Machine Learning-based Intrusion Detection for Smart Grid Computing: A Survey

NITASHA SAHANI, RUOXI ZHU, JIN-HEE CHO, and CHEN-CHING LIU, Virginia Tech, USA

Machine learning (ML)-based intrusion detection system (IDS) approaches have been significantly applied and advanced the state-of-the-art system security and defense mechanisms. In smart grid computing environments, security threats have been significantly increased as shared networks are commonly used, along with the associated vulnerabilities. However, compared to other network environments, ML-based IDS research in a smart grid is relatively unexplored, although the smart grid environment is facing serious security threats due to its unique environmental vulnerabilities. In this article, we conducted an extensive survey on ML-based IDS in smart grids based on the following key aspects: (1) The applications of the ML-based IDS in transmission and distribution side power components of a smart power grid by addressing its security vulnerabilities; (2) dataset generation process and its usage in applying ML-based IDSs in the smart grid; (3) a wide range of ML-based IDSs used by the surveyed papers in the smart grid environment; (4) metrics, complexity analysis, and evaluation testbeds of the IDSs applied in the smart grid; and (5) lessons learned, insights, and future research directions.

CCS Concepts: • **Computing methodologies** → **Machine learning algorithms**; • **Security and privacy** → **Intrusion detection systems;**

Additional Key Words and Phrases: Smart grid, security vulnerabilities, and threats, cyberattacks, substation automation, SCADA, AMI, machine learning, intrusion detection, metrics

ACM Reference format:
Nitasha Sahani, Ruoxi Zhu, Jin-Hee Cho, and Chen-Ching Liu. 2023. Machine Learning-based Intrusion Detection for Smart Grid Computing: A Survey. *ACM Trans. Cyber-Phys. Syst.* 7, 2, Article 11 (April 2023), 31 pages.
https://doi.org/10.1145/3578366

1 INTRODUCTION

An interconnected network, known as an electrical grid that consists of substations, transformers, and transmission lines, ensures the delivery of electricity from a generation power plant to power

Nitasha Sahani and Ruoxi Zhu contributed equally to this research.

This work was partially supported by the National Science Foundation under Grant No. CPS-1837359, the Department of Energy Solar Energy Technologies Office, Award No. DE-EE0009339 at Virginia Tech, and Commonwealth Cyber Initiative, State of Virginia. This research was also partly supported by NSF Grant CNS-2141095 and 2106987, and Virginia Tech's Integrated Security Destination Area-The Integrated Security Education and Research Center (ISDA-ISERC) Research Program.

Authors' addresses: N. Sahani and R. Zhu, Virginia Tech, Blacksburg, Virginia, VA, 24061; emails: nitashas@vt.edu, ruoxi@vt.edu; J.-H. Cho, Virginia Tech, Falls Church, VA; email: jicho@vt.edu; C.-C. Liu, Virginia Tech, Blacksburg, VA; email: ccliu@vt.edu.

2378-962X/2023/04-ART11 $15.00
https://doi.org/10.1145/3578366

distribution spaces such as residences, industry, or commercial buildings. However, as the need for centralized control and management increases along with communications between electric utilities and consumers, the previously isolated power grid is connected to the Internet through a communication network. Additionally, digital technology also has sensors in the transmission lines with control capabilities. The control and automation capabilities in the power grid are known as the "smart grid," responding to rapidly changing electrical demand and reacting digitally to any adverse fluctuations from regular operating criteria in terms of faults, attacks, or intrusions. A smart grid tends to ensure system reliability, power availability, and system performance efficiency during physical or network disturbances by integrating the physical power system with the cyber system.

1.1 Motivation

Smart grid network architecture includes **Home Area Network (HAN), Neighborhood Area Network (NAN)**, and **Wide Area Network (WAN)**. The HAN and NAN involve the metering structure, smart meters, and data concentrators, whereas the WAN involves applications like **Supervisory Control and Data Acquisition (SCADA)** [128]. As this arrangement involves the inter-dependency of communication technology [9] at different network levels, the system becomes more susceptible to internal and/or external cyberattacks. An IDS's key role is to monitor the data traffic flow and detect suspicious activities or threats by identifying unauthorized access and accordingly raising an alarm notifying an administrator to block such security breaches or automating the mitigation process. IDSs are commonly categorized into two types. Anomaly-based IDS detects threats based on any deviation from normal behaviors. However, signature-based IDS compares the traffic flow with known attack patterns and raises a system threat concern when they match. Depending on the placement of an IDS in a system, it can be host-based (i.e., software applications installed on individual client computers) or network-based (i.e., placed in the network at multiple points as hardware sensors or installed system software connected to network analyzing data packet flow) [21]. Depending on whether a smart grid environment is more centralized or decentralized (or distributed), one can choose either approach for optimal deployment [65].

Conventional IDSs have shown limitations in addressing the dynamic nature of the communication network in a smart grid in terms of scalability and/or adaptiveness when the smart grid faces highly real-time dynamic traffic patterns. In addition, they should support security services for legacy protocols, such as services to support security goals, including confidentiality, integrity, availability, non-repudiation, and authentication. Further, the IDS also should support hardware and software resource constraints and associated maintenance cycles in the system [35, 77].

Compared to other environments, IDS deployment in the smart grid is highly challenging because of system security impact and its associated economic repercussions when the system is attacked or fails. Along with power system network security constraints, the sensor networks and the complex communication process between the utility and the consumers in the smart grid should ensure smooth and reliable power transfer and usage data. However, as the sensor network is part of the system, the security challenges related to data integrity, availability, and connectivity are at stake. Furthermore, as a **Cyber-Physical System (CPS)**, the failure to detect such intrusions in the smart grid can introduce a physical impact on the power system, such as a major blackout, loss of

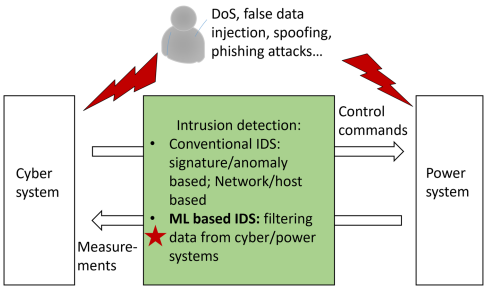


Fig. 1. Motivation.

control, or system collapse. Therefore, it is obvious that there are benefits of deploying ML-based IDS to enhance the process of self-learning and self-configuration by the computers from data patterns and improve predictions based on the information-extensive data exemplars without human interventions depending on the learned behavior.

Since accurate, reliable intrusion detection is critical to ensuring the security and performance of smart grid systems, ML-based IDS techniques provide the powerful capability to detect and classify cyberattacks accurately. In particular, ML-based IDS can potentially detect zero-day attacks (unknown anomalies) and known anomalies underneath the complex cyber-physical data flow in real time. However, ML-based IDS techniques must be adjusted to adapt to unique features of a particular CPS environment, such as smart grids. Therefore, as the motivation illustrated in Figure 1, we have conducted an extensive survey on how ML-based IDS research has been explored to detect cyberattacks in smart grid environments. This will allow us to obtain insights and limitations of the state-of-the-art IDS developed for the smart grid and identify the gaps that need to be addressed in future research.

1.2 Comparison with the Existing Survey Papers

In this section, we compare our survey article with other existing survey papers on IDS applicable in smart grid environments in terms of their key contributions, compared to those in our survey article.

Zhu and Sastry [136] investigated existing SCADA-specific IDS techniques and discussed their key taxonomies. Based on the specific needs of a different SCADA system, the authors discussed different IDS techniques, including ML-based IDS, in terms of detection time, self-security, and fallacy analysis. However, they did not discuss attack types considered in the surveyed IDS techniques. Mitchell and Chen [77] conducted an extensive survey on IDS techniques for CPS architectures with their key performance requirements and IDS evaluation metrics. The authors classified IDSs based on a detection algorithm and audit material where each technique is discussed under different application domains. The authors partially discussed the datasets used for different implementations, methodologies, and key design principles. Mitchell and Chen [78] also presented a survey about IDS in wireless networks in terms of security measurements in three IDS types—anomaly-based, specification-based, signature-based, and reputation-based IDS—under different attack scenarios. However, they did not discuss IDS features to deal with issues in smart grid environments.

Tong et al. [113] extensively surveyed IDS techniques for the **Advanced Metering Infrastructure (AMI)** in terms of threat analyses based on attack surfaces, techniques, and attack consequences in AMI. They discussed the state-of-the-art ML-based IDS solutions and their classification with the key guidelines for designing and deploying the IDS for the AMI and research challenges. However, their survey on metrics, attacks, and evaluation methodology is significantly limited.

Buczak and Guven [18] surveyed ML and data mining-based IDS for its use in general communication networks. The authors used a common IDS classification, such as anomaly-based, misuse-based, and hybrid IDS, and classified them based on the deployment type, e.g., network-based and host-based to describe each ML-based IDS technique. Borkar et al. [17] also surveyed IDS techniques of a general network along with an internal intrusion detection and protection system (i.e., IDS and IPS). However, these surveys [17, 18] do not cover IDS features to deal with security issues raised by the unique characteristics of the smart grid.

Unlike the existing survey papers on ML-based IDS discussed above, our survey article provides details of existing ML-based IDS techniques to build fundamental ideas to be deployed in smart grid environments. For the convenience of readers, we summarized the details of the key differences between our survey article and those existing survey papers in Table 1.

Table 1. Comparison of Our Article with the Existing Survey Papers

Key Criteria	Our survey article (2023)	Zhu and Sastry [136] (2010)	Mitchell and Chen [77] (2014)	Mitchell and Chen [78] (2014)	Tong et al. [113] (2016)	Buczak and Guven [18] (2016)	Borkar et al. [17] (2017)
Vulnerabilities of cyber systems	✓	✓	✘	✘	✓	✘	✘
Application domain	SCADA, WSN, WMN, AMI	SCADA	CPS	WN, CPS	AMI	General network	General network
Performance evaluation of ML techniques	✓	✓	✓	✓	▲	✓	✘
IDS types based on different ML-based designs	✓	✓	✓	✓	✓	✓	✘
Attack types in smart grids	✓	✘	▲	▲	✘	▲	✓
IDS metrics	✓	✘	✓	✓	✘	✓	✘
Evaluation methods/tools	✓	✘	✘	✘	✘	✘	✘
Pros and cons of ML methods	✓	✓	✓	✓	✓	✓	✓
Lessons learned and future research directions	✓	▲	✓	✓	▲	✓	▲

✓: Surveyed and classified; ▲: Partially addressed; ✘: Neither surveyed nor classified.

1.3 Key Contributions

The **following key contributions** in this article can be summarized as follows:

(1) We conducted an extensive survey on ML-based IDS techniques for smart grid computing environments. To our knowledge, there has been no prior survey paper that mainly discusses ML-based IDS techniques to be deployed in smart grid environments with specific discussions regarding security vulnerabilities and attacks, ML-based IDS techniques, metrics, validation methods, and complexity analysis for securing smart grid CPSs.
(2) We classified ML-based IDS techniques in smart grid environments based on distribution systems and transmission systems, which are two key components in smart grid systems. The weak links between cyber and physical systems in a smart grid environment induce more potential attack vulnerabilities. We discuss the existing IDS techniques based on unique vulnerability aspects of the smart grid environments.
(3) We discussed methodologies used to analyze the performance of ML-based IDS techniques deployed in the smart grid environment, in terms of dataset generation to model attack behaviors, testbeds (i.e., simulation, emulation, and real testbeds), and metrics.
(4) Based on the detailed survey conducted in this article, we discussed limitations and insights and suggested promising future research directions.

The remainder of this survey article is structured as follows: Section 2 provides the structure of a cyber system in the smart grid including **Wide-Area Measurement Systems (WAMS), Substation Automation Systems (SAS)**, and **Distributed Energy Devices (DED)** along with key security vulnerabilities and common attack scenarios. Section 3 discusses ML-based IDS techniques for the smart grid application domain. Key performance metrics, evaluation methodologies, and the time complexity of the ML-based IDS techniques used for the smart grid are discussed in Section 4. Section 5 provides the insights and lessons learned from the conducted survey in this work. Finally, Section 6 summarizes the key findings from this extensive survey and suggests future research directions. The organization of the survey article is illustrated in Figure 2.

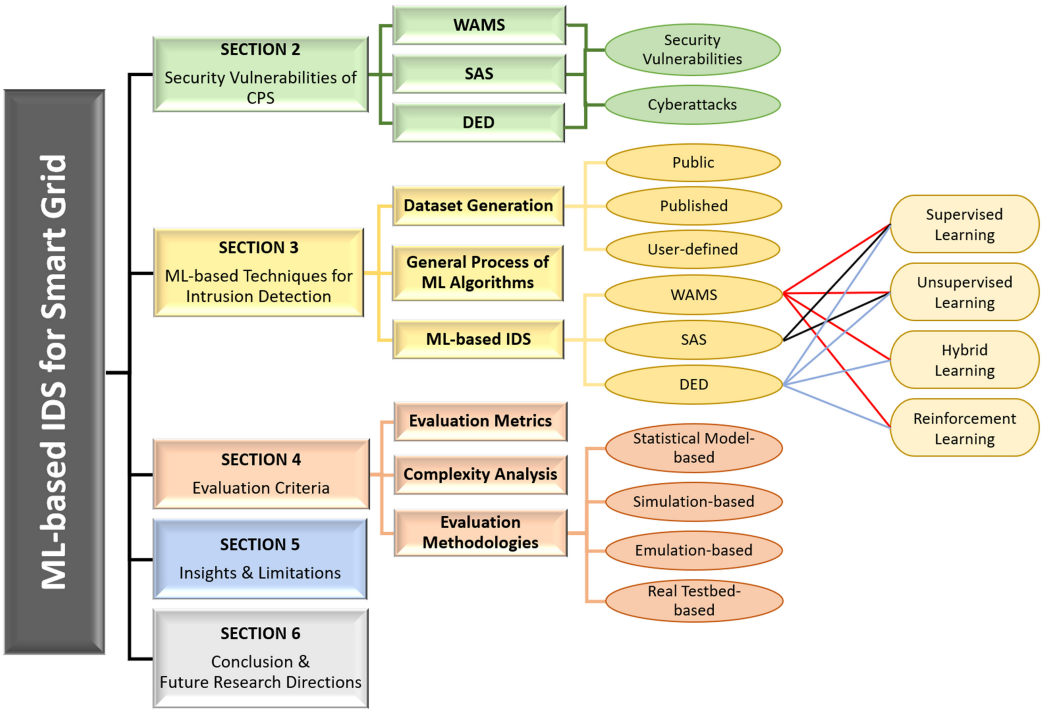


Fig. 2. The organization of survey article.

2 SECURITY VULNERABILITIES OF CPS IN SMART GRID

Information and Communications Technology (ICT) [70] in a smart grid is highly integrated with the power infrastructure. A cyber system integrated with a power system builds a comprehensive CPS together. Different system vulnerabilities can introduce security threats to the power system to make the CPS unstable and unreliable [87]. In Figure 3, we demonstrate the hierarchical architecture of a smart grid with three major information systems working together: *WAMS, SAS, and DED.*

2.1 Wide-Area Measurement Systems (WAMS)

WAMS leverage the high-speed wide area networks to poll power system measurements from field sensors. In this article, we generalize the WAMS into two systems, synchrophasor systems, and traditional SCADA systems. As a conventional **Industrial Control System (ICS)** used in a power system, SCADA collects measurement data from **Remote Terminal Units (RTU)** or **Intelligent Electronic Devices (IEDs)** in substations and transmits the controlled or monitored data from the control center back to the grid. WAN can implement **Distributed Network Protocol 3 (DNP3)** [53] and Modbus [111], which are the specialized protocols for communications between the substations and control center in a SCADA system. Compared with the SCADA system, synchrophasor data are generated by physical devices, such as **Phasor Measurement Units (PMU)**.

2.1.1 Security Vulnerabilities in WAMS. As the control and monitoring functions of SCADA and synchrophasor networks highly rely on cyber infrastructure, cybersecurity concerns within communication networks can negatively impact the normal operations of a power system. WAMS has the following security vulnerabilities:

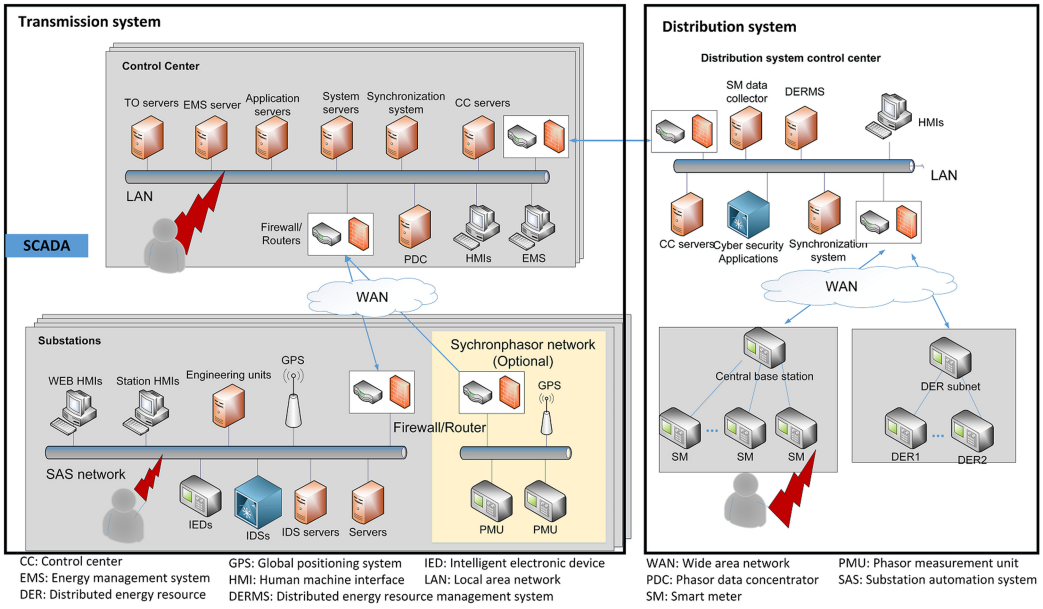


Fig. 3. Example of cyber systems in a smart grid.

- The existing SCADA in the power system still uses standardized technologies and protocols that expose vulnerabilities to attackers, as they might have knowledge of the loophole of those technologies.
- A few companies developed an **Energy Management System (EMS)** integrated with WAMS. The widespread availability of technical information provides useful information to cyber adversaries to intrude into the WAMS based on known vulnerabilities.
- Due to a lack of security mechanisms embedded in the communication networks of WAMS, the data exchange can be highly vulnerable to **False Data Injection (FDI)** attacks.

2.1.2 Cyberattacks in WAMS. Most existing survey papers focus on the attacks that are common in any communication network, such as scanning attacks [15, 36, 68, 74, 104, 133], **Denial of Service (DoS)** attacks [1, 25, 64, 74, 97, 106], or **Man-In-The-Middle (MITM)** attacks [15, 36, 68, 74, 104, 133]. The attacker uses scanning (or reconnaissance) attacks to discover the services in the cyber system to penetrate power systems. DoS and MITM attacks in the context of WAMS aim to make a power system inaccessible to authorized operators due to communication network interruption. By launching those attacks, the adversary can compromise the communication links between the substation and control center, so the transmission of measurements and control commands are damaged or delayed. Reconnaissance attacks are commonly considered when developing an IDS for WAMS [106, 117]. The reconnaissance attackers aim to intrude into a targeted system by using Trojan or phishing emails to collect information on an affected communication system before launching harmful attacks on the target physical device. The cyber attacker targeting a SCADA system of Ukraine's power grid uses this as a first step before launching its attack vector to achieve its ultimate attack goal [20].

2.2 Substation Automation Systems (SAS)

An SAS provides protection, control, automation, monitoring, and communication capabilities as part of a comprehensive substation control and monitoring solution [91]. To take advantage of

modern ICT, IEC 61850 is developed as a new global standard for substation automation. Even though IEC 62351 standard provides guidance on security measures for IEC 61850-based SAS, the deployment of security measures in the substation **Local Area Network (LAN)** is still in development. Therefore, it is critical to develop IDS that achieves the QoS requirements of cyber infrastructure in power systems.

2.2.1 Security Vulnerabilities in SAS. The modern substations have the following security vulnerabilities:

- The protection and control functions at digital substations heavily depend on the Ethernet-based communication within a substation LAN. Once any device within the substation is under attack, the basic functions at the substation level can be manipulated.
- Most IEDs deployed at an SAS are from third-party vendors. The adversary may leverage the loophole of the firmware of the IEDs to launch the attacks that can make the IEDs malfunction.
- As some cyber infrastructures at the SAS has TCP/IP interface, they can be vulnerable to various network attacks, such as DoS or MITM attacks.
- Cybersecurity mechanisms are rarely considered when protocols, such as IEC 61850, DNP3, and Modbus, are developed. Even though some authentication mechanisms are proposed in IEC 62351 or DNP3-SA, their weaknesses are well known as discussed in References [7, 108]. Therefore, the plain text traffic (e.g., **Generic Object-Oriented Substation Event (GOOSE)** or **Sampled Values (SV)**) can be easily modified by unauthorized access.

2.2.2 Cyberattacks in SAS. In an SAS, attackers can perform FDI attacks [8, 10, 27, 30, 31, 36, 41, 47, 48, 59, 64, 93, 99, 116, 120, 126] and **False Command Injection (FCI)** [1, 27, 48, 59, 72, 86, 106]. FDI attackers can inject bad data that can compromise measurements from different base-level grid sensors within a substation LAN or through remote access. This will allow undetected errors to contribute to faulty state variable estimations, such as bus voltage and line current measures. Furthermore, erroneous data injection in power system measurements can lead to faulty control command dispatch that causes grid-network states to fluctuate [123]. FDI attackers can execute random commands on SAS due to the lack of proper validation of the input commands. At a substation level, false control command injection will have a physical system impact, resulting in widespread outages or cascading failures.

2.3 Distributed Energy Devices (DED)

This segment of power components in the smart grid involves all the on-site generation (e.g., **Distributed Energy Resources (DERs)**), and decentralized energy sources (e.g., electric vehicles, battery energy systems, microgrids, and smart meters). Cybersecurity [44] in the distribution system has a significant impact on the reliability of the power grid. Due to the large-scale penetration of DEDs, the control system design becomes complex when it is integrated with multiple energy resources. A **Distribution Management System (DMS)** uses the measurements to determine the system states while the operators take appropriate actions for any abnormal operating conditions accordingly. With the large deployment of smart meters recording power consumption, AMI [135] is an integrated system for monitoring hundreds of distributed smart meters with two-way communications between the meters and the DMS. According to the functionalities of DEDs, the different communication techniques in a WAN, NAN, or HAN are utilized in the form of a **Wireless Sensor Network (WSN)** or **Wireless Mesh Network (WMN)**. Wireless networks are widely used as the communication network for the distribution system, because the physical extent of the distribution system is relatively small, compared to a transmission system. **Internet-of-Energy (IoE)**

provides a comprehensive structure for the communication up-gradation and automation of the distributed electricity infrastructure. The communication capability requirements for automation, monitoring, and remote control of these components provide vulnerabilities for cyber intrusions.

2.3.1 Security Vulnerabilities in DED. Due to the limited processing capabilities of DEDs, the major challenges are from security vulnerabilities and resource constraints [22], as mentioned below:

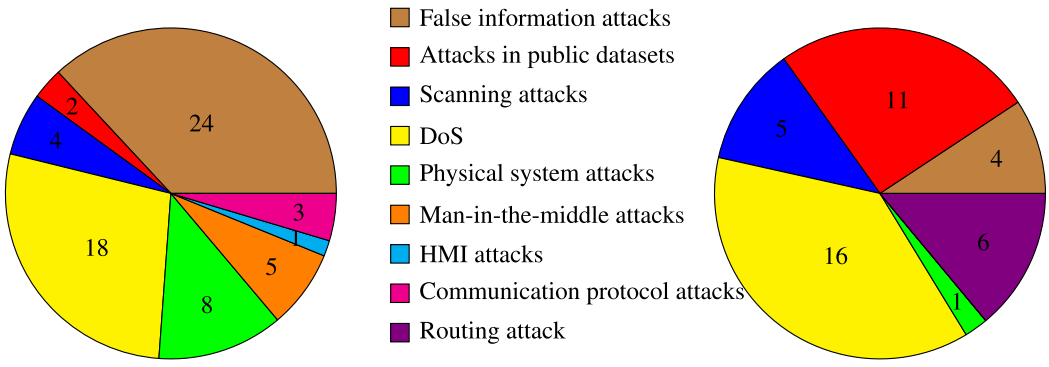
- Hierarchical network structures commonly used in WSNs or WMNs expose high vulnerabilities to routing failures in between various network topologies.
- The resource constraints (e.g., computational power, battery life) in wireless networks make the deployment of effective IDSs much more challenging.
- Some sensor nodes are often located remotely, exposing them to physical tampering.
- The resource constraints in wireless networks bring great challenges in meeting the system requirements in Quality-of-Service (e.g., data latency), reliability, and security (e.g., confidentiality, integrity, availability, authentication).

2.3.2 Cyberattacks in DED. Network attacks can be either active or passive. Active, unauthorized attackers break into a system with the intent of injecting or modifying the data stream. Passive attackers are more stealthy to collect information and plan to launch future attacks, such as phishing or tapping. Most attackers aim to steal information, as these distributed devices contain customer confidential information and have multiple vulnerable points due to their distributed nature. Apart from general network attacks such as DoS [15, 67, 76, 82, 83, 104, 117, 118] and MITM, three types of attacks are commonly observed in WSN: *Node capturing*, *jamming attacks*, and *routing attacks*. WSN consists of various sensor nodes distributed at a certain area where an attacker can launch the node-capturing attack to tamper software or hardware [90]. In wireless networks, a jamming attack is to disrupt wireless communications at the receiver side by sending random signals [118]. It is cheap for attackers to launch such attacks at wireless nodes due to the wireless medium with high accessibility [127]. A routing attack aims to mislead a routing path to a compromised node [28]. In Sybil attacks, a compromised node pretends to have multiple identities to other nodes, aiming to disrupt normal operations of a given system [58]. Other common routing attacks include sinkhole attacks [33, 42, 102] and wormhole attacks [103, 117, 118].

The frequency of different attack types used in the surveyed papers in the smart grid environment is summarized in Figure 4. The category name "Attacks in public datasets" refers to the attack scenarios already present in the public datasets (e.g., DARPA or KDD).

3 ML-BASED IDS TECHNIQUES FOR SMART GRID ENVIRONMENTS

We mainly discuss ML-based IDS for the smart grid based on the three categories: supervised, unsupervised, hybrid, and **Reinforcement Learning (RL)** in this survey [11]. Supervised ML methods train using labeled data in which an algorithm learns to obtain the given output when a certain input is provided by a feedback process for repeated corrections and error reduction process. It learns from the attributes present in the training dataset. However, as unlabeled data are used to train in unsupervised ML, the algorithm learns to discover the similarity or correlation between the input and the desired output. In this classification, hybrid learning is considered to improve the performance of multiple ML techniques integrated into a single framework, consisting of unsupervised learning, supervised learning, or a mix of both learning types. Further, RL, as a well-investigated learning algorithm in a real environment, does not have the training data to correct the answers. An RL agent learns the best action to maximize a reward through trial and error by adapting its action to a given environment. By assigning the rewards for the actions,



(a) Attacks frequency in WAMS and SAS (b) Attacks frequency in DED

Fig. 4. (a) Attack frequency in WAMS and SAS, and (b) Attack frequency in DED.

the agent will maximize the total accumulated reward during the process. To deal with a large state space (e.g., a state variable in power systems), the so-called **Deep Reinforcement Learning (DRL)** has been employed by combining **Deep Neural Network (DNN)** with RL [79].

We describe data generation and the general process of ML techniques to provide a basic background of ML techniques for easy understanding of our survey article as below.

3.1 Dataset Generation

The type of dataset and associated features are critical in determining the efficiency of ML-based approaches, as the learning phase depends on the volume and quality of the data. The datasets used for cybersecurity study purposes are mostly packet-level data, network flow data, or public datasets. The packet header attributes and the traffic features are described in detail in Reference [18]. Broadly, the datasets are classified into three types: public, published, and synthetic (i.e., user-defined) as follows:

- **Public datasets:** These are commonly used as the standard datasets that are frequently cited in many publications so the performance of the proposed ML techniques is compared against other counterparts that have been validated by the same dataset. Some of the widely used datasets [18], such as DARPA and KDD, are also utilized for the implementation of ML-based IDS in the smart grid. Those public datasets consist of network data with simulated attack cases, such as **User-to-Root (U2R), Remote-to-Local (R2L)**, or Probe and scan, which are common for underlying communication channel protocols but not relevant to the smart grid. Therefore, since those public datasets do not include new types of attack scenarios that are predominantly seen in smart grid environments, they cannot be representatives of attacks in the smart grid. However, there are existing public datasets specific to the SCADA environment, such as BATADAL [112], SWaT [43], and WADI [4]. These are world-class datasets that can allow experiments to ensure the security of critical infrastructure. Hence, those datasets can be used for intrusion detection in the context of the smart grid.
- **Published datasets:** We categorize the data from the existing related publications that used a certain network configuration and existing extracted features as *published datasets*. Keshk et al. [59] used a power system dataset generated from their simulation experiment in Reference [48] and used them to validate the performance of the considered IDS techniques. This simulated dataset reflects a realistic environment, such as system configurations describing

a simulated SCADA system, and provides a proper measure to weigh the reliability of the techniques for intrusion detection.

- **User-defined synthetic datasets:** This dataset is generated from a simulated testbed or software-based topology. As the real physical system data of a power system is not available due to its confidential nature, the realistic simulation environment is designed to provide realistic operational details of the CPS and validates the authenticity of the model of the ML-based IDS. Synthetic datasets are widely used to generate datasets for validating IDS techniques in the smart grid. Synthetic datasets can be categorized as follows:
  - **Testbed-based datasets:** This type of dataset is generated from CPS testbeds in which a virtual SCADA system is implemented with the simulated physical infrastructures. The CPS simulation testbed simulating both a power system and a computer network can be either a software-based simulation or hardware in the loop. To collect different kinds of attack data, the testbed provides the flexibility to simulate the attacks at any component of the system.
  - **Software-based datasets:** Datasets can be collected from the software-based network simulation. For an IDS for AMI, the simulation environment for WSN or WMN is critical for the evaluation. NS-3 or NS-2, as a discrete event network simulator, can efficiently build the model of a wireless network with scalability [42, 76]. The simulator can produce system conditions when the cyberattacks are launched or in normal conditions. Zhang et al. [133] opted to use the software MATLAB to simulate complex hybrid networks including WAN, NAN, or HAN. Most existing papers focused on detecting anomaly features of communication networks in the smart grid in which a proper network simulation should be able to collect the datasets and evaluate the proposed IDS. However, those network simulators cannot integrate the responses from the physical system and explore the interactions between the cyber system and the physical system, such as a power grid.

3.2 General Process of ML Techniques

ML-based IDS follows the below steps for its performance validation [11, 18]:

- **Datasets collection:** The protocols of different networks should be considered to collect the datasets in smart grid environments. For instance, to evaluate the performance of a SCADA IDS in Modbus protocol, the datasets generated from a simulator or testbed should contain the features of Modbus packets. In addition, simulation environments should satisfy the standard of Modbus [66]. To train and test a given model, the datasets include both anomaly data from various simulated attacks and the data traffic for normal operations.
- **Pre-processing:** With the collected data, the first step is to label the malicious or non-malicious data for supervised methods. According to the knowledge of the datasets, the labeling rules are predefined in terms of the signatures for attack or normal traffic. One major step for pre-processing is standardization, which is a critical step in data mining. This step is to scale the values of the features into the predefined range, such as a real number in $[0, 1]$, which can effectively improve the performance of the implemented ML-based IDS.
- **Feature extraction:** Feature extraction is a process to utilize the predefined values of features with the intent of grouping raw data based on the features. A dimensionality reduction technique is often used in the process, such as **Principal Component Analysis (PCA)** or **Independent Component Analysis (ICA)**, to derive principal features by reducing the random variables [46].
- **Training:** Before the training phase, data have to be split into training sets and testing sets. Then, the training data are fed into the model. Via cross-validation, the model is iteratively tuned until reaching the user-defined thresholds.

- **Testing:** After the best model parameters for each algorithm are determined after fitting and tuning, the testing sets are used to evaluate the performance of the chosen model. The testing data should be unseen during the training phase to avoid over-fitting.
- **Evaluation:** By using appropriate evaluation metrics, the models are evaluated to ensure the consistency, robustness, and accuracy of a given IDS technique.

Table 1 in the supplement document describes briefly different ML techniques used in the surveyed papers and their overall characteristics (pros and cons).

3.3 ML-based IDS for WAMS

3.3.1 Supervised Learning. Demertzis and Iliadis [27] use **Extreme Learning Machine (ELM)** with a Gaussian radial basis function kernel for the classification of cyberattacks in the SCADA system. As the dataset was generated from a simulated power system SCADA architecture, the learning algorithm was trained to identify line maintenance and short-circuit faults based on given scenarios with power system disturbances along with other cyberattacks. The Adaptive Elitist Differential Evolution optimization method was used for selecting optimal weights and biases of the ELMs along with 10-fold cross-validation. DNNs are sophisticated **Artificial Neural Networks (ANNs)** with more than two hidden layers and use complex mathematical modeling for data processing. Dogaru and Dumitrache [31] proposed DNN-based cyberattack detection using a simulated dataset generated from an IEEE 9-bus model for binary classification. This model effectively detects FDI attacks that alter the control center commands for the controlled process at a lower level (i.e., RTUs) related to the protection of transmission lines and associated devices. To classify Modbus/TCP and DNP3 cyberattacks, Siniosoglou et al. [105] proposed a novel **Autoencoder-Generative Adversarial Network (GAN)** architecture, called **anoMaly dEtection aNd claSsificAtion (MENSA)**. This method deployed DNNs considering the adversarial loss and the reconstruction difference. The authors evaluated the proposed IDS in four smart grid environments: labs, substations, hydropower, and power plants. In addition, **Deep Convolutional Neural Network (CNN**) as a special neural network is used as deep-learning-based locational detection architecture to obtain the exact locations of FDI attacks in a power system SCADA in real time [122]. da Silva et al. [25] examined One-class **Support Vector Machine (SVM)**-based IDS for anomaly and signature-based IDS in **software-defined networking (SDN)** SCADA. The algorithm is implemented on a simulated system consisting of a primary control center, multiple intermediary control centers, distribution substations, and numerous field devices. Other similar studies [56, 72, 89, 119] also proved a one-class SVM to be efficient with high accuracy rates. In References [85, 86], Common Path Mining is used to efficiently self-learn patterns for cyber intrusion detection from a pool of data containing a combination of synchrophasor measurement data and the audit logs of power system configuration. A stochastic ML-based **Hidden Markov Model (HMM)** is developed to detect anomalies in the SCADA network based on a Modbus dataset simulated with a normal scenario and six other attack vectors, such as DoS, command/code injection, and reconnaissance attacks [106]. By using reconstruction difference for the error minimization, Radoglou Grammatikis et al. [94] proposed a multivariate IDS with three ML-based detection layers to detect anomalies against network flows, Modbus/TCP packets, and operational data.

3.3.2 Unsupervised Learning. For the raw data derived from a smart grid, unsupervised learning is beneficial to discover unknown patterns in communication data and be the pre-processing for the following training process. Clustering is the most common unsupervised learning technique. There are multiple approaches for clustering the datasets into groups. The k-means is a kind of centroid-based clustering. To implement an IDS in the smart grid, k-means is used as a data mining tool for a large amount of power system or cyber system data. In Maglaras and Jiang [73], k-means

is utilized to cluster the alarms into groups with the outputs of the last classification. In addition, it was used to identify the node vulnerability level under FDI attack, which is helpful to distinguish different data sources in Xu et al. [126]. As the algorithm will be trapped in the local optimal with the k centroids that initially are selected at ransom, some methods are further refined in terms of the specific application domain. For example, **Particle Swarm Optimization (PSO)** is used to obtain the initial centroids [126]. The k-**Nearest Neighbors (**k-**NN)** groups the cases based on the similarity measures.

3.3.3 Ensemble Learning. Combining multiple ML methods to increase the detection accuracy and lower FAR in intrusion detection, hybrid learning is developed in which it used fuzzy logic-based IDS along with an online clustering algorithm to extract the fuzzy rules from the data stream [68]. Hu et al. [52] proposed a novel IDS based on adaptive feature boosting and ensemble learning to extract representative features from CPS data. The feature booster can improve the performance of attack classification in smart grid environments. They implemented a hardware-in-the-loop security testbed to evaluate the proposed method with a realistic dataset. Similarly, an integrated framework for IDS for smart grids is proposed with **Gradient Boosting Feature Selection (GBFS)** [114]. The most promising features are selected to reduce the complexity of the classifier, leading to a significant reduction in the execution time. Khoei et al. [60] examined three ensemble learning techniques, including bagging-based, boosting-based, and stacking-based, for their intrusion detection performance. The authors compared the other supervised learning techniques to show that the stacking-based ensemble learning outperformed the considered existing counterparts. However, their work only validated its performance under **Distributed Denial-of-Service (DDoS)** attacks. Instead of tuning the hyper-parameters to improve the performance, References [52, 60, 114] focused on selecting the most promising features that can successfully reduce the overhead and increase execution speed for SCADA-based smart grid communication.

3.3.4 RL. In the context of IDS in the smart grid, the actions taken by the RL agent are rewarded based on the performance of the power system [101]. The main goal of the RL is to maximize the total rewards of an agent's actions under a given environment in terms of an attacker's or defender's perspective. For example, the attacker aims to take its optimal action to introduce the most damage to a defense system in a given smart grid environment [30, 64]. The defender aims to maximize intrusion detection accuracy in the smart grid [30].

3.3.5 Comparison of the Different Learning Processes for WAMS. One of the primary concerns of WAMS is ensuring data integrity. Hence, along with usual IT network attacks, it is observed that most of the existing approaches consider FDI attacks as targeted intrusions to detect. Different ML-based learning is preferred based on available resources and an acceptable time scale for attack detection. For example, supervised methods detect anomalies in SCADA network data or power system measurements, providing better classification accuracy and scalability. However, as the bulk power grid has large datasets, testing times and hence detection time can be possibly higher. Unsupervised methods can detect unlabeled attack scenarios better and help pre-process or cluster the features/alarms. Hybrid learning combines the merits of supervised, unsupervised, and RL to improve model performance. However, detection architecture may be complicated, thus increasing the computation time with large-scale datasets. Using RL in IDS for smart grids is a relatively new exploration, as it partially eliminates the need for rigorous model training for better efficiency.

3.4 ML-based IDS for SAS

3.4.1 Supervised Learning. Choi et al. [24] implemented *Naïve Bayes* as a binary classifier to efficiently detect SYN flood attack and buffer overflow attack. In SAS, GOOSE communication in

the IEC 61850 standard is used as an additional feature in the usual TCP/IP model. The standard packet features are used for IDS learning. **Neural network (NN)**, which is set to learn supervised, is used to detect the attacks such as DoS and MITM attacks in the substation network domain in Kreimel et al. [63].

3.4.2 Unsupervised Learning. **Self-Organizing Map (SOM)** is trained using unsupervised learning to reduce the data dimension. Valdes et al. [116] used SOM to detect FDI attacks at IEEE 61850-based substations in the smart grid. In the inner loop, multiple patterns of the falsified data are determined. As the outer loop, SOM is used to modify the criteria and merge similar patterns into one class. In Reference [131], the packets collected from an actual operating IEC 61850 substation are used to implement the IDS based on the unsupervised method, **Expect Maximization (EM)**. As MMS or GOOSE packets are grouped into two, EM is applied to remove the outliers from those sets.

3.4.3 Comparison of the Different Learning Processes for SAS. The commonly perceived threat to SAS is the compromise of a communication network by exploiting protocol vulnerabilities. Supervised methods (e.g., Naïve Bayes and NNs) use communication protocol features along with the network behavior to improve intrusion detection accuracy. However, it is not effective for zero-day attacks. Similarly, unsupervised learning methods learn the SAS network data exchange behavior, provide dimensionality reduction, and cluster them to spot outliers.

3.5 ML-based IDS for DED

3.5.1 Supervised Learning. Li et al. [67] proposed an IDS for AMI of the smart grid using an **online sequence Extreme Learning Machine (OS-ELM)** in which a pre-conditioned gain ratio threshold is used for the feature selection to improve the accuracy and reduce computational complexity with dimensionality reduction. Under the variations in several hidden nodes or network topology, a tradeoff is observed between testing speed and accuracy. As an improvement over the OS-ELM technique [67], Zhang et al. [132] developed a **genetic algorithm (GA)**-ELM based-IDS where the input bias and weights are optimized using the GA. This method improved the accuracy of intrusion detection compared to ELM and OS-ELM. However, the work mainly detected network attacks on AMI using the KDD99 dataset and did not consider other common types of attacks in different smart grid environments. Vijayanand et al. [117] came up with an SVM-based IDS to detect attack signatures and used a public dataset, i.e., ADFA-LD for multi-class classification. Multiple SVM classifiers are used and trained with kernel functions, including Gaussian, **Multilayer Perceptron (MLP)**, and polynomial with a holdout cross-validation method and comparative performance analysis of the proposed methods with an ANN technique and other existing ML methods is done. This work emphasized the importance of feature selection in terms of accuracy as a result of dimensionality reduction. However, it did not achieve optimal detection, as the detection accuracy is low under different attack types.

Vijayanand et al. [118] developed a multi-SVM with a GA-based feature selection method to improve the quality of an IDS for WMNs. This work used NS-3 simulated network for packet generation and GA for feature selection, leveraging an adaptive heuristic global search method. They analyzed the computational complexity and communication overhead of the proposed ML method and reported the outperformance of their method in detection accuracy under all the considered attack types. Sedjelmaci and Senouci [100] proposed an IDS in a distributed arrangement at the smart meter level along with a centralized IDS at the collector level with simulated DoS and FDI attacks. The algorithm incorporates a rule-based IDS with an SVM-based learning mechanism on the KDD99 dataset. The authors analyzed the performance of their method in terms of energy consumption and detection accuracy at a customer level, smart meter level, and collector level. The

results showed that hybrid detection accuracy is observed at above 90% at all levels; however, the use of a public dataset does not have extended features.

Garofalo et al. [42] used **Decision Tree (DT)** to develop an IDS in WSNs for both signature-based and anomaly-based intrusions. They used the NS-3 simulator to simulate sinkhole attacks where the **AODV (Ad hoc On-demand Distance Vector)** routing protocol is attacked under a network configuration with a hierarchical structure consisting of the central control agent and local field agents. The authors showed the performance of the proposed DT-based IDS with a high detection rate, low energy consumption, and efficient implementation in WSN. However, they did not conduct a performance comparative analysis to prove the credibility of the proposed DT-based IDS against the existing ML-based counterparts. Korba et al. [61] developed an anomaly-based framework in an AMI environment using different methods, such as DT, Random Forest, ANN, and SVM, to detect power overloading cyberattacks in which the intruder compromises HAN or NAN to create a peak energy demand and causes a blackout to damage the grid infrastructure.

Lu and Tian [71] developed an IDS in the AMI based on the feedback loop of the **Long Short-Term Memory (LSTM)** model and a **Recurrent NN (RNN)**. The authors utilized the stacked encoder NN method for feature dimensionality reduction in the AMI communication information data. Similarly, to detect DoS attacks in the Electric **Vehicle Charging Station (EVCS)**, Basnet and Ali [13] developed DNN and LSTM algorithms to classify DoS attacks. Considering the potential vulnerabilities of EV communication, such as wireless communication links between vehicle to EVCS, **Vehicle to Grid (V2G)**, or **Vehicle-to-Vehicle (V2V)**, more attack scenarios and features should be considered for the IDS [13, 62]. Yao et al. [130] used a cross-layer fusion of CNN and LSTM to consider regional, global, and periodic features to detect abnormality in the metering information data. This work only used a standard dataset for testing, including known network attacks or synthetic attack behaviors. References [71, 130] used the LSTM model and an NN for improved intrusion detection in the AMI. The proposed approaches, however, were not validated on a real AMI communication dataset for the effectiveness of capturing both network and spatio-temporal abnormal features of electricity metering information.

Wang et al. [121] proposed a CNN-based intrusion detection mechanism to capture temporal and local features of the AMI communication network as aggregated features for efficiently detecting network intrusions. The authors considered the CNN-based IDS using the **Gated Recurrent Unit (GRU)** to reduce the model parameters and increase the convergence speed. However, it is debatable if the proposed approach can perform real-time detection to ensure AMI network security.

Durairaj et al. [32] proposed a DL-based method, **Deep Belief Network (DBN)**, alternatively a class of DNN, for microgrid communications. However, since the technique is only validated by attack data heuristically generated to consider two attack types, it is uncertain if the method can detect other attack types.

Routing Protocol for Low-Power and Lossy Networks (RPL) commonly makes the AMI vulnerable to routing attacks. Savitha and Basarkod [98] proposed a random forest-based IDS to increase the security and reliability of routing operations in AMI. In the online classification phase, the authors used an ML algorithm (i.e., Random Forest) to classify offline attacks as input for secure rank estimation. Along with ML performance metrics, the authors validated the efficiency of the proposed method through routing metrics, such as average delay, throughput, and packet delivery ratio. However, the efficiency of the ML-based approach, compared to that of RPL, was not significant.

Sun et al. [110] proposed a two-stage IDS for AMI. To improve SVM-based intrusion detection, they used the **Temporal Failure Propagation Graph (TFPG)** technique to generate attack routes. This work identified the smart meter under attack by calculating the similarity between a detected abnormal event and pre-defined cyber attacks, using the dataset generated by NS-3 based

AMI test platform. However, this work only validated the performance of their approach under limited cyberattack scenarios.

3.5.2 Unsupervised Learning. As DED's increased penetration in the distribution network creates vulnerabilities, there should be a bridge to fill the gap caused by a lack of studies using unsupervised learning-based IDS techniques in AMI environments and the communication infrastructure in the form of WMS or WSN. Raciti and Nadjm-Tehrani [93] developed the embedded anomaly detection for the trusted meter prototype using *k-means clustering* to determine if any energy consumption measurement is normal or not. To detect FDI attacks in AMI environments, Anwar et al. [10] utilized *k*-means to identify the vulnerable node clusters. The authors combined *k*-means clustering and outlier detection for the anomaly detection of smart meter data traffic in a HAN [75]. If normal data are used as training data, then the anomaly in smart meter data traffic is identified when objects do not fall into any of the clusters. Parvez et al. [88] proposed a strategy for securing an AMI with *k-NN clustering* technique to classify the authenticated neighbor meters. The *k*-NN is sensitive to the irrelevant features of the data and cannot deal with the complex dataset of the infrastructures with limited computational capability like a smart grid. Eik Loo et al. [33] proposed an IDS for WSNs by using fixed-width clustering. Multiple routing attacks are simulated where the routing features of the particular routing protocol are used as the learning features. However, the authors did not analyze the difference in the proposed IDS for the base station.

Xia et al. [125] developed a **Federated learning (FL)**-based attention DBN framework to detect network intrusion attacks in the communication network between components of smart meters and data concentrators in real-time. They also ensured the privacy protection of AMI by reducing FL time overhead through the proposed client selection algorithm. However, the assumptions about inference parameter attacks are vulnerable to smart attackers, resulting in faulty attack classification.

3.5.3 Ensemble Learning. As various networks with different standards are integrated into a CPS, it is effective to utilize hybrid approaches to ensure cybersecurity for the complex CPS. Therefore, hybrid learning incorporating multiple learning algorithms will effectively boost the performance of the IDS in different scenarios with some extra complexity introduced. Zhang et al. [134] proposed hybrid learning methods with SVM and **Artificial Immune System (AIS)** for distributed IDSs to detect the potential cyberattacks in HANs, NANs, and WANs. Although the hybrid approach improved detection accuracy, it introduced a significant, unacceptable computational overhead in most wireless environments. Otoum et al. [82] proposed the **Adaptively Supervised and Clustered Hybrid IDS (ASCH-IDS)** for WSNs using clustered sensors. The signature-based IDS uses the Random Forest procedure, while the anomaly-based IDS utilizes the density-based spatial clustering to detect zero-day attacks along with other network attacks. Rose et al. [95] tested a hybrid algorithm with *k*-means clustering to limit the training data size from the KDD99 dataset and SVM to detect anomalies with improved time complexity in real-time IoE environment. The proposed approach performed almost perfect detection accuracy along with improved training and testing times. Aloqaily et al. [6] proposed a three-phase hybrid learning IDS to ensure the security of smart connected vehicle cloud environments in which DBN and ID3-based DT are used for data dimensionality reduction and attack classification, respectively. The model is trained and tested using the NS-3 network traffic data and NSL-KDD dataset to detect inherent attacks present in KDD. Faisal et al. [37] implemented an ensemble learning method (Bagging) using the KDD99 dataset for an IDS at AMIs to enhance the security and reliability of the AMI smart grid network based on testing for 38 attack scenarios. Although the algorithm is adaptable, scalable, and supports legacy protocols and hardware, it was not validated under real-time environments. El Mrabet et al. [34] proposed a **deep learning (DL)**-based IDS for anomaly detection in a HAN and NAN

network of the AMI infrastructure through a two-step defense. This model is trained using the NSL-KDD dataset, and its accuracy is compared against other ML counterparts, including SVM, Random Forest, and Naïve Bayes.

Na et al. [80] developed a hybrid model to detect FDI attacks in an AMI system. They used CNN for feature extraction and network dimensionality reduction as input to the **weighted Random Forest classifier (WRFC)**. To improve detection accuracy and avoid overfitting problems, the authors considered a probabilistic approach for the WRFC. The authors mainly considered the efficiency of the proposed method. However, they did not consider the computational overhead and detection time, critical in real-time detection in the AMI system, which is the limited processing capability.

3.5.4 RL. In RL, an RL agent aims to maximize the rewards introduced by its chosen action. Otoum et al. [83] proposed a hybrid IDS for WSNs by employing RL, such as Q-learning for model-free learning, as the analytic engine of the IDS. The authors demonstrated the performance of RL-based IDS in terms of accuracy rate, detection rate, and FNR.

3.5.5 Comparison of the Different Learning Processes for DED. As the distributed devices require constant monitoring and remote access, they highly rely on effective communication for data exchange. Due to geographically distributed DEDs, communication networks are not always air-gapped and thus have many vulnerable access points. IT/ cyber networks in the CPS of the smart grid are primarily exposed to common network attacks. Hence, most reviewed papers use the KDD99 dataset, which includes frequently observed network attacks such as DoS, U2R, and R2L. Since most existing approaches use the KDD datasets to validate their intrusion detection accurately, they do not guarantee robustness under other attacks, such as zero-day attacks or other power system-specific attacks. In the smart grid, intrusion detection algorithms need to consider both data features and system features (e.g., physical system measurement data and system response) and learn the inter-dependency of network behaviors for efficient detection. Due to the highly invariable nature of AMI network data, supervised and unsupervised learning are widely adopted to lower the repeated learning overhead under resource-constrained, distributed smart meters. In addition, many approaches commonly leverage hybrid learning by combining different learning methods for effective dimensionality reduction and a faster detection mechanism.

To compare the differences between similar studies, a comparison table has been added in the supplement document (Table 3 of the supplement document) to highlight the merits and demerits of different learning methods in smart grid systems such as WAMS, SAS, and DED. Additionally, all the surveyed papers discussed above are summarized and characterized under different categories in Tables 4–10 of the supplement document.

4 EVALUATION OF ML-BASED IDS FOR A SMART GRID

4.1 Metrics

In this section, the metrics that are commonly used to measure the quality of existing ML-based IDS for smart grid environments are surveyed. It is commonly measured based on **False-Positive Rate (FPR), True Positive Rate (TPR)**, and detection accuracy. The common metrics are used for detecting both binaries (i.e., attack or normal) and multi-class (i.e., more than two classes such as different attack class types or normal) classification, as described in Figure 5(a). A general description of different metrics for IDS is described in Reference [18]. Here, the metrics have been categorized in terms of measuring the effectiveness and efficiency of ML-based IDS techniques used for smart grid environments.

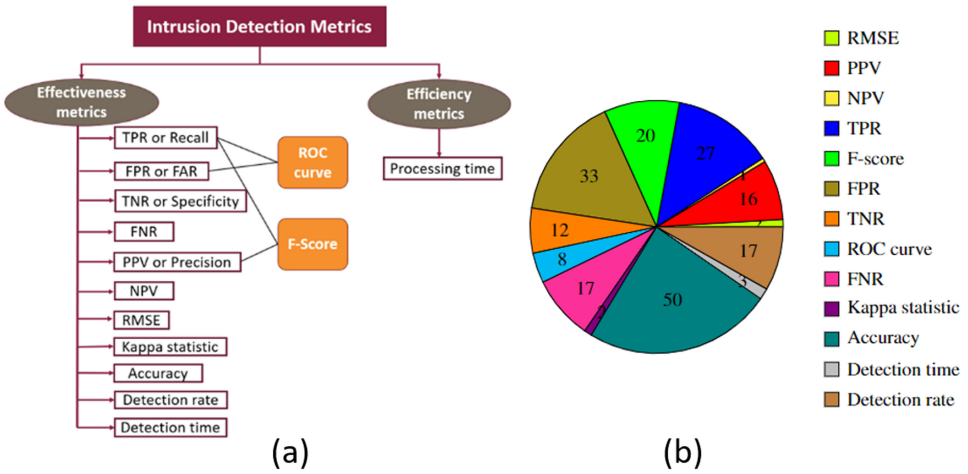


Fig. 5. Metrics of measuring the quality of ML-based IDS techniques in the smart grid: (a) Classification tree of IDS metrics; and (b) Effectiveness metrics trends.

We summarized the common metrics used to measure the quality of ML-based IDS in the smart grid in Table 2. In addition, we summarized the frequency of those metrics in Figure 5(b) to show the overall trends of existing metrics used in ML-based IDS techniques for the smart grid based on the surveyed papers in this work. Since only three papers used the processing time consisting of testing and training time, the frequency figure for the efficiency metrics is omitted.

The overall trends obtained from this survey on the metrics are as follows: First, there has been a substantial lack of efficiency metrics. In addition, no metrics are developed to capture the adverse impact (in the form of a power outage or loss) introduced to services to be provided in the smart grid environments. Hence, there is a clear need for objective indicators measuring the service quality in the smart grid in transmission and distribution networks, introduced by the ML-based IDS techniques.

4.2 Complexity Analysis of ML-based IDS in the Smart Grid

A smart grid environment has limited memory and computational power while needing real-time monitoring. An online approach with low time complexity and reliable performance is required to provide an efficient, optimal solution. A testing phase is usually fast with a smaller segment of data and follows a linear computational time, compared to the training dataset. Most of the ML methods can be tested online. However, an ML's time complexity is critical in reducing its training duration. In general, ML methods with linear time complexity $O(n)$ can be easily implemented online. The ML methods with $O(n^2)$ are acceptable while the methods with $O(n^3)$ or higher are used offline due to their high complexity. Table 3 summarizes the time complexity of various ML methods used to develop IDS techniques for the smart grid.

Unsupervised methods often require linear computational time. The k-means has $O(jmni)$ and k-NN has $O(n \log r)$ in their complexity, which allows them to be applicable to online applications. For incremental capability, clustering methods can be updated efficiently. In supervised learning methods, different ML methods based on their level of design complexity and the size of the dataset show different time complexity. An ANN can be linear with $O(emkn)$ or higher based on the number of neurons and the number of epochs present in the ANN network with lower streaming capability. Naïve Bayes and Bayesian networks have high streaming capability, as they

Table 2. Metrics to Measure the Quality of ML-based IDS for the Smart Grid

Metric	Definition
TPR or Sensitivity or Recall [1, 25, 27, 32, 41, 42, 48, 50, 59, 61, 64, 71, 89, 95, 95, 97–99, 105, 114, 118, 119, 121, 122, 125, 130, 132]	A measure of recall depicting the number of instances IDS correctly detects malicious activities over all the items present in the class
False positive rate (FPR) or False Alarm Rate (FAR) [6, 8, 25, 33, 37, 41, 42, 57, 59–61, 64, 67, 68, 71, 74, 80, 86, 89, 93, 95, 97, 99, 105, 114, 116–118, 121, 125, 130–132]	The ratio between the number of instances when IDS detects a normal activity as malicious over the whole set of instances
True negative rate (TNR) or Specificity [25, 41, 42, 61, 71, 89, 95, 98, 118, 121, 130, 132]	The ratio between correct negative classification (i.e., not P) and the whole set of data of class not P in multi-class classification
False Negative Rate (FNR) [6, 25, 37, 41, 42, 61, 67, 68, 71, 83, 89, 95, 117, 118, 121, 130, 132]	The ratio between the number of instances IDS detects a malicious activity as normal behavior and the whole set of data
Positive Predictive Value (PPV) or Precision [1, 25, 27, 32, 48, 50, 64, 71, 98, 114, 118, 119, 121, 122, 125, 130]	The measure of the precision of the method realized by the ratio between predicted correct positive classification, P, and all the items predicted to be under class P
Negative predictive value (NPV) [25]	The ratio between predicted true negative classification, P, and all the items predicted to be under the class P
F-score [1, 27, 32, 36, 41, 48, 50, 52, 64, 71, 94, 95, 98, 105, 114, 119, 121, 122, 125, 130]	A weighted average scaled in [0, 1] of the precision and recall values as a measure of the method's accuracy
Receiver Operating Characteristics (ROC) curve [27, 31, 41, 47, 59, 61, 89, 122]	The tradeoff between the TPR and FPR in which sensitivity is on the y-axis and FAR is on the x-axis
Root Mean Square Error (RMSE) [27, 61]	Quantification of the standard deviation of the prediction errors from the observed values to give a measure of data concentration
Kappa statistic [37, 97]	A measure of the quality of the performance or accuracy of the classifier as compared to that of another classifier depending on random guesses according to the class frequency
Accuracy [1, 6, 8, 13, 25, 27, 30, 32, 34, 37, 42, 47, 48, 50–52, 57, 59–63, 67, 68, 71, 72, 74, 80, 82, 83, 85, 86, 94, 95, 97, 98, 105, 106, 110, 114, 116–119, 121, 125, 130–133]	The ratio between total correct positive and negative prediction and all the items in the whole dataset
Detection rate [6, 15, 24, 33, 59, 60, 80, 82, 83, 93, 95, 99, 104, 110, 126, 130, 132]	The probability of detection and is given by the TPR of the method in a multi-class classification task
Detection time [8, 86, 125]	A measure of how fast an intrusion is detected (i.e., the time interval between an attacker's system penetration and the IDS identifying the attacker) where longer detection time exposes high-security vulnerability
Processing time [37, 67, 68]	A measure of the time it takes to build the model, such as the training and testing times of the data

have a linear time complexity $O(mn)$. GA, HMM, SVM, and Random Forests have quadratic time complexity $O(n^2)$; thus, their streaming capability is typically medium. Some of the methods with the highest computational time (e.g., $O(n^3)$) use association rules and sequence mining with low streaming capability.

Through feature extraction and dimensionality reduction of large datasets, the training time is expected to be reduced. Hence, many ML-based IDS approaches use hybrid learning for better performance. The requirements for accurate detection and time complexity of training of the model are often considered based on weighted decisions based on the functional requirements of the system.

Table 3 summarizes the time complexity of various ML methods used to develop IDS techniques for the smart grid. It gives an idea about the suitability of the ML method in terms of its efficiency and implementation feasibility.

4.3 Evaluation Methodologies

In this section, we discuss evaluation methodologies used for validating the performance of ML-based IDS techniques for smart grid environments in terms of four kinds of evaluation methods: *analytical/statistical model-based, simulation-based, emulation-based, and real testbed-based.*

4.3.1 Statistical Model-based Evaluation. These models are widely used to evaluate the performance of a wide range of applications, in which the internal dynamics of the system are expressed

Table 3. Big-O Complexity Analysis of ML-based IDS Techniques for the Smart Grid

ML method	Complexity in Big-O	Notations
Supervised ML		
ANN [55]	$O(emnk)$	k: Number of neurons e: Number of epochs
SVM [19]	$O(n^2)$	
Naïve Bayes [124]	$O(mn)$	
Common Path Mining [3]	$\geq O(n^3)$	
Random Forests [124]	$O(Mmn \log n)$	M: Number of trees
HMM [40]	$O(nc^2)$	c: Number of categories
DT [92]	$O(mn^2)$	
Genetic Algorithm [81]	$O(glmn)$	g: Number of generations l: Population size
Ensemble Learning [38]	$O(n)$	
Unsupervised ML		
K-means Clustering [54]	$O(jmni)$	j: Number of clusters i: Iterations till threshold
K-NN Clustering [124]	$O(n \log r)$	r: Number of neighbors
Self-organizing Map [96]	$O(S^2)$	S: Sample size

Note: m refers to the number of attributes in each instance, and n is the number of instances where $n >> m$.

as mathematical models. The analytical models are commonly used to describe critical threats like FDI attacks targeting state estimation by manipulating the operator with the falsified system states. Xu et al. [126] used an analytical model to describe the attack models and predicted the false data after which the k-means clustering is implemented to identify the node vulnerability level. Similarly, Do Nascimento Alves et al. [30] used the raw data of the measurements to depict an image by the analytical model describing a physical system, then the CNN is applied as the image classification task. Esmalifalak et al. [36] used SVM to detect the stealthy false data and compared ML-based models with the statistical-based model (i.e., multivariate Gaussian distribution) to detect the anomalies based on the historical data. As inter-vehicle communication is vital in routing EVs around static charging stations, Kosmanos et al. [62] proposed an ML-based IDS with a new evaluation metric, **Position Verification using Relative Speed (PVRS)**, to detect spoofing attacks.

Pros and Cons: These models usually do not need the training to carry out the predictions and have been proven to have good overall accuracy. However, the mathematical models of the target system usually need to be simplified. Therefore, the performance of the models is often dramatically influenced by different assumptions made.

4.3.2 Simulation-based Evaluation. In regard to the physical system of a smart grid, power system simulators provide realistic system operation states that can either present the impact of cyber attacks or provide realistic power system measurements to generate datasets. For instance, Foroutan and Salmasi [41] used MATPOWER in MATLAB to establish the simulation of the IEEE 118 bus system providing the historical data for the pre-processing of the proposed learning approach. Some power system simulators, such as DIgSILENT [49], PSSE [115], or Simulink in MATLAB [109], have the capability to interface with network simulators. Most of the software has a proper **Application Program Interface (API)** for integrating other communication simulators.

Different discrete-time event network simulators, e.g., NS-2 or NS-3 [33, 42, 76, 117, 118], are used to generate the communication environment.

Pros and Cons: According to the scalability of different software, simulation-based evaluation can generate a proper simulation environment. Although open-source software helps, the accuracy of the performance is highly dependent upon the quality of the software. The simulation results may not be precise enough to evaluate real-time operations.

4.3.3 Emulation-based Evaluation. Emulation means one system imitating another system usually by combining software and hardware [12]. For host-based attacks, the emulated operating system (e.g., CPU or GPU) allows tracking of the behaviors of the attack process, and the corresponding IDS deployed in the emulated system provides realistic performance [29]. For instance, to investigate the vulnerabilities of an AMI [16], Raspberry Pi with an extension module can be emulated as a smart meter to measure the voltage and current, and a ZigBee module is used to complete the data transmitting. With this emulation framework, any possible attack scenarios can be implemented at the imitated communication structure of the AMI. The real PMU [26] device is included in the emulation to investigate the vulnerabilities of PMU measurements [48]. Some other actual data acquisition and actuator components, such as IED, the **Programmable Logic Controller (PLC)**, or RTU, are integrated with other system simulators to establish an emulation environment [115].

Pros and Cons: The emulation strategy is commonly used for investigating particular devices to provide the most accurate results. However, using the hardware may be costly, and it is difficult to establish an exhaustive emulation environment for systematic analysis of the bulk power system.

4.3.4 Real Testbed-based Evaluation. A real testbed for an IDS is an elaborate platform for rigorous, reliable testing of cybersecurity experiments. For any potential research or new module, a real testbed can prove the performance and provide realistic results. A typical CPS testbed should include software, hardware, and the key components of networking. As hardware-in-the-loop is now the focus of the testbed design, RTDS and OPAL-RT are the most favorable hardware platforms to model the power system, which is carried out with real-time discrete simulation [2, 45, 129].

Pros and Cons: For ML-based IDS, the comprehensive testbed provides the datasets of the communication system as well as the logs or records from physical systems [66, 74, 116]. Due to confidentiality issues, measurements (e.g., voltages, currents, and switching status) and ICT data (e.g., communication protocols, system logs, and security logs) from the power grids are not publicly available. A realistic testbed is a good alternative for the research of the interactions between physical and cyber systems of the smart grid. However, there are multiple software/hardware included in one testbed. To complete one CPS testbed for the study of cybersecurity, integrating multiple evaluation methods will be a time-consuming and expensive task.

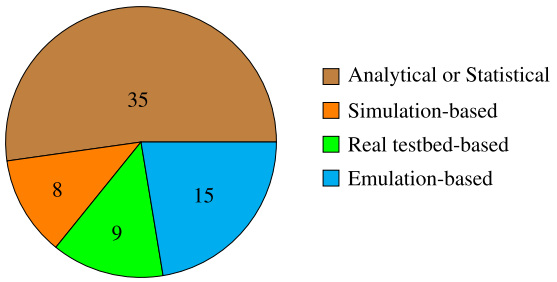


Fig. 6. Evaluation methodologies used for evaluating ML-based IDS for the smart grid.

Figure 6 summarizes the frequencies of different evaluation methods used in the surveyed papers. In terms of the nature of the CPS, the simulation, emulation, or testbed-based evaluation methods have more insights into the physical characteristics of a power system. The performance of

Table 4. Comparison of Evaluation Methodologies

Key Criteria	Scalability	Real-time application	Mobility	Visualization	Cost	Authenticity	Configurability
Statistical Model-based Evaluation	High	✘	✓	✘	Low	Low	✓
Simulation-based Evaluation	High	✘	✓	✓	Medium	Medium	✓
Emulation-based Evaluation	Medium	✘	✓	✓	Medium	Medium	✓
Real Testbed-based Evaluation	Low	✓	✘	✓	High	High	✓

ML-based IDS on power systems can be visualized by simulating the interaction of cyber and power systems. However, it is a significant investment in terms of time and cost as compared to analytical or statistical evaluation methods. The statistical analysis can be flexible to handle the different scales of the system and various types of experiments, which can be efficient for future research.

The key differences between the four primary evaluation methodologies are discussed in Table 4. As observed in Table 4, although a real testbed is ideal for considering realistic scenarios for the evaluation, it usually lacks scalability due to its high cost. Other characteristics of each methodology under various criteria have also been elaborated.

5 INSIGHTS & LIMITATIONS

From our extensive survey, we found the following **insights**:

- **High-performance classification and regression analysis with supervised methods:** Supervised methods follow a periodic trend in the data contents. Thus, it is easy to identify and detect intrusion in the system. The controllability and scalability are greatly improved with advanced hybrid classifiers with high accuracy rates. On the distribution side of the power grid, the buffer memory of the system can be reduced.
- **Efficient data pre-processing using unsupervised learning:** Unsupervised methods used in smart grid IDS utilize the consistency of the measurements or the physical features to classify the anomalous data and normal data. No need for data labeling from experts makes the set of clustering-based learning economical. Hence, it can be easily used as the pre-processing for other supervised learning. As discussed in Reference [116], the unsupervised methods are efficiently used as the pre-processing to reduce the dimensionality of the features.
- **Dynamic detection of malicious activities in a system:** Traditional IDS cannot handle the dynamic data flow by updating new attack signatures and high FAR. Furthermore, protocol-based attacks are difficult to detect in a smart grid. A network-based IDS is restricted only to network anomalies and creates delays in the process. However, a host-based IDS cannot guarantee the integrity of detection if any attack modifies the audit logs on which it depends. Hence, ML-based IDS can detect malicious activities with decreased FAR as it dynamically learns without repeated attack signature updates.
- **Flexibility of using the self-adaptive model for IDS updating:** ML approach involves the process of self-learning from data patterns. It can accordingly improve predictions based on the information-extensive form without human intervention and adapt actions depending on the learned behavior. Self-adaptive IDS models have a high potential for fast incremental learning to detect intrusion or anomalies in the smart grid.

- **High benefits in detecting zero-day attack:** A zero-day attack exploits a zero-day vulnerability in a network/system or unknown software vulnerabilities. It is highly challenging to detect zero-day attacks with existing signature-based IDS, because the attack signatures cannot be immediately configured in the blacklist dataset. In a smart grid where service availability is critical, the delayed service induced by the database updates for the IDS may introduce a harmful impact. In addition, in detecting novel attack behaviors, ML-based IDS techniques have shown high benefits [39]. It can be effective in predicting the results of malicious actions. The useful decision from ML is based on the exhaustive data of past interactions within the power system and cyber system. However, there has been a lack of studies to detect zero-day attacks in the smart grid, because most of the ML methods cannot fully detect unseen features during the training phase.
- **Efficiency-aware ML technique selection:** IDS are placed at different gateways in a smart grid for anomaly detection. Systems, such as the SCADA system running in real-time, need the IDS to be updated frequently to efficiently detect new attack signatures and other intrusions online. However, non-essential devices in the system, like metering, which do not need to exchange data in real-time, tend to use the IDS offline to lower the communication overhead and latency. Hence, the use of an ML technique should be determined based on its implementation mode, either online or offline. Many ML-based IDS use hybrid approaches to detect both anomaly attacks (e.g., zero-day attacks) and known attacks. ANNs and SVM, which learn the profiles or characteristics of normal activity and flag any deviation, end up with high FAR, as they tend to classify normal power system disturbances as anomalies. However, for the online setup, these tend to have a better detection accuracy due to their generalization capability and low complexity. With a small amount of training data, Random Forests perform better. With a large amount of data available for training and clustering, Naïve Bayes may take longer computation time. If one aims to capture attack signatures offline, then GA, DT, and fuzzy logic are more efficient. Therefore, ML technique selection highly depends on the type of intrusion and implementation mode (i.e., online or offline).

From our survey, we also summarize the **lessons learned** and discuss some **limitations** as follows:

- **Lack of uniformity in the topological study:** Various techniques address different characteristics of the smart grid, depending on topological variations. Thus, it is inherently difficult to compare the performance of these ML techniques and understand the implementation process [65].
- **Limited investigations on the threshold choice for clustering methods:** For clustering-based unsupervised approaches, choosing an appropriate threshold for the algorithms is challenging. It may have a significant impact on the outputs of the clustering. Research needs to clarify the process of selecting critical thresholds used in the used clustering method in the proposed IDS.
- **Lack of studies investigating outliers under different attack scenarios:** According to the performance of the clustering approaches, they have low FAR with a relatively low detection rate. The clustering centers may be dragged due to outliers. Since smart grid communications have become more complex and are threatened by more diverse cyber attacks, researchers need to consider the outliers under more diverse attack scenarios during the clustering process.
- **Lack of network data related to a smart grid environment:** The real power system data may not be available due to its confidential nature. User-defined datasets can be used for training and testing. However, they do not often cover all the possible attributes of the real

network data and may have a potential bias in data selection. The existing public datasets [69, 107], which lack some of the typical communication overheads for the data packets in the smart grid communication protocols, are not suitable for implementing an IDS in a smart grid. The public dataset, such as BATADAL [112], SWaT [43], and WADI [4], focus on a SCADA system in the power grid and cannot provide the specific features related to power system measurements and protocols or new smart devices (e.g., smart inverters, IEDs, and communication infrastructure).

- **Lack of CPS-related evaluation metrics:** Most existing approaches use standardized metrics for an ML algorithm. However, considering the unique characteristics of CPS in the smart grid, novel metrics should be developed to evaluate the impact of the IDS on both systems and their interaction under cyberattacks.
- **Need of a sufficient amount of proper datasets:** For the communication system in a smart grid, the testbed should be able to generate normal and attack data traffic over a long period. The simulators should be scalable to systematically evaluate the methods and extensible to test other attack types. Normal system disturbances, such as fault conditions or voltage fluctuations, can be flagged as an anomaly if an IDS fails to discriminate such behavior from attack signatures. Hence, a large number of datasets are required to maintain detection accuracy, as the quality of model training is directly influenced by the features trained. In addition, smart grid data generated by various testbeds are reused by many other researchers. This allows for easy comparison analysis of different ML methods. In general, the simulated or synthetic network data reflects a power system network topology to provide the efficiency of varying ML techniques for the IDS.
- **Need of relevant features characterizing the smart grid:** Public datasets were used to validate ML-based methods in the smart grid and have the features embedded in the data. However, the unique characteristics of the cyber system of the smart grid are not present in the dataset. To deploy the learning methods in the smart grid, we need to select the features based on: (1) The characteristics of different protocols, e.g., Modbus, DNP3, and IEC 61850, which are widely used in a SCADA system, or Zigbee in a wireless network; and (2) The specificity of the vulnerabilities of a wireless network or a SCADA system in the power system environment, such as routing protocols in WSN/WMN or the functional codes in the headers of DNP3 and Modbus, along with the dimensionality reduction to avoid over-fitting.
- **Challenges of fair performance comparison:** In our survey, we found that clustering is the most popular unsupervised learning technique, because smart grid datasets are usually unlabeled but contain multiple features. Similarly, SVM is the most popular supervised learning technique, as training is faster even with limited data (due to the confidential nature of smart grid data). Therefore, it is suitable for real-time SCADA data screening for intrusion detection. Bayesian network algorithm, inductive learning, and sequence pattern mining are some of the least-used ML methods in the smart grid due to their high time complexity. Although clustering and SVM have medium time complexity, they have been popularly employed, because computational time can be easily relaxed with a decent level of sacrifice for detection accuracy. Since labeled standard data are often unavailable, the existing studies modified supervised and unsupervised methods to reduce FAR and improve detection accuracy. Oftentimes, it is difficult to perform a fair comparison of multiple ML-based IDS techniques, because each algorithm has been validated under a different dataset. Due to this reason, it is challenging to make recommendations for the best ML method to detect anomalies, because the answer may depend on the implementation, datasets, system topology, and attack types, and detection accuracy under online real-time application and anomaly classification.

- **Requirements for self-adaptive models:** To smoothly run an interdependent smart grid, Alcaraz et al. [5] discussed the major four requirements, including (1) operational performance; (2) reliability and integrity in the control; (3) resilience; and (4) security and data privacy. As anomaly classification is required in real-time, low computational overhead, and comprehensibility can increase operational capabilities, such as faster SCADA controls. In addition, they improve the resiliency of the system and maintain stability during anomalies and other power system disturbances. The communication infrastructure requires security and confidentiality to avoid malicious perturbation in the system. The ML algorithm should be self-adaptive for detecting anomalies in the dynamic topology of the smart grid. Instead of the repeated learning phase, the IDS should be updated with newly detected attack features and reflect the grid topology to reduce redundant training, computation power, and cost.
- **Challenges in implementation:** From the numerical results of validating existing ML-based IDS techniques, the performance shows high accuracy according to the nature of ML techniques. However, the implementation of IDS in the smart grid is challenging due to the following reasons: (1) Any possible solution for an IDS in the smart grid has to be proposed based on the location of the IDS. That is, the IDS located at a different section of the smart grid has various accessibility to the data. For instance, the IDS in substations located at the process bus only has access to GOOSE or SV messages. Hence, the location of the IDS should be discussed specifically, which determines the accessible dataset for the ML techniques; and (2) Smart grid involves hundreds of infrastructures with different functional features. Some ML methods may offer a good accuracy rate in terms of anomaly awareness. However, the computational complexity may be a burden for some devices, such as smart meters or IEDs. Therefore, the implementation of the ML-based IDS would limit the range of options.

To more effectively deliver the key distinctions and relationships of the similar terms, we illustrate them in Table 2 in the supplement document.

6 CONCLUSIONS & FUTURE WORK DIRECTIONS

A smart grid environment is efficient only if the complete CPS works in synchronization. Any disturbance occurring on the cyber side has a physical impact on the power system, which causes various levels of damage, such as congestion in the transmission system, cascading failures, or major blackouts [20, 84]. Although an IDS is designed to detect any anomaly present in the system and accordingly alert the system operator for taking appropriate actions, the ML method should be able to evaluate the impact factor. As the power grid runs time-sensitive operations, fast anomaly detection can allow the system to take more proactive actions to minimize potential damage to be introduced to the system.

We suggest the following **future research directions** based on what we learned from this survey:

- **Developing various types of ML-based IDS:** Most of the existing ML-based IDSs for a smart grid are based on anomaly or signature-based detection methods. Enhanced versions of anomaly or signature-based or other directions of IDS using novel ML techniques are in need to meet the challenging goals of an IDS to be deployed in the smart grid with its unique vulnerability characteristics.
- **Developing efficiency or service availability metrics for a smart grid:** We need to develop specific intrusion detection metrics for impact analysis in the smart grid. This will give a proper measure of the performance of different ML methods specific to smart grid environments.

- **Extensive studies of IDS in the distribution network of a smart grid:** We rarely found existing works on ML-based IDS techniques for distribution networks of the smart grid, although WMN, AMI, and WSN have become an inherent part of the network and pose serious vulnerabilities threatening the system security. Although ML-based IDS techniques have been extensively explored in wireless networks, specific setup related to the distribution network of the smart grid consisting of DERs, AMIs, and data concentrators has been little explored.
- **Considering smart grid SCADA network design features:** A SCADA network has a similar structure with other applications, such as industrial, gas, and water networks, and might deal with similar communication packet datasets. However, a smart grid has specific data packet headers and protocols, so the research for customized smart grid networks should be focused on for proper realization of the base-level grid network and its impacts on its physical power network.
- **Designing detailed attack scenarios and models reflecting different vulnerabilities in a smart grid:** Based on the network vulnerabilities and an attacker's resources, the cost, and the intent of a damage level, the attack strategy may differ. The smart grid constitutes three levels of security requirements, which are at a physical level, communication infrastructure level, and information level [14]. The attacker model needs to be part of the study, as it plays an effective role in determining what ML method to implement depending on the reaction time and complexity along with necessary security considerations.
- **Accommodating dynamically changing system topology in the distribution grid:** Upon changing a distribution network, the topology of power distribution and associated data transfer network also changes. The reconfiguration process of the communication infrastructure should be flexible to accommodate variabilities with required security considerations. Accordingly, the IDS should be able to handle changing network topologies due to node joining or leaving due to failure. The limited computational and memory capabilities may cause new challenges when deploying the IDS in WSN, WMN, or AMI environments.
- **Developing lightweight, adaptive online ML-based IDS:** ML-based IDS consumes more time to train the model based on available features of data packets while requiring less time to detect anomalies in the system. However, in the smart grid, the normal operation depends on instantaneous action and fast control decisions. Thus, the IDS detecting discrepancy needs to be real-time with minimum communication latency to avoid any damage to the physical system. Hence, we should consider the requirements of data rates, reliability, and latency to employ online ML methods.
- **Improving zero-day attack classification:** A smart grid with its topological uniqueness makes the system vulnerable to different novel attacks. The learning method needs to be robust against those variations. To handle zero-day attacks exploiting unknown vulnerabilities, anomaly-based IDS should be designed computationally efficient to detect novel malicious activities.
- **Developing an efficient intrusion prevention system (IPS) to assist IDS in a smart grid:** An IDS only monitors traffic, detects and identifies anomalies, and alerts an operator to the attack. However, it does not have a proactive defense to thwart suspicious activities before the attacker intrudes into the system. The literature has discussed promising IPS techniques such as moving target defense [23] and defensive deception [137].
- **Enhancing an IDS's supporting capability for an integrated smart grid with a wireless distribution network and transmission SCADA network:** Any IDS design should be able to fully support functional requirements to sufficiently address the unique features of a smart grid. An efficient IDS can be with sensors in both the wireless distribution network

and transmission SCADA networks with separate analysis units. These units can provide input to an integrated module for correlating the distributed analyses.

REFERENCES

[1] Uttam Adhikari, Thomas Morris, and Shengyi Pan. 2016. WAMS cyber-physical test bed for power system, cybersecurity study, and data mining. *IEEE Trans. Smart Grid* 8, 6 (2016), 2744–2753.

[2] Hossein Ghassempour Aghamolki, Zhixin Miao, and Lingling Fan. 2015. A hardware-in-the-loop SCADA testbed. In *North American Power Symposium (NAPS)*. IEEE, 1–6.

[3] Rakesh Agrawal and Ramakrishnan Srikant. 1995. Mining sequential patterns. In *IEEE 11th International Conference on Data Engineering*. 3–14.

[4] Chuadhry Ahmed, Venkata Palleti, and Aditya Mathur. 2017. WADI: A water distribution testbed for research in the design of secure cyber physical systems. 25–28. DOI: https://doi.org/10.1145/3055366.3055375

[5] Cristina Alcaraz, Lorena Cazorla, and Gerardo Fernandez. 2014. Context-awareness using anomaly-based detectors for smart grid domains. In *International Conference on Risks and Security of Internet and Systems*. Springer, 17–34.

[6] Moayad Aloqaily, Safa Otoum, Ismaeel Al Ridhawi, and Yaser Jararweh. 2019. An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Netw.* 90 (2019), 101842.

[7] Raphael Amoah, Seyit Camtepe, and Ernest Foo. 2016. Securing DNP3 broadcast communications in SCADA systems. *IEEE Trans. Industr. Inform.* 12, 4 (2016), 1474–1485.

[8] Dou An, Qingyu Yang, Wenmao Liu, and Yang Zhang. 2019. Defending against data integrity attacks in smart grid: A deep reinforcement learning-based approach. *IEEE Access* 7 (2019), 110835–110845.

[9] Emilio Ancillotti, Raffaele Bruno, and Marco Conti. 2013. The role of communication systems in smart grids: Architectures, technical solutions and research challenges. *Comput. Commun.* 36, 17–18 (2013), 1665–1697.

[10] Adnan Anwar, Abdun Naser Mahmood, and Zahir Tari. 2015. Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid. *Inf. Syst.* 53 (2015), 201–212.

[11] Taiwo Oladipupo Ayodele. 2010. Types of machine learning algorithms. *New Adv. Mach. Learn.* 3 (2010), 19–48.

[12] Ruzena Bajcsy, Terry Benzel, Matt Bishop, B. Braden, C. Brodley, Sonia Fahmy, Sally Floyd, W. Hardaker, A. Joseph, George Kesidis, et al. 2004. Cyber defense technology networking and evaluation. *Commun. ACM* 47, 3 (2004), 58–61.

[13] Manoj Basnet and Mohd Hasan Ali. 2020. Deep learning-based intrusion detection system for electric vehicle charging station. In *2nd International Conference on Smart Power & Internet Energy Systems (SPIES)*. IEEE, 408–413.

[14] Omar Ali Beg, Taylor T. Johnson, and Ali Davoudi. 2017. Detection of false-data injection attacks in cyber-physical DC microgrids. *IEEE Trans. Industr. Inform.* 13, 5 (2017), 2693–2703.

[15] Robin Berthier and William H. Sanders. 2011. Specification-based intrusion detection for advanced metering infrastructures. In *IEEE 17th Pacific Rim International Symposium on Dependable Computing*. IEEE, 184–193.

[16] Altir Christian D. Bonganay, Josef C. Magno, Adrian G. Marcellana, John Marvin E. Morante, and Noel G. Perez. 2014. Automated electric meter reading and monitoring system using ZigBee-integrated Raspberry Pi single board computer via Modbus. In *IEEE Students' Conference on Electrical, Electronics and Computer Science*. IEEE, 1–6.

[17] Amol Borkar, Akshay Donode, and Anjali Kumari. 2017. A survey on intrusion detection system (IDS) and internal intrusion detection and protection system (IIDPS). In *IEEE International Conference on Inventive Computing and Informatics (ICICI)*. 949–953.

[18] Anna L. Buczak and Erhan Guven. 2015. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun. Surv. Tutor.* 18, 2 (2015), 1153–1176.

[19] Christopher J. C. Burges. 1998. A tutorial on support vector machines for pattern recognition. *Data Mining Knowl. Discov.* 2, 2 (1998), 121–167.

[20] Defense Use Case. 2016. Analysis of the cyber attack on the Ukrainian power grid. *Electric. Inf. Sharing Anal. Cent.* 388 (2016).

[21] Varun Chandola, Arindam Banerjee, and Vipin Kumar. 2009. Anomaly detection: A survey. *ACM Comput. Surv.* 41, 3 (2009), 1–58.

[22] Lipi Chhaya, Paawan Sharma, Govind Bhagwatikar, and Adesh Kumar. 2017. Wireless sensor network based smart grid communications: Cyber attacks, intrusion detection system and topology control. *Electronics* 6, 1 (2017), 5.

[23] Jin-Hee Cho, Dilli P. Sharma, Hooman Alavizadeh, Seunghyun Yoon, Noam Ben-Asher, Terrence J. Moore, Dong Seong Kim, Hyuk Lim, and Frederica F. Nelson. 2020. Toward proactive, adaptive defense: A survey on moving target defense. *IEEE Commun. Surv. Tutor.* 22, 1 (2020), 709–745. DOI: https://doi.org/10.1109/COMST.2019.2963791

[24] Kyung Choi, Xinyi Chen, Shi Li, Mihui Kim, Kijoon Chae, and JungChan Na. 2012. Intrusion detection of NSM based DoS attacks using data mining in smart grid. *Energies* 5, 10 (2012), 4091–4109.

[25] Eduardo Germano da Silva, Anderson Santos da Silva, Juliano Araujo Wickboldt, Paul Smith, Lisandro Zambenedetti Granville, and Alberto Schaeffer-Filho. 2016. A one-class NIDS for SDN-based SCADA systems. In *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*. IEEE, 303–312.

[26] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke. 2010. Synchronized phasor measurement applications in power systems. *IEEE Trans. Smart Grid* 1, 1 (2010), 20–27.
[27] Konstantinos Demertzis and Lazaros Iliadis. 2018. A computational intelligence system identifying cyber-attacks on smart energy grids. In *Modern Discrete Mathematics and Analysis*. Springer, 97–116.
[28] Hongmei Deng, Wei Li, and Dharma P. Agrawal. 2002. Routing security in wireless ad hoc networks. *IEEE Commun. Mag.* 40, 10 (2002), 70–75.
[29] Patricia Derler, Edward A. Lee, and Alberto Sangiovanni Vincentelli. 2011. Modeling cyber–physical systems. *Proc. IEEE* 100, 1 (2011), 13–28.
[30] Helton do Nascimento Alves, Newton G. Bretas, Arturo S. Bretas, and Ben-Hur Matthews. 2019. Smart grids false data injection identification: A deep learning approach. In *IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*. 1–5.
[31] Delia Ioana Dogaru and Ioan Dumitrache. 2019. Cyber security of smart grids in the context of big data and machine learning. In *22nd International Conference on Control Systems and Computer Science (CSCS)*. IEEE, 61–67.
[32] Danalakshmi Durairaj, Thiruppathy Kesavan Venkatasamy, Abolfazl Mehbodniya, Syed Umar, and Tanweer Alam. 2022. Intrusion detection and mitigation of attacks in microgrid using enhanced deep belief network. *Energy Sources, Part A: Recov. Utiliz. Environ. Ef.* 44 (2022), 1–23.
[33] Chong Eik Loo, Mun Yong Ng, Christopher Leckie, and Marimuthu Palaniswami. 2006. Intrusion detection for routing attacks in sensor networks. *Int. J. Distrib. Sensor Netw.* 2, 4 (2006), 313–332.
[34] Zakaria El Mrabet, Mehdi Ezzari, Hassan Elghazi, and Badr Abou El Majd. 2019. Deep learning-based intrusion detection system for advanced metering infrastructure. In *2nd International Conference on Networking, Information Systems & Security*. 1–7.
[35] Zakaria El Mrabet, Naima Kaabouch, Hassan El Ghazi, and Hamid El Ghazi. 2018. Cyber-security in smart grid: Survey and challenges. *Comput. Electric. Eng.* 67 (2018), 469–482.
[36] Mohammad Esmalifalak, Lanchao Liu, Nam Nguyen, Rong Zheng, and Zhu Han. 2014. Detecting stealthy false data injection using machine learning in smart grid. *IEEE Syst. J.* 11, 3 (2014), 1644–1652.
[37] Mustafa Amir Faisal, Zeyar Aung, John R. Williams, and Abel Sanchez. 2012. Securing advanced metering infrastructure using intrusion detection system with data stream mining. In *Pacific-Asia Workshop on Intelligence and Security Informatics*. Springer, 96–111.
[38] Elisabetta Fersini, Enza Messina, and Federico Alberto Pozzi. 2014. Sentiment analysis: Bayesian ensemble learning. *Decis. Supp. Syst.* 68 (2014), 26–38.
[39] Ivan Firdausi, Alva Erwin, Anto Satriyo Nugroho, et al. 2010. Analysis of machine learning techniques used in behavior-based malware detection. In *IEEE 2nd International Conference on Advances in Computing, Control, and Telecommunication Technologies*. 201–203.
[40] G. David Forney. 1973. The Viterbi algorithm. *Proc. IEEE* 61, 3 (1973), 268–278.
[41] S. Armina Foroutan and Farzad R. Salmasi. 2017. Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method. *IET Cyber-Phys. Syst.: Theor. Applic.* 2, 4 (2017), 161–171.
[42] Alessia Garofalo, Cesario Di Sarno, and Valerio Formicola. 2013. Enhancing intrusion detection in wireless sensor networks through decision trees. In *European Workshop on Dependable Computing*. Springer, 1–15.
[43] Jonathan Goh, Sridhar Adepu, Khurum Nazir Junejo, and Aditya Mathur. 2016. A dataset to support research in the design of secure water treatment systems. In *International Conference on Critical Information Infrastructures Security*. Springer, 88–99.
[44] Muhammed Zekeriya Gunduz and Resul Das. 2020. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* 169 (2020), 107094.
[45] Adam Hahn, Aditya Ashok, Siddharth Sridhar, and Manimaran Govindarasu. 2013. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Trans. Smart Grid* 4, 2 (2013), 847–855.
[46] Mark A. Hall and Lloyd A. Smith. 1999. Feature selection for machine learning: Comparing a correlation-based filter approach to the wrapper. In *FLAIRS Conference*. 235–239.
[47] Youbiao He, Gihan J. Mendis, and Jin Wei. 2017. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Trans. Smart Grid* 8, 5 (2017), 2505–2516.
[48] Raymond C. Borges Hink, Justin M. Beaver, Mark A. Buckner, Tommy Morris, Uttam Adhikari, and Shengyi Pan. 2014. Machine learning for power system disturbance and cyber-attack discrimination. In *7th International Symposium on Resilient Control Systems (ISRCS)*. IEEE, 1–8.
[49] Junho Hong, Chen-Ching Liu, and Manimaran Govindarasu. 2014. Integrated anomaly detection for cyber security of the substations. *IEEE Trans. Smart Grid* 5, 4 (2014), 1643–1653.
[50] Wei-Chih Hong, Ding-Ray Huang, Chih-Lung Chen, and Jung-San Lee. 2020. Towards accurate and efficient classification of power system contingencies and cyber-attacks using recurrent neural networks. *IEEE Access* 8 (2020), 123297–123309.

[51] Emmanuel Hooper. 2010. Strategic and intelligent smart grid systems engineering. In *International Conference for Internet Technology and Secured Transactions*. IEEE, 1–6.
[52] Chengming Hu, Jun Yan, and Xue Liu. 2020. Adaptive feature boosting of multi-sourced deep autoencoders for smart grid intrusion detection. In *IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 1–5.
[53] IEEE. 2010. IEEE standard for electric power systems communications—distributed network protocol (DNP3). *IEEE Std 1815-2010* (2010), 1–775.
[54] Anil K. Jain and Richard C. Dubes. 1988. *Algorithms for Clustering Data*. Prentice-Hall, Inc.
[55] Anil K. Jain, Jianchang Mao, and K. Moidin Mohiuddin. 1996. Artificial neural networks: A tutorial. *Computer* 29, 3 (1996), 31–44.
[56] Jianmin Jiang and Lasith Yasakethu. 2013. Anomaly detection via one class SVM for protection of SCADA systems. In *International Conference on Cyber-enabled Distributed Computing and Knowledge Discovery*. IEEE, 82–88.
[57] Paria Jokar, Nasim Arianpoo, and Victor C. M. Leung. 2013. Intrusion detection in advanced metering infrastructure based on consumption pattern. In *IEEE International Conference on Communications (ICC)*. IEEE, 4472–4476.
[58] Chris Karlof and David Wagner. 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Netw.* 1, 2–3 (2003), 293–315.
[59] Marwa Keshk, Nour Moustafa, Elena Sitnikova, and Gideon Creech. 2017. Privacy preservation intrusion detection technique for SCADA systems. In *IEEE Military Communications and Information Systems Conference (MilCIS)*. 1–6.
[60] Tala Talaei Khoei, Ghilas Aissou, When Chen Hu, and Naima Kaabouch. 2021. Ensemble learning methods for anomaly intrusion detection system in smart grid. In *IEEE International Conference on Electro Information Technology (EIT)*. IEEE, 129–135.
[61] Abdelaziz Amara Korba, Nouredine Tamani, Yacine Ghamri-Doudane, et al. 2020. Anomaly-based framework for detecting power overloading cyberattacks in smart grid AMI. *Comput. Secur.* 96 (2020), 101896.
[62] Dimitrios Kosmanos, Apostolos Pappas, Leandros Maglaras, Sotiris Moschoyiannis, Francisco J. Aparicio-Navarro, Antonios Argyriou, and Helge Janicke. 2020. A novel intrusion detection system against spoofing attacks in connected electric vehicles. *Array* 5 (2020), 100013.
[63] Philipp Kreimel, Oliver Eigner, Francesco Mercaldo, Antonella Santone, and Paul Tavolato. 2020. Anomaly detection in substation networks. *J. Inf. Secur. Applic.* 54 (2020), 102527.
[64] Mehmet Necip Kurt, Oyetunji Ogundijo, Chong Li, and Xiaodong Wang. 2018. Online cyber-attack detection in smart grid: A reinforcement learning approach. *IEEE Trans. Smart Grid* 10, 5 (2018), 5174–5185.
[65] Nishchal Kush, Ernest Foo, Ejaz Ahmed, Irfan Ahmed, and Andrew Clark. 2011. Gap analysis of intrusion detection in smart grids. In *Proceedings of 2nd International Cyber Resilience Conference*.
[66] Antoine Lemay and José M. Fernandez. 2016. Providing SCADA network data sets for intrusion detection research. In *9th Workshop on Cyber Security Experimentation and Test (CSET 16)*.
[67] Yuancheng Li, Rixuan Qiu, and Sitong Jing. 2018. Intrusion detection system using Online Sequence Extreme Learning Machine (OS-ELM) in advanced metering infrastructure of smart grid. *PloS One* 13, 2 (2018), e0192216.
[68] Ondrej Linda, Milos Manic, Todd Vollmer, and Jason Wright. 2011. Fuzzy logic based anomaly detection for embedded network security cyber sensor. In *IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*. IEEE, 202–209.
[69] Richard Lippmann, Joshua W. Haines, David J. Fried, Jonathan Korba, and Kumar Das. 2000. The 1999 DARPA off-line intrusion detection evaluation. *Comput. Netw.* 34, 4 (2000), 579–595.
[70] Chen-Ching Liu, Alexandru Stefanov, Junho Hong, and Patrick Panciatici. 2011. Intruders in the grid. *IEEE Power Energy Mag.* 10, 1 (2011), 58–66.
[71] Guanyu Lu and Xiuxia Tian. 2021. An efficient communication intrusion detection scheme in ami combining feature dimensionality reduction and improved LSTM. *Secur. Commun. Netw.* 2021 (2021).
[72] Leandros A. Maglaras and Jianmin Jiang. 2014. Intrusion detection in SCADA systems using machine learning techniques. In *Science and Information Conference*. IEEE, 626–631.
[73] Leandros A. Maglaras and Jianmin Jiang. 2014. OCSVM model combined with K-means recursive clustering for intrusion detection in SCADA systems. In *10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*. IEEE, 133–134.
[74] Leandros A. Maglaras, Jianmin Jiang, and Tiago J. Cruz. 2016. Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems. *J. Inf. Secur. Applic.* 30 (2016), 15–26.
[75] Divya M. Menon and N. Radhika. 2016. Anomaly detection in smart grid traffic data for home area network. In *International Conference on Circuit, Power and Computing Technologies (ICCPCT)*. IEEE, 1–4.
[76] Sudip Misra, P. Venkata Krishna, Kiran Isaac Abraham, Navin Sasikumar, and S. Fredun. 2010. An adaptive learning routing protocol for the prevention of distributed denial of service attacks in wireless mesh networks. *Comput. Math. Applic.* 60, 2 (2010), 294–306.

[77] Robert Mitchell and Ing-Ray Chen. 2014. A survey of intrusion detection techniques for cyber-physical systems. *ACM Comput. Surv.* 46, 4 (2014), 1–29.
[78] Robert Mitchell and Ray Chen. 2014. A survey of intrusion detection in wireless network applications. *Comput. Commun.* 42 (2014), 1–23.
[79] Volodymyr Mnih, Koray Kavukcuoglu, David Silver, Andrei A. Rusu, Joel Veness, Marc G. Bellemare, Alex Graves, Martin Riedmiller, Andreas K. Fidjeland, Georg Ostrovski, et al. 2015. Human-level control through deep reinforcement learning. *Nature* 518, 7540 (2015), 529–533.
[80] Li Na, Xue Xiaohui, Ma Xiaoqin, Meng Xiangfu, and Yuan Peisen. 2021. Fake data injection attack detection in AMI system using a hybrid method. In *IEEE Sustainable Power and Energy Conference (iSPEC)*. IEEE, 2371–2376.
[81] Pietro S. Oliveto, Jun He, and Xin Yao. 2007. Time complexity of evolutionary algorithms for combinatorial optimization: A decade of results. *Int. J. Autom. Comput.* 4, 3 (2007), 281–293.
[82] Safa Otoum, Burak Kantarci, and Hussein Mouftah. 2018. Adaptively supervised and intrusion-aware data aggregation for wireless sensor clusters in critical infrastructures. In *IEEE International Conference on Communications (ICC)*. IEEE, 1–6.
[83] Safa Otoum, Burak Kantarci, and Hussein Mouftah. 2019. Empowering reinforcement learning on big sensed data for intrusion detection. In *IEEE International Conference on Communications (ICC)*. IEEE, 1–7.
[84] Seemita Pal, Biplab Sikdar, and Joe H. Chow. 2017. Classification and detection of PMU data manipulation attacks using transmission line parameters. *IEEE Trans. Smart Grid* 9, 5 (2017), 5057–5066.
[85] Shengyi Pan, Thomas Morris, and Uttam Adhikari. 2015. Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data. *IEEE Trans. Industr. Inform.* 11, 3 (2015), 650–662.
[86] Shengyi Pan, Thomas Morris, and Uttam Adhikari. 2015. Developing a hybrid intrusion detection system using data mining for power systems. *IEEE Trans. Smart Grid* 6, 6 (2015), 3104–3113.
[87] Rajendra Kumar Pandey and Mohit Misra. 2016. Cyber security threats—Smart grid infrastructure. In *IEEE National Power Systems Conference (NPSC)*. 1–6.
[88] Imtiaz Parvez, Arif I. Sarwat, Longfei Wei, and Aditya Sundararajan. 2016. Securing metering infrastructure of smart grid: A machine learning and localization based key management approach. *Energies* 9, 9 (2016), 691.
[89] Ahmed Patel, Hitham Alhussian, Jens Myrup Pedersen, Bouchaib Bounabat, Joaquim Celestino Júnior, and Sokratis Katsikas. 2017. A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems. *Comput. Secur.* 64 (2017), 92–109.
[90] Al-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong. 2006. Security in wireless sensor networks: Issues and challenges. In *8th International Conference Advanced Communication Technology*. IEEE.
[91] Silvio E. Quincozes, Célio Albuquerque, Diego Passos, and Daniel Mossé. 2021. A survey on intrusion detection and prevention systems in digital substations. *Comput. Netw.* 184 (2021), 107679.
[92] J. R. Quinlan. 1993. *The Morgan Kaufmann Series in Machine Learning*. Elsevier.
[93] Massimiliano Raciti and Simin Nadjm-Tehrani. 2013. Embedded cyber-physical anomaly detection in smart meters. In *Critical Information Infrastructures Security*. Springer, 34–45.
[94] Panagiotis Radoglou Grammatikis, Panagiotis Sarigiannidis, Georgios Efstathopoulos, and Emmanouil Panaousis. 2020. ARIES: A novel multivariate intrusion detection system for smart grid. *Sensors* 20, 18 (2020), 5305.
[95] Thomas Rose, Kashif Kifayat, Sohail Abbas, and Muhammad Asim. 2020. A hybrid anomaly-based intrusion detection system to improve time complexity in the Internet of Energy environment. *J. Parallel Distrib. Comput.* 145 (2020), 124–139.
[96] Dmitri G. Roussinov and Hsinchun Chen. 1998. A scalable self-organizing map algorithm for textual classification: A neural network approach to thesaurus generation. *Cc-Ai, the Journal for the Integrated Study of Artificial Intelligence, Cognitive Science and Applied Epistemology* 15, 1 (1998), 81–111.
[97] Rishabh Samdarshi, Nidul Sinha, and Paritosh Tripathi. 2015. A triple layer intrusion detection system for SCADA security of electric utility. In *Annual IEEE India Conference (INDICON)*. IEEE, 1–5.
[98] M. M. Savitha and P. I. Basarkod. 2022. Random forest based intrusion detection system for AMI. In *IEEE 4th International Conference on Advances in Electronics, Computers and Communications (ICAECC)*. IEEE, 1–7.
[99] Naoum Sayegh, Imad H. Elhajj, Ayman Kayssi, and Ali Chehab. 2014. SCADA intrusion detection system based on temporal behavior of frequent patterns. In *17th IEEE Mediterranean Electrotechnical Conference*. IEEE, 432–438.
[100] Hichem Sedjelmaci and Sidi Mohammed Senouci. 2016. Smart grid security: A new approach to detect intruders in a smart grid neighborhood area network. In *International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE, 6–11.
[101] Arturo Servin. 2007. Towards traffic anomaly detection via reinforcement learning and data flow. Department of Computer Science, University of York.
[102] Hosein Shafiei, Ahmad Khonsari, H. Derakhshi, and Payam Mousavi. 2014. Detection and mitigation of sinkhole attacks in wireless sensor networks. *J. Comput. Syst. Sci.* 80, 3 (2014), 644–653.

[103] Kalpana Sharma, M. K. Ghose, et al. 2010. Wireless sensor networks: An overview on its security threats. *IJCA, Special Iss. "Mobile Ad-hoc Networks" MANETs* 1495 (2010), 42–45.

[104] Sooyeon Shin, Taekyoung Kwon, Gil-Yong Jo, Youngman Park, and Haekyu Rhy. 2010. An experimental study of hierarchical intrusion detection for wireless industrial sensor networks. *IEEE Trans. Industr. Inform.* 6, 4 (2010), 744–757.

[105] Ilias Siniosoglou, Panagiotis Radoglou-Grammatikis, Georgios Efstathopoulos, Panagiotis Fouliras, and Panagiotis Sarigiannidis. 2021. A unified deep learning anomaly detection and classification approach for smart grid environments. *IEEE Trans. Netw. Serv. Manag.* 18, 2 (2021), 1137–1151.

[106] Kyriakos Stefanidis and Artemios G. Voyiatzis. 2016. An HMM-based anomaly detection approach for SCADA systems. In *IFIP International Conference on Information Security Theory and Practice*. Springer, 85–99.

[107] S. J. Stolfo et al. 1999. KDD cup 1999 dataset. *UCI KDD Repository*. Retrieved from http://kdd.ics.uci.edu.

[108] Maximilian Strobel, Norbert Wiedermann, and Claudia Eckert. 2016. Novel weaknesses in IEC 62351 protected smart grid control systems. In *IEEE International Conference on Smart Grid Communications (SmartGridComm)*. 266–270.

[109] Wencong Su, Wente Zeng, and Mo-Yuen Chow. 2012. A digital testbed for a PHEV/PEV enabled parking lot in a smart grid environment. In *IEEE PES Innovative Smart Grid Technologies (ISGT)*. IEEE, 1–7.

[110] Chih-Che Sun, D. Jonathan Sebastian Cardenas, Adam Hahn, and Chen-Ching Liu. 2020. Intrusion detection for cybersecurity of smart meters. *IEEE Trans. Smart Grid* 12, 1 (2020), 612–622.

[111] Andy Swales et al. 1999. Open modbus/tcp specification. *Schneider Electric* 29 (1999).

[112] Riccardo Taormina, Stefano Galelli, Nils Ole Tippenhauer, Elad Salomons, Avi Ostfeld, Demetrios G. Eliades, Mohsen Aghashahi, Raanju Sundararajan, Mohsen Pourahmadi, M. Katherine Banks, et al. 2018. Battle of the attack detection algorithms: Disclosing cyber attacks on water distribution networks. *J. Water Resour. Plan. Manag.* 144, 8 (2018), 04018048.

[113] Weiming Tong, Lei Lu, Zhongwei Li, Jingbo Lin, and Xianji Jin. 2016. A survey on intrusion detection system for advanced metering infrastructure. In *6th International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)*. IEEE, 33–37.

[114] Darshana Upadhyay, Jaume Manero, Marzia Zaman, and Srinivas Sampalli. 2020. Gradient boosting feature selection with machine learning classifiers for intrusion detection on power grids. *IEEE Trans. Netw. Serv. Manag.* 18, 1 (2020), 1104–1116.

[115] Alfredo Vaccaro, Marjan Popov, Domenico Villacci, and Vladimir Terzija. 2010. An integrated framework for smart microgrids modeling, monitoring, control, communication, and verification. *Proc. IEEE* 99, 1 (2010), 119–132.

[116] Alfonso Valdes, Richard Macwan, and Matthew Backes. 2016. Anomaly detection in electrical substation circuits via unsupervised machine learning. In *IEEE 17th International Conference on Information Reuse and Integration (IRI)*. IEEE, 500–505.

[117] R. Vijayanand, D. Devaraj, and B. Kannapiran. 2017. Support vector machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid. In *4th International Conference on Advanced Computing and Communication Systems (ICACCS)*. IEEE, 1–7.

[118] R. Vijayanand, D. Devaraj, and B. Kannapiran. 2018. Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection. *Comput. Secur.* 77 (2018), 304–314.

[119] Defu Wang, Xiaojuan Wang, Yong Zhang, and Lei Jin. 2019. Detection of power grid disturbances and cyber-attacks based on machine learning. *J. Inf. Secur. Applic.* 46 (2019), 42–52.

[120] Huaizhi Wang, Jiaqi Ruan, Guibin Wang, Bin Zhou, Yitao Liu, Xueqian Fu, and Jianchun Peng. 2018. Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks. *IEEE Trans. Industr. Inform.* 14, 11 (2018), 4766–4778.

[121] Ning Wang, Zhihui Liu, Ruizhe Yao, and Li Zhang. 2022. Construction and analysis of cross-layer aggregation neural network for AMI intrusion detection. In *4th Asia Energy and Electrical Engineering Symposium (AEEES)*. IEEE, 148–153.

[122] Shuoyao Wang, Suzhi Bi, and Ying-Jun Angela Zhang. 2020. Locational detection of the false data injection attack in a smart grid: A multilabel classification approach. *IEEE Internet Things J.* 7, 9 (2020), 8218–8227.

[123] Yong Wang, Zhaoyan Xu, Jialong Zhang, Lei Xu, Haopei Wang, and Guofei Gu. 2014. SRID: State relation based intrusion detection for false data injection attacks in SCADA. In *European Symposium on Research in Computer Security*. Springer, 401–418.

[124] Ian H. Witten, Eibe Frank, and Mark A. Hall. 2005. *Practical Machine Learning Tools and Techniques*. Morgan Kaufmann.

[125] Zhuoqun Xia, Yaling Chen, Bo Yin, Haolan Liang, Hongmei Zhou, Ke Gu, and Fei Yu. 2022. Fed_ADBN: An efficient intrusion detection framework based on client selection in AMI network. *Expert Syst.* (2022).

[126] Ruzhi Xu, Rui Wang, Zhitao Guan, Longfei Wu, Jun Wu, and Xiaojiang Du. 2017. Achieving efficient detection against false data injection attacks in smart grid. *IEEE Access* 5 (2017), 13787–13798.
[127] Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. 2005. The feasibility of launching and detecting jamming attacks in wireless networks. In *6th ACM International Symposium on Mobile ad hoc Networking and Computing*. 46–57.
[128] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. 2012. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Commun. Surv. Tutor.* 15, 1 (2012), 5–20.
[129] Y. Yang, H. T. Jiang, K. McLaughlin, L. Gao, Y. B. Yuan, W. Huang, and S. Sezer. 2015. Cybersecurity test-bed for IEC 61850 based smart substations. In *IEEE Power & Energy Society General Meeting*. IEEE, 1–5.
[130] Ruizhe Yao, Ning Wang, Zhihui Liu, Peng Chen, and Xianjun Sheng. 2021. Intrusion detection system in the advanced metering infrastructure: A cross-layer feature-fusion CNN-LSTM-based approach. *Sensors* 21, 2 (2021), 626.
[131] Hyunguk Yoo and Taeshik Shon. 2015. Novel approach for detecting network anomalies for substation automation based on IEC 61850. *Multim. Tools Applic.* 74, 1 (2015), 303–318.
[132] Ke Zhang, Zhi Hu, Yufei Zhan, Xiaofen Wang, and Keyi Guo. 2020. A smart grid AMI intrusion detection strategy based on extreme learning machine. *Energies* 13, 18 (2020), 4907.
[133] Yichi Zhang, Lingfeng Wang, Weiqing Sun, Robert C. Green, and Mansoor Alam. 2011. Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid. In *IEEE Power and Energy Society General Meeting*. IEEE, 1–8.
[134] Yichi Zhang, Lingfeng Wang, Weiqing Sun, Robert C. Green II, and Mansoor Alam. 2011. Distributed intrusion detection system in a multi-layer network architecture of smart grids. *IEEE Trans. Smart Grid* 2, 4 (2011), 796–808.
[135] Jixuan Zheng, David Wenzhong Gao, and Li Lin. 2013. Smart meters in smart grid: An overview. In *IEEE Green Technologies Conference (GreenTech)*. IEEE, 57–64.
[136] Bonnie Zhu and Shankar Sastry. 2010. SCADA-specific intrusion detection/prevention systems: A survey and taxonomy. In *1st Workshop on Secure Control Systems (SCS)*.
[137] Mu Zhu, Ahmed H. Anwar, Zelin Wan, Jin-Hee Cho, Charles Kamhoua, and Munindar P. Singh. 2021. A survey of defensive deception: Approaches using game theory and machine learning. *IEEE Commun. Surv. Tutor.* (2021), 1–1. DOI: https://doi.org/10.1109/COMST.2021.3102874

Received 26 August 2021; revised 24 August 2022; accepted 26 November 2022