Machine Learning Based Physical-Layer Intrusion Detection and Location for the Smart Grid

Gautham Prasad, Yinjia Huo, Lutz Lampe, and Victor C. M. Leung
The University of British Columbia, Vancouver, BC.
Email:{gauthamp, yortka, lampe, vleung}@ece.ubc.ca.

***Abstract*—Security and privacy of smart grid communication data is crucial given the nature of the continuous bidirectional information exchange between the consumer and the utilities. Data security has conventionally been ensured using cryptographic techniques implemented at the upper layers of the network stack. However, it has been shown that security can be further enhanced using physical layer (PHY) methods. To aid and/or complement such PHY and upper layer techniques, in this paper, we propose a PHY design that can detect and locate not only an active intruder but also a passive eavesdropper in the network. Our method can either be used as a stand-alone solution or together with existing techniques to achieve improved smart grid data security. Our machine learning based solution intelligently and automatically detects and locates a possible intruder in the network by reusing power line transmission modems installed in the grid for communication purposes. Simulation results show that our cost-efficient design provides near ideal intruder detection rates and also estimates its location with a high degree of accuracy.**

I. Introduction

Communication technologies have played a crucial role in realizing the concept of smart grid by providing means for bidirectional data exchange to protect, monitor, and control activities across the grid [1], [2]. Communications enable several features of the smart grid including automated meter reading (AMR), advanced metering infrastructure (AMI), demand response, situational awareness, and distribution grid management, among others [1]–[3]. Due to the nature of the data transmitted as a part of these operations, security and privacy in the smart grid is critical [4]–[6].

Security of the smart grid communication data must be ensured against broadly two kinds of attacks, namely, passive and active. Passive attacks involve an adversarial entity snooping the data and affecting the confidentiality of the transmitted message, whereas active attacks attempt at tampering the data to violate its integrity or hamper its availability [4]. Various techniques have been proposed in past to defend against both these types of attacks using methods primarily designed to be implemented at higher layers of the network stack [4]–[7]. Cryptographic encryption techniques are used to ensure data confidentiality and privacy so that an eavesdropper is unable to decode the communication message [8], [9], while intrusion detection systems (IDSs), cryptographic hashing, and digital watermarking are applied to verify data integrity and availability [9]–[11].

To complement the above security techniques and introduce a first line of defense against potential attacks, several physical layer (PHY) security solutions have also been proposed [12]. For example, intentional jamming by legitimate communication devices in the direction of a detected eavesdropper assists in ensuring data confidentiality [13]–[15]. Similarly, PHY signature-based intrusion detection solutions have been designed to detect active attacks impacting data integrity [16], [17]. While PHY intrusion detection solutions rely on an active intruder (INT) for successful fingerprinting, intentional PHY jamming ensures security even against passive eavesdroppers. However, the performance of PHY jamming techniques typically rely on the knowledge of the transmitter-eavesdropper channel. Therefore, they are more suitable to guarantee privacy from legitimate network nodes as opposed to providing data confidentiality against a malicious INT.

With this backdrop, we propose a PHY intrusion detection and location (IDL) solution for the smart grid in this paper that is capable of detecting the presence of and locating a malicious communication node. To this end, we consider the smart grid distribution network where communication is often enabled over the power lines [18, Ch. 9]. Wired communication systems are typically considered to be inherently secure from malicious INTs. However, the power line is a shared medium that is widely accessible and vulnerable to potential intrusions despite power line communication (PLC) restricting the mobility of the INT tapping in. Although some measures exist to detect nodes that tap into the power lines to steal energy by observing the energy consumption data from smart meters or by installing dedicated radio-frequency identification (RFID) tags and/or wireless sensors [19]–[21], a PHY method to detect or locate passive INTs that only snoop communication signals traveling through the power lines is not found in the literature. Nevertheless, we show in this paper that our proposed solution is *also* applicable to detect and locate potential energy theft.

A. Contributions and Highlights

While an active illegitimate participant is relatively easier to detect by listening for signatures, detecting and locating a passive eavesdropper is more challenging. In this paper, we propose a method that can successfully detect and locate both these types of intruders in typical smart grid network settings. We exploit the PLC channel state information (CSI) inherently estimated by PLC modems, to detect and locate an INT. PLC CSI is dependent on the physical characteristics of the power line, the network topology, and the loads connected to the line. A change in the nature of any of these parameters

This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

results in a change in the estimated CSI. When a malicious INT is plugged in to the line at any part of the network, all PLC modems that are in some proximity of the INT notice a change in the estimated channel frequency responses (CFRs) in their communication links. However, not all changes in the CSI are caused by an INT. On the contrary, channel changes are commonly caused due to changing load conditions in the distribution network. Therefore, we face the task of distinguishing CSI changes caused due to an INT and other legitimate network activities. To this end, we apply machine learning (ML) algorithms that can intelligently and automatically determine the presence of an INT by continuously monitoring the CSI, which is inherently estimated within the PLC modems for communication purposes.

In addition to detecting the presence of an INT, we design a solution to also precisely locate the INT as a relative distance from one of the PLC modems. For this purpose, we exploit the time domain version of the estimated CFR, i.e., the channel impulse response (CIR). Portions of the PLC signals traveling through the network reflect at locations where they experience a change in impedance. Therefore, reflections commonly occur at splices, junctions, and branch terminations [18, Ch. 2]. When an INT taps into the network, PLC signals also reflect at those locations, unless the device impedance of the INT is perfectly matched to the power line impedance across the entire operating bandwidth. With the use of medium- and broad-band PLC (BB-PLC), the communication signals span a bandwidth of up to 85 MHz [22]. Designing perfect impedance matching circuits across the entire frequency band is not a practical solution [23]. Therefore, a portion of the BB-PLC signal reflects at the location of the INT, which we observe as signal peaks in the estimated CIR. We thus design an ML-based solution, similar to our intrusion detection method, to monitor the CIR to also estimate the location of the INT. The foundational principle of using a change in the estimated PLC CSI to identify abnormal behaviors in the smart grid network has already been previously used to assess cable damages and faults for preventing in-service power outages [24], [25]. However, this paper contrasts itself from these prior works in terms of the anomaly (INT v/s cable defects) modeling, investigation methodology, ML operation, and feature engineering involved.

Outline: The rest of the paper is organized as follows. In Section II, we present our proposed ML-based solution by also including the methodology of modeling the INT and deriving its impact on the PLC channel. We evaluate our solution in Section III, where we present simulation results for a generic smart-grid distribution network under varying load conditions. We present a brief discussion of our solution in Section IV, where we reflect on some of the notable characteristics of our proposed technique. Finally, we draw conclusions in Section V.

II. PHY IDL

In this section, we present our PHY IDL solution by introducing the procedure for INT modeling, deriving its impact on the PLC channel, and applying ML algorithms that can effectively identify and locate the INT.

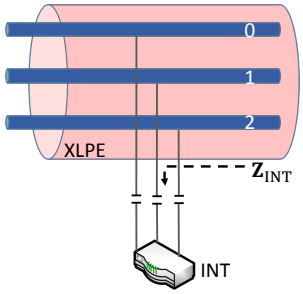

Fig. 1. A triple-core XLPE cable with an INT tapped into it to decouple PLC data from any or all of the conductor pairs, and presenting a device input impedance of $\mathbf{Z}_{\text{INT}}$.

A. Intrusion Modeling

We introduced in Section I that the entry of an INT changes the PLC CSI. However, to distinguish the channel changes caused by an INT and from all other factors, the malicious node and its impact need to be modeled accurately. In this work, we consider a triple conductor cross linked polyethylene (XLPE) insulated cable, such as [26] and also shown in Fig. 1, which is applicable for both low- and medium-voltage networks. We let the INT tap into the cable at any point in the network. Although we consider single-input single-output (SISO) PLC, we expect the INT to be capable of multiple-input multiple-output (MIMO) operation, such that it is able to decouple PLC signals from any/all pairs of conductors. We characterize such an INT with its input impedance, $\mathbf{Z}_{\text{INT}}$, which is a 2×2 matrix for a 2×2 MIMO operation. We denote $\mathbf{Z}_{\text{INT}}$ to be the composite input impedance that also captures the effect of the coupler used by the INT. Fig. 1 shows a typical capacitive coupling method used at the INT node. However, it may also choose to decouple the differential mode signals from the cable using an inductive coupler. Typically, we expect the INT to be another PLC modem, and we therefore have *a-priori* knowledge of $\mathbf{Z}_{\text{INT}}$, since most PLC modems use a widely accepted fixed input impedance value [27]. However, the INT may choose to obfuscate its $\mathbf{Z}_{\text{INT}}$ to render its detection harder simply by applying a series/parallel impedance preceding its coupling circuity. Thus, we consider $\mathbf{Z}_{\text{INT}}$ to be an unknown parameter in our work.

B. PLC Channel Modeling

To independently model and capture individual effects at different parts of the PLC network, we use the bottom-up approach of modeling the PLC channel [28]. We compute the transfer function of each of the ℓth unit of the network, $\mathbf{H}_\ell(f)$, where $\mathbf{H}_\ell(f)$ is the 2×2 matrix at every frequency f. The final transfer function between any two points with $\mathcal{L}$ total units in between them can then be computed as

$$\mathbf{H}(f) = \prod_{\ell=1}^{\mathcal{L}} \mathbf{H}_\ell(f). \tag{1}$$

The computation of every $\mathbf{H}_\ell(f)$ requires the knowledge of the sub-network topology of the ℓth network unit, the loads connected at any branch terminations, and the cable parameters characterized by its per-unit-length (PUL) parameters. We compute the PUL parameters of the cable with the homogeneous insulation approximation to obtain the closed form expressions for the PUL resistance ($\mathbf{R}$), capacitance ($\mathbf{C}$), inductance ($\mathbf{L}$), and conductance ($\mathbf{G}$) values [29, Chs. 3, 5]. Further, we consider a known static network topology, which is characteristic of smart grid distribution networks, and use variable loads at different positions of the network, whose variations are randomized. The loads here include electrical loads, PLC modems, sensors, transformers, and any other valid components connected to the network. Thus, when an INT taps into the network at any ℓth unit, it changes the topology and introduces an additional load to consequently change $\mathbf{H}_\ell(f)$. To detect the resultant change in $\mathbf{H}(f)$ and distinguish it from other changes introduced by valid network activities, e.g., load variations, we use an ML-based detection approach.

C. ML for PHY IDL

For our PHY IDL solution we employ SISO PLC and use one of the pairs of the power line conductors for data transmission. Consequently, we use the end-to-end SISO CFR, $H(f)$, which is one of the elements of $\mathbf{H}(f)$ computed as in (1). Along with this, modems that are enabled with the in-band full-duplex functionality also regularly estimate the single-ended reflection channel, H_{SE}, as a part of its self-interference cancellation procedure [30], [31]. Since H_{SE} is a single-ended transfer function and can be estimated without requiring any pilot signal from a far-end transmitter, it can be computed by the PLC modem even when it has no data to transmit. It can be estimated by transmitting a known random signal of relatively low power for channel estimation that essentially manifests as noise for any other communication signal traveling through the network. This is particularly advantageous when considering PLC modems located at smart meters that update data infrequently, e.g., up to once in 60 minutes [32].

We divide our IDL tasks into three categories of INT detection, branch location, and position determination. We formulate the INT detection and branch location tasks as supervised ML classification, and the INT position determination as a supervised regression task. We conceive that each of our machines for the three tasks can be trained offline using synthetic PLC channel data, and can then all be loaded on to the PLC modems in the network. Therefore, we are not limited by the number of H and H_{SE} samples required for the training process.

For classification and regression, we consider the support vector machine (SVM) and boosting ML algorithms due to their known performance excellence in other use-cases [33]. SVM is a classical ML technique that creates support vectors of hyperplanes for a given training data set for classification. Due to the sparsity it provides, and because of the large margin principle, SVM is able to provide accurate predictions for new data samples [33, Ch. 14]. On the other hand, boosting is a meta-ML algorithm that consolidates several weak learners into a strong learner [33, Ch. 16]. At each iteration, a new machine is trained by allocating higher weights to each data sample that suffers from inaccuracy in the previous iterations. The new machine is trained quickly with updated weights using weak learners and is added to the models trained in the previous iterations to form the new ensemble. The ensemble constructed through iterations is able to provide accurate results for classification (adaptive boosting) as well as regression (least-squares boosting).

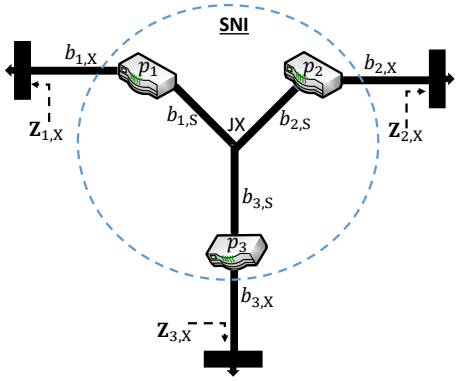

Fig. 2. The considered Y-network topology for the SNI, where we randomly place an INT at any of the $b_{i,\text{S}}$ or $b_{i,\text{X}}$ branches ($i = 1, 2, 3$). (JX: Junction)

Training the machines with either of the two ML algorithms requires extracting features from the raw data of H and H_{SE}. Since the introduction of the INT gives rise to additional peaks in the CIR waveform, we use the peak amplitudes and locations in the CIRs of H and H_{SE}, along with the mth order moments ($m = \{1, 2, 3, 4\}$) of $\angle H$ and $\angle H_{\text{SE}}$ for both detecting and locating the INT. Depending on the reflections from the INT, the signal transmission undergoes a different overall attenuation. Therefore, we also use the mth order moments ($m = \{1, 2, 3, 4\}$) of $|H|$ and $|H_{\text{SE}}|$ for detecting the INT.

III. Evaluation

We evaluate our solution in this section, by presenting simulation results that show the performance of our method in terms of detection and false alarm rates in identifying the presence of an INT, and also the prediction accuracy in locating it.

A. Simulation Settings

Most low- and medium-voltage network topologies can be decomposed into multiple radial and/or Y-sub-networks. Given typical PLC ranges [34], we consider an elementary building-block sub-network such as the one shown in Fig. 2. It consists of three PLC modems, p_i, $i = 1, 2, 3$, located at the branch end points of the Y-network, which we refer to as the sub-network of interest (SNI). Without loss of generality, we consider branch lengths of each $b_{i,S}$ to be 500 m, and branch extensions beyond every p_i as $b_{i,X}$ of length 500 m. The latter are connected to equivalent extension impedances,

$Z_{i,X}$, which emulate realistic network extensions beyond the extended branches. These extension branches introduce topological ambiguity in locating an INT. For example, an INT on $b_{1,S}$ and $b_{1,X}$ both introduce similar signal peaks in the CIR of H_{SE} seen by p_1. The use of the end-to-end transfer function, H, together with H_{SE} assists us in countering this challenge. Additionally, we also employ a cooperative IDL procedure, where we collect the detection results from all p_i, $i = 1, 2, 3$, in the SNI shown in Fig. 2, to arrive at a final decision on the presence of INT in the SNI. The same procedure is applicable in every SNI of the overall network.

We place the INT randomly on any of the six branches, and use p_i, $i = 1, 2, 3$, to detect the presence of the INT. As specified in Section II-A, the INT may choose to obfuscate its inherent device impedance using an external series/parallel impedance. Therefore, for both training and testing phases of our method, we model the INT with a randomized impedance in $\mathcal{U}(10, 1000)$ Ω, where $\mathcal{U}(a, b)$ represents a uniformly distributed random variable between a and b. We generate the training and testing samples using the open-source channel generator of [35].

B. Numerical Results

1) INT Detection and Branch Location: We jointly perform the two classification tasks of detecting an INT and locating the branch on which it lies. To this end, we cooperatively determine if an INT is present between two PLC modems. For example, we use p_1 and p_2 to both indicate if an INT is present on either $b_{1,S}$ or $b_{2,S}$. Using the results from all three pairs of modems, we can determine not only whether an INT is present in the SNI, but also the branch on which it has tapped into. For this task, we use 1000 training samples for each INT condition, i.e., 1000 H and H_{SE} samples with no INT, and 1000 each with INT on $b_{i,S}$ or $b_{i,X}$ for $i = 1, 2, 3$. For every sample, we randomize the load conditions $Z_{i,X} \sim (\mathcal{U}(0, 50) + j\mathcal{U}(-50, 50))$ Ω to emulate realistic network extensions [36, Table 1.1]. For training samples with an INT presence, we place the INT at a random location on the branch. We train the machine with an ample amount of training samples and an appropriate number of iterations such that the performance of the machine is saturated, while also ensuring that we do not cause over-fitting. Recall that since we train the machine using synthetic data even in real deployments, we are not constrained by the number of training samples to use.

We then test our trained machine using 1400 test samples, which contain all possible INT presence configurations, i.e., INT on $b_{i,S}$ or $b_{i,X}$ for $i = 1, 2, 3$, and also without any INT. We tested our results for four different INT characteristics, each with 1400 test samples, for device impedances of 10 Ω, 100 Ω, 500 Ω, and 1000 Ω, which capture a wide range of possible impedances that an INT modem might present to the line. The results of our evaluation are presented in Fig. 3. Our results show that using SVM yields unsatisfactory performance while boosting techniques provide near perfect detection rates as well as negligible false alarms across various INT impedance values. This is because SVM enforces

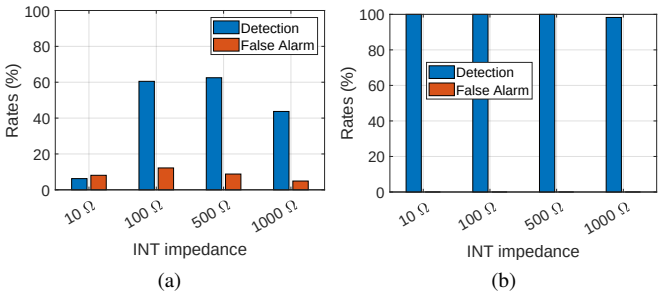

Fig. 3. Detection and false alarm rates for detecting an INT using (a) SVM with radial basis function kernel and (b) adaptive boosting classification.

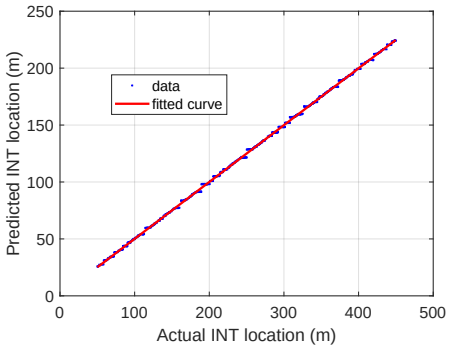

Fig. 4. The INT location performance of our solution, which shows that the predicted location values nearly match the actual locations on an average.

sparsity on the resultant support vectors that determine the classification boundary, which limits the expressive capability of the trained machine and results in under-fitting. In contrast, through stage-wise iteration, boosting techniques can train an ensemble with sufficient comprehensiveness for the prediction. Moreover, from the results of SVM, we can see that prediction performance for extreme INT impedance values is even worse. This also shows that the SVM is trained to deal with a range of typical values and lacks the capability of generalization. Therefore, for the classification task, the boosting techniques are preferred over SVM models.

2) INT Location: Once we establish the branch on which the INT lies on, we use the modem closest to the INT to further estimate its precise location. For this regression task, we use 4000 training samples that contain INT tapped into the branch at a random location between 50 and 450 m away from the nearest modem on the 500 m long branch. The number of training samples are again chosen to ensure saturated performance of the machine, which was trained using the least-squares boosting algorithm [33, Ch. 16]. Next, we test our solution with 1000 other samples with randomized locations of the INT and random load conditions. We set our testing samples to 1000 since this was sufficient to provide us with a clear performance trend, as shown in Fig. 4. We observe that the fit line of our predictions nearly matches the actual INT locations, indicating a high degree of accuracy.

IV. Discussion

In this section, we present a brief discussion of our solution by reflecting on some of the notable characteristics of our

proposed design, its implementation aspects, comparison with related arts, potential drawbacks, and possible extensions.

A. Comparison with Related Works

1) ML-based IDS: ML-based IDSs have been proposed in the past to detect the presence of an INT or identify suspicious network activities, e.g., [37]. However, methods like these rely on acquiring energy consumption data for analysis. In contrast, our proposed solution requires only the communication CSI for IDL, and therefore ensures privacy of transmitted data. Nevertheless, our solution does not necessarily intend to replace the state-of-the-art IDSs, but can instead function as a complementary technique to the existing methods as it introduces little additional cost.

2) IDS with Alternative Data Collectors: IDSs have also been proposed using different data acquisition devices, such as dedicated sensors or micro-phasor measurement units [11], [38]. On the other hand, our method proposes the re-use of existing grid components, i.e., PLC modems installed for communication purposes, for added functionalities of IDL. Note that our solution is also applicable in distribution networks that do not use PLC as the sole communications technology but instead as a hybrid solution in conjunction with other wired and wireless communication alternatives, e.g., [39]. For grids that do not currently employ PLC, our solution, together with other methods such as [40], [41] that re-use PLC modems for grid health diagnostics, provide a compelling incentive for the use of PLC as a multidimensional smart grid enabling technology.

3) PHY Intrusion Detection of Passive Entities: A different class of PHY IDSs have also been developed in the past, which primarily aim at detecting passive entities, typically humans, as INTs by exploiting fluctuations caused in PHY parameters due to human motion or other human activities, e.g., breathing [42], [43]. While our solution also aims at detecting a passive entity, we are also able to locate its position without relying on any INT activity. When the INT physically moves or changes its state of operation, our solution is still able to detect such changes and identify its presence, as evidenced in Fig. 3, which shows successful detection of the INT across a range of impedance behaviors.

B. Salient Features

1) Privacy: Unlike many higher layer INT detection techniques [4], our solution does not involve decoding the transmitted signals. Since our solution operates entirely at the PHY, the application level data is protected during our evaluation, ensuring complete privacy of the data being used for IDL.

2) Automated Solution: Our ML-based IDL solution provides an entirely automated procedure that does not require any manual intervention either for collecting or interpreting the data. Thereby, we substantially reduce human errors and the involved cost when compared to many alternative INT detection methods [4].

C. Alternative Adaptations of our IDL Solution

Our analysis thus far has focused on detecting and locating an active or passive INT that may affect the confidentiality, integrity, and availability of the communication data being transmitted over the power lines. However, our solution can be used in its native form to also detect potential energy thefts. A device tapping into the line to steal energy also presents a similar change in PLC CSI as we have considered. The device impedance presented in this case is typically expected to be in the order of a few Ohms. Our results in Fig. 3 has shown that our solution is also able to detect an INT whose impedance is as low as 10 Ohms, indicating that our detection technique is also applicable to identify potential energy theft as well.

D. Applications of IDL

The results of IDL can be used in conjunction with conventional INT detection solutions that are implemented at the upper layers of the network stack for continued legacy use with the combined results. Additionally, INT location provides useful inputs to other PHY security techniques, like intentional jamming, e.g., [15], which require knowledge of the transmitter-eavesdropper channel to optimize the jamming beamforming to degrade the decoding ability at the INT. With a known network topology, cable characteristics, and INT impedance, locating the INT provides complete CSI between the malicious node and any PLC modem in the network.

E. Implementation Architecture

An instinctive implementation of our solution involves remotely loading our trained machines on to the PLC modems throughout the network. They can be updated at any time in the future and as often as required simply by reloading an upgraded version of the machine, possibly trained with new data or an improved ML algorithm. This then enables all PLC modems to use their inherently estimated H and H_{SE} to extract features from them and automatically detect and locate a potential INT in a distributed manner. Alternatively, the individual H and H_{SE} data from all PLC modems can be collected at a central location, say, a sub-station, where the data can then be processed in a centralized manner. Both these methods have their own benefits and drawbacks. While the distributed IDL method introduces additional storage and computational requirements within the modem, the centralized IDL solution presents additional signaling overheads. We note that irrespective of the chosen implementation architecture, the performance of our solution remains the same.

F. Performance in the Real World

Our simulation results in Fig. 3 and Fig. 4 are based on our machines being trained and tested using synthetic PLC data. However, for practical applications, we propose that our machines be trained offline using computer generated data but deployed in the real-world for IDL. Therefore, the performance of our method relies on the accuracy of the PLC channel model used for offline training. Practical performance evaluation thus forms the natural extension of our work.

V. Conclusion

We have presented a machine learning based intelligent and automated intrusion detection and location solution using PLC modems installed in the grid for communication purposes. Our low-cost solution monitors the channel state information inherently estimated by the PLC modems for behavior deviations caused by an intruder. Our design can be used as a stand-alone solution or in conjunction with existing IDSs to obtain enhanced security and privacy of the smart grid data. Our method can also be adapted to identify potential energy theft without requiring any additional data acquisition devices or the decoding of energy consumption data.

References

[1] "Communications requirements of smart grid technologies," *US Department of Energy, Tech. Rep*, pp. 1–69, 2010.

[2] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surveys & Tuts.*, vol. 15, no. 1, pp. 5–20, 2013.

[3] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informatics*, vol. 9, no. 1, pp. 28–42, 2013.

[4] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys & Tuts.*, vol. 16, no. 4, pp. 1933–1954, 2014.

[5] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Commun. Surveys & Tuts.*, vol. 19, no. 1, pp. 397–422, 2017.

[6] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Commun. Surveys & Tuts.*, 2019.

[7] F. M. Cleveland, "Cyber security issues for advanced metering infrastructure (AMI)," in *IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*, pp. 1–5, 2008.

[8] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, "A key management scheme for secure communications of advanced metering infrastructure in smart grid," *IEEE Trans. Ind. Electron.*, vol. 60, no. 10, pp. 4746–4756, 2013.

[9] J. Benoit, "An introduction to cryptography as applied to the smart grid," *Cooper Power Systems*, 2011.

[10] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2435–2443, 2015.

[11] J. Hong and C.-C. Liu, "Intelligent electronic devices with collaborative intrusion detection systems," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 271–281, 2019.

[12] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys & Tuts.*, vol. 16, no. 3, pp. 1550–1573, 2014.

[13] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *IEEE/SP 15th Workshop on Statistical Sig. Proc.*, pp. 417–420, 2009.

[14] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Sig. Proc.*, vol. 61, no. 20, pp. 4962–4974, 2013.

[15] G. Prasad, O. Taghizadeh, L. Lampe, and R. Mathar, "Securing MIMO power line communications with full-duplex jamming receivers," in *IEEE Int. Symp. Power Line Commun. Applicat. (ISPLC)*, pp. 1–6, 2019.

[16] A. Tomko, C. Rieser, and L. Buell, "Physical-layer intrusion detection in wireless networks," in *IEEE Military Commun. Conf. (MILCOM)*, pp. 1–7, 2006.

[17] K. Remley, C. A. Grosvenor, R. T. Johnk, D. R. Novotny, P. D. Hale, M. McKinley, A. Karygiannis, and E. Antonakakis, "Electromagnetic signatures of WLAN cards and network security," in *IEEE Int. Symp. Sig. Proc. Info. Tech.*, pp. 484–488, 2005.

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

[19] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1319–1330, 2013.

[20] P. Jokar, N. Arianpoo, and V. C. Leung, "Electricity theft detection in AMI using customers consumption patterns," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, 2016.

[21] S. K. Singh, R. Bose, and A. Joshi, "Energy theft detection in advanced metering infrastructure," in *IEEE World Forum on IoT (WF-IoT)*, pp. 529–534, 2018.

[22] L. Yonge, J. Abad, K. Afkhamie, L. Guerrieri, S. Katar, H. Lioe, P. Pagani, R. Riva, D. M. Schneider, and A. Schwager, "An overview of the HomePlug AV2 technology," *Hindawi J. Elec. Comp. Eng.*, 2013.

[23] N. Taherinejad, L. Lampe, and S. Mirabbasi, "An adaptive impedance-matching system for vehicular power line communication," *IEEE Trans. Veh. Tech.*, vol. 66, pp. 927–940, Feb 2017.

[24] Y. Huo, G. Prasad, L. Atanackovic, L. Lampe, and V. C. M. Leung, "Grid surveillance and diagnostics using power line communications," in *IEEE Int. Symp. Power Line Commun. Appl. (ISPLC)*, pp. 1–6, 2018.

[25] Y. Huo, G. Prasad, L. Atanackovic, L. Lampe, and V. C. M. Leung, "Cable diagnostics with power line modems for smart grid monitoring," *IEEE Access*, 2019 (accepted, in-press).

[26] HELUKABEL, "Medium voltage power cables," http://mdmetric.com/prod/helukabel/N.Medium%20Voltage%20Power.pdf, 2016.

[27] "Integrated powerline communication analog front-end transceiver and line driver," http://www.maximic.com/datasheet/index.mvp/id/6333.

[28] F. Versolatto and A. M. Tonello, "An MTL theory approach for the simulation of MIMO power-line communication channels," *IEEE Trans. Power Del.*, vol. 26, no. 3, pp. 1710–1717, 2011.

[29] C. R. Paul, *Analysis of multiconductor transmission lines*. John Wiley & Sons, 2008.

[30] G. Prasad, L. Lampe, and S. Shekhar, "In-band full duplex broadband power line communications," *IEEE Transactions on Communications*, vol. 64, no. 9, pp. 3915–3931, 2016.

[31] G. Prasad, L. Lampe, and S. Shekhar, "Digitally controlled analog cancellation for full duplex broadband power line communications," *IEEE Trans. Commun.*, vol. 65, pp. 4419–4432, Oct 2017.

[32] "Advanced metering infrastructure and customer systems," *Office of Electricity Delivery and Energy Reliability, US Department of Energy*, pp. 1–98, 2016.

[33] K. Murphy, *Machine Learning: A Probabilistic Perspective*. Adaptive computation and machine learning, MIT Press, 2012.

[34] devolo, "BPL modem MV: Data communication at the medium voltage level," https://bit.ly/2E3n1Oj.

[35] F. Gruber and L. Lampe, "On PLC channel emulation via transmission line theory," in *Proc. IEEE Int. Symp. Power Line Commun. Appl. (ISPLC)*, pp. 178–183, 2015.

[36] L. T. Berger, A. Schwager, P. Pagani, and D. Schneider, *MIMO power line communications: narrow and broadband standards, EMC, and advanced processing*. CRC Press, 2014.

[37] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796–808, 2011.

[38] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures π," in *IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, pp. 232–237, 2011.

[39] Itron, "OpenWay powered by Itron Riva technology," https://www1.itron.com/Documents/OpenWay-Riva.pdf, 2014.

[40] G. Prasad, Y. Huo, L. Lampe, A. Mengi, and V. C. M. Leung, "Fault diagnostics with legacy power line modems," in *IEEE Int. Symp. Power Line Commun. Applicat. (ISPLC)*, pp. 1–6, 2019.

[41] Y. Huo, G. Prasad, L. Lampe, and V. C. M. Leung, "Smart-grid monitoring: Enhanced machine learning for cable diagnostics," in *IEEE Int. Symp. Power Line Commun. Applicat. (ISPLC)*, pp. 1–6, 2019.

[42] J. Lv, D. Man, W. Yang, X. Du, and M. Yu, "Robust WLAN-based indoor intrusion detection using PHY layer information," *IEEE Access*, vol. 6, pp. 30117–30127, 2018.

[43] C. Wu, Z. Yang, Z. Zhou, X. Liu, Y. Liu, and J. Cao, "Non-invasive detection of moving and stationary human with WiFi," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 11, pp. 2329–2342, 2015.