# Network Security Challenges and Countermeasures for Software-Defined Smart Grids: A Survey

Dennis Agnew , Sharon Boamah , Arturo Bretas * , Janise McNair

Posted Date: 28 March 2024

doi: 10.20944/preprints202403.1701.v1

Keywords: smart grid; software-defined networking; network security; cybersecurity

*Article*

# Network Security Challenges and Countermeasures for Software-Defined Smart Grids: A Survey

**Dennis Agnew [1], Sharon Boamah [1], Arturo Bretas [1,2,3,*] and Janise McNair [1]**

[1] Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL
[2] Electric Grid Security and Communications, Sandia National Laboratories, Albuquerque, NM
[3] G2Elab, Grenoble INP, CNRS, Université Grenoble Alpes, 38000 Grenoble, France
* Correspondence: asbreta@sandia.gov

**Abstract:** Grid modernization has been ushered in by rising electricity consumption, deteriorating infrastructure, and increasing reliability concerns for electric utilities. New advances, collectively referred to as the smart grid, include modern electronics, technology, telecommunications, and computing capabilities. Smart grid telecommunication frameworks provide two-way communication to support grid operations. Software-defined networking (SDN) has been proposed as a method of monitoring and controlling telecommunication networks, enabling increased smart grid visibility, control, and security. However, being connected to telecommunications infrastructure means that smart grid networks are exposed to cyber-attacks. Attackers may use unauthorized access to intercept messages, inject false data into system measurements, flood communication channels with false data packets, or target centralized controllers to cripple network control. Defense and security techniques against these threats are constantly evolving, necessitating an up-to-date, comprehensive study analyzing cyber attacks and defense methods for smart grid networks. Previous smart grid security surveys do not contain recent techniques and to our knowledge most, if not all, address only one type of attack type and/or one type of defense. This survey considers the latest security techniques, simultaneous multi-pronged cyber attacks and defense utilities to meet the challenges of the next-generation SDN smart grid research with the goal of identifying future research needs, describing the open security challenges, and exposing both emerging threats and their potential impact on SD-SG deployment.

**Keywords:** smart grid; software-defined networking; network security; cybersecurity

## 1. Introduction

Rising electricity consumption, deteriorating infrastructure, and increasing reliability concerns have inspired new advances in grid modernization and new deployments of smart grids (SG) to replace conventional power grids. According to the US Department of Energy, SGs will enable utilities to do wide-ranging data collection and implement widespread electrical system control in real-time, resulting in more reliable electricity for all grid users. While traditional power grids suffer from outdated, unreliable equipment, and require manual administration and frequent power outages, the use of SGs introduces a variety of modern technologies, such as IoT sensors, analytic processes, including machine learning, and new control systems, to more effectively monitor and manage energy consumption, generation, and distribution [1]. There are still several challenges in SG, such as the time-consuming and tedious need for manual network administration. Furthermore, SG networks are made up of hardware and software from various vendors, which can result in interoperability issues for contact between those devices.

Current research efforts have proposed the use of software-defined networking (SDN) techniques to improve SG performance [1,2]. SDN is a network design technique that allows networks to be intelligently controlled, or programmed, through the use of software applications and a network controller function that is separate from network data delivery functions. This allows for greater flexibility, adaptability, and scalability in network infrastructure management [3]. Figure 1 illustrates a Software-Defined Smart Grid (SD-SG) architecture. A centralized software controller manages and configures all SG network devices and protocols. The application plane can be used to perform real-

 doi:10.20944/preprints202403.1701.v1



time monitoring and analysis, allowing for proactive identification and resolution of SG network issues [4]. The upper layer analysis and control functions can then be used to implement SG network policy in terms of data movement or storage, telecommunications, energy movement or storage, and customer prioritization. While existing SDN research can provide general security response solutions, SD-SG are susceptible to a range of utility-specific cyber attacks such as distributed denial of service (DDoS), unauthorized access, false data injection, etc [5]. Furthermore, the introduction of SDN introduces the SD-SG to additional attacks that target the controller or other specific elements of the SDN network. SGs have a significant impact on the lives of numerous persons. Renewable energy sources play a crucial role in providing power to residential areas, supporting commercial enterprises, and aiding service providers in satisfying the escalating requirements for sustainable energy. SG technology has a profound impact on how we live and conduct our daily lives, being deeply ingrained in our modern lives. Therefore, the consequences of cyber attacks, even in an SD-SG system could include severe consequences, ranging from power outages for customers, to widespread stoppage of service and millions of dollars of damages for providers [6].

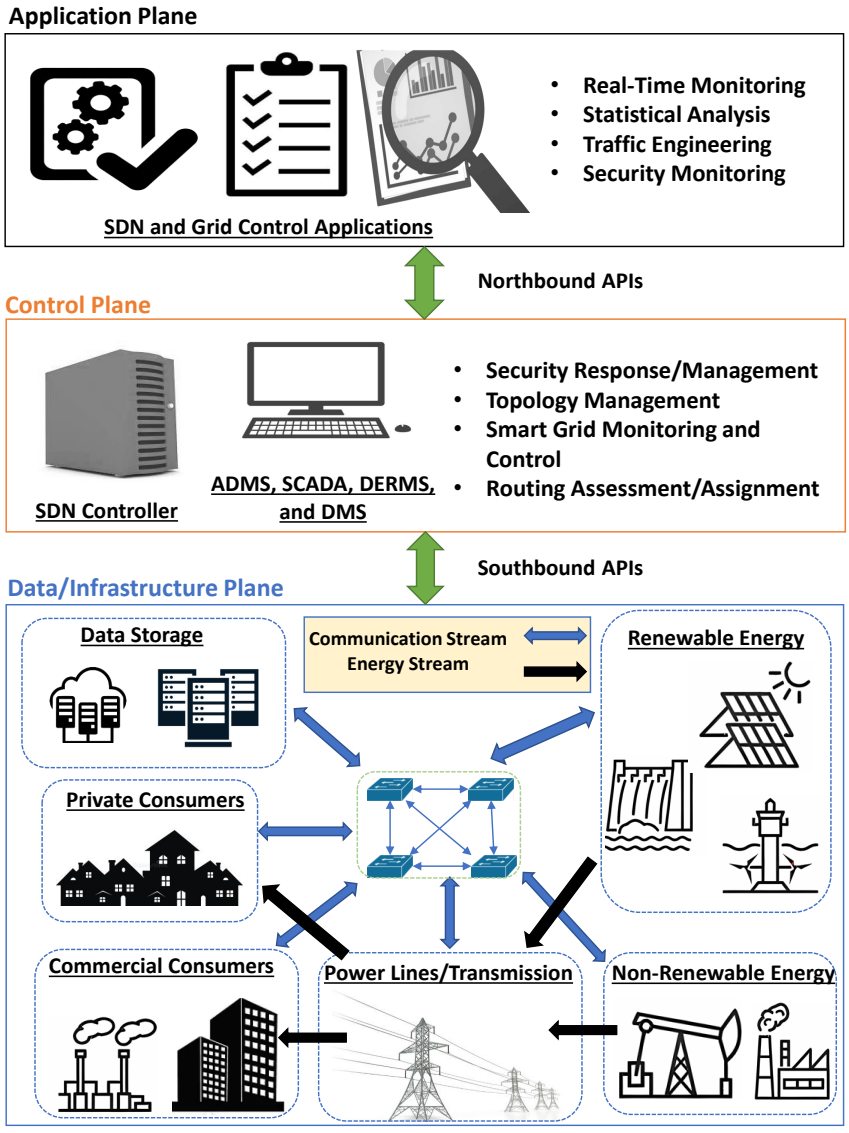



**Figure 1.** A Software-Defined Smart Grid (SD-SG) Architecture.

There is a need for a review that centralizes, summarizes, and analyzes these approaches for the development of future efforts. Past surveys on security in smart grid networks either only briefly touch

 doi:10.20944/preprints202403.1701.v1



on network security, are now outdated and do not contain recent techniques and attack types, or at the time faced a body of literature that addressed only one type of cyber attack, e.g., Denial-of-Service (DoS), and/or one type of defense per study [1,7–11]. This survey fills the gap in this void by providing a comprehensive, up-to-date survey of current cyber threats to SD-SG networks as well as novel future directions and open challenges for SD-SG network security research. The contributions of this survey are as follows:

- An updated survey of cyber attacks affecting SD-SG and current SD-SG mitigation techniques.
- A novel discussion of defense systems that consider multi-pronged cyberattacks and defenses that can be applied to various types of SD-SG networks.
- A review of open challenges of SD-SG cybersecurity and potential mitigation techniques for emerging cyberattacks such as low rate denial of service, controller botnet attacks, and black hole attacks for SD-SG network security.

The rest of the paper is organized as follows. Section 2 provides background information of SDN and SD-SG. Section 3 describes related surveys and highlights the contributions of this work. Note that Table 1 presents a list of acronyms and their definitions used throughout the paper. A literature review of SD-SG network security of DDoS/DoS, SDN controller attacks, and multi-pronged cyberattack threats and defense mechanisms are discussed in Section 4, Section 5, and Section 6, respectively. Next, Section 7 presents a discussion of emerging threats on the horizon of SD-SG security solutions. In Section 8, we discuss the open challenges of current SD-SG security solutions. Lastly, the paper is concluded in Section 9.

 doi:10.20944/preprints202403.1701.v1



**Table 1.** List of Acronyms and Definitions.

| Acronyms | Definitions |
|---|---|
| SG | Smart Grid |
| SD-SG | Software-Defined Smart Grid |
| SDN | Software-Defined Networking |
| DDoS | Distributed Denial-of-Service |
| LDoS | Low Rate Denial of Service |
| ICT | Information and Communication Technologies |
| SDWSNs | Software-Defined Wireless Sensor Networks |
| HANs | Home Area Networks |
| NANs | Neighborhood Area Networks |
| WANs | Wide Area Networks |
| APIs | Application Programming Interface |
| ForCES | Forwarding And Control Element Separation |
| PCEP | Path Computation Element Communication Protocol |
| NetConf | Network Configuration Protocol |
| I2RS | Interface to Routing System |
| FML | Flow-Based Management Language |
| RESTful | Representational State Transfer |
| ALTO | Application Layer Traffic Optimization |
| NVP | Nicira Network Virtualization Platform |
| QoS | Quality of Service |
| OVSDB | Open vSwitch Database Management |
| BC | Blockchain |
| POF | Protocol Oblivious Forwarding |
| P2P | Peer-to-Peer Communication |
| RNNs | Deep Recurrent Neural Networks |
| BiLSTM | Bidirectional Long Short RNN |
| SCADA | Supervisory Control and Data Acquisition |
| MTD | Moving Target Defense |
| IDS | Intrusion Detection Systems |
| HIDS | Host IDS |
| SIDS | Signature-Based IDS |
| AIDS | Anomaly-Based IDS |
| ML | Machine Learning |
| SD-CPC | Software-Defined Controller Placement Camouflage |
| VSF | Virtual Security Functions |
| RED | Random Early Detection |
| TCP | Transmission Control Protocol |
| AQM | Active Queue Management |
| C&C | Commmand and Control Channel |
| DNS | Domain Name System |
| DDNS | Dynamic DNS |
| WSN | wireless sensor networks |
| MANETs | mobile ad hoc networks |
| SDDCs | software-defined data centers |
| CECD-AS | Cross-Layer Ensemble CorrDet with Adaptive Statistics |
| FDI | False Data Injection |
| TCP-SYN | Transmission Control Protocol-Synchronize |
| TSA | Time Synchronization Attack |
| MITM | Man-in-the-Middle |

## 2. Background

Network security is a critical component of SG systems which are interconnected with and reliant on communication networks [12,13]. SG provides greater transparency and accessibility to energy providers, allowing effective monitoring and management of energy consumption in real-time[14] and allowing utility companies to provide customers with real-time feedback on energy consumption that will assist customers in making informed decisions about energy usage [15]. These features come from a high-level interdependence between the power grid level and the networking level of SG architectures [5,16,17]. Unfortunately, this high level of inter-dependency creates a system-wide vulnerability to cyber-attack scenarios where an attack in the network may alter the behavior of

 doi:10.20944/preprints202403.1701.v1



the power grid[5]. Furthermore, as the SG infrastructure expands, the network's complexity grows, requiring more sophisticated management tools and expertise to manage network performance [18] with respect to energy demand and supply, network management, customer service, monitoring and control, and real-time data delivery to a variety of locations[19].

Managing the complex infrastructure of an SG can be a daunting task with traditional networking, requiring significant manual intervention and human resources [1]. On the other hand, SDN research has shown rapid improvements and discoveries since its public launch in 2009. Compared to traditional networks, SDN has improved utilization, efficiency of resources, flexibility of network services, and reduced cost of maintenance [20]. Table 2 shows the current research efforts that have proposed the use of SDN techniques to improve SG network security and performance [1,2].

**Table 2.** Comparison of Survey Articles on SD-SG Network Security: ✓designates the topic is covered, ∗ designates the topic is partially covered, and — designate the topic is not covered.

| References | Publication Year | DDoS/DoS Attacks | Controller Attacks | Defense Techniques for each Cyberattack | Defense System Considers Multi-Pronged Attacks | Emerging Threats |
|---|---|---|---|---|---|---|
| [1] | 2019 | — | ∗ | ∗ | — | — |
| [7] | 2017 | ∗ | — | — | — | — |
| [8] | 2015 | — | ∗ | ∗ | — | — |
| [9] | 2019 | ∗ | — | ∗ | — | — |
| [10] | 2018 | ✓ | — | ∗ | — | — |
| [11] | 2015 | — | —- | ∗ | — | — |
| **This Survey** | 2023 | ✓ | ✓ | ✓ | ✓ | ✓ |

### *2.1. Software Defined Networking (SDN)*

SDN is a network management structure that enables user-controlled management of forwarding in network nodes. SDN developed over several decades and was realized by researchers at Stanford University [21–23]. SDN has the following characteristics, illustrated in Figure 2:

- Control plane and data plane are separated from one another.
- The controller acts as the central logic and external entity. Its job is to direct the traffic through the network and maintain the status of the network.
- Forwarding decisions are based on flow policies and not the destination. A flow represents a common set of instructions for the exchange of packets between a source and a destination. SDN controllers provide policies that are used to establish flow tables. The flow tables are then implemented by forwarding devices.
- The network has the ability to be programmed through software applications running on top of the SDN controller.
- Application programming interfaces (APIs) are used to pass information between planes of the SDN infrastructure.

As shown in Figure 2, the infrastructure layer is composed of routers, switches, and access points. This represents the physical network equipment in the network and this layer forms the data plane. The controller communicates with the data plane, i.e., sends instructions to the switches and routers, using southbound programming interfaces (Southbound API) such as OpenFlow [24], ForCES [25], PCEP [26], NetConf [27], or I2RS [28]. If there is more than one controller present, these controllers communicate with each other using Eastbound and Westbound APIs (East/West APIs) such as ALTO [29] or Hyperflow [30]. This allows the controllers to maintain a global view of the network. The topmost layer is the application plane. In this layer, the network operator is able to set the policies for the network, depending on functional applications for various tasks such as energy efficiency, access control, mobility management, and/or security management. The application layer communicates the policies to the network through the control layer using the Northbound APIs such as FML [31], Procera [32], Frenetic [33], and RESTful [29]. Depending on the desired results, the network operator can send the necessary changes to the control layer using these APIs so that the controller can make necessary changes in the infrastructure layer.

 doi:10.20944/preprints202403.1701.v1



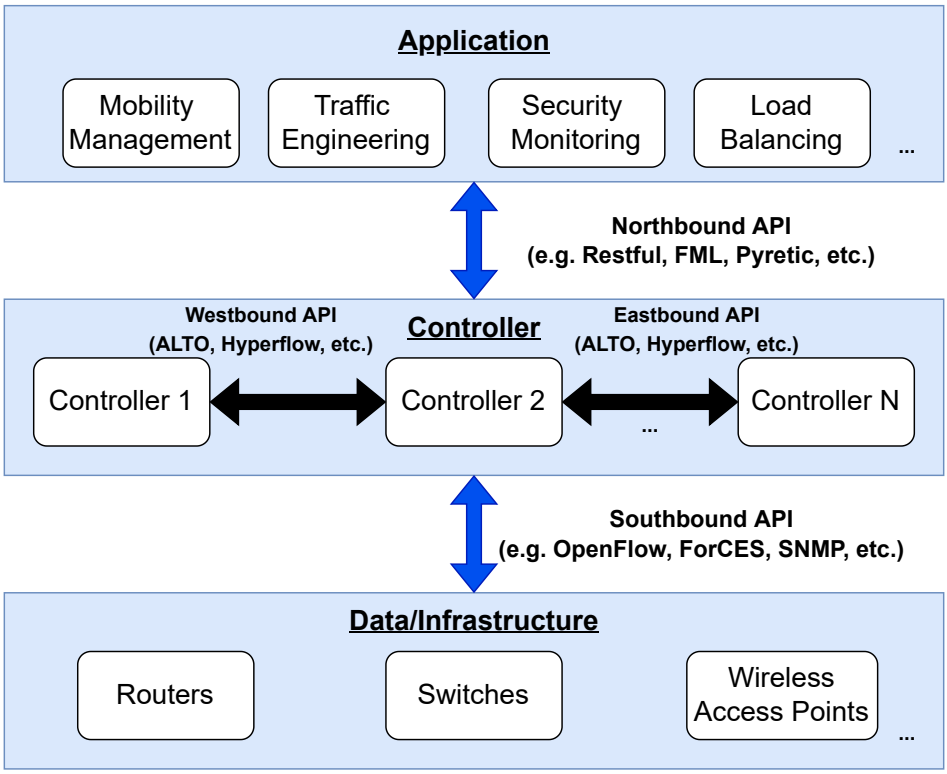



**Figure 2.** General SDN Architecture.

SDN is contrast to traditional networks, wherein flow management, or flow policy, is defined by the forwarding devices. The only way to change this policy is by physically reconfiguring the devices themselves. Because of these hurdles, network management policies in traditional networks are not as dynamic and are difficult to scale. SDN offers the ability to quickly change data flows, enabling the network operator to meet the changing traffic demands.

### *2.2. Software-Defined Smart Grid (SD-SG)*

As aforementioned, SD-SG are a form of SG that utilizes SDN technology to better manage bus communications, network topology organization, security, and grid network visibility and control. Furthermore, SD-SG can leverage the data analytic processes available with SDN to control the grid's communication layer. A high-level overview of this integration and SDN within a SG can be seen in Figure 1. Each layer as it pertains to SD-SG can be defined as follows:

- ***Infrastructure/Data Layer:*** The data layer creates the flow of data from and to SG entities such as energy sources, servers, power transmission lines, and private/commercial consumers. The data is transmitted to programmable SDN-based switches and routers for routing to the intended location. Control layer policies for routing choices are implemented in this layer.
- ***Control Layer:*** The control layer consists of the SDN controller(s) and the advanced distribution management system (ADMS), where ADMS consists of supplementary control and data acquisition (SCADA), distributed energy resource management (DERMS), and a distribution management system (DMS) to monitor the smart grid system. This layer receives system data from and transmits system data to the application layer.
- ***Application Layer:*** The application layer receives system data from the lower two layers to ensure that the system is operating in accordance with the policies established by the control layer. It executes real-time system monitoring and analysis, including statistical analysis, traffic engineering, security monitoring, mobility management, flow filtration, and load balancing.

While existing SDN research can provide general network management, including security response, and solutions, SD-SGs are susceptible to a range of utility-specific cyber attacks such as

 doi:10.20944/preprints202403.1701.v1



distributed denial of service (DDoS), unauthorized access, false data injection, etc [5]. Furthermore, a software-defined version of SG will introduce additional attacks that target the controller, or other specific elements of the SD-SG network, in an attempt to gain control of the whole system [6].

### *2.3. SD-SG Cyber Threats*

Research in the field of SD-SG security has examined a variety of attacks. From an investigation of the literature of SDN-based security protocols, we find that the main attack types fall into the following categories, also shown in Figure 3:

- ***Distributed Denial-of-Service (DDoS):*** In DDoS/DoS attacks, a multi-node attack in launched on a victim in an attempt to consume all of the server's resources so that the server is unable to respond to legitimate requests [34].
- ***Controller Attacks:*** Controllers in SDN networks are vulnerable to a variety of attacks, including, but not limited to, DoS, hijacking, and unauthorized access [3,35]. These attacks seek to exploit the centralized nature of SDN controllers, which creates a single point of failure. Thus, for simple, centralized, SDN controller architectures, these attacks can disrupt the entire network by attacking the controller.
- ***Multi-Pronged Attacks:*** We refer to multi-pronged attacks as the case where multiple cyber attacks of different types are attempted simultaneously. For example, an attack can gain unauthorized access and launch both DDoS/DoS and controller attacks on a network. These can consist of a combination of DDoS and controller attacks as well as others (e.g. man-in-the-middle, false data injection, etc.). Very few researchers have addressed the case of multi-pronged attacks [36].

Next, we examine the research field concerning the cyber attacks outlined above.

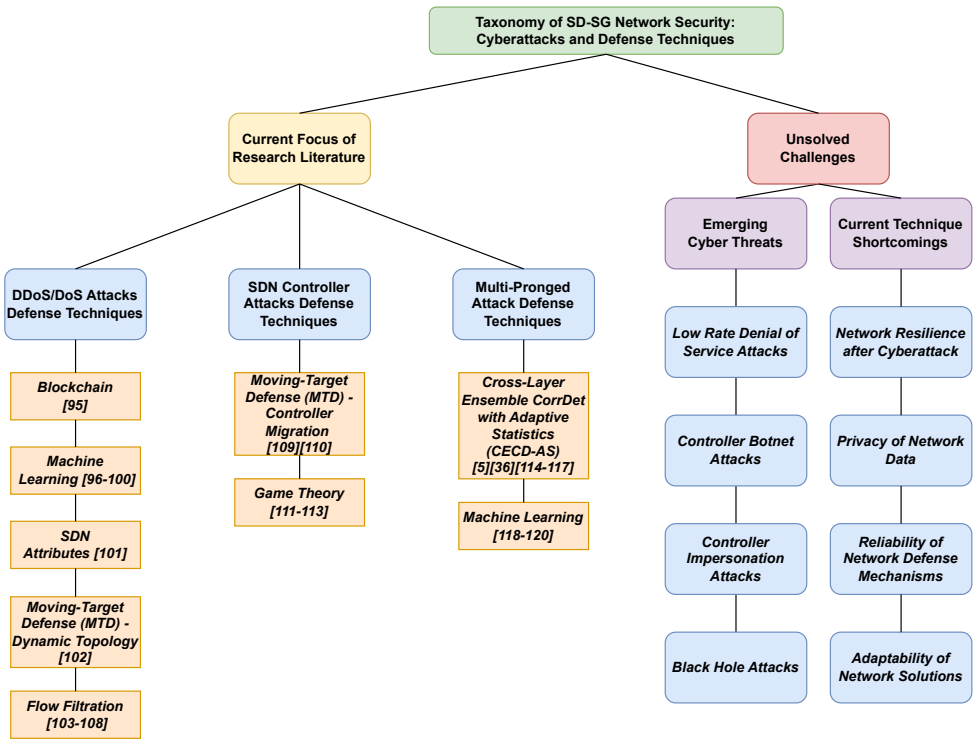



**Figure 3.** Taxonomy of SD-SG Network Security: Cyberattacks and Defense Techniques.

 doi:10.20944/preprints202403.1701.v1



## 3. Related Work

This survey presents examination of network security threats and defense methods for SD-SG, including multi-pronged cyberattacks. Table 2 summarizes the comparison of this work with other related survey articles. Related literature has only briefly covered these topics, and to our knowledge, has not covered multi-pronged cyberattacks. Table 3 summarizes related literature for both SG and SD-SG security. This paper focus on SD-SG network security and persistent threats, therefore related work that focuses on SG security in general, as seen in Table 3 , is outside its scope. Furthermore, in this paper, relevant literature published within the last five years of the paper's publication date is considered, towards ensuring that we survey the most recent literature and solutions. This section provides a review of related literature and surveys of SD-SG and highlights the missing components which are found in this survey.

Ibdah et al. [7] discuss the vulnerabilities of using SDN in SG systems. The authors start by outlining the architecture of SDN-based SG systems as well as the security risks associated with this technology. The paper then proposes a five-component security framework for SDN-based SG systems: secure communication, secure data storage, secure computation, secure authentication, and secure access control. The authors go into detail about each of these components and how they can be used in an SDN-based SG system. The authors use the Mininet network emulator to simulate the effectiveness of their proposed security framework. The simulation shows that the proposed framework is effective at mitigating various types of security attacks, such as DoS attacks, data tampering, and unauthorized access. Although the authors provide a discussion of the security of SD-SG systems, the discussion is very brief and focuses on DDoS attacks and the proposal of their framework. The researchers do not provide a comprehensive review of SD-SG security, as this survey does.

Abujubbeh et al. [9] discuss the application of software-defined wireless sensor networks (SD-WSNs) in SGs. The authors begin by presenting the advantages of SDWSNs over traditional wireless sensor networks, such as increased flexibility, scalability, and adaptability. The paper presents an SDN architecture for SDWSNs in SGs to provide a centralized control plane for network management. The authors describe the architecture's various components, such as sensor nodes, SDN controllers, and network infrastructure. In addition, the paper discusses the various challenges that SDWSNs face in SGs, such as security, energy efficiency, and network reliability. The authors emphasize the importance of overcoming these challenges in order to effectively use SDWSNs in SGs. In contrast to this survey, this paper only provides a brief discussion of DDoS attacks and their defense techniques and negates other network security threats mentioned in this survey. Furthermore, this paper concentrates on SDWSNs instead of general SD-SG.

Kim et al. [11] discuss the evolution of SG infrastructure as well as the potential for SDN to enable advanced SG capabilities. The authors begin by outlining SG infrastructure and the role of information and communication technologies (ICT) in enabling advanced functionalities like demand response, distribution automation, and advanced metering. The paper provides a discussion about the difficulties that traditional SG infrastructures face, such as a lack of interoperability and flexibility. The paper proposes using SDN to address the challenges that traditional SG infrastructures face while also enabling advanced functionalities. The authors describe the different components of an SDN-enabled SG architecture, such as the SDN controller, network infrastructure, and applications. The authors review the potential advantages of an SDN-enabled SG infrastructure, such as increased reliability, security, and energy efficiency. They highlight a number of use cases in which SDN can enable advanced functionality such as dynamic load balancing and network slicing. However, this paper deos not discuss DDoS and controller attacks and only briefly introduce anonymity/intrusion attacks and defense techniques, all topics covered within this survey.

Rehmani et al. [1] present a comprehensive literature review of SDN in SG communications. The authors discuss the challenges posed by SGs and how SDNs can assist in overcoming them. This paper examines the benefits of SDN-based communication for SGs, including enhanced network performance, resource management, and security. The authors provide a comprehensive analysis of existing SG

 doi:10.20944/preprints202403.1701.v1



communication solutions based on SDN, including their architectures, protocols, applications, and security. Additionally, the paper identifies unresolved research issues and challenges that must be addressed to facilitate more efficient use of SDN-based communication in SGs. It provides insights into technologies and identifies areas for future research and development. However, the paper's security section mentioned within the paper only provides a brief overview of the security of SD-SG, and the security papers covered are now outdated. Furthermore, it does not provide an in-depth discussion of future research efforts for SD-SG security threats as mentioned in this paper.

**Table 3.** Topics Explored in this Software Defined Smart Grid Security Survey.

| Main Domain | Sub-Topic: Cyberattack | References |
|---|---|---|
| Smart Grid Security | DDoS/DoS/Physical-DoS (PDoS) | [37–40] |
| | Spoofing, Sniffing, and Message Relay | [41–44] |
| | MITM,Eavesdropping, and Homograph | [45–49] |
| | Meter Manipulation and Theft | [50–53] |
| | FDI | [54–57] |
| | Impersonation, Session Key Exposure, and TSA | [58–63] |
| | TCP-SYN Flooding | [64–67] |
| | Jamming | [68–73] |
| | RAM Exhaustation/CPU Overload | [74–76] |
| | Brute Force | [77–80] |
| | Message Replay, Covert | [81–86] |
| | Sybil | [87–90] |
| | Multi-Attack | [91–94] |
| SD-Smart Grid Security | DDoS/DoS | [95–108] |
| | SDN Controller | [109–113] |
| | Multi-Attack | [5,36,114–120] |

Akkaya et al. [8] investigated the use of software-defined networking (SDN) in wireless local networks (WLANs) for SG applications. The authors begin by outlining the difficulties that traditional WLANs face when supporting SG applications, such as scalability, reliability, and security. The paper presents an SDN-based architecture for WLANs in SG applications, which includes a centralized control plane capable of dynamically reconfiguring the network to meet changing needs. The authors detail the proposed architecture, including the various components and their functions, and use the NS-3 network simulator [121] to simulate the effectiveness of the proposed SDN-based architecture. The simulations show that the proposed architecture outperforms traditional WLANs in terms of network performance, resource utilization, and security. The researchers investigate the relevant security aspects for each deployment scenario as they progress. However, the researchers only provide a discussion of anomaly/intrusion detection systems and only provide a brief discussion of controller attacks. The paper does not provide a discussion of DDoS attacks or defense techniques for the attacks mentioned in this paper.

Demirci et al. [10] suggest implementing software-defined networking (SDN) to improve the security of SG systems. The authors discuss the challenges encountered by conventional SG systems, such as the lack of network traffic visibility and control, which makes it difficult to detect and respond to security threats. The paper proposes an SDN-based security framework for SG systems that consists of three elements: network visibility, policy enforcement, and threat detection and response. The authors provide a thorough description of each of these components and discuss how they can be implemented using SDN. To evaluate the efficacy of the proposed framework, the authors emulate their networking using the Mininet [122]. The simulation demonstrates that the proposed framework can enhance network visibility, policy enforcement, and threat detection and response in comparison to conventional SG systems. However, this paper focuses on proposing their framework instead of

 doi:10.20944/preprints202403.1701.v1



a comprehensive review of the network security of SD-SG. The authors discuss DDoS attacks but only briefly address anomaly/intrusion attacks and defense techniques for each attack in contrast this survey which a more comprehensive review of network security threats. Furthermore, they provide no mention of controller attacks in the current literature.

### *3.1. Specific Contributions of This Study*

Table 2 illustrates the range of prior research that has discussed SD-SG network security. The aforementioned discussions often provided concise segments about SD-SG security within a broader survey or study. However, a comprehensive examination of SD-SG security has remained absent until the present study. Moreover, the prior studies on SD-SG, as evidenced by Table 2, have presented fragmented discussions of SD-SG attacks and their defense techniques. A comprehensive survey encompassing a diverse range of SD-SG attacks and their defense techniques and developing them into a single manuscript is necessary. Moreover, the existing literature has not explored the emerging threats such as low rate denial of service, controller botnet attacks, and black hole attacks of SD-SG network security nor provided potential mitigation techniques, as is undertaken in this particular study in Section 7. In addition, no studies have provided a discussion of defense systems that consider multi-pronged cyberattacks and provide multi-pronged defenses that can be applied to various types of SD-SG networks. With these contributions, our work distinguishes itself from previous research.

## 4. DDoS/DoS Attacks

As previously stated, DoS attacks can be conducted to flood target nodes or components in the SD-SG in order to cause harm or a full shutdown. DDoS attacks can have devastating consequences for SD-SG [5,36], and have grown in popularity among cyber attackers targeting SDN frameworks due to their ease of use [123]. Various solutions against DDoS/DoS attacks have been proposed, including blockchain, machine learning (ML), SDN properties, and moving target defenses. Blockchain approaches can increase network security by validating network traffic and the behavior of nodes. However, the current shortcomings are that they require recording, storing, and validating the blockchain process which can add overhead and strain to the system.

A lightweight blockchain architecture capable of protecting an SD-SG from DDoS/DoS attacks and providing recovery of nodes has yet to be created. ML models can be taught to detect DDoS/DoS threats, but they fail when it comes to detecting DDoS/DoS attacks launched using zero-day exploits, or when using techniques that the model has yet to be trained and tested on. Trained ML solutions need to be consistently updated with the latest data available which may not be feasible. A robust ML model that can detect novel DDoS/DoS attacks and provide recovery solutions for victimized nodes remains to be observed. Beyond blockchain and deep learning, techniques for access control and rate limiting; distributed software-defined networking architectures; and graph learning approaches have been proposed. These strategies have yielded promising results in terms of improving SD-SG system security against DDoS attacks. We have selected representative current efforts for DDoS attack detection and mitigation for SD-SG to present and analyze in the following.

### *4.1. Blockchain*

Blockchain (BC) offers a peer-to-peer (P2P) communication system that keeps track of every connection-related record for each network member in an easily accessible and properly kept database. The information of the database is stored in the form of blocks, and each block has a unique hash value identification. In addition, the blockchain has the characteristics of decentralization and does not rely on central nodes. It is a potential solution for enforcing a verification system at every edge of SD-SG's SDN networks, and addressing trust-management issues to make the more system resilient to authentication attacks [124,125]. These systems employ a consensus mechanism to detect and report network threats. Xiong et al. [95] proposed a distributed SDN control architecture for SG that is protected by blockchain. The core idea presented was to use blockchain technology to ensure the

 doi:10.20944/preprints202403.1701.v1



consistency of the control layer strategy and the flow rules to prevent faulty or malicious data from being accepted in the network. Figure 4 shows the proposed architecture, which includes three layers. The first layer is the data layer which is the common switch and flow forwarding process for SDN as described in a previous section. The second layer is a control layer consisting of a distributed SDN cluster structure. All SDN controllers are connected to each other in a distributed blockchain. The third layer is the blockchain layer. In this layer, the cluster head SDN controllers are responsible for verifying whether devices are "on-chain". Several processes are proposed for the SDN cluster controllers to authenticate both data and devices using blockchain-based verifications. Simulations showed that the blockchain-based distributed consensus mechanism was able to protect the system from DDoS attacks at rates of 400 packets/s, maintaining bandwidth greater than $> 80\%$. This study's findings indicated that incorporating blockchain technology in SG systems has the potential to improve both security and resilience when faced with DDoS attacks. The present limitations of this effort are the requirement for regular updates of the blockchain while ensuring minimal workload by controllers. Future research should focus on developing efficient systems that prioritize the speed of verification among blockchain participants by the controllers while minimizing any additional costs or burdens.

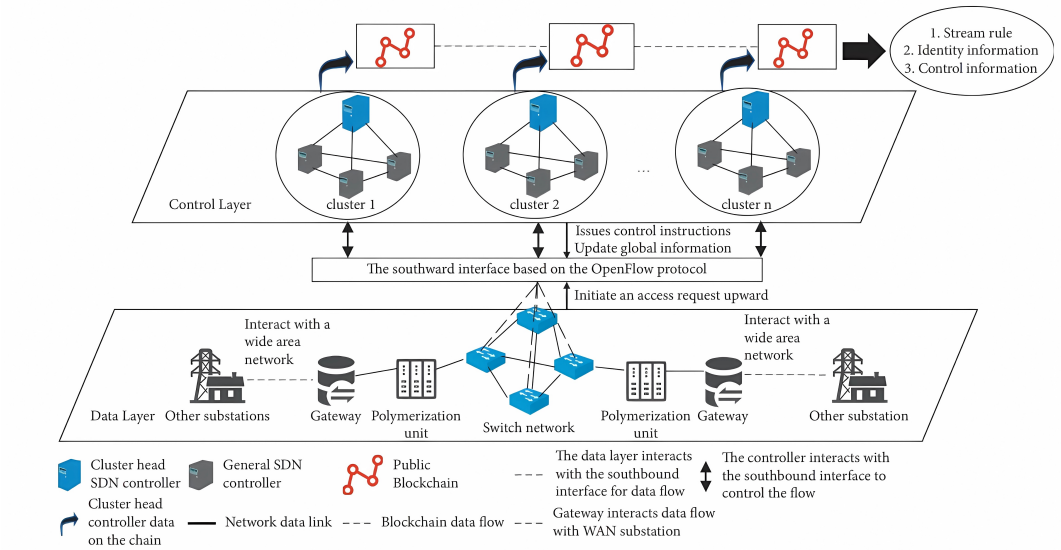



**Figure 4.** ClusterBlock Design presented in [95].

### *4.2. Machine Learning*

Machine learning developed from a collection of powerful Artificial Intelligence (AI) techniques and has been widely used in data mining, which allows a system to train data to learn useful structural patterns and models. This application of ML is well suited for network security [126]. Recent techniques use various ML models, including deep-learning models, to develop classifiers that can detect DDoS attacks in SDN-based SCADA and SG systems. In addition, these papers emphasize that a good match between classifier and data set is key to developing a successful model. Polat et al. [96] proposed an approach for accurately detecting DDoS attacks in SDN-based SCADA systems using parallel recurrent neural networks (RNNs). Their proposed method utilizes long short-term memory (LSTM) and gated recurrent units (GRU) RNN models. An original dataset was created by employing non-attack data and DDoS attack traffic data from an experimental topology environment that mimics a small-scale SDN-based SCADA system. The proposed RNN model using parallel LSTM and GRU layers was trained and tested through the dataset. This approach obtained an average accuracy of 97.62% to classify DDoS attacks. The limitations of this study reside in the fact that they generated a unique dataset from their experimental setup. It is unclear how well this testbed represents other systems, and the extent to which their DDoS attack scenario accurately reflects real-world attacks. In future research, it is important to examine the representativeness of their testbed and assess the performance

 doi:10.20944/preprints202403.1701.v1



of their machine learning models in real-world applications. Additionally, it is crucial to evaluate their models against unforeseen DDoS attack scenarios and compare their effectiveness with other existing scenarios.

However, in contrast to the aforementioned study, Nagaraj et al. [97] proposed GLASS, a graph learning approach for enhancing the security of SDN-based SG systems against distributed denial-of-service (DDoS) attacks. Unlike previous studies, the proposed method employed graph convolutional neural networks (GCNNs) to detect DDoS attacks for various scenarios in real-time by learning the patterns of normal and malicious network traffic and used unsupervised learning methods to identify compromised entities. The approach not only involved detecting attacks but also used spectral clustering to identify DDoS-compromised entities and proposed mitigation strategies. Mitigation is applied by sending updated flow policies to the main SDN controller's northbound interface for reconfiguring the flow tables in switches. The controller limits the flow of TCP SYN packets to the compromised nodes, which improves the network performance considerably. The authors tested the proposed approach's performance on a simulated SG network for the IEEE 118-bus power grid system that commonly uses IEEE C37.118.2 or IEC 61850 over TCP/IP communication schemes. Anomalous network traffic (i.e. DoS attack) was generated using tools such as hping3 [127], to initiate TCP flooding attacks. A detection rate of $> 97\%$, and a throughput of 84% were maintained using the mitigation technique compared to 4% throughput during DDoS attack scenarios without applying the techniques. The shortcomings of this work reside in the simplicity of the attack scenario and the yet-to-be-realized effectiveness of the GCNN in complex attack scenarios. Moreover, when the SD-SG is represented as a graph, there are difficulties in training it when the structure changes due to natural events such as outages or disasters. Additionally, the use of GCNNs poses a challenge in terms of computational time and overhead in the application layer when scaling the grid. Hence, future endeavors should explore adaptable GCNNs that consider these challenges.

In [98], the authors assert that Entropy-based Anomaly Detection methods that make use of feature distributions of the network have been successful in detecting DoS attacks. On this account, they propose the Shannon Entropy to identify anomalies in the communication network of an SG using SDN traffic feature distributions like source Internet Protocol (IP) address and destination IP address. A high entropy implies scattering of the feature distribution whereas a low entropy indicates convergence of the feature distribution. Principal Component Analysis (PCA) is used for pre-processing the traffic flow before classification. However, this is ongoing research and the authors expect to implement this proposed entropy-based anomaly detection technique on an SDN-based testbed. Thus, this proposed method has not been validated to confirm its efficiency in effectively detecting anomalies in SD-SG. Future research should examine the practicality of implementing and the impact on SD-SG network performance.

In contrast to prior studies, Allen et al. [99] propose a Hybrid, Distributed, and Decentralized (HDD) SDN architecture to secure the Phasor Measurement Unit (PMU) subsystem network. HDD-SDN utilizes the physically distributed controller approach for fault tolerance and fail-over operations while employing the parallel execution of machine learning models to detect anomalous behavior for a resilient SD-SG. The proposed method uses the parent-child multiple controllers model. The parent controller re-configures the network and allocates and manages resources whereas the child controller determines anomalies in packets and monitors the status of the parent node and other devices within the sub-region network. The authors implement the K-means algorithm in parallel with the incremental K-means algorithm. The standard K-means algorithm recalculates the cluster centers using the entire data set while the incremental K-means updates the previous centers with only newly input data in each iteration. These clustering techniques detect anomalies in the network traffic data and PMU measurement data. The proposed anomaly detection technique using clustering provides approximately 90% accuracy. One of the shortcomings of work is that it introduces a single point of failure and vulnerability into the system through the parent-child relationship between controllers. In the event that the parent controller is compromised or experiences a failure, the entire system

 doi:10.20944/preprints202403.1701.v1



will encounter interruptions. In addition, the utilization of the K-means method for face detection is hindered by challenges related to the expansion of dimensions and the impact of outliers on the classification process. Future research should explore these areas and provide solutions to address them.

The authors in [100] focus on the early-stage anomaly detection of the communication network traffic in near real-time with 96% accuracy. Alfan et al., propose CyResGrid, an approach that uses a hybrid deep learning model of a Graph Convolutional Long-Short Term Memory (GC-LSTM) and a deep convolutional network for time-series classification-based anomaly detection in Operational Technology (OT) communication networks for power grids. GC-LSTM comprises two machine learning models, namely, Graph Convolutional Network (GCN) and LSTM. The GCN processes the OT network topological information in the spatial domain. The LSTM learns the time-series data of the observed OT network traffic in the temporal domain. Hence, GC-LSTM can learn from both the spatial and temporal domains. The deep convolutional network in CyResGrid uses Bayesian optimization for hyperparameter tuning to detect anomalies. The authors simulated the power system in real-time with the Root Mean Square (RMS) dynamic model of the IEEE 39-bus test system in DIgSILENT PowerFactory whereas the OT network emulation is based on Mininet. They considered DDoS and active reconnaissance which involves OT network scanning. The experimental analysis indicates that the proposed CyResGrid outperforms the compared state-of-the-art deep learning-based time-series classification of anomalies. CyResGrid can be improved to detect more variations of anomalies in the SD-SG. The primary shortcoming of this effort is that the scalability of their solution has not been evaluated yet. As previously stated, Graph Convolutional Networks (GCNs) need significant computing resources, and their scalability and resource costs have not yet been thoroughly evaluated. Future studies should focus on exploring a more efficient implementation of GCNs for the purpose of implementing SD-SG.

### *4.3. SDN Attributes*

As was stated in Section 2, SDN network architectures enables flexibility, control, and security via the SDN controller and its management of data flows through switches and routers. Researchers have made use of these characteristics to develop security models for SD-SG that leverage the centralized SDN controllers; customizable data plane flows; and natural SDN network resilience. Mahmood et al. [101] presented S-DPS, an SDN-based DDoS protection system for SG. The proposed system employs a centralized SDN controller to monitor the network. DDos attacks are detected and classified based on employing lightweight Tsallis entropy-based defense mechanisms. Tsallis entropy has usually been characterized through its entropic index to evaluate non-extensive systems. It is commonly applied to edge detection and image segmentation in image processing. Traffic features are extracted from new packets destined to the SDN controller. The SDN controller matches or identifies flows associated with SDN characteristics that demonstrate an anomaly in their entropy values or changes in entropy. Using the proposed techniques both low-rate (LR)- and high-rate HR-DDoS attacks are successfully detected, followed by the application of countermeasures, such as rate limiting and filtering. A specific action by the controller is associated with each flow in flow tables. The S-DPS SG system was simulated for various attack scenarios. Detection rates of DDoS attacks of 100% were observed with a 0% false positive rate. A shortcomming of this work is that the testbed design utilizes a single POX controller to accommodate the detecting module. Nevertheless, this creates a single point of vulnerability that might cause the entire system to fail. Additionally, POX is a legacy controller that is implemented using Python. Many practical applications utilize advanced controller systems, such as ONOS, for instance. The implementation of a distributed strategy with modern controllers has not yet been achieved. Moreover, the efficacy of their system in addressing more practical attack scenarios has not yet been achieved.

 doi:10.20944/preprints202403.1701.v1



*4.4. Moving Target Defense - Dynamic Topology*

Used as a countermeasure, a moving target defense (MTD) implements flow, path or route/switching mutation to defend normal operations in communication networks, making it difficult for attackers to launch successful DoS attacks along a given set of devices or paths. MTD increases ambiguity and complexity for system attackers; decreases their chances of identifying targets (e.g., vulnerable system components); and raises the cost of attacks and scans, e.g., reconnaissance attacks [128]. An example of a MTD is shown in Figure 5. The SDN controller communicates with the switches with the help of southbound API, to instruct the switches on which links to use for flows. The green links are “on”, i.e., are active flows being used by the network. The red links contain data that is false or are links that are no long active because they have been turned off by the SDN controller. When an attacker attacks these links, the false packets are not routed to the correct destination and are essentially dropped, which prevents them from affecting the intended network traffic.

Abdelkhalek et al. [102] proposed a MTD routing mechanism to improve the security of SDN-enabled SG systems. This approach combines the advantages of the dynamic programmability of SDN and the randomness of MTD topology changes for cyber attack prevention and mitigation in the smart grid. Their proposed mechanism randomized the network topology by changing the paths that network flows take in response to a DoS attack. The SDN controller senses the blocking of the communication path and switches the data flow to another available channel. The focus of this work is on DoS attacks on links and connections between the substations and the control center. One shortcoming of this work is that DDoS attacks and attacks on nodes/devices as single points of failure were not considered and should be investigated for future work. The proposed mechanism was simulated using a Real-time power system simulator (OPAL-RT), Mininet network and SDN emulator, and external hosts to act as the attacker and the maintenance node. The proposed approach demonstrated significantly reduced packet drop percentages. Researchers also examined the link switching time that would minimize packet drops during DoS attacks.

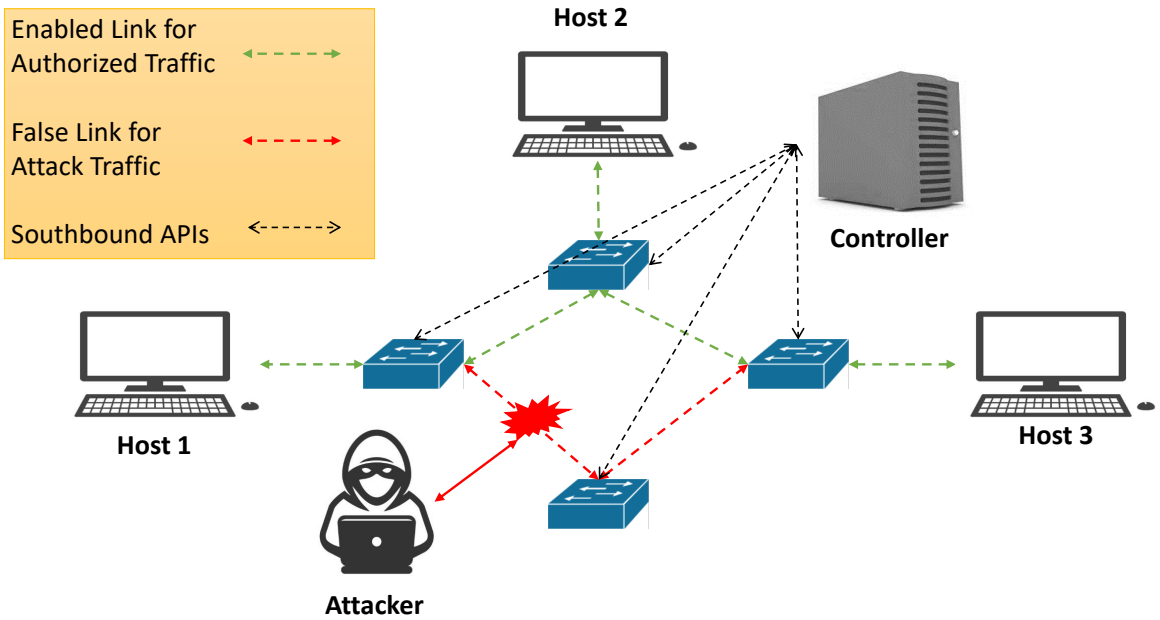



**Figure 5.** Moving Target Defense Example Architecture.

*4.5. Flow Filtration*

Static state estimation (SSE) does not consider any history of the measurement vector **z**, but instead provides a snapshot of the system. This "memoryless" assumption of SSE proved sufficient for real-time monitoring in early EMS. For one, power networks were not as regimented at the distribution

 doi:10.20944/preprints202403.1701.v1



level–with far fewer microgrids, distributed energy resources, and net load dynamics compared to today's systems. Secondly, the measurement data fed to the state estimator almost always came from measurement devices with slow sampling rates, such as the 2-4 second range of SCADA. One might argue, then, that the true bottleneck for capturing dynamic behavior in state estimation was slow metering rates. That said, Schweppe's formulation arrived just shortly after the introduction of the Kalman filter in 1961 [129], which inspired power researchers to seek formulations beyond the still-developing SSE. The practical hangup of slow meter sampling rates would be relieved somewhat with the introduction of synchronized phasor measurements in the 1980s [130]. Phasor Measurement Units (PMUs) provide higher sampling rates when compared to SCADA, but also GPS coordination to avoid uncertainty associated with asynchronicity. Like SSE, dynamic state estimation (DSE) encompasses a wide range of methods. Early DSE formulations considered the same set of measurements and state variables as those used in SSE: active and/or reactive power flow and injections, and complex bus voltages. Other approaches seek to better capture load dynamics by considering generator rotor angle and speed as differential-algebraic state variables [103–105], however this review will primarily consider DSE-based anomaly detection implementations that use algebraic state variables. DSE can be accomplished by modeling the power system as a discrete time dynamic system. The Kalman filter is used [106] to estimate the state variables at time $k$ through prediction and measurement update steps upon each iteration:

Predict:

$$\hat{\mathbf{x}}_{k|k-1} = \mathbf{A}_k \hat{\mathbf{x}}_{k-1|k-1} \tag{1}$$

$$\mathbf{F}_{k|k-1} = \mathbf{A}_k \mathbf{F}_{k-1|k-1} \mathbf{A}_k^T + \mathbf{Q}_k. \tag{2}$$

Update:

$$\mathbf{K}_k = \mathbf{F}_{k|k-1} \mathbf{H}_k^T \left( \mathbf{H}_k \mathbf{F}_{k|k-1} \mathbf{H}_k^T + \mathbf{R}_k \right)^{-1} \tag{3}$$

$$\hat{\mathbf{x}}_{k|k} = \hat{\mathbf{x}}_{k|k-1} + \mathbf{K}_k \left( \mathbf{z}_k - \mathbf{H}_k \hat{\mathbf{x}}_{k|k-1} \right) \tag{4}$$

$$\mathbf{F}_{k|k} = \mathbf{F}_{k|k-1} - \mathbf{K}_k \mathbf{H}_k \mathbf{F}_{k|k-1} \tag{5}$$

where, at time $k$, $\mathbf{A}_k$ is the state transition matrix, $\mathbf{K}_k$ the Kalman gain matrix, and $\mathbf{H}_k$ the measurement matrix. $\mathbf{F}_{k|k}$ and $\mathbf{F}_{k|k-1}$ denote the state covariance matrix estimates based on measurements up to times $k$ and $k-1$. $\mathbf{Q}_k$ and $\mathbf{R}_k$ are the process and observation noise covariance matrices, respectively. The authors of the first Kalman filter power system DSE approach [131] hinted at its compatibility with anomaly detection methods which, at the time, were under study for SSE. Early work soon after [132,133] formulated bad data detection by analyzing the innovation process:

$$\mathbf{v}_k = \mathbf{y}_k - \mathbf{h}(\hat{\mathbf{x}}_{k|k-1}). \tag{6}$$

Additional approaches for bad data processing in DSE include asymmetry analysis based on the skewness of the normalized estimation error [106,107]. DSE anomaly detection research remains an active field [105,108], especially since dynamic load and generation profiles are commonplace in microgrid systems with distributed energy resources (DERs).

### *4.6. Summary and Lessons Learned*

This section presents a comprehensive examination of the taxonomy of defense strategies employed to mitigate DDoS and DoS attacks in the context of SD-SG network security. In this section, we have provided solutions of Blockchain, Machine Learning (ML), SDN attributes, and MTD. The performance of each has been thoroughly examined, along with the respective benefits they offer. It was observed that each proposed solution has demonstrated enhancements in the areas of confidence

 doi:10.20944/preprints202403.1701.v1



augmentation within the system, precise identification of attacks, and utilization of the inherent properties of SDN, such as the installation of flow rules, to bolster the security of SD-SG against DDoS and DoS attacks. Furthermore, there exist certain domains have not been thoroughly investigated. Future research efforts should focus on examining the most suitable deployment site to minimize network overhead, enhance the speed of response of defense systems, and explore methods to retain throughput in order to restore connectivity in areas affected by DDoS attacks.

A number of defenses against controller attacks have been put forth, including moving-target defense (MTD) and deep learning. A new direction in SD-SG network security is game theory. With the aid of game theory, developers create games in which the security system (a player) must make several decisions in order to achieve a predetermined objective, such as protecting the controller from an attacker (another player). Although game theory can be used to improve controller security and to avoid data leakage to ensure data privacy, its implementation inside a system can result in additional system overhead. In the next section, we examine the latest research for controller attack defenses.

## 5. SDN Controller Attacks

As seen in the background as well as the algorithms, protocols, and strategies for DoS attacks, SDN Controllers are one of the most important components of any SD-SG framework. Access to the controller enables an operator to have complete control over network topology, as well as control to change or generate traffic rules for their applications. This makes SDN controllers an appealing target for cyber attackers, and a focus of concern for secure network management[134]. This section examines SD-SG controller attack defense strategies and categorizes them based on MTD and game theory. In this section, we examine the latest literature on the defense of SDN controllers, highlighting approaches that use MTD defenses and game theory.

### *5.1. Moving-Target Defense for Controller Attacks - Controller Migration*

As discussed in Section 4.4, MTD defenses implement flow, path or route/switching mutation to defend normal operations in communication networks. In this section, MTD is applied to protect against controller attacks by virtually migrating the controller instance instead of altering the network topology, in contrast to section 4.4 . Lin et al. [109] proposed an MTD approach based on virtual security functions (e.g. firewalls, IDS, traffic classifier, etc.) to improve the security of SDN networks in SG. Furthermore, researchers suggest migrating the virtual security functions to resource-rich servers which will help mitigate the effects on the virtual security functions. The proposed work includes a three-layer architecture consisting of an SDN controller layer, a virtual security function layer, and an infrastructure layer. In addition to the normal SDN controller components, there is a new component called migration controllers that manage the dynamic scheduling of physical resources. The infrastructure layer holds the standard hardware resource servers running VSF instances and OpenFlow switches. The virtual security function enables the migration of the virtual security instantiation to new locations in the network to respond to network attacks. Thus, the proposed approach aims to defend against controller attacks by proposing a moving target defense of virtualized security in SD-SG, making it difficult for attackers to locate and exploit vulnerabilities. The authors used a simulation of a real-world SG topology to assess the effectiveness of the virtual security function instances pre-migration algorithm, compared to using a random algorithm or a greedy algorithm for migration. The method worked well against cyber attacks that targeted the controller's location or attempted to exploit vulnerabilities in the controller's software. A shortcoming of this study is the presence of a persistent SDN controller responsible for overseeing the migration of other controllers. The study does not address the possibility of the migration controller being attacked and compromised, which would render the migration scheme ineffective as the attackers may modify the migration process. Incorporating a migration scheme into the controller responsible for managing the migration should be considered in future studies. A shortcoming of the work is that, despite the implementation of a distributed approach for the controller architectures, the entire framework introduces single points

 doi:10.20944/preprints202403.1701.v1



of failure due to certain modules such as the "AllocatoR" being responsible for selecting the optimal location for SDN controllers to move to. These specialized modules might become vulnerable sources of failure and targets for attackers to exploit. Future work should aim to decentralize these modules in order to enhance ambiguity.

Similarly, Azab et al. [110] propose "MystifY," a proactive MTD approach for improving resilience against attacks for the Software Defined Control Plane in Software Defined Cyber-Physical Systems (SD-CPS). The strategy changes the controller's network addresses and/or ports on a regular basis, making it difficult for attackers to track the controller's location and exploit vulnerabilities. First, the most suitable controller–deployment location is determined. Then, the controller is dynamically relocated among heterogeneously configured hosts. However in contrast to other approaches, the workload of the controller is also migrated among a set of multiple controllers for robust and increased resilience with controller operations. SG is chosen as a case study for simulation within the overall field of CPS. The simulation uses PYGRID, a Python-based software development and assessment framework for grid-aware SDN. The downtime due to SDN controller migration and workload migration are examined to observe the overall impact on grid operations. According to the findings, MystifY can reduce the success rate of various attacks by not allowing the attacker to identify the location or identity of the controller. The method worked especially well against attacks that targeted the controller's network location or attempted to exploit vulnerabilities in the controller's software.

### *5.2. Game Theory*

We define game theory as involving multi-decision scenarios, which are games in which each player makes decisions that maximize their own benefits while anticipating the rational choices of their fellow participants, in this case, cyber attackers [135]. In game theory, each participant makes decisions and takes actions to produce the desired, ideal result. Applied to SD-SG network security, SD-SG security studies use gaming theory to evaluate cyber threat scenarios and then use the control planes and data planes as players.

Sivaraman et al. [111] propose a game-theoretic approach to improving data privacy in SD-SG, with the goal of reducing passive information leakage through compromised controllers. The proposed privacy framework is based on the formulation of a noncooperative game among the switches. The requirements for privacy are quantified using information theory mutual information and differential privacy. An iterative best response algorithm is used to compute the game's Nash equilibrium [136]. The proposed scheme's performance is compared to the globally optimal solution and the exponential mechanism (for differential privacy). When compared to the global solutions, the theoretical game performed nearly optimally on the IEEE 30, 118, and 300 [137] bus systems. In summary, the proposed approach can be used to improve data privacy in SG systems and protect against compromised controllers. A shortcoming of this study is that the impact of quick scalability has not been assessed. The technique given is tailored for specific IEEE bus systems, but its performance under real-life scenarios of rapid expansion and grid education has not been evaluated yet. This aspect should be investigated in future research.

In contrast to other game-based approaches, Samir et al. [112] suggest a Software-Defined Controller Placement Camouflage (SD-CPC), a stochastic game-based MTD method for improving SDN controller resilience against cyber threats. Figure 6 shows a model of a game-based MTD. The technique seeks to make SDN controllers less vulnerable to attackers by dynamically relocating virtualized controllers and changing their IP addresses. There are two participants in the game: player 1 is the system defender, and player 2 is the attacker. The attacker targeted the most vulnerable regions of the network in their simulations, while the system defender determined the best location to migrate the controllers in reaction. The technique performed particularly well against attacks that tried to exploit vulnerabilities in the controller's software or targeted the controller's location. The proposed game had minimal influence on system performance, and the proposed SD-CPC approach offers an effective and efficient MTD solution for improving SDN resilience to advanced persistent threats to

 doi:10.20944/preprints202403.1701.v1



controllers. A shortcoming of this study is its exclusive focus on a single defender and attacker. The extent to which this system can handle and counter more complex and coordinated attacks has not been determined yet and should be investigated in future research.

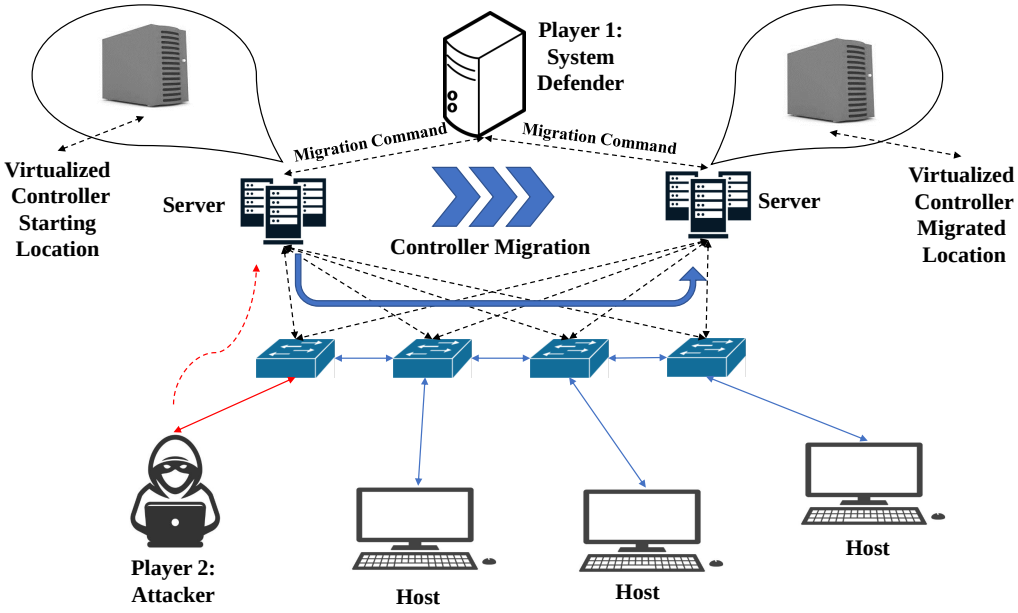
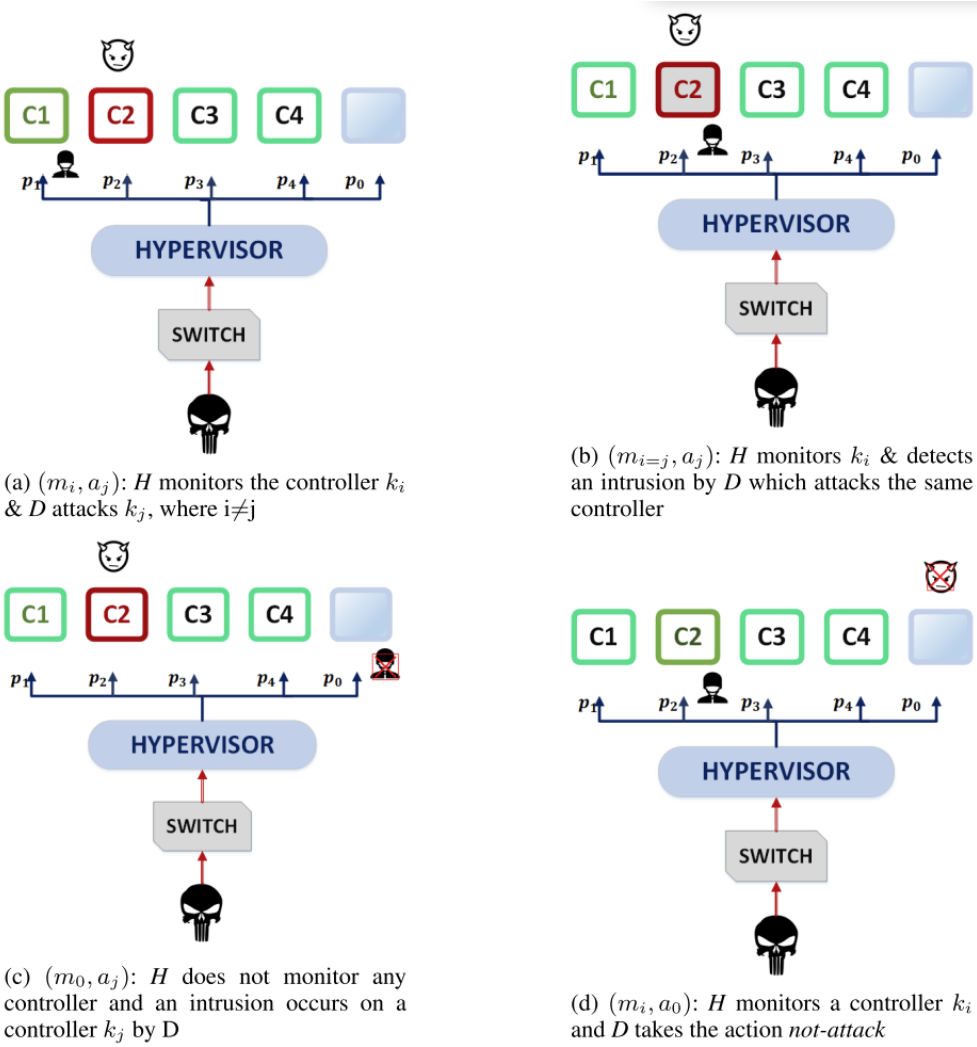



**Figure 6.** Software-defined Smart Grid (SD-SD) Moving Target Defense (MTD) Game Example.

We have seen that SDN-related problems like SDN controller assignment, and anomalies detection and mitigation can be modeled as games [113]. Rumaisa et al., considering an Intrusion Detection System (IDS)-SDN architecture such as the one shown in Figure 7, formulate the strategic interaction between a hypervisor and a possible attack source, while the hypervisor monitors its virtual SDN (vSDN) controllers in the Control Plane and the attack source launches DDoS attacks via compromised switches. The game is modeled as a non-cooperative dynamic Bayesian game-theoretic IDS [113]. Figure 7 provides an example game scenario from [113]. The four scenarios show strategic interactions between the hypervisor and the attacker. In the game model, a hypervisor can distribute its limited resources to optimally monitor guest virtualized SDN controllers. It follows a realistic approach of a malicious entity, which, via a compromised switch, aims to minimize its detection by deviating its behavior between normal behavior and malicious behavior. The resulting analysis indicates that the non-cooperative dynamic Bayesian game-theoretic IDS increases the probability of a hypervisor detecting distributed attacks, minimizes false positives, and reduces monitoring costs. An inherent shortcoming of the approach is that the use of a single hypervisor creates a new potential target for attackers. The attacker may attempt to directly target the hypervisor in order to render the game ineffective. Future work should consider protection measures to be implemented.

 doi:10.20944/preprints202403.1701.v1






(a) $(m_i, a_j)$: $H$ monitors the controller $k_i$ & $D$ attacks $k_j$, where i≠j

(b) $(m_{i=j}, a_j)$: $H$ monitors $k_i$ & detects an intrusion by $D$ which attacks the same controller

(c) $(m_0, a_j)$: $H$ does not monitor any controller and an intrusion occurs on a controller $k_j$ by D

(d) $(m_i, a_0)$: $H$ monitors a controller $k_i$ and $D$ takes the action *not-attack*

**Figure 7.** Scenarios for Strategic Interactions between a Hypervisor and an Attacker [113].

### *5.3. Summary and Lessons Learned*

In this section, we examined the taxonomy of mitigation measures used to mitigate SDN controller-based attacks. We have presented solutions in the form MTD and game theory. We have conducted an analysis of the individual advantages associated with each proposed option. It has been observed that each proposed solution has the objective of enhancing the security of the controller in order to prevent the unauthorized disclosure of sensitive information, or alternatively, frequently relocating the virtualized instances of the controller to create a continuously evolving and dynamic environment for controllers to thwart targeting by attackers. Nevertheless, there are a few areas that require further investigation in future research. Future research should focus on investigating methods for detecting hacked controllers and examining the impact of frequently changing the virtual location of the controller on the quality of service (QoS) for end users. In the event that a controller has already been compromised, it is clear that the approaches proposed in existing literature would be insufficient.

Game-theoretic techniques are still a new area of research for SD-SG systems. Another new area of SD-SG research focuses on the creation of multi-pronged attack-defensive solutions. SD-SG can become subjected to multiple varying cyberattacks such as false data injection (FDI), man-in-the-middle (MITM), and DDoS/DoS. To our knowledge, no other research has focused on the multiple-attack scenario. However, at the University of Florida, with the support of a grant from the National Science Foundation (NSF), we have developed a suite of cross-layered strategies enhanced by machine learning algorithms to detect multi-pronged cyberattacks with greater performance than other state-of-the-

 doi:10.20944/preprints202403.1701.v1



art single-attack methods. We have developed distributed SDN-controller strategies to enable risk mitigation and throughput maintenance during cyberattacks.

## 6. Multi-Pronged Attacks

### *6.1. Cross-Layered Machine Learning Approach*

Our suite of Cross-Layer Ensemble CorrDet with Adaptive Statistics (CECD-AS) strategies has been developed to provide a robust, comprehensive framework that can detect various cyberattack threats such as FDI, DoS, and MITM attacks [5,36,114–117]. Allen et al. [36] present an SDN-based cross-layered approach that aims at protecting SGs against cyber threats by incorporating data from both the power grid and the networking and communication layers into a machine learning model. The cross-layer architecture is shown in Figure 8. The smart grid layer provides physical/physics-based monitoring and measurements, while the communication network layer monitors and provides cyber-based measurements. The analysis layer trains and tests the cross-layer data to model the system's normal operations versus anomalous operations. The data are trained to detect and identify the presence of single attacks and multiple types of cyber attacks including false data injection (FDI), denial of service (DoS), and man-in-the-middle (MITM) attacks. The management layer is responsible for mitigation actions using the SDN-based control of the SD-SG system.

Multi-pronged attack defensive SD-SG solutions are primarily cross-layered, machine learning algorithm-assisted approaches that dynamically update the statistical model of both the system measurement parameters and the network parameters based on power flow traffic to improve the likelihood of detection of multi-pronged cyberattacks. Our multi-disciplinary smart grid team at the University of Florida, consisting of experts in power, networks, and machine learning, has developed several ground-breaking cross-layered machine learning algorithms and demonstrated robustness in the presence of a range of SG attacks.

CECD-AS algorithm to analyze data from the power grid and SDN-communication layers and detect any anomalous behavior in real-time in the SD-SG as shown in Procedure 1. The equations necessary for the implementation of the CECD-AS algorithm are as follows:

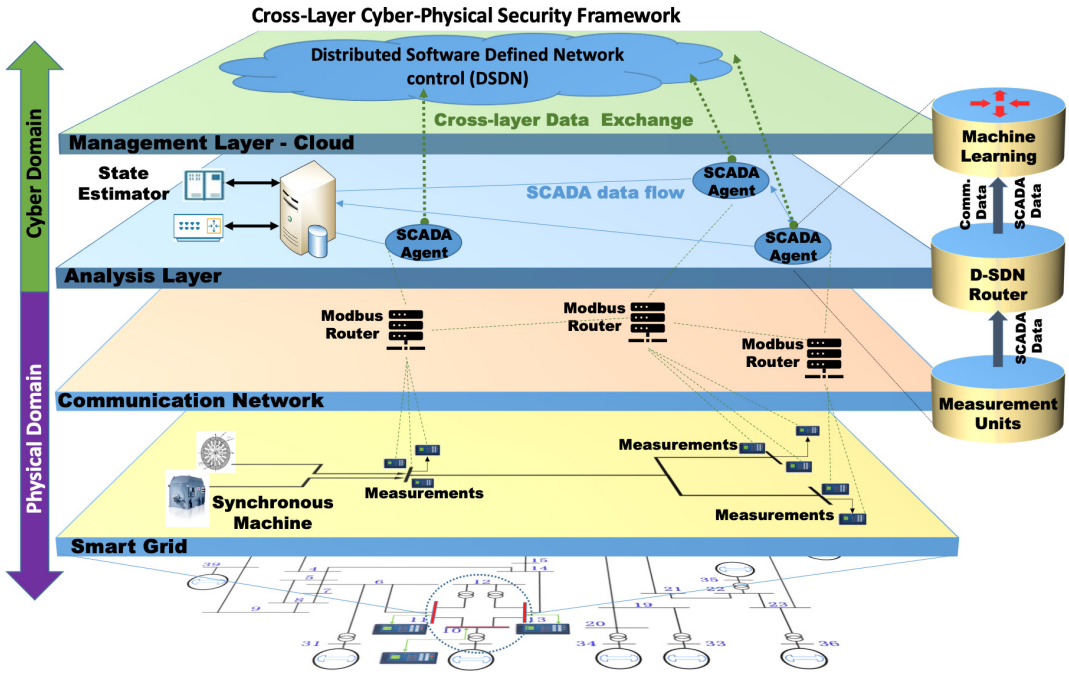



**Figure 8.** Cross-Layer Cyber-Physical Security Architecture Presented in [36].

 doi:10.20944/preprints202403.1701.v1



The Mahalanobis Distance Equation:

$$\delta_m^{ECD}(\mathbf{z}_m) = (\mathbf{z}_m - \boldsymbol{\mu}_m)^T \Sigma_m^{-1} (\mathbf{z}_m - \boldsymbol{\mu}_m) \tag{7}$$

The threshold equation for the CECD-AS Algorithm:

$$\boldsymbol{\omega}_m = \boldsymbol{\mu}_{\boldsymbol{thr,m}} + \eta * \boldsymbol{\sigma}_{\boldsymbol{thr,m}} \tag{8}$$

Woodbury Matrix Identity [138] in equations (9) and (10) respectively are used:

$$\boldsymbol{\mu}_{new,m} = (1-\alpha)\boldsymbol{\mu}_m + \alpha(\mathbf{z}_m - \boldsymbol{\mu}_m) \tag{9}$$

$$\Sigma_{new,m}^{-1} = \frac{1}{1-\alpha}\left[\Sigma_m^{-1} - \frac{(\mathbf{z}_m - \boldsymbol{\mu}_m)(\mathbf{z}_m - \boldsymbol{\mu}_m)^T}{\frac{1-\alpha}{\alpha} + (\mathbf{z}_m - \boldsymbol{\mu}_m)^T(\mathbf{z}_m - \boldsymbol{\mu}_m)}\right] \tag{10}$$

As discussed in [36], the threshold value $\tau_m$ for each local Cross-layer CorrDet detector is updated using equation (11) with updated $\boldsymbol{\mu}_{thr,m,-\beta}$ and $\sigma_{thr,m,-\beta}$, where $-\beta$ signifies the use of past $\beta$ number of samples for updating threshold

$$\tau_m = \mu_{thr,m,-\beta} + \eta * \sigma_{thr,m,-\beta}. \tag{11}$$

The framework is also designed to enable an efficient integrated approach across various components of the SG. The authors demonstrate the effectiveness of the framework using a case study with results showing greater than $> 98\%$ classification accuracy against the aforementioned multi-pronged cyberattacks. Overall, the proposed approach provides a comprehensive and proactive approach to SG cybersecurity, which is essential for ensuring the reliability and resilience of modern power systems. CECD-AS is a continuation of our previous works and ML algorithms [115–117] which are discussed next.

First, the Ensemble CorrDet with Adaptive Statistics (ECD-AS) algorithm as well as the research efforts presented in [116,117] formed the foundation for the CECD-AS algorithm which made multi-pronged cyberattack detection possible. Nagaraj et al. [115] propose the ECD-AS strategy to detect FDI attacks in the IEEE 118-bus system [139]. The paper presents a method for using adaptive statistics to detect bad data in power systems that takes into account the normal or anomalous characteristics of the continuously changing state of a power system. The ECD-AS algorithm extends the work of the CorrDet algorithm [116] and the ECD algorithm [117]. ECD-AS can be understood as a collection of CorrDet detectors that capture adaptive statistics for each local CorrDet environment. The data-driven bad data detection technique proposed in this paper employs adaptive mean, adaptive covariance, and adaptive anomaly threshold calculated with a sliding window approach for incoming data to adapt to changes in system state. Extensive experimentation with the hyper-parameters of the ECD-AS process reveals, in the case study on the IEEE 118-bus system, an optimal solution with much superior bad data detection results than the state-of-the-art ML algorithm in accuracy, precision, recall, and F1-score. A shortcoming of this work is that how well it scales to bigger grid sizes has yet to be determined because it was tested solely on the IEEE 118 system. Further research should explore this topic.

 doi:10.20944/preprints202403.1701.v1



**Procedure 1** Cross-Layer Ensemble CorrDet with Adaptive Statistics (CECD-AS) algorithm

*Train a Cross-Layer Ensemble CorrDet classifier*:
**Input:** $\mathbf{Z}$, $\mathbf{Y}$, $\widetilde{\mathbf{Z}}$
**for** Every local Cross-layer CorrDet classifier $m = 1 : M$ **do**
    Initialize the mean $\boldsymbol{\mu}_m$ and covariance $\Sigma_m^{-1}$ of normal statistics using the sample mean and covariance of normal samples in the training set with selected *triple elements* associated with $\phi_m$
    Initialize the squared Mahalanobis distance $\mathbf{ffi}_{Z,m}$ using equation (7)
    Initialize the threshold $\tau_m$ using equation (8)
**end for**

*Test using the Cross-Layer Ensemble CorrDet classifier with Adaptive Statistics*:

**for** Every test sample $k = 1 : K_2$ **do**
    Compute the squared Mahalanobis distance $\mathbf{ffi}_{\widetilde{z}_k}$ using equation (7)
    **if** $\forall m, \delta_{\widetilde{z}_k} < \tau_m$ **then**
        Classify $\widetilde{z}_k$ as normal sample: $\widetilde{y}_k = 0$
        Update the mean $\boldsymbol{\mu}_m$ and covariance $\Sigma_m^{-1}$ using equation (9) and equation (10)
        Update the sliding window by adding $\mathbf{ffi}_{\widetilde{z}_k}$ to $\mathbf{B}$ and removing the oldest value from $\mathbf{B}$.
        Update the mean $\mu_{thr,m,-\beta}$ and variance $\sigma_{thr,m,-\beta}$ of squared Mahalanobis distances in the updated sliding window of each local Cross-layer CorrDet detector
        Update the threshold value $\tau_m$ for each local Cross-layer CorrDet detector using equation (11)
    **else**
        Classify $\widetilde{z}_k$ as abnormal sample: $\widetilde{y}_k = 1$
    **end if**
**end for**
**Output:** $\widetilde{\mathbf{Y}}$

Aljohani et al. presented the Cross-Layer Ensemble CorrDet with Adaptive Statistics (CECD-AS) algorithm in [114], which implemented a cross-layered cyber-physical power system state estimation framework.. To estimate the state of the power system, the framework incorporates data from the physical layer, and communication layer and synchronizes the measurements for the CECD-AS machine learning algorithm. Results showed that the real-time CECD-AS approach outperforms state-of-the-art state estimation methodologies in terms of F1-score for a variety of cyber attacks due to its ability to learn from data collected in multiple layers of SG and to adapt to dynamic spatio-temporal changes in measurement data. A shortcoming of this technique is that data synchronization is required. Any errors or discrepancies can lead to unanticipated adverse outcomes in the classification process. Hence, it is crucial to guarantee that the sliding window has the same duration for both layers of the grid. Future research should explore a more resilient sliding window approach to address synchronization difficulties.

In [5], Agnew et. al. extended the SDN architecture layer of the CECD-AS approach to a flat, distributed design for DoS cyber attack resiliency. As shown in Figure 9, the proposed architecture makes use of a collection of Open Network Operating System (ONOS) [140] controllers that have a distributed control and decision-making control plane for the SD-SG, referred to as D3-SDN for the 3-controller system. In [141], a subsequent benchmarking study was conducted to compare the performance of the proposed architecture with another common controller solution in SD-SG research, the POX controller[101,142,143] to demonstrate that the D3-SDN framework increased throughput and reduced latency during the midst of DoS attack scenarios when compared to the POX controller architecture. A shortcoming of this research is that we have not yet determined how well the controller framework performs in comparison to other widely used controllers such as RYU or Opendaylight. Future analytical studies should conduct performance comparisons between the ONOS framework and other modern controllers.

 doi:10.20944/preprints202403.1701.v1



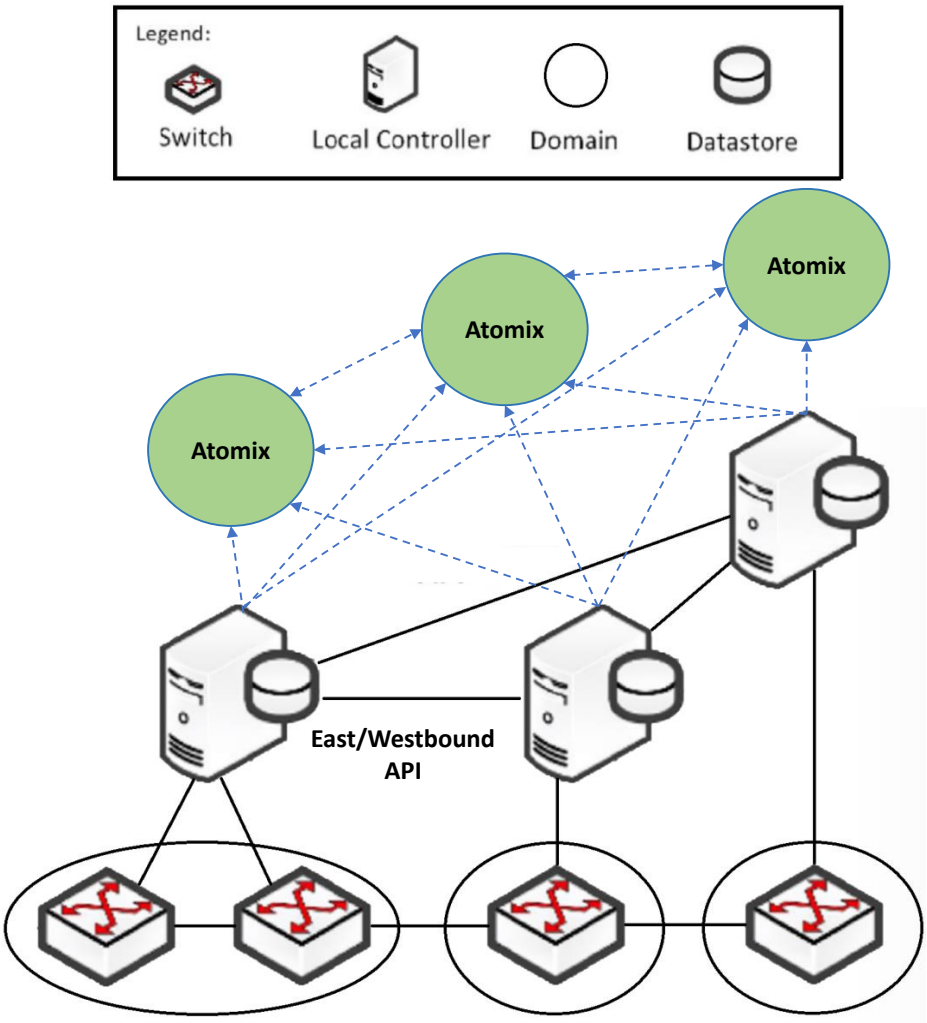



**Figure 9.** Distributed, Flat SDN Controller Architecture [141,144].

*6.2. Machine Learning*

According to the analysis conducted in [118], cyber-attack detection solutions based on a single machine learning model encounter issues like poor generalization and ineffective detection of all attack types. Zakaria et al. [119] design BoostIDS which is a novel framework that leverages ensemble learning to efficiently detect and mitigate security threats like DDoS, probe, fuzzers, and backdoor attacks in SD-SG. BootIDS is deployed as an application in the application plane of the SDN architecture and consists of two modules. The first module uses Boosting Feature Selection algorithm to select relevant SG features. The second module uses a Lightweight Boosting algorithm to effectively detect intrusions in an SD-SG. The experimental results prove that the BoostIDS has higher precision, accuracy, detection rate, and f1-score when compared with existing machine learning intrusion detection systems. A shortcoming of this work is that it is only meant to be utilized for a single controller framework. Nevertheless, in the event that a malicious actor successfully infiltrates the controller, the framework would be rendered inoperable. Further work should integrate a distributed strategy or failsafe.

Unlike the previous studies, deep learning is considered in [120] for anomaly detection of multi-pronged cyberattacks since it has great feature learning capabilities. A Hybrid Convolutional Neural Network (HYBRID-CNN) is proposed by Penpeng et. al., to identify abnormal flow due to multiple attacks such as scan, DoS, Root to Local (R2L), probe, and User to Root (U2R) attacks in SD-SG. The proposed method uses a Deep Neural Network (DNN) to memorize global features whereas the Convolutional Neural Network generalizes local features for better feature learning capabilities. Although the HYBRID-CNN effectively detects abnormal data flow with a good detection rate, one

 doi:10.20944/preprints202403.1701.v1



shortcoming of this work is that it is biased toward some attack classes. This is due to the unbalanced data sets used in the implementation. However, it provides better results than the traditional and deep learning methods. Future studies should strive to utilize a dataset that is more impartial and balanced for the purposes of training and testing.

### *6.3. Summary and Lessons Learned*

This section provides an overview of the taxonomy of multi-pronged cyberattack solutions pertaining to the security of SD-SG networks. The performance and benefits of each solution were examined and analyzed during our discussion. We observed that the main focus of each solution is to gather measurements from the communication layer and the power grid in a cross-layered manner in order to boost overall security. Nevertheless, it is imperative to acknowledge that there exist certain domains that necessitate further investigation in subsequent research efforts. The discussion regarding the optimization of these solutions has not yet taken place. The articles given do not thoroughly address the added complexity caused by the requirement for consistent time-stamped measurements from each physical and network layer, as well as each communicating device in the forwarding layer. Furthermore, their methodology necessitates comprehensive data from both layers of the SD-SG and fails to yield adequate results in the absence of either. Future research endeavors should focus on the development of optimized systems that can effectively minimize overhead and offer versatile multi-attack capabilities, functioning independently in each layer without reliance on the other.

## 7. Emerging Security Threats to SD-SG

In this section, we examine emerging potential threats to SD-SG network security in the form of cyber attacks that have yet to be researched for SD-SG and provide potential solutions found in other SDN security literature. As shown in Figure 3, the emerging threats to SD-SG network security research are the following: Low Rate Denial-of-Service (LDoS) Attacks, Controller Botnet Attacks, Controller Impersonation Attacks, and Black Hole Attacks.

### *7.1. Low Rate Denial-of-Service (LDoS) Attack*

LDoS attacks are a stealthier version of the aggressive nature of DDoS attacks [145]. LDoS attacks send low-rate traffic to a target device or network over a long period of time. LDoS attacks consume network bandwidth, computing power, and memory to degrade the target's performance or availability. LDoS attacks are intended to avoid detection and avoid flooding the target system or network with traffic. LDoS attacks can avoid intrusion detection systems and other security measures that spot high-volume attacks by sending low-volume traffic via short bursts of packets over time. LDoS attacks are aimed at long-term disruption which would cause. Over time this will degrade the QoS of affected businesses, service providers, and end users while avoiding detection by existing solutions.

Currently, defense methods of LDoS attacks involve filtering LDoS attacks, improving network parameters, and reallocation of resources [145]. Researchers used the comb filter to filter LDoS attacks from transmission control protocol (TCP) traffic by analyzing the amplitude spectrum to determine periodic parameters of the LDoS attack [146]. Other Researchers have employed using the random early detection (RED) algorithm which is an active queue management (AQM) method deployed on the router. The RED algorithm avoids congestion by pre-emptively dropping packets before the router's bufer becomes full. Research efforts [147,148] have deployed modified variations of RED and AQM methods on routers to detect LDoS attacks. Other efforts [149] have deployed machine learning models based on Q-learning to dynamically allocate resources as needed. Integration of these algorithms and methods could find vitality in SD-SG network security research. One possible challenge in transferring these techniques is the high computing cost and the lack of evaluation on larger systems such as power grids. The system's overhead and latency are increased when network traffic is filtered at the controller or application layer; this can have a significant negative influence on grid performance. Future research should explore methods of implementing these solutions or alternative approaches to enhance the

 doi:10.20944/preprints202403.1701.v1



communication performance of the SD-SG grid without compromising its efficiency. A potential solution is to transfer the processing to the dataplane layer in order to decrease communication latency and alleviate the computational burden on the controller.

### *7.2. Controller Botnet Attacks*

Botnets are malware-infected zombie networks that are controlled by a single master called the botmaster. A botnet is comprised of the following elements: bots, botmaster and command and control channel (C&C) [150]. Bots are malware-infected computers that compose the botnet network and can number in the hundreds of thousands. The C&C channel is a server that is responsible for disseminating commands and receiving information for later access by the botmaster. With control of the botnet, the botmaster can initiate cyberattacks, disseminate spam or malware, conduct ransom attacks, steal personal information, etc., and cause millions in damages [150]. A botnet architecture is shown in Figure 10. Additionally, botmasters may offer infected computers to other hackers for use in their own attacks. Because of their crucial role in network governance as aforementioned, SDN controllers are desirable targets for botmasters want to take control of them for their own advantage. The utilization of an impacted controller has the potential to propagate malware from the botnet to other devices inside the network, impacting all interconnected nodes on the network. In addition, the individual in possession of the botnet could employ the controller to initiate various cyberattacks, such as launching Denial of Service (DoS) attacks on additional networks. Moreover, the controller can be employed to collect network statistics in order to identify additional vulnerabilities within the network. Compromise controllers may cause network disruptions and outages that affect businesses, service providers, and end users.

Current research has used a variety of methods to detect botnets such as honeypots, IDSs, and machine learning [150]. Honeypots act as decoy nodes on a network for attackers to target and defense frameworks have been developed that use them [151–153]. When attackers target this device, this allows for the network operators to gain information on the size of the strength of the botnet without exposing the legitimate network nodes [154]. Other research has developed methods that detect botnet C&C server bots by using Domain Name System (DNS) queries [155–157]. The botnet C&C servers are typically Dynamic DNS (DDNS) providers. Furthermore, researchers have created IDSs to detect botnets [158–160]. A potential challenge in transferring these strategies to the SD-SG is the need to manage the additional overhead and optimize the placement of honeypot instances, as well as the machine learning (ML) and intrusion detection systems (IDS). The honeypot systems must be disguised as typical grid buses, necessitating the use of unnecessary communication to create the illusion. This will result in additional communication overhead. In order to ensure optimal performance of the grid, it is necessary to integrate ML and IDS into existing legacy systems. However, it is important to be cautious and avoid any negative impact on the grid's performance. This integration will include analyzing all traffic on the grid, which may require some adjustments to enhance the grid's efficiency. One potential option could be to utilize existing buses as honeypots sometimes, while also operating them as ordinary buses at other times. This will enable the integration of honeypots into network operations without incurring any additional expenses for network operators or communication costs. Implementing a distributed approach at the data plan layer for ML and IDS solutions has the potential to decrease communication latency and limitations. With the correct modifications, these techniques could be utilized in SD-SG defense frameworks.

 doi:10.20944/preprints202403.1701.v1



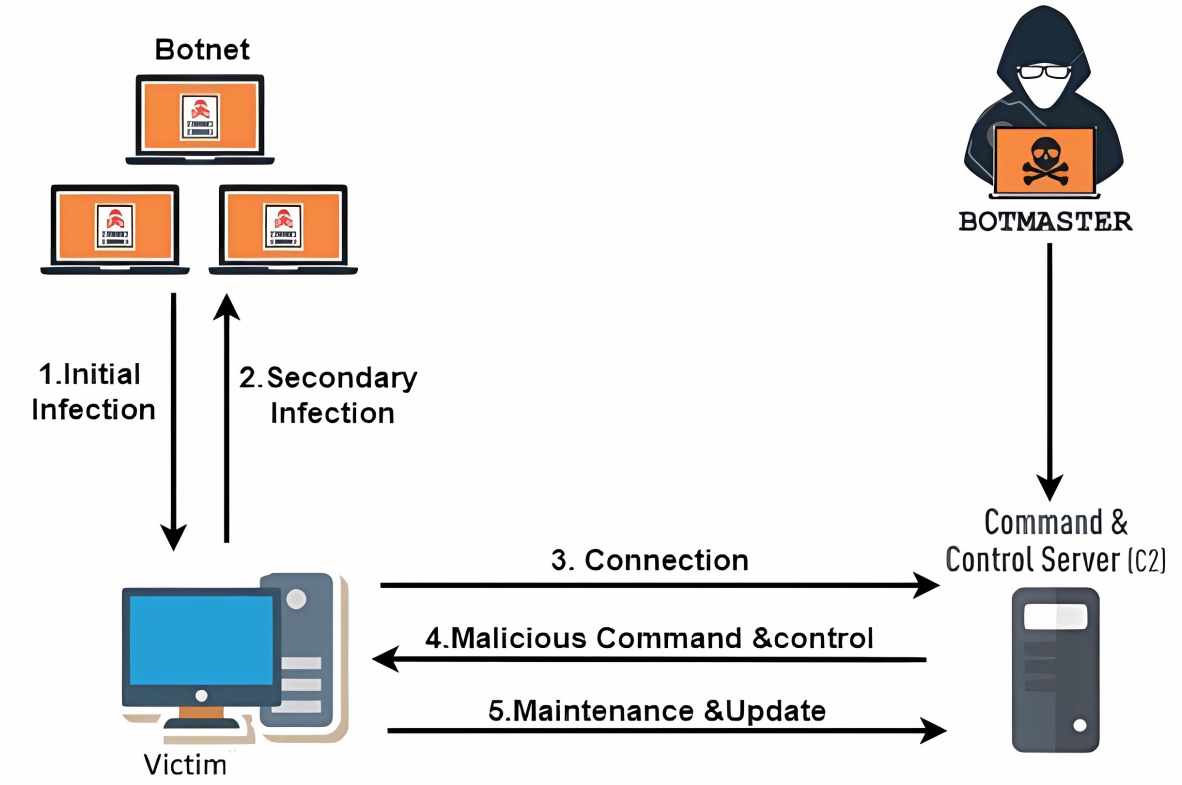



**Figure 10.** Botnet Life Cycle presented in [150].

*7.3. Controller Impersonation Attacks*

Controller Impersonation attacks involve an attacker transmitting false signals to a device or network in order to mimic a legitimate controller [161,162]. As a result, the intruder can gain access to and authority within an SDN network without authorization. In order to gain access to sensitive information, alter network traffic, or carry out other attacks, an attacker may pose as a controller and send false signals to SDN-enabled network routers or switches. To address this issue, researchers have proposed authentication models to legitimate controller traffic [161] or have proposed using IDSs and ML algorithms to detect these attacks [163]. Controller impersonation attacks necessitate further research efforts in SD-SG network security because an imposter controller can destabilize the network topology and, as a result, the power grid layer itself. This would result in a disruption of QoS for enterprises, service providers, and end users, potentially leading to significant financial losses for providers as they endeavor to mitigate the danger. A challenge that may develop when transferring the solution to SD-SG is the positioning of the authentication service. The distance between controllers may be significant, resulting in increased latency and overhead while transmitting authentication codes to the authentication or ML module. One such approach is determining the most efficient position for the authentication module, taking into account both the minimum distance and latency between all controllers. Additionally, the security of this module against prospective attackers should be considered.

*7.4. Black Hole Attacks*

A black hole attack is a cyberattack that happens when a malicious node, such as an SDN-enabled router or switch, drops, or 'swallows', every packet it receives, causing a "black hole" in the network [164,165]. Black hole attacks are one of the most devastating attacks in wireless sensor networks (WSN) [166]. WSN networks have been developed and proposed in the current SG paradigm [9]. It is possible that an attacker will take possession of these nodes to make it behave this way. Additionally, the attacker can escalate this attack by seizing control of a controller and forcing nearby switches to

 doi:10.20944/preprints202403.1701.v1



direct network messages to the black hole in order to be dropped by modifying the flow tables of the forwarding devices. This would eventually lead to network disruptions and disruption of QoS for businesses, service providers, and end users. The potential costs associated with addressing the consequences of this attack may vary depending on factors such as the ability to identify the attacker and the specific switches that have been compromised. Research has proposed a variety of methods for detection of black hole attacks such as IDs [167,168], Clustering [169,170], Cryptography [171,172], or Trust-based voting schemes [173,174]. These methods are intended to mitigate, detect, and/or prevent these techniques. Although black hole attacks are more common in wireless networks than in wired networks, SD-SG can use both wired and wireless connections. As a result, it is critical that security for these attacks be developed because a black hole attack can result in data loss and QoS disruption. One possible challenge that could occur when transferring these solutions to SD-SG is the potential complexity of managing keys or trust-based voting schemes, which may be particularly challenging for larger systems like grids and could result in delays while waiting for authentication. Clustering has demonstrated effectiveness in MANETS. A possible solution could involve employing a distributed SDN approach, where the controllers themselves implement anti-black hole attack methods for their section of the grid. This approach would enhance the performance of these techniques by assigning each controller a smaller portion of the grid to monitor.

### *7.5. Summary and Lessons Learned*

Future SD-SG network security research should concentrate on the development of defenses against the attacks aforementioned. Other SDN applications and research disciplines, such as localized SDN networks, mobile ad hoc networks (MANETs), and software-defined data centers (SDDCs), have developed customized security frameworks to combat these attacks [175]. However, substantial research and ongoing investigation are deficient in these areas of SD-SG research which is needed because customized solutions for other applications do not consider the architecture or behavior of the communication layer of SD-SG. Thus, previous specialized solutions for other domains will not adapt well to the SD-SG security. Therefore, if these vulnerabilities are identified in SD-SG's security, cybercriminals could use them to disrupt SD-SG users' QoS. In order to defend the grid from these cyberattacks, SD-SG-specific defense strategies must be developed.

## 8. Open Challenges

SD-SG will only continue to grow as a critical infrastructure for delivering power and energy to customers. In this section, new emerging challenges are outlined, including resiliency, privacy, reliability and adaptability.

### *8.1. Network Resilience after Cyberattack*

One challenge is resiliency, which is defined as how quickly a network can recover victimized nodes and restore connectivity to end users in the event of a cyberattack. As mentioned in [176], resilience in communication networks has a vital impact on society. The availability of the smart grid infrastructure, which includes/depends on the availability of the smart grid communications infrastructure will be a key indicator in the ability to sustain operations in the presence of external dangers, as well as a key protection against a significant breakdown in energy services to public and private entities.

As discussed in Section 4, DoS attacks pose a significant risk to the resilience of SD-SG networks. While research has focused on using SDN properties, such as the controller's global view of the network, to provide detection and mitigation for attack. While these tactics are effective for detecting and mitigating these attacks, they are not able to recover nodes that have failed due to DDoS/DoS attacks or due to being hijacked and used to launch DDoS/DoS attacks. The demand for an SD-SG controller technique capable of recovering fallen nodes remains unfulfilled. Other strategies have used moving target defensive techniques that focus on randomizing link pathways to make DDoS/DoS

 doi:10.20944/preprints202403.1701.v1



attacks successful. However, a strategy that allows for moving target defense while also providing node recovery has yet to be developed. The unsolved task of recovering fallen nodes and regaining those nodes with minimal overhead and strain on the SD-SG network infrastructure remains. Previous methods would fail in future SD-SG security applications because they would be unable to recover fallen nodes, resulting in a drop in quality of service. An inherent technical challenge that may occur in an MTD system with node recovery is the determination of whether the node has been successfully recovered to a secure state and is no longer compromised. One possible solution is to implement a probationary period for the node, during which it is closely watched by the "probationary module" in a local controller, under the supervision of the network operator, for a predetermined amount of time. The duration should be sufficiently long to observe traffic patterns and employ machine learning techniques to assess the probability of the node being still compromised. An efficient method is required to monitor the node without significantly burdening the controller. As previously stated, a probationary period could be established to oversee nodes that have been identified as compromised and have regained access. Another potential solution is to create a history-based voting scheme that keeps track of nodes that have been successfully attacked and feeds that information to an ML model that can use that information as a feature for future ML classifications to identify if a compromised node is acting compromised again faster than before, reducing the time of data leakage.

### *8.2. Privacy of Network Data*

The capacity to protect the privacy of data shared within the SD-SG presents an additional challenge. The privacy risk of these networks is significantly increased by controller attacks. As previously stated, such attacks can be leveraged to take unauthorized control of the SDN controller, which has entire network authority. SDN controllers can be used by attackers to monitor data transmission and, if necessary, divert traffic to hostile hosts. Furthermore, a reliable method that can identify both a compromised controller and the attacker who launched the attack has not yet been developed. Changing the controllers' ports to confuse attackers and relocating the controller through the use of software can continuously alter the topology, which would be a deterrent to attackers, but they would necessitate regular synchronization of routing logic across the network to ensure proper communication delivery due to continuously fluctuating communication links. Furthermore, it has not yet been realized that a moving target defense can recognize a compromised controller and/or the attacker. These strategies primarily aim to for prevention, leaving the issue of identifying which controller(s) are compromised, as well as the identity of the attacker, remains unresolved. Previous methods would fail in future privacy strategies because they fail to identify which controllers or forwarding devices are affected and instead focus solely on the detection of attacks. As a result, infected devices may still be present on the network, posing additional security threats like leaking the private data of users.

### *8.3. Reliability of Network Defense Mechanisms*

It is important for the SD-SG to guarantee reliability in its communication infrastructure by ensuring that very few cyber attacks work. Furthermore, the attacks that do succeed should have little to no impact. Fast recovery mechanisms should be investigated for sustainable and continuous provisioning of services with no interruptions. Further work is required on not only detecting complex cyberattacks but also mitigating these attacks within an optimal time for reliability in the time-critical SD-SGs. Considering the machine learning techniques for detection or identification, a common challenge is the unavailability and imbalance of SD-SG data sets for implementation and evaluation. This makes it difficult to ensure that model designs will be robust in real systems. There is an additional need to explore mechanisms that reduce the constraints with training data availability or imbalance, including transfer learning, federated learning, and data augmentation. Another issue is characterizing communication network traffic that has dynamic patterns that could reflect changes in the network topology or users' service demands. The current data training phase of machine learning and/or deep learning-based techniques continually has to be updated for training to adapt to the dynamic network

 doi:10.20944/preprints202403.1701.v1



traffic. Using advanced online training algorithms and automated updates depending on the network traffic pattern remains an important research area that can be explored to provide reliability in SD-SG. One technical challenge when creating a dependable solution for SD-SG that can respond quickly to attacks and enable recovery is that disabling forwarding agents (i.e. switches and routers) might result in service disruptions and the need to educate customers about Quality of Service (QoS). Hence, it is imperative that the accuracy and effectiveness of these predictions are appropriately elevated, which poses a challenge owing to the constantly changing cyberattack landscape. Hence, an optimal resolution would need a synthesis of machine learning solutions and models that can cross-validate each other's decisions rather than depending solely on a single detection and mitigation solution.

Furthermore, the reviewed research still mostly considers a single SDN controller for updating flow rules, leaving single point of failure vulnerabilities that can result in a total shutdown of the communication network. On the other hand, while the use of more than one SDN controller improves the reliability of the SD-SG, it presents new challenges such as reducing SDN controller signaling and management overhead, optimally placing SDN controllers, optimally allocating resources to SDN controllers, synchronizing the network states among SDN controllers, and selecting a cluster head from a cluster of SDN controllers. The effectiveness of previous solutions in ensuring the reliability of future SD-SG is likely to diminish due to the presence of singular controller frameworks. These frameworks introduce vulnerabilities by creating single points of failure and bottlenecks that might negatively impact network performance. To address these challenges, it is imperative for upcoming solutions to incorporate evenly distributed SDN control layers. One potential technical challenge is determining the segmentation of the SD-SG and finding the most optimal location for the SDN controllers throughout the process of replacing legacy systems. An interim approach could be to create a cloud-based, evenly dispersed SDN controller architecture that can be quickly implemented until the ideal physical locations for the controllers are determined.

### *8.4. Adaptability of Network Solutions*

As researchers continue to develop unique models and methods to defend SD-SG against attacks, the challenge of adaptability, or defense methods that are not rigidly configured, arises. To genuinely provide a holistic defense against cyber attackers, researchers must examine how flexible their solutions are to a variety of attack types, numbers of attackers, and attack scenarios. A significant portion of current research focuses on specialized SD-SG defense strategies for specific attacks. However, these are data-driven and must be regularly updated with monitored data from various sources. These strategies require data collection from both the power grid and network layers, which may add overhead and delay to SD-SG operations. A robust defense model for a diverse, multi-pronged cyberattack solution capable of detecting and responding to novel or unforeseen attacks has not yet been realized. The efficacy of previous solutions in addressing future smart grid security challenges may be limited due to their exclusive focus on specific attack types. The previous solutions have been tailored to address specific attacks, and the effectiveness of combining these solutions has not been fully explored or evaluated. There exist various alternative solutions for a given attack. An ongoing technical challenge is the dynamic nature of cyberattacks, which constantly evolve and often exhibit unique behavioral patterns. In order to tackle this challenge, future research endeavors should focus on developing a framework that can anticipate the intended actions of the communication nodes, rather than relying solely on pre-existing training data, as demonstrated in the recent study [177] that utilized communication state estimation to forecast the states of the communication layer. This framework could be efficiently included into the SDN architecture, allowing machine learning solutions to compare expected communication metrics with received metrics for the purpose of detecting attacks.

## 9. Conclusions

Current SG systems require time-consuming manual network management and are vulnerable to both physical and network security issues due to hardware and software anomalies. Mirroring

 doi:10.20944/preprints202403.1701.v1



other modern networks, SDN has been proposed as a way to automate the monitoring and control of SG communication networks, resulting in SD-SG to improve network administration, visibility, control, and security. However, just as with other modern networks, cyber-attacks are constantly evolving, requiring evolving defense and security techniques. This document presents an up-to-date, comprehensive study analyzing current state-of-the-art cyber attacks and defense methods proposed in SD-SG literature. This survey offers a thorough examination of various cyberattacks, including previously unexplored multi-pronged attacks that occur simultaneously. It goes beyond other surveys that only briefly mention security or focus on specific types of attacks or defenses. Additionally, the survey discusses potential solutions and approaches, identifies areas for future research, and highlights the ongoing challenges in SD-SG network security.

**Acknowledgments:** This material is based upon work supported by the National Science Foundation under Grant Number 1809739 and L3 Harris.

## References

1. Rehmani, M.H.; Davy, A.; Jennings, B.; Assi, C. Software defined networks-based smart grid communication: A comprehensive survey. *IEEE Communications Surveys & Tutorials* **2019**, *21*, 2637–2670.
2. Aggarwal, S.; Kumar, N.; Tanwar, S.; Alazab, M. A survey on energy trading in the smart grid: Taxonomy, research challenges and solutions. *IEEE Access* **2021**, *9*, 116231–116253.
3. Maleh, Y.; Qasmaoui, Y.; El Gholami, K.; Sadqi, Y.; Mounir, S. A comprehensive survey on SDN security: threats, mitigations, and future directions. *Journal of Reliable Intelligent Environments* **2022**, pp. 1–39.
4. Kabbara, N.; Nait Belaid, M.O.; Gibescu, M.; Camargo, L.R.; Cantenot, J.; Coste, T.; Audebert, V.; Morais, H. Towards Software-Defined Protection, Automation, and Control in Power Systems: Concepts, State of the Art, and Future Challenges. *Energies* **2022**, *15*, 9362.
5. Agnew, D.; Aljohani, N.; Mathieu, R.; Boamah, S.; Nagaraj, K.; McNair, J.; Bretas, A. Implementation Aspects of Smart Grids Cyber-Security Cross-Layered Framework for Critical Infrastructure Operation. *Applied Sciences* **2022**, *12*, 6868.
6. Singh, S.K.; Bose, R.; Joshi, A. Entropy-based electricity theft detection in AMI network. *IET Cyber-Physical Systems: Theory & Applications* **2018**, *3*, 99–105.
7. Ibdah, D.; Kanani, M.; Lachtar, N.; Allan, N.; Al-Duwairi, B. On the security of SDN-enabled smartgrid systems. 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA). IEEE, 2017, pp. 1–5.
8. Akkaya, K.; Uluagac, A.S.; Aydeger, A. Software defined networking for wireless local networks in smart grid. 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops). IEEE, 2015, pp. 826–831.
9. Abujubbeh, M.; Al-Turjman, F.; Fahrioglu, M. Software-defined wireless sensor networks in smart grids: An overview. *Sustainable Cities and Society* **2019**, *51*, 101754.
10. Demirci, S.; Sagiroglu, S. Software-defined networking for improving security in smart grid systems. 2018 7th International Conference on Renewable Energy Research and Applications (ICRERA). IEEE, 2018, pp. 1021–1026.
11. Kim, J.; Filali, F.; Ko, Y.B. Trends and potentials of the smart grid infrastructure: From ICT sub-system to SDN-enabled smart grid architecture. *Applied Sciences* **2015**, *5*, 706–727.
12. Priyadarshini, I.; Kumar, R.; Sharma, R.; Singh, P.K.; Satapathy, S.C. Identifying cyber insecurities in trustworthy space and energy sector for smart grids. *Computers & Electrical Engineering* **2021**, *93*, 107204.
13. Kong, P.Y. A review of quantum key distribution protocols in the perspective of smart grid communication security. *IEEE Systems Journal* **2020**, *16*, 41–54.
14. Butt, O.M.; Zulqarnain, M.; Butt, T.M. Recent advancement in smart grid technology: Future prospects in the electrical power network. *Ain Shams Engineering Journal* **2021**, *12*, 687–695.
15. Sirojan, T.; Lu, S.; Phung, B.T.; Ambikairajah, E. Embedded edge computing for real-time smart meter data analytics. 2019 International Conference on Smart Energy Systems and Technologies (SEST). IEEE, 2019, pp. 1–5.
16. Kong, P.Y. Routing in communication networks with interdependent power grid. *IEEE/ACM Transactions on Networking* **2020**, *28*, 1899–1911.

17. Aljohani, N.; Agnew, D.; Nagaraj, K.; Boamah, S.A.; Mathieu, R.; Bretas, A.S.; McNair, J.; Zare, A. Cross-Layered Cyber-Physical Power System State Estimation towards a Secure Grid Operation. 2022 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2022, pp. 1–5.
18. Fan, D.; Ren, Y.; Feng, Q.; Liu, Y.; Wang, Z.; Lin, J. Restoration of smart grids: Current status, challenges, and opportunities. *Renewable and Sustainable Energy Reviews* **2021**, *143*, 110909.
19. Kumari, A.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Rodrigues, J.J. Fog computing for smart grid systems in the 5G environment: Challenges and solutions. *IEEE Wireless Communications* **2019**, *26*, 47–53.
20. Sun, S.; Fu, X.; Luo, B.; Du, X. Detecting and mitigating ARP attacks in SDN-based cloud environment. IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2020, pp. 659–664.
21. McKeown, N.; Anderson, T.; Balakrishnan, H.; Parulkar, G.; Peterson, L.; Rexford, J.; Shenker, S.; Turner, J. OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM computer communication review* **2008**, *38*, 69–74.
22. Nisar, K.; Jimson, E.R.; Hijazi, M.; Memon, S.K. A survey: Architecture, security threats and application of SDN. *Journal of Industrial Electronics Technology and Application* **2019**, *2*, 64–69.
23. Zhang, Y.; Chen, M. Performance evaluation of Software-Defined Network (SDN) controllers using Dijkstra's algorithm. *Wireless Networks* **2022**, *28*, 3787–3800.
24. Kreutz, D.; Ramos, F.M.; Verissimo, P.E.; Rothenberg, C.E.; Azodolmolky, S.; Uhlig, S. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE* **2014**, *103*, 14–76.
25. Haleplidis, E.; Salim, J.H.; Halpern, J.M.; Hares, S.; Pentikousis, K.; Ogawa, K.; Wang, W.; Denazis, S.; Koufopavlou, O. Network programmability with ForCES. *IEEE Communications Surveys & Tutorials* **2015**, *17*, 1423–1440.
26. Vasseur, J.P.; Le Roux, J.L. Path computation element (PCE) communication protocol (PCEP). Technical report, 2009.
27. Enns, R. NETCONF configuration protocol. Technical report, 2006.
28. Hares, S.; White, R. Software-defined networks and the interface to the routing system (I2RS). *IEEE Internet Computing* **2013**, *17*, 84–88.
29. Zhou, W.; Li, L.; Luo, M.; Chou, W. REST API design patterns for SDN northbound API. 2014 28th international conference on advanced information networking and applications workshops. IEEE, 2014, pp. 358–365.
30. Tootoonchian, A.; Ganjali, Y. Hyperflow: A distributed control plane for openflow. Proceedings of the 2010 internet network management conference on Research on enterprise networking, 2010, Vol. 3, pp. 10–5555.
31. Hinrichs, T.L.; Gude, N.S.; Casado, M.; Mitchell, J.C.; Shenker, S. Practical declarative network management. Proceedings of the 1st ACM workshop on Research on enterprise networking, 2009, pp. 1–10.
32. Voellmy, A.; Kim, H.; Feamster, N. Procera: A language for high-level reactive network control. Proceedings of the first workshop on Hot topics in software defined networks, 2012, pp. 43–48.
33. Foster, N.; Harrison, R.; Freedman, M.J.; Monsanto, C.; Rexford, J.; Story, A.; Walker, D. Frenetic: A network programming language. *ACM Sigplan Notices* **2011**, *46*, 279–291.
34. Ahmed, Z.; Afaqui, N.; Humayan, O. Detection and prevention of DDoS attacks on software defined networks controllers for smart grid. *International Journal of Computer Applications* **2019**, *975*, 8887.
35. Santos, R.; Souza, D.; Santo, W.; Ribeiro, A.; Moreno, E. Machine learning algorithms to detect DDoS attacks in SDN. *Concurrency and Computation: Practice and Experience* **2020**, *32*, e5402.
36. Starke, A.; Nagaraj, K.; Ruben, C.; Aljohani, N.; Zou, S.; Bretas, A.; McNair, J.; Zare, A. Cross-layered distributed data-driven framework for enhanced smart grid cyber-physical security. *IET Smart Grid* **2022**, *5*, 398–416.
37. Hahn, A.; Govindarasu, M. Cyber attack exposure evaluation framework for the smart grid. *IEEE Transactions on Smart Grid* **2011**, *2*, 835–843.
38. Pedramnia, K.; Rahmani, M. Survey of DoS Attacks on LTE infrastructure used in AMI System and Countermeasures. 2018 Smart Grid Conference (SGC). IEEE, 2018, pp. 1–6.
39. Lee, S.; Shin, M.; Jang, H.s. A Study on the Application of Cross-Certification Technology for the Automatic Authentication of Charging Users in ISO 15118 Standard. *The Journal of Society for e-Business Studies* **2020**, *25*, 1–14.

40. Fehér, M.; Yazdani, N.; Hansen, M.T.; Vester, F.E.; Lucani, D.E. Smart meter data compression using generalized deduplication. GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, 2020, pp. 1–6.
41. Wang, Y.; Ruan, D.; Gu, D.; Gao, J.; Liu, D.; Xu, J.; Chen, F.; Dai, F.; Yang, J. Analysis of smart grid security standards. 2011 IEEE International Conference on Computer Science and Automation Engineering. IEEE, 2011, Vol. 4, pp. 697–701.
42. Ali, M.Q.; Al-Shaer, E.; Duan, Q. Randomizing AMI configuration for proactive defense in smart grid. 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm). IEEE, 2013, pp. 618–623.
43. Rajkumar, V.S.; Tealane, M.; Ştefanov, A.; Presekal, A.; Palensky, P. Cyber attacks on power system automation and protection and impact analysis. 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe). IEEE, 2020, pp. 247–254.
44. Mohan, S.N.; Ravikumar, G.; Govindarasu, M. Distributed intrusion detection system using semantic-based rules for SCADA in smart grid. 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D). IEEE, 2020, pp. 1–5.
45. Baig, Z.A.; Amoudi, A.R. An Analysis of Smart Grid Attacks and Countermeasures. *J. Commun.* **2013**, *8*, 473–479.
46. Fritz, J.J.; Sagisi, J.; James, J.; Leger, A.S.; King, K.; Duncan, K.J. Simulation of man in the middle attack on smart grid testbed. 2019 SoutheastCon. IEEE, 2019, pp. 1–6.
47. Wlazlo, P.; Sahu, A.; Mao, Z.; Huang, H.; Goulart, A.; Davis, K.; Zonouz, S. Man-in-the-middle attacks and defence in a power system cyber-physical testbed. *IET Cyber-Physical Systems: Theory & Applications* **2021**, *6*, 164–177.
48. Khan, A.A.; Kumar, V.; Ahmad, M. An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach. *Journal of King Saud University-Computer and Information Sciences* **2022**, *34*, 698–705.
49. El Mrabet, Z.; Kaabouch, N.; El Ghazi, H.; El Ghazi, H. Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering* **2018**, *67*, 469–482.
50. Farokhi, F. Review of results on smart-meter privacy by data manipulation, demand shaping, and load scheduling. *IET Smart Grid* **2020**, *3*, 605–613.
51. Kim, J.Y.; Hwang, Y.M.; Sun, Y.G.; Sim, I.; Kim, D.I.; Wang, X. Detection for non-technical loss by smart energy theft with intermediate monitor meter in smart grid. *IEEE Access* **2019**, *7*, 129043–129053.
52. Singh, P.; Masud, M.; Hossain, M.S.; Kaur, A. Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid. *Computers & Electrical Engineering* **2021**, *93*, 107209.
53. Han, W.; Xiao, Y. FNFD: A fast scheme to detect and verify non-technical loss fraud in smart grid. Proceedings of the 2016 ACM International on Workshop on Traffic Measurements for Cybersecurity, 2016, pp. 24–34.
54. Musleh, A.S.; Chen, G.; Dong, Z.Y. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Transactions on Smart Grid* **2019**, *11*, 2218–2234.
55. Duan, J.; Zeng, W.; Chow, M.Y. Resilient distributed DC optimal power flow against data integrity attack. *IEEE Transactions on Smart Grid* **2016**, *9*, 3543–3552.
56. Chung, H.M.; Li, W.T.; Yuen, C.; Chung, W.H.; Wen, C.K. Local cyber-physical attack with leveraging detection in smart grid. 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm). IEEE, 2017, pp. 461–466.
57. Jiang, Q.; Chen, H.; Xie, L.; Wang, K. Real-time detection of false data injection attack using residual prewhitening in smart grid network. 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm). IEEE, 2017, pp. 83–88.
58. Srivastava, A.; Agarwal, A. Emerging technology IoT and OT: overview, security threats, attacks and countermeasures. *IJERT* **2021**, *10*, 86–93.
59. Wu, L.; Wang, J.; Zeadally, S.; He, D. Anonymous and efficient message authentication scheme for smart grid. *Security and Communication Networks* **2019**, *2019*.
60. Chaudhry, S.A.; Yahya, K.; Garg, S.; Kaddoum, G.; Hassan, M.M.; Zikria, Y.B. LAS-SG: An Elliptic Curve-Based Lightweight Authentication Scheme for Smart Grid Environments. *IEEE Transactions on Industrial Informatics* **2022**, *19*, 1504–1511.

61. Ebrahimabadi, M.; Younis, M.; Karimi, N. Hardware assisted smart grid authentication. ICC 2021-IEEE International Conference on Communications. IEEE, 2021, pp. 1–6.
62. Chen, T.; Cheng, Q.; Li, X. An anonymous key agreement protocol with robust authentication for smart grid infrastructure. *Science China Information Sciences* **2022**, *65*, 1–3.
63. Shereen, E.; Dán, G. Model-based and data-driven detectors for time synchronization attacks against PMUs. *IEEE Journal on Selected Areas in Communications* **2019**, *38*, 169–179.
64. Bogdanoski, M.; Suminoski, T.; Risteski, A. Analysis of the SYN flood DoS attack. *International Journal of Computer Network and Information Security (IJCNIS)* **2013**, *5*, 1–11.
65. Holik, F.; Flå, L.H.; Jaatun, M.G.; Yayilgan, S.Y.; Foros, J. Threat modeling of a smart grid secondary substation. *Electronics* **2022**, *11*, 850.
66. Ansilla, J.; Vasudevan, N.; JayachandraBensam, J.; Anunciya, J. Data security in Smart Grid with hardware implementation against DoS attacks. 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]. IEEE, 2015, pp. 1–7.
67. Kwon, Y.; Kim, H.K.; Lim, Y.H.; Lim, J.I. A behavior-based intrusion detection technique for smart grid infrastructure. 2015 IEEE Eindhoven PowerTech. IEEE, 2015, pp. 1–6.
68. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Computer networks* **2020**, *169*, 107094.
69. Gai, K.; Qiu, M.; Ming, Z.; Zhao, H.; Qiu, L. Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. *IEEE Transactions on Smart Grid* **2017**, *8*, 2431–2439.
70. Ma, J.; Liu, Y.; Song, L.; Han, Z. Multiact dynamic game strategy for jamming attack in electricity market. *IEEE Transactions on Smart Grid* **2015**, *6*, 2273–2282.
71. Lu, Z.; Wang, W.; Wang, C. Camouflage traffic: Minimizing message delay for smart grid applications under jamming. *IEEE Transactions on Dependable and Secure Computing* **2014**, *12*, 31–44.
72. Zhang, T.; Ji, X.; Xu, W. Jamming-resilient backup nodes selection for RPL-based routing in smart grid AMI networks. *Mobile Networks and Applications* **2022**, pp. 1–14.
73. Xu, H.; Jin, X.; Jin, Q.; Luo, K.; Han, W. Cooperative Jamming Attack Strategy against Power Balance of Wireless Smart Grid Networks. 2021 22nd IEEE International Conference on Industrial Technology (ICIT). IEEE, 2021, Vol. 1, pp. 1042–1047.
74. Chen, P.Y.; Cheng, S.M.; Chen, K.C. Smart attacks in smart grid communication networks. *IEEE Communications Magazine* **2012**, *50*, 24–29.
75. Sun, C.C.; Cardenas, D.J.S.; Hahn, A.; Liu, C.C. Intrusion detection for cybersecurity of smart meters. *IEEE Transactions on Smart Grid* **2020**, *12*, 612–622.
76. Fadlullah, Z.M.; Fouda, M.M.; Kato, N.; Shen, X.; Nozaki, Y. An early warning system against malicious activities for smart grid communications. *IEEE Network* **2011**, *25*, 50–55.
77. Cairns, K.; Hauser, C.; Gamage, T. Flexible data authentication evaluated for the smart grid. 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm). IEEE, 2013, pp. 492–497.
78. Nge, C.L.; Ranaweera, I.U.; Midtgård, O.M.; Norum, L. A real-time energy management system for smart grid integrated photovoltaic generation with battery storage. *Renewable energy* **2019**, *130*, 774–785.
79. Nicanfar, H.; Jokar, P.; Leung, V.C. Smart grid authentication and key management for unicast and multicast communications. 2011 IEEE PES Innovative Smart Grid Technologies. IEEE, 2011, pp. 1–8.
80. Sha, K.; Alatrash, N.; Wang, Z. A secure and efficient framework to read isolated smart grid devices. *IEEE Transactions on Smart Grid* **2016**, *8*, 2519–2531.
81. Tran, T.T.; Shin, O.S.; Lee, J.H. Detection of replay attacks in smart grid systems. 2013 international conference on computing, management and telecommunications (ComManTel). IEEE, 2013, pp. 298–302.
82. Farraj, A.; Hammad, E.; Kundur, D. A distributed control paradigm for smart grid to address attacks on data integrity and availability. *IEEE Transactions on Signal and Information Processing over Networks* **2017**, *4*, 70–81.
83. Pavithra, L.; Rekha, D. Prevention of replay attack for isolated smart grid. Next Generation Information Processing System: Proceedings of ICCET 2020, Volume 2. Springer, 2021, pp. 251–258.
84. Li, H.; Lu, R.; Zhou, L.; Yang, B.; Shen, X. An efficient merkle-tree-based authentication scheme for smart grid. *IEEE Systems Journal* **2013**, *8*, 655–663.
85. Tanveer, M.; Kumar, N.; Naushad, A.; Chaudhry, S.A.; others. A robust access control protocol for the smart grid systems. *IEEE Internet of Things Journal* **2021**, *9*, 6855–6865.

86. Ahmed, S.; Lee, Y.; Hyun, S.H.; Koo, I. Feature selection–based detection of covert cyber deception assaults in smart grid communications networks using machine learning. *IEEE Access* **2018**, *6*, 27518–27529.
87. Wei, D.; Lu, Y.; Jafari, M.; Skare, P.M.; Rohde, K. Protecting smart grid automation systems against cyberattacks. *IEEE Transactions on Smart Grid* **2011**, *2*, 782–795.
88. Najafabadi, S.G.; Naji, H.R.; Mahani, A. Sybil attack Detection: Improving security of WSNs for smart power grid application. 2013 Smart Grid Conference (SGC). IEEE, 2013, pp. 273–278.
89. Sriranjani, R.; Hemavathi, N.; Parvathy, A.; Salini, B.; Nandhini, L. Received Signal Strength and Optimized Support Vector Machine based Sybil Attack Detection Scheme in Smart Grid. 2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT). IEEE, 2023, pp. 1–5.
90. Kumari, D.; Singh, K.; Manjul, M. Performance evaluation of sybil attack in cyber physical system. *Procedia Computer Science* **2020**, *167*, 1013–1027.
91. Fehér, M.; Yazdani, N.; Aranha, D.F.; Lucani, D.E.; Hansen, M.T.; Vester, F.E. Side channel security of smart meter data compression techniques. 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). IEEE, 2020, pp. 1–6.
92. Ali, M.Q.; Yousefian, R.; Al-Shaer, E.; Kamalasadan, S.; Zhu, Q. Two-tier data-driven intrusion detection for automatic generation control in smart grid. 2014 IEEE Conference on Communications and Network Security. IEEE, 2014, pp. 292–300.
93. Gayathri, B.; Yammani, C. Multi-Attacking Strategy on Smart Grid with Incomplete Network Information. 2019 8th International Conference on Power Systems (ICPS). IEEE, 2019, pp. 1–5.
94. Sakhnini, J.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M. Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach. *Physical Communication* **2021**, *47*, 101394.
95. Xiong, A.; Tian, H.; He, W.; Zhang, J.; Meng, H.; Guo, S.; Wang, X.; Wu, X.; Kadoch, M. A distributed security SDN cluster architecture for smart grid based on blockchain technology. *Security and Communication Networks* **2021**, *2021*, 1–9.
96. Polat, H.; Türkoğlu, M.; Polat, O.; Şengür, A. A novel approach for accurate detection of the DDoS attacks in SDN-based SCADA systems based on deep recurrent neural networks. *Expert Systems with Applications* **2022**, *197*, 116748.
97. Nagaraj, K.; Starke, A.; McNair, J. GLASS: A Graph Learning Approach for Software Defined Network Based Smart Grid DDoS Security. ICC 2021-IEEE International Conference on Communications. IEEE, 2021, pp. 1–6.
98. Jung, O.; Smith, P.; Magin, J.; Reuter, L. Anomaly Detection in Smart Grids based on Software Defined Networks. SMARTGREENS, 2019, pp. 157–164.
99. Starke, A.; McNair, J.; Trevizan, R.; Bretas, A.; Peeples, J.; Zare, A. Toward Resilient Smart Grid Communications Using Distributed SDN with ML-Based Anomaly Detection. Wired/Wireless Internet Communications; Chowdhury, K.R.; Di Felice, M.; Matta, I.; Sheng, B., Eds.; Springer International Publishing: Cham, 2018; pp. 83–94.
100. Presekal, A.; Ştefanov, A.; Rajkumar, V.S.; Palensky, P. Attack Graph Model for Cyber-Physical Power Systems using Hybrid Deep Learning. *IEEE Transactions on Smart Grid* **2023**, pp. 1–1. doi:10.1109/TSG.2023.3237011.
101. Mahmood, H.; Mahmood, D.; Shaheen, Q.; Akhtar, R.; Changda, W. S-DPs: An SDN-based DDoS protection system for smart grids. *Security and Communication Networks* **2021**, *2021*, 1–19.
102. Abdelkhalek, M.; Hyder, B.; Govindarasu, M.; Rieger, C.G. Moving target defense routing for SDN-enabled smart grid. 2022 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, 2022, pp. 215–220.

103. Zhao, J.; Gómez-Expósito, A.; Netto, M.; Mili, L.; Abur, A.; Terzija, V.; Kamwa, I.; Pal, B.; Singh, A.K.; Qi, J.; Huang, Z.; Meliopoulos, A.P.S. Power System Dynamic State Estimation: Motivations, Definitions, Methodologies, and Future Work. *IEEE Transactions on Power Systems* **2019**, *34*, 3188–3198. doi:10.1109/TPWRS.2019.2894769.
104. Zhao, J.; Singh, A.K.; Mir, A.S.; Taha, A.; Rouhani, A.; Gomez-Exposito, A.; Meliopoulos, A.; Pal, B.; Kamwa, I.; Qi, J.; Mili, L.; Mohd Ariff, M.A.; Netto, M.; Glavic, M.; Yu, S.; Wang, S.; Bi, T.; Van Cutsem, T.; Terzija, V.; Huang, Z. Power system dynamic state and parameter estimation-transition to power electronics-dominated clean energy systems: IEEE task force on power system dynamic state and parameter estimation **2021**.
105. Liu, Y.; Singh, A.K.; Zhao, J.; Meliopoulos, A.P.S.; Pal, B.; Ariff, M.A.b.M.; Van Cutsem, T.; Glavic, M.; Huang, Z.; Kamwa, I.; Mili, L.; Mir, A.S.; Taha, A.; Terzija, V.; Yu, S. Dynamic State Estimation for Power System Control and Protection. *IEEE Transactions on Power Systems* **2021**, *36*, 5909–5921. doi:10.1109/TPWRS.2021.3079395.
106. Bretas, N. An iterative dynamic state estimation and bad data processing. *International Journal of Electrical Power & Energy Systems* **1989**, *11*, 70–74. doi:https://doi.org/10.1016/0142-0615(89)90010-0.
107. Bretas, A.S.; Bretas, N.G.; Massignan, J.A.D.; London Junior, J.B.A. Hybrid Physics-Based Adaptive Kalman Filter State Estimation Framework. *Energies* **2021**, *14*. doi:10.3390/en14206787.
108. Jin, Z.; Zhao, J.; Ding, L.; Chakrabarti, S.; Gryazina, E.; Terzija, V. Power system anomaly detection using innovation reduction properties of iterated extended kalman filter. *International Journal of Electrical Power & Energy Systems* **2022**, *136*, 107613. doi:https://doi.org/10.1016/j.ijepes.2021.107613.
109. Lin, G.; Dong, M.; Ota, K.; Li, J.; Yang, W.; Wu, J. Security function virtualization based moving target defense of SDN-enabled smart grid. ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019, pp. 1–6.
110. Azab, M.; Samir, M.; Samir, E. "MystifY": A proactive Moving-Target Defense for a resilient SDN controller in Software Defined CPS. *Computer Communications* **2022**, *189*, 205–220.
111. Sivaraman, V.; Sikdar, B. A game-theoretic approach for enhancing data privacy in sdn-based smart grids. *IEEE Internet of Things Journal* **2020**, *8*, 10583–10595.
112. Samir, M.; Azab, M.; Samir, E. SD-CPC: SDN controller placement camouflage based on stochastic game for moving-target defense. *Computer Communications* **2021**, *168*, 75–92.
113. Niazi, R.A.; Faheem, Y. A Bayesian Game-Theoretic Intrusion Detection System for Hypervisor-Based Software Defined Networks in Smart Grids. *IEEE Access* **2019**, *7*, 88656–88672. doi:10.1109/ACCESS.2019.2924968.
114. Aljohani, N.; Agnew, D.; Nagaraj, K.; Boamah, S.A.; Mathieu, R.; Bretas, A.S.; McNair, J.; Zare, A. Cross-Layered Cyber-Physical Power System State Estimation towards a Secure Grid Operation. 2022 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2022, pp. 1–5.
115. Nagaraj, K.; Zou, S.; Ruben, C.; Dhulipala, S.; Starke, A.; Bretas, A.; Zare, A.; McNair, J. Ensemble CorrDet with adaptive statistics for bad data detection. *IET Smart Grid* **2020**, *3*, 572–580.
116. Trevizan, R.D.; Ruben, C.; Nagaraj, K.; Ibukun, L.L.; Starke, A.C.; Bretas, A.S.; McNair, J.; Zare, A. Data-driven physics-based solution for false data injection diagnosis in smart grids. 2019 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2019, pp. 1–5.
117. Ruben, C.; Dhulipala, S.; Nagaraj, K.; Zou, S.; Starke, A.; Bretas, A.; Zare, A.; McNair, J. Hybrid data-driven physics model-based framework for enhanced cyber-physical smart grid security. *IET Smart Grid* **2020**, *3*, 445–453.
118. El Houda, Z.A.; Brik, B.; Khoukhi, L. Ensemble Learning for Intrusion Detection in SDN-Based Zero Touch Smart Grid Systems. 2022 IEEE 47th Conference on Local Computer Networks (LCN), 2022, pp. 149–156. doi:10.1109/LCN53696.2022.9843645.
119. Abou El Houda, Z.; Brik, B.; Khoukhi, L. Ensemble Learning for Intrusion Detection in SDN-Based Zero Touch Smart Grid Systems. 2022 IEEE 47th Conference on Local Computer Networks (LCN). IEEE, 2022, pp. 149–156.
120. Pengpeng, D.; Jinguo, L.; Liangliang, W.; Mi Wen, Y.G. HYBRID-CNN: An Efficient Scheme for Abnormal Flow Detection in the SDN-Based Smart Grid. Security and Communication Networks, 2020, p. 20. doi:https://doi.org/10.1155/2020/8850550.
121. Riley, G.F.; Henderson, T.R. The ns-3 network simulator. *Modeling and tools for network simulation* **2010**, pp. 15–34.

122. De Oliveira, R.L.S.; Schweitzer, C.M.; Shinoda, A.A.; Prete, L.R. Using mininet for emulation and prototyping software-defined networks. 2014 IEEE Colombian conference on communications and computing (COLCOM). Ieee, 2014, pp. 1–6.
123. Dantas Silva, F.S.; Silva, E.; Neto, E.P.; Lemos, M.; Venancio Neto, A.J.; Esposito, F. A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios. *Sensors* **2020**, *20*, 3078.
124. Rahman, A.; Montieri, A.; Kundu, D.; Karim, M.R.; Islam, M.J.; Umme, S.; Nascita, A.; Pescapé, A. On the Integration of Blockchain and SDN: Overview, Applications, and Future Perspectives. *Journal of Network and Systems Management* **2022**, *30*, 73.
125. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.Y.; Zhang, X.; Ghias, A.M.; Koh, L.H.; Yang, L. Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things Journal* **2020**, *8*, 18–43.
126. Xie, J.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Wang, C.; Liu, Y. A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges. *IEEE Communications Surveys & Tutorials* **2018**, *21*, 393–430.
127. Gao, J.; Chai, S.; Zhang, B.; Xia, Y. Research about DoS Attack against ICPS. *Sensors* **2019**, *19*, 1542. doi:10.3390/s19071542.
128. Cho, J.H.; Sharma, D.P.; Alavizadeh, H.; Yoon, S.; Ben-Asher, N.; Moore, T.J.; Kim, D.S.; Lim, H.; Nelson, F.F. Toward proactive, adaptive defense: A survey on moving target defense. *IEEE Communications Surveys & Tutorials* **2020**, *22*, 709–745.
129. Kalman, R.E.; Bucy, R.S. New Results in Linear Filtering and Prediction Theory. *Journal of Basic Engineering* **1961**, *83*, 95–108. doi:10.1115/1.3658902.
130. Phadke, A. Synchronized phasor measurements-a historical overview. IEEE/PES Transmission and Distribution Conference and Exhibition, 2002, Vol. 1, pp. 476–479 vol.1. doi:10.1109/TDC.2002.1178427.
131. Debs, A.S.; Larson, R.E. A Dynamic Estimator for Tracking the State of a Power System. *IEEE Transactions on Power Apparatus and Systems* **1970**, *PAS-89*, 1670–1678. doi:10.1109/TPAS.1970.292822.
132. Nishiya, K.I.; Takagi, H.; Hasegawa, J.; Koike, T. Dynamic state estimation for electric power systems—introduction of a trend factor and detection of innovation processes. *Electrical Engineering in Japan* **1976**, *96*, 79–87. doi:https://doi.org/10.1002/eej.4390960511.
133. Nishiya, K.; Hasegawa, J.; Koike, T. Dynamic state estimation including anomaly detection and identification for power systems. *IEE Proceedings C Generation, Transmission and Distribution* **1982**, *129*, 192–198. doi:10.1049/ip-c.1982.0032.
134. Zainudin, A.; Akter, R.; Kim, D.S.; Lee, J.M. Towards Lightweight Intrusion Identification in SDN-based Industrial Cyber-Physical Systems. 2022 27th Asia Pacific Conference on Communications (APCC). IEEE, 2022, pp. 610–614.
135. Rathore, S.; Bhandari, A. Review of game theory approaches for DDoS mitigation by SDN. *Proceedings of the Indian National Science Academy* **2022**, *88*, 634–650.
136. Daskalakis, C.; Goldberg, P.W.; Papadimitriou, C.H. The complexity of computing a Nash equilibrium. *Communications of the ACM* **2009**, *52*, 89–97.
137. Power Systems Test Case Archive. http://labs.ece.uw.edu/pstca/, 2018.
138. Alvey, B.; Zare, A.; Cook, M.; Ho, D.K. Adaptive coherence estimator (ace) for explosive hazard detection using wideband electromagnetic induction (wemi). Detection and Sensing of Mines, Explosive Objects, and Obscured Targets XXI. International Society for Optics and Photonics, 2016, Vol. 9823, p. 982309.
139. Dabbagchi, I.; Christie, R. Power systems test case archive. *University of Washington* **1993**.
140. Berde, P.; Gerola, M.; Hart, J.; Higuchi, Y.; Kobayashi, M.; Koide, T.; Lantz, B.; O'Connor, B.; Radoslavov, P.; Snow, W.; others. ONOS: towards an open, distributed SDN OS. Proceedings of the third workshop on Hot topics in software defined networking, 2014, pp. 1–6.
141. Agnew, D.; Boamah, S.; Mathieu, R.; Cooper, A.; McNair, J.; Bretas, A. Distributed Software-Defined Network Architecture for Smart Grid Resilience to Denial-of-Service Attacks. *arXiv preprint arXiv:2212.09990* **2022**.
142. Kaur, S.; Singh, J.; Ghumman, N.S. Network programmability using POX controller. ICCCS International conference on communication, computing & systems, IEEE. sn, 2014, Vol. 138, p. 70.
143. Cokic, M.; Seskar, I. Software defined network management for dynamic smart GRID traffic. *Future Generation Computer Systems* **2019**, *96*, 270–282.

144. Oktian, Y.E.; Lee, S.; Lee, H.; Lam, J. Distributed SDN controller system: A survey on design choice. *computer networks* **2017**, *121*, 100–111.
145. Zhijun, W.; Wenjing, L.; Liang, L.; Meng, Y. Low-rate DoS attacks, detection, defense, and challenges: a survey. *IEEE access* **2020**, *8*, 43920–43943.
146. Wu, Z.; Wang, M.; Yan, C.; Yue, M. Low-rate DoS attack flows filtering based on frequency spectral analysis. *China Communications* **2017**, *14*, 98–112.
147. Zhang, C.; Yin, J.; Cai, Z.; Chen, W. RRED: robust RED algorithm to counter low-rate denial-of-service attacks. *IEEE Communications Letters* **2010**, *14*, 489–491.
148. Kuzmanovic, A.; Knightly, E.W. Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants. Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, 2003, pp. 75–86.
149. Liu, T.; He, Y.; Xiong, Q. A Q-learning based real-time mitigating mechanism against LDoS attack and its modeling and simulation with CPN. *J. Comput. Res. Develop.* **2011**, *48*, 432–439.
150. Shinan, K.; Alsubhi, K.; Alzahrani, A.; Ashraf, M.U. Machine Learning-Based Botnet Detection in Software-Defined Network: A Systematic Review. *Symmetry* **2021**, *13*, 866.
151. Luo, X.; Yan, Q.; Wang, M.; Huang, W. Using MTD and SDN-based honeypots to defend DDoS attacks in IoT. 2019 Computing, Communications and IoT Applications (ComComAp). IEEE, 2019, pp. 392–395.
152. Ja'fari, F.; Mostafavi, S.; Mizanian, K.; Jafari, E. An intelligent botnet blocking approach in software defined networks using honeypots. *Journal of Ambient Intelligence and Humanized Computing* **2021**, *12*, 2993–3016.
153. Shafi, Q.; Basit, A. DDoS botnet prevention using blockchain in software defined internet of things. 2019 16th international Bhurban conference on applied sciences and technology (IBCAST). IEEE, 2019, pp. 624–628.
154. Wang, H.; Wu, B. SDN-based hybrid honeypot for attack capture. 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE, 2019, pp. 1602–1606.
155. Sanjeetha, R.; Raj, A.; Saivenu, K.; Ahmed, M.I.; Sathvik, B.; Kanavalli, A. Detection and mitigation of botnet based DDoS attacks using catboost machine learning algorithm in SDN environment. *International Journal of Advanced Technology and Engineering Exploration* **2021**, *8*, 445.
156. Zafar, M.J.; Zubair, M. Botnet Detection and Prevention in Software Defined Networks (SDN) using DNS Protocol. *International Journal of Computer Science and Information Security (IJCSIS)* **2019**, *17*.
157. Zha, Z.; Wang, A.; Guo, Y.; Montgomery, D.; Chen, S. BotSifter: an SDN-based online bot detection framework in data centers. 2019 IEEE Conference on Communications and Network Security (CNS). IEEE, 2019, pp. 142–150.
158. Ieracitano, C.; Adeel, A.; Morabito, F.C.; Hussain, A. A novel statistical analysis and autoencoder driven intelligent intrusion detection approach. *Neurocomputing* **2020**, *387*, 51–62.
159. Nguyen, M.T.; Kim, K. Genetic convolutional neural network for intrusion detection systems. *Future Generation Computer Systems* **2020**, *113*, 418–427.
160. Ashraf, J.; Moustafa, N.; Bukhshi, A.D.; Javed, A. Intrusion Detection System for SDN-enabled IoT Networks using Machine Learning Techniques. 2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW). IEEE, 2021, pp. 46–52.
161. Mutaher, H.; Kumar, P. Security-enhanced SDN controller based Kerberos authentication protocol. 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2021, pp. 672–677.
162. Li, W.; Meng, W.; Kwok, L.F. A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures. *Journal of Network and Computer Applications* **2016**, *68*, 126–139.
163. Derhab, A.; Guerroumi, M.; Gumaei, A.; Maglaras, L.; Ferrag, M.A.; Mukherjee, M.; Khan, F.A. Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. *Sensors* **2019**, *19*, 3119.
164. Hsieh, Y.T.; Ku, C.Y. Detection of gray hole attack in software defined networks **2018**.
165. Gurung, S.; Chauhan, S. A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability. *Wireless Networks* **2020**, *26*, 1981–2011.
166. Kalkha, H.; Satori, H.; Satori, K. Preventing black hole attack in wireless sensor network using HMM. *Procedia computer science* **2019**, *148*, 552–561.

 doi:10.20944/preprints202403.1701.v1




167. Gruebler, A.; McDonald-Maier, K.D.; Alheeti, K.M.A. An intrusion detection system against black hole attacks on the communication network of self-driving cars. 2015 sixth international conference on emerging security technologies (EST). IEEE, 2015, pp. 86–91.
168. Gite, P.; Chouhan, K.; Krishna, K.M.; Nayak, C.K.; Soni, M.; Shrivastava, A. ML Based Intrusion Detection Scheme for various types of attacks in a WSN using C4. 5 and CART classifiers. *Materials Today: Proceedings* **2021**.
169. Shi, F.; Liu, W.; Jin, D.; Song, J. A cluster-based countermeasure against blackhole attacks in MANETs. *Telecommunication Systems* **2014**, *57*, 119–136.
170. Katal, A.; Wazid, M.; Goudar, R.; Singh, D. A cluster based detection and prevention mechanism against novel datagram chunk dropping attack in MANET multimedia transmission. 2013 IEEE Conference on Information & Communication Technologies. IEEE, 2013, pp. 479–484.
171. Shukla, M.; Joshi, B.K.; Singh, U. Mitigate wormhole attack and blackhole attack using elliptic curve cryptography in MANET. *Wireless Personal Communications* **2021**, *121*, 503–526.
172. Kumar, A.; Varadarajan, V.; Kumar, A.; Dadheech, P.; Choudhary, S.S.; Kumar, V.A.; Panigrahi, B.K.; Veluvolu, K.C. Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocessors and Microsystems* **2021**, *80*, 103352.
173. Keerthika, V.; Malarvizhi, N. Mitigate black hole attack using hybrid bee optimized weighted trust with 2-Opt AODV in MANET. *Wireless Personal Communications* **2019**, *106*, 621–632.
174. Naveena, S.; Senthilkumar, C.; Manikandan, T. Analysis and countermeasures of black-hole attack in manet by employing trust-based routing. 2020 6th international conference on advanced computing and communication systems (ICACCS). IEEE, 2020, pp. 1222–1227.
175. Chica, J.C.C.; Imbachi, J.C.; Vega, J.F.B. Security in SDN: A comprehensive survey. *Journal of Network and Computer Applications* **2020**, *159*, 1–23.
176. Galasso, C.; McNair, J.; Fujii, M.; Dong, Z. Resilient infrastructure. *Communications Engineering* **2022**, *1*, 27.
177. Mathieu, R.; Boamah, S.; Cooper, A.; Agnew, D.; Mcnair, J.; Bretas, A. Communication Network Layer State Estimation Measurement Model for a Cyber-Secure Smart Grid. ISGT NA 2024, 2024.