thereby, in literature [Shiu *et al.*, 2011], several theories and practical solutions have been proposed to affirm the potential of physical layer security (PLS) also known as information-theoretic security to adequately enhance security of digital communication systems.

The foundation of information-theoretic approach is based on Shannon's concept of perfect secrecy [Shannon, 1949], which was established by Wyner [Wyner, 1975], and further explored by Csiszár and Körner [Csiszár and Körner, 1978] for a basic wiretap channel, who demonstrated in landmark studies that there are channel codes that guarantee a certain degree of data secrecy as well as resilience against transmission failures. PLS means implementing security of the communication system in the physical layer by exploiting the physical characteristics of a communication channel, such as channel randomness, fading, noise, interference, time/frequency diversity, and the differences between the user's links in such a way that an intruder can not decode the original data from the legitimate communication channel [Bloch *et al.*, 2008]. Besides this, PLC is a promising technique and is considered a complementary method along with the traditional cryptographic techniques to strengthen data security. Further, the physical layer security (PLS) performance can be measured in terms of following performance metrics such as

1. **Average secrecy capacity (ASC):** The average of maximum of all rates that can be achieved to ensure the confidentiality of the transmitted data for complete secrecy is called the average secrecy capacity. This indicates that the maximum amount of data can be securely transmitted to the receiver without any leakage to an eavesdropper [Pan *et al.*, 2016]. In other words, for a degraded Gaussian wiretap channel, it is defined as the maximum difference of instantaneous channel capacity of the authorized channel and the eavesdropper channel where the authorized channel should have higher data rate than the eavesdropper channel.
2. **Secrecy outage probability (SOP):** Characterizing the outage probability in terms of secure communication is known as SOP. It is defined as the probability that the instantaneous secrecy capacity falls below a predefined threshold rate [Pan *et al.*, 2016]. This concept of outage probability has two practical implications. First, it gives the percentage of fading knowledge for a communication channel under which it can maintain a safe bit rate per channel usage. Secondly, it provides a security measure when Bob and Alice don't have any channel state information (CSI) about an eavesdropper. In this case, Alice can set a constant secrecy rate for Bob to maintain secrecy between them.
3. **Strictly positive secrecy capacity (SPSC):** In the realm of PLS, SPSC is often used as an essential criterion to express the guarantee of secure communication between transmitter and receiver in terms of secrecy capacity. It is the probability of when instantaneous secrecy

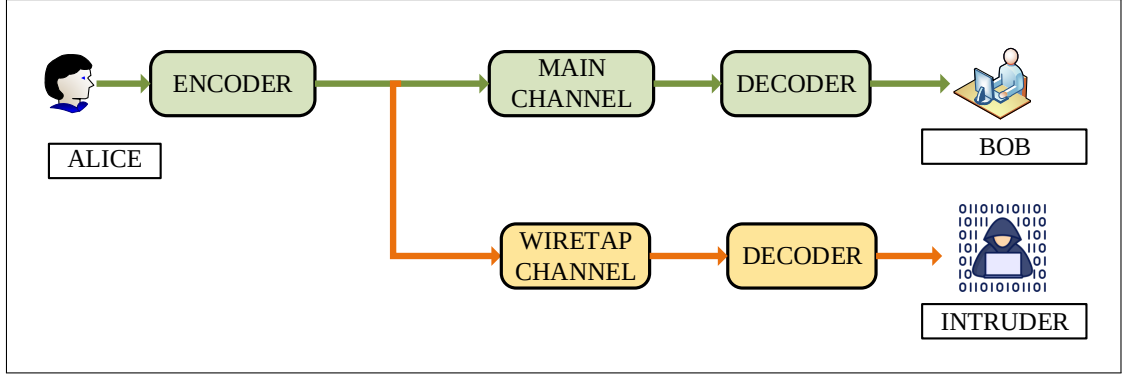


Figure 1.4: Basic wiretap channel model.

capacity is greater than zero [Pan *et al.*, 2016].

4. **Secrecy throughput:** Secrecy throughput is a measure of the effective transmission rate of confidential information in the presence of potential eavesdroppers in a communication system. It quantifies the amount of information that can be securely transmitted from the transmitter to the receiver per unit of time while ensuring that an eavesdropper does not intercept any information. In PLS analysis, secrecy throughput is one of the essential parameters that defines the average secrecy rate subjected to SOP constraints, which considers the reliability and security simultaneously [Zhou *et al.*, 2011].

A fundamental wiretap channel model is utilized to study PLS performance as shown in Fig. 1.4. The figure elucidates that Alice and Bob are the authorized users communicating with each other over the main channel. At the same time, an intruder exists who wants to overhear the secret message transmitted between Alice and Bob by forming a wiretap channel. This whole process is called wiretapping. In Fig. 1.4, we consider a passive eavesdropper where the location of the eavesdropper is fixed and separated by a certain distance. The CSI of the main channel and the wiretap channel are presumed to be known. The secrecy of the communication channel largely depends on the channel conditions, such as signal-to-noise ratio (SNR), fading characteristics, etc. An eavesdropper has better channel condition when it is nearer to Alice and the wiretap channel is less faded as compared to the main channel. Due to this, an eavesdropper receives a better SNR signal from Alice, and hence, the main channel becomes less secure and the chances of secrecy outage are higher. Similarly, when an eavesdropper is situated farther from Alice, the wiretap channel degrades more because when the eavesdropper's distance increases from Alice, the SNR at the eavesdropper's link becomes poor. Consequently, the chance of secrecy and outage is higher.

Akin to the eavesdropping scenario, another type of intruder or interference in a communication network is a jammer who deliberately or intentionally wants to disrupt the existing communication network at the physical layer by lowering SNR at the receiver side by injecting a noise signal into the authorized communication link called as jamming [Grover *et al.*, 2014]. This action of the jammer sometimes results in conflict and denial-of-service (DoS) in the communication network. In literature, many types of jammers have been investigated with their different modes of attacks as follows [Grover *et al.*, 2014], [Pirayesh and Zeng, 2022]:

- **Constant Jamming Attacks:** In this type of jamming scenario, the jammer continuously emits a strong noise signal all the time to interfere with the communication link. This kind of jamming attack is energy inefficient and easy to detect but is very easy to launch and can damage network communications to the point that no one can communicate at any time.

- **Deceptive jamming:** In deceptive jamming, the jammer continuously transmits a regular signal instead of emitting a random noise signal. It deceives the communication link and believes that a legitimate transmission is taking place so that they remain in receiving states until the jammer is turned off or dies. In comparison to a constant jammer, it is more difficult to detect because it transmits legitimate signals instead of random bits. Similar to the constant jammer, the deceptive jammer is also energy inefficient due to the continuous transmission but is very easily implemented.
- **Random pulse jamming:** This kind of jamming is also called reactive jamming, where the jammer injects jamming signals for random periods and turns to on (active) and off (idle) state and disrupts the communication between authorized links. This type of jamming attack allows the jammer to save more energy compared to a constant jamming attack. However, it is much more challenging to detect a random pulse jammer than a constant jammer.

1.7.2 Differential Chaos Shift Keying Modulation Technique

Chaos-based communication systems have been widely researched in the past two decades due to the manifold and excellent properties of chaotic signals [Kocarev *et al.*, 1992; Cuomo and Oppenheim, 1993; Dedieu *et al.*, 1993; Kolumbán *et al.*, 1996, 1997; Tam *et al.*, 2002]. Some important properties of chaotic signals are as follows [Tse and Lau, 2003], [Xia and Lau, 2004], [Yu and Yao, 2005]:

- Chaotic signals have a high sensitivity to initial conditions. Therefore, by changing the initial conditions, it is theoretically possible to produce an infinite number of uncorrelated chaotic signals.
- Chaotic signals exhibit impulse-like auto-correlation and low cross-correlation. The power spectrum of chaotic signals is white wideband.
- Prediction of long-term behavior of a chaotic signal is not possible.
- Chaos signals are entirely self-generated for given conditions or control parameters. There is no need to add any random variables or external noise.
- Chaotic signals possess many benefits similar to spread-spectrum signals, including secure communication, anti-jamming, suppression of inter-user interference, and mitigation of multipath fading.
- Chaotic signals can be generated using very simple circuitry. Chaos based communication does not require additional spreading and de-spreading circuitry. Thus, chaos offers potentially cost-effective alternative for spread-spectrum communications.

Among them, coherent chaos shift keying (CSK) [Cuomo and Oppenheim, 1993], [Dedieu *et al.*, 1993] and non-coherent differential chaos shift keying (DCSK) modulation schemes [Kolumbán *et al.*, 1996] have been thoroughly investigated with a great deal of interest in recent years due to their feasible implementation [Mandal and Banerjee, 2004]. DCSK modulation has shown unique advantages compared to other chaotic modulation schemes as follows [Kaddoum *et al.*, 2012], [Kong *et al.*, 2015]:

- The demodulation of DCSK is performed using non-coherent detection, which means that the receiver does not need a precise replica of the chaotic sequence and chaotic synchronization. Moreover, DCSK does not require CSI information at the receiver side.
- DCSK demodulation is not affected by any threshold-shift issues. The detector's threshold is

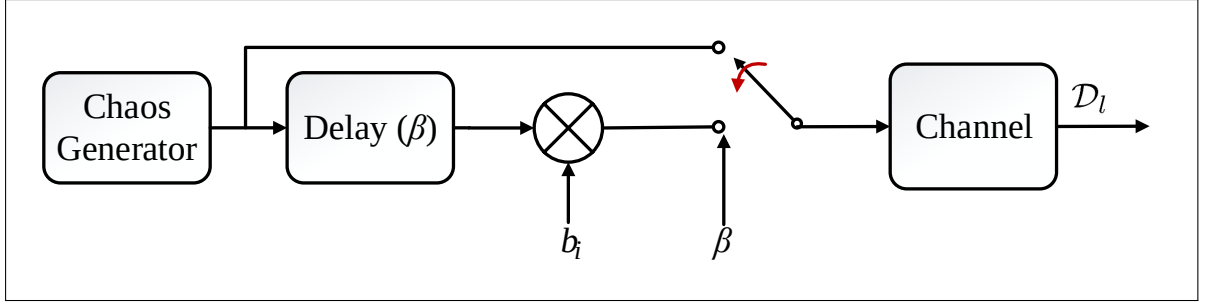


Figure 1.5: Basic diagram of DCSK modulator.

unaffected by the noise level.

- DCSK is more immune to channel distortion since the channel often remains stable over a symbol period. Consequently, both the reference and data samples are affected by the same distortion. Therefore, DCSK poses a stronger resilience to multipath fading and nonlinear distortions.
- In DCSK modulation scheme, chaotic map uses some initial seed values to generate the chaotic carrier signal. Further, on the receiver side, to decode that chaotic signal, the receiver should know the initial seed value of the chaotic signal. If the receiver has no information about the initial seed value, it cannot decode the transmitted chaotic signal. Hence, these properties of chaos signal make the interception and decoding of data more difficult for an unknown receiver or eavesdropper.

The above-mentioned unique properties of chaotic signals and DCSK modulation scheme help in providing secure communication in the eavesdropping scenarios. This renders it an effective modulation scheme for PLC.

Figure 1.5 illustrates the DCSK modulation scheme. A chaos generator generates the chaotic signal using logistic and cubic map such as, $s_l = 2s_{l-1}^2 - 1$. Each chaotic signal consists of two segments; the first segment contains the reference signal, and the second is a data-carrying signal. If the data-carrying signal is identical to the reference signal, bit '1' is transmitted. Whereas, if the data-carrying signal is an inverted copy of the reference signal, '-1' is sent. Let 2β denote the spreading factor that defines the number of chaotic samples sent for each bit. For the i^{th} bit duration, the output of DCSK modulator $\mathcal{D}_l$ is

$$\mathcal{D}_l = \begin{cases} s_l, & 1 \leq l \leq \beta, \\ b_i s_{l-\beta}, & \beta < l \leq 2\beta. \end{cases} \quad (1.10)$$

In (1.10), s_l is the chaotic signal used as reference signal, $s_{l-\beta}$ shows its delayed copy, and $b_i \in \{+1, -1\}$. For $\beta = 5$, the DCSK signal is generated as follows:

$$\begin{aligned} \mathcal{D}_l = \text{bit '1'} &= \begin{cases} 0.2900, -0.7724, 0.4738, -0.9959, -0.9637, & \text{is reference signal} \\ 0.2900, -0.7724, 0.4738, -0.9959, -0.9637, & \text{is data signal} \end{cases} \\ \mathcal{D}_l = \text{bit '-1'} &= \begin{cases} 0.2900, -0.7724, 0.4738, -0.9959, -0.9637, & \text{is reference signal} \\ -0.2900, 0.7724, -0.4738, 0.9959, 0.9637, & \text{is data signal.} \end{cases} \end{aligned}$$

Based on the Gaussian approximation, for large values of β , following assumption can be made [Kaddoum *et al.*, 2012]

$$\mathbb{E} [s_{i,1}^2 + s_{i,2}^2 + \dots + s_{i,\beta}^2] \approx \mathbb{E} [s_{i+1,1+\beta}^2 + s_{i+2,2+\beta}^2 + \dots + s_{i+\beta,2\beta}^2] \approx 2\beta \mathbb{E} [s_l^2].$$

1.8 Modeling Dependence Among Random Variables

In literature, the Pearson correlation coefficient is mostly utilized to measure the linear relationship among the RVs. Besides this, another statistical method exists and is used to model and capture the complex relationships between multiple RVs in terms of dependence factors called the Copula approach.

1.8.1 Copula-based Approach

Copula was first investigated by Sklar in mathematical and statistical problems [Sklar, 1959]. Copula is a mathematical function that expresses the joint correlated multivariate distribution function or their PDFs into their individual marginal uniform distribution function or PDFs on the unit interval with some mutual dependency. Thus, Copula merges univariate PDFs to generate a joint PDF with a specific dependency structure. This copula-based method provides a high degree of flexibility in modeling and significantly reduces the computational load compared to other non-Copula based approaches. Additionally, Copula can capture both linear and non-linear dependence among the RVs. Furthermore, Copulas have been utilized in statistics, economics, survival analysis, image processing, machine learning, and a wide range of engineering applications [Nelsen, 2006].

Herein, we discuss one of the fundamental and essential theorems for Copula given by Sklar, also known as Sklar's theorem. According to the theorem, a Copula function establishes a relationship between related marginal PDFs and multivariate joint PDFs.

Theorem 1.1 (Sklar's theorem). *Let $F(\alpha_1, \alpha_2, \dots, \alpha_d)$ be a joint cumulative distribution function (CDF) of the RVs defined on $[0, 1]^d$ with their uniform univariate margins $F(\alpha_{d_1})$ for $d_1 = 1, 2, \dots, d$ over $[0, 1]$. Then, there exists a function in the real domain called Copula function $\mathbb{C}$ defined as*

$$F(\alpha_1, \alpha_2, \dots, \alpha_d) = \mathbb{C}(F(\alpha_1), F(\alpha_2), \dots, F(\alpha_d)). \quad (1.11)$$

Using the chain rule in (1.11), the corresponding joint PDF can be written as

$$\begin{aligned} f(\alpha_1, \alpha_2, \dots, \alpha_d) &= \frac{\partial^d \mathbb{C}(F(\alpha_1), F(\alpha_2), \dots, F(\alpha_d))}{\partial \alpha_1 \partial \alpha_2 \dots \partial \alpha_d} \\ &= \frac{\partial^d \mathbb{C}(F(\alpha_1), F(\alpha_2), \dots, F(\alpha_d))}{\partial F(\alpha_1) \partial F(\alpha_2) \dots \partial F(\alpha_d)} \times \prod_{d_1=1}^d \frac{\partial F(\alpha_{d_1})}{\partial \alpha_{d_1}} \\ &= \frac{\partial^d \mathbb{C}(F(\alpha_1), F(\alpha_2), \dots, F(\alpha_d))}{\partial F(\alpha_1) \partial F(\alpha_2) \dots \partial F(\alpha_d)} \times \prod_{d_1=1}^d f(\alpha_{d_1}) \\ &= \mathbb{C}_f(F(\alpha_1), F(\alpha_2), \dots, F(\alpha_d)) \times \prod_{d_1=1}^d f(\alpha_{d_1}). \end{aligned} \quad (1.12)$$

In (1.12), $\mathbb{C}_f(F(\alpha_1), F(\alpha_2), \dots, F(\alpha_d))$ represents the Copula density function and $f(\alpha_{d_1})$ denotes the marginal PDFs.

In literature, numerous types of Copulas have been proposed thus far. In this thesis, we utilize the Farlie-Gumbel-Morgenstern (FGM) Copula function to analyze the performance metrics of the proposed system model. This is because FGM Copula offers easy and fast modeling of correlated RVs and simple closed-form expressions. Additionally, FGM Copula describes the actual dependence between correlated RVs [Sriboonchitta and Kreinovich, 2018]. Several advantages of FGM Copula are discussed as follows:

1. **Simplicity and ease of use:** The FGM Copula is relatively easy and provides a simple mathematical form, making it easier to understand and apply than other Copulas. Due to its

simple structure, the FGM Copula requires fewer estimating parameters, which can simplify the estimation process and reduce computational complexity.

2. **Flexibility and modeling dependence:** The FGM Copula can model moderate levels of dependence between variables. This is useful in situations where the dependence is neither very weak nor very strong. The FGM Copula can capture both positive and negative dependence between variables and offers flexibility in various applications.
3. **Analytical tractability:** The FGM Copula often allows the formation of closed-form solutions, which simplifies analytical work and makes computations straightforward and less resource-intensive, which is beneficial for practical applications.
4. **Easy interpretability:** The parameters of the FGM Copula are generally easier to interpret than other Copula functions. The FGM Copula also provides a clear dependence structure among the random variables.

Despite the numerous advantages of the Copula-based method, Copula functions have been associated with some limitations, which are enumerated as follows:

1. **Model selection and specification:** Selecting the appropriate Copula model is complex and requires a deep understanding of the data sets and different Copula families. The process can be time-consuming and requires expertise. Incorrectly specifying the copula model can lead to inaccurate results and potentially misleading the interpretation of the dependence structure.
2. **Complexity with high dimensional data:** In Copula-based methods, as the number of variables increases, the complexity of modeling their joint distribution with Copulas increases exponentially. This leads to significant computational and estimation challenges. Estimating parameters for high-dimensional Copulas is difficult and computationally intensive.
3. **Tail dependence:** All Copula function can not effectively capture extreme co-movements (tail dependence) between variables. This is a significant drawback in fields like finance and risk management, where understanding tail dependence is crucial.

Despite these few limitations, copulas are extensively used in various fields due to their numerous advantages enlisted above.

1.9 Related Work

PLS has been extensively investigated in wireless communication scenarios. In recent years, PLS has attracted much attention from the PLC community due to its growing importance in data security. To this end, in [Pittolo and Tonello, 2013] and [Pittolo and Tonello, 2014], the authors have analyzed and compared the PLS performance of a single-input single-output (SISO) PLC system and a wireless system. It was found that the secrecy rate is lower in PLC systems than in wireless communication systems. In [Zhuang and Lampe, 2014], the PLS of a multi-input multi-output (MIMO) PLC system has been evaluated. Here, it was established that MIMO PLC is more secure than SISO PLC systems. The secrecy performance of a cooperative PLC system was investigated over correlated Log-normal communication channels in the presence of a passive eavesdropper in [Salem *et al.*, 2017].

In the past few years, PLC systems have been designed considering many traditional modulation schemes. Meanwhile, the DCSK modulation scheme has been introduced in PLC systems

Table 1.1: A comparison of the proposed work with existing works on PLC secrecy performance with channel correlation.

References	Channel gain	Modulation scheme	Channel correlation	ST Optimization	Performance metrics
A, Pittolo et al., 2013	Log-normal	BPSK	Pearson correlation coefficient	No	Secrecy rate
Y. Zhuang et al., 2014	Rayleigh	BPSK	Pearson correlation coefficient	No	Secrecy capacity
A. Salem et al., 2017	Log-normal	BPSK	Pearson correlation coefficient	No	ASC and SOP
Our Work (Chapter 2)	Log-normal	DCSK	Copula-based modelling	Yes	SOP, SPSC and ST

BPSK: Binary phase shift keying, **ST:** Secrecy Throughput

for its robustness. In [Kaddoum and Tadayon, 2017], the performance of DCSK systems over the multipath power line channel model was investigated in the presence of background, impulsive, and phase noise, where the authors concluded that the DCSK schemes perform better than direct sequence differential phase shift keying (DS-DPSK) and the direct sequence code division multiple access (DS-CDMA) schemes. Similarly, the authors in [Zheng *et al.*, 2017] analyzed the performance of M-ary DCSK (M-DCSK) with background, impulsive, and phase noises, over narrow-band PLC, where it was shown that M-DCSK outperforms direct sequence M-ary differential phase shift keying (DS-MDPSK). Further, the authors in [Zheng *et al.*, 2017] extended their work in [Miao *et al.*, 2020] where the replica piecewise (RP)-MDCSK system was designed and studied for PLC with asynchronous impulsive noise. Moreover, the authors demonstrated that RP-MDCSK has a significantly lower bit error rate (BER) than DCSK and DS-MDPSK.

Recently, Copula theory has been explored by researchers in the field of communication channel modeling [Huang *et al.*, 2015]. In [Gholizadeh *et al.*, 2015], the authors utilized the Copula method to obtain the capacity of a correlated ergodic MIMO channel over Nakagami- m fading, where three types of Copulas were used i.e., normal, Clayton, and t Copula for channel parameter estimation. In [Huang *et al.*, 2015], the authors computed a closed-form expression for the outage probability under cross-correlated Weibull fading using selection combining reception technique by exploiting the survival-Gumbel Copula approach. Similarly, the authors in [Mathur *et al.*, 2015] computed the average symbol error rate and average BER for PLC systems using a quadrature phase shift keying (QPSK) modulation scheme over Nakagami- m distributed additive background noise, wherein the Copula approach was used to analyze dependence among decision variables. Furthermore, the authors in [Ghadi and Hodtani, 2020] utilized the FGM Copula method to establish the closed-form expressions for the outage probability and coverage region over correlated Rayleigh fading multiple access channels. In [Ghadi and Hodtani, 2021], the authors analyzed the PLS performance of a correlated Rayleigh distributed wiretap fading channel, where closed-form expressions for the ASC, SOP, and secrecy coverage region (SCR) were derived using the FGM Copula approach.

1.10 Motivation

- Akin to wireless communication networks, it is important to develop robust, reliable, and trustworthy PLC communication networks for Industry 4.0 and IoT applications. PLC channels are natively ubiquitous, broadcast, and characterized by multipath propagation, because

Table 1.2: Literature summary of previously published relevant works on PLC secrecy performance considering single eavesdropper with the proposed work.

References	Channel gain	Modulation scheme	No. of Eaves-droppers	ST Opti-mization	Performance metrics
A, Pittolo et al., 2013	Log-normal	BPSK	Single	No	Secrecy rate
Y. Zhuang et al., 2014	Rayleigh	BPSK	Single	No	Secrecy capacity
A. Salem et al., 2017	Log-normal	BPSK	Single	No	ASC and SOP
Our Work (Chapter 3)	Log-normal	DCSK	Multiple	Yes	ASC, SOP, SPSC, and ST

Table 1.3: A difference between the proposed work with existing related works on PLC jamming and eavesdropping.

References	Channel gain	Modulation scheme	Scenario	Performance metrics
A, Pittolo et al., 2013	Log-normal	BPSK	Eavesdropping	Secrecy rate
Y. Zhuang et al., 2014	Rayleigh	BPSK	Eavesdropping	Secrecy capacity
A. Salem et al., 2017	Log-normal	BPSK	Eavesdropping	ASC and SOP
Y. Ai et al., 2017	Rayleigh	BPSK	Jamming	System capacity
V. Mohan et al., 2019	Log-normal	DCSK	Eavesdropping	ASC, SOP, and SPSC
V. Mohan et al., 2022	Log-normal	DCSK	Eavesdropping	ASC, SOP, and SPSC
Our Work (Chapter 4)	Log-normal	MPSK	Jamming	ASER, OP

of several branches and impedance mismatches. Thus, the channels are used by all users in the network, making it more susceptible to eavesdroppers and jammers. Therefore, secrecy becomes an essential issue in maintaining information confidentiality between the legitimate transmitters and receivers. Hence, it becomes crucial to analyze, explore, and investigate the security aspects of PLC systems for reliable deployment in Industry 4.0 and IoT networks.

- PLS is considered a promising technique that can offer an additional level of protection on top of the existing security schemes to safeguard the transmission of data. Among the Copula family, FGM Copula facilitates the easy statistical characterization of correlated joint distribution and shows the actual correlation among them. Further, the DCSK modulation technique offers unique advantages over other conventional modulation techniques. These facts motivate us to investigate PLS performance of the PLC system by employing FGM Copula and DCSK modulation technique.

- In [Pittolo and Tonello, 2013, 2014], [Zhuang and Lampe, 2014], [Salem *et al.*, 2017], the authors investigated the PLS performance of the PLC systems where the authors employed BPSK modulation and a non-Copula based approach was utilized to characterize the correlation between the RVs. However, the explicit closed-form expressions and secrecy throughput optimization were not evaluated. To address these research gaps, we propose the DCSK-based PLC system where the DCSK modulation technique aids in improving the secrecy and the Copula-based method eases the numerical analysis of the considered PLC system. Further, an optimization problem is formulated in terms of secrecy throughput. Likewise, the authors in [Pittolo and Tonello, 2013, 2014], [Zhuang and Lampe, 2014], [Salem *et al.*, 2017] analyzed the PLS performance of the considered PLC systems against only single eavesdropper scenario, wherein multiple eavesdroppers were not considered and secrecy throughput optimization was not reported. Therefore, we examine the PLS performance of the DCSK-based PLC systems under multiple eavesdroppers scenario and we also propose an algorithm for maximizing the secrecy throughput.
- Similarly, in [Kaddoum and Tadayon, 2017], [Zheng *et al.*, 2017], and [Miao *et al.*, 2020], the BER performance of the PLC systems employing DCSK and M-ary DCSK modulation techniques, respectively, was analyzed. However, in this thesis, we incorporate the DCSK modulation technique to study the PLS performance of the PLC communication systems.
- Finally, in [Pittolo and Tonello, 2013, 2014], [Zhuang and Lampe, 2014], [Salem *et al.*, 2017], overall PLC system performance was evaluated by considering only eavesdropping scenario. There is a dearth of published research on PLC network jamming except [Ai *et al.*, 2017]. The authors in [Ai *et al.*, 2017] analyzed the PLC system performance in the presence of a jamming attack by utilizing Bayesian game theory where the Bayesian Nash equilibrium of the game is derived. Inspired by this research gap, in this thesis, we explore and study the impact of random pulse jammer on PLC systems performance over Log-normal fading channel gain with Bernoulli-Gaussian additive noise. Herein, the series-based expressions of average symbol error rate (ASER) and outage probability (OP) are derived.

In Table 1.1-1.3, we have presented the comparison of our works with existing works in literature.

1.11 Key Contributions and Novelty

The principal contributions and novelty of our thesis work are encapsulated as follows:

- We investigate the PLS performance of a DCSK-based PLC system by utilizing a novel FGM Copula approach, where a wiretap power line channel model is analyzed to compute the secrecy between the main channel and the wiretap channel. Both PLC channels are considered to be Log-normally distributed and correlated, and the Bernoulli-Gaussian model characterizes the PLC channel noise. The PLS performance is numerically expressed in terms of SOP and SPSC. To obtain useful insight into the PLC system, the asymptotic SOP analysis is conducted. Furthermore, an algorithm is presented to maximize the secrecy throughput under SOP constraints.
- We anatomize the PLS performance of a PLC system by considering the DCSK modulation scheme in the presence of multiple eavesdroppers. A wiretap power line channel model is examined to measure the secrecy between the main channel and the eavesdropper channels, where the main channel and eavesdropper channels are subjected to Log-normally distributed channel gain. Concurrently, PLC channel noise is modeled by the Bernoulli-Gaussian process. Further, the complete study of the PLS of the PLC system is expressed in terms of ASC, SOP, and SPSC. Besides, to obtain useful insights into the PLC system, an algorithm is proposed

to maximize the secrecy throughput under security and reliability constraints. Moreover, an asymptotic SOP analysis and some special cases have been discussed.

- Finally, we evaluate the performance of the considered PLC system in the presence of a random jammer, wherein, subjected to the state of the jammer, we compute the PDF of the instantaneous signal-to-jamming-plus-noise ratio (SJNR) and the instantaneous SNR. Utilizing the statistical characterization of the SJNR and SNR, we derive the series-based expressions of the ASER and OP of the considered PLC system. Additionally, the asymptotic ASER analysis is performed in terms of the coding gain and diversity order in the high SNR regime. In order to gain more insights into ASER and OP analysis of the considered PLC system, we demonstrate the effect of the different system parameters through the numerical results.

1.12 Organization of Thesis

The thesis comprises a total of five chapters. A concise overview of the research works discussed in each chapter is provided in the following summary:

Chapter 1: This chapter provides an overview of PLC systems, including their classification, benefits, applications, technical challenges, channel modeling for PLCs, and the classification and modeling of noise in PLCs. In addition, we explore the concepts of PLS, Copula theory, and DCSK modulation. A concise summary of the related work, motivation, and key contributions and novelty are mentioned in Chapter 1.

Chapter 2: In Chapter 2, we study the PLS performance of PLC systems by employing the DCSK modulation technique, where the PDF of SNR of the main and eavesdropper channel is computed by utilizing the FGM Copula-based approach. After that, the detailed secrecy analysis of the proposed PLC system has been done in terms of SOP and SPSC. Moreover, Chapter 2 covers the asymptotic analysis of the SOP and the secrecy throughput optimization. Finally, we illustrate and discuss the numerical results.

Chapter 3: This chapter deals with the PLS performance of the DCSK-based PLC systems in the presence of multiple eavesdroppers. The PLS performance is evaluated in terms of derived closed-form expressions of ASC, SOP, and SPSC by assuming two cases: 1) when all the channels are assumed to be independent and identically distributed (IID) following Log-normal distribution; and 2) the wiretap channels are considered to be identical but correlated Log-normally distributed and independent of the main channel. We present an algorithm to maximize the secrecy throughput for the considered PLC system under correlated SOP constraints in Chapter 3. Additionally, this chapter includes important insights by investigating some special cases and observing the impact of various system parameters through the numerical results.

Chapter 4: In this chapter, we focus on the impact of a random pulse jammer on the considered PLC system, where both the main and jammer channels are assumed to follow Log-normal distribution with additive Bernoulli-Gaussian noise. Conditioned upon the jammer's state, we compute the PDF of the instantaneous SJNR and the instantaneous SNR. Capitalizing on the statistical characterization of the SJNR and SNR, we derive the series-based expressions of the ASER and OP for the considered PLC system. Further, Chapter 4 includes asymptotic ASER study and numerical results and discussion.

Chapter 5: This chapter presents the findings and conclusions derived from our research works. Additionally, it also outlines the areas for further research and describes the possible

extensions to this work.