IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 7, 2019, accepted April 2, 2019, date of publication April 9, 2019, date of current version April 18, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2909807

Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems

PANAGIOTIS I. RADOGLOU-GRAMMATIKIS AND PANAGIOTIS G. SARIGIANNIDIS, (Member, IEEE)
Department of Informatics and Telecommunications Engineering, University of Western Macedonia, Kozani 501 00, Greece
Corresponding author: Panagiotis G. Sarigiannidis (psarigiannidis@uowm.gr)

This work was supported by the European Union's Horizon 2020 Research and Innovation Programme under Agreement 787011 (SPEAR).

ABSTRACT The smart grid (SG) paradigm is the next technological leap of the conventional electrical grid, contributing to the protection of the physical environment and providing multiple advantages such as increased reliability, better service quality, and the efficient utilization of the existing infrastructure and the renewable energy resources. However, despite the fact that it brings beneficial environmental, economic, and social changes, the existence of such a system possesses important security and privacy challenges, since it includes a combination of heterogeneous, co-existing smart, and legacy technologies. Based on the rapid evolution of the cyber-physical systems (CPS), both academia and industry have developed appropriate measures for enhancing the security surface of the SG paradigm using, for example, integrating efficient, lightweight encryption and authorization mechanisms. Nevertheless, these mechanisms may not prevent various security threats, such as denial of service (DoS) attacks that target on the availability of the underlying systems. An efficient countermeasure against several cyberattacks is the intrusion detection and prevention system (IDPS). In this paper, we examine the contribution of the IDPSs in the SG paradigm, providing an analysis of 37 cases. More detailed, these systems can be considered as a secondary defense mechanism, which enhances the cryptographic processes, by timely detecting or/and preventing potential security violations. For instance, if a cyberattack bypasses the essential encryption and authorization mechanisms, then the IDPS systems can act as a secondary protection service, informing the system operator for the presence of the specific attack or enabling appropriate preventive countermeasures. The cases we study focused on the advanced metering infrastructure (AMI), supervisory control and data acquisition (SCADA) systems, substations, and synchrophasors. Based on our comparative analysis, the limitations and the shortcomings of the current IDPS systems are identified, whereas appropriate recommendations are provided for future research efforts.

INDEX TERMS Advanced metering infrastructure, cyberattacks, intrusion detection system, intrusion prevention system, SCADA, security, smart grid, substation, synchrophasor.

I. INTRODUCTION

The Smart Grid (SG) constitutes a technological evolution of the traditional electrical grid, by introducing Information and Communications Technology (ICT) services. The functionality of a typical electrical grid is mainly based on the energy generation, transmission and distribution processes. More concretely, it includes power plants, step-up transmission substations, step-down transmission substations, distribution substations and transmission and distribution lines. On the other hand, as illustrated in Fig. 1 [1], SG provides the required infrastructure and the communication channels that allow the real-time bidirectional interaction between the consumers and the utility companies. This communication can provide multiple benefits such as processes that enable auto metering and maintenance, self-healing, efficient energy management, reliability and security [2]–[6].

However, despite the fact that SG introduces multiple advantages, it also introduces crucial security challenges, since it combines heterogeneous communications

The associate editor coordinating the review of this manuscript and approving it for publication was Fangfei Li.

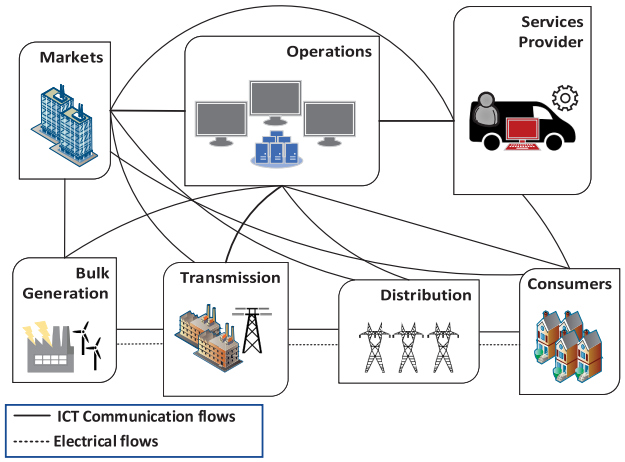

FIGURE 1. An abstract architecture model of the SG [1].

networks [7] such as Internet of Things (IoT) [8]–[11] devices, industrial devices [12], wireless components and Wireless Sensor Networks (WSNs) [13] characterized by various security threats [14], [15]. In addition, the integration of smart devices, such as smart meters, that communicate with each other without human intervention induces more security concerns. Furthermore, the necessary existence of legacy technologies, such as conventional Supervisory Control and Data Acquisition (SCADA) systems, increase the potential risks, since these systems may not integrate modernized security solutions. The security breaches in SG mainly target on the availability, integrity and confidentiality of individual entities [14], [15]. In more detail, the different kinds of Denial of Service (DoS) attacks aim to disrupt the network services and cause significant damages such as a power outage [16]–[18]. A characteristic example was the cyberattack against a Ukrainian substation resulting in the power outage for more than 225,000 people [19]. On the other hand, the false data injection attacks [20]–[23] can modify the data of smart meters in order to succeed in more economical pricing. Finally, various types of Man in the Middle (MiTM) can violate the privacy of the systems [24], [25]. Furthermore, a remarkable and more dangerous category of cyberattacks, which threatens the SG architecture, is the Advanced Persistent Threat (APT). This term specifies a set of organized and long duration attacks by security specialists against a particular target, such as politicians and industries. Examples of these attacks are Stuxnet [26], Duqu [27], Flame [27], and Gauss [27].

An Intrusion Detection System (IDS) and even its evolution, the Intrusion Prevention System (IPS), can operate as a second line of defense in a communication network, by enhancing the operation of the encryption and authorization mechanisms. For instance, if a cyberattack bypasses the encryption and authorization mechanisms, the IDS or IPS can timely inform the security administrator or perform appropriate preventive countermeasures. The term Intrusion Detection and Prevention System (IDPS) will be used from now on in this paper for referring to both previous terms. In general, the rapid progress of computer networks necessitated the development of appropriate mechanisms that have the ability to automate the process of detecting or/and preventing possible security violations. The presence of these systems in SG is required, since the security policy violations in this ecosystem may cause dangerous situations and disastrous accidents. A significant advantage of the specific systems is that they possess the ability to recognize zero-day attacks by using artificial intelligence mechanisms. Therefore, in this paper, we provide an analysis of 37 cases of IDPS systems devoted to SG, by evaluating and comparing the cyberattacks that they are able to detect, their methodology, the detection performance and finally the consumption of computing resources. Based on this analysis, we specify the limitations and shortcomings that characterize these systems and provide research directions for future work.

In particular, the rest of this paper is organized as follows: Section II discusses the related surveys in the literature and provides the motivation and contributions of our study. Sections III and IV introduce an overview of SG and IDPS systems respectively. Section V presents and explains the requirements that should characterize these systems. Section VI provides an analysis of 37 IDPS cases, by investigating their main characteristics. Section VII interprets, evaluates and compares the results exported from the previous analysis. Finally, Section VIII provides trends and research directions concerning the security of SG, focusing on IDPS systems, while section IX presents the concluding remarks of this study.

II. MOTIVATION AND CONTRIBUTION

Although SG can provide multiple benefits, like better energy management and improved reliability, its independent and interconnected nature generates at the same time critical cybersecurity vulnerabilities that in turn can lead to a wide range of consequences such as power outage, brownout, energy theft, energy consumer privacy breach. In particular, most of the communication protocols adopted by SG are characterized by severe security gaps, since do not comprise authentication and access control mechanisms, thus enabling possible adversaries to launch various cyber-physical attacks. Fig. 2 depicts a pictorial view of such attacks against SG. A characteristic example of cyberattacks against a critical infrastructure was the Stuxnet worm [26], which exploited four zero-days vulnerabilities. Furthermore, the diversity and complexity of communications that take place in SG, as well as the huge volume of data generated by the various subsystems, hinder the adoption of conventional security measures. Therefore, it is clear that the presence of IDPS systems is vital for the entire operation of SG and mainly for ensuring the essential security requirements: Confidentiality, Integrity and Availability (CIA).

Several studies have examined the security issues in the SG paradigm, by analyzing security challenges, threats and corresponding countermeasures. Some of these are listed

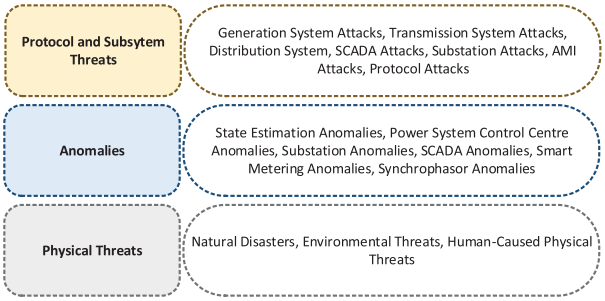

FIGURE 2. SG cyberattacks.

in [8], [14], [15], [28]–[38]. Since that the nature and means of cyberthreats evolve rapidly, the creation of corresponding surveys and review papers is quite crucial, as they present state of the art and identify possible challenges, security gaps and research directions. Other works follow a more precise approach, by examining the security issues regarding particular protocols that are commonly utilized in the SG communications. Concretely, in [39], [40], the authors examined the security issues of IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) and IEC 61850 [41], [42] standards respectively. Similarly, in [43] the authors investigate various encryption and authentication protocols for SG. Nevertheless, only a few studies have examined the contribution of the IDPS systems for the contemporary electrical grid. Specifically, in [44], the authors provided an extensive study and comparison of multiple IDPSs devoted to the Cyber-Physical Systems (CPSs), such as SG. Similarly, in [45], [46] the authors investigated various IDPS instances concerning the protection of IoT; SG is considered as the largest use case of IoT [47]. On the contrary to the previous studies, the papers [48], [49] follow a more specific approach and examine the IDPS systems devoted to the protection of the Advanced Metering Infrastructure (AMI). Finally, the work [50] evaluates three open-source Security Information and Event Management (SIEM) systems for SG. In particular, the platforms studied are a) the AlienVault OSSIM [51], b) the Cyberoam iView [52] and c) the Prelude SIEM [53]. According to the authors' evaluation criteria, AlienVault OSSIM and Prelude SIEM present the best performance.

Based on the previous description, only two studies [48], [49] focus exclusively on the examination of the IDPS systems for SG; however they are limited only to protecting the AMI domain. In the light of the aforementioned results, this work is motivated by the importance of the security issues in SG, providing a comprehensive survey of the IDPS systems which discusses critical topics such as the detection methodology, limitations, shortcomings and the ongoing security requirements. Moreover, this survey examines not only IDPSs that monitor and control the AMI components, but also SCADA systems, substations and synchrophasors. Furthermore, contrary to previous works, we analyze thoroughly each case, by investigating its architecture, the detection technique, the kinds of cyberattacks that are detected, the resources consumption, performance, the utilized datasets and the software packages. In conclusion, the desired purpose of this paper is to constitute a stopping point for the interested parties that intend to work with the IDPS systems for SG. The contribution of our work is summarized in the following sentences:

- **Identifying the requirements for effective IDPS systems devoted to protecting the SG components**: Since SG consists of several and heterogeneous technologies, components and communication interfaces, the conventional IDPS systems (coming from computer networks) cannot meet the security requirements of SG. In this paper, we identify these requirements that subsequently are utilized to evaluate the various relevant IDPS found in the literature.
- **Providing a comprehensive and comparative analysis of IDPS systems devoted to protecting SG**: In particular, we investigate thoroughly 37 IDPSs capable of detecting cyberattacks against either the entire SG ecosystem, AMI, SCADA, substations and synchrophasors.
- **Identifying existing weaknesses of the current IDPS systems for SG**: Based on our analysis and taking into account the requirements of IDPS systems for the SG paradigm, we identify the weaknesses of the existing IDPSs found in the literature.
- **Identifying the appropriate IDPS for the entire SG ecosystem**: Accordingly, based on our analysis and after identifying the weaknesses of the existing IDPS, we specify the appropriate IDPS for SG, as well as its type and attributes.
- **Determining the current research trends and providing directions for future work in this field**: Finally, we present the ongoing trends in this field, by identifying possible directions and technologies for future research work.

III. SMART GRID PARADIGM

Many organizations such as the Electric Power Research Institute (ERPI), the Department of Energy (DoE) and the European Commission Task Force for Smart Grid have been involved in the definition of the SG paradigm. The term of SG is defined as the connection of the current electrical grid with ICT services, by ensuring the corresponding sustainability and allowing the remote control of all processes from generation to distribution, the bidirectional communication between consumers and utilities, the distributed production, storage and smart measurement of electricity. In this section, we provide an overview of the SG paradigm by analyzing its components and the corresponding communications.

A. SMART GRID COMPONENTS

The SG paradigm combines various kinds of systems, technologies and infrastructures such as microgrids, AMI, substations, synchrophasor systems, SCADA systems and electric vehicles [14], [54]. From these technologies, AMI

and SCADA systems are the most critical and vulnerable to cyberattacks and for this reason, most of the IDPS systems analyzed below focus on these technologies. Furthermore, substations and synchrophasor systems are also an attracted target for cyberattackers, since they are crucial for the normal functionality of SG. In addition, a remarkable attribute of SG is its ability to form microgrids whose operation is based on renewable energy resources. Nevertheless, such microgrids infrastructures characterized by special features may exhibit different kinds of vulnerability. Subsequently, we provide a brief overview of these technologies. More information about the components of SG is provided in [54].

The AMI provides all operations that are necessitated for the bidirectional data exchange between the end users and utility companies. In particular, AMI consists of three kinds of components: a) smart meters, b) data collectors and c) AMI headend. Smart meters undertake to monitor the power consumption and other measurements of the electrical appliances. Data collectors are responsible for storing the information provided by multiple smart meters that belong in a specific geographic area. Finally, the AMI headend is a central server of the utility company which receives, stores and manages the information of the data collectors. Based on the information aggregated on the AMI headend, the utility company is able to take the right decisions concerning the processes of the electricity generation, transmission and distribution. It is noteworthy that these components belong to different geographic areas that can be characterized by different attributes and constraints. Hence, each of these areas utilizes appropriate communication technologies that are determined according to the corresponding attributes.

SCADA systems are part of the industrial environment and their primary operation is to monitor and control the automated function of other components. In particular, a SCADA system consists of a) measuring instruments, b) logic controllers such as a programmable logic controller or a Remote Terminal Unit (RTU), c) a Master Terminal Unit (MTU) d) a communication network and e) an HMI. Measuring instruments refer to sensors that monitor physical measurements such as the temperature, pressure and voltage. Logic controllers are mainly responsible for collecting data from the measuring instruments, detecting abnormal behaviors and activating or deactivating technical components. The logic controllers interact with MTU which is a central host through which the system operator can send commands to logic controllers and receive data. The interaction between MTU and the logic controllers is realized via the communication network. This communication network is based on industrial protocols, such as Modbus [55]–[57] and Distributed Network Protocol 3 (DNP3) [58]. Finally, HMI is a software package with graphics capabilities installed on MTU and facilitates the interaction between MTU and logic controllers.

Substations play a significant role in the electrical grid operation. They participate in the transmission and distribution operations of the electrical grid. Specifically, they receive the generated power, configure the distribution function and control the power increase [54]. They can include various devices and software components such as Intelligent Electronic Devices (IEDs), RTUs, HMI and Global Positioning System (GPS).

A synchrophasor system constitutes an emerging technology which is necessary for the operations of the modern electrical grid. Mainly, it consists of Phasor Measurement Units (PMUs), Phasor Data Concentrators (PDCs), a communication network and a Graphical User Interface (GUI) software. A PMU is a device which executes various measurements from current/voltage waveforms, such as frequency, phase angle, active power and reactive power. A PDC undertakes to aggregate the information of PMUs and transform them into a single flow. The communication between PMUs and PDCs is usually carried out through IEEE C37.118.2 and IEC 61850 [41], [42] standards. Finally, the GUI application is responsible for visualizing appropriately the various data from PDCs.

A special characteristic of SG is its ability to form isolated microgrids that can operate either with the support of the main electrical grid or independently. Microgrids usually employ renewable energy resources such as solar energy, wind energy and hydroelectric energy. At this point, it should be noted that based on the existing literature we could not find any IDPS system which focuses on protecting microgrids. This state is a crucial research challenge in this field, since microgrids are characterized by different operation features compared to the main electrical grid that may exhibit various kinds of vulnerabilities.

B. SMART GRID COMMUNICATIONS

Fig. 3 illustrates a generic architecture of SG divided in terms of communication features. In the first layer, there are three types of network areas: a) Home Area Networks (HANs), b) Business Area Networks (BANs) and c) Industry Area Networks (IANs), characterized by the presence of the consumer. In particular, the main characteristic of these network areas is the presence of smart meters that monitor the energy consumption of electronic appliances and transmit them to the next layer. HAN refers to a network, which includes electronic and smart devices of a home. The second type, i.e., the BAN, represents a network, which comprises devices and technologies required for the functionality of an organization. Lastly, the IAN identifies a network, which incorporates all the functional elements required for industry. As illustrated in Fig. 3, the devices of these networks usually utilize ZigBee and Z-wave [14], [54]. In rare cases, they also can use IEEE 802.11 (Wi-Fi) or Power Line Communications (PLC).

On the other hand, the second layer refers to the Neighbor Area Network (NAN) which identifies a small geographic area of multiple HANs, BANs and IANs. This network comprises data collector devices that communicate with smart meters of the previous networks and aggregate the information coming from them. In this kind of network, the respective devices usually employ IEEE 802.16 (WiMAX - Worldwide Interoperability for Microwave Access), IEEE 802.11 (WiFi

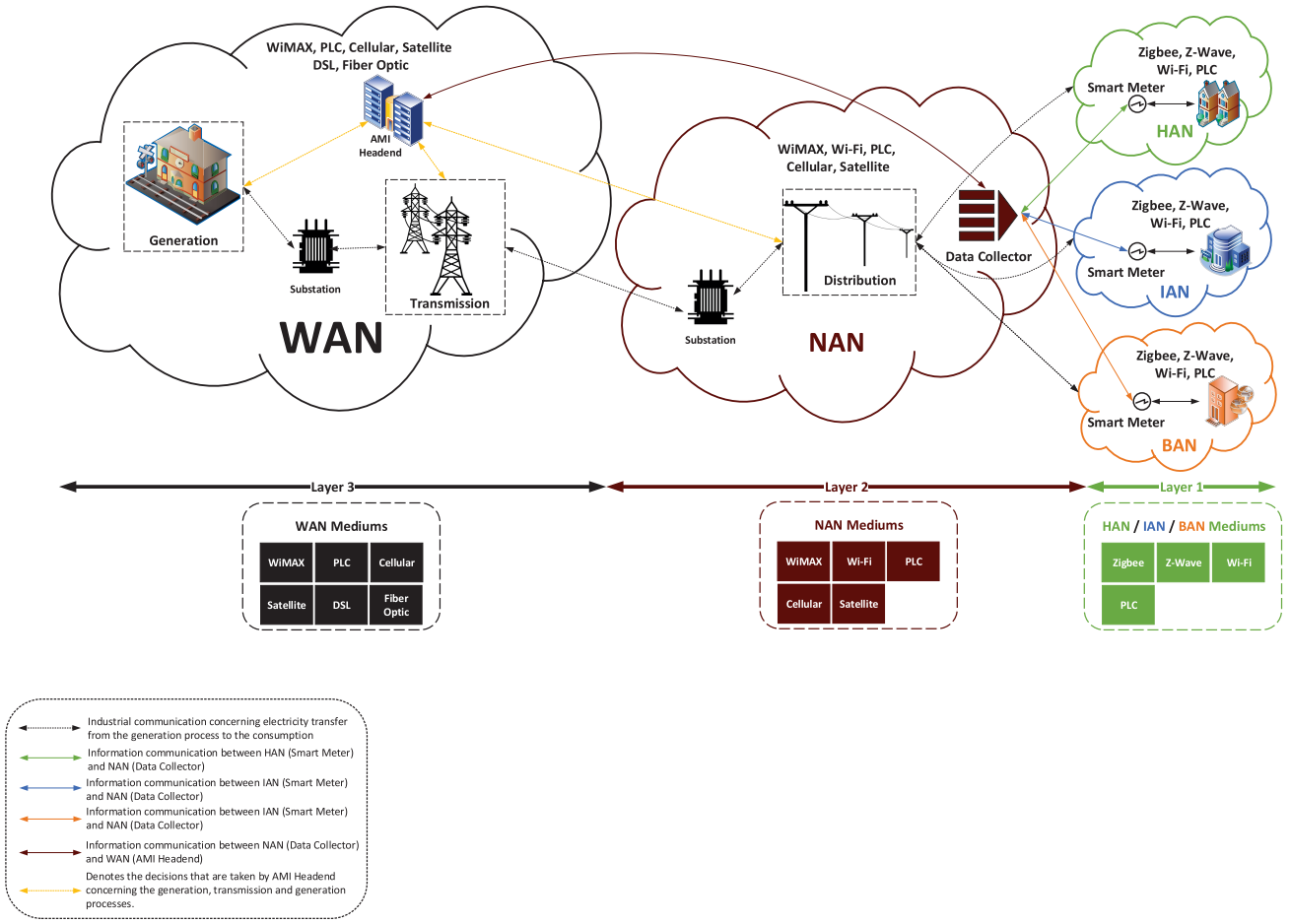

FIGURE 3. The SG architecture in terms of communication.

- Wireless Fidelity) standards [14], [54]. Alternatively, they can also use PLC, satellite, cellular, or Digital Subscriber Line (DSL) communications.

The third layer is characterized by the Wide Area Networks (WANs) that are responsible for connecting multiple NANs with many other entities such as the AMI headend, microgrids and transmission networks. This layer aggregates various information from multiple entities in order to optimize the generation, transmission and distribution processes. The elements of the particular network can communicate with each other with various communication types such as IEEE 802.16, PLC, DSL, satellite, cellular and fibre-optic communications [14], [54].

Finally, it should be noted that Fig. 3 presents a general architectural schema, from which one or more network areas can be excluded in some cases. For example, the presence of NAN can be excluded in some cases where the data collector is not needed. Nevertheless, the exclusion of NAN does not exclude the distribution process.

IV. OVERVIEW OF IDPS SYSTEMS

The rapid evolution of the computing systems and the global utilization of Internet generate new security threats as well as the need for appropriate security measures such as the IDPS systems. According to the RFC document 2828, the intrusion detection process aims at auditing and analyzing security events in order to identify timely potential malicious activities. In 1980, the term of IDS was introduced, which can be considered as a hardware and/or software system automating the process of monitoring, auditing, analyzing and identifying possible threats. Specifically, in 1980, James Anderson [59] inferred that the log files of a computing system can be a very efficient source for monitoring its state and how the individual users interact with it. Based on Anderson's technical report, researchers started to develop the first IDSs that suitably analyzed log files for facilitating the security administrators' work. A remarkable case is Dorothy Denning's paper [60], in which she proposed a theoretical IDS model that is based on an abstract pattern of features. Based on her work, if a computing system does not meet the features defined, then it will have probably been affected by a kind of threat. The next subsections provide an overview of the IDPS systems, emphasizing the architecture and the detection techniques.

A. ARCHITECTURE OF IDPS SYSTEMS

As illustrated in Fig. 4 an IDS usually consists of three main modules: a) one or more Agents, b) the Analysis Engine

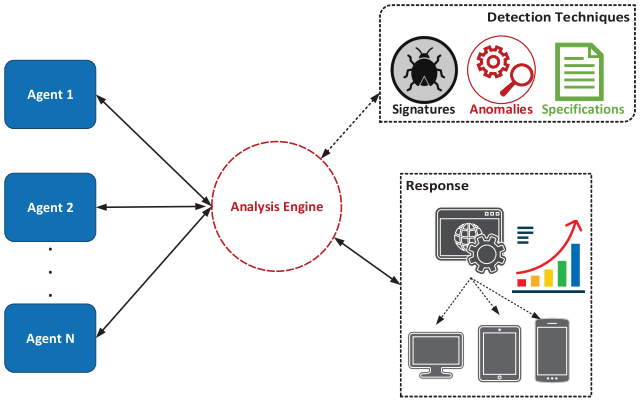

FIGURE 4. IDS/IPS architecture.

and c) the Response Module. The Agents aim at auditing and collecting useful information that is preprocessed and transmitted to the Analysis Engine. Usually, this information is obtained from the log files and network traffic. The number of Agents is defined depending on the network topology. In this context, based on the Agent location, an IDS can be classified into three categories: a) Host-based IDS (HIDS), b) Network-based IDS (NIDS) and c) Distributed IDS. The first type, called HIDS monitors and records only data related to a single computing system, such as the processes of the operating system and system calls. NIDS focuses on the total network traffic, which is exchanged between the entities of a network, by analyzing attributes and patterns of the communication protocols. Finally, the Distributed IDS combines the two aforementioned cases by aggregating information regarding the total network traffic (case of NIDS) as well as utilizing appropriate agents, each of which can monitor a single computing system, as in the case of HIDS. Next, the Analysis Engine aims at analyzing the collected information and detecting cyberattack patterns or possible abnormal behaviors, utilizing specific attack signatures or statistical and artificial intelligence techniques. Finally, the Response Module informs the system administrator through alerts and warnings regarding the outcome of the Analysis Engine. In some cases, the Response Module may be able to execute specific actions to mitigate automatically the intrusions. In such a case, the system is called IPS.

B. INTRUSION DETECTION TECHNIQUES

The Analysis Engine utilizes specific techniques to detect possible threats and anomalies. Mainly, three types of intrusion detection techniques are defined: a) Signature-based, b) Anomaly-based and c) Specification-based. The functionality of the first type (Signature-based) is based on matching the actions that take place in a computing system with a predetermined set of intrusion patterns called signatures. If the characteristics of an action match with one of the signatures, then a corresponding alert is extracted. It is noteworthy that this technique requires the knowledge of all vulnerabilities of the system tested. The use of this technique yields great reliability with a low rate of false positives, but its weak point lies in the inability to detect unknown attacks that are not specified by any signature. As a result, IDPSs utilizing this method must refresh regularly the set of signatures in order to include new kinds of attacks. On the other side, the functionality of the second technique (Anomaly-based) is based on the determination of the abnormal behaviors as intrusions. Usually, this method employs statistical analysis processes or machine learning techniques such as Bayesian networks, neural networks [61], [62] and Markov models to detect malicious activities. The use of this technique is more inaccurate in comparison with the previous one. However, it has the advantage of recognizing unknown cyberattacks. Finally, the third technique (Specification-based) utilizes a set of predetermined rules that define the normal behavior of the system tested. These rules are called specifications. If the characteristics of an action differ with one of the specifications, then a corresponding alert is exported. Therefore, this method can detect unknown attacks, since it can detect the possible anomalies. In comparison with the signature-based approach, this technique is based on the assumption that if all specifications are applied, the security policy of the system cannot be compromised. Conversely, the signature-based technique does not make any such assumption. At this point, it should be noted that the term 'hybrid' is adopted from now on for characterizing an IDPS that use two or more of the above techniques.

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

$$TPR = \frac{TP}{TP + FN} \tag{3}$$

$$TNR = \frac{TN}{TN + FP} \tag{4}$$

$$FPR = \frac{FP}{FP + TN} = 1 - TNR \tag{5}$$

$$FNR = \frac{FN}{FN + TP} = 1 - TPR \tag{6}$$

V. REQUIREMENTS OF IDPS SYSTEMS IN THE SMART GRID

The IDPS systems devoted to protecting SG present different requirements compared to the IDPS of the conventional computer networks. Therefore this section is focused on analyzing these requirements and the evaluation metrics we adopt for evaluating and comparing the IDPS cases studied in the next section. According to the previous IDPS overview, the primary purpose of an IDPS system is to identify timely indications of possible intrusions attempts. It would be desirable that the results of an intrusion detection process can originate from the value of a binary variable. However, the cyberattacks are characterized by more complicated operations and the information generated by IDPSs is more complex.

Consequently, we identify the following requirements for evaluating the performance of the IDPS cases in the next section.

- **Detecting a wide range of intrusions**: Identifying malicious activities that originate from external unauthorized users or malicious insiders. It should be highlighted that the modern IDPSs must include appropriate mechanisms to deal with zero-day attacks.
- **Timely intrusion detection**: The term 'timely' does not necessarily refer to real-time detection, as this state introduces significant operational and response issues. However, it is required to detect an intrusion within a reasonable time. Thus, the detection latency should be calculated during the development and testing process of a modern IDPS.
- **High detection performance**: A number of basic terms are explained before defining the adopted IDPS performance metrics in this work. As True Positive (TP) is considered as the number of the correct classifications that detected the cyberattacks as abnormal behavior. On the other hand, as True Negative (TN) is identified as the number of correct classifications that recognized non-malicious activities as normal behavior. Accordingly, as False Positive (FP) is considered as the number of incorrect classifications that identified non-malicious activities as abnormal behavior. Finally, as False Negative (FN) is deemed as the number of incorrect classifications that recognized cyberattacks as normal behavior. On the basis of these terms, many metrics can be calculated to evaluate the classification performance. Some of them that are defined by the Equations (1)-(6) are: Accuracy (ACC), Precision, True Positive Rate (TPR), False Positive Rate (FPR), True Negative Rate (TNR) and the False Negative Rate (FNR). It should be noted that TPR is also called 'detection rate', 'recall', 'sensitivity' or 'probability of detection'. More detailed, ACC represents the ratio between the correct predictions and the total number of samples. ACC is considered as an efficient metric when there is an equal number of samples between the predefined classes. For instance, if a training set is composed of 98% normal behavior samples and 2% malicious behavior samples, then the training accuracy of the classification model can easily reach 98%, predicting each case as normal behavior. Conversely, if the training set consists of 60% normal behaviors samples and 40% malicious behaviors samples, then the training accuracy may be reduced to 60%. Therefore, in some cases, ACC can mislead a security operator, by giving the false sense of achieving high classification accuracy. Precision is calculated by dividing TP with the sum of TP and FP. Particularly, Precision expresses what proportion of samples that are classified as malicious behavior, indeed present a malicious behavior. Consequently, Precision provides information concerning the performance of the classification with respect to FP; nevertheless we consider that an intrusion detection classification in an industrial environment, such as SG should pay more attention to FN. Accordingly, TPR is calculated by dividing TP with the sum of TP and FN. Specifically, this metric measures what proportion of intrusions that truly present a malicious behavior was categorized by the classification model as an intrusion. In contrast to Precision, TPR provides information with respect to FN. TNR is the fraction between TN and the sum of TN and FP, indicating the proportion of normal behaviors that are predicted as normal. Actually, TNR is the opposite of TPR. In some cases, TNR is also called as Specificity or Selectivity. FPR or differently Fall-Out is calculated by dividing FP with the sum of FP and TN. Actually, FPR is the opposite of TNR, identifying the proportion of normal behaviors that are detected as intrusions. Finally, FNR is the fraction of FN with the sum of FN and TP. Respectively with the previous case, FNR is the opposite of TPR, indicating the proportion of intrusions that are detected as normal behaviors. Also, it is worth mentioning that many researchers utilize Receiver Operating Characteristic (ROC) curves to evaluate the performance of a classifier. This curve constitutes a graphical plot between FPR in the x-axis and TPR in the y-axis. Normally, in order to define the performance of ROC curve in a numerical value, the Area Under the Curve (AUC) is calculated. This value refers to the probability of a classifier to rank a randomly selected positive event higher than a randomly selected negative event.
- **Attentive performance of computing resources**: Some entities in SG, such as the smart meters, are characterized by constrained computing resources. Therefore, they may not support the computationally expensive operations of the conventional IDPSs. Consequently, the memory, the computational power and the energy consumption should be taken into consideration during the development and testing process of an IDPS.
- **Scalability**: SG consists of several technologies and components that define the corresponding different communication interfaces. Therefore, an efficient IDPS for SG should be scalable, having the capability to monitor and interpret these communications, by decoding and analyzing the corresponding communication protocols of SG, thus identifying possible cyberattack patterns. Moreover, it should be capable of aggregating and analyzing logs from the various SG components.
- **Resilient against Cyberattacks**: An IDPS for SG should be resilient against cyberattacks, possessing the capability to prevent various cyberattacks, protect itself and activate appropriate self-healing mechanisms in case of emergency. For instance, if a cyberattack cannot be hindered, an appropriate mechanism should replace the violated component, thus ensuring the normal operation.
- **Friendly visual-based user interface**: The information generated by IDPS (alerts and warnings) should be

presented appropriately to the SG operator or the security administrator.

VI. IDPS SYSTEMS IN THE SMART GRID

It is clear that the IDPS systems devoted to protecting SG differ substantially from the IDPSs focused on conventional computer networks. In particular, the multiple interconnected and at the same time, independent interactions among the aforementioned SG components require a distributed IDPS which will be able to monitor and control the network traffic and syslogs of all subsystems and connections. Moreover, such an IDPS has to take into account the hybrid nature of SG which includes both industrial and ICT components. Specifically, it has to adapt its functionality depending on the legacy nature and constrained computing capabilities of the industrial and IoT devices, such as RTUs and smart meters. Finally, it has to handle and address timely a wide variety of cyberattacks and possible anomalies due to the heterogeneous character of SG components.

In this section, we study 37 different cases of IDPSs for SG. Table 1 summarizes these cases cumulatively, while Table 2 compares them by presenting their most significant characteristics. The comparison of the IDPSs examined is based on the target system they monitor as well as their detection technique and performance. The target system can be a) the entire SG ecosystem, b) AMI, c) SCADA system, d) substation and e) synchrophasor. In particular, subsection VI-A discusses the IDPS systems concerning the entire SG ecosystem. Subsection VI-B presents those IDPSs focusing on AMI. Subsections VI-C and VI-D are devoted to the IDPSs monitoring the SCADA systems and substations respectively. Finally, subsection VI-E focuses on IDPSs regarding synchrophasors. Since each IDPS is devoted to protecting a specific category of target systems, we can examine and compare their architecture, detection technique, the kinds of cyberattacks they can detect and finally their performance.

A. IDPS SYSTEMS FOR THE ENTIRE SG ECOSYSTEM

As described before, SG consists of multiple and heterogeneous communications that may present various security gaps and vulnerabilities, thereby making it possible to launch disastrous cyberattacks. Moreover, SG includes components characterized by constrained resources that hinder the adoption of conventional cybersecurity mechanisms. Thus, it is clear that the presence of efficient and lightweight IDPS systems is necessary for the protection of SG. Subsequently, we investigate per paragraph appropriate IDPS systems capable of protecting the entire SG ecosystem.

In [63], the authors proposed an IDS for the entire SG ecosystem, whose functionality is mainly based on three entities: a) an Ontology Knowledge Base (OKB), b) a Support Vector Machine (SVM) [64] model and c) a fuzzy risk analyzer. The system architecture consists of a number of HIDSs and NIDSs that are allocated to different elements of SG. In more detail, each NIDS or HIDS includes four function modules: a) the trust manager, b) the autonomic manager, c) the knowledge manager and d) the fuzzy risk manager. The detection of the possible threats is accomplished by applying an SVM [64] model whose training process lasted for 30 hours by using a dataset, which includes 3600 records of attacks. The specific dataset is a part of OKB and includes a) records from the KDD 1999 dataset [65] and b) simulated experiments from the authors. It includes multiple types of

TABLE 1. A summarized presentation of the most important features found in compiling IDPSs for the smart grid paradigm.

Important Features	Values
Number of IDPSs that focused on the entire SG ecosystem	3
Number of IDPSs that focused on AMI	13
Number of IDPSs that focused on SCADA	10
Number of IDPSs that focused on Substations	8
Number of IDPSs that focused on Synchrophasors	3
Number of IDPSs that used signature-based technique	3
Number of IDPSs that used anomaly-based technique	17
Number of IDPSs that used specification-based technique	12
Hybrid IDPSs	5
Visual-based IDPSs	1
IDPSs that take account resource consumption	2
IDPSs that calculate detection latency	0
IDPSs comprising self-hiling capabilities	0
Utilized Public Datasets	1. KDD CUP 1999 [65] 2. NSL-KDD [65], [68], [69] 3. ADFA-LD [78], [79] 4. CER Smart Metering Project [82] 5. ISCX2012 [88], [89]
Utilized Software Packages	1. Suricata [105], [139], [140] 2. MOA [74]–[76] 3. Protege [66] 4. Matlab 5. NS2 [85] 6. WEKA [70], [71] 7. Table TstBench [94] 8. VirtualBox [162] 9. Python 10. Wireshark [112]–[114] 11. Snort [104]–[106] 12. OpenPDC [156], [157] 13. NRL core [159], [160] 14. OpenPMU [163] 15. C/C++ 16. ITACA [128] 17. Pcapy [115] 18. Impacket [116] 19. Conpot [123] 20. MongoDB [125], [126] 21. THC Hydra [150] 22. Seringe [151] 23. Colasoft Packet Builder [164] 24. Nmap [165] 25. Metasploit [166], [167] 26. hping [168]

TABLE 2. Summary of 37 IDPSs cases in SG.

Literature work	Target System	Detection Technique	Protocols	Attacks	Performance	Dataset	Software
A. Patel et al. [63]	Etire SG ecosystem	Anomaly-based	Not provided	1. Dos Attacks 2. Packet splitting 3. Command insertion 4. Shellcode mutation 5. Brute force attacks 6. Payload mutation 7. Duplicate Insertion	AUC = 0.99451	1. KDD CUP 1999 [65] 2. Simulated data	Protege [66]
Y. Zhang et al. [67]	Entire SG ecosystem	Anomaly-based	Not provided	1. DoS attacks 2. U2R attacks 3. R2L attacks 4. Probing attacks	1. CLONALG ACC = [80.1%, 99.7%] 2. AIRS2Parallel ACC = [82.1%, 98.7%]	NSL-KDD [65], [68], [69]	1. Matlab 2. WEKA [70], [71]
Q.He and R.S. Blum [72]	Entire SG ecosystem	Anomaly-based	Not provided	Not provided	TPR = 95%	Not required	Not provided
M.A. Faisal et al. [73]	AMI	Anomaly-based	Not provided	1. DoS attacks 2. R2L attacks 3. U2R attacks 4. Probing attacks	1. ACC, FPR, FNR, Size, Running time, RAM-Hours of Active Classifier = 94.67%, 3.31%, 9.13%, 134.55 KB, 3.46 secs., 1.23E-7. 2. ACC, FPR, FNR, Size, Running time, RAM-Hours of Leveraging Bagging = 98.33%, 0.78%, 5.15%, 401.01 KB, 20.92 secs., 2.22E-6. 3. ACC, FPR, FNR, Size Running time, RAM-Hours of Single Classifier Drift = 97.74%, 1.07%, 6.79%, 187.30KB, 6.74 secs., 3.34E-7.	1. KDD CUP 1999 [65] 2. NSL-KDD [65], [68], [69]	MOA [74]–[76]
R. Vijayanand [77]	AMI	Anomaly-based	Not provided	1. Exploits 2. DoS attacks 3. Fuzzers 4. Backdoor attacks 5. Worms 6. Generic attacks	1. ACC > 90% 2. TPR = 89.2% 3. TNR = 93.4%	ADFA-LD [78], [79]	Matlab
Y. Li et al [80]	AMI	Anomaly-based	Not provided	Not provided	1. ACC = 97.239% 2. FPR = 5.897% 3. FNR = 3.614%	CER Smart Metering Project [82]	Not provided
P.Y. Chen [83]	AMI	Anomaly-based	Not provided	False data injection attacks	1. FPR of the first attack = 0% 2. FPR of the second attack = 0.43%	Not required	Not provided
N. Boumkheld et al. [84]	AMI	Anomaly-based	AODV [86]	Blackhole attacks	1. TPR = 100% 2. ACC = 99% 3. Precision = 66% 4. AUC = 1	Simulated data	1. NS2 [85] 2. WEKA [70], [71]
I. Ullah and H. Mahmoud [87]	AMI	Anomaly-based	Not provided	1. DoS attacks 2. L2L attacks 3. Secure shell attacks 4. Botnet	1. Precision = 99.70% 2. TPR = 99.60%	ISCX2012 [88], [89]	WEKA [70], [71]
F.A.A. Alseiari and Z. Aung [91]	AMI	Anomaly-based	Not provided	1. DoS attacks 2. Port scanning	Figures present the values of TPR and FPR.	Simulated data	Not provided
V. Gulisano et al. [92]	AMI	Anomaly-based	Not provided	Energy exfiltration attacks	TPR = 91%	Not provided	Not provided
R. Berthier and W.H. Sanders [94]	AMI	Specification-based	ANSI C12.22	1. Meter reading attacks 2. Service switch attacks	1. TPR = 100% 2. TNR = 99.57% 3. CPU Consumption = 0.3% 4. RAM Consumption = 10MB	Not required	1. Table TstBench [94] 2. VirtualBox [162] 3. Python
X. Liu et al. [97]	AMI	Specification-based	Not provided	False data injection attacks	Figures present the values of TPR	Not required	Not provided
R. Mitchell and R. Chen [98]	AMI	Specification-based	Not provided	1. Reckless attacks 2. Random attacks	1. TPR = 100% 2. FPR of reckless attacks $\leq 0.2\%$ 3. FPR of random attacks $\leq 0.6\%$ 4. ROC curves are presented	Not required	Not provided
P.Jokar and V.Leung [99]	AMI	Specification-based	1. ZigBee	1. Spoofing attacks 2. Radio Jamming 3. Replay attacks 4. Stenography attacks 5. Back-off manipulation 6. DoS against CFP 7. DoS against GTS	1. Theoretical analysis 2. ROC curves are presented	Not required	Matlab
M. Attia et al. [102]	AMI	Specification-based	Not provided	1. Blackhole attacks 2. Time delay attacks	1. TPR = 90% 2. FPR = 6%	Not required	Matlab
T.H. Morris et al. [103]	SCADA	Signature-based	Modbus [55]–[57]	Not provided	Not provided	Not required	Snort [104]–[106]
H. Li et al. [107]	SCADA	Signature-based	DNP3 [58]	1. Protocol anomalies 2. Reconnaissance attacks 3. DoS attacks 4. Mixed attacks	Not provided	Not required	Snort [104]–[106]

TABLE 2. Summary of 37 IDPSs cases in SG.

E. Hodo et al. [108]	SCADA	Anomaly-based	IEC-104 [109]	1. ARP attacks 2. DoS attacks 3. Replay attacks	1. TPR, FPR, Precision, AUC of Naive Bayes = 0.846, 0.055, 0.907, 0.905 2. TPR, FPR, Precision, AUC of IBk = 0.847, 0.300, 0.850, 0.766 3. TPR, FPR, Precision, AUC of J48 = 0.917, 0.090, 0928, 0.929 4. TPR, FPR, Precision, AUC of RandomForest = 0.914, 0.136, 0.919, 0.965 5. TPR, FPR, Precision, AUC of RandomTree = 0.894, 0.210, 0.895, 0.843 6. TPR, FPR, Precision, AUC of DecisionTable = 0.917, 0.062, 0.933, 0.963 7. TPR, FPR, Precision, AUC of OneR = 0.846, 0.328, 0.845, 0.759	IEC-104 dataset generated by the authors	WEKA [70], [71]
N. Goldenberg and A. Wool [111]	SCADA	Anomaly-based	Modbus [55]–[57]	Not Provided	1. ACC = 100% 2. Precision = 100% 3.TPR = 100% 4. TNR = 100% 5. FPR = 0% 6. FNR = 0%	Real datasets generated by authors	1. Wireshark [112]–[114] 2. Pcapy [115] 3. Impacket [116]
S.D. Anton et al. [117]	SCADA	Anomaly-based	Modbus [55]–[57]	Not provided	1. ACC of SVM with DS1, DS2 and DS3 is 100%, 100% and 99.99% respectively 2. ACC of Random Forest with DS1, DS2 and DS3 is 100%, 99.99% and 99.99% 3. ACC of KNN with DS1, DS2 and DS3 is 99.7%, 99.9% and 99.9%. 4. ACC of k-means with DS1, DS2 and DS3 is 98.1%, 55.62% and 63.36%	Lemay and Fernandez [118]	Not provided
P.H. Wang et al. [121]	SCADA	Anomaly-based	Modbus [55]–[57]	1. Reconnaissance attacks 2. DoS attacks	1. TPR of reconnaissance attacks = 90% 2. TPR of DoS attacks = 95.12%	Data from a honeypot	1. Conpot [123], 2. Python 2.7 3. MongoDB [125], [126]
Y. Yang et al. [127]	SCADA	Specification-based	IEC-104 [109]	1. Packet injection attacks 2. Replay attacks 3. Data manipulation	1. ACC = 100% 2. Precision = 100% 3. TPR = 100% 4. TNR = 100% 5. FPR = 0% 6. FNR = 0%	Not required	ITACA [128]
Y. Yang et al. [129]	SCADA	Hybrid	IEC-104 [109]	1. Unauthorized read commands 2. Unauthorized reset commands 3. Unauthorized remote control and adjustment commands 4. Spontaneous packets storm 5. Unauthorized interrogation commands 6. Buffer overflows 7. Unauthorized broadcast requests 8. IEC-104 port communication	1. ACC = 100% 2. Precision = 100% 3. TPR = 100% 4. TNR = 100% 5. FPR = 0% 6. FNR = 0%	Not required	Snort [104]–[106]
Z.Feng et al. [130]	SCADA	Hybrid	Profinet	1. Reconnaissance attacks 2. DoS attacks 3. MiTM attacks 4. Protocol anomalies	Numerical results are not provided	Not required	Snort [104]–[106]
S.C. Li et al. [135]	SCADA	Anomaly-based	Modbus [55]–[57]	1. Reconnaissance attacks 2. Response injection attacks 3. Command injection attacks 4. DoS attacks	1. ACC of j48 = 99.8361% 2. ACC of 1st neural network = 97.4185% 3. ACC of 2nd neural network = 97.4603% 4. ACC of 3rd neural network = 97.3876%	Simulated dataset generated by authors	1. Wireshark [112]–[114] 2. WEKA [70], [71]
B. Kang et al. [138]	Substation	Signature-based	MMS [141] / IEC 61850 [41], [42]	Active power limitation attacks	Two examples that were detected.	Not required	Suricata [105], [139], [140]
Y. Kwon et al. [142]	Substation	Specification-based	1. MMS [141] / IEC 61850 [41], [42] 2. GOOSE [143] / IEC 61850 [41], [42]	1. DoS attacks 2. Port scanning 3. Portable executable attacks 4. GOOSE attacks 5. MMS attacks 6. SNMP attacks	1. FPR = 0% 2. FNR = 1.1% 3. TPR = 98.9% 4. Precision = 100%	Real data from a substation in South Korea	Wireshark [112]–[114]

TABLE 2. Summary of 37 IDPSs cases in SG.

Y. Yang et al. [144]	Substation	Specification-based	1. MMS [141] / IEC 61850 [41], [42] 2. GOOSE [143] / IEC 61850 [41], [42] 3. SMV [42] / IEC 61850 [41], [42]	1. DoS attacks 2. MiTM attacks 3. Packet injection	Not provided	Real data from a substation in China	1. ITACA [128] 2. Wireshark [112]–[114]
M. Kabir-Querrec et al. [145]	Substation	Specification-based	GOOSE [143] / IEC 61850 [41], [42]	Not Provided	Not provided	Not required	Not Provided
H. Yoo and T. Shon [146]	Substation	Anomaly-based	1. MMS [141] / IEC 61850 [41], [42] 2. GOOSE [143] / IEC 61850 [41], [42]	Not Provided	FPR = $[1\%, 6\%]$	Real data from a substation	WEKA [70], [71]
U. Premaratne et al. [149]	Substation	Hybrid	IEC 61850 [41], [42]	1. DoS attacks 2. Traffic analysis attacks 3. Password cracking attacks	Not provided	Real data from a substation	1. Snort [104]–[106] 2. THC Hydra [150] 3. Seringe [151]
J. Hong et al. [152]	Substation	Specification-based	1. GOOSE [143] / IEC 61850 [41], [42] 2. SMV [42] / IEC 61850 [41], [42]	1. DoS attacks 2. Replay attacks	FPR= 1.61×10^{-4}	Not required	1. Wireshark [112]–[114] 2. Colasoft Packet Builder [164] 3. Nmap [165]
Y. Yang et al. [153]	Substation	Specification-based	1. MMS [141] / IEC 61850 [41], [42] 2. GOOSE [143] / IEC 61850 [41], [42] 3. SMV [42] / IEC 61850 [41], [42]	1. DoS attacks 2. MiTM attacks 3. Packet injection	Not provided	Real data from a substation in China	1. ITACA [128] 2. Wireshark [112]–[114]
S.Pan et al. [155]	Synchrophasor	Hybrid	Not provided	1. Single line-to-ground faults 2. Replay attacks 3. Command injection attacks 4. Disable relay attacks	ACC = 90.4%	Simulated data	1. Snort [104]–[106] 2. OpenPDC [156], [157]
R.Khan et al. [158]	Synchrophasor	Hybrid	IEEE C37.118 [154]	1. ARP spoofing attacks 2. Port scanning 3. GPS spoofing 4. Packet drop attacks 5. Replay attacks 6. Command injection attacks 7. Physical attacks	Not provided	Not required	1. NRL core [159], [160] 2. OpenPMU [163] 3. C/C++
Y. Yang et al. [161]	Synchrophasor	Specification-based	IEEE C37.118 [154]	1. Reconnaissance attacks 2. MiTM attacks 3. DoS attacks	FPR= 0%	Not required	1. ITACA [128] 2. Nmap [165] 3. Metasploit [166], [167] 4. hping [168]

attacks, such as DoS attacks, packet splitting attacks, command insertion attacks, payload mutation attacks, brute force attacks, duplicate insertion and shellcode mutation attacks. Next, in order to reduce the FP alarms, the authors utilized a fuzzy logic technique to determine a risk value for each element of the SG environment. These values vary from 0 to 1. Finally, OKB is employed to identify the targets of attacks. An ontology can be characterized as a dictionary which determines the information about an application domain and the relations between them. By using the Protege software [66], the particular IDS is connected to the CoreSec ontology in order to determine the most appropriate option of OKB. Concerning the evaluation of the proposed system, the authors argue that AUC approaches 0.99451.

In this article [67], Y. Zhang et al. suggested a distributed IDS for the entire SG ecosystem, which is called SGDIDS and is based on the functionality of an Artificial Immune System (AIS). The particular system consists of individual IDS modules that cooperate in a hierarchical manner. More concretely, each HAN, NAN and WAN includes a distinct IDS which is responsible for monitoring and controlling the corresponding communications. The HAN IDS is composed of three units: a) data collector unit, b) AIS classification model and c) detection results recording unit. On the other

hand, the NAN IDS receives the results of HAN IDSs and also utilizes the AIS algorithms. Accordingly, the WAN IDS obtains the alerts or warnings of the NAN IDSs and utilizes the same classification algorithms. If a lower layer IDS (e.g., HAN IDS) cannot classify some network activities, then the next higher layer IDS (e.g., NAN IDS) will undertake to categorize these activities. Each IDS employs the CLONALG and AIRS2Parallel detection algorithms. However, each type of the previous IDSs was trained with different samples of the NSL-KDD dataset [65], [68], [69], since different areas networks are commonly exposed to different attacks. The training processes were carried out with the utilization of the WEKA [70], [71] software package. Finally, the authors argue that ACC of the CLONALG and AIRS2Parallel algorithms reach 99.7% and 98.7% respectively.

In this work [72], the authors proposed new locally optimum tests and apply them in SG intrusion and fault detection problems. Considering that the dynamic time behavior of an examined system can be approached as a discrete-time linear state-space model, a failure or intrusion can be recognized by observing a change in specific system parameters. In particular, one way to detect such changes is the utilization of hypothesis testing. For this reason, the authors develop two locally optimum tests: the Locally Optimum Unknown Direction (LOUD) and the Locally Optimum Estimated Direction (LOED) tests. Both of them are appropriate for detecting small changes in the examined system. However, if the change is large, the Generalized Likelihood Ratio (GLR) test can be applied in this case. Consequently, in this paper, the combination of the above methods was proposed, i.e., the LOUD-GLR and the LOED-GLR tests. The combined test employ LOUD or LOED, if the change in the system is quite small and then switches to GLR, if the change looks large. Finally, concerning the evaluation of the proposed method, the best TPR approaches 95%.

B. IDPS SYSTEMS FOR AMI

AMI constitutes the main novelty of SG which enables a bidirectional communication between the utility companies and energy consumers. Nevertheless, although this communication benefits both directions, it is based on ICT services and components that may be characterized by severe vulnerabilities. A characteristic example is the false data injection attacks against smart meters. Hence, the corresponding intrusion detection mechanisms should be adapted appropriately in order to control AMI components. The following paragraphs analyze IDPS systems suitable for the AMI protection.

In this article [73], the authors presented a novel intrusion detection architecture for AMI and evaluated a plethora of evolving machine learning algorithms by using the Massive Online Analysis (MOA) software [74]–[76]. In particular, the proposed architecture consists of three different IDSs, which can be installed in smart meters, data collectors and AMI headends respectively. Each IDS includes four components: a) the data acceptor module, b) the pre-processing unit, c) the stream mining module and d) the decision-making unit. It is worth mentioning that IDSs can either be incorporated into the AMI components or can be implemented as an individual hardware card. Regarding the evaluation of the evolving machine learning algorithms, the authors utilized the KDD CUP 1999 dataset and an improved version of this, called NSL-KDD [65], [68], [69] that include multiple types of attacks, such as, DoS, Remote to Local (R2L) attacks, User to Root (U2R) attacks and probing attacks. Also, they utilized multiple evaluation measures such as: a) ACC, b) the size of the classifier in Kilobyte (KB), c) the processing time of the classifier, d) the consumption rate of the Random Access Memory (RAM), e) FPR and f) FNR. The MOA software provides 16 evolving machine learning algorithms, from which seven were evaluated. These algorithms are a) Accuracy Updated Ensemble b) Active Classifier, c) Leveraging Bagging, d) Limited Attribute Classifier, e) Bagging using ADWIN, f) Bagging using Adaptive-Size Hoeffding Tree and g) Single Classifier Drift. Active Classifier and Single Classifier Drift are proposed for the IDS which controls network activities of smart meters. Correspondingly, the authors consider that the Leveraging Bagging algorithm is suitable for the IDS which is responsible for the data collector. Finally, the Active Classifier algorithm is suggested for the IDS of the AMI headends.

In [77] R. Vijayanand et al. presented an anomaly-based IDS which controls the AMI communications. In detail, the proposed system is integrated into the data collector and utilizes a Multi-SVM classifier [64]. A Multi-SVM [64] classifier consists of multiple SVM [64] classifiers that can detect various types of attacks. More specifically, the authors employed the ADFA-LD dataset [78], [79] and applied the mutual information technique to select the most important features from the particular dataset. The mutual information technique is a filter feature selection method which is based on the entropy concept and distinguishes those features that achieve the best classification ACC. The features that were selected from ADFA-LD Dataset are a) Source bytes, b) Destination time to leave (ttl), c) Source mean, d) Destination mean and e) Ct_state_ttl. The possible attacks that can be detected utilizing the aforementioned features are a) exploits, b) DoS attacks, c) fuzzers, d) backdoors, e) worms and f) generic attacks. Considering the training process of the proposed model, for each of these attacks, an SVM [64] classifier was developed by using a different kernel function. In particular, the polynomial function was employed for DoS and backdoor attacks; the Gaussian function was utilized for normal behaviors and generic attacks and the mlp function was used for worms, fuzzers and exploits. Concerning the evaluation of the proposed system, ACC exceeds 90%. TPR and TNR are calculated at 89.2% and 93.4% respectively. Finally, it is worth mentioning that the training and testing processes were conducted by using the Matlab software package.

Li *et al.* [80] introduced an intrusion detection method for AMI, whose operation is mainly based on the Online Sequence Extreme Learning Machine (OS-ELM) [81].

OS-ELM is a special feedforward neural network model which utilizes the online sequence learning for its training process. More specifically, their methodology consists of three phases: a) data preprocessing phase, b) initialization phase and c) online sequence learning phase. In the first phase, the training data is preprocessed by using the Gain Ratio Evaluation feature selection method. The second phase initializes randomly the parameters for the training process of the neural network. Finally, the third method constitutes the training process. The dataset that was employed for the training process can be found on the website [82]. However, it is highlighted that the specific dataset does not include network records that identify cyberattacks nor abnormal behavior patterns. Regarding the evaluation process, multiple experiments were conducted in order to determine the appropriate parameters for the proposed model. Moreover, the authors evaluated their model with other classification algorithms. They claim that their solution overtakes the other algorithms and ACC approaches 97.239%. Accordingly, FPR and FNR are calculated at 5.897 and 3.614 respectively.

This article [83] describes an anomaly-based intrusion detection method which focuses on the false data injection attacks. In particular, the proposed method is based on a spatiotemporal evaluation, which controls the correlations between the state estimations of AMI. As state estimations are considered various actions such as, energy supply/demand and electricity pricing. In more detail, the specific method can mainly be divided into two phases. The first method creates a set of state estimations which is characterized by spatial correlations and temporal consistencies. The second method applies a voting system which classifies each state estimation into three categories: a) good, b) abnormal and c) unknown. Concerning the evaluation of the proposed method, two false data injection attacks were simulated. The target of the first attack was to maximize the energy transmission costs, while the second attack intended to cause a power outage. The authors declare that for the first attack, their method does not generate any FP. On the other hand, the second attack results 0.43% FPR.

Boumkheld *et al.* [84] developed an IDS which exclusively focuses on blackhole attacks. The specific kind of attacks constitutes a DoS attack which aims to drop all network packets by advertising malicious nodes or malicious paths. More concretely, their system controls the communications of an AMI NAN. To simulate the specific kind of attack, they utilized the Network Simulator 2 (NS2) [85] simulator and examined the AMI network as an ad-hoc network by using the Ad-Hoc On-Demand Distance Vector (AODV) protocol [86]. In more detail, their simulation includes 100 smart meters nodes, 1 data collector and 2 malicious nodes. The IDS can be considered as a different node that communicates only with the data collector node. In order to detect the possible blackhole attacks, the authors applied the Naive Bayes Classifier which is based on the Bayes theorem. The features that were used as input in the Naive Bayes Classifier are a) the number of route request packets, b) the number of route reply packets and c) the number of dropped packets. Finally, to evaluate their IDS they used the Waikato Environment for Knowledge Analysis (WEKA) [70], [71] software. The authors claim that their system recorded 100%*TPR*, 99%*ACC*, 66% Precision and AUC approaches 1.

I. Ullah and H. Mahmoud in [87] presented an intrusion detection framework for AMI, which also applies the anomaly detection technique. The architecture of the proposed system is composed of individual IDS modules that are placed in different locations in HANs, NAN and WAN correspondingly. If an IDS module detects a possible threat, then a related notification will be sent to the system administrator of AMI. Also, there is a central IDS module which aggregates and examines further the alarms generated by the various IDS modules. The authors utilized the ISCX2012 dataset [88], [89] and the WEKA [70], [71] software in order to evaluate a plethora of machine learning classification algorithms. The particular dataset includes various network attacks that are classified into four categories: DoS, LAN to LAN (L2L), Secure Shell (SSH) and Botnet. They evaluated 20 algorithms of which the most efficient are: J48 [90], JRip, BayesNet, SVM [64] and MLP. The most efficient algorithm was J48 [90] which achieved 99.70% Precision and 99.60% TPR.

In this work [91], the authors suggested a flow-based distributed IDS for AMI, based on the clustering technique. The proposed system is composed of multiple IDS units that are installed on the data collectors and the AMI headend. Initially, the IDS units of the data collectors monitor and analyze the network traffic, which is exchanged between the data collectors and smart meters. Subsequently, they detect the potential abnormal flows and send a summary report of them to the IDS unit of the AMI headend. The latter undertakes to investigate further the specific anomalies. The detection process is based on the Mini-Batch K-Means algorithm and a sliding window technique. For the training procedure of the Mini-Batch K-Means clustering algorithm, the authors created their own dataset which consists of the Transmission Control Protocol/Internet Protocol (TCP/IP) network flows features. Also, it is worth mentioning that they utilized the Principal Component Analysis (PCA) technique in order to reduce the dimensionality of the dataset. Finally, the number of clusters (k) was specified at 4, as the specific value achieved the best silhouette score and FPR. In order to evaluate the performance of their model, the authors simulated 3 attack scenarios: a) TCP SYN Flooding DoS attacks, b) stealth port scanning attacks and c) a combination of the previous ones.

Gulisano *et al.* [92] introduced a two-tier IDS which controls the activities that take place on AMI. More concretely, their framework monitors and attempts to detect timely possible attack patterns by analyzing the network traffic features between the communications of the data collectors and smart meters. In order to detect timely the potential threats, the authors adopted the data streaming technique [93], in which the analysis of the communication

traffic is carried out by using acyclic directed graphs. In more detail, their system consists of two modules called Device Modeler and Pattern Matcher respectively. The first module undertakes to monitor the communication traffic and detect attack behaviors utilizing a Bayesian Network. Specifically, it monitors the number of requests from the data collectors, the hour and the ID of smart meters. On the other hand, the second module receives the corresponding alerts and implements a secondary analysis with the support of a cybersecurity specialist. In order to evaluate their system, they simulated energy exfiltration attacks, by introducing incorrect consumption measurements. They report that TPR approaches 91%.

In [94], the authors developed an IDS for AMI, in which the communications are based on the ANSI C12.22 [95] protocol. More specifically, the proposed system utilizes a specification-based model which consists of four modules that were developed by using the Python programming language. The first module is called dissector and its work is to capture the network traffic. The second module called parser analyzes the network traffic by using specific patterns. The third module applies determined specifications that define the normal behavior of a device. Finally, the last module monitors the operational state of the devices that can be characterized by three types: a) 'in-use', b) 'off-line' and c) 'to configure'. The security specifications were determined by combining a specific threat model and a system model based on [96]. In more detail, these specifications are classified into three categories: network-based, device-based and application-based. In order to evaluate the IDS, the authors utilized virtual machines as devices and the Table TstBench software [94] to emulate the ANSI C12.22 protocol. In the experimental section, they state that the proposed IDS scored 100% and 99.57% TPR and TNR respectively. However, it is noteworthy, that only two types of attacks (meter reading attacks and service switch attacks) were examined as abnormal behaviors. Finally, concerning the evaluation of the computational performance, they utilized 0.3% of the Central Processing Unit (CPU) of the virtual machines and 10 MB of memory.

In [97], X.Liu et al. present a specification-based IDS which has been specially designed for the smart meter's communications. Particularly, first, they introduce a modeling process which describes the information exchange among the components of a smart meter based on a colored Petri net. Based on this process, they introduce a threat model which includes two classes of attacks: a) attacks on data and b) attacks on commands. Finally, they propose an IDS for detecting false data injection attacks accomplished via the access of the smart meter's physical memory. The architecture of the proposed IDS consists of three elements: a) Secret Information, b) Event Log and c) Spying Domain. Secret Information is a confidential data structure which is accessible only for the legitimate procedures and also it is utilized to encrypt the Event Log. Event Log is used for storing all the events that are relevant to the smart meter's activities. Spying Domain consists of random storage areas that include the hash code of Secret Information. Through Event Log, when a cyberattacker attempt to access the storage units, an alarm is activated. Concerning the evaluation procedure, the authors developed a tool which configures appropriately the physical memory, the spying domain and the possible storage areas that are affected by the cyberattack. Evaluation figures indicate the values of TPR according to the different parameters.

Mitchell and Chen [98] presented a specification-based IDS which includes individual IDSs for the AMI headend, data collectors and smart meters. For each of the aforementioned devices, a particular set of behavior rules have been identified and transformed into a state machine. Specifically, the IDS controlling the AMI headend has the ability to monitor the activities of the other AMI headends and data collectors. Accordingly, the data collector IDS is able to control the behavior of the other data collectors and smart meters. Finally, the third kind of IDSs can only monitor the other smart meters. The threat model applied by the authors, includes two kinds of attacks: reckless and random attacks. The authors argue that their methodology accomplishes 100% TPR, while FPR does not exceed 0.2% and 6% for reckless and random attacks respectively. Also, ROC curves are presented.

In this paper [99], P.Jokar and V.Leung presented a specification-based IPS for the SG applications that employ ZigBee-based HANs. In particular, the proposed system mainly focuses on the network traffic features at the Physical (PHY) and Medium Access Control (MAC) layers. It consists of agents that monitor the network behavior of various sensor nodes, while at the same time, it can be used for prevention actions. Also, a central-IPS undertakes to extract and analyze particular features of the network traffic, thus detecting possible attacks. If a potential cyberattack or an abnormal behavior is detected, then a specific prevention response will be selected by using the Q-learning method which is a reinforcement learning technique. It should be noted that the overall network traffic is controlled by the central-IPS which constantly communicates with multiple agents. The set of the specification rules is based on 6 characteristics: a) Datagram of IEEE 802.15.4 [100] and Smart Energy Profile 2.0 (SEP 2.0) [101] protocols, b) traffic rate, c) Received Signal Strength (RSS), d) sequence number, e) Packet Error Rate (PER) and f) node availability. Regarding the evaluation of the proposed system, the authors carried out a theoretical analysis of six attacks against IEEE.802.15.4, thereby demonstrating that the proposed IPS can successfully address these attacks. Specifically, the attacks examined are: a) radio jamming attacks, b) replay attacks, c) stenography attacks, d) back-off manipulation attacks, e) DoS against data transmission during the Contention Free Period (CFP) and f) DoS against Guaranteed Time Slot (GTS) requests. Subsequently, the authors conducted two experiments in order to demonstrate that their system dynamically selects the appropriate prevention

activity. The corresponding ROC curves are presented. Finally, the authors discussed five techniques that can bypass IDPSs. These techniques are: a) obfuscation, b) fragmentation, c) protocol violation, d) generating network traffic that targets on IDPS and e) DoS attacks on IDPS. They argue that only fragmentation techniques cannot be identified by their proposed system.

In [102], the authors developed a specification-based IDS for AMI, which combines temporal and spatial detection techniques, by using Matlab. In more detailed terms, the proposed system focuses on blackhole and time delay attacks. The blackhole attack was described previously. On the other hand, the time delay attacks aim at introducing additional delay time when the packets are transmitted. In particular, their methodology monitors the number of the transmitted packets and the transmission delay time between these packets by using specific numerical intervals that were calculated by using the mean value and the standard deviation of the normal distribution. Concerning the evaluation of the proposed model, the authors compared their algorithm only with the spatial-based, the temporal-based detection technique and with the development of an SVM [64] model. They report that the SVM [64] model achieves the best TPR, but their model achieves the best FPR and the second best TPR. Specifically, TPR and FPR approach 90% and 6% respectively.

C. IDPS SYSTEMS FOR SCADA SYSTEMS

The safe operation of SCADA systems is crucial for the entire functionality of critical infrastructures, such as SG. These systems enable operators to monitor, control and automate the actions that take place in an industrial environment. However, their communications are based on insecure protocols, such as Modbus [55]–[57] and DNP3 [58] that do not integrate authentication and access control mechanisms, thus enabling MiTM attacks. Hence, the IDPS systems that are responsible for protecting SG, should necessarily take into account the security weaknesses of SCADA communications. Below we analyze per paragraph appropriate IDPS systems devoted to protecting SCADA systems.

In [103], T.H. Morris et al. focus their attention on the Modbus [55]–[57] protocol, providing a set of signature rules. Modbus is a master-slave, industrial protocol, which was released by Gould Modicon (now Schneider Electric) in 1979 for the communication between MTU (master) and logic controllers (slave). MTU sends a specific query to the logic controller and subsequently the second transmits its response to MTU. More specifically, the authors introduce 50 signature rules that concern the Modbus/TCP as well as the Modbus protocol over a serial communication interface. The Snort [104]–[106] IDS was utilized for testing these rules; however, the paper describes these rules in a generic format, in order to be applied by various IDS systems. Each rule is defined in a specific text field and is accompanied with specific details that concern the protocol specifications. Nevertheless, it is worth mentioning that the authors do not provide numerical results regarding the effectiveness of these rules.

In [107], H. Li et al. focus on the DNP3 [58] protocol providing appropriate signature rules utilizing the Snort IDS [104]–[106]. DNP3 is an industrial protocol, which was standardized by IEC TC-57 and was deployed by IEEE Electric Power Engineering Association (PES). According to the authors, the deployment process of DNP3 focused on the reliability of communications, ignoring the information security aspects. In particular, DNP3 is characterized by significant security deficiencies such as the lack of encryption, authentication and authorization mechanisms. Therefore, it is vulnerable to a plethora of cyberattacks such as reconnaissance attacks, DoS, protocol anomalies and mixed attacks. In this work, the authors developed an intrusion detection template which subsequently was utilized for generating signature rules for the DNP3 protocol. The signature rules generated can detect the aforementioned cyberattacks. Moreover, the authors denote that the specific template can be used for developing signature rules for other industrial protocols, such as Modbus [55]–[57] and Profinet. Finally, it is noteworthy that the authors do not provide any evaluation process.

In [108] E. Hodo et al. present an anomaly-based IDS for a SCADA simulated environment which utilizes the IEC 60870-5-104 [109] (IEC-104) protocol. In 1995, the International Electromechanical Commission (IEC) was released IEC-60870-5-101 which includes essential telecontrol messages between a logic controller and a controlling server. After six years later, IEC released IEC-104 which combines the application messages of IEC-101 with TCP/IP. However, IEC-104 is characterized by several security issues, since its functionality is based on TCP/IP which itself presents various vulnerabilities. Moreover, the application data are exchanged without any authentication mechanism, i.e., as plaintext. The authors create their own dataset which includes passive Address Resolution Protocol (ARP) poisoning attacks, DoS attacks and replay attacks that replace legitimate packets with malicious ones. Based on this dataset and utilizing WEKA [70], [71], they evaluated multiple machine learning algorithms, such as Naive Bayes IBk, J48 [90], Random Forest [110], OneR, RandomTree and DecisionTable. J48 [90] and DecisionTable scored the best ACC.

In [111] N. Goldenberg and A. Wool present an anomaly-based IDS which is devoted to the Modbus/TCP [55]–[57] communications. More detailed, the functionality of the specific IDS is based on a Moore Deterministic Finite Automaton (DFA) which in turn is based on the high periodicity of the Modbus [55]–[57] network traffic. In particular, the proposed DFA monitors the queries and responses between MTU and each logic controller, thereby identifying the normal and abnormal states. More detailed, the DFA consists of: a) a set of states, b) an alphabet which is a set of input symbols, c) a transition function and d) the first state. A state denotes how normal the Modbus [55]–[57] network traffic is and can take four values: a) Normal, b) Retransmission, c) Miss and d) Unknown. From the

aforementioned values, only the Unknown state is considered as a malicious behavior. On the contrary, the Retransmission and Miss values denote a benign behavior with some anomalies. The input symbols and the transition function determine the states for each communication. The input symbols are divided into two classes: a) known symbols and b) unknown symbols. The first category includes those symbols that were observed during the learning phase and result in a known state (Normal, Retransmission, Miss), while the second category implies those symbols that result in the Unknown state. To evaluate their methodology, the authors generated two real datasets using Wireshark [112]–[114], Pcapy [115] and Impacket [116]. Based on the experimental results, the authors argue that their model did not present any false alarm.

In [117], S.D. Anton et al. provide a comparison of four machine learning algorithms concerning the detection of anomalies in a Modbus/TCP dataset. More specifically, the authors utilized the dataset of Lemay and Fernandez [118] which was divided into three sub-datasets, namely DS1, DS2 and DS3. DS1 consists of 3319 packets and contains the network traffic between MTU and 6 RTUs, including 75 malicious cases. Similarly, with the same architecture of one MTU and 6 RTUs, DS2 contains 11166 packets from which 10 cases are malicious. Finally, DS3 includes 365906 packets with 2016 malicious cases and was generated by the combination of eight datasets. From these sub-datasets, specific features were extracted and used for the training of the machine learning algorithms. It is noteworthy that the extracted features concern only the TCP/IP stack. The algorithms evaluated are: a) SVM [64], Random Forest [110], K-Nearest Neighbor (KNN) [119] and k-means [120]. ACC of SVM [64] with DS1, DS2 and DS3 is equal to 100%, 100% and 99.99% respectively. Accordingly, ACC of Random Forest [110] with DS1, DS2 and DS3 is 100%, 99.99% and 99.99%. ACC of KNN with DS1, DS2 and DS3 is 99.7%, 99.9% and 99.9%. Finally, ACC of k-means [120] with DS1, DS2 and DS3 is 98.1%, 55.62% and 63.36%.

In [121], P.H. Wang et al. implement an anomaly-based IDS utilizing a clustering technique as well as data captured by a honeypot system. A honeypot [122] is a specific device or software which intentionally possesses specific vulnerabilities in order to attract the cyberattackers. More detailed, the proposed IDS focuses on detecting intrusions against the Modbus [55]–[57] protocol, by gathering and using the information provided by a Conpot [123] honeypot. Conpot [123] is a software package which represents a Siemens programmable logic controller simulating the Modbus protocol. During their experiments, the authors considered that each request to Conpot was a cyberattack. Subsequently, they combined a similarity evaluation method of the requests with an agglomerative hierarchical clustering [124] to extract representative Sequential Attack Patterns (SAPs). After this process, their system is capable of classifying new requests as existing SAP or unexpected SAP. Finally, the authors developed a visualization method which visualizes the flow graphs of the represented SAPs. Concerning the software packages utilized by the authors, they are Conpot [123], Python 2.7 and MongoDB [125], [126]. Based on the evaluation results the proposed system can detect reconnaissance and DoS attacks with TPR 90% and 95.12% respectively. FPR of both aforementioned attacks is calculated at 0%.

In [127], Y. Yang et al. provide a specification-based IDS for the IEC-104 [109] protocol. The core of their system is named Detection State Machine (DSM) and its functionality is based on the Finite State Machines (FSM) methodology. More detailed, the operation of IEC-104 [109] is determined through the correlations of FSM. In contrast to the traditional FSM-based systems, their implementation applies a set of alarms that are capable of distinguishing the protocol malfunctions. To deploy and demonstrate their methodology, the authors employ the Internet Traffic and Content Analysis (ITACA) software [128]. Concerning, the evaluation results, the authors argue that the True Positive Rate (TPR) and False Positive Rate (FPR) of their IDS are calculated at 100% and 0% respectively.

In [129], Y. Yang et al. provide signature and specification rules for the IEC-104 [109] protocol, by using the Snort IDS [104]–[106]. After studying the security issues of the specific protocol, the authors deployed attack signatures and specification rules for the following attacks: a) unauthorized read commands, b) unauthorized reset commands, c) unauthorized remote control and adjustment commands, d) spontaneous packets storm, e) unauthorized interrogation commands, f) buffer overflows, g) unauthorized broadcast requests and h) IEC-104 port communication. Concerning the evaluation process, 364 packets were examined from which 41 packets were malicious. Based on the experimental results, all malicious packets were detected with zero FPs.

In [130], Z.Feng et al. focus their attention on the security of the Profinet [131], [132] protocol by deploying effective signature and specification rules utilizing Snort [104]–[106]. Profinet is an industrial standard which was standardized by IEC 61158 and IEC 61784 and was developed by Profibus & Profinet International. According to the authors, Profinet suffers from severe security issues, since it does not integrate encryption, authentication and authorization mechanisms, thus making possible the accomplishment of MiTM attacks. In this paper, the authors enhance the potential of Snort [104]–[106] by decoding the Profinet attributes as well as deploying appropriate signatures for detecting MiTM, DoS and reconnaissance attacks. Moreover, the authors deployed specification rules for identifying possible anomalies. To evaluate their work, the authors utilize the traffic package of [133] and also they create a DoS attack scenario based on [134]. According to the evaluation process, the proposed signature and specification rules can detect intrusions against Profinet.

In [135], S. C. LI et al. implement an anomaly-based IDS for the Modbus protocol, adopting classification data mining models. In particular, they developed a J48 decision tree as well as three neural networks, utilizing WEKA.

To train the above models, they create a dataset by constructing a real testbed consisting of a programmable logic controller, MTU, a cyberattacker unit and a cyberdefender unit. This dataset includes a) reconnaissance attacks, b) response injection attacks, c) command injection attacks and d) DoS attacks. To create their dataset, the authors utilized Wireshark [112]–[114] as well as a PHP script to convert the Packet Description Markup Language (PDML) format of Wireshark [112]–[114] to Comma-Separated Values (CSV) format. Since their dataset includes very few malicious records, the authors utilized the zeroR [136] classifier. Specifically, 92.5% of the dataset includes normal records. Hence, based on zeroR [136], ACC of the data mining models generated by the authors has to overcome 92.5%. The training process employed 39 features, but they are not specified by the paper. Based on the evaluation results, ACC of j48 is calculated at 99.8361%. Accordingly, ACC of the first, second and third neural network is calculated at 97.4185%, 97.4603% and 97.3876%.

D. IDPS SYSTEMS FOR SUBSTATIONS

A substation is a critical location of the electrical grid, where the electrical energy can be transformed, split and combined. Usually, the operations of contemporary substations are automated and controlled by a Substation Automated System (SAS) which incorporates many industrial and ICT components such as IEDs, RTUs and computers. The communication among these components is based on the IEC 61850 [41], [42] standard which determines the following goals: 1) interoperability, 2) long term stability and 3) simplified configuration. However, it should be noted that IEC 61850 does not identify any cybersecurity feature for the safe and normal functionality of SAS. Consequently, possible cyberattacks can exploit the security gaps of the protocols defined by this standard, thus making it possible to generate disastrous consequences. Although IEC 62351 [137] defines primary security measures, such authentication mechanisms to secure the protocols defined by IEC 61850, many vendors and manufacturers do not adopt these solutions. Therefore, in any case, IDPS is considered as a necessary tool for the protection of SAS. Each of the following paragraphs describes an IDPS instance, devoted to protecting substations.

B. Kang et al. in [138] introduced an IDS framework for substations, which employs signatures and focuses on the active power limitation attacks. In particular, they developed a stateful analysis plugin which can be incorporated into the Suricata IDPS [105], [139], [140]. The specific plugin includes three functions: a) the application layer protocol decoder, b) the rule match engine and c) the state manager. The first function decodes the application layer packets and extracts their corresponding attributes. The second function applies content and state inspection rules in order to detect particular attack patterns. The content inspection rules examine particular conditions for each application layer packet, while the state inspection rules check the existence of specific flags that should characterize the protected devices. Lastly, the state manager updates the states of the protected devices. In order to evaluate their framework, the authors applied their stateful analysis plugin in a scenario which utilizes the Manufacturing Message Specifications (MMS) [141] protocol based on the directions of IEC 61850 [41], [42] standard. They described two attack examples that are detected successfully, but they do not provide numerical results.

This work [142] analyzes a specification-based IDS which is deployed in a substation in South Korea. More specifically, their IDS is based on the analysis of Generic Object Oriented Substation Events (GOOSE) [143] and MMS [141] protocols, examining general network traffic characteristics, such as the number of bits per second (bps), the number of packets per second (pps) and the number of connections per second (cps). For the mentioned characteristics, specific intrusion detection algorithms were created utilizing statistical analysis techniques. Details about the architecture of the IDS are not provided. Regarding the evaluation procedure, a real dataset was utilized consisting of multiple network attacks, such as: port scanning attacks, DoS attacks, GOOSE attacks, MMS attacks, Simple Network Management Protocol (SNMP) attacks, Network Time Protocol (NTP) attacks and ARP attacks. The authors argue that their model scored 100% Precision, 0% FPR, 1.1% FNR and 98.9% TPR.

In [144], Y. Yang et al. provide a specification based IDPS devoted to protecting substations utilizing the IEC 61850 [41], [42] protocol and particularly the communications based on MMS, GOOSE and Sampled Measure Value (SMV). More concretely, the proposed IDPS consists of five modules: a) configuration module, b) network traffic capture module, c) process core module, d) rule module and e) result module. The first one is responsible for examining the attributes of a specific substation, thus determining them with specific values and limits. The second undertakes to capture and isolate the network traffic of MMS, GOOSE and SMV. The process core module adopts the ITACA software in order to analyze in detail the attributes of the aforementioned protocols. The rule module applies the specification rules to the preprocessed IEC 61850 network traffic. Finally, the last module informs the security administrator regarding potential violations. Concerning the specification rules, they can be classified into four categories: a) access-control detection, b) protocol whitelisting detection, c) model-based detection and d) multi-parameter detection. The first one specifies the legitimate MAC and IP addresses as well as TCP ports, thereby forming a whitelist. The rules of the second category detect as malicious those packets that are not related to IEC 61850. The next category is devoted to identifying each specification rule relevant to the attributes of the previous protocols. The last category includes some rules related to the physical characteristics of a substation. It is worth mentioning, that all rules provided by the authors are not identified accurately. Regarding the evaluation process, data from a real substation in China was utilized. According to the authors, the proposed IDS is capable of detecting a plethora of cyberattacks, such as

DoS, MiTM and packet injection attacks. However, it should be noted that numerical results are not provided.

In [145], M. Kabir-Querrec et al. introduce a specification-based IDPS which focuses on IEC 61850 [41], [42] communications of a substation. In particular, the architecture of their IDPS is based on the data object model defined by IEC 61850, by introducing a new intrusion detection function. This data object model consists of many Logical Nodes (LNs) that satisfy specific functions. All LNs required for a function form a new logical entity called Logical Device (LD). A physical device, such as IED can consist of many LDs. LNs can exchange data among themselves using a concept named Piece of Information for COMmunication (PICOM). Although IEC 61850 incorporates a function for security processes named Generic Security Application (GSAL), the author deployed a new one which is devoted to detecting possible anomalies, by determining the normal specifications of the standard. To define a new function inside IEC 61850, the following steps have to be accomplished: a) a formal description of the function is needed, b) the function has to be decomposed into LNs and c) the interaction with the other functions has to be determined. Hence, the authors created an LN called CYSN which is responsible for sniffing the GOOSE messages and transmitting them to two dedicated LNs that in turn are devoted to checking the specifications, thus generating the respective alert in case of a security violation. More detailed, the first one called CYComChkSingle undertakes to verify the structure and parameters of each message. Accordingly, the second one named CYComChkMany verifies the consistency of the messages based on a specific time slot. However, it is worth mentioning that the authors do not provide detailed information concerning the content and format of these specifications. In addition, the paper does not include any evaluation procedure.

H. Yoo and T. Shon in [146] provide an anomaly-based IDPS for the substations utilizing the IEC 61850 standard. In particular, the proposed IDPS focus on MMS and GOOSE protocols, by adopting a one-class SVM classification model, thus identifying patterns that correspond only to the normal and legitimate network traffic. More detailed, their IDPS consists of four processes: a) data capturing and preprocessing, b) outlier processing, c) one-class SVM training and d) anomaly detection. The first process is devoted to capturing and preprocessing MSS and GOOSE packets, thus providing three sets of data. The first set comprises the attributes of each MMS and GOOSE packet. These attributes are described in detail in the paper. The second set includes the network flows formed by MMS and GOOSE communications and finally, the third one includes traffic information such as pps and bps. The second process is employed only before the training of the classification model. It is responsible for removing the outlier values of the training set, since such values may denote an anomalous situation. For this process, the Expectation Maximization (EM) [147] and Local Outlier Factor (LoF) [148] were utilized through the WEKA software. It should be noted that in an industrial environment, an anomaly may occur even if each component operates normally. Finally, the last processes focus on training and testing the one-class SVM classification model respectively. The training process was implemented by using data from a real substation. Regarding the evaluation process, FPR ranges between 1% and 6%.

U. Premaratne et al. in [149] introduce a hybrid signature-based IDPS for a substation utilizing the IEC 61850 protocol [41], [42]. The proposed IDPS combines signature and specification rules regarding DoS attacks, traffic analysis attacks, and password cracking attempts. In particular, the authors simulated these cyberattacks, thereby extracting the corresponding signature and specification rules that in turn were incorporated into Snort [104]–[106]. To simulate these attacks, they employed the ping command, THC Hydra [150] and Seringe [151]. Nevertheless, although the authors argue that their IDPS is devoted to monitoring IEC 61850 packets, it is not able to identify cyberattacks against IEC 61850 protocols, such as GOOSE and MMS. Moreover, the authors do not provide numerical results, regarding the efficiency of their system.

J. Hong et al. in [152] provide a specification-based IDPS which is also devoted to protecting IEC 61850 [41], [42] substations, by analyzing multicast GOOSE and SMV messages. After providing a brief description concerning the format of GOOSE and SMV protocols, the authors describe in detail two specification rules that are used to detect possible GOOSE and SMV cyberattacks respectively. In particular, concerning the GOOSE cyberattacks, their IDPS can detect relevant replay attacks, DoS attacks, attacks generating malicious GOOSE data, malicious activities that change GOOSE control data and finally, actions that modify the time information. Accordingly, concerning the SMV attacks, the proposed IDPS can detect relevant DoS attacks and malicious actions that modify or generate SMV data. Regarding the architecture of the proposed IDPS, it consists of four modules: a) packet filtering module, b) packet parser module, c) specification-based IDS module and d) HMI module. More detailed, the first module is responsible for capturing only GOOSE and SMV packets. Accordingly, the second one undertakes to extract from the GOOSE and SMV packets the corresponding attributes. The specification-based IDS module applies the specification rules and the last module informs the system operator about possible cyberattacks and anomalies. The authors tested the effectiveness of their implementation under real conditions, by constructing a CPS testbed, which in turn enables the execution of the various cyberattacks. Based on the authors, FPR can reach 1.61×10^{-4}.

In [153] Yi. Yang et al. have developed a specification-based IDPS capable of identifying cyberattacks against IEC 61850 [41], [42] substations. Regarding the architecture of the suggested IDPS, it is composed of the following modules: a) configuration module, b) network traffic capturing module, c) IDPS process core, d) rule module and e) result module. The first module determines the configuration files that are used to specify the specification rules. The second

module undertakes to sniff IEC 61850 packets. The following module analyses the IEC 61850 packets, by extracting their attributes. The fourth module is responsible for matching the IEC 61850 packets with a predefined set of specification rules. Finally, the last module informs the system operator or the security administrator about the possible intrusions. Concerning the specification rules adopted by this IDPS, they can be classified into four categories: a) access control detection rules, b) protocol-based detection rules, c) anomaly behavior detection rules and d) multi-parameter detection rules. The first kind of rules is responsible for allowing only the network traffic coming from legitimate MAC and IP addresses. Accordingly, the rules of the second category undertake to allow only the network traffic specified by the protocols that are defined by the IEC 6185 standard. The next rules identify normal behaviors related to the attributes of the protocols incorporated into IEC 61850. Finally, the last category identifies some specifications concerning specific attributes of the physical environment. It should be noted that the authors do not provide numerical results regarding the performance of their implementation.

E. IDPS SYSTEMS FOR SYNCHROPHASORS

The modern electrical grids usually are equipped with synchrophasor systems capable of providing real-time information concerning electricity measurements, such as current, voltage and frequency. These systems complement the traditional SCADA systems, by offering additional wide monitoring of the entire electrical grid. Thus the system operator can identify possible functional problems more quickly, make better decisions and prevent devastating situations. Although their role is passive, a successful cyberattack against such systems can lead to revealing significant information related to the operation of the electrical grid. In particular, synchrophasors usually employ the IEEE C37.118 protocol [154], which does not integrate any authentication mechanisms, thus making it possible to launch MiTM cyberattacks. Therefore, it is clear that the detection and prevention of cyberattacks against synchrophasors are crucial. Each of the following paragraphs analyses an IDPS devoted to protecting such systems.

Pan *et al.* [155] proposed a hybrid IDS for the synchrophasor systems, which combines anomaly-based and signature-based techniques. In particular, their work is based on the common-path mining approach and Snort [104]–[106]. They examined an architecture of three bus two line transmission system, which consists of a real-time digital simulator, four relays, four PMUs, a PDC, an energy management system, which runs the OpenPDC [156], [157] software and a personal computer which executes Snort [104]–[106]. The input data are captured by the mentioned entities and are compared with common paths. A common path is a sequence of system states that may be a specification of normal behavior or a signature of a cyberattack. Based on these characteristics, the particular IDS can classify an activity as: a) system disturbance, b) normal operation and c) cyberattack. The training process of the common-path mining algorithm includes the creation of a dataset which comprises 25 scenarios of 10000 simulation instances. These scenarios are classified into three categories, namely a) singe-line-to-ground faults, b) normal operations and c) cyberattacks. According to the evaluation results, ACC is calculated at 90.4%.

Khan *et al.* [158] introduced a hybrid IDS which is mainly based on specification-based and signature-based techniques for synchrophasor systems that utilize the IEEE C37.118 protocol [154]. In more detail, the general architecture of the proposed system consists of separate HIDSs and NIDSs called agents and sensors respectively. The agents monitor the operation of PMUs or PDCs, while the sensors govern the overall network traffic. Also, there is a management server, which aggregates and correlates all information coming from the individual agents or sensors. In addition, a database server is responsible for recording any detection alert or warning. The agents and sensors comprise six components: a) PCAP filters, b) IEEE C37.118 decoder, c) analyzer/detector, d) state manager, e) events manager and f) console. The PCAP filters are developed by using the C/C++ programming language and are responsible for capturing the IEEE C37.118 packets. The IEEE C37.118 decoder analyzes the previous sniffing packets and extracts the appropriate information. The analyzer/detector utilizes a set of rules in order to detect abnormal behaviors. This set is composed of four categories rules: a) signature-based rules, b) range-based rules, c) threshold-based rules and d) stateful behavior-based rules. According to the authors, the specific set of rules is able to detect a plethora of cyberattacks, such as, ARP poisoning attacks, replay attacks, port scanning attacks, DoS attacks, GPS spoofing attacks, command injection attacks and physical attacks. Subsequently, the analyzer/detector communicates with the state manager, which stores possible alerts or warnings in the database server. Next, the event manager communicates with the management server, whose operation was discussed previously. Finally, the console is a command line or a GUI environment with which the user can configure the operations of the previous components, e.g., the detection rules. For the evaluation process, they employ the NRL Core software [159], [160]. However, it is worth mentioning that numerical results are not provided.

Y. Yang et al. in [161] suggest a specification-based IDPS capable of protecting synchrophasor systems utilizing the IEEE C37.118 protocol. More specifically, their IDPS consists of three kinds of rules including: a) access control rules, b) protocol-based rules and c) behavior-based rules. The access control rules define a whitelist with the legitimate source and destination MAC and IP addresses as well as the corresponding ports at the transport layer based on the Open Systems Interconnection (OSI) model. Accordingly, the protocol-based rules adopt also a whitelist which in turn defines the application layer protocols allowed for the interaction among the synchrophasor components. In this case, this list will enable only the IEEE C37.118 traffic. Finally, the last category identifies behavior rules based on the attributes of

the IEEE C37.118 packets, by utilizing a deep packet inspection process. All rules are described sufficiently in the paper. Concerning the evaluation process, the authors tested their IDPS in a real testbed, by executing reconnaissance, MiTM and DoS cyberattacks. According to the experimental results, FPR of the proposed IDPS is calculated at 0%.

VII. DISCUSSION

SG consists of a complicated and heterogeneous set of technologies, including AMI, SCADA systems, substations, synchrophasors electric vehicles, etc. These technologies optimize the existing processes of the traditional electrical grid, but also generate multiple hazards, such as cyberattacks that can cause disastrous consequences, such as a power outage. In particular, most of the cyberattacks usually target SCADA systems because they utilize insecure, legacy communication interfaces and protocols. Characteristics examples are the Stuxnet worm [26] and the Russian cyberattack against a Ukrainian substation, resulting in the power outage for more than 225,000 people [19]. Moreover, in 2009 Chinese and Russian cyberattackers attempted to penetrate the US electrical grid, by carrying out reconnaissance cyberattacks [169]. Furthermore, in 2014, a campaign of cyberattacks, named Dragonfly [170] was implemented against electrical energy infrastructures of many countries, including the US, Germany, France, Italy, Spain, Poland and Turkey. The Repository of Industrial Security Incidents (RISI) [171] comprises 242 reported SCADA cybersecurity incidents dating from 1982 to 2014. It is clear that the IDPS systems are an efficient and necessary measure for the protection of SG, by timely detecting or even preventing the cybersecurity issues. In this work, we present a comprehensive compilation of 37 IDPS systems, designed for the protection of SG, including IDPSs that protect the entire SG ecosystem, AMI, SCADA systems, substations and synchropahsors.

Table 1 summarizes the results of our analysis by highlighting the most important features found. In particular, 3 IDPSs focus on the entire SG ecosystem, 13 on AMI, 10 on SCADA systems, 8 on substations and 3 on synchrophasors. The majority of IDPSs employ the anomaly detection technique or particular specifications that define the normal behavior. Concretely, 17 IDPSs employ the anomaly detection technique, 12 models are characterized as specification-based, 3 IDPS employ attacks signatures and 5 cases combine the aforementioned detection methods. Each of these techniques is characterized by advantages and disadvantages. The signature-based IDPS usually achieves high performance; however, it is characterized by the inability to detect unknown threats. Also, generating cyberattack signatures is a very time-consuming process. On the other hand, the anomaly-based technique is able to detect zero-day attacks but presents high FPR. Finally, the specification-based IDPS combines the advantages of the previous ones; however, in an environment, such as SG which includes multiple alterations and modifications, these specification rules must be redefined continuously. Therefore, the solution of developing hybrid IDPSs sounds more promising, since the combination of the detection techniques can meet the aforementioned issues.

In addition, it is noteworthy that none of the examined IDPSs include information about the detection latency, while only two cases [73], [94] comprise information about the consumption of the computing resources. However, the detection latency is a significant evaluation measure, especially in critical systems such as SG, since various cyberattacks can cause disastrous consequences. Also, the consumption of the computing resources must be taken into account, given the establishment of the IoT era, which is characterized by constrained resource capabilities. Moreover, all IDPS cases studied are not quite scalable, since they cannot monitor and interpret data from multiple sources such as the various communication protocols utilized in SG as well as the logs of the various components like electricity measurements of HMI and smart meters. Furthermore, none of the IDPSs examined does not include self-healing capabilities, providing appropriate mechanisms in case of emergency. As mentioned in Section V, in critical infrastructures, such as SG, recovery mechanisms, should be activated immediately in emergency situations, in order to replace the violated components, thus restoring the normal operation of the system. Finally, it is worth mentioning that although SG encompasses many complex domains and a huge number of heterogeneous components (e.g., smart devices), only one IDPS includes visual-based mechanisms for facilitating the detection process.

Undoubtedly, the IDPS cases examined before provide an additional layer for the protection of SG as well as a valuable effort in this research field. However, none of them satisfy all requirements defined by Section V. In general, we consider that the security mechanisms in this domain have to take into account both the physical and cyber features of the various components, by adopting situational awareness processes in a cross-layer approach. Based on Endsley [172], situational awareness consists of three layers. The first layer is the perception of information, which identifies the elements of an environment and their behavior. The second layer is the comprehension of information received from the previous layer, comprising storing and interpreting processes. Finally, the projection level includes predictive and prescriptive algorithms that intend to interpret relevant events. McGuinness and Foy [173] introduced an additional layer, named Resolution aiming to identify the appropriate practices that optimize a specific situation. Therefore, based on the previous definitions, we consider that an appropriate IDPS for SG should apply a hybrid methodology, including signature and specification rules as well as anomaly detection processes. Moreover, it should be capable of monitoring and interpreting a set of various SG communication protocols from the physical layer to the application layer on the basis of the OSI model, thereby having the capability to detect cyberattack patterns in a cross-layer approach. Furthermore, it should analyze logs from the various components, systems and software applications, thus being capable of detecting attacks at the application level. Finally, it should include appropriate

self-healing mechanisms that will enable the normal operation of the entire system, in case of a disastrous cyberattack.

VIII. RESEARCH TRENDS AND DIRECTIONS

It is clear that IDPS systems are critical for any security system that is deployed in SG. Their role lies in further detecting whether an attacker has compromised grid systems and gained access to power grid networks. They should be capable of identifying threats and attacks in the whole SG, by having global visibility, while being able to access both power and information systems such as MTU, RTU, PLC, PMU, smart meters and data concentrators. Moreover, they should be scalable, by combining various intrusion detection techniques and monitoring different types of communication and data such as network traffic, software and system logs as well as raw data like electricity measurements. Thus, they should be capable of identifying the type of cyberattacks and activating the appropriate preventive mechanisms respectively, such as for example the interruption of a network flow if it is considered as a DoS attack. Furthermore, IDPSs for SG should be resilient against those cyberattacks that aim at bypassing it, by using techniques like for example obfuscation, packet fragmentation, code packing and encryption, code mutation, and DoS attacks [99]. Finally, they should provide appropriate self-healing mechanisms that will be activated during emergency situations, by isolating critical parts of SG or enabling collaborative and redundant mechanisms that in turn will provide sufficient solutions, until the normal operation is restored. In this section, we aim at determining the research trends in this field, also providing specific directions for future work.

Based on the analysis of Section VII, we have seen that the existing IDPS are generally unable to interpret the application layer data for the SG communications, either for a single packet, or at a session layer, where the state of a connection should be monitored for inconsistencies [174]. As a result, most commercial IDPSs do not employ specifications rules, determining the normal attributes of SCADA and ICS protocols (e.g., Modbus, IEC 61850 [41], [42], IEC-104 [109]). Furthermore, traditional approaches cannot be adopted to discriminate between cyberattacks and accidental faults [175]. The Software Defined Network (SDN) technology can offer significant solutions regarding the previous limitations. The SDN technology provides global visibility and virtualization capabilities, thus making possible the generation of specification rules. More specifically, SDN enables the slice of the physical communication network into several virtualized networks devices and deliver traffic belonging to each critical grid control application. The virtualized network slices a) inherently enhance security with traffic isolation, b) enable more fine-grained status monitoring and c) simplify the labor-intensive protocol vulnerability assessment, i.e., limited to one particular application per virtual network slice [176]. Therefore, by taking full advantage of the SDN technology, we consider that the research efforts should focus on developing SDN-based IDPS systems that will also be capable of monitoring microgrids. However, based on the existing literature at this time, we could not find any IDPS devoted to protecting microgrids.

In the light of the aforementioned remarks, the interconnected and interdependent nature of SG creates new challenges for the SG security, such as coordinated attacks, APTs, DoS attacks and botnets. In particular, coordinated attacks and APTs represent a more dangerous category because they are sophisticated human-driven attacks against specific targets. They are usually perpetrated over long periods by groups of experts that leverage open source intelligence, social engineering techniques and zero-day vulnerabilities. The contemporary solutions for the energy sector protection are the SIEM systems. In particular, SIEM systems deploy multiple agents in a hierarchical manner to aggregate and normalize information from different resources, such as security-related events from end-user devices, servers, network devices and operating systems [177], [178]. Typically, these systems are composed of six components/processes which are the source device, the log collection, the parsing/normalization of the logs, the rule engine, the log storage and the event monitoring and retrieval. Moreover, they can integrate specialized security mechanisms, such as firewalls, antiviruses, and IDPSs in order to analyze logs and issue alert notifications or perform another response when a threat is detected. However, the current SIEM systems present three significant limitations regarding the energy sector. Firstly, their functionality focuses only on the ICT environment without having the ability to control other infrastructures, such as the industrial systems. Secondly, even if they can operate in the industrial sector, usually they utilize corresponding correlation rules for a few industrial protocols. Finally, the electrical grid is composed of multiple technological entities that generate a huge volume of data that cannot be efficiently handled by the current SIEMs. The adaptation and integration of appropriate host and network IDPS systems inside in a SIEM will be able to enhance significantly the level of the situational awareness. Hence, we think that a possible research field in this domain is the development of a SIEM tool which will solve the aforementioned limitations, by applying appropriate IDPS agents. More specifically, this tool should be able to decode, analyze and correlate various security events paying attention to the attributes of industrial protocols, such as IEC 61850 [41], [42], DNP3 [58] and Modbus [55]–[57]. The distributed agents should be able to monitor and control each device of SG, by implementing a deep packet inspection process in analyzing each attribute of the corresponding protocols from the physical to the application layer and based on specific threshold values should have the ability to identify possible anomalous behaviors.

Finally, based on the analysis of Section VII, we have seen that, the IDPS systems should prevent cyberattacks timely, by applying effective countermeasures, such as self-healing mechanisms. In contrast to the traditional electrical grid, SG has the ability to incorporate self-healing mechanisms in order to protect itself from natural disasters or

cyberattacks. In this field, self-healing entails the division of the main utility grid into individual microgrids, that can collaborate with each other in the case of emergency. Based on recent studies [34], [176], [179], [180], the collaboration among individual, independent microgrids, called islands, can enhance the functionality of the entire utility grid, by increasing its resilience and reliability. In particular, based on the type of emergency, the self-healing mechanism is responsible for interconnecting or isolating the corresponding microgrids. For instance, in the case of a cyberattack, the self-healing should be able to isolate the compromised systems. However, it should be highlighted that this countermeasure reduces the microgrid's observability (i.e., the capability to estimate the state of each system), thereby affecting the situational awareness and other processes. Consequently, by using the visualization capabilities of SDN, we consider that it is possible to generate efficient self-healing measures without reducing the observability of the whole grid, thus providing a powerful mechanism for critical states.

IX. CONCLUSIONS

SG includes several asynchronous interconnections among heterogeneous ICT and industrial components that on the one hand optimize the existing processes of the traditional electrical grid, but also generate multiple hazards. In particular, the combination of legacy and smart devices as well as the huge volume of data generated by them hinder the utilization of conventional security measures. Moreover, the security gaps of SCADA and SAS protocols like Modbus [55]–[57], DNP3 [58] and IEC 61850 [41], [42] enable cyberattackers to launch various attacks, thus endangering confidentiality, integrity and availability of the entire SG. Hence, an efficient IDPS system capable of protecting SG communications is considered as a necessary component of the contemporary electrical grid.

In this work, we present a comprehensive compilation of several IDPS systems devoted to protecting SG. In particular, first, we identify the attributes of SG, by analyzing its main components, the types of networks and the corresponding communication technologies. Next, we provide a comprehensive analysis of various IDPS systems, found in the literature based on specific evaluation requirements that need to be met. More detailed, we analyze and evaluate 37 IDPS systems by studying their architecture, intrusion detection methodology as well as their programming characteristics. Finally, based on this analysis, we specify the appropriate IDPS for SG and determine research directions for future work.

In our future work, we intend to address the aforementioned deficiencies by developing a SIEM system exclusively for the SG paradigm. The proposed SIEM will be based on the SDN technology and will integrate big data analytics and specification-based techniques. More specifically, it will be able to aggregate, normalize and correlate various security events as well as decode and analyze multiple industrial and ICT protocols, thus defining the corresponding specification and correlation rules.

REFERENCES

[1] D. Von Dollen, "Report to NIST on the smart grid interoperability standards roadmap," Electr. Power Res. Inst. (EPRI), Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SB1341-09-CN-0031, 2009.
[2] M. L. Tuballa and M. L. Abundo, "A review of the development of smart grid technologies," *Renew. Sustain. Energy Rev.*, vol. 59, pp. 710–725, Jun. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032116000393
[3] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renew. Sustain. Energy Rev.*, vol. 57, pp. 302–318, May 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032115014975
[4] N. S. Nafi, K. Ahmed, M. A. Gregory, and M. Datta, "A survey of smart grid architectures, applications, benefits and standardization," *J. Netw. Comput. Appl.*, vol. 76, pp. 23–36, Dec. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804516302314
[5] A. A. Cecilia and K. Sudarsanan, "A survey on smart grid," in *Proc. Int. Conf. Emerg. Trends Eng., Technol. Sci. (ICETETS)*, Feb. 2016, pp. 1–7.
[6] J. N. Bharothu, M. Sridhar, and R. S. Rao, "A literature survey report on smart grid technologies," in *Proc. Int. Conf. Smart Electr. Grid (ISEG)*, Sep. 2014, pp. 1–8.
[7] F. Khan, A. U. Rehman, M. Arif, M. Aftab, and B. K. Jadoon, "A survey of communication technologies for smart grid connectivity," in *Proc. Int. Conf. Comput., Electron. Elect. Eng. (ICE Cube)*, Apr. 2016, pp. 256–261.
[8] C. Bekara, "Security issues and challenges for the IoT-based smart grid," *Procedia Comput. Sci.*, vol. 34, pp. 532–537, Aug. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050914009193
[9] Z. M. Fadlullah, A.-S. K. Pathan, and K. Singh, "Smart grid Internet of Things," *Mobile Netw. Appl.*, vol. 23, no. 4, pp. 879–880, Aug. 2018. doi: 10.1007/s11036-017-0954-2.
[10] E. Spanò, L. Niccolini, S. Di Pascoli, and G. Iannacconeluca, "Last-meter smart grid embedded in an Internet-of-Things platform," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 468–476, Jan. 2015.
[11] Y. E. Song, Y. Liu, S. Fang, and S. Zhang, "Research on applications of the Internet of Things in the smart grid," in *Proc. 7th Int. Conf. Intell. Hum.-Mach. Syst. Cybern.*, vol. 2, Aug. 2015, pp. 178–181.
[12] Y. Lopes, N. C. Fernandes, and K. Obraczka, "Smart grid communication: Requirements and SCADA protocols analysis," in *Proc. Simposio Brasileiro de Sistemas Eletricos (SBSE)*, May 2018, pp. 1–6.
[13] E. Fadel *et al.*, "A survey on wireless sensor networks for smart grid," *Comput. Commun.*, vol. 71, pp. 22–33, Nov. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366415003400
[14] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Elect. Eng.*, vol. 67, pp. 469–482, Apr. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0045790617313423
[15] F. Wang, Z. Lei, X. Yin, Z. Li, Z. Cao, and Y. Wang, "Information security in the smart grid: Survey and challenges," in *Geo-Spatial Knowledge and Intelligence*, H. Yuan, J. Geng, C. Liu, F. Bian, and T. Surapunt, Eds. Singapore: Springer, 2018, pp. 55–66.
[16] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic honeypot game model for distributed denial of service attacks in the smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2474–2482, Feb. 2017.
[17] R. C. Diovu and J. T. Agee, "Quantitative analysis of firewall security under DDoS attacks in smart grid AMI networks," in *Proc. IEEE 3rd Int. Conf. Electro-Technol. Nat. Develop. (NIGERCON)*, Nov. 2017, pp. 696–701.
[18] R. C. Diovu and J. T. Agee, "A cloud-based openflow firewall for mitigation against DDoS attacks in smart grid AMI networks," in *Proc. IEEE PES PowerAfrica*, Jun. 2017, pp. 28–33.
[19] A. Hansen, J. Staggs, and S. Shenoi, "Security analysis of an advanced metering infrastructure," *Int. J. Crit. Infrastruct. Protection*, vol. 18, pp. 3–19, Sep. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548217300495
[20] Z. Guan, N. Sun, Y. Xu, and T. Yang, "A comprehensive survey of false data injection in smart grid," *Int. J. Wireless Mobile Comput.*, vol. 8, no. 1, pp. 27–33, 2015.
[21] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1580–1590, Jul. 2017.
[22] W.-L. Chin, C.-H. Lee, and T. Jiang, "Blind false data attacks against AC state estimation based on geometric approach in smart grid communications," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6298–6306, Nov. 2018.

[23] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid.*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[24] J. Zhao, J. Wang, and L. Yin, "Detection and control against replay attacks in smart grid," in *Proc. 12th Int. Conf. Comput. Intell. Secur. (CIS)*, Dec. 2016, pp. 624–627.

[25] T.-T. Tran, O.-S. Shin, and J.-H. Lee, "Detection of replay attacks in smart grid systems," in *Proc. Int. Conf. Comput., Manage. Telecommun. (ComManTel)*, Jan. 2013, pp. 298–302.

[26] C. Baylon, "Lessons from Stuxnet and the realm of cyber and nuclear security: Implications for ethics in cyber warfare," in *Ethics and Policies for Cyber Operations*. Cham, Switzerland: Springer, 2017, pp. 213–229. [Online]. Available: https://doi.org/10.1007/978-3-319-45300-2_12

[27] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, "The Cousins of Stuxnet: Duqu, flame, and gauss," *Future Internet*, vol. 4, no. 4, pp. 971–1003, 2012. [Online]. Available: http://www.mdpi.com/1999-5903/4/4/971

[28] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: Classification by sources of threats," *J. Elect. Syst. Inf. Technol.*, vol. 5, no. 3, pp. 468–483, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2314717218300163

[29] T. Bhatt, C. Kotwal, and N. Chaubey, "Survey on smart grid: Threats, vulnerabilities and security protocol," *Int. J. Electron., Elect. Comput. Syst. (IJEECS)*, vol. 6, no. 9, pp. 340–348, 2017.

[30] A. Anzalchi and A. Sarwat, "A survey on security assessment of metering infrastructure in smart grid systems," in *Proc. SoutheastCon*, Apr. 2015, pp. 1–4.

[31] B. B. Gupta and T. Akhtar, "A survey on smart power grid: Frameworks, tools, security issues, and solutions," *Ann. Telecommun.*, vol. 72, no. 9, pp. 517–549, Oct. 2017. doi: 10.1007/s12243-017-0605-4.

[32] 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, 4th Quart., 2014.

[33] M. M. Pour, A. Anzalchi, and A. Sarwat, "A review on cyber security issues and mitigation methods in smart grid systems," in *Proc. SoutheastCon*, Mar./Apr. 2017, pp. 1–4.

[34] 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, 1st Quart., 2017.

[35] S. Goel and Y. Hong, "Security challenges in smart grid implementation," in *Smart Grid Security*. London, U.K.: Springer, 2015, pp. 1–39. doi: 10.1007/978-1-4471-6663-4_1.

[36] A. Sanjab, W. Saad, I. Guvenc, A. Sarwat, and S. Biswas. (2016). "Smart grid security: Threats, challenges, and solutions." [Online]. Available: https://arxiv.org/abs/1606.06992

[37] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," in *Proc. SoutheastCon*, Apr. 2015, pp. 1–6.

[38] R. Leszczyna, "Standards on cyber security assessment of smart grid," *Int. J. Crit. Infrastruct. Protection*, vol. 22, pp. 70–89, Sep. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548216301421

[39] A. E. Ibhaze, M. U. Akpabio, and S. N. John, "A review on smart grid network security issues over 6LOWPAN," in *Proc. 2nd Int. Conf. Internet Things, Data Cloud Comput. (ICC)*, New York, NY, USA, 2017, Art. no. 180. [Online]. Available: http://doi.acm.org/10.1145/3018896.3056797

[40] A. Elgargouri, R. Virrankoski, and M. Elmusrati, "IEC 61850 based smart grid security," in *Proc. IEEE Int. Conf. Ind. Technol.(ICIT)*, Mar. 2015, pp. 2461–2465.

[41] P. Matoušek. (2018). Description of IEC 61850 communication. Faculty for Information Technology. [Online]. Available: http://www.fit.vutbr.cz/research/view_pub.php.en?id=11832

[42] R. E. Mackiewicz, "Overview of IEC 61850 and benefits," in *Proc. IEEE PES Transmiss. Distrib. Conf. Exhibit.*, May 2006, pp. 376–383.

[43] M. Sharma and A. Agarwal, "Survey on authentication and encryption techniquesfor smart grid communication," in *Proc. 7th India Int. Conf. Power Electron. (IICPE)*, Nov. 2016, pp. 1–5.

[44] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surv.*, vol. 46, no. 4, p. 55, 2014. [Online]. Available: http://doi.acm.org/10.1145/ 2542049

[45] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, Apr. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517300802

[46] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure Internet of Things," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2016, pp. 84–90.

[47] 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, 1st Quart., 2017.

[48] W. Tong, L. Lu, Z. Li, J. Lin, and X. Jin, "A survey on intrusion detection system for advanced metering infrastructure," in *Proc. 6th Int. Conf. Instrum. Meas., Comput., Commun. Control (IMCCC)*, Jul. 2016, pp. 33–37.

[49] J. Jow, Y. Xiao, and W. Han, "A survey of intrusion detection systems in smart grid," *Int. J. Sensor Netw.*, vol. 23, no. 3, pp. 170–186, 2017.

[50] R. Leszczyna and M. R. Wróbel, "Evaluation of open source SIEM for situation awareness platform in the smart grid environment," in *Proc. IEEE World Conf. Factory Commun. Syst. (WFCS)*, May 2015, pp. 1–4.

[51] *OSSIM: Open Source SIEM*. [Online]. Available: https://www.alienvault.com/products/ossim

[52] *Cyberoam Iview: The Intelligent Logging & Reporting Solution*. [Online]. Available: https://www.cyberoam.com/cyberoamiview.html

[53] *Prelude SIEM: Prelude Universal Open-Source SIEM Project*. [Online]. Available: https://www.prelude-siem.org/

[54] V. C. Gungor *et al.*, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2013.

[55] I. Modbus. (2004). *MODBUS Application Protocol Specification v1. 1a*. [Online]. Available: http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1a.pdf

[56] I. Modbus. (2004). *Modbus messaging on TCP*. [Online]. Available: http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

[57] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, "Attack taxonomies for the modbus protocols," *Int. J. Crit. Infrastruct. Protection*, vol. 1, pp. 37–44, Dec. 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S187454820800005X

[58] S. East, J. Butts, M. Papa, and S. Shenoi, "A taxonomy of attacks on the DNP_3 protocol," in *Critical Infrastructure Protection III*, C. Palmer and S. Shenoi, Eds. Berlin, Germany: Springer, 2009, pp. 67–81.

[59] J. P. Anderson, "Computer security threat monitoring and surveillance," James P. Anderson Company, Washington, DC, USA, Tech. Rep. 79F296400, 1980, pp. 1–56.

[60] D. E. Denning, "An intrusion-detection model," *IEEE Trans. Softw. Eng.*, vol. SE-13, no. 2, pp. 222–232, Feb. 1987.

[61] K. Gurney, *An Introduction to Neural Networks*. Boca Raton, FL, USA: CRC Press, 2014.

[62] J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural Netw.*, vol. 61, pp. 85–117, Jan. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0893608014002135

[63] A. Patel, H. Alhussian, J. M. Pedersen, B. Bounabat, J. C. Júnior, and S. Katsikas, "A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems," *Comput. Secur.*, vol. 64, pp. 92–109, Jan. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404816300748

[64] M. A. Hearst, S. T. Dumais, E. Osuna, J. Platt, and B. Scholkopf, "Support vector machines," *IEEE Intell. Syst. Appl.*, vol. 13, no. 4, pp. 18–28, Jul. 1998.

[65] M. Tavallaee, E. Bagheri, W. Lu, and A.-A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. 2nd IEEE Symp. Comput. Intell. Secur. Defence Appl.*, Jul. 2009, pp. 1–6.

[66] R. R. de Azevedo, F. Freitas, S. C. de Almeida, M. J. S. C. Almeida, E. C. de Barros Filho, and W. C. Veras, "CoreSec: An ontology of security aplied to the business process of management," in *Proc. Euro Amer. Conf. Telematics Inf. Syst. (EATIS)*, New York, NY, USA, 2008, Art. no. 13. [Online]. Available: http://doi.acm.org/10.1145/1621087.1621100

[67] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, "Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2011, pp. 1–8.

[68] L. Dhanabal and S. P. Shantharajah, "A study on NSL-KDD dataset for intrusion detection system based on classification algorithms," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 4, no. 6, pp. 446–452, 2015.

[69] S. Revathi and A. Malathi, "A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection," *Int. J. Eng. Res. Technol.*, vol. 2, no. 12, pp. 1848–1853, 2013.
[70] I. H. Witten, E. Frank, and M. A. Hall, *Data Mining: Practical Machine Learning Tools and Techniques*. San Mateo, CA, USA: Morgan Kaufmann, 2016.
[71] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The WEKA data mining software: An update," *ACM SIGKDD Explorations Newslett.*, vol. 11, no. 1, pp. 10–18, 2009. [Online]. Available: http://doi.acm.org/10.1145/1656274.1656278
[72] Q. He and R. S. Blum, "Smart grid monitoring for intrusion and fault detection with new locally optimum testing procedures," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2011, pp. 3852–3855.
[73] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study," *IEEE Syst. J.*, vol. 9, no. 1, pp. 31–44, Mar. 2015.
[74] A. Bifet, G. Holmes, R. Kirkby, and B. Pfahringer, "MOA: Massive online analysis," *J. Mach. Learn. Res.*, vol. 11, pp. 1601–1604, May 2010.
[75] *Massive Online Analysis*. [Online]. Available: https://moa.cms.waikato.ac.nz/
[76] A. Bifet, R. Gavaldà, G. Holmes, and B. Pfahringer, *Machine Learning for Data Streams: With Practical Examples in MOA*. Cambridge, MA, USA: MIT Press, 2018. [Online]. Available: https://moa.cms.waikato.ac.nz/book/
[77] R. Vijayanand, D. Devaraj, and B. Kannapiran, "Support vector machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid," in *Proc. IEEE 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017, pp. 1–7.
[78] G. Creech and J. Hu, "Generation of a new IDS test dataset: Time to retire the KDD collection," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2013, pp. 4487–4492.
[79] A. I. Abubakar, H. Chiroma, S. A. Muaz, and L. B. Ila, "A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems," *Procedia Comput. Sci.*, vol. 62, pp. 221–227, Sep. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050915025788
[80] Y. Li, R. Qiu, and S. Jing, "Intrusion detection system using online sequence extreme learning machine (OS-ELM) in advanced metering infrastructure of smart grid," *PLoS ONE*, vol. 13, no. 2, 2018, Art. no. e0192216.
[81] G.-B. Huang, D. H. Wang, and Y. Lan, "Extreme learning machines: A survey," *Int. J. Mach. Learn. Cybern.*, vol. 2, no. 2, pp. 107–122, Jun. 2011. doi: 10.1007/s13042-011-0019-y.
[82] *CER Smart Metering Project*. [Online]. Available: www.ucd.ie/issda/CER-electricity
[83] P. Y. Chen, S. Yang, J. A. McCann, J. Lin, and X. Yang, "Detection of false data injection attacks in smart-grid systems," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 206–213, Feb. 2015.
[84] N. Boumkheld, M. Ghogho, and M. El Koutbi, "Intrusion detection system for the detection of blackhole attacks in a smart grid," in *Proc. 4th Int. Symp. Comput. Bus. Intell. (ISCBI)*, Sep. 2016, pp. 108–111.
[85] T. Issariyakul and E. Hossain, "Introduction to network simulator 2 (NS2)," in *Introduction to Network Simulator NS2*. Boston, MA, USA: Springer, 2012, pp. 21–40.
[86] C. Perkins, E. Belding-Royer, and S. Das, *Ad Hoc On-Demand Distance Vector (AODV) Routing*, Internet Engineering Task Force, document RFC 3561, 2003.
[87] I. Ullah and Q. H. Mahmoud, "An intrusion detection framework for the smart grid," in *Proc. IEEE 30th Can. Conf. Elect. Comput. Eng. (CCECE)*, Apr./May 2017, pp. 1–5.
[88] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Comput. Secur.*, vol. 31, no. 3, pp. 357–374, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404811001672
[89] *Intrusion Detection Evaluation Dataset (ISCXIDS2012)*. [Online]. Available: http://www.unb.ca/cic/datasets/ids.html
[90] Y. Zhao and Y. Zhang, "Comparison of decision tree methods for finding active objects," *Adv. Space Res.*, vol. 41, no. 12, pp. 1955–1959, 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S027311770700796X
[91] F. A. A. Alseiari and Z. Aung, "Real-time anomaly-based distributed intrusion detection systems for advanced metering infrastructure utilizing stream data mining," in *Proc. Int. Conf. Smart Grid Clean Energy Technol. (ICSGCE)*, Oct. 2015, pp. 148–153.
[92] V. Gulisano, M. Almgren, and M. Papatriantafilou, "METIS: A two-tier intrusion detection system for advanced metering infrastructures," in *Proc. Int. Conf. Secur. Privacy Commun. Netw.*, J. Tian, J. Jing, and M. Srivatsa, Eds. Cham, Switzerland: Springer, 2015, pp. 51–68.
[93] M. Stonebraker, U. Çetintemel, and S. Zdonik, "The 8 requirements of real-time stream processing," *ACM SIGMOD Rec.*, vol. 34, no. 4, pp. 42–47, 2005. [Online]. Available: http://doi.acm.org/10.1145/1107499.1107504
[94] R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *Proc. IEEE 17th Pacific Rim Int. Symp. Dependable Comput.*, Dec. 2011, pp. 184–193.
[95] A. F. Snyder and M. T. G. Stuber, "The ANSI C12 protocol suite-updated and now with network capabilities," in *Proc. Power Syst. Conf., Adv. Metering, Protection, Control, Commun., Distrib. Resour.*, Mar. 2007, pp. 117–122.
[96] C. Ko, P. Brutch, J. Rowe, G. Tsafnat, and K. Levitt, "System health and intrusion monitoring using a hierarchy of constraints," in *Recent Advances in Intrusion Detection*, W. Lee, L. Mé, and A. Wespi, Eds. Berlin, Germany: Springer, 2001, pp. 190–203.
[97] 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, Sep. 2015.
[98] R. Mitchell and I.-R. Chen, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1254–1263, Sep. 2013.
[99] P. Jokar and V. C. M. Leung, "Intrusion detection and prevention for ZigBee-based home area networks in smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1800–1811, May 2018.
[100] Y. Kabalci, "IEEE 802.15.4 technologies for smart grids," in *Smart Grids and Their Communication Systems*. Singapore: Springer, 2019, pp. 531–550. doi: 10.1007/978-981-13-1768-2_15.
[101] Z. Alliance and H. P. Alliance, "Smart energy profile 2.0 technical requirements document," Zigbee Aliance, Davis, CA, USA, Tech. Rep. ZigBee-105553, Apr. 2010.
[102] M. Attia, H. Sedjelmaci, S. M. Senouci, and E.-H. Aglzim, "A new intrusion detection approach against lethal attacks in the smart grid: Temporal and spatial based detections," in *Proc. Global Inf. Infrastruct. Netw. Symp. (GIIS)*, Oct. 2015, pp. 1–3.
[103] T. H. Morris, B. A. Jones, R. B. Vaughn, and Y. S. Dandass, "Deterministic intrusion detection rules for MODBUS protocols," in *Proc. 46th Hawaii Int. Conf. Syst. Sci.*, Jan. 2013, pp. 1773–1781.
[104] *Snort*. [Online]. Available: https://www.snort.org/
[105] W. Park and S. Ahn, "Performance comparison and detection analysis in snort and suricata environment," *Wireless Pers. Commun.*, vol. 94, no. 2, pp. 241–252, May 2017. doi: 10.1007/s11277-016-3209-9.
[106] T. Fleming and H. Wilander, "Network intrusion and detection: An evaluation of snort," Linköping Univ., Linköping, Sweden, Tech. Rep., 2018.
[107] H. Li, G. Liu, W. Jiang, and Y. Dai, "Designing snort rules to detect abnormal DNP3 network data," in *Proc. Int. Conf. Control, Autom. Inf. Sci. (ICCAIS)*, Oct. 2015, pp. 343–348.
[108] E. Hodo, S. Grebeniuk, H. Ruotsalainen, and P. Tavolato, "Anomaly detection for simulated IEC-60870-5-104 trafiic," in *Proc. 12th Int. Conf. Availability, Rel. Secur. (ARES)*, New York, NY, USA, 2017, pp. 100:1–100:7. [Online]. Available: http://doi.acm.org/10.1145/3098954.3103166
[109] P. Matoušek, "Description and analysis of IEC 104 protocol," Faculty Inf. Technol., Brno Univ. Technol., Brno, Czech Republic, Tech. Rep., 2017.
[110] A. Liaw and M. Wiener, "Classification and regression by randomforest," *R News*, vol. 2, no. 3, pp. 18–22, 2002.
[111] N. Goldenberg and A. Wool, "Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems," *Int. J. Critical Infrastructure Protection*, vol. 6, no. 2, pp. 63–75, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548213000243
[112] *Wireshark*. [Online]. Available: https://www.wireshark.org/
[113] U. Banerjee, A. Vashishtha, and M. Saxena, "Evaluation of the capabilities of wireshark as a tool for intrusion detection," *Int. J. Comput. Appl.*, vol. 6, no. 7, pp. 1–5, 2010.

[114] V. Ndatinya, Z. Xiao, V. R. Manepalli, K. Meng, and Y. Xiao, "Network forensics analysis using wireshark," *Int. J. Secur. Netw.*, vol. 10, no. 2, pp. 91–106, 2015.
[115] *Pcapy*. [Online]. Available: https://www.secureauth.com/labs/open-source-tools/pcapy
[116] *Impacket*. [Online]. Available: https://www.secureauth.com/labs/open-source-tools/impacket
[117] S. D. Anton, S. Kanoor, D. Fraunholz, and H. D. Schotten, "Evaluation of machine learning-based anomaly detection algorithms on an industrial modbus/tcp data set," in *Proc. 13th Int. Conf. Availability, Rel. Secur. (ARES)*, New York, NY, USA, 2018, pp. 41:1–41:9. [Online]. Available: http://doi.acm.org/10.1145/3230833.3232818
[118] A. Lemay and J. M. Fernandez, "Providing SCADA network data sets for intrusion detection research," in *Proc. 9th Workshop Cyber Secur. Experimentation Test (CSET)*, Austin, TX, USA: USENIX Association, 2016, pp. 1–8. [Online]. Available: https://www.usenix.org/conference/cset16/workshop-program/presentation/lemay
[119] P. Cunningham and S. J. Delany, "k-Nearest neighbour classifiers," *Multiple Classifier Syst.*, vol. 34, pp. 1–17, Mar. 2007.
[120] A. K. Jain, "Data clustering: 50 years beyond K-means," *Pattern Recognit. Lett.*, vol. 31, no. 8, pp. 651–666, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167865509002323
[121] P.-H. Wang, I.-E. Liao, K.-F. Kao, and J.-Y. Huang, "An intrusion detection method based on log sequence clustering of honeypot for modbus TCP protocol," in *Proc. IEEE Int. Conf. Appl. Syst. Invention (ICASI)*, Apr. 2018, pp. 255–258.
[122] M. Baykara and R. Das, "A novel honeypot based security approach for real-time intrusion detection and prevention systems," *J. Inf. Secur. Appl.*, vol. 41, pp. 103–116, Aug. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214212616303295
[123] A. Jicha, M. Patton, and H. Chen, "SCADA honeypots: An in-depth analysis of conpot," in *Proc. IEEE Conf. Intell. Secur. Informat. (ISI)*, Sep. 2016, pp. 196–198.
[124] W. H. E. Day and H. Edelsbrunner, "Efficient algorithms for agglomerative hierarchical clustering methods," *J. Classification*, vol. 1, no. 1, pp. 7–24, 1984. doi: 10.1007/BF01890115.
[125] *MongoDB*. [Online]. Available: https://www.mongodb.com/
[126] K. Banker, *MongoDB in Action*. Shelter Island, NY, USA: Manning Publications, 2011.
[127] Y. Yang, K. McLaughlin, S. Sezer, Y. B. Yuan, and W. Huang, "Stateful intrusion detection for IEC 60870-5-104 SCADA security," in *Proc. IEEE PES Gen. Meeting Conf. Expo.*, Jul. 2014, pp. 1–5.
[128] J. Hurley, A. Munoz, and S. Sezer, "ITACA: Flexible, scalable network analysis," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 1069–1073.
[129] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, "Intrusion detection system for IEC 60870-5-104 based SCADA networks," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2013, pp. 1–5.
[130] Z. Feng, S. Qin, X. Huo, P. Pei, Y. Liang, and L. Wang, "Snort improvement on profinet RT for industrial control system intrusion detection," in *Proc. 2nd IEEE Int. Conf. Comput. Commun. (ICCC)*, Oct. 2016, pp. 942–946.
[131] S. Simatic. (2008). *PROFINET System Description*. [Online]. Available: http://www.siemens.fi/pool/products/industry/iadt_is/tuotteet/automaatiotekniikka/teollinen_tiedonsiirto/profinet/man_pnsystem_description.pdf
[132] P. Ferrari, A. Flammini, and S. Vitturi, "Performance analysis of PROFINET networks," *Comput. Standards Interfaces*, vol. 28, no. 4, pp. 369–385, Apr. 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0920548905000528
[133] D. Zhang, J. Wang, and H. Zhang, "Peach improvement on profinet-DCP for industrial control system vulnerability detection," in *Proc. 2nd Int. Conf. Elect., Comput. Eng. Electron.*, 2015, pp. 1–6. doi: 10.2991/icecee-15.2015.305.
[134] M. Baud and M. Felser, "Profinet IO-device emulator based on the man-in-the-middle attack," in *Proc. IEEE Conf. Emerg. Technol. Factory Autom.*, Sep. 2006, pp. 437–440.
[135] S.-C. Li, Y. Huang, B.-C. Tai, and C.-T. Lin, "Using data mining methods to detect simulated intrusions on a modbus network," in *Proc. IEEE 7th Int. Symp. Cloud Service Comput. (SC2)*, Nov. 2017, pp. 143–148.
[136] S. B. Aher and L. M. R. J. Lobo, "Data mining in educational system using weka," in *Proc. Int. Conf. Emerg. Technol. Trends (ICETT)*, vol. 3, 2011, pp. 20–25.
[137] F. Cleveland, "IEC TC57 WG15: IEC 62351 security standards for the power system information infrastructure," White Paper, 2012. [Online]. Available: http://www.collegioingegnerivenezia.it/images/Articoli_Pubblicazioni/2016_Cybersecurity/WhitePaperSecurityStandardsIEC_TC57_March_2014.pdf
[138] B. K. K. M. S. Sezer, "Towards a stateful analysis framework for smart grid network intrusion detection," in *Proc. 4th Int. Symp. ICS SCADA Cyber Secur. Res.*, BCS Learn. Develop., 2016, pp. 1–8.
[139] *Suricata*. [Online]. Available: https://suricata-ids.org/
[140] K. Wong, C. Dillabaugh, N. Seddigh, and B. Nandy, "Enhancing suricata intrusion detection system for cyber security in SCADA networks," in *Proc. IEEE 30th Can. Conf. Elect. Comput. Eng. (CCECE)*, Apr./May 2017, pp. 1–5.
[141] J. T. Sørensen and M. G. Jaatun, "An analysis of the manufacturing messaging specification protocol," in *Ubiquitous Intelligence and Computing*, F. E. Sandnes, Y. Zhang, C. Rong, L. T. Yang, and J. Ma, Eds. Berlin, Germany: Springer, 2008, pp. 602–615.
[142] Y. Kwon, H. K. Kim, Y. H. Lim, and J. I. Lim, "A behavior-based intrusion detection technique for smart grid infrastructure," in *Proc. IEEE Eindhoven PowerTech*, Jun. 2015, pp. 1–6.
[143] C. Kriger, S. Behardien, and J.-C. Retonda-Modiya, "A detailed analysis of the goose message structure in an IEC 61850 standard-based substation automation system," *Int. J. Comput. Commun. Control*, vol. 8, no. 5, pp. 708–721, 2013.
[144] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, and S. Sezer, "Multidimensional intrusion detection system for IEC 61850-based SCADA networks," *IEEE Trans. Power Del.*, vol. 32, no. 2, pp. 1068–1078, Apr. 2017.
[145] M. Kabir-Querrec, S. Mocanu, J.-M. Thiriet, and E. Savary, "Power utility automation cybersecurity: IEC 61850 specification of an intrusion detection function," in *Proc. 25th Eur. Saf. Rel. Conf. (ESREL)*, 2015, pp. 1–9.
[146] H. Yoo and T. Shon, "Novel approach for detecting network anomalies for substation automation based on IEC 61850," *Multimedia Tools Appl.*, vol. 74, no. 1, pp. 303–318, 2015.
[147] T. K. Moon, "The expectation-maximization algorithm," *IEEE Signal Process. Mag.*, vol. 13, no. 6, pp. 47–60, Nov. 1996.
[148] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: Identifying density-based local outliers," in *Proc. Int. Conf. Manage. Data (SIGMOD)*, vol. 29. 2000, pp. 93–104.
[149] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan, "An intrusion detection system for IEC61850 automated substations," *IEEE Trans. Power Del.*, vol. 25, no. 4, pp. 2376–2383, Oct. 2010.
[150] R. Van Hauser, "THC-HYDRA, 8.4th EDN," github. com, Tech. Rep., 2017.
[151] *ARP Seringe*. [Online]. Available: http://www.securiteam.com/tools/5QP0I2AC0I.html
[152] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in *Proc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2014, pp. 1–5.
[153] Y. Yang, K. McLaughlin, L. Gao, S. Sezer, Y. Yuan, and Y. Gong, "Intrusion detection system for IEC 61850 based smart substations," in *Proc. Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.
[154] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.
[155] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3104–3113, Nov. 2015.
[156] *OpenPDC*. https://github.com/GridProtectionAlliance/openPDC
[157] G. P. Alliance, "OpenPDC documentation."
[158] R. Khan, A. Albalushi, K. McLaughlin, D. Laverty, and S. Sezer, "Model based intrusion detection system for synchrophasor applications in smart grid," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2017, pp. 1–5.
[159] J. Ahrenholz, C. Danilov, T. R. Henderson, and J. H. Kim, "CORE: A real-time network emulator," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Nov. 2008, pp. 1–7.
[160] S. Tan, W.-Z. Song, Q. Dong, and L. Tong, "SCORE: Smart-grid common open research emulator," in *Proc. 3rd IEEE Int. Conf. Smart Grid Commun. (IEEE SmartGridComm)*, Nov. 2012, pp. 282–287.
[161] Y. Yang *et al.*, "Intrusion detection system for network security in synchrophasor systems," in *Proc. IET Int. Conf. Inf. Commun. Technol. (IETICT)*, Apr. 2013, pp. 246–252.

[162] P. Li, "Selecting and using virtualization solutions: Our experiences with VMware and virtualbox," *J. Comput. Sci. Colleges*, vol. 25, no. 3, pp. 11–17, 2010.
[163] D. M. Laverty, R. J. Best, P. Brogan, I. Al Khatib, L. Vanfretti, and D. J. Morrow, "The OpenPMU platform for open-source phasor measurements," *IEEE Trans. Instrum. Meas.*, vol. 62, no. 4, pp. 701–709, Apr. 2013.
[164] *Colasoft Packet Builder*, Colasoft, 2011, pp. 8–20.
[165] G. Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. New York, NY, USA: ACM, 2009.
[166] D. Kennedy, J. O'Gorman, D. Kearns, and M. Aharoni, *Metasploit: The Penetration Tester's Guide*. San Francisco, CA, USA: No Starch Press, 2011.
[167] R. Masood, U. Ghazia, and Z. Anwar, "SWAM: Stuxnet worm analysis in Metasploit," in *Proc. Frontiers Inf. Technol.(FIT)*, Dec. 2011, pp. 142–147.
[168] S. Sanfilippo *et al.*, "Hping," Tech. Rep., 2006.
[169] S. Gorman, "Electricity grid in US penetrated by spies," *Wall Street J.*, vol. 8, pp. 1–3, Apr. 2009.
[170] D. Starkey. *Hacker Group Dragonfly Takes Aim at us Power Grid*. [Online]. Available: https://www.geek.com/tech/hacker-groupdragonfly-takes-aim-at-us-power-grid-1715157/
[171] *RISI—The Repository of Industrial Security Incidents*. [Online]. Available: http://www.risidata.com/
[172] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Hum. Factors*, vol. 37, pp. 32–64, Sep. 1995.
[173] B. McGuinness and L. Foy, "A subjective measure of SA: The crew awareness rating scale (CARS)," in *Proc. 1st Hum. Perform., Situation Awareness, Autom. Conf.*, vol. 16. Savannah, Georgia: SA Technol., 2000, pp. 286–291.
[174] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, and S. Sezer, "Multidimensional intrusion detection system for IEC 61850-BASED SCADA networks," *IEEE Trans. Power Del.*, vol. 32, no. 2, pp. 1068–1078, Apr. 2017.
[175] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta, "A multidimensional critical state analysis for detecting intrusions in SCADA systems," *IEEE Trans. Ind. Informat.*, vol. 7, no. 2, pp. 179–186, May 2011.
[176] D. Jin *et al.*, "Toward a cyber resilient and secure microgrid using software-defined networking," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2494–2504, Sep. 2017.
[177] I. Aguirre and S. Alonso, "Improving the automation of security information management: A collaborative approach," *IEEE Secur. Privacy*, vol. 10, no. 1, pp. 55–59, Jan./Feb. 2012.
[178] G. Cerullo, V. Formicola, P. Iamiglio, and L. Sgaglione. (2014). "Critical infrastructure protection: Having SIEM technology cope with network heterogeneity." [Online]. Available: https://arxiv.org/abs/1404.7563
[179] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.
[180] K. Boroojeni *et al.*, "A novel cloud-based platform for implementation of oblivious power routing for clusters of microgrids," *IEEE Access*, vol. 5, pp. 607–619, 2017.

PANAGIOTIS I. RADOGLOU-GRAMMATIKIS received the Diploma degree (five years) from the Department of Informatics and Telecommunications Engineering, University of Western Macedonia, Greece, in 2016, where he is currently pursuing the Ph.D. degree. He is also a Research Associate with the University of Western Macedonia in national and European funded research projects. His main research interests include information security, intrusion detection, vulnerability research, and applied cryptography.

PANAGIOTIS G. SARIGIANNIDIS received the B.Sc. and Ph.D. degrees in computer science from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2001 and 2007, respectively. He has been an Assistant Professor with the Department of Informatics and Telecommunications, University of Western Macedonia, Kozani, Greece, since 2016. He has published over 120 papers in international journals, conferences, and book chapters. He has been involved in several national, EU, and international projects. He is currently a Project Coordinator of the H2020 Project entitled SPEAR: Secure and PrivatE smArt gRid (H2020-DS-2016-2017/H2020-DS-SC7-2017). His research interests include optical and wireless telecommunications, resource allocation, the Internet of Things, and security and privacy in smart networks.