Jamming Detection in Power Line Communications Leveraging Deep Learning Techniques

Muhammad Irfan[1], Aymen Omri[2], Javier Hernandez Fernandez[2], Savio Sciancalepore[3], and Gabriele Oligeri[1]

[1]Division of Information and Computing Technology (ICT), College of Science and Engineering (CSE),
Hamad Bin Khalifa University (HBKU), Doha, Qatar; {muir45306, goligeri}@hbku.edu.qa
[2]Iberdrola Innovation Middle East, Doha, Qatar; {aomri, j.hernandezf}@iberdrola.com
[3]Eindhoven University of Technology, Eindhoven, Netherlands; s.sciancalepore@tue.nl

***Abstract*—[1]Power Line Communications (PLC) is a well-established technology that allows devices connected to the power line to communicate with each other. While the majority of research in this field is devoted to issues of availability, the topic of Denial of Service (DoS) attacks has not been sufficiently addressed. Typically, current solutions might detect a jammer when situated near the target devices, yet the equipment under jamming interference may face challenges in communicating an alarm. However, when these systems are placed at a significant distance from the jammer, the negligible impact of the jamming renders its detection hardly detectable. In this work, we propose a solution to identify the presence of a jammer in a PLC infrastructure even when deployed at a significant distance. We analyze the physical layer of the PLC link and adopt state-of-the-art Deep Learning techniques to detect jamming even at a distance where the jammer's effect is negligible, thus allowing the device to trigger an alarm. Considering a jammer featuring the same transmission power as legitimate devices, we prove that we can detect the presence of such a jammer with an overwhelming probability (higher than 0.99) even at a distance of 75 m from the source.**

***Index Terms*—PLC Security; Physical-Layer Security; Artificial Intelligence for Security.**

I. Introduction

Power Line Communications (PLC) enables data exchange over existing power cables, thus leveraging an already widespread infrastructure and making it an efficient solution for applications such as Smart Grids (SGs) [1]. There are two main types of PLC [2]: Broadband and Narrowband. Broadband PLC operates at higher frequency ranges and can achieve data rates of hundreds of Mbps, thus being used for high-speed Internet access and multimedia streaming applications. Conversely, narrowband PLC operates at lower frequencies and are characterized by lower data rates, thus being a better fit for applications such as smart metering and SG management [3]. PLC technology is a building block for the development of SG, a key component of future sustainable energy systems. It also plays a crucial role in creating home automation networks, allowing devices to communicate with each other and the Internet through power lines. Being such a widely deployed network, PLC eliminates the need to install new wired networks for data transmission.

Although being a promising technology, PLC is affected by several challenges, such as signal attenuation [4], noise [5], and interference—the power line medium was originally intended for power transmission [2], not for data communication. Nevertheless, significant advancements have been made to improve its reliability and efficiency, making PLC a promising solution for various communication needs [3]. Given their central role in critical infrastructures, enforcing PLC security becomes paramount. A major challenge in PLC comes from Denial of Service (DoS) attacks, i.e., a set of (malicious) techniques to prevent data exchange between two parties. Among the various DoS attacks, one of the most effective is jamming, i.e., the injection of noise into the communication medium in order to prevent the receiver from discriminating and retrieving the legitimate signal. Jamming is usually identified as a physical-layer attack since the jamming signal may be unstructured—no modulation—thus involving simple hardware architectures. On the contrary, jamming is extremely successful, effectively preventing data exchange between two parties. Such attacks are particularly detrimental in several application scenarios characterized by sensing and controlling. Typical examples involve a temperature sensor that raises an alarm or a remote command from the control center to open/close a valve in emergency situations. Detecting jamming attacks is particularly important, although it involves several challenges. Firstly, a smart adversary might inject a non-modulated signal statistically similar to the noise already present in the PLC link, making detection harder. Moreover, when a powerful jamming signal is injected into the PLC infrastructure, all communications are shut down, making reporting the jamming detection event challenging. Standard jamming detection techniques, e.g., the ones resorting to communication metrics such as Signal-to-Noise Ratio (SNR), Bit-Error Rate (BER), and packet-error rate become unreliable, or even, unavailable in some specific scenarios. Indeed, when a jammer is deployed, the previous metrics cannot distinguish between a communication line failure and an attack.

Contribution. This work focuses on detecting jamming signals in PLC systems at the physical layer of the PLC link. We combine state-of-the-art Deep Learning (DL) techniques with information extracted from the physical layer of the power line. We propose an innovative technique to convert

[1]Personal copy of the authors. Not for redistribution.

physical layer information (I-Q samples) into images, and subsequently use these images as input of a Convolutional Neural Networks (CNN). We prove that this technique is effective for jamming detection (accuracy higher than 0.99) when other solutions based on higher layer metrics simply fail (BER equal to zero).

Roadmap. The rest of this paper is organized as follows. Sec. II surveys the most important works from the literature, Sec. IV illustrates our scenario, system, and adversary model, motivating the importance of jamming detection in PLC, Sec. IV outlines the methodology to generate data and apply our solution, Sec. V reports the results associated with our analysis, Sec. VI discusses the impact and limitations of our contribution, and finally, Sec. VII tightens the conclusions.

II. Related Work

Cyber-physical or Operational Technology (OT) attacks refer to attacks carried out on control operations of SGs. Such attacks may disrupt the corresponding networks' confidentiality, integrity, and availability [6]. Attacks on the availability aim to stop access to the service, e.g., via time delay, jamming, and other forms of DoS [7]. Security services in PLC networks are usually provided using cryptographic techniques implemented at higher layers. Different methods have been designed to protect the PLC at the physical layer, such

as [8], [9], [10]. Prasad *et. al.* [10] proposed physical layer security for MIMO broadband PLC in-band full-duplex jamming, showing that the eavesdropper's decoding performance is degraded and the secrecy rate is maximized. Shafie *et. al.* [9] introduced artificial noise between legitimate communicating devices. A low channel-to-noise signal (CNR) is sent from the receiver to the sender and, in response, gets an amplified CNR at each OFDM sub-channel.

In the context of jamming detection for SGs, Gai *et.al.* [11] proposed a *Maximum Attacking Strategy using Jamming and Spoofing* technique to interrupt operations of cognitive radio networks in wireless SG networks. Kurt *et. al.* [12] investigated two different attack models for SGs, and they investigated the injection of Additive White Gaussian Noise (AWGN) to the communication channel to compromise a subset of meters. They employed CUSUM-based detectors to detect such types of attacks. Shin *et. al.* [13] proposed a counter-measure against reactive jamming attacks for low-cost resource-constrained devices in SG, involving isolating the compromised node. Neural networks are widely used for applications such as image classification, speech recognition, malware analysis, health care, and recommendation systems. Various types of neural networks have been proposed; CNN [14] is famous for classification tasks such as compiler optimization level recognition [15][16], weather classification [17], jamming detection and identification [18]. However, to the best of our knowledge, jamming detection in PLC networks through DL techniques has not been investigated at the time of this writing.

III. Reference Scenario and Motivation

Fig. 1 depicts our reference scenario and adversary model, characterized by three entities, namely, Alice ($\mathcal{A}$), Bob ($\mathcal{B}$), and Eve ($\mathcal{E}$). Our scenario considers a standard PLC network constituted by a house where different devices, e.g., $\mathcal{A}$ and $\mathcal{B}$, communicate via the power line medium. This work focuses on the challenges associated with availability: a malicious entity ($\mathcal{E}$) would like to stop communication between $\mathcal{A}$ and $\mathcal{B}$, thus deploying techniques to implement a Denial of Service (DoS) attack.

DoS attacks in PLC can have a significant impact, given the critical nature of many services that depend on such systems. In the following, we summarize some potential objectives of an adversary carrying out such attacks.

- *Disruption of Energy Services.* Energy distribution management is a critical component of SG systems; thus, preventing the associated communications could disrupt these services, leading to a power outage.
- *Interruption of Communications.* Power lines are not as broadcast as the wireless medium; DoS attacks, while having the same complexity, can be much more disruptive in PLC networks. DoS attacks could potentially interrupt PLC communications over a wide area, affecting different industries and services, e.g. including Internet Service Providers (ISPs) and public safety communications.
- *Impact on Home Automation.* Many home automation systems use PLC technologies for inter-device communications. DoS attacks can potentially disrupt these systems, causing inconvenience to homeowners and potentially compromising safety systems.
- *Financial consequences.* Similar to other scenarios, interruptions in PLC can lead to financial losses. Industries relying on PLC for operations might face downtime, thus losing productivity and revenues, and requiring additional costs to harden the systems for future attacks.
- *Safety Risks.* PLC systems might be adopted for supporting safety-critical tasks in critical infrastructures, e.g., traffic light coordination and hospital power systems. DoS attacks in this scenario can lead to risks for people's safety.

In our scenario, $\mathcal{E}$ is performing a jamming attack, by injecting a signal into the PLC network with the aim of disrupting the communication between $\mathcal{A}$ and $\mathcal{B}$. With reference to the PLC wiretap channel model illustrated in Fig. 2, $h_{\mathcal{A}-\mathcal{B}}$ and $h_{\mathcal{E}-\mathcal{B}}$ are the complex channel gains of the link $\mathcal{A}$-$\mathcal{B}$ and the link $\mathcal{E}$-$\mathcal{B}$, respectively, while $n_{\mathcal{B}}$ is the corresponding additive white Gaussian noise. Accordingly, the instantaneous signal-to-noise-ratio (SNR) at $\mathcal{B}$, can be expressed as in Eq. 1.

$$\gamma_{\mathcal{A}-\mathcal{B}} = \frac{P_T \, H_{\mathcal{A}-\mathcal{B}}}{P_J \, H_{\mathcal{E}-\mathcal{B}} + N_{\mathcal{B}}}, \tag{1}$$

where, P_T is the transmit signal power, P_J is the jamming signal power, $H_{X-\mathcal{B}}$ is the squared magnitude value of the complex channel gain $h_{X-\mathcal{B}}$, $X \in \{\mathcal{A}, \mathcal{E}\}$, and $N_{\mathcal{B}}$ is the corresponding noise power.

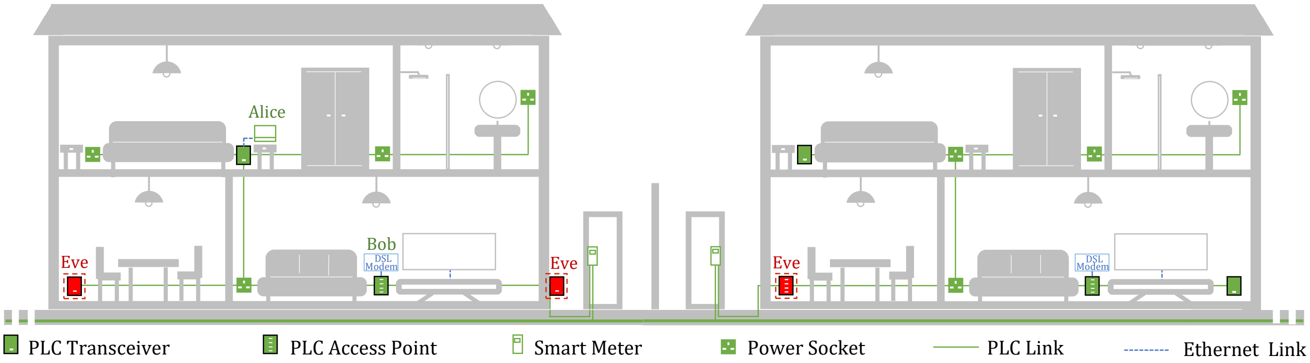

Fig. 1. An example of a broadband in-home PLC system, where $\mathcal{A}$ and $\mathcal{B}$ exchange PLC signals in the presence of a PLC jammer device ($\mathcal{E}$).

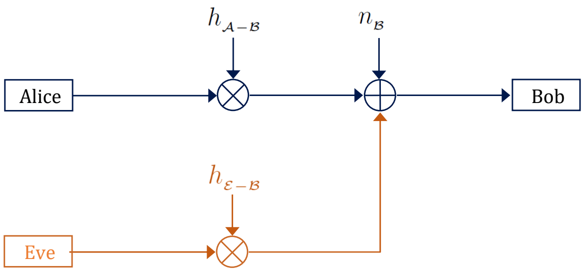

Fig. 2. Block diagram of the PLC wiretap channel model.

We consider the PLC channels to be Rayleigh fading channels, in line with the corresponding literature [19], [20], [21], with the associated probability density function (PDF) modeled according to Eq. 2.

$$f_{H_{X-\mathcal{B}}}(x) = \frac{1}{\bar{H}_{X-\mathcal{B}}(F_C, d_{X-\mathcal{B}})} \exp\left(\frac{-x}{\bar{H}_{X-\mathcal{B}}(F_C, d_{X-\mathcal{B}})}\right), \tag{2}$$

where, $\bar{H}_{X-\mathcal{B}}(F_C, d_{X-\mathcal{B}})$ is the mean of $H_{X-\mathcal{B}}$, which models the average frequency-distance dependent PLC channel attenuation, F_C is the carrier frequency, and $d_{X-\mathcal{B}}$ is the distance associated with the $X - \mathcal{B}$ link. According to [21], $\bar{H}_{X-\mathcal{B}}(F_C, d_{X-\mathcal{B}})$ can be expressed as in Eq. 3.

$$\bar{H}_{X-\mathcal{B}}(F_C, d_{X-\mathcal{B}}) = \exp\Big(-2\left[a_0 + a_1\, F_C^{a_2}\right] d_{X-\mathcal{B}}\Big). \tag{3}$$

where, a_0, a_1, and a_2 are PLC signal attenuation parameters related to the PLC environment.

Table I summarizes the main notation used in this manuscript and the values associated with the various parameters.

IV. Methodology

In this section, we describe the methodology adopted to detect the presence of a jammer in a PLC system. The core of our solution involves translating the received signals (I-Q samples) into images, and then, exploiting state-of-the-art solutions for image classification in order to detect which images (and correspondingly, I-Q samples) are affected by jamming.

TABLE I
Notation, description, and analyzed values.

Parameter	Notation	Value
Transmit Power [dBμV]	P_T	120
Noise Power [dBμV]	P_N	70
Nbr. of SC per OFDM Symbol	N_{SC}	512
FFT Nbr.	N_{FFT}	512
Carrier Frequency [Hz]	F_c	20e6
Sub-Carrier spacing [Hz]	Δ_f	15e3
Nbr. of OFDM Symbols per Frame	N_{Symb}^{Frm}	20
Sampling Time [s]	T_{samp}	$1/(2 \times F_c)$
OFDM Symbol Duration [s]	T_{Symb}	$N_{FFT} \times T_{samp}$
Frame Duration [s]	T_{Frame}	$N_{Symb}^{Frm} \times T_{Symb}$
Total Nbr. of Frames	N_{Frame}	$\lceil T_{Sim}/T_{Frame} \rceil$
Total Nbr. of OFDM Symbols	N_{Symb}	$N_{Frame} \times N_{Symb}^{Frm}$
Distance $\mathcal{A}$-$\mathcal{B}$ [m]	$d_{\mathcal{A}-\mathcal{B}}$	30
Distance $\mathcal{E}$-$\mathcal{B}$ [m]	$d_{\mathcal{E}-\mathcal{B}}$	30
Simulation time [s]	T_{Sim}	2

Signal processing. Without loss of generality, in this work we consider the reference modulation scheme BPSK, i.e., Binary Phase Shift Keying. Accordingly, bit values $\{0, 1\}$ are modulated by changing the phase of a reference frequency f_0 (carrier), i.e., when $b = 0$, the phase ϕ becomes $\phi = 0$, while when $b = 1$, $\phi = \pi$, where b represent the bit to be transmitted, as depicted by Eq. 4.

$$x(t) = \cos\left(2\pi f_0 t + \phi\right), \tag{4}$$

where, $x(t)$ is the PLC frequency signal to be transmitted. BPSK modulation becomes straightforward when considering the complex representation of Eq. 4. Indeed, when considering the complex I-Q plane, BPSK modulation involves a null imaginary component ($Q = 0$) and a real component I equals to $\{-1, 1\}$ as a function of the phase ϕ value, i.e., either 0 or π. According to this representation, each bit value can be mapped in the I-Q plane as per Eq. 5.

$$\begin{aligned} b = 0 &\rightarrow Q = 0, I = 1 \\ b = 1 &\rightarrow Q = 0, I = -1 \end{aligned} \tag{5}$$

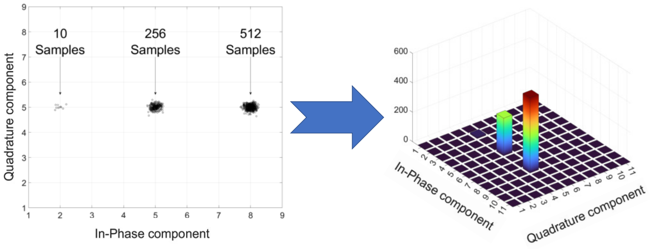

Fig. 3. The I-Q samples are translated into pixel values by estimating their density through a bi-variate histogram.

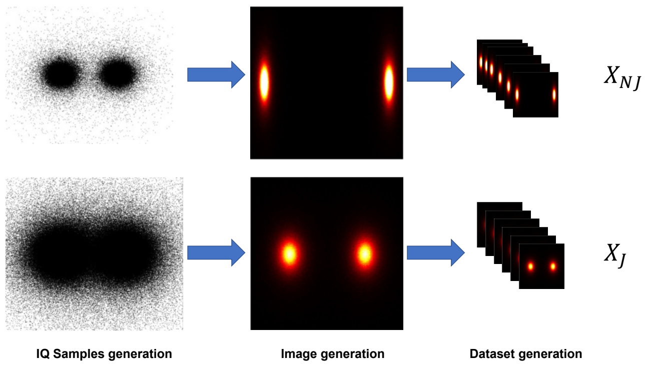

Fig. 4. I-Q samples are converted to images, which in turn are organized into two datasets, i.e., X_{NJ} and X_J.

Our solution's preliminary step involves converting I-Q samples into images. Many solutions have already been proposed to generate red-green-blue (RGB) images from I-Q samples [22], [23], [18], and in the following, we re-adapt state-of-the-art solutions in order to maximize performance in our use case. Based on empirical considerations, we consider $1,597,440$ I-Q samples per image and a total number of 1500 images for each experiment (750 jamming and 750 no-jamming). Figure 3 summarizes the overall process. The I-Q plane is split into tiles, i.e., 224×224, and then, a bi-variate histogram is computed. For each tile, we compute the number of I-Q samples and, in turn, we map such a number into a pixel value. As a toy example, Fig. 3 shows three clouds of I-Q samples with 10, 256, and 512 samples, placed on three different tiles at positions $[2, 5]$, $[5, 5]$, and $[8, 5]$. We highlight that the position of the clouds is not meaningful and we chose such positions for the sake of clarity. The bi-variate histogram counts the number of I-Q samples per tile, i.e., 10, 256, and 512, respectively, and the output is considered as the value of a pixel in the image. Thus, assuming h is the output of the bi-variate histogram, the pixel coordinates p_R, p_G, and p_B will be:

- $0 \leq h \leq 255$, then $p_R = 0, p_G = 0, p_B = h$,
- $256 \leq h \leq 511$, then $p_R = 0, p_G = h - 255, p_B = 255$,
- $h > 511$, then $p_R = h - 510, p_G = 255, p_B = 255$.

Finally, we observe that if $h > 767$, the output is clipped—this issue can be controlled by properly adjusting the number of samples in the I-Q plane, as previously discussed. Figure 4 summarizes the image generation process. We generate I-Q samples according to the model proposed in Section III, we convert the I-Q samples into images, and finally, we generate two *datastores* of images, i.e., X_J and X_{NJ}, including images from the jammed and not-jammed communication links, respectively.

Deep Learning. The datastores X_J and X_{NJ} are now considered for the classification process. We split each datastore X_y with $y \in \{J, NJ\}$ into three subsets of sizes 0.6, 0.2, and 0.2, compared to the original one, i.e., $\mathcal{T}, \mathcal{V}, \mathcal{S}$, which are considered for training, validation, and testing, respectively. We consider a state-of-the-art DL classifier (CNN), based on a Residual Network (Resnet-18) and Inception-v3 already implemented in MatLab2022b. The neural network models are pre-trained with images from the ImageNet database [24], thus requiring some modifications. Firstly, the input layers have been adapted in order to fit the output of the bi-variate histogram (image size), i.e., 224×224, while the output layer has been changed to fit the number of classes of our problem, i.e., *Jamming* and *No Jamming*. Finally, the model has been (partially) re-trained in order to include the features of the images generated from the I-Q samples.

V. Performance Analysis

We start our analysis by considering the model from Fig. 2. We set a distance between the transmitter ($\mathcal{A}$) and the receiver ($\mathcal{B}$) of 30 m. Moreover, we set the distance between $\mathcal{E}$ (Jammer) and $\mathcal{B}$ as varying between 5 and 60 m, as depicted in Fig. 5. Moreover, we consider different (relative) jamming transmission power spanning between 0.1 and 1. The relative jamming power is computed as a fraction of the transmission power of $\mathcal{A}$ (120 dBμV). Figure 5 shows the BER as a function of the distance between $\mathcal{E}$ and $\mathcal{B}$. We identify a theoretical boundary, i.e., jamming power equal to 1—solid red line, which highlights the scenario where the jammer adopts the same transmission power of the legitimate transmitter. While we acknowledge that the jamming power can be arbitrarily large, by setting the same transmission power as the legitimate transmitter, we identify the case of an adversary using the same hardware as the legitimate one—this being the case of an adversary using the same commercial devices or being able to control one of the devices already deployed. It is worth noting that when the relative jamming power is 1, and the jammer is at the same distance as the legitimate transmitter, the BER is 0.15. Moreover, we observe that the jamming power significantly affects the BER, i.e., reducing the jamming power makes the BER smaller independently of the distance between the jammer and the receiver. Finally, it is worth mentioning that, given the considered parameters, the jammer affects the receiver up to a distance of 50 m when the relative jamming power is smaller than 1, i.e., less or equal

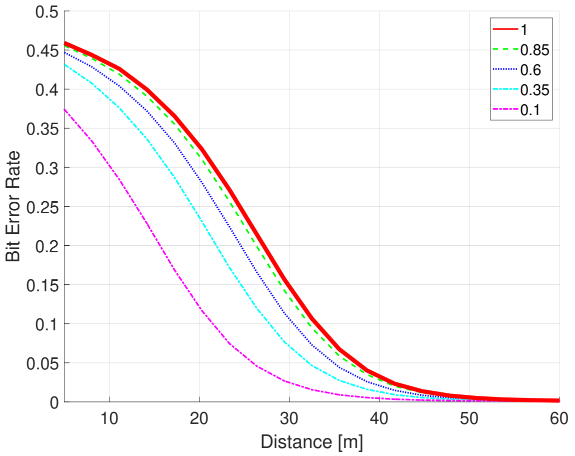

Fig. 5. Bit-Error Rate as a function of the distance between the jammer and the receiver. The jamming power is relative to the transmission power.

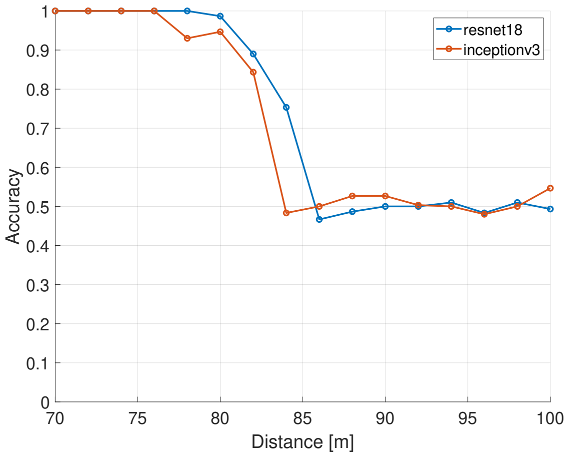

Fig. 6. Accuracy as a function of the distance between the jammer and the receiver assuming the jammer and the legitimate transmitting device feature the same transmission power.

to the power of the legitimate transmitter. This is a critical distance for standard detection techniques based on higher layer jamming detection metrics such as the SNR and BER. Indeed, when the jammer is placed at a given location, all devices in the neighborhood (less than 50 m) can potentially detect its presence, but they cannot communicate it, as the power line medium is jammed. Conversely, the devices far away from the jammer (at a distance larger than 50 m) cannot detect its presence since the BER is close to zero, and the associated metrics do not allow to infer the presence of the jammer. Our solution is specifically designed to detect the presence of a jammer far away from its location, i.e., when the distance between the receiver and the jammer is greater than 50 m. We consider the scenario where the jamming power equals the transmission power of the legitimate device. Figure 6 shows the results associated with the proposed classifier while varying the distance between the jammer and the receiver from 70 to 100 m. Our results show that the jammer can be identified with overwhelming probability (> 0.99) when the distance between the jammer and the receiver is less than 75 m. Both the considered neural networks (*resnet18* and *inceptionv3*) behave similarly, although *resnet18* is slightly more robust to the channel noise when the distance is larger than 75 m. Finally, Fig. 7 shows the accuracy of our solution when the distance between the jammer and the receiver is set to 70 m, and the relative jamming power spans between 0 and 0.5, i.e., between no jamming and half of the power of the legitimate transmitter. Figure 7 shows that our solution can detect with overwhelming probability (> 0.95) the presence of a jammer in this cenario when its relative transmitting power is higher than 0.2. As in the previous case, both neural networks have similar performance, although *resnet18* is more robust to channel noise (and jamming).

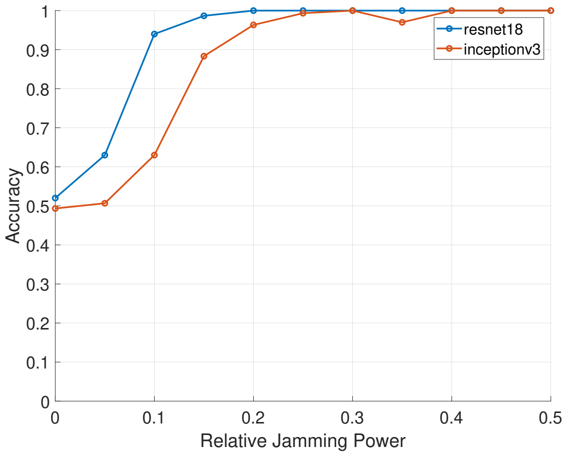

Fig. 7. Accuracy as a function of the jamming power, expressed as the relative fraction with respect to the source ($\mathcal{A}$). We assume the distance between the jammer ($\mathcal{E}$) and the receiver ($\mathcal{B}$) is 70 m.

VI. Discussion

PLC is gaining traction in several application scenarios, thus becoming a concrete alternative to Ethernet and wireless for data communications. Nevertheless, jamming a PLC link is as easy as for the wireless but with the same detrimental impact of the wired infrastructure—the receiving devices are connected to the power line, and contrary to the wireless scenario, they might have limited options to mitigate the attack. Jamming detection has received much attention in the RF scenario, while only a few contributions focused on PLC systems. Our work highlights the limitations of current solutions while shedding light on future challenges. Detecting jamming in PLC systems is difficult since the main objective of the jammer is to prevent communications. Therefore, even assuming the PLC devices can detect the presence of a jammer, they cannot communicate it (via the same PLC infrastructure), thus precluding an effective response. Our solution goes beyond the classical jamming detection approaches, providing a methodology to detect the presence of a jammer at a location where the jammer does not impact the current state of the power line (BER close to zero). Under this assumption, each PLC device can monitor the current state of the medium and infer the presence of a jammer from a high distance (about 80 m). We highlight that, while model generation (training/validation) is intense, testing can be performed even by resource-constrained devices, thus allowing any device being able to collect I-Q samples from the power line to detect the presence of a jammer. Also, the time to gather I-Q samples necessary for jamming detection is very limited (sampling time of $1/(2 \times F_c) = 0.025$ s). Our solution is particularly suitable for scenarios where the jammer is deployed in a target infrastructure, and a set of monitoring devices are in close proximity. As a toy example, recalling Fig. 1, wherever the jammer (Eve) will be deployed will affect the devices in close proximity, e.g., the devices belonging to the same building, but all the devices far away from the jammer will be able to detect its presence, thus triggering alarms and countermeasures.

VII. Conclusion and Future Work

We have proposed a Deep-Learning based approach to detect jamming in a PLC system when the distance between the jammer and the receiver is significant (up to 75 m) while the associated BER is almost zero. While standard solutions based on BER simply fail, our solution can detect the presence of a jammer with a probability greater than 0.99. Given the potential impact of jamming in PLC systems, we believe that our solution, which combines I-Q samples converted into images and CNNs, paves the way for future research in the area. In the future, we plan to apply our solution to an actual PLC deployment.

Acknowledgments

This publication was supported by the NPRP grant NPRP12C-0814-190012-SP165 from the Qatar National Research Fund (a member of Qatar Foundation), and Iberdrola S.A. as part of its innovation department research studies. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of Iberdrola Group.

References

[1] C. Cano, A. Pittolo, D. Malone, L. Lampe, A. M. Tonello, and A. G. Dabak, "State of the Art in Power Line Communications: From the Applications to the Medium," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 7, pp. 1935–1952, July 2016.

[2] L. Lampe, A. Tonello, and T. Swart, *Power Line Communications: Principles, Standards and Applications from Multimedia to Smart Grid*, John Wiley & Sons, 2016.

[3] M. Caprolu, J. Hernandez Fernandez, A. Alassi, and R. Di Pietro, "Increasing renewable generation feed-in capacity leveraging smart meters," in *2020 IEEE Green Energy and Smart Systems Conference (IGESSC)*, 2020, pp. 1 – 7.

[4] Javier Hernandez Fernandez, Aymen Omri, and Roberto Di Pietro, "Power Grid Surveillance: Topology Change Detection System Using Power Line Communications," *International Journal of Electrical Power & Energy Systems*, vol. 145, 2022.

[5] Javier Hernandez Fernandez, Aymen Omri, and Gabriele Oligeri, "A Noise Reduction Scheme for OFDM NB-PLC Systems," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 2, 2022.

[6] Muhammad Nouman Nafees, Neetesh Saxena, Alvaro Cardenas, Santiago Grijalva, and Pete Burnap, "Smart grid cyber-physical situational awareness of complex operational technology attacks: A review," *ACM Computing Surveys*, vol. 55, no. 10, pp. 1–36, 2023.

[7] Muhammed Zekeriya Gunduz and Resul Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer networks*, vol. 169, pp. 107094, 2020.

[8] A. Pittolo and A. M. Tonello, "Physical Layer Security in PLC Networks: Achievable Secrecy Rate and Channel Effects," in *2013 IEEE 17th International Symposium on Power Line Communications and Its Applications*, 2013, pp. 273–278.

[9] Ahmed El Shafie, Mohamed F Marzban, Rakan Chabaan, and Naofal Al-Dhahir, "An artificial-noise-aided secure scheme for hybrid parallel plc/wireless ofdm systems," in *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–6.

[10] Gautham Prasad, Omid Taghizadeh, Lutz Lampe, and Rudolf Mathar, "Securing mimo power line communications with full-duplex jamming receivers," in *2019 IEEE International Symposium on Power Line Communications and its Applications (ISPLC)*. IEEE, 2019, pp. 1–6.

[11] Keke Gai, Meikang Qiu, Zhong Ming, Hui Zhao, and Longfei Qiu, "Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2431–2439, 2017.

[12] Mehmet Necip Kurt, Yasin Yılmaz, and Xiaodong Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 498–513, 2018.

[13] Incheol Shin and Minkyoung Cho, "On localized countermeasure against reactive jamming attacks in smart grid wireless mesh networks," *Applied Sciences*, vol. 8, no. 12, pp. 2340, 2018.

[14] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton, "Imagenet classification with deep convolutional neural networks," *Communications of the ACM*, vol. 60, no. 6, pp. 84–90, 2017.

[15] Shouguo Yang, Zhiqiang Shi, Guodong Zhang, Mingxuan Li, Yuan Ma, and Limin Sun, "Understand code style: Efficient cnn-based compiler optimization recognition system," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019, pp. 1–6.

[16] Davide Pizzolotto and Katsuro Inoue, "Identifying compiler and optimization options from binary code using deep learning approaches," in *2020 IEEE International Conference on Software Maintenance and Evolution (ICSME)*. IEEE, 2020, pp. 232–242.

[17] Mohamed Elhoseiny, Sheng Huang, and Ahmed Elgammal, "Weather classification with deep convolutional neural networks," in *2015 IEEE international conference on image processing (ICIP)*. IEEE, 2015, pp. 3349–3353.

[18] Saeif Alhazbi, Savio Sciancalepore, and Gabriele Oligeri, "Bloodhound: Early detection and identification of jamming at the phy-layer," in *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*, 2023, pp. 1033–1041.

[19] A. Mathur, M. R. Bhatnagar, and B. K. Panigrahi, "PLC Performance Analysis Over Rayleigh Fading Channel Under Nakagami-m Additive Noise," *IEEE Communications Letters*, vol. 18, no. 12, pp. 2101 – 2104, Dec. 2014.

[20] C. Abou-Rjeily, "Power Line Communications Under Rayleigh Fading and Nakagami Noise: Novel Insights on the MIMO and Multi-Hop Techniques," *IET Communications*, vol. 12, no. 2, pp. 184 – 191, 2018.

[21] Y. Ai and M. Cheffena, "Capacity Analysis of PLC over Rayleigh Fading Channels with Colored Nakagami-m Additive Noise," in *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, Sep. 2016, pp. 1–5.

[22] Saeif Alhazbi, Savio Sciancalepore, and Gabriele Oligeri, "The day-after-tomorrow: On the performance of radio fingerprinting over time," in *39th Annual Computer Security Applications Conference 2023*, 2023.

[23] Gabriele Oligeri, Savio Sciancalepore, Simone Raponi, and Roberto Di Pietro, "PAST-AI: Physical-layer authentication of satellite transmitters via deep learning," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 274–289, 2023.

[24] O. Russakovsky et al., "ImageNet Large Scale Visual Recognition Challenge," *Int. Jour. of Comp. Vision*, vol. 115, no. 3, pp. 211–252, 2015.