Review

Intrusion Detection System in Smart Grid-A Review

Shampa Banik *, Trapa Banik, Shudipta Banik

Posted Date: 8 September 2023

doi: 10.20944/preprints202309.0611.v1

Keywords: Smart Grid (SG); Advanced Metering Infrastructures (AMI); Smart Meters (SM); Intrusion Detection System (IDS)

Article

Intrusion Detection System in Smart Grid—A Review

Shampa Banik [1,*], Trapa Banik [2] and Shudipta Banik [3]

[1] IEEE Student Member, Dept. of Computer Science, Tennessee Tech University, Tennessee, USA
[2] IEEE Student Member, Dept. of ECE, Tennessee Tech University, Tennessee, USA; tbanik42@tntech.edu
[3] Dept. of Computer Science, East Delta University, Chittagong, Bangladesh; shudipta.cse16@gmail.com
* Correspondence: sbanik42@tntech.edu

Abstract: The smart grid system, an improvised form of the traditional grid, is considered a critical cyber-physical system. Due to its complex combination of smart and legacy technologies, this technology is characterized by a wide range of features such as full duplex communication, advanced metering infrastructure, remote monitoring, and control. However, despite this system's substantial environmental and socio-economic impact on modern life, it poses severe security vulnerabilities due to its integration and interconnected and interdependent cyber-physical components. Based on the rapid development of cyber-physical systems (CPS), academics and industries have investigated relevant techniques to enhance and strengthen the security measures of the SG system. The intrusion detection system is a countermeasure, a powerful safeguard against various cyber-attacks and threats. The contribution of the IDSs to the SG paradigm is examined in this study. A comprehensive review has been presented in this study, highlighting different techniques, basic ideas, and analyses. Besides discussing the contemporary pertinent research studies, the shortcomings of the existing IDS for the SG system are also identified with a recommendation for future research direction.

Keywords: Smart Grid (SG); Advanced Metering Infrastructures (AMI); Smart Meters (SM); Intrusion Detection System (IDS)

1. INTRODUCTION

The smart grid (SG) paradigm is the next technological leap with the modernized and advanced version of the traditional electric power grid that incorporates cyber-physical system (CPS) components like digital communication networks and advanced automation and control systems. It offers numerous benefits like improved service quality, increased reliability, and efficient use of the current infrastructure and renewable energy sources, leveraging real-time data from sensors and intelligent devices to monitor and control power production, transmission, and distribution.

The conceptual model, represented in Figure 1, comprises seven logical domains explained by NIST's framework: The transmission and storage of enormous volumes of energy is referred to as bulk generation; Long-distance transmission is the act of sending energy. Sending electricity to the end-user or consumer is distribution.

Therefore, digitalizing these seven logical premises is severely vulnerable to the security risks of a wide range of potential attacks and threats that might cause cascading effects on human life and the entire nation [2]. The security and dependability of innovative grid systems are gravely threatened by cyber-physical attacks, even with the growing reliance on cutting-edge technologies like smart meters and automated control systems. Denial of service, false data injection, and physical damage are some of the most prevalent categories of cyber-physical attacks identified in this study research. A reckless intruder or attacker can infiltrate the network and rapidly interrupt the entire process, leading to a catastrophe. On the other hand, some advanced adversaries may perform distributed attacks at a time instead of not disrupting the regular system operation. For example, the Advanced Persistent Attack (APT) attack in Ukraine in 2016 [3], another cyber attack employed in Stuxnet [4]. Implementing sufficient security measures throughout the entire smart grid infrastructure, including hardware, software, and communication protocols, is challenging to reduce the risks of cyber-physical attacks. Assault detection and prevention should be the goals of these measures, and they should also guarantee

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 September 2023 doi:10.20944/preprints202309.0611.v1

the quick recovery of vital systems in the case of an assault. Developing robust countermeasures in the SG system has become a grave concern for technical, organizational, and regulatory issues and continuing research and development initiatives. As a part of countermeasures, the intrusion detection system plays a pivotal role in the SG system to protect the system by detecting any of these types of cyber-physical attacks or threats and making the system aware of any further disaster. Leveraging these characteristics and identifying unknown assaults are the main goals of SG IDS design.

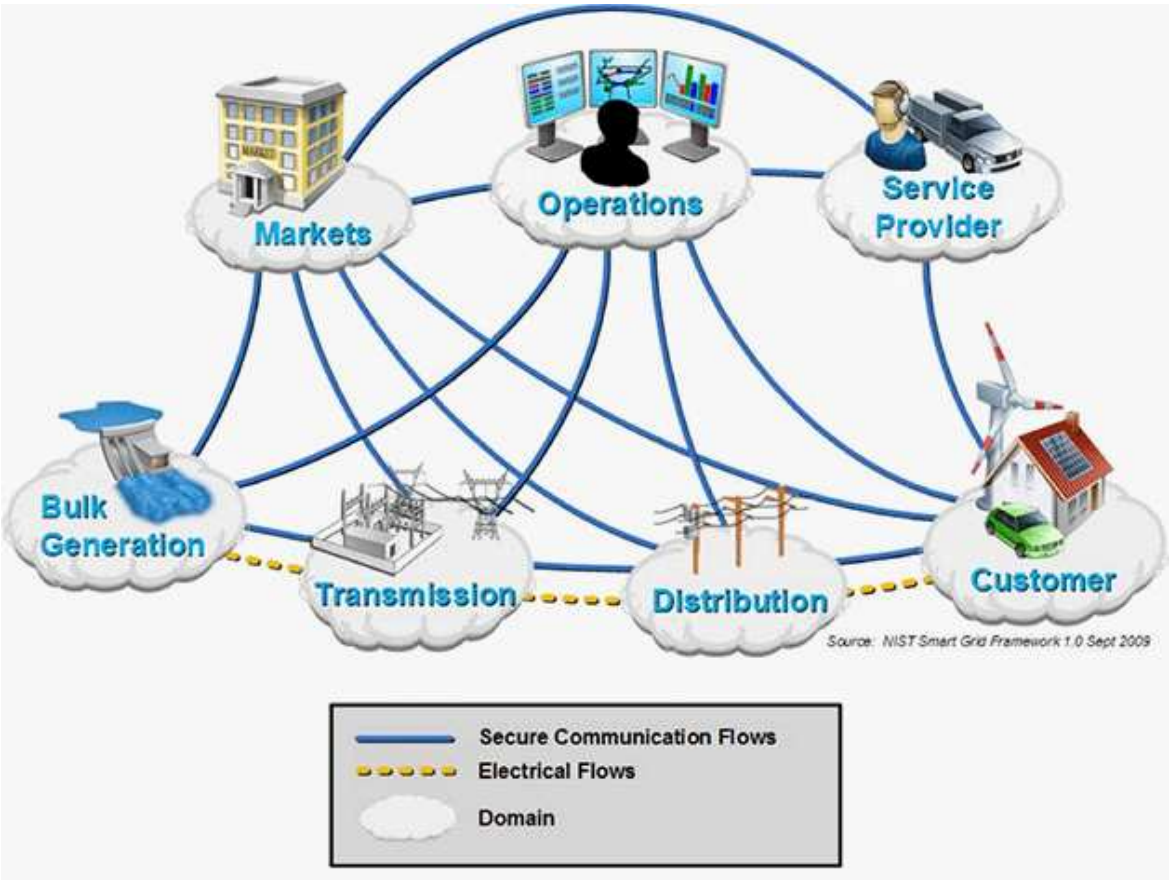

Figure 1. Smart Grid's conceptual model [1].

The smart grid relies on advanced metering infrastructure (AMI), which enables bidirectional communication between users and utilities. The main functions of AMI are electricity measurement, adaptive pricing, and demand-side management. Securing AMI is crucial due to threats such as energy theft, smart meter compromise, and denial of service, which can lead to grid instability, blackouts, and customer data leaks [5]. An intrusion detection system in advanced metering infrastructure can combat smart grid cyber threats. The anomaly-based intrusion detection method can identify little changes in the investigated parameter, while the signature-based method only detects known attacks [6].

An anomaly-based IDS has been suggested in this study that is based on state-of-the-art machine learning focusing on one of the crucial components of AMI that generates big consumption data daily. Here, the intrusion detection technique would detect any attack or adversaries on AMI incorporating the anomaly or abnormality detection technique. Despite the sheer number of researchers investigating this particular area of SG, only some detection methodologies tried to blend up network and smart meter data to reveal the strange pattern for proper detection.

As a contribution, SG IDS design principles and methodologies are reviewed in recent relevant research studies in this document. Then, one taxonomy of the IDS study in the SG system has been introduced to better analyze. After examining the potential gap in the reviewed literature, a concept of

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 September 2023 doi:10.20944/preprints202309.0611.v1

anomaly-based IDS targeting the AMI in the SG system is recommended for future direction in this domain.

The structure of our review's findings comprises six distinct sections. Section 2 is the research overview on IDS for the SG system with a discussion according to the taxonomy of the IDS study from different aspects. Section 3 discusses the potential gap from the existing research and recommends a solution model to bridge the gap as a future research direction. And lastly, Section 4 concludes the paper.

2. Overview of Intrusion Detection System

The intrusion detection system (IDS) is a subsequent security measure and a protection mechanism against cyber-attacks. IDS scans the network for unusual activity and records it. To identify internal or external cyber-attacks, IDS combines hardware and software techniques. IDS's primary responsibilities are attack detection and prevention, situational awareness, evidence gathering, and connection topology management. This paper presents the conceptual taxonomy based on the IDS study in the SG domain as depicted in Figure 2. This taxonomy will follow the survey throughout our research.

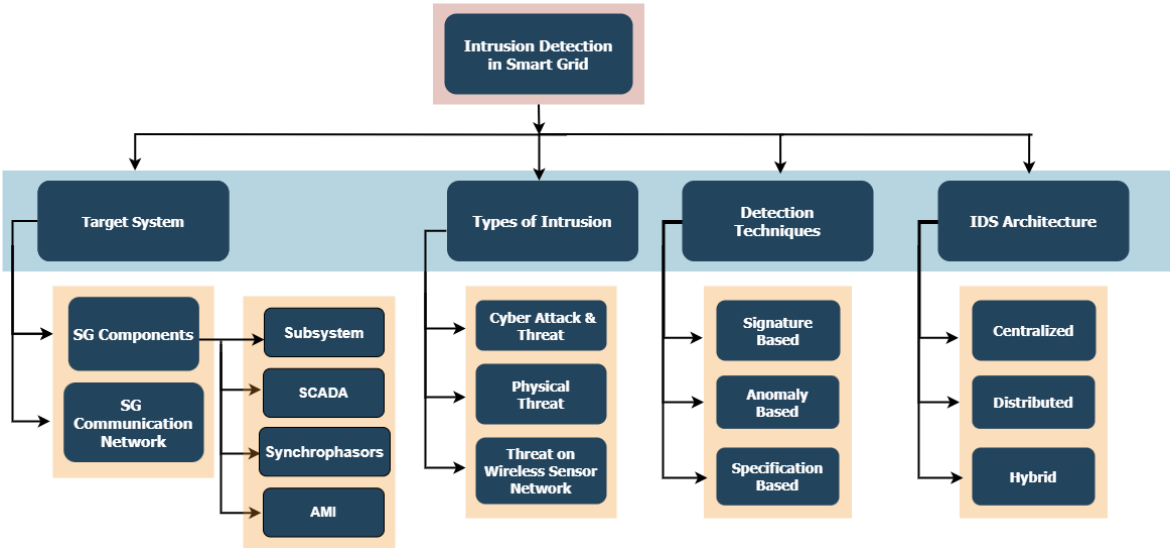

Figure 2. A map of the IDS of SG system taxonomies used in the literature.

The purpose of an intrusion detection system, as stated in RFC document 2828, is to swiftly audit and analyze security events to identify possibly harmful activities. Since their inception in the 1980s, intrusion detection systems (IDS) have been used to automate the processes of monitoring, auditing, analyzing, and identifying potential hazards. In particular, James Anderson [7] suggested that a computing system's log files may be a particularly effective source for tracking the system's status and how different users interact. Researchers began to create the first IDS that properly evaluated log files to ease the job of security managers based on Anderson's technical report.

2.1. Target System: Smart Grid Paradigm

The definition of the SG paradigm has engaged several institutions, including the Electric Power Research Institute (ERPI), the Department of Energy (DoE), and the European Commission Task Force for Smart Grid [8]. The SG paradigm integrates numerous infrastructures, systems, and technologies, such as synchrophasor systems, substations, microgrids, AMI, SCADA systems, and the entire SG. As AMI and Supervisory Control and Data Acquisition (SCADA) systems are the most important and vulnerable to attacks from these technologies, most of the IDS solutions studied here concentrate on them. Due to their importance to the ongoing operation of SG, substations and synchrophasor systems are particularly alluring targets for online criminals. A notable feature of SG is its ability to produce

 doi:10.20944/preprints202309.0611.v1

SG that uses sustainable energy sources. These distinctive grid infrastructures could, however, exhibit varied types of vulnerability. A wide range of intrusions generally occurs in SG, targeting components such as the SG substation, SCADA system, synchrophasor, AMI, and the SG communication network. This section examines the SG paradigm's components and related communications to give a general overview.

1. **Intrusion on Smart Grid Components** This section examines the SG paradigm's components and related communications to give a general overview. The substations play a pivotal role in the operation of SG.

    - **Substation:**The substations play a pivotal role in the operation of SG. Substations operate SG's transmission and distribution processes. A Substation Automated System (SAS) with IEDs, RTUs, and computers controls modern substation operations [9]. In particular, they participate in the generated power, set up the distribution system, and manage the power expansion. They may contain various hardware and software elements, including GPS, RTUs, HMIs, and Intelligent Electronic Devices (IEDs) [10]. The substation can be one of the most significant targets for an intruder to disrupt the system's regular operation or functionalities and the total power supply, which may cause a cascading effect on society and nations. Modern substations must address cybersecurity risks in supervisory control and data acquisition (SCADA) systems as IEC 61850 smart substations emerge. This study presents a new IDS for IEC 61850 substation cybersecurity evaluating multidimensional physical knowledge and behaviours to deliver a comprehensive and effective cyber threat mitigation solution [11]. A 500kV smart substation cyber-physical testbed implements and validates this SCADA-specific ID.

      In [12], M. Kabir-Querrec et al. provides a specification-based IDPS that centres on substation communications according to IEC 61850. In particular, IEC 61850's data object model is the foundation for their IDPS's architecture, including a novel intrusion detection function.

      Using the IEC 61850 standard, H. Yoo and T. Shon [13] present an anomaly-based IDPS for the substations. The proposed IDPS zeros in on MMS and GOOSE protocols using a one-class SVM classification model to zero in on patterns that correspond exclusively to regular and legitimate network traffic.
    - **SCADA System:** SG is a system based on SCADA systems, a part of the industrial control system and environment, that necessitate monitoring and managing the automated operation of other components. A SCADA system is made up of the following components in particular: a) measuring devices; b) logic controllers, such as programmable logic controllers or Remote Terminal Units (RTU); c) Master Terminal Units (MTU); d) communication network; and e) an HMI. Measurement instruments track objective quantities like temperature, pressure, and voltage. The primary duties of logic controllers include gathering data from the measuring devices, identifying unusual behaviours, and activating or deactivating technical components [9]. The system operator can give commands to logic controllers and receive data through MTU, a central host through which the logic controllers communicate. The communication network is used to realize the interface between MTU and the logic controllers. This communication system uses industrial protocols like Distributed Network Protocol 3 (DNP3) and Modbus. The interface between MTU and logic controllers is facilitated by HMI, a software package with graphical capabilities installed on MTU. All of the components of SCADA in the SG system are highly vulnerable to attack by any intrusion or hacking, as illustrated in Figure 3. Due to the interdependency of each component to run the whole system of SCADA, any unauthorized access to any of its members by an intruder may cripple the entire SG system. E. Hodo et al. offer an anomaly-based IDS for a SCADA-simulated environment using the IEC 60870–5-104 [109] (IEC-104) protocol in [14]. S.D. Anton et al. compare four machine

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 September 2023 doi:10.20944/preprints202309.0611.v1

learning techniques for Modbus/TCP anomaly detection in [15]. They employed Lemay and Fernandez's dataset [16] that was separated into three sub-datasets: DS1, DS2, and DS3. DS1 contains 3319 packets of MTU-to-6 RTU network traffic, including 75 malicious occurrences. DS2 has 11166 packets, with 10 malicious ones with one MTU and six RTUs. Finally, eight datasets produced 365906 packets with 2016 harmful cases in DS3. These sub-datasets provided features for machine learning algorithm training.

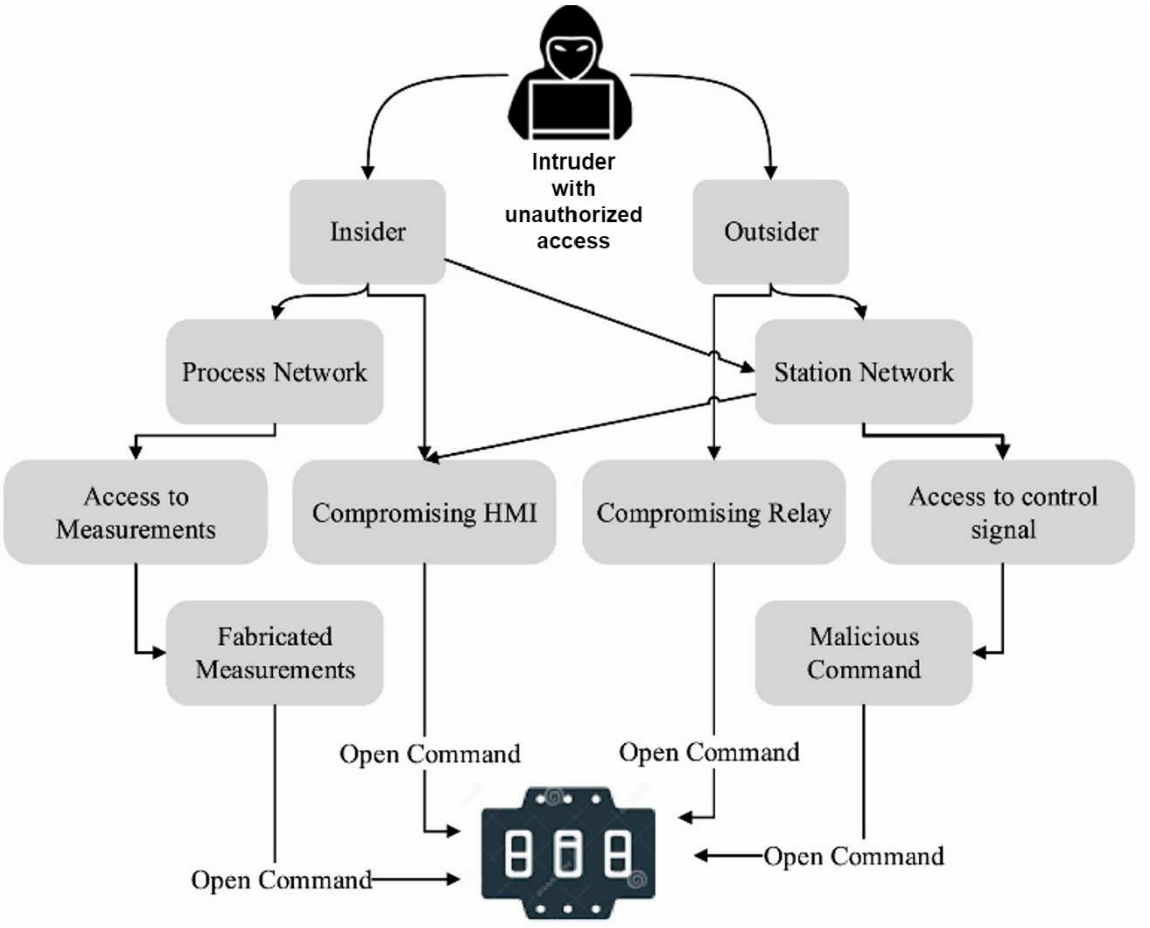

Figure 3. Action of intruder targeting the substation in smart grid [17].

- **Synchrophasor:** A synchrophasor system is an emerging technology required for the functioning of the contemporary electrical grid. It primarily consists of Phasor Measurement Units (PMUs), Phasor Data Concentrators (PDCs), a communication network, and GUI software. A PMU is an instrument that performs numerous measurements from current/voltage waveforms, including frequency, phase angle, active power, and reactive power. A PDC takes on the task of compiling PMUs' information and combining it into a single flow. The IEEE C37.118.2 and IEC 61850 [18] standards are typically used for communication between PMUs and PDCs. The GUI application's final responsibility is to visualize the various data from PDCs properly. For synchrophasor systems that employ the IEEE C37.118 protocol, Khan et al. [19] presented a hybrid IDS primarily based on specification-based and signature-based approaches. The suggested system's general design comprises two types of detectors, or HIDSs and NIDSs, respectively, called agents and sensors. Agents monitor PMUs and PDCs' performance, while sensors control data flow throughout the network. In addition, a management server compiles and correlates data from all the sensors and agents. Any detection notice or warning is also documented in

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 September 2023 doi:10.20944/preprints202309.0611.v1

a database server. In [20], Y. Yang et al. proposes a specification-based IDPS that can secure IEEE C37.118-based synchrophasor systems. Access control, protocol-based, and behaviour-based rules are the three main categories of rules in their intrusion detection and prevention system (IDPS).

- **Intrusion on AMI:** An AMI system comprises three basic parts: smart meters, data collectors, and a headend. Smart meters try to track the electrical appliances' power usage and other metrics [21]. Data collectors must store the information produced by numerous smart meters in a particular region. The AMI headend, which receives, stores, and maintains the data collected by the data collectors, is the utility company's central server. The utility firm can make the best decisions for the power generation, transmission, and distribution processes based on the information gathered on the AMI headend. In [22], the authors examined the recent academic approaches to intrusion detection systems and techniques for AMI and discussed the threats that could potentially affect this industry. Numerous contributions have been made to secure the AMI: In [23], authors created a specification-based Intrusion Detection System (IDS) for Home area networks (HANs) responsible for data transfer among smart meters and household devices. The IDS design targets ZigBee's physical and medium access control layers and defines its normal behaviour based on extracted specifications. Any change from usual behaviour may signal an attack. In [24], authors suggest an IDS for AMI, consisting of three local IDSs in smart meters, data concentrators, and the head-end. The IDS uses stream data mining to identify network assaults. This paper introduces an IDS for the neighbourhood area network (NAN), an AMI subsystem connecting smart meters to data concentrators. The IDS uses data mining to detect malicious activities caused by blackhole attacks in this area.

  Another well-suited distributed IDS architecture for AMI is an Extreme Learning Machine (ELM). ELM's quick training speed and robust model generalization ability are ideally suited for intrusion detection in the smart meter of the SG system. An ELM intrusion detection model based on a genetic algorithm (GA) is proposed as a solution to the issue that the ELM's random input weights and hidden layer bias prevent the model from performing at its ideal level [25].

2. **Smart Grid Communication**

A generalized SG architecture separated into communication aspects is shown in Figure 3. Three different network area types—Home Area Networks (HANs), Business Area Networks (BANs), and Industry Area Networks (IANs)—are present in the first layer and are identified by the presence of consumers. The existence of smart meters, which track and communicate information about electrical appliance energy usage, is precisely the critical feature of these network areas. A network connecting a home's electronic and intelligent gadgets is called a HAN. The second form, or BAN, is a network comprising the hardware and software needed for an organization to operate. The IAN also specifies a network that includes all the functional components needed for industry. The devices of these networks often use ZigBee and Z-wave, as shown in Figure 4. Rarely, they may also employ Power Line Communications (PLC) or IEEE 802.11 (Wi-Fi). The authors in [26] suggested a structure for IDS deployment in the smart grid. The proposed system will collect and correlate notifications from various intelligent grid sensors. In the innovative grid network, sensors might be installed in HANs, NANs, or even the vast area network. We looked at the intrusion detection classification algorithms' results on the ISCX2012 dataset.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 September 2023 doi:10.20944/preprints202309.0611.v1

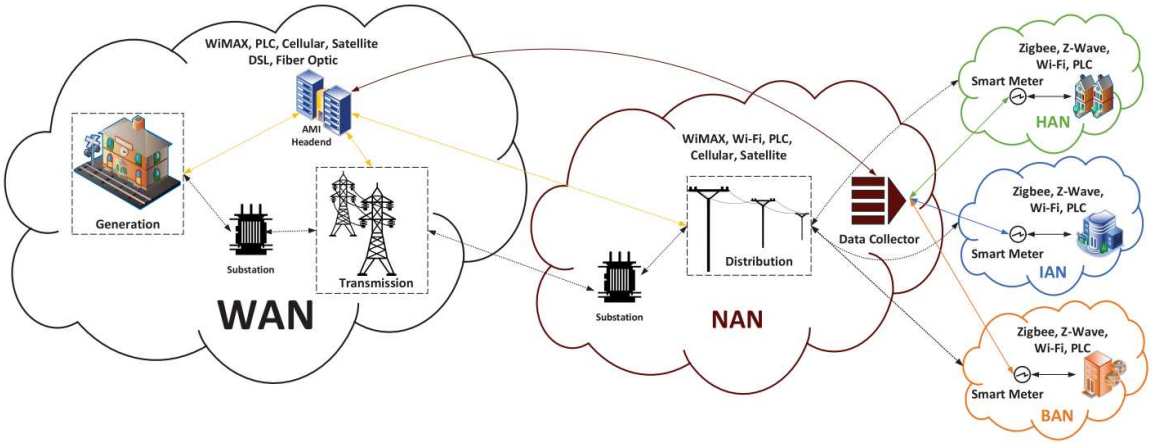

Figure 4. The communication architecture of SG system [9].

2.2. Types of Intrusion

Although many studies have been conducted to look at where intrusion detection systems are at the moment, they all have slightly different focuses on things like assessing, comparing, and summarizing the intrusion detection strategies that have been researched, as well as on finding research gaps and future research objectives. For instance, Aburomman and Reaz [27] present a review of IDS based on ensemble and hybrid classifiers against coordinated attacks like distributed denial-of-service (DDoS) attacks. In contrast, Zhou et al. [28] provides an overview of collaborative IDS. As Arshad et al. [29] point out, future IDS research should focus more on computing overhead, energy usage, and privacy consequences when comparing current IDS. Berman et al. [30] presented a thorough analysis of deep learning strategies in the context of computer security. Buczak and Guven summarize data mining and machine learning [31] and argue that the methods for quick incremental learning should be further explored. Mitchell and Chen [32] examine possible intrusion detection methods for CPS and talk about the pros and cons of using different intrusion detection methods for CPS. They point out that the distinctiveness of intrusion detection in CPS may be seen in features such as physical process monitoring, closed control loops, advanced attacks, and legacy technology. In addition, they stress the importance of putting more work toward specification-based and federated IDS.

While Tong et al. [22] presented an overview of IDS for SG's AMI alone, the IDS for SG's ecosystems and subsystems is covered in great detail by Grammatikis and Sarigiannidis [9]. Furthermore, Grammatikis et al. note that no IDS is proven in the literature for defending the SG microgrids. Intrusion refers to when an unauthorized user gains access to the system either physically or cyber and gets the ability to control the system with a malignant intention to breach the three main cyber-security requirements for the SG: *availability*, *Integrity*, and *Confidentiality* (CIA). Various forms of cyber-attacks or physical threats and anomalies are now considered when it comes to "Intrusion" in SG, in addition to cyber and physical threats or attacks. The threat taxonomy refers to both generic cyber-attacks and specific attacks and threats that exploit the smart grid system, as illustrated in Figure 5.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 September 2023 doi:10.20944/preprints202309.0611.v1

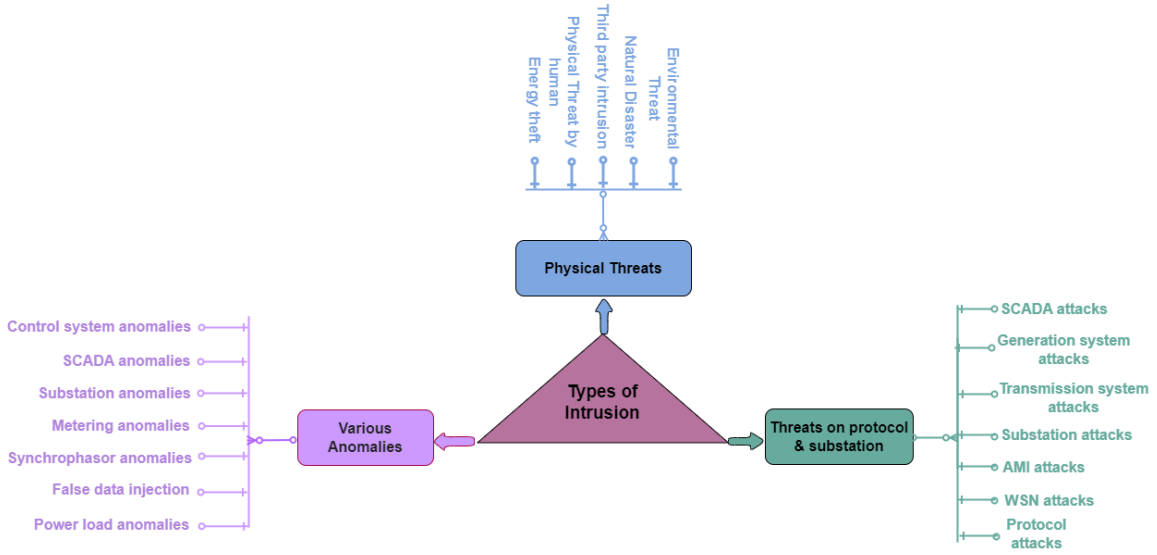

Figure 5. Threat taxonomy of intrusion in SG.

1. **Cyber Attack and Threat**

   Recently, the SG system is mainly prone to a crucial type of intrusion, that is, cyber-attacks or threats, which are network-based. Exploiting badly the trusted perimeter built by the set-up of firewalls with wrong inbound and wrong outbound rules is a common way for an intruder or attacker to get into the communication network system and put a malicious payload on the control system. In the first phase of this type of intrusion, the intruder gets into the network through unauthorized access, where the intruder could be either an insider or an outsider with the ill intention to do malicious action on the system and gain any profit. For instance, an intruder could wait for a legitimate user to join the trusted control system network via VPN and then take over that VPN connection. The network-based attacks mentioned above are dangerous because they allow an attacker from outside to get into the web of a trusted control system.

   Due to resource (device, deployment, and communication) constraints imposed by communication standards and sensor nodes, for a reliable hierarchical smart grid, it is essential that several communication standards can work together securely. The negative impacts of cyber-attacks can be mitigated by creating various intrusion detection and prevention system solutions.

   - **Potential cyber-attacks:** In terms of cyber-attacks, they can take many different forms, some of which include man-in-the-middle (MITM) attacks, denial-of-service (DoS) attacks, false data injection attacks (FDIA), and other cyber-physical assaults on the smart grid. These attacks include hacking into power plants or distribution network control systems, deceiving sensors and monitoring systems, or destabilizing communication networks that link different grid components. The evaluation of the state of the power system could be hampered by a significant class of cyber-attacks known as FDIA (False Data Injection Attack). The FDIA might compel the state estimator to give the system operator false data, which might have unforeseen consequences for the power system. The FDI attack was found in [33] after a series of attacks and a processed innocuous data set. Such injection assaults, whether they target the smart meter or the command line, can produce seriously abnormal load patterns or power consumption in Singapore, to quote one example [34,35]. The correctness of the calculation and analysis depends on how well the state is estimated [36,37]. A denial-of-service (DoS) attack, as defined by [38,39], is an attempt to overwhelm a targeted computer system or network with traffic or requests to disrupt routine operations and prevent authorized users from accessing it. In Man-in-the-Middle (MitM) cyber-attacks, the

 doi:10.20944/preprints202309.0611.v1

attacker intercepts a conversation between two parties to covertly listen in, manipulate, or impersonate one or both of the participants [40,41]. Two frequently utilized MITM attack strategies are ARP spoofing and DNS spoofing. In a replay attack, a hacker intercepts previously obtained data and maliciously retransmits it to pass it off as coming from the original sender and gain unauthorized access to a system or network. The attacker sends a packet of messages [42] to the victim host in the fake system.

Another most perilous form of cyber attack is the Advanced Persistent Attack (APT). For instance, the intrusion on a Ukrainian Advanced Persistent Attack (APT) caused a blackout for more than 225,000 people, which took a prolonged period for the security specialists to coordinate in pursuit of a particular goal [3].

Backdoors and holes in the network boundaries can be caused by IT infrastructure components that are weak or are set up wrong. Networking devices at the edge, like fax machines or modems that have been forgotten but are still connected, can be used to get around proper access control [43].

In particular, access remote terminal units (RTUs) are used for remote management of the dial-up. Many departments don't require a password for authentication, and the default passwords for modems attached to field equipment are often left unchangeable, making them vulnerable to attack. Also, bad guys can use the devices' flaws to install backdoors that will let them get into the restricted area in the future. Another possible network-based entry point is through safe peer utility links.

- **Cyber-attacks on common SG protocols:** smart grid components use various protocols or standards that inherit security vulnerabilities. Protocols like TCP/IP and remote procedure calls (RPC) are often used. The Modbus protocol, widely used in industrial control systems like water, oil, gas, and SG, is a SCADA protocol. Since the Modbus system wasn't designed for highly security-critical environments, it is a noteworthy concern because there are several ways to attack it. The Modbus is a simple client-server system for low-speed serial communications in process control networks. Process control systems use this to exchange SCADA information used to run and handle industrial processes [44]. The most common Modbus attacks are as follows: 1) Baseline response replay, 2) Direct slave control, 3) Modbus network scanning, 4) Passive survey, 5) Broadcast message spoofing, 6) Rogue interloper, and 7) Response delay. Suppose an attacker can sniff network traffic using a protocol analysis tool. In that case, they can potentially intercept SG Distributed Network Protocol 3.0 (DNP3) messages and obtain unencrypted plaintext frames containing vital information like source and destination addresses. Intercepted data, such as control and setting information, could be used on another SG system or intelligent equipment device (IED) later, potentially shutting down services or, at the very least, causing service disruptions.

2. **Physical Threats:** Along with these examples of cyber-attacks, a wide range of physical threats can have detrimental effects, such as damaging equipment and even creating power outages of the SG system. While our study does not focus on physical attacks of the SG, we do concur that the possibility of such attacks is more likely to be launched against the power lines themselves, in addition to transformers and substations [45]. Although uncommon, attacks on the power grid's physical infrastructure, including power lines, transformers, and substations, could happen. However, the smart grid is more likely to be attacked physically through its softer entry points. For instance, smart meters are more likely to be attacked physically due to their ease of access and prevalence. According to research by Anderson and Fuloria [46], an attacker might remotely turn off millions of smart meters simultaneously.

   Apart from these, any third-party integration might cause a severe adverse impact on securing the SG system. On the other side, sometimes energy theft becomes a grave security concern for

 doi:10.20944/preprints202309.0611.v1

identifying intrusion in the SG system. An attacker can successfully reprogram industrial control systems by injecting malware targeting the vulnerable points of industrial control systems; one example is the Stuxnet attack [9] against the Iranian nuclear program, which exploited four zero-day vulnerabilities.

Moreover, besides human errors, equipment failures account for numerous blackouts on the current SG system, including those in North America, Switzerland/Italy, London/West Midlands, Turkey, and South Australia. Research into systems for detecting incidents with the potential to lead to cascading failures was spurred by the North American Blackout [47].

3. **Threats on WSN:** Wireless sensor networks (WSN) are integral to the Smart Grid's communication framework. Smart Grid network cyber security issues and their remedies have been explored in detail elsewhere due to their unique characteristics; sensor nodes in WSN present individual attack vectors, vulnerabilities, and security requirements. Communication between sensor nodes in a WSN is more concerned with the data than the address of a specific sensor node, so address-specific security threats and remedies may not apply. One of the weakest, most convoluted, and most challenging parts of Smart Grid security is the protection of WSNs. The WSN security is a multifaceted research issue as the security of the entire Smart Grid network can be built upon this. There are various kinds of attacks and threats on WSNs. In external attacks, most hacking incidents involve an intruder located beyond the coverage area of a wireless sensor network (WSN). Jamming the network, using all available resources, or launching a denial of service (DOS) attack are examples of external aggression.

   For internal attacks, an intruder is supposed to be an insider of WSN. This type of adversary is generally performed for physical tampering of nodes, the revelation of confidential information, causing a denial of service to authorized nodes, etc. In the active type of attack, the adversary compromises the security characteristics of WSN to modify and steal the data. An attacker carries out this type of assault to perform an adversary on data by modifying packets, injecting fake data, depleting network resources, and capturing nodes. Examples of active attacks on WSN include spoofing, jamming, wormholes, hello floods, denial of service, sinkholes, etc. On the other hand, passive attacks are performed by an intruder mainly by observing network activities by performing reconnaissance attacks. This type of attack targets the confidentiality of the network. An example of such attacks is an analysis of traffic, decryption of vulnerable data, capturing information, etc.

   To implement an efficient IDS, the nature of attacks should be understood beforehand to develop countermeasures at various network layers. WSNs typically employ hierarchical network architectures, which leaves the networks extremely susceptible to routing problems while switching between topologies. This paper investigates topology control for the cyber security of wireless sensor networks as an alternative to well-studied options like intrusion detection systems and cryptographic security [48]. Many authors have been surveyed recently regarding IoT-related topics, and they all tend to focus on specific parts of IDS. A review of machine learning approaches with a particular emphasis on intrusion detection systems (IDS) for WSNs and the Internet of Things [32,49]. Research by Buczak and Guven [31] indicates several concerns with approaches, particularly for the complexity of those requiring acquisition, and discusses IDS on the general system commonly used for specialized WSN and IoT.

2.3. Intrusion Detection Techniques

To detect potential threats and anomalies, the Analysis Engine employs particular techniques. To identify dangers and unusual occurrences, the Intrusion Analysis Engine uses several different methods. A signature-based method, an anomaly-based method, and a specification-based method are the three main categories of intrusion detection approaches frequently adopted in SG technology. The first type's functionality, called "Signature-based," compares what happens in a computing system to a specified set of infiltration patterns. A corresponding alert is extracted if an action's attributes match

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 September 2023 doi:10.20944/preprints202309.0611.v1

one of the signatures. Significantly, this technique necessitates knowledge of every system testing vulnerability. This method produces excellent dependability and a low percentage of false positives, but its weakness is that it cannot identify unknown attacks that are not determined by any signature. Because of this, IDS, using this technique, must periodically update the set of signatures to include new types of assaults. On the other hand, the second technique's (anomaly-based) effectiveness is predicated on the identification of abnormal actions as intrusions. Typically, this strategy uses statistical analytic procedures or machine learning techniques to identify malicious behaviour, including Bayesian networks, neural networks [50], and Markov models. In comparison to the prior method, the use of this one could be more precise. However, it offers the benefit of identifying unidentified cyber-attacks.

The third method, known as specification-based, uses a set of established guidelines to characterize the typical operation of the system being tested. These guidelines are known as specifications.

Figure 6 illustrates the frequently used Intrusion detection technique in smart grid systems.

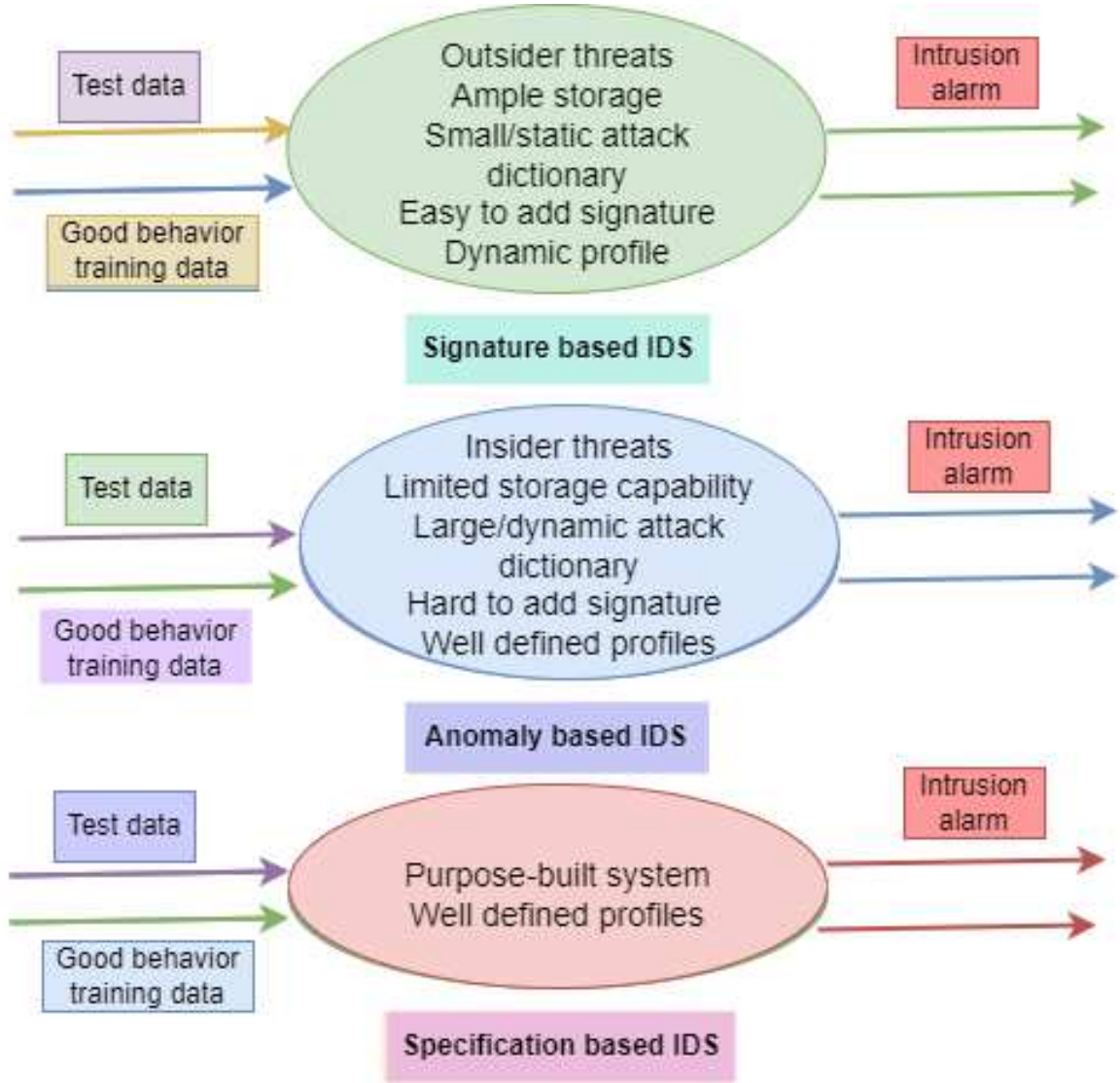

Figure 6. Frequently used Intrusion detection technique in SG.

1. **Signature-Based IDS:** The second category (Signature-based) works by comparing events in a computer system against a list of known malicious patterns, or "signatures." Each action is compared to each signature, and an alert is generated if a match is found. It is essential to highlight that this method necessitates complete familiarity with the tested system's weaknesses. Although this method has a low false-positive rate and high dependability, it cannot identify

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 September 2023 doi:10.20944/preprints202309.0611.v1

attacks that do not match any known signature. USING MATLAB, an AMI IDS incorporating temporal and geographic detection approaches, was developed by the authors of [51]. The suggested system is primarily concerned with blackhole and time delay attacks. However, the time delay attacks aim to make the packet transmissions sluggish.

Intrusion detection methods based on signatures examine data gathered during execution to see if it matches a known pattern of malicious activity. Misuse detection, supervised detection, pattern-based detection, and intruder profiling are used to describe this technique [32].

This means that IDS employing this technique must routinely update their signature sets to account for emerging threats. However, the second method's usefulness is predicated on labelling anomalous actions as malicious intrusions. Bayesian networks, neural networks, and Markov models are examples of the statistical analytic procedures and machine learning techniques typically used in this approach to detect hostile actions. The application of this method is less precise than its predecessor. One benefit is that it can identify previously unseen forms of cyberattack.

2. **Anomaly-Based IDS:**

   Intrusion detection methods that identify anomalies in runtime behaviour are called "anomaly-based." The commonplace can be defined in two ways: regarding a set of training data (semi-supervised) or the past of the test signal (unsupervised). Unsupervised machine learning is illustrated through clustering.

   Anomaly-based detection finds intrusive behaviour that deviates from the allowed range or the white list. It can identify unusual suspicious behaviour in the smart grid. An anomaly-based intrusion detection technique trains the model using a normalized baseline against which every activity is analyzed [52]. Attackers are likelier to experiment with novel approaches to undermine the intelligent grid system, and attacks are more likely to be discovered by anomaly-based intrusion detection.

   Denning [53] established the first anomaly detection model as an adjunct to misuse-based detection techniques. The purpose of statistical models that describe typical behaviours is to detect outliers. An anomaly-based IDS operates under the hypothesis that routine activities can be predicted statistically and that outliers indicate malicious intent. Point, contextual, and collective anomalies are the three deviations identified by [54]. Anomaly detection studies typically centre on point anomalies and single data instances. Each data object carries contextual attributes and behaviour characteristics, making contextual anomalies conditional anomalies. Sequence, graph, or spatial data exhibits a collective abnormality.

   ARIES, as detailed in [55], is a novel anomaly-based intrusion detection system (IDS) that can reliably safeguard SG communications against intrusion. ARIES has three detection layers—(a) network flows, (b) Modbus/Transmission Control Protocol (TCP) packets, and (c) operational data—to identify potential cyberattacks and irregularities. The ARIES Generative Adversarial Network (ARIES GAN) was built utilizing cutting-edge error reduction techniques to detect anomalies in operational data (i.e., time series electricity measurements), with a focus on the third layer (operational data-based detection).

3. **Specification-Based IDS** Finally, the third method (Specification-based) relies on predefined rules that characterize the typical operation of the system under test. Specifications refer to these guidelines. An alert is sent when an action's properties deviate from one of the requirements. Because it can identify potential irregularities, this approach can reveal previously unknown attacks. This method differs from the signature-based approach in that it is predicated on the idea that the system's security policy can't be breached if all specifications are met. However, this is different from the signature-based method. The word "hybrid" is now used to describe an IDPS combining two or more approaches mentioned above.

   A specification-based intrusion detection framework has been developed to categorize substation scenarios and detect cyber-attacks in [56]. The proposed intrusion detection approach uses

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 September 2023 doi:10.20944/preprints202309.0611.v1

Bayesian networks to graphically encode causal links among available information to build patterns with temporal state changes. This lets the proposed system identify cyber assaults and substation scenarios. A modified 2-bus 2-generator system from the IEEE 9-bus 3-generator system is used to explore the non-pilot directional over the current relay protection technique. Nine power system scenarios were devised and implemented for the case study. On the other hand, to maintain the reliability and stability of the grid's distribution infrastructure, a specification-based intrusion detection sensor has been introduced to monitor advanced metering infrastructures (AMI) [57]. To check for device security and compliance with a security policy, this sensor analyzes network, transport, and application levels of communication between meters and access points. It detects all security policy violations by imposing limitations on C12.22 standard protocol transfers. Using a formal framework, these limitations were confirmed, and a sensor prototype was tested with genuine AMI network traffic. An associated warning is exported if an action's characteristics don't match one of the specifications. Because it can identify potential anomalies, this approach can identify undiscovered attacks. This technique is predicated on the presumption that the system's security policy cannot be compromised, unlike the signature-based method, if all requirements are followed. The signature-based process, in contrast, does not rely on any such presumption. It's important to note that the term "hybrid" is now commonly used to denote an IDPS that combines two or more approaches.

2.4. Intrusion Detection Functions and Performance Metrics

The intrusion detection technique is comprised of two core functions: 1. Suspicious data collection 2. Data analysis

An IDS collects audit data through a process called "data collection." The result is a database or set of files, which may be binary or readable by humans. Data can be gathered by, for instance, keeping track of system calls made on a local node, traffic received by a network interface, or reputation scores based on rumours. When a CPS examines the information it has gathered, this is known as data analysis [32]. The outcome may be discrete (bad/good), continuous (bad chance between 0% and 100%), or ternary (bad/good/inconclusive). Pattern matching, statistical analysis, and data mining are all kinds of analysis. The state-of-the-art security and defence mechanisms have been significantly applied and upgraded using machine learning (ML) based intrusion detection system (IDS) approaches. Researchers in IDS commonly utilize the True Positive Rate (TPR), the inverted False Positive Rate (FPR), and the False Negative Rate (FNR) to evaluate performance [58]. An IDS generates a false negative when it incorrectly detects a hostile node as trustworthy. Since FPs and FNs are the most critical measures of IDS performance, the authors in [59] looked into reducing FNs using a two-tier intrusion detection strategy that simultaneously addresses anomaly and signature detection for WSN in the SG system.

In scientific literature, completeness is the opposite of a false negative (FNR). However, when an IDS successfully finds a rogue node, this is known as a detection (or true positive). Lastly, a false positive happens when an IDS incorrectly detects a suitable node as an attacker. A false positive is often called a false alarm in the literature, while FPR's inverse is called accuracy. False-positive rate (FPR) is synonymous with false-positive probability p_{fp} and false-negative rate (FNR) with false-negative probability p_{fn} in the academic literature.

$$\text{TPR} = 1 - \text{FNR} = 1 - p_{\text{fn}}$$

Time to detection is the time that intervals between when an intruder enters the protected system (in the case of an insider) or when an attack is launched (in the possibility of an external attacker) and when the IDS detects the intruder. Power consumption, communication latency, and CPU utilization are vital parameters for resource-constrained target systems. The efficiency of packet sampling refers to the proportion of processed packets flagged as hostile by the IDS; the underlying principle is that it is inefficient to sample many boxes if only a tiny fraction of them cause intrusion detection.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 September 2023 doi:10.20944/preprints202309.0611.v1

2.5. Intrusion Detection System Architecture

IDSs can be installed at the network's edge router, in a subset of hosts, or each connected device for adequate intrusion detection. At the same time, IDS's capacity to often query the network state may cause an increase in communication overhead between the LLN (Low Power Lossy Networks) nodes and the border router. In reality, three primary methods for IDS implantation were outlined by Zarpelo et al. [60].

- **Centralized Architecture:** C-IDS is typically used in centralized infrastructure. Because of this, the LLN can collect and send data across international borders. As a result, centralized IDS may examine all data travelling between the LLN and the Internet. Since it is challenging to monitor each node during an ongoing attack [61], it is not sufficient to identify attacks affecting nodes within the LLN. The primary objective is to determine how to defend against a botnet attack. Kasinathan et al. [62,63] @devised a centralized placement that allows them to think about beating DDoS assaults so that even if one were to occur, the transmission of IDS data would continue unabated. Wallgren et al. [64] implemented a centralized method for detecting attacks on the physical domain in the border router.
- **Distributed IDS:** Every LLN node uses D-IDSs, and those used in nodes with limited resources are optimized as much as possible. Because of this, a lightweight distributed IDS was introduced. Light methodology matching attack signatures and packet payloads were identified by Oh et al. [65], and alternative methods requiring fewer matches were proposed. By assigning nodes to monitor their neighbours in the distributed placement, Lee et al. [66] provide a lightweight way of keeping tabs on a node's power consumption. These nodes serve as "watchdogs" in a network. Cervantes et al. [67] proposed a method to detect and mitigate sinkhole attacks by combining their ideas of trust and reputation with the watchdog nodes. This method is called "Intrusion detection of Sinkhole attacks on IPv6 over Low -Power Wireless Personal- Area Networks (6LoWPAN) for IoT"(INTI). Because of this, the node's function may shift every time the network is reconfigured or an attack occurs.
- **Hybrid IDS:** H-IDS uses the advantages of both centralized and distributed deployments, eliminating both limitations. The first method divides the network into clusters, with the cluster's primary node hosting an IDS instance and then being responsible for monitoring its neighbours. This means a hybrid IDS deployment can be configured to use more resources than a standard IDS deployment [68].

  Le et al. [69] also successfully organized the network into smaller clusters, each with its cluster head, from the same number of initial nodes. Each cluster head might host an IDS instance, with nodes relaying information about themselves and their neighbours to the central node. The second method involves inserting IDS modules into the border router and many additional network nodes in addition to a centralized hub. Using the Routing Protocol Low-power and Lossy (RPL) network data, Raza et al. [70] developed the IDS they called SVELTE, in which the hosts of the border routers are tasked with processing-intensive IDS modules that are responsible for detecting any intrusion attempt. According to Pongle et al., [71], network nodes are to blame for any observable shifts in their immediate vicinity. Additionally, network nodes communicated neighbourhood details to a centrally located module hosted by a border router tasked with data storage and analysis. This facilitates the detection of intrusions and the early detection of attacks. Thanigaivelan et al. presented an IDS in [72] that divides tasks between individual nodes and the router's perimeter. The IDS module can monitor its neighbouring nodes, looking for signs of intrusion and alerting its fellow IDS modules if it finds any.

3. RESEARCH TRENDS AND DIRECTION

The prominent feature and detection techniques of the selected papers have been presented in Table 1 to determine the central concepts underpinning the research.

 doi:10.20944/preprints202309.0611.v1

Table 1. Summary of the selected papers based on the Main Concept, Feature, and Limitation.

SL#	Literature Work	Target System	Attacks	Detection Techniques
1	The 2015 Ukraine Blackout [3]	The SCADA of the Ukraine Grid	False Data Injection (FDI) and Denial-of Services (DoS)	Not provided
2	IDS Framework [26]	HAN and NAN and many IDS sensors in WAN.	Denial-of Services (DoS)	Anomaly based.
3	IDS for Advanced Metering Infrastructure [73]	Advanced metering infrastructure (AMI)	Denial-of Services (DoS)	Data-Stream based
4	Bloom Filter Based IDS [74]	SCADA	HMI compromise, Man-in-the-middle attack	Anomaly based
5	Cyber Security Solution towards IDS [75]	DNP3 in SCADA	Length Overflow Attack, DFC Flag Attack, and Reset Function Attack	Protocol-based detection rules
6	The Snort detection rule template for anomaly DNP3 [76]	DNP3 in SCADA	Protocol anomalies, reconnaissance attack, Denial-of Services (DoS) attack	Signature-based
7	A Stateful Analysis Framework of IDS [77]	Substation	Denial-of Services (DoS), Port scanning, MMS, SNMP attacks	Specification-based
8	Multidimensional IDS [78]	Substation	DoS, MiTM, Packet Injection attacks	Specification-based
9	IDS based on log sequence clustering of honeypot [79]	Modbus TCP in SCADA	Reconnaissance, DoS attacks	Anomaly based
10	A nifty collaborative IDS [80]	Entire SG	DoS, Packet splitting, Command injection, Duplicate insertion, Payload mutation	Anomaly based
11	Support vector machine based IDS [81]	AMI	Worms, Fuzzer, DoS, Backdoor attacks	Anomaly based
12	IDS for blackhole attacks in a smart grid [5]	AMI	Blackhole attack	Anomaly based
13	Case analysis based IDS for SG [9]	AMI	L2l, DoS, Botnet, Secure shell attacks	Anomaly based
14	Real-time anomaly-based distributed IDS for AMI [82]	AMI	Port scanning, DoS attacks	Anomaly based
15	IDS and prevention for ZigBee-based home area networks in SG [83]	AMI	Spoofing, Radio Jamming, Replay, Black-off manipulation	Specification-based
16	Machine learning-based IDS on an industrial Modbus/TCP data set [15]	Modbus TCP in SCADA	Reconnaissance, DoS attacks	Anomaly based
17	The IDS for Profinet DCP [84]	Profinet in SCADA	Reconnaissance, DoS, MiTM, Protocol anomalies	HYbrid
18	Data mining methods to detect simulated intrusions on a Modbus network [85]	Modbus TCP in SCADA	Reconnaissance, DoS, Command injection, Response injection attacks	Anomaly based
19	A behavior-based intrusion detection technique for smart grid infrastructure [86]	Substation	Port scanning, DoS, GOOSE, MMS, SNMP attacks	Specification based
20	Power utility automation cybersecurity: IEC 61850 specification of an IDS [12]	Substation	Not provided	Specification based
21	IDS of cyber intrusions using network-based multicast messages for substation automation [87]	Substation	Replay, DoS attacks	Specification based
22	IDS for IEC 61850 based smart substations [11]	Substation	Packet injection, MiTM, DoS attacks	Specification based
23	a hybrid IDS using data mining for power systems [88]	Synchrophasor	Single-line-to-ground faults, Replay attack, Command injection, Disable relay attack	Hybrid
24	Model based IDS for synchrophasor applications in SG [19]	Synchrophasor	ARP spoofing, Port scanning, GPS scanning, Replay attack, Command injection, Physical attacks	Hybrid
25	IDS for network security in synchrophasor [20]	Synchrophasor	Reconnaissance, MiTM, DoS attacks	Specification based
26	Accurate modeling of Modbus/TCP for IDS in SCADA [89]	Modbus TCP in SCADA	Not provided	Anomaly based
27	Stateful IDS for IEC 60870-5-104 SCADA security [90]	SCADA	Packet injection, Replay attack, Data manipulation	Specification based
28	IDS for IEC 60870-5-104 based SCADA networks [91]	SCADA	Unauthorized read/reset command, Spontaneous packet storm, Buffer overflow	Hybrid

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 September 2023 doi:10.20944/preprints202309.0611.v1

This study discusses various aspects of recent research on IDS for the SG system. However, most of the IDS system is more likely to focus on the communication network of the SG system. The following gaps have been identified from the literature overview.

- AMI relies on the flow of ICT that facilitates two-way communication between power distributors and consumers. It is severely vulnerable to various kinds of attacks and threats. So, the security issues related to AMI connectivity, data integrity, and availability are at stake. AMI has not been prioritized well in recent research on IDS in the SG domain, a crucial application component of SG. To our knowledge, no sheer number of research or work on the IDS focuses on the AMI.
- Lack of research addressing how to map the intrusion process to the complex smart grid architecture.
- Lack of research on eliminating False positives for fluctuations of smart meter (SM) data at the AMI headend.
- No significant idea has been found addressing the scalability issue for the IDS in the SG system.
- As the SG is a vast system, very few computational analyses have been found considering the compatibility issues incorporated with any new IDS into the SG system.

Upon analyzing the gaps above, an IDS is proposed in this study where the AMI is subjected as a target for any intrusion. As AMI is widely spread everywhere and due to its physically accessible properties, it is vulnerable to a wide range of threats and attacks. The main idea is to detect unusual patterns or anomalies from the SG system's smart meter data from the AMI headend. Recognizing consumer load patterns from SM data regarding abnormality or anomaly detection can be pivotal in developing a robust IDS in this domain. Hence, one feasible strategy has been suggested to detect intrusion based on SM data anomalies and load patterns and deploy the IDS model accordingly. Since the AMI deals with a large amount of data collected daily, it plays a strong indicator in evaluating the grid's functioning and operation in case of any intrusion. The suggested model of IDS is depicted in Figure 7.

The proposed IDS model is entirely process-oriented and is described as follows:

- The data gathered from SM should be considered while developing a generative model for identifying intrusion based on anomaly detection—the AMI headend and data collectors with an installed IDS made up of the proposed system. In the first stage, the IDS units monitor network traffic between the data collectors and the smart meters. After spotting potential anomalous flows, they transmit their findings to the AMI headend's IDS department. The latter then analyses the anomalies and triggers an intrusion alarm. The entire system is based on the state-of-the-art of machine learning, which has three phases: a) training, b) testing, and c) analysis and response action.
- In more detail, the goal of the first module is to use a Bayesian Network to monitor communication traffic, identify attack activities, and train the model. It specifically keeps track of the number of data collector requests, the time, and the ID of smart meters. The second module tests the model with testing data and evaluates the outcomes. In the third module, secondary analysis is done upon careful analysis of the pattern of anomalies from the modelled data. It generates intrusion alarms associated with the decision taken from the investigation before. To evaluate the system, two kinds of attacks, a) attacks on commands and b) attacks on data, will be performed behaviour simulated in an environment that would generate anomalous consumption metrics indicating intrusion caused by these assaults. Suppose a potential cyberattack or unusual behaviour is identified. In that case, the alarm will be triggered immediately, estimating the system's state into three levels of indication of intrusion: a) normal, b) abnormal, and c) uncertain.
- The proposed IDS generates an alarm whenever an irregularity deviates from or does not match the normalized baseline. This is certainly a unique component of this model when the abnormality exceeds the threshold values for each meter data. The decision tree technique would be considered to implement this part of the model.

 doi:10.20944/preprints202309.0611.v1

- These alerts can also be sent off by unexpected user logins, new IP addresses trying to join the intelligent grid network, newly added devices accepted to the network without permission, and other events. Because they alert to even the most negligible abnormal behaviour in the network, anomaly-based intrusion detection solutions may have more excellent false-positive rates.
- For another single system, it is much easier to deploy IDS in commodity networks because of lots of bandwidth everywhere and lots of computational power. However, in the SG, some parts of the network have very little bandwidth, particularly at the AMI. Likewise, many devices have low computational power.
- For full-fledged intrusion detection, we need to consider this compatibility issue of the IDS within the SG system. Our proposed model consists of two parts. The computationally intensive part would be deployed in AMI headend, where a lot of bandwidth can handle big data. The utility end would be employed in the last part of generating an intrusion alarm. This is computationally less hard where the outcome from the first phase would be less amount of data that can be dealt with the low amount of bandwidth,
- Considering the issue with the scalability, we recommend our intrusion detection methodology be mapped to the SG architecture. As AMI is widely segregated and easily accessible to anyone, it is important to address the scalability issue here. The first phase of our proposed intrusion detection technique can be deployed distributively in each AMI, where the machine learning model will be applied right after the data collection process. The last phase would be performed at the utility end with a rigorous analysis of the outcome from the prior phase to eliminate False positives for fluctuations of meter data and generate an alarm based on the decision model.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 September 2023 doi:10.20944/preprints202309.0611.v1

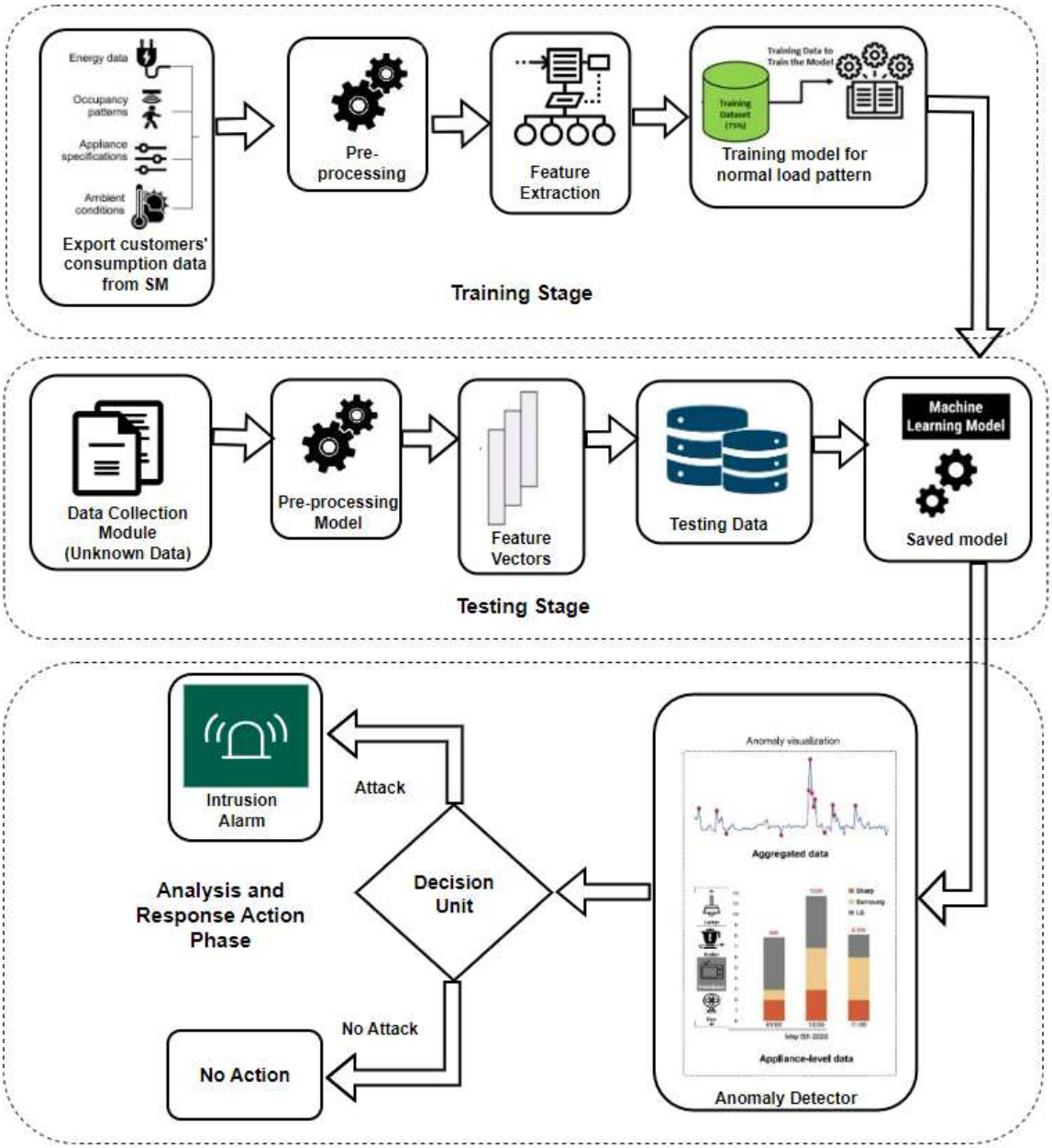

Figure 7. Intrusion detection technique based on SM data.

4. Conclusions

This paper summarizes recent research on intrusion detection systems for SG systems. Due to the complex, heterogeneous, and interconnectivity among the wide ranges of system components, implementation and deployment of IDS in the SG is highly challenging compared to other systems. To recover key systems quickly after an attack, the IDS countermeasure must be able to identify and prevent attacks in real-time. Besides highlighting the most common methodologies of the existing IDS along with their limitations and strengths. This paper recommends a proactive approach as a future research direction for detecting intrusion targeting the AMI application of the SG system. The key element of this approach is based on smart meter (SM) data using machine learning techniques. This approach aims to analyze any anomaly or irregular pattern in the consumers' power consumption behaviour and mark this as a critical status that the IDS can detect "zero-day intrusion or attack." The type or class of intrusion can be detected in the consecutive phase depending on the degree of

anomalies. The degree of anomalies will follow the intrusion alarm generated from the proposed model.

References

1. Avi, Avi Gopstein, Cuong Nguyen, Danielle Sass Byrnett, Kerry Worthington, and Villarreal Christopher. *Framework and roadmap for smart grid interoperability standards regional roundtables summary report*. US Department of Commerce, National Institute of Standards and Technology, 2020.
2. Jesús Lázaro, Armando Astarloa, Mikel Rodríguez, Unai Bidarte, and Jaime Jiménez. A survey on vulnerabilities and countermeasures in the communications of the smart grid. *Electronics*, 10(16):1881, 2021.
3. Defense Use Case. Analysis of the cyber attack on the ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 388(1-29):3, 2016.
4. Gregg Keizer. Is stuxnet the best malware ever? 2010.
5. Nadia Boumkheld, Mounir Ghogho, and Mohammed El Koutbi. Intrusion detection system for the detection of blackhole attacks in a smart grid. In *2016 4th International Symposium on Computational and Business Intelligence (ISCBI)*, pages 108–111. IEEE, 2016.
6. Priti Prabhakar, Sujata Arora, Anita Khosla, Rajender Kumar Beniwal, Moses Ndole Arthur, José Luis Arias-Gonzáles, Franklin Ore Areche, et al. Cyber security of smart metering infrastructure using median absolute deviation methodology. *Security and Communication Networks*, 2022, 2022.
7. James P Anderson. Computer security threat monitoring and surveillance. *Technical Report, James P. Anderson Company*, 1980.
8. Zhong Fan, Parag Kulkarni, Sedat Gormus, Costas Efthymiou, Georgios Kalogridis, Mahesh Sooriyabandara, Ziming Zhu, Sangarapillai Lambotharan, and Woon Hau Chin. Smart grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Communications Surveys & Tutorials*, 15(1):21–38, 2012.
9. Panagiotis I Radoglou-Grammatikis and Panagiotis G Sarigiannidis. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *Ieee Access*, 7:46595–46620, 2019.
10. V Cagri Gungor, Dilan Sahin, Taskin Kocak, Salih Ergut, Concettina Buccella, Carlo Cecati, and Gerhard P Hancke. A survey on smart grid potential applications and communication requirements. *IEEE Transactions on industrial informatics*, 9(1):28–42, 2012.
11. Yi Yang, Kieran McLaughlin, Lei Gao, Sakir Sezer, Yubo Yuan, and Yanfeng Gong. Intrusion detection system for iec 61850 based smart substations. In *2016 IEEE Power and Energy Society General Meeting (PESGM)*, pages 1–5. IEEE, 2016.
12. Maelle Kabir-Querrec, Stéphane Mocanu, Jean-Marc Thiriet, and Eric Savary. Power utility automation cybersecurity: Iec 61850 specification of an intrusion detection function. In *ESREL 2015-25th European Safety and Reliability Conference*. CRC Press, 2015.
13. Hyunguk Yoo and Taeshik Shon. Novel approach for detecting network anomalies for substation automation based on iec 61850. *Multimedia Tools and Applications*, 74:303–318, 2015.
14. Ersi Hodo, Stepan Grebeniuk, Henri Ruotsalainen, and Paul Tavolato. Anomaly detection for simulated iec-60870-5-104 trafiic. In *Proceedings of the 12th international conference on availability, reliability and security*, pages 1–7, 2017.
15. Simon Duque Anton, Suneetha Kanoor, Daniel Fraunholz, and Hans Dieter Schotten. Evaluation of machine learning-based anomaly detection algorithms on an industrial modbus/tcp data set. In *Proceedings of the 13th international conference on availability, reliability and security*, pages 1–9, 2018.
16. Antoine Lemay and José M Fernandez. Providing {SCADA} network data sets for intrusion detection research. In *9th Workshop on Cyber Security Experimentation and Test (CSET 16)*, 2016.
17. Abolfazl Rahiminejad, Jordan Plotnek, Ribal Atallah, Marc-André Dubois, Dorian Malatrait, Mohsen Ghafouri, Arash Mohammadi, and Mourad Debbabi. A resilience-based recovery scheme for smart grid restoration following cyberattacks to substations. *International Journal of Electrical Power & Energy Systems*, 145:108610, 2023.

18. Petr Matoušek. Description of iec 61850 communication. In *Technical Report*. Brno University of Technology, 2018.
19. Rafiullah Khan, Abdullah Albalushi, Kieran McLaughlin, David Laverty, and Sakir Sezer. Model based intrusion detection system for synchrophasor applications in smart grid. In *2017 IEEE Power & Energy Society General Meeting*, pages 1–5. IEEE, 2017.
20. Yu Yang, Kieran McLaughlin, Sakir Sezer, Timothy Littler, Bernardi Pranggono, Paul Brogan, and HF Wang. Intrusion detection system for network security in synchrophasor systems. 2013.
21. Zakaria El Mrabet, Naima Kaabouch, Hassan El Ghazi, and Hamid El Ghazi. Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering*, 67:469–482, 2018.
22. Weiming Tong, Lei Lu, Zhongwei Li, Jingbo Lin, and Xianji Jin. A survey on intrusion detection system for advanced metering infrastructure. In *2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)*, pages 33–37. IEEE, 2016.
23. Paria Jokar, Hasen Nicanfar, and Victor CM Leung. Specification-based intrusion detection for home area networks in smart grids. In *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 208–213. IEEE, 2011.
24. Mustafa Amir Faisal, Zeyar Aung, John R Williams, and Abel Sanchez. Securing advanced metering infrastructure using intrusion detection system with data stream mining. In *Intelligence and Security Informatics: Pacific Asia Workshop, PAISI 2012, Kuala Lumpur, Malaysia, May 29, 2012. Proceedings*, pages 96–111. Springer, 2012.
25. Ke Zhang, Zhi Hu, Yufei Zhan, Xiaofen Wang, and Keyi Guo. A smart grid ami intrusion detection strategy based on extreme learning machine. *Energies*, 13(18):4907, 2020.
26. Imtiaz Ullah and Qusay H Mahmoud. An intrusion detection framework for the smart grid. In *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–5. IEEE, 2017.
27. Abdulla Amin Aburomman and Mamun Bin Ibne Reaz. A survey of intrusion detection systems based on ensemble and hybrid classifiers. *Computers & security*, 65:135–152, 2017.
28. Chenfeng Vincent Zhou, Christopher Leckie, and Shanika Karunasekera. A survey of coordinated attacks and collaborative intrusion detection. *computers & security*, 29(1):124–140, 2010.
29. Junaid Arshad, Muhammad Ajmal Azad, Roohi Amad, Khaled Salah, Mamoun Alazab, and Razi Iqbal. A review of performance, energy and privacy of intrusion detection systems for iot. *Electronics*, 9(4):629, 2020.
30. Daniel S Berman, Anna L Buczak, Jeffrey S Chavis, and Cherita L Corbett. A survey of deep learning methods for cyber security. *Information*, 10(4):122, 2019.
31. Anna L Buczak and Erhan Guven. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, 18(2):1153–1176, 2015.
32. Robert Mitchell and Ray Chen. A survey of intrusion detection in wireless network applications. *Computer Communications*, 42:1–23, 2014.
33. Mohamed I Ibrahem, Sherif Abdelfattah, Mohamed Mahmoud, and Waleed Alasmary. Detecting electricity theft cyber-attacks in cat ami system using machine learning. In *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6. IEEE, 2021.
34. Soo Wan Yen, Stella Morris, Morris AG Ezra, and Tang Jun Huat. Effect of smart meter data collection frequency in an early detection of shorter-duration voltage anomalies in smart grids. *International journal of electrical power & energy systems*, 109:1–8, 2019.
35. Shampa Banik, Sohag Kumar Saha, Trapa Banik, and SM Hossain. Anomaly detection techniques in smart grid systems: A review. *arXiv preprint arXiv:2306.02473*, 2023.
36. Gaoqi Liang, Junhua Zhao, Fengji Luo, Steven R Weller, and Zhao Yang Dong. A review of false data injection attacks against modern power systems. *IEEE Transactions on Smart Grid*, 8(4):1630–1638, 2016.
37. Danda B Rawat and Chandra Bajracharya. Detection of false data injection attacks in smart grid communication systems. *IEEE Signal Processing Letters*, 22(10):1652–1656, 2015.
38. Ercan Nurcan Ylmaz, Bünyamin Ciylan, Serkan Gönen, Erhan Sindiren, and Gökçe Karacayılmaz. Cyber security in industrial control systems: Analysis of dos attacks against plcs and the insider effect. In *2018 6th international istanbul smart grids and cities congress and fair (icsg)*, pages 81–85. IEEE, 2018.
39. K Narasimha Mallikarjunan, K Muthupriya, and S Mercy Shalinie. A survey of distributed denial of service attack. In *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, pages 1–6. IEEE, 2016.

40. Patrick Wlazlo, Abhijeet Sahu, Zeyu Mao, Hao Huang, Ana Goulart, Katherine Davis, and Saman Zonouz. Man-in-the-middle attacks and defence in a power system cyber-physical testbed. *IET Cyber-Physical Systems: Theory & Applications*, 6(3):164–177, 2021.
41. Shampa Banik, Trapa Banik, SM Hossain, and Sohag Kumar Saha. Implementing man-in-the-middle attack to investigate network vulnerabilities in smart grid test-bed. *arXiv preprint arXiv:2306.00234*, 2023.
42. Junfeng Zhao, Jing Wang, and Lei Yin. Detection and control against replay attacks in smart grid. In *2016 12th International Conference on Computational Intelligence and Security (CIS)*, pages 624–627. IEEE, 2016.
43. Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2011.
44. Modbus Application Protocol Specification. V1. 1b. *Modbus Organization*, 2006.
45. Lindah Kotut and Luay A Wahsheh. Survey of cyber security challenges and solutions in smart grids. In *2016 cybersecurity symposium (CYBERSEC)*, pages 32–37. IEEE, 2016.
46. Ross Anderson and Shailendra Fuloria. Who controls the off switch? In *2010 First IEEE International Conference on Smart Grid Communications*, pages 96–101. IEEE, 2010.
47. Eric H Allen, Robert B Stuart, and Thomas E Wiedman. No light in august: power system restoration following the 2003 north american blackout. *IEEE Power and Energy Magazine*, 12(1):24–33, 2013.
48. Lipi Chhaya, Paawan Sharma, Govind Bhagwatikar, and Adesh Kumar. Wireless sensor network based smart grid communications: Cyber attacks, intrusion detection system and topology control. *Electronics*, 6(1):5, 2017.
49. R Vijayanand, D Devaraj, and B Kannapiran. Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection. *Computers & Security*, 77:304–314, 2018.
50. JE Albuquerque Filho, Laislla CP Brandão, Bruno JT Fernandes, and Alexandre MA Maciel. A review of neural networks for anomaly detection. *IEEE Access*, 2022.
51. Mohamed Attia, Hichem Sedjelmaci, Sidi Mohammed Senouci, and El-Hassane Aglzim. A new intrusion detection approach against lethal attacks in the smart grid: temporal and spatial based detections. In *2015 Global Information Infrastructure and Networking Symposium (GIIS)*, pages 1–3. IEEE, 2015.
52. Chih-Che Sun, Adam Hahn, and Chen-Ching Liu. Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, 99:45–56, 2018.
53. Dorothy E Denning. An intrusion-detection model. *IEEE Transactions on software engineering*, (2):222–232, 1987.
54. Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. *ACM computing surveys (CSUR)*, 41(3):1–58, 2009.
55. Panagiotis Radoglou Grammatikis, Panagiotis Sarigiannidis, Georgios Efstathopoulos, and Emmanouil Panaousis. Aries: A novel multivariate intrusion detection system for smart grid. *Sensors*, 20(18):5305, 2020.
56. Shengyi Pan, Thomas H Morris, and Uttam Adhikari. A specification-based intrusion detection framework for cyber-physical environment in electric power system. *Int. J. Netw. Secur.*, 17(2):174–188, 2015.
57. Robin Berthier and William H Sanders. Specification-based intrusion detection for advanced metering infrastructures. In *2011 IEEE 17th Pacific rim international symposium on dependable computing*, pages 184–193. IEEE, 2011.
58. Nitasha Sahani, Ruoxi Zhu, Jin-Hee Cho, and Chen-Ching Liu. Machine learning-based intrusion detection for smart grid computing: A survey. *ACM Transactions on Cyber-Physical Systems*, 7(2):1–31, 2023.
59. Safa Otoum, Burak Kantarci, and Hussein T Mouftah. Mitigating false negative intruder decisions in wsn-based smart grid monitoring. In *2017 13th International wireless communications and mobile computing conference (IWCMC)*, pages 153–158. IEEE, 2017.
60. Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga. A survey of intrusion detection in internet of things. *Journal of Network and Computer Applications*, 84:25–37, 2017.
61. Ashfaq Hussain Farooqi and Farrukh Aslam Khan. Intrusion detection systems for wireless sensor networks: A survey. In *International Conference on Future Generation Communication and Networking*, pages 234–241. Springer, 2009.

62. Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A Spirito, and Mark Vinkovits. Denial-of-service detection in 6lowpan based internet of things. In *2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)*, pages 600–607. IEEE, 2013.
63. Prabhakaran Kasinathan, Gianfranco Costamagna, Hussein Khaleel, Claudio Pastrone, and Maurizio A Spirito. An ids framework for internet of things empowered by 6lowpan. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 1337–1340, 2013.
64. Linus Wallgren, Shahid Raza, and Thiemo Voigt. Routing attacks and countermeasures in the rpl-based internet of things. *International Journal of Distributed Sensor Networks*, 9(8):794326, 2013.
65. Doohwan Oh, Deokho Kim, and Won Woo Ro. A malicious pattern detection engine for embedded security systems in the internet of things. *Sensors*, 14(12):24188–24211, 2014.
66. Tsung-Han Lee, Chih-Hao Wen, Lin-Huang Chang, Hung-Shiou Chiang, and Ming-Chun Hsieh. A lightweight intrusion detection scheme based on energy consumption analysis in 6lowpan. In *Advanced Technologies, Embedded and Multimedia for Human-centric Computing: HumanCom and EMC 2013*, pages 1205–1213. Springer, 2014.
67. Christian Cervantes, Diego Poplade, Michele Nogueira, and Aldri Santos. Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pages 606–611. IEEE, 2015.
68. Jean-Paul A Yaacoub, Ola Salman, Hassan N Noura, Nesrine Kaaniche, Ali Chehab, and Mohamad Malli. Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems*, 77:103201, 2020.
69. Anhtuan Le, Jonathan Loo, Kok Keong Chai, and Mahdi Aiash. A specification-based ids for detecting attacks on rpl-based network topology. *Information*, 7(2):25, 2016.
70. Shahid Raza, Linus Wallgren, and Thiemo Voigt. Svelte: Real-time intrusion detection in the internet of things. *Ad hoc networks*, 11(8):2661–2674, 2013.
71. Pavan Pongle and Gurunath Chavan. Real time intrusion and wormhole attack detection in internet of things. *International Journal of Computer Applications*, 121(9), 2015.
72. Nanda Kumar Thanigaivelan, Ethiopia Nigussie, Rajeev Kumar Kanth, Seppo Virtanen, and Jouni Isoaho. Distributed internal anomaly detection system for internet-of-things. In *2016 13th IEEE annual consumer communications & networking conference (CCNC)*, pages 319–320. IEEE, 2016.
73. Mustafa Amir Faisal, Zeyar Aung, John R Williams, and Abel Sanchez. Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study. *IEEE Systems journal*, 9(1):31–44, 2014.
74. Saranya Parthasarathy and Deepa Kundur. Bloom filter based intrusion detection for smart grid scada. In *2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–6. IEEE, 2012.
75. Xiao Chun Yin, Zeng Guang Liu, Lewis Nkenyereye, and Bruce Ndibanje. Toward an applied cyber security solution in iot-based smart grids: An intrusion detection system approach. *Sensors*, 19(22):4952, 2019.
76. Hao Li, Guangjie Liu, Weiwei Jiang, and Yuewei Dai. Designing snort rules to detect abnormal dnp3 network data. In *2015 International Conference on Control, Automation and Information Sciences (ICCAIS)*, pages 343–348. IEEE, 2015.
77. BooJoong Kang, Kieran McLaughlin, and Sakir Sezer. Towards a stateful analysis framework for smart grid network intrusion detection. In *4th International Symposium for ICS & SCADA Cyber Security Research 2016 4*, pages 124–131, 2016.
78. Yi Yang, Hai-Qing Xu, Lei Gao, Yu-Bo Yuan, Kieran McLaughlin, and Sakir Sezer. Multidimensional intrusion detection system for iec 61850-based scada networks. *IEEE Transactions on Power Delivery*, 32(2):1068–1078, 2016.
79. Pin-Han Wang, I-En Liao, Kuo-Fong Kao, and Jyun-Yao Huang. An intrusion detection method based on log sequence clustering of honeypot for modbus tcp protocol. In *2018 IEEE International Conference on Applied System Invention (ICASI)*, pages 255–258. IEEE, 2018.
80. Ahmed Patel, Hitham Alhussian, Jens Myrup Pedersen, Bouchaib Bounabat, Joaquim Celestino Júnior, and Sokratis Katsikas. A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems. *Computers & Security*, 64:92–109, 2017.

81. R Vijayanand, D Devaraj, and B Kannapiran. Support vector machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid. In *2017 4th International conference on advanced computing and communication systems (ICACCS)*, pages 1–7. IEEE, 2017.
82. Fadwa Abdul Aziz Alseiari and Zeyar Aung. Real-time anomaly-based distributed intrusion detection systems for advanced metering infrastructure utilizing stream data mining. In *2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, pages 148–153. IEEE, 2015.
83. Paria Jokar and Victor CM Leung. Intrusion detection and prevention for zigbee-based home area networks in smart grids. *IEEE Transactions on Smart Grid*, 9(3):1800–1811, 2016.
84. Zihao Feng, Sujuan Qin, Xuesong Huo, Pei Pei, Ye Liang, and Liming Wang. Snort improvement on profinet rt for industrial control system intrusion detection. In *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, pages 942–946. IEEE, 2016.
85. Szu-Chuang Li, Yennun Huang, Bo-Chen Tai, and Chi-Ta Lin. Using data mining methods to detect simulated intrusions on a modbus network. In *2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2)*, pages 143–148. IEEE, 2017.
86. YooJin Kwon, Huy Kang Kim, Yong Hun Lim, and Jong In Lim. A behavior-based intrusion detection technique for smart grid infrastructure. In *2015 IEEE Eindhoven PowerTech*, pages 1–6. IEEE, 2015.
87. Junho Hong, Chen-Ching Liu, and Manimaran Govindarasu. Detection of cyber intrusions using network-based multicast messages for substation automation. In *ISGT 2014*, pages 1–5. IEEE, 2014.
88. Shengyi Pan, Thomas Morris, and Uttam Adhikari. Developing a hybrid intrusion detection system using data mining for power systems. *IEEE Transactions on Smart Grid*, 6(6):3104–3113, 2015.
89. Niv Goldenberg and Avishai Wool. Accurate modeling of modbus/tcp for intrusion detection in scada systems. *international journal of critical infrastructure protection*, 6(2):63–75, 2013.
90. Y Yang, K McLaughlin, S Sezer, YB Yuan, and W Huang. Stateful intrusion detection for iec 60870-5-104 scada security. In *2014 IEEE PES General Meeting | Conference & Exposition*, pages 1–5. IEEE, 2014.
91. Yi Yang, Kieran McLaughlin, Tim Littler, Sakir Sezer, Bernardi Pranggono, and HF Wang. Intrusion detection system for iec 60870-5-104 based scada networks. In *2013 IEEE power & energy society general meeting*, pages 1–5. Ieee, 2013.