

Threat Assessment and Denial of Service Attacks in Software Defined Network based Smart Grid: A Survey

FAHEEM AHMAD QURESHI

Abstract- Smart Grid (SG) is the super critical infrastructure (CI) that fulfils the energy demands of the public, state departments, and also energises and regulates the operations of other CIs. This significant role of SG demands an efficient and reliable underlying infrastructure; power system, communication layer, and SG applications; to enable a secure and operational SG. Although SG has revolutionised the traditional electric grid but its communication layer still lacks efficient management, network automation, programmability, scalability, monitoring, and control. Software defined networks (SDN), offering a greater degree of flexibility, control, and programmability, has a great scope to complement the communication domain of SG; meanwhile also introduces certain vulnerabilities. The emerging SDN based SG (SDN-SG) paradigm is in infancy stages in terms of threat assessment and defence mechanisms. Like, one of the severest cyber attacks, denial of service (DoS) attacks, which overwhelms the network resources to curtail the availability of the network for legit users, are still not well-addressed for SDN-SG in the literature. This paper comprehensively surveys the vulnerabilities and associated assessment models of SDN-SG. First, the existing threat assessment models and their adaptability for SDN-SG is evaluated. Afterwards, DoS attacks and associated mitigation techniques for SDN and their scope for SDN-SG are comprehensively studied. Various DoS attacks are identified which are still unaddressed in SDN-SG. In the end, machine learning (ML) techniques are reviewed for securing SDN-SG against a wide spectrum of DoS attacks. Furthermore, we also present challenges, issues, and future research directions related to threat assessment, DoS attacks, and ML based mitigation techniques for SDN-SG.

Index Terms— Software defined network (SDN), smart grid (SG), Cyber Security, Threat Assessment, Denial of Service (DoS) Attacks.

I. INTRODUCTION

The economic, safety, and societal functions of the state are maintained by various cyber-physical infrastructures. All infrastructures have their due role, but some are termed as Critical Infrastructures (CIs); essential for regulating the state operations [1]. CIs are

the backbone of the state and the electric grid (EG) is termed to be the super CI that is vital for the Faheem Ahmad Qureshi is Lead Application Engineer specialized in IT/OT layers of SCADA implementation for critical infrastructure and plant automation at National Agricultural Development Company (NADEC), Riyadh, Saudi Arabia (e-mail: faheemaq92@gmail.com). operations of other CIs. EG not only fulfil the energy demands of the public, but also energises other CIs. The existing grid framework is highly centralised, producer-controlled, outdated to support the Information and Communication Technologies (ICT), automation technologies, and also lacks the ability to fulfil the energy demands of the state [2], [3]. To address these issues, the modern form of the EG also known as Smart Grid (SG) has emerged as an effective solution [4]. SG has merged the communication technologies with the electrical grid to incorporate the novel concepts of ICT and automation to enable the two-way communication in SG [5], [6]. The communication layer of SG operates on propriety network devices with pre-installed network protocols. The network operator cannot exercise real-time changes in routing devices i.e. lacks programmability. And also the control is distributed over the network devices, that restrict the agile command and control of SG. To express the desired network policies, network operators need to configure each SG network device separately i.e. no network automation here. All these factors make the SG infrastructure static and non-adaptive with natural reluctance for novelty and innovation [7], and are also prone to security threats [8], [9]. Moreover, SG has emerged with an effort to maximise the efficiency and reliability of the power grid by absorbing the emerging research trends, but existing communication protocols lack interoperability to absorb these novel features [10]. These issues can be addressed with the emerging programmable networking infrastructure – Software Defined Networks (SDN) [11].

SDN with isolated data and control planes reinforced with the SDN applications enable programmable and efficient net-work management, and also enhanced adaptability for inno-vation and security, as desired in SG [12]. Application of SDN for SG (SDN-SG) communication has supplemented the operations of SG, meanwhile is also vulnerable to security threats. As the emerging SDN-SG is in infancy stages required to be assessed for a wide spectrum of possible vulnerabilities using any specified threat assessment technique. These threats can provoke cyberattacks such as Denial of Services (DoS) attacks, that interrupt the services for the legit users, is one of the major known threat for SDN-SG that need to be addressed. Furthermore, these threats also have the potential to trigger cascading failures – a unique feature of SDN-SG, in which the interconnected nature of SDN-SG propagates the effect of an attack from victim resources to other SDN-SG equipment, demands the attention of the research community to make SDN-SG more secure.

TABLE I: List of acronyms and corresponding definitions.

Acronyms	Definitions
AMI	Advanced Metering Infrastructure
API	Application Programmable Interface
BAN	Building Area Network
CAN	Consumer Area Network
CI	Critical Infrastructure
CIA	Confidentiality, Integrity, and Availability
CPS	Cyber Physical Systems
DER	Distributed Energy Resources
DoS	Denial of Service
DR	Demand Response
EBI	East Bound Interface
EFA	Event Flooding Attack
EV	Electric Vehicle
FAN	Field Area Network
HAN	Home Area Network
HMM	Hidden Markov Model
ICMP	Internet control message protocol
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IAN	Industrial Area Network

IoT	Internet of Things
MG	Micro Grid
ML	Machine Learning
MPLS	Multi-protocol Label Switching
NAN	Neighbourhood Area Network
NBI	North Bound Interface
QoS	Quality of Service
QoE	Quality of Experience
RERs	Renewable Energy Resources
REST	Representational State Transfer
SBI	South Bound Interface
SCADA	Supervisory Control And Data Acquisition
SG	Smart Grid
SDN	Software Defined Network
SDN-SG	Software Defined Networks based Smart Grid
SVM	State Vector Machine
TCAM	Ternary Content Addressable Memory
TCP	Transmission Control Protocol
UAVs	Unmanned Aerial Vehicles
UDP	User Datagram Protocol
VANETs	Vehicular Ad-hoc Networks
WAN	Wide Area Network
WSN	Wireless Sensor Network
WBI	West Bound Interface

A. Need for Threat Assessment in SDN-SG

Threat modelling is a technique to identify threats to help designers and architects of a system to diagnose security issues with the aim of proposing countermeasures for mitigating the threats [60]. SDN-SG is maturing with time, but still have certain exploitable vulnerabilities that can be used to trigger cyberattacks, such as the SG equipment underlying the SDN switch can be an exploitable arena to launch an attack. Consider, an SDN switch is supervising a particular power substation and an attacker gets successful to have the spoofed access to the substation AMI and flood attack traffic on it. This flood traffic will then be traversed to SDN switch to overwhelms its resources to affect its availability for substation activities – substation gets disconnected from the main grid. Such circumstances demand an extensive threat assessment to assess and critique the security of this underlying SG equipment. What is the possibility for an attacker to have the physical accessibility to the SG equipment.? Are the protocols on which SG equipment operates are updated with security patches

to block cyberattacks? Are the firewalls of substation SCADA and AMI systems are functionalising properly or not? These are some of the factors to assess the status of SDN-SG security. Furthermore, threat assessment can also indicate other possible exploitable domains. Such as, is the circuit breaker or relay can be used for launching the attack or not? If the circuit breaker or relay is fragile enough to get compromised by an attacker to launch an attack, then what are the possible paths? How SDN-SG will get effected under each case? These are some cases; there might be much more. SDN-SG, being the super critical infrastructure, demands a very rigorous evaluation of these security threats to make it secure and reliable [61]. Here, a successful threat assessment of SDN-SG can highlight all such vulnerabilities and their effect on SDN-SG, so that attack mitigation techniques can be formulated accordingly to secure SDN-SG against such threats.

From the above discussion, it is now clear that threats can be mitigated only if they get identified by the appropriate threat assessment method. There are various threat modelling approaches that can be investigated to determine their suit-ability to identify the threats in the SDN communication infrastructure of SG. Are these techniques are applicable to SDN-SG or not? If applicable, then are these techniques can be applied without any alteration or require some degree of customisation for SDN-SG? Can these techniques have the tendency to evaluate the threats of SDN-SG at north, south, and east/westbound interfaces that might lead towards cascading failures within SDN-SG? Some of the threat assessment techniques studied in the literature are Spoofing identity, Tampering with data, Repudiation, Information Disclosure, Denial of Service, Elevation of privilege (STRIDE) [62], Common Vulnerability Scoring System (CVSS) [63], Attack Trees [64], and Hidden Markov Model (HMM) [65]. These techniques are studied for SDN and in this article, we discuss how these existing threat

assessment models can be applied to SDN-SG. We also discuss the design requirements for threat assessment models for SDN-SG.

Standalone techniques, hybrid models of any of multiple standalone models, or any newly devised threat assessment technique can be utilised to develop the system model and security assessment framework outlining prominent attack vectors² in SDN-SG considering all the threats related to the controller, application and SDN-SG power system layer elements. Attack vectors that can cause cascading failures in SDN-SG, and associated mitigation techniques also need to be investigated.

B. Denial of Service (DoS) Attacks in SDN-SG

DoS attacks overwhelm the resources of the system to be unavailable for benign traffic [66]. The term, benign traffic, used in this article refers to the traffic flow that is normal and free from any sort of adversaries - traffic under no attack. In SDN-SG, DoS attacks can block access for time-critical traffic that can lead to SG failure causing havoc for other CIs that depend upon SG for energy [67]. SDN-SG needs a mitigation technique to detect and protect SDN-SG to minimise the impact of attacks and intrusion attempts while maintaining the operation of SDN-SG. Investigation of attack mitigation techniques based on machine learning (ML) can be utilised for handling cyberattacks in SDN-SG. ML-based attack mitigation schemes have the ability to handle the existing attacks, moreover, the learning abilities of ML can also tackle unknown attack. Investigation of these ML techniques for securing the SDN-SG against known and unknown attacks will be a research contribution to the cybersecurity of SDN-SG. Furthermore, SDN-SG specified evaluation metrics to evaluate the security of SDN-SG are also required for the efficient detection of cyberattacks.

TABLE II: Comparison of the comprehensive survey related to cyberattacks, DoS attacks, threat assessment and ML-based defence systems for SDN-SG. ✓ indicates that topic covered, C indicates topic is not covered, while ÷ indicates topic is partially covered. Gray highlighted articles are very closely relevant.

Article	Year	Design Requirements of DoS Attacks		DoS Attacks			Attack Mitigation Technique			Design Requirements of Threat Assessment		Threat Assessment			ML based Attack Mitigation			Future Research Directions			Main Topic
		SG	SDN-SG	SDN	SG	SDN-SG	SDN	SG	SDN-SG	SG	SDN-SG	SDN	SG	SDN-SG	SDN	SG	SDN-SG	DoS Attacks	ML based Solutions	Threat Assessment	
[13]	2011	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	C	C	C	C	C	✓	SDN cognitive radio security
[14]	2012	C	C	C	✓	C	C	✓	C	✓	C	C	✓	C	C	C	C	✓	C	✓	SG security
[15]	2013	✓	C	C	✓	C	C	✓	C	✓	C	C	✓	C	C	C	C	✓	C	✓	SG security
[16]	2014	C	C	C	÷	C	C	C	C	✓	C	C	✓	C	C	C	C	C	C	✓	SG smart home security
[17]	2015	C	C	✓	C	C	✓	C	C	C	C	÷	C	C	÷	C	C	✓	C	C	SDN cloud computing security
[18]	2015	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	C	C	C	✓	✓	✓	SDN security
[19]	2015	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	÷	C	C	✓	C	C	SDN security
[20]	2015	C	C	C	÷	C	C	÷	C	✓	C	C	✓	C	C	÷	C	C	C	C	SG metering risk assessment
[21]	2015	C	C	C	✓	C	C	C	C	✓	C	C	✓	C	C	C	C	C	C	✓	SG risk assessment
[22]	2016	✓	C	C	✓	C	C	C	C	C	C	C	✓	C	C	C	C	C	C	C	SG metering security
[12]	2016	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	C	C	C	C	C	C	SDN Security
[23]	2016	C	C	C	C	✓	C	C	C	C	C	÷	C	C	C	C	C	C	C	C	SDN optical networks security
[24]	2016	C	C	C	C	C	✓	C	✓	C	C	C	✓	C	C	÷	C	C	C	✓	SG vulnerability analysis
[25]	2017	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	C	C	C	✓	C	C	SDN Wireless Sensor Networks security
[26]	2017	C	C	÷	C	C	✓	C	C	C	C	✓	C	C	C	C	C	C	C	C	SDN Fault management
[27]	2017	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	C	C	C	C	✓	C	SDN topology discovery attacks
[28]	2017	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	÷	C	C	✓	✓	C	Stateful

																					SDN security
[29]	2017	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	÷	C	C	C	C	C	General SDN security
[30]	2018	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	C	C	C	C	C	✓	SDN control plane security
[31]	2018	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	✓	C	C	C	C	✓	General SDN security
[32]	2018	C	C	÷	C	C	✓	C	C	C	C	÷	C	C	C	C	C	✓	C	✓	Hybrid SDN security
[33]	2018	✓	C	C	✓	C	C	✓	C	✓	C	C	✓	C	C	C	C	C	C	✓	IoT enabled SG security
[34]	2018	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	C	C	C	C	C	C	SDN security
[35]	2018	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	÷	C	C	C	C	C	SDN security
[36]	2018	C	C	C	÷	C	C	C	C	✓	C	C	✓	C	C	C	C	C	C	✓	Risk assessment of SG
[37]	2018	C	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	C	C	C	C	✓	SG security
[11]	2019	C	C	÷	C	÷	✓	C	✓	C	C	C	C	✓	C	C	C	✓	C	C	SG communication security
[38]	2019	C	C	✓	C	C	✓	C	C	C	C	÷	C	C	✓	C	C	✓	C	C	SDN-IoT security
[39]	2019	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	÷	C	C	✓	C	C	SDN cloud computing security
[40]	2019	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	C	C	C	✓	C	C	SDN security
[41]	2019	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	✓	C	C	C	✓	C	SDN ML based security
[42]	2019	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	C	C	C	C	C	C	General SDN security
[43]	2019	C	C	✓	C	C	✓	C	C	C	C	÷	C	C	✓	C	C	✓	C	✓	SDN IDS
[44]	2019	C	C	✓	C	÷	✓	C	÷	C	C	✓	C	C	✓	C	÷	✓	C	✓	Network security using SDN
[45]	2019	C	C	✓	C	C	✓	C	C	C	C	÷	C	C	C	C	C	C	C	C	SDN security
[46]	2019	✓	C	C	✓	C	C	✓	C	✓	C	C	✓	C	÷	C	✓	C	✓	✓	SG security and privacy issues
[47]	2019	✓	C	C	✓	C	C	✓	C	C	C	C	÷	C	C	÷	C	✓	C	C	SG communication security
[48]	2019	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	✓	C	C	✓	C	✓	SDN security
[49]	2019	C	C	C	÷	C	C	C	C	✓	C	C	✓	C	C	C	C	C	C	✓	Risk

																					assessment of SG
[50]	2019	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	✓	C	C	✓	✓	✓	SDN DoS/DDoS attacks
[51]	2019	C	C	C	✓	C	C	✓	C	✓	C	C	✓	C	C	✓	C	C	✓	✓	IoT enabled SG security
[52]	2019	C	C	✓	C	C	✓	C	C	C	C	÷	C	C	✓	C	C	C	✓	C	SDN-UAVs security
[53]	2019	C	C	✓	C	C	✓	C	C	C	C	C	C	C	✓	C	C	C	C	C	SDN ML based security
[54]	2019	C	C	C	C	C	C	C	C	✓	C	C	✓	C	C	C	C	C	C	✓	SG security risk management
[55]	2020	C	C	÷	C	C	✓	C	C	C	C	✓	C	C	C	C	C	C	C	C	SDN blockchain security
[56]	2020	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	✓	C	C	✓	✓	✓	SDN security
[57]	2020	C	C	÷	C	C	✓	C	C	C	C	✓	C	C	C	C	C	C	C	C	SDN security
[58]	2020	C	C	✓	C	C	✓	C	C	C	C	✓	C	C	✓	C	C	✓	✓	✓	SDN VANETS security
[59]	2020	✓	C	C	✓	C	C	✓	C	✓	C	C	✓	C	C	÷	C	C	✓	C	Security of IoT devices in SG
This article	2020	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	SDN-SG threat assessment and DoS attacks

C. Contribution of this Survey Article

In this survey article, we make the following contributions:

- We review previous survey articles of threat assessment and DoS attacks of SDN, SG, and SDN-SG and highlight the important features considered in them (Subsection I-D).
- We cover a broad description of SDN, SG, and SDN-SG (Section II).
- We provide an in-depth discussion about threat assessment methods of SDN (Section III), SG (Section IV) and their suitability for SDN-SG (Section V).
- We provide a detailed survey of DoS attacks in SDN (Section VI) along with their impacts, and mitigation techniques and also evaluate each DoS attack for SDN-SG (Section VII).
- We discuss the application of ML for handling and

mitigating DoS attacks in SDN (Subsection VI-G) and further extended it for SDN-SG (Subsection VII-G).

- We outline open issues, challenges, and future research directions related to threat assessment, DoS attacks, and ML-based attack mitigation techniques in SDN-SG (Section VIII).

D. Review of Related Survey Articles

Threat assessment of vulnerabilities that might occur in topology discovery of SDN, DoS attacks, and attack mitigation techniques are studied in [27], [29]. Fault management and security threats of SDN are comprehensively analysed in [26]. A very detailed threat assessment of SDN has been performed in the article [35] for a wide variety of cyberattacks including DoS attacks. Authors of [18], [19], [40], [42] have categorised various attacks and associated mitigation techniques of SDN with much emphasis on

DoS attacks. Vulnerabilities analysis of SDN is also reviewed in detail in these articles. Application of ML for securing SDN applications is surveyed in detail in [41] while authors of [31] have applied ML for the overall security of SDN. A very detailed survey of SDN security has been performed by authors of [56] in which vulnerabilities analysis, as well as DoS attacks and mitigation techniques based on ML, are studied comprehensively. Authors of [27], [53] envisioned ML-based solutions for the DoS attacks. Early detection of DoS/ DDoS attacks in SDN is discussed by the authors in the article [50] by identifying the attack traffic at the edge switch. In addition to the security of isolated operations of SDN, other operational versions of SDN are also discussed in the literature. Hybrid SDN architectures consisting of both the SDN and traditional networks are surveyed in [32]. Distributed control of SDN has been advocated in [30] for fault tolerance and consistency in SDN. Stateful SDN featuring programmable data planes and their security against DoS attacks is comprehensively covered in [28]. SDN is also implemented with other networking paradigms and the security of such developed systems is surveyed in the literature. Like, a convolution of features of Cognitive Radio Networks (CRN) and SDN and its threat assessment is provided by the authors of article [13]. SDN based WSN are discussed in detail in [25] with much focus on threat assessment, DoS attacks, and associated mitigation techniques. DoS attacks and threat assessment of SDN in the context of cloud computing are elaborated in [17], [39]. Application of blockchain technologies with SDN to evaluate the threat assessment as well as generalise attack mitigation techniques of the blockchain-based SDN is surveyed in the article [55]. Implementation of SDN for the security of VANETs is considered in detailed in the survey article [58] highlighting the security threat design challenges of SDN based VANETs. Article [52] partially discusses the threat assessment of SDN application for UAVs. ML-based solutions are reviewed and also further extended as a future research direction. Application of SDN for IoT is discussed in [38]. DoS attacks and ML-based

attack mitigation solutions are discussed for SDN architecture.

Security evaluation of SG infrastructure considering threat assessment, DoS attacks, and mitigation techniques have been performed by the authors in the articles [14], [15], [37]. Assessment of possible risks that might occur in the SG system is highlighted by the authors to model a detailed risk assessment model [20], [21], [36], [49], [54]. IoT devices have been implemented to perform SG applications and are also vulnerable to cyber threats and attacks. A very detailed survey of IoT based SG system has been carried out by the authors [33], [51], [59] to enable a secure IoT-SG. Furthermore, there also several articles related to security concerns of SG metering [22], data security and privacy [46], [68], SG HAN security [16], and reinforcing the SG communication against possible vulnerabilities [24], [47].

Authors in [11] delineate a detailed survey of SDN-SG communication. Advantages, routing schemes, architectural schemes, resilience, traffic optimisation, privacy and security, and various SDN based case studies for SG are provided. However, DoS attacks are just discussed, and also there is not much work on the threat assessment of SDN-SG. It is evident from the above discussion that all these survey articles have reviewed threat assessment and DoS attacks of SDN and SG only, but, do not include studies on threat assessment, DoS attacks, and ML-based attack mitigation solutions on SDN-SG in any form. Although some of the articles have envisioned these domains as future research directions, but neither has comprehensively reviewed them. Thus, in this survey article, we fill this research gap and provide a comprehensive review of threat assessment and DoS attacks for SDN-SG. Comparison of the existing survey articles with the proposed article is presented in Table II. The closely related articles, discussing threat assessment and DoS attacks in SDN-SG or considering the threat assessment and DoS as future research direction, are highlighted in Gray colour.

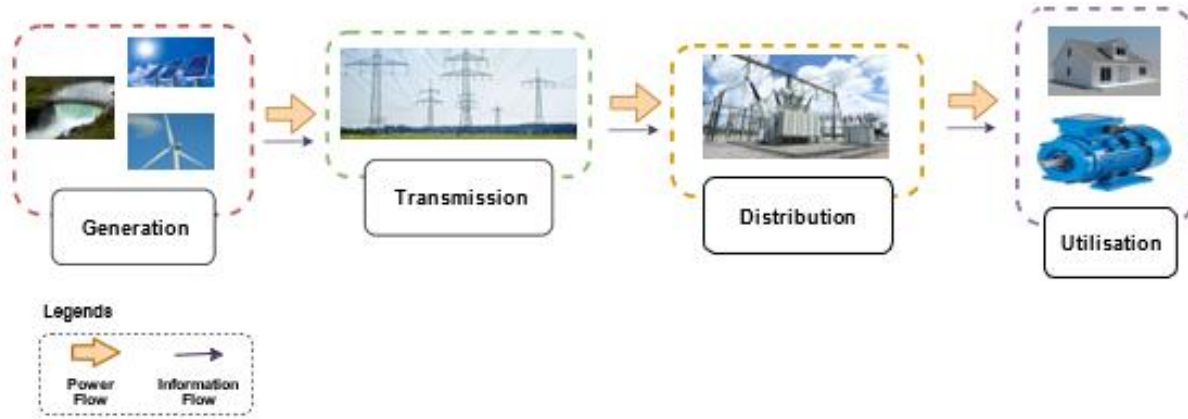


Fig. 1: Traditional Electric Grid: Uni-directional flow of power and information. Consumer are not able to feedback energy or information.

A. Article Structure

Acronyms and their definitions used in this article are provided in Table I. The rest of the paper is organised as follows: Background, operations, and security concerns of SDN, SG, and SGN-SG are discussed in Section II. Section III and Section IV surveyed the threat assessment of SDN and SG respectively. We highlight the need for threat assessment and adaptability of existing threat assessment models for SDN-SG in Section V. DoS attacks in the case of SDN are surveyed in Section VI. The scope and effect of DoS for SDN-SG is further investigated in Section VII. Open issues, challenges, and future research directions are discussed in Section VIII. Finally, we conclude the paper in Section IX.

II. SG AND SDN: BACKGROUND, OPERATIONS, AND SECURITY

In the following subsections, significance of the EG is provided. Evolution of the traditional EG into the modern grid has been discussed. Furthermore, the implementation of software-defined networks for the EG and associated security challenges are also discussed.

A. Overview of Smart Grid

Over the past 134 years, EG networks have evolved from small localised stations such as the one in Pearl Street Station in New York in 1882 [69], to a fully controlled and digitised Smart Grid (SG) system serving various geographical areas. Traditionally the

term “grid” represented all the four major components of the electric power system such as the: power system generation; power system transmission; power system distribution; and power system control [4]. The EG is considered to be the super CI that supports the working of other CIs and underlying CPS. Considering the significance of EG, the research community has put great efforts to enhance its efficiency and security.

The traditional EG has served mankind for the duration of over one century, but with the passage of time, its infrastructure is now outdated to fulfil the energy demands of the society. Such as, in most of the developing countries, legacy EGs are still utilising the conventional procedures of inefficient generation, long-distance transmission causing power dissipation, error-prone distribution, and energy craving electrical appliances [2]. Talking about the feasibility of the existing EG for emerging technologies, the grid infrastructure is reluctant to absorb the ICT, automation, control technologies [3], and also the integration of renewable energy resources (RERs) [70]. This restricts the implementation of modern EG features like dual power flow and dual information flow [71], contrast to the unidirectional flow of power and information in the traditional EG as shown in Fig. 1. Furthermore, operations of the traditional grid is on inefficient electro-mechanical fault management and mitigation mechanisms and hence are more prone to fail-overs [72]. To tackle these issues and challenges, smart grid, the next-generation EG was proposed to

fulfil future electricity demands smartly and efficiently.

- 1) *Smart Grid*: In the SG, power system generation, distribution and management, and control are upgraded by the incorporation of two-way communication and sophisticated communication technologies [5], [6] providing (a) reliability (b) scalability, in response to increasing customers and their respective demands (c) efficient, by maximising the utilisation of resources and minimising losses (d) flexible, by allowing the system to include and adapt new technologies and (e) secure, providing adequate resilience against electrical faults [73]–[75].

SG operational framework lies mostly in two-way communication between producers of energy and consumers, thus engaging the end-customers in the grid operations [73]. SG has also significantly enhanced sensing and actuation abilities which can be used to provide data acquisition, information exchange and control between grid components. Such data acquisition and control are facilitated through an upgraded, reliable and robust communication infrastructure providing near real-time communications for instantaneous monitoring and command and control of the SG [4], [73], [76]–[78].

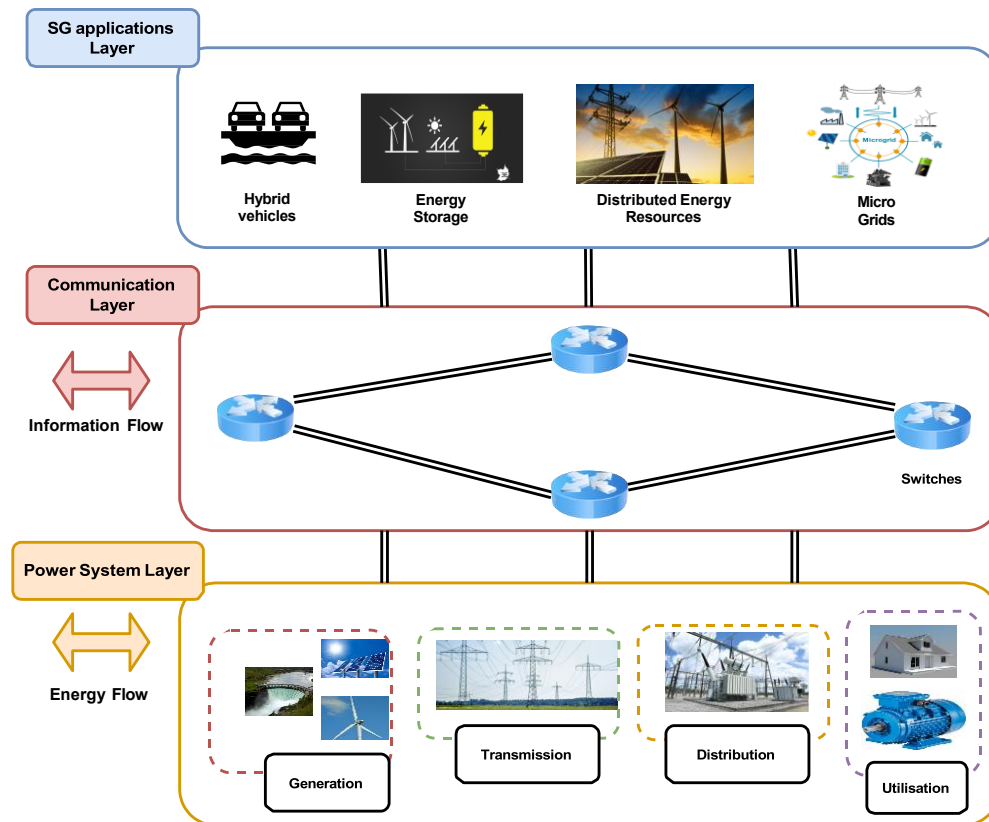


Fig. 2: Framework of SG: Layer-1: Power system elements, Layer-2: Communication layer providing connectivity among power system elements, Layer-3: SG application layer enabling emerging technologies into SG.

- 2) *Smart Grid Network Architecture*: SG is a heterogeneous complex network that can be divided into three-layer architecture [79] as presented in Fig. 2. The first layer, electric power layer consists of a) power generation containing electric power plants, b) power transmission supporting the transportation of power from

remote power plants to the distribution stations, c) power distribution disseminating the energy to end consumers, and d) power utilisation premises accommodating all sort of residential, commercial, and industrial consumers [80], [81].

After the electrical power system, comes the communication layer that constitutes the communication network for SG including Consumer Area Network (CAN), Neighbourhood Area Network (NAN), and Wide Area Network (WAN) [7], [9], [82]. CAN contains Home Area Network (HAN), Building Area Network (BAN), and Industrial Area Network (IAN) which enables the connectivity among the devices in the consumer premises. HAN deals with residential users, while BAN and IAN deal with commercial users respectively. NAN, also termed as Field Area Network (FAN) collects the data from consumers (CAN) and transmits it to the electric utility for further processing. It includes services such as smart metering, real-time pricing, and distribution automation. WAN accounts for the wide-area monitoring, wide-area control, and wide-area protection of SG. WAN aggregates data from all the associated NANs to have the overall global view of the SG for reliable monitoring of the grid.

In the last, Smart applications layer offers state of art features like supervisory control and data acquisition systems (SCADA) for remote monitoring and control of SG [83], Advanced Metering Infrastructure (AMI) enabling remote metering/billing and dynamic tariffs [84], intelligent Demand re-sponse (DR) management to efficiently meet load requirements [85], plug-in electric vehicles [86], and energy storage systems [87]. Furthermore, Micro-Grids (MG) [88] and Distributed Energy Resources (DER) [89] are the two most

prominent applications of the SG.

3) *Special requirements of smart grid in terms of communication:* The two-way communication and automation requirements of SGs requires a communication network that is integrated, high performing, reliable, scalable and secure. Desired requirements of SG in terms of communication are further outlined below:

- (i) Real Time Monitoring and Management - The use of smart-meters exchanging information on energy usage, demand, time and frequency of use etc enabling features and applications such as real-time billing, load balancing and demand-side management requires an efficient real-time communication system.
- (ii) Fault Tolerant and reliable Communications - The integration of RERs, electric hybrid vehicles etc into SG demands a highly reliable communication infrastructure. In addition, it is desirable that SG communications are more resilient and responsive against failures i.e. auto-nomic and self-healing [8].

Secure - SG communication needs to be more resilient to cyber-attacks [7], [9]. As SG applications like SCADA, AMI, coordination of DERs and MGs with the main grid, demand response and dynamic pricing, all are enabled by SG networks like CAN, NAN, and WAN, which require resilient and highly secure SG communication infrastructure.

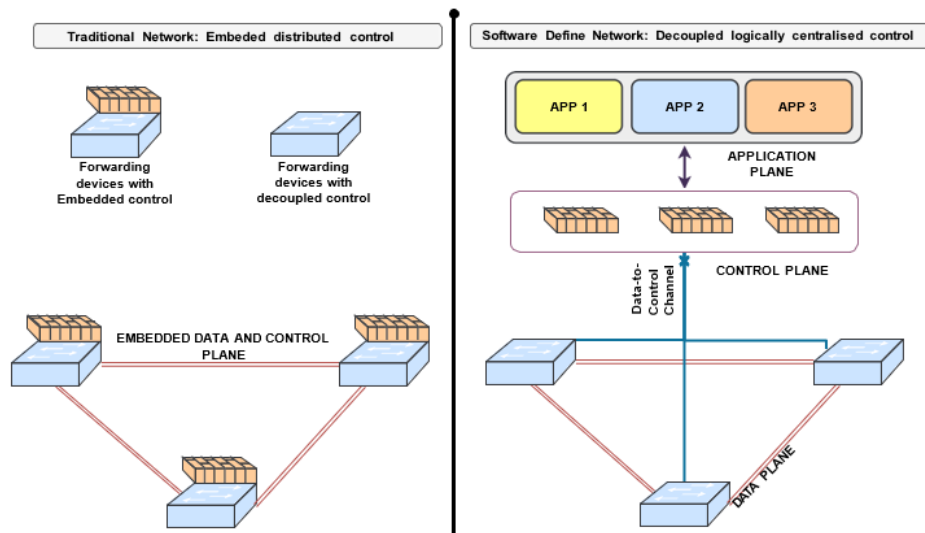


Fig. 3: Comparison of traditional networks and SDN.

- (iii) Interoperability - SG communications have to operate in a diversified environment across different vendors and networks such as HAN, NAN, FAN, and WANs and they also need to be able to absorb new technologies like hybrid electric vehicles and cloud technologies.
- (iv) Scalability - SG is a customer-oriented and needs to be scalable to match the ever-increasing number of customers and associated demands [90].
- (v) Automation - In SG automation techniques reducing error-prone human involvement is required to reconfigure and reroute traffic dynamically depending on the under-lying characteristics and conditions of the network.
- (vi) Energy Efficient - Energy crisis and green computing is the major issue of the current era calling for energy-efficient infrastructures. Traditional networks are also not energy efficient as their operation is mostly dependant on old power-hungry infrastructure [12].

To overcome the said issues in traditional networks and to accommodate the SG applications, Software-Defined Net-working (SDN) has emerged as a novel solution and natural candidate to offer programmability, adaptability for innovation, and network resilience.

B. Software Defined Networks (SDN)

SDN is an emerging communication environment that provides a flexible and configurable networking paradigm in which resources are programmable [12]. In conventional net-works the control plane is distributed among the forwarding devices like routers or switches, whereas SDN provides a logically centralised control plane with the help of a centralised controller [91] which is shown Fig. 3. The centralised controller provides the global view of the network, allowing efficient traffic engineering, optimisation, and link failure recovery [92]. SDN architecture comprises of three planes as shown in Fig. 3:

- (i) Data Plane: contains forwarding devices that

route the traffic following rules defined by the control plane.

- (ii) Control Plane: defines routing flow rules and also implements policies defined by the application layer.
- (iii) Data-Control Link: traverse control traffic between switches and SDN controller enabling the flow of packet_in requests, installation of flow rules and implementation of network policies.
- (iv) Application Plane: allows the development and implementation of networking applications and policies.

Communication between these planes is provided by Application Programmable Interfaces (APIs). These APIs are communication protocols that define the set of rules for interaction between the data, control, and application planes. Fig. 4 is depicting the role of each interface in SDN architecture. These APIs are further described as:

- (i) Southbound Interface: A communication protocol enabling the interaction between the SDN controller and forwarding elements in the data plane. This API pushes the flow rules and network configurations to the switches to define paths to route the data.
- (ii) Northbound Interface: The ability of SDN to support SDN applications is enabled by this interface as connects the control and application plane. It provides information about underlying network elements to the application developers for network abstraction required for the development of applications. Moreover, this API also implements network policies in the control plane and control then executes those policies.
- (iii) East/ Westbound Interfaces: These interfaces are utilised in the distributed SDN architectures. SDN con-troller talks to each other using the eastbound interface. The westbound interface allows the communication of legacy network devices with the SDN controller.

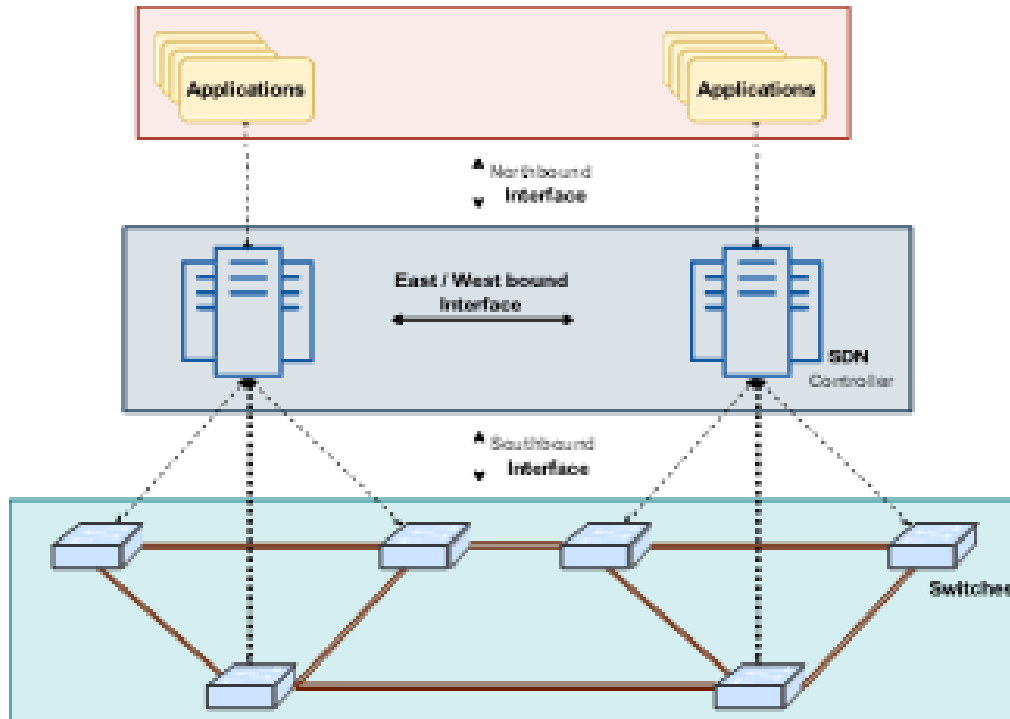


Fig. 4: Interfaces of SDN architecture.

1) *Operational Mechanism of SDN*: In SDN, switches route the traffic following the flow rules installed by the SDN controller. Installation of flow rules and routing of traffic is provided by specified steps as shown in Fig. 5. The most critical role for SDN operations is the flow of control traffic via data-control link – highlighting the significance of the data-control link. There are two types of channels that can be applied: In-band channel and the out-band channel. For the In-band mechanism, control traffic and data traffic have to share the same channel. Implementing in-band mode is complex as switch first have to search and establish a data-control link to the switch. Moreover, as the channel is shared so the congestion of channel caused by data traffic might affect the flow of control traffic. Delayed or denied control traffic can compromise SDN communication. Whereas in out-band mode, there is a dedicated channel for the flow of control traffic between switches and SDN controller; enabling reliable SDN communication. This in-band channel is more expensive than its counterpart, as additional resources are required, but it is more secure and reliable.

C. SDN based SG

1) *Software Defined Networks for Smart Grid*: The

flow of information in SG to communicate the data needs to be regulated by a set of developed rules and regulations as standards. Institute of Electrical and Electronics Engineers (IEEE), International Electrotechnical Commission (IEC), and other standardisation bodies have developed certain protocols for the SG system.

These protocols have well addressed the application of SG environments in terms of communication but are not sufficient in addressing the communication requirements in terms of QoS, traffic engineering and prioritisation and resilience to handle the time-critical traffic of SDN-SG [11]. Initially, SG communication was carried out using multi-protocol label-switching (MPLS), but it lacks the feasibility for the progressive innovation in SG as MPLS switching and routing elements need to be reconfigured with any update in SG communication policies [93]. This reconfiguration process temporarily disrupts the MPLS functionality and thus also SG operations which are not acceptable in super CI like SG. As a result, researchers have employed SDN to incorporate ever-changing and dynamic demands of SG. However, SDN in SG system is still in the infancy stage and lacks standardisation and as a result, researchers have

customised SG standards to ensure the proper operation and regulation of the SG system.

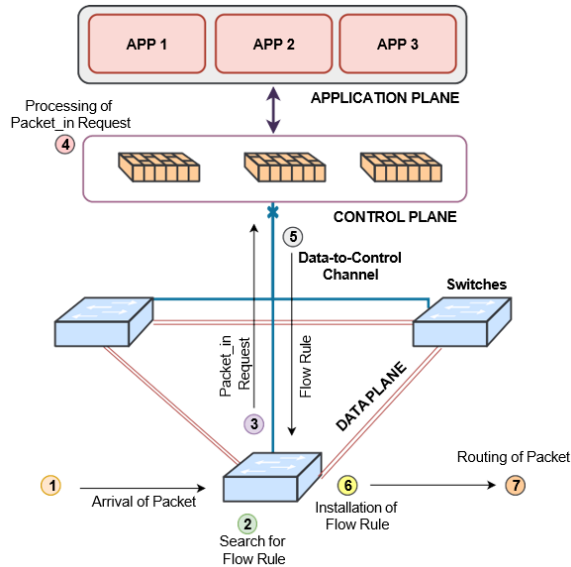


Fig. 5: Operational procedures of SDN.

2) *Features of SDN bringing novelty to SG:* SDN controller applications can be modelled as such so that they can identify the malware packets and drop them. In addition, SDN also introduces novel features such as programmability, centralised

control, and network management to SG communication. Comparative analysis of the traditional EG, SG, and SDN-SG is formulated in Table III.

Simulation Study of SDN-SG: The Integrated SDN-SG environment requires a platform of simulation that supports both EG system components and also the communication components which can be achieved by either incorporating the EG simulators with communication simulators or by formulating a novel simulation environment that can support SDN-SG. Various contributions have embedded network simulator NS-3 with MATLAB [104], Mininet [94], and hybrid systems modelling and evolution (THYME) [11]. Some papers are discussing the usage of MATLAB [105], while others are utilising MATLAB with OMNeT++ [106]. Simulator like Distribution System Solver network (DSSnet) has also been proposed to have built-in support for both the power and communication aspects of SDN-SG [107]. Various simulation studies are carried out by employing the real testbeds environments of power grids like the IEEE 39 Bus System [97] or WSCC 9 Bus test system [108] etc.

TABLE III: Comparative Analysis of traditional electric grid, SG, and SDN-SG. Adopted and improved from [11].

Parameters	Traditional Electric Grid	Smart Grid	SDN Smart Grid
Programmability	No programmability	Programmability at limited level	Highly Programmable [94]
Scalability	Limited Scalability	Scalable	Highly scalable [90]
Adaptability for innovation	Reluctant to innovation	Innovation is absorbable	Highly Adaptive to innovation [11], [95]
Standardisation	Standards are well established	Standards are maturing	Standardisation is in infancy stage [11]
Universal Language	Vendor specified	Vendor specified	Open universal language [11], [95]
Interoperability	Heterogeneous environment with lack of compatibility	Lack of compatibility between various vendor specified de-vices	Highly interoperable because of universal language of operation in SDN technology [11]
Network Management	Manual, time consuming and error-prone	Automatic, efficient and error prone	Automatic and fault tolerant [96]

Network Resilience	Prone to attacks to physical and cyber infrastructure	Reasonable resilience	Highly resilient to attacks [94], [97]
Granularity	Depend upon propriety hardware	Depend upon propriety hardware	Traffic can be identified and managed at either packet or flow level [95]
Protocol Independence	Protocols dependence	Protocols dependence	Protocol independence using open flow infrastructure [11]
Traffic Management	Not possible	Possible at minor scale	Fully capable of efficient traffic monitoring and management [96]
Consistency	Not possible	Possible	Possible [98]
Nature of control	Distributed	Distributed	Centralised [11], [99]
Implementation of network policies	Time consuming	Time consuming	Rapid and Agile [99]
Network Applications	Not possible	Require tangible physical hardware	SDN controller allow formulation of network applications at software level without recruitment of any hardware [90]
Feasibility for clouds and network virtualisation	Not possible	Not possible	Programmability feature of SDN have support for it [100], [101]
Configuration	Manual	Automatic and distributed	Automated configuration performed by the centralised SDN controller [102]
Economics of System	High due to high losses	Medium as losses are well controlled in SG	Relatively economical [103]

In this section, SDN, SDN application for SG, and the novelty that SDN will bring to SG were discussed. Brief history and transition of traditional EG to SG and then SDN-SG is described. Moreover, comparative analysis of traditional grid, SG, and SDN-SG is also provided to highlight the significance of SDN-SG.

III. THREAT ASSESSMENT AND MODELLING OF SDN

This section presents a detailed review of the literature for threat assessment and modelling of SDN in which we studied the existing threat modelling based approaches that are applied for SDN. Also, an evaluation of these approaches for applicability in SDN-SG is discussed.

A. Threat Assessment and Modelling

A threat is defined as any actor that intends to

harm the system. For any real-world practical systems, threats are plausible that are required to be investigated and mitigated accordingly. Threats are usually easy to enumerate than to characterise, easy to characterise than to measure [60]. This calls for the system that can define a formal framework to measure these threats – threat assessment models.

Threat assessment is the process of determining the risks — exploitable vulnerabilities and threats — that can be utilised to launch a cyberattack on the system. Risks evaluate the severity of threats and the probability of their occurrence.

$$Risk = Impact \times Likelihood \quad (1)$$

Impact determines the degree of damage that a particular threat can cause to system, while likelihood is the possibility of its occurrence. The outcome of this

practice is also the security risk assessment of the system that determines the capacity of the system to react to threats. But the question is how to perform these threat assessments? Security of a system is evaluated by the threat assessment of the vulnerabilities of the system subject to certain metrics. Cyber threat models constitute certain metrics – a standard of measurement – to measure the desired attribute and behaviour of the interest [130]. Consistent and fine metrics are key enablers of the cyber threat models as threats can be identified only in, they are measured correctly and accurately. A

quality metric is characterised to be clear, unambiguous, inexpensive - cost of measurements does not exceed the value of data, and interpretable [130]. Significance of these metrics is realised by a performance engineer H. James Harrington as, “Measurement is the first step that leads to control and eventually improvement. If you can’t measure something, you can’t understand it. If you can’t understand it, you can’t control it. If you can’t control it, you can’t improve it” [131].

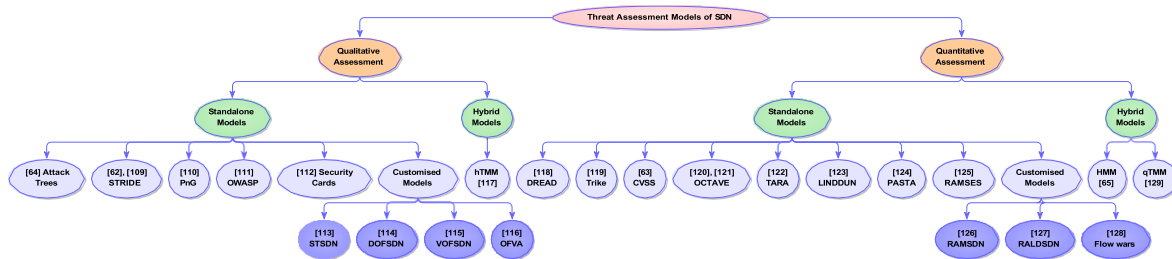


Fig. 6: Threat assessment models for evaluating security risks in SDN.

Behaviours of the complex systems like SDN, SG, or SDN- SG cannot be categorised by a single metric. A measurement framework, combining various metrics and their relationships, aka cyber threat model, is devised to evaluate behaviours of complex systems. Purpose of the cyber threat models is to address the intent and also the capabilities of the cyber threats – marked as threat attributes [60].

B. Threat Attributes

These are the distinguishing and discrete features of any threat making it unique relative to other threat types. These attributes define the willingness and abilities of the threat. There are two broad families to classify threat attributes: commitment and resource attribute [132].

- **Commitment Attributes:** describes the threat willingness to achieve its goal of harming the system. These are threat capabilities – drive of the threat to achieve its goal. Greater the commitment, greater is the ability of threat to harm the system and vice versa. Commitment attributes are defined by: 1) Intensity, as a measure of degree of willingness to harm the system, 2) Stealth, to keep

the threat undetectable by maintaining a level of secrecy, and

- 3) Time: total duration of time required by the threat to accomplish its goal of harming the system.

- **Resource Attributes:** accounts for the abilities of threats i.e. the resources (knowledge or access to the system) available to threat to achieve its goal. Higher the resources a threat has, more is its ability to harm the system. The resources attributes are further classified as, 1) Technical personnel, involves a certain group of people with desired skills set to enable the threat in its pursuit of a goal, 2) Knowledge, to understand and bypass applied defence mechanisms, and 3) Access, is the ability of the threat to infiltrate into the system.

Application of these threat attributes is utilised to define generic threat matrix. In this matrix, threats are shelved in accordance with their severity. This threat matrix provides the analyst with a platform to observe the wide spectrum of threats. This study highlights possible attack paths and also helps to identify suitable mitigation techniques.

C. Evaluation Metrics for Threat Assessment of SDN

We have discussed threat assessment as a technique to determine threats in a system. But, how these threats are identified? Here comes the role of evaluation metrics. Metric is defined as a standard of measurement. Evaluation metrics are first defined and then utilised to measure any desired attribute, such that any attribute crossing a specified threshold hint the presence of security threat. When SDN was introduced in the literature, its threats were evaluated against various evaluation metrics as shown in Table V. Here we can observe that each threat assessment method is considering certain evaluation metrics and associated features to evaluate the vulnerabilities of SDN networks, such as STRIDE is assessing controller activity by evaluating features like authentication, data integrity and tampering, Access control, and privacy [133], whereas CVSS is providing a threat scoring model by quantifying flow and routing control functions [35].

D. Threat Assessment Methods of SDN

Various threat assessment models have utilised different techniques to evaluate the risks and threats of the system. These methods comprehensively provide the abstraction of the system, attacker profiles, and potential threats leading to systems failures. Classification of these assessment models has been elaborated in this survey article as quantitative models and qualitative models as illustrated in Fig. 6. Qualitative assessment models are subjective that classify threats according to the impact and likelihood of occurrence of threat, whereas quantitative

assessment is objective that quantifies threats in terms of security risk values. These threat assessment models are further divided into two types depending upon the nature of the operation: 1) standalone models that are the complete package and operate without any external assistance, while 2) Hybrid models leverage the benefits of multiple standalone models together. Moreover, customised models are the assessment methods proposed by the authors without using any standard assessment technique, rather devising new assessment method. *It must be noted here that for the customised models used throughout the survey articles, the abbreviated form of a model derived from the initials of the title is used. Please refer to the provided citation for the full form of the acronym.* A comprehensive summary of these threat assessment methods is presented in Table IV. Details of these models are elaborated in Fig. 6 and further discussed as follows:

1) Quantitative Assessment Methods: List of quantitative

assessment models deployed for the threat assessment of SDN are as follow:

Standalone Threat Assessment Models: DREAD [118] is an acronym for Damage, Reliability/Reproducibility), Exploitability, Affected Users, and Discoverability, that quantify each threat out of 10 for each element of the title – thus providing a risk assessment in addition to threat model. Nonetheless, it requires another threat assessment technique for categorisation of attack vectors.

TABLE IV: Threat assessment methods and their adaptability for SDN.

Assessment thod			Publisher/ Inventor	Year	No. of Steps	Description	SDN Application	Ref
Quantitative	Standalone	DREAD	Microsoft	2003	3	Quantify threat vectors for risk assessment.	Unaware of SBI, NBI, and EBI/WBI vulnerabilities of SDN.	[118]
		Trike	-	2005	-	It identify relevant mitigation techniques, consistent, but has lack of documentation.	Only DoS and privacy based threats of SDN can be assessed using this technique. Unaware of SBI,	[119]

					NBI, and EBI/WBI vulnerabilities of SDN.	
CVSS	National Infrastructure Advisory Council (NIAC)	2005	3	Score calculation based method that has consistent results and also support prioritisation of mitigation mechanism.	One of most suitable technique for SDN that can identify and quantify wide spectrum of threats and also score model can incorporate the criticality of SG equipment. Unaware of SBI, NBI, and EBI/WBI vulnerabilities of SDN.	[63]
OCTAVE/ Allegro	CERT Carnegie Mellon Software Engineering Institute	2007	8	It has support for risk management, scalable, but it is time consuming and has inefficient documentation.	Not suitable for SDN as only evaluates activities not continuous processes. Unaware of SBI, NBI, and EBI/WBI vulnerabilities of SDN.	[120], [121]
TARA	Intel Corporation	2009	-	It	Can identify threat agents in SDN. Unaware of SBI, NBI, and EBI/WBI vulnerabilities of SDN.	[122]
LINDDUN	Deng	2010	6	Helps find relevant mitigation techniques and also supports prioritisation of mitigation mechanism, but is time consuming.	Suitable only for privacy threats of SDN. Unaware of SBI, NBI, and EBI/WBI vulnerabilities of SDN.	[123]
PASTA	Tony UcedaVelez	2012	8	Risk management technique that has built-in feature	SDN finds its suitability for PASTA, as this threat assessment	[124]

					of prioritising threats.	method include both the technical and business requirements by taking security input from administrator. Unaware of SBI, NBI, and EBI/WBI vulnerabilities of SDN.	
		RAMSES	Niemiec, Marcin and Jaglarz, Piotr and Jekot, Marcin and Chołda, Piotr and Boryło, Piotr	2019-	It can identify threats in NBI activity	This technique has the ability to identify both the known and unknown threats of NBI of SDN and can be further extended for NBI of SDN-SG as NBI in both cases remains almost same.	[125]
		Customised Models		-	Authors devised threat assessment technique	Customised models have greater degree of flexibility for SDN architectures.	[126]-[128]
	Hybrid	HMM	Zhijie Fan, Ya Xiao, Amiya Nayak, Chengxiang Tan	2019-	Quantification of the network status to assess threats like network scanning attack, flooding attack, switch compromised attack and ARP attack.	Hybrid techniques can cover all the possible threats of SDN. Hybrid models can be tuned to detect SBI, NBI, and EBI/WBI vulnerabilities.	[65]
		qTMM	Bradley Potteiger, Goncalo Martins, and Xenofon Koutsoukos	2016-	It has automated components and produce consistent results and also support mitigation mechanisms.	Hybrid techniques can cover all the possible threats of SDN. Hybrid models can be tuned to detect SBI, NBI, and EBI/WBI vulnerabilities.	[129]
Qualitative	Standalone	Attack Trees	Bruce Schneider	1999	Few iterations It produce consistent results and also support priori-	It can address only known threats of SDN by considering	[64]

					tisation of mitigation mechanism	each threat individually. Unaware of SBI, NBI, and EBI/WBI vulnerabilities of SDN.	
	STRIDE	Loren Kohnfelder, Praerit Garg (1999), adopted by Microsoft (2002)	1999	2	Most mature technique that also helps to find suitable mitigation mechanism, but it is time consuming.	It can address only known threats of SDN like spoofing, tampering or DoS. Aware of SBI, NBI, and EBI/WBI vulnerabilities of SDN.	[62]
	PnG	-	1999	-	It has consistent results, but is valid for only a subset of cyber threats.	Limited suitability for SDN because of narrow threats dataset. Unaware of SBI, NBI, and EBI/WBI vulnerabilities of SDN.	[110]
	OWASP-Top10	OWASP	2001	-	Supports wide spectrum of threats and also produce consistent results.	Suitable for identifying vulnerabilities in SDN applications. Unaware of SBI, NBI, and EBI/WBI vulnerabilities of SDN.	[111]
	Security Cards	-	2013	-	It can identify uncommon threats but also leads to frequent false positive.	This technique has the ability to identify both the known and unknown threats of SDN. SDN by considering each threat individually. Unaware of SBI, NBI, and EBI/WBI vulnerabilities of SDN.	[112]
	Customised Models	-	-	-	Authors devised threat assessment	Customised models have greater degree of	[113]-[116]

						technique	flexi- bility for SDN architectures.	
	Hybrid	hTMM	Software Engineering Insti- tute	2018	5	It produce consistent results and also support priori- tisation of mitigation mechanism.	Hybrid techniques can cover all the possible threats of SDN. Hybrid models can be tuned to detect SBI, NBI, and EBI/WBI vulnerabilities.	[117]

Security audit framework was proposed as “Trike” that implements the threat modelling from the defensive perspective to assess the risks of attacks [119]. Trike is a very detailed assessment technique that quantifies threats score and their likelihood of occurrence but it is limited to vulnerabilities related to DoS and elevation of privileges attacks only.

Security score model known as the Common Vulnerability Scoring System (CVSS) quantifies the vulnerabilities of the system by producing a numeric score that reflects the severity of threat [63]. It is one of the most recognised threat assessment technique suitable for cyber and also cyber-physical systems. CVSS is implemented in conjunction with other threat assessment models to identify and categorise threats and then CVSS score of threats can be calculated with online available calculators.

The operational, technological and security risks of the system are considered in Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) in defining the threat assessment model [120], [121]. It was initially introduced by Microsoft in 1999 but then evolved into its current form Allegro in 2007. It provides more robust risk assessment results without any need for risk assessment knowledge. It is an eight-

step assessment technique that evaluates four classes of threats: human attacker using cyber means, a human attacker using physical means, technical threats, and natural disasters. Although it is providing a comprehensive but it is more related to the evaluation of physical threats with least focus on cyber threats.

Threat Agent Risk Assessment (TARA) [122] identifies risk agents and also rank them according to there severity level i.e. intended objectives and methods deployed to achieve objectives. TARA with the assessment of existing vulnerabilities database determines the most exposed attack surfaces. Nonetheless, TARA is identifying the generalised vulnerabilities with a lack of detailed information for various type of cyberattacks.

Risk assessment of threats relating to privacy concerns and data security are considered in Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance (LINDDUN) that provides a compact framework for privacy assessment [123]. LIND-DDUN is a six-step technique that is well-known for identifying privacy concerns, but its main drawback is extensive time consumption.

TABLE V: Evaluation metrics for evaluating the performance of SDN security.

Assessment Model	Evaluation Metrics	Features Considered	Ref
STRIDE	Controller activity	Authentication, data integrity and tampering, Access control, privacy	[133]
	Security breaches	User access, data transmission, and control command distribution	[134]

Attack Tree	Data flooding	Confidentiality, Integrity, Availability	[135]
	Denial of Access	Attack cost, discoverability	[136]
	Information security	Software , Hardware, Service Tools, Reputation, Human Resource	[137]
CVSS	Quantification of threats	Exploitability and impact	[138]
	Scoring model of threats	Flow and routing control functions	[35]
TV-HARM	Security posture	Network centrality measure, attack rate, attack impact	[139]
HMM	Network scanning and flooding	Number of destination port, ports to hosts ratio, unsuccessful flows, average number of packets and bytes per flow, percentage of pair-flows	[65]
DELTA	Attack surface	Spoofing, redundant connection requests, corrupted control messages, TLS connection misuse	[57]
Customised Models not utilising any defined assessment technique			
RAMSES	NBI activity	Traffic demand requests	[125]
EAMSDN	SDN Controller Resource	Load on SDN controller, Traffic, delay, Traffic rate	[140]
SPHINX	Network security	Accuracy (attack detection, benign traffic), Sensitivity (false alarms, lack of genuine alarms), Performance (latency), Resource utilisation	[141]
SDNASEE	Energy	Energy efficiency by optimising network resources, traffic engineering, and security policies updating	[12]
STDPSDN	Availability	Bandwidth available relative to attack rate	[142]
SESDN	IP-MAC Address	ARP response time, Attack detection time	[143], [144]
FICUR	Traffic Patterns for security	Attack detection time, Controller utilisation	[145], [146]
SDNIPS	Intrusion	Success rate of intrusion detection relative to attack rate	[147]
SASDN	Security	Integrity, Confidentiality, Authenticity, Consistency, Availability	[148]
SSDNM	Entropy	Measuring the degree of randomness in the traffic	[149]
DDoSSDN	Network performance	Packets/sec, Flows/sec, Rate of Datapath misses, Entropy, % of packets dropped	[150]

Process for Attack Simulation and Threat Analysis (PASTA) evaluates the risks of the system considering both the technical and business objectives [124]. a risk-centric assessment technique that also supports strategic decision making by taking inputs from policymakers, operations, and governance – making it a very suitable assessment technique for enterprise SDN setups. PASTA constitutes eight steps to perform a comprehensive assessment, but it also requires support from other threat assessment methods for its various steps.

Hybrid Threat Assessment Models: Quantitative Threat Modelling Method (qTMM), aggregates the features of Attack Trees, STRIDE, and CVSS methods [129]. This is one of the most comprehensive and detailed techniques that effectively identify, categorise and quantify the threats of the desired system. However, privacy and confidentiality related threats still demand further enhancements.

Hidden Markov Model (HMM) quantifies network status to assess threats like network scanning attack,

flooding attack, switch compromised attack and ARP attack [65]. This is one of the most developed techniques for SDN based threat assessment.

2) *Qualitative Assessment Methods:* List of qualitative assessment models deployed for the threat assessment of SDN are as follow:

Standalone Threat Assessment Models: Attack Trees is considered to be the most accepted practise to model threats in either cyber, cyber-physical, or only physical systems. Attack Trees employ tree diagrams for tracing the source and path of attack – Attack root being the attack source and attack roots being the path followed to launch the attack [64]. One of its advantages is dividing the complex system into multiple sub-units and performing threat assessment for each component rather than the whole system. However, for the fine-grained detailed assessment, Attack Tree needs to be incrementally replicated for each component that might uphills the cost of the whole procedure.

The most commonly used and matured threat modelling method is Spoofing identity, Tampering with data, Repudiation, Information Disclosure, Denial of Service, Elevation of privilege (STRIDE) that identify the already known threats in any system [62], [109]. STRIDE performs the categorisation of considered threat vectors with threats specified in its tile; with each threat is defined as the violation of specified system property. This attack vector categorisation is then utilised to assess the system components and their trust boundaries to evaluate the vulnerabilities that arise as a result of interaction between system components. However, STRIDE works in conjunction with another assessment method to define the complete threat model.

The role of the human as an attacker is considered in Persona non Grata (PnG) that utilised human skills and motivations for threat modelling [110]. This technique recommends the appointment of a technical cyber expert to indicate threats by observing the operational trends – just like the investigation by an inspector for any criminal activity based on evidence. Therefore, the probability for human error exists over here and also results are not that much robust as achieved by counter digital versions of assessment techniques operated by powerful computer systems.

Applications based vulnerability testing is provided by Open Web Application Security Project (OWASP) as OWASP-Top10 that is also acknowledged as a minimum industry standard for any application testing [111]. OWASP is more suitable for the vulnerability analysis of software components of cyber or cyber-physical systems. However, it is not a complete system to assess the overall system and require another assessment model for cyber vulnerabilities.

Security Cards is a brainstorming technique to discover attacks in any system that uses a deck of 42 cards in which 9 cards for Human Impact, 13 cards for Adversary's Motivations, 11 cards for Adversary Resources, and 9 cards for Adversary's Methods [112]. Usually, a field specialist is employed to analyse the system – not a formally accepted technique but produce good results in identifying unusual and complex threats. Again, as it is a possibility of human cannot be neglected in this case also.

Hybrid Threat Assessment Models: Convolution of Security Cards and PnG evolved as a hybrid technique known as Hybrid Threat Modelling Method (hTMM) [117]. The main objective of this conjunction to mitigate false positives and consistent results. The desired requirement of comprehension for all sort of vulnerabilities is still not achieved in this technique.

It is comprehended from the above discussion that standalone threat assessment techniques are not sufficient for the detailed and comprehensive threat assessment of SDN. Authors have deployed the hybrid threat assessment techniques in which the one technique supplement the deficiency of others and vice-versa. Considering only the standalone models, STRIDE, CVSS, and Attack Trees are found to be the most suitable assessment methods for SDN; but still not the complete solution. Moving towards hybrid models, qTMM and HMM are the most suitable techniques for SDN. Implementation of standalone models is viable for the case when the assessment of any particular threat offered by the specified specialised assessment model of that threat is desired. However, for the overall and comprehensive threat assessment for evaluating all possible threats of the system, hybrid techniques are more favourable. Furthermore, various standalone and hybrid assessment techniques are also still not deployed for

threat assessment of SDN; highlighting the research gap to implement those techniques for SDN to check their suitability.

E. Review of Threat Assessment techniques for SDN
SDN technology has reasonably attracted the communication market, meanwhile also encountering security issues for which many studies assessing the vulnerabilities of SDN have been carried out in the literature. Various threat assessment techniques are reviewed in Table IV are although well-developed and practical assessment methods, but are not a suitable option for SDN in their current state. Dynamics of SBI, NBI, EBI/WBI and data-control path of SDN needs to be addressed here. A customised hybrid model by merging multiple techniques is desired to evaluate the security risks of SDN using these techniques. First, the traditional security testing tools like Nessus, Metasploit, and Nmap are utilised for assessing the security of SDN. Although these security tools have rich vulnerabilities dataset and threats libraries but are unable to produce desired results, as these tools are suitable for legacy networks – unaware of the SDN environment. The efforts to develop the threat assessment model of SDN are further extended by [113] in which authors highlight the attacks at data, control, and application layer of SDN that might compromise the availability and confidentiality of SDN network. This study reveals the fact that threats and vulnerabilities of SDN are unique compare to legacy networks and demand SDN aware threat assessment models.

Numerous studies in the literature address the security assessment of SDN. Authors in [133] are of the view in-incorporation of new features like logically centralised control and programmability are basically the potential threats of envisioned SDN paradigm. In [116], the vulnerabilities arisen due to the separation and centralisation of the control plane are discussed. Floodlight vulnerabilities leading to DoS and spoofing attacks are elaborated in [114], [115]. SDN breaches that can overwhelm the network resources are explored in [151]. OpenFlow is considered to be the *de-facto* standard protocol for southbound communication in SDN. [152] is highlighting the vulnerabilities of OpenFlow for topology poisoning attack by exploiting the host tracking service (HTS). All of these assessment tools

are limited to either frequent attacks like ARP spoofing or specific (not all) vulnerabilities in different elements of SDN. Authors in [57] have proposed a novel security evaluation tool known as DELTA that can evaluate the wide spectrum of cyber threats. It successfully discovers 26 known and 9 unknown attack scenarios in the SDN environment. DELTA employs black-box fuzzy logic to detect unknown attack cases by providing randomise in-puts and discover the test cases that lead to SDN crash. The feasibility of the proposed technique is evaluated by its implementation to four open-source SDN controllers – ONOS [153], OpenDaylight (ODL) [154], Floodlight [155], and Ryu [156]. Limitation of the proposed model is its ability to minimise human involvement in the whole process – as human feedback and interaction are required at various steps, and secondly, it requires the installation of an application agent at the SDN controller. Authors in [135] have performed a risk assessment for SDN based spacecraft communication. Attack Tree threat assessment model is utilised to identify vulnerabilities related to confidentiality, data integrity, and availability. Article [125] quantifies the risks in NBI of SDN as a product of impact and likelihood of risks. *Here impact is defined as network status corresponding to network traffic request, while likelihood targets the reputation of the source of network traffic.*

Application of graphical security assessment model has been presented in [139] in which a threat scanner observes the run-time SDN flows and defines threat scenarios that might occur. Evaluation of the risk coefficient as a metric for threat assessment in SDN has been done in [126] to assess the vulnerabilities related to DDoS attacks that can overwhelm data and control plane resources. Possible paths for launching a DoS attack on SDN are discussed in [136] using Generalised Stochastic Petri Net (GSPN) model. Authors develop a relation between risks score and the average time taken by an attacker to exploit a vulnerability to identify DoS threats. Security assessment of data and control plane is considered in [134] to identify vulnerabilities leading to DoS, data tampering and repudiation using Attack Tree and Petri Net threat assessment models.

TABLE VI: Evaluation of existing literature for threat assessment of SDN environment.

Ref	Data Plane	Control Plane	Application Plane	Data-Control Link	SBI	NBI	EBI/WBI	Known threats	Unknown threats	Assessment Model
[113]	✓	✓	✓	C	C	C	C	✓	C	Customised model - STSDN
[133]	C	✓	C	C	C	C	C	✓	C	STRIDE
[114]	C	C	C	C	✓	C	C	✓	C	Customised model - DOFSDN
[115]	C	C	C	C	✓	C	C	✓	C	Customised model - VOFSDN
[57]	✓	✓	✓	C	✓	C	C	✓	✓	DELTA
[135]	✓	✓	C	C	C	C	C	✓	C	Attack Trees
[125]	C	C	C	C	C	✓	C	✓	C	RAMSES
[139]	✓	✓	✓	C	C	C	C	✓	✓	TV-HARM
[126]	✓	✓	C	C	C	C	C	✓	C	Customised Model - RAMSDN
[136]	C	✓	C	C	C	C	C	✓	✓	Attack Trees
[134]	✓	✓	C	C	C	C	C	✓	✓	Attack Trees, STRIDE
[127]	✓	✓	✓	C	✓	✓	C	✓	C	Customised model - RALDSN
[116]	✓	✓	C	C	✓	C	C	✓	C	Customised model - OFVA
[128]	✓	✓	C	C	✓	C	C	✓	C	Customised model - Flow wars
[138]	✓	✓	C	C	C	C	C	✓	✓	CVSS
[65]	✓	✓	C	C	✓	C	C	✓	✓	Hidden Markov Method (HMM)
[137]	✓	✓	C	C	C	C	C	✓	C	Attack Trees
[35]	✓	✓	C	C	C	C	C	✓	✓	CVSS

Convolution of multiple threat assessment methods or machine learning techniques has also been elaborated in the literature. Application of machine learning (Bayesian network methodology) with CVSS is utilised in [138] to explore the vulnerabilities in SDN switches and SDN controller. Researchers implemented a hybrid threat assessment model hTMM in [65] to quantify the security status of SDN related to network scanning, flooding, ARP poisoning, and switch vulnerabilities. Comparative analysis of these assessment techniques specific to SDN is illustrated in the Table VI in which “✓” represents that particular vulnerability is discussed

while “C” depicts that specified vulnerability is not discussed in that research article.

SDN communication mutates itself with time against cyber-attacks and is now matured enough to encompass the majority of security threats. We have studied numerous security evaluation and risk assessment models of SDN, but in case of SDN application to other domains, these models do not successfully serve the purpose. There are application specified requirements that need to be addressed for devising threat assessment models. Talking about SDN-SG, here the communication requirements of SG

are the basic ingredients that need to be addressed to develop threat assessment models for SDN-SG.

F. Summary and Insights

In this section, we have provided a detailed description of the threat assessment. The need for threat assessment for the security of any system is discussed. Definition of threats and risks in the context of cyberattacks is defined. Significance of evaluation metrics as a means to identify cyber threats is assessed. Threat assessment metrics and attributes are studied to highlight the motivation for developing threat assessment models. Various threat assessment methods are reviewed for their suitability for SDN. We have analysed that some assessment techniques only identify known threats, while others also account for unknown threats. Furthermore, existing literature for the threat assessment of SDN is also presented. We envisage that there is a need for a comprehensive threat assessment model of SDN that can encompass all the vulnerabilities related to various layers of SDN architecture. SDN has been applied to a variety of organisations and is also coupled with other networks. Furthermore, various APIs are deployed for NBI, SBI in standalone, and EBI/WBI in distributed SDN. A customised and adaptive threat assessment model is desired that can evaluate the threats of such diversified SDN applications.

IV. THREAT ASSESSMENT AND MODELLING OF SG

EG has evolved over time into SG by absorbing the technical as well as security advancements; like threat assessments of SG to identify the potential threats in an effort to propose suitable mitigation techniques. Possible vulnerabilities in the electrical layer as well as in communication and application layers of SG were assessed with the implementation of various threat assessment techniques such as STRIDE [157], Attack Trees [158], DREAD [159], and CVSS [160]. These are generalised threat assessment techniques, out of which some are also applied for SDN, but their suitability for integrated SDN-SG is still not tested.

A. Threat Assessment Techniques of SG

Various evaluation metrics utilised for the threat assessment of SG are tabulated in Table VII. Because of the operation of SG on traditional

networks, these evaluation metrics are also considering the features that are suitable for non-SDN networks. Like, there is no metric that is evaluating the scenarios related to packet_in messages flooding, data-control link exhaustion, SDN control saturation, exploitation of SDN interfaces or vulnerabilities of SDN OpenFlow protocols.

- 1) *Application of STRIDE for SG threat assessment:* Industrial Control Systems (ICS) is one of the major element of SG system and authors of article [157] have performed the software enteric threat assessment of SG ICS critical components using STRIDE to evaluate the likelihood and impact of identified threats. Cloud-based SG ICS systems are considered in this study. Various vulnerabilities subject to various ICS components are also quantified with a strategy keep the least vulnerable elements on the public cloud while other ICE elements with a high-risk factor are proposed to be migrated to private cloud. Although all of the assessment is for non-SDN networks, however, this migration strategy could also be applied in securing the cloud-based SDN-SG.
- 2) *Application of DREAD for SG threat assessment:* Implementation of DREAD along with STRIDE has been performed in the article [159] to classify and evaluate risks related to wireless attacks on AMI architecture of SG respectively. Vulnerabilities related to DoS attack, false data injection and man in the middle attacks are considered. Classification of attack is achieved by categorising the trends as manual, automatic, semi-automatic attacks. Again, the scope of this technique is evaluated for traditional networks with no evidence for SDN networks.
- 3) *Application of CVSS for SG threat assessment:* CVSS is an efficient assessment method to quantify vulnerabilities and the same work has been performed in the article [160] to establish a risk assessment model to score the vulnerabilities as per their critically level. The proposed method is implemented for the risk assessment of AMI domain of SG. three evaluation criterion are considered; 1) Base group – access control and CIA 2) Temporal group – report confidence, exploitability, and remediation level, and 3) Environmental group – potential damage. As CVSS is a generalised assessment method and proposed method is a very detailed scoring system much related to SDN-SG; potential scope for SDN-SG. However, CVSS cannot quantify the threats during the course of time when connections are established between devices

inside the system [161] – requires another technique to supplement this deficiency for SDN-SG application.

- 4) *Application of OWASP for SG threat assessment:* Confidentiality and integrity of electric meter data, authentication and configuration related vulnerabilities are considered in the article [162] to highlight the significance of electric meters security. A very detailed analysis of SG security and threat assessment is provided in the article with much focus on OWASP vulnerabilities list and vulnerabilities pathways [163]. Information security of SG is discussed in article [164] with much focus on the CIA of the communication infrastructure. In all of these articles, the role of OWASP is limited to provide just the vulnerabilities list and their pathways that are then tested for various sections of SG – the vulnerabilities of traditional networks; what about SDN networks? It needs to be tested whether OWASP can also assess the information breaches in SDN-SG or not. All these vulnerabilities are for distributed networks, however, SDN-SG is a centralised network.
- 5) *Application of Attack Trees for SG threat assessment:* Authors in articles [158] have performed the vulnerability analysis of SCADA system of SG using Attack Tree assessment method. In SCADA system, multiple geographical dispersed SG substations are connected through an intranet, a dial-up network, wireless networks, or Virtual private network (VPN) and usually, these access points are protected using some passwords. The first step to launch an attack on SCADA system is to access the system by breaching the password. In these articles, authors have quantified the vulnerability assessment with loss of electric load in the power system - attack intrudes the system and comprises the electrical assets to affect the load profile. The work is much focused on password breaches and has also envisioned to extend these studies to determine the bottleneck of SG communication system [165].

In these papers, assessment is more related to protecting the access to the SCADA system, that can also be applied for SDN-SG for eliminating the password breaches of SCADA system - but still subject to availability of practical evidence.

- 6) *Application of LINDDUN for SG threat assessment:* SG is a consumer utility that also

gathers the data about the consumer usage pattern that ignites privacy issues and as part of the research study in the article [166], authors tried to assess the privacy requirements using LINDDUN assessment model. Firstly, threat tree analysis is carried out to identify the privacy-related vulnerabilities followed by the LINDDUN implementation for ensuring the privacy of personal information of the consumer. LINDDUN analysis the use cases in which standard guidelines of privacy are violated – ensuring the Privacy by design, privacy in the context of system engineering, privacy dependability. This approach is more focused on consumer behaviours and data, a generalised assessment method that can claim fair scope for SDN-SG for evaluating privacy threats.

- 7) *Application of OCTAVE for SG threat assessment:* SG is a consumer-based utility with space for the inclusion of new services at every time. These services require a rigorous assessment before their incorporation in the SG. The authors of article [167] are also implementing OCTAVE for cost-benefit analysis of ICT based new services. Both the technical as well as business perspectives are considered in the assessment method. This could be a productive assessment technique for business point of view, but it lacks sufficient technical details. When implemented for SDN-SG case, this technique could be part of the threat assessment method to evaluate new services of SDN-SG but lacks the completeness to be served solely as a whole technique.
- 8) *Application of customised models for SG threat assessment:* A cost-benefit analysis based risk assessment of SG communication network has been performed using a customised model with much focus on the economic impacts of cyberattacks related to DoS attack, malware/worms, intrusion, protocol attacks and routing attacks [168]. Deterioration of SG assets such as loss of equipment, services, confidential information, time, or records caused by the cyberattacks is evaluated in the proposed threat assessment method. The main objective of this study is to further supplement the confidentiality, integrity, and availability (CIA) of SG communication network. Still, all the assessment

is related to traditional communication networks with no evaluation of SDN related equipment.

- 9) INSpIRA, security tool-chain, was proposed with an effort to integrate security within the risk assessment mechanism. The engineering chain of this security tool convulses the best features of multiple threat assessment methods like STRIDE and DREAD. Firstly, the vulnerabilities, their causes and failures occur are evaluated and are categorised in the form of the structure tree. For each branch of structure tree, there is an associated function with related failure path and also specified mitigation and recovery strategy. This vulnerability-cause and recovery-based strategy could find a great scope for SDN-SG in which various domains of SDN-SG and associated vulnerabilities could be categorised into structure trees for better and efficient threat assessment.

A vulnerability known as Aurora Attack is identified in the article [169] in which attacker penetrates to the communication network of the SG control centre and inject false data to trip relays of transmission and generation equipment of SG. Here, quantification of this attack is performed by setting risk scores regarding discovery, finger printing, access, threat detection, connection speed and also the type of network like Ethernet network, dialup connections, wired, or wireless. These scores are then utilised to rank the SG relays according to their criticality level. This assessment method is considering a single vulnerability that is discussed in very detail; but not other vulnerabilities. For the case of SDN-SG, relays are the important elements of the protective system of SG. Here this assessment can be applied for assessing Aurora vulnerability of relays, however, in SDN-SG there could be more pathways for reaching out relays and launch Aurora attack. Whether this technique can also quantify the aurora vulnerability of SDN-SG, this needs to be investigated.

In the article [170], accurate behaviour rules of power flows are defined and further used to identify possible threats. It is clear that any attack on the communication system of SG will have a corresponding effect on the power flow. Power phasor angle is measured at each node such that phasor difference between neighbouring nodes depicts the

deviation from intended values – inconsistency in the system. Here, the indirect approach for vulnerabilities assessment of SG is performed that is also applicable for SDN-SG, but relying solely on the indirect approach is not reliable. Like it can be used to verify the results of primary direct assessment technique.

A detailed model for information security of SG is presented in the article [171] in which the SG system decomposed into blocks with respect to their functionality like generation, transmission, distribution, and utilisation to define the product flow diagram (PFD) describing the relative position of SG components. Then for each block, assessment is performed for each component of the block as use case diagram (UCD). Then inter-block and intrablock flow of data is analysed to formulate data flow diagram (DFD). Using DFD, threats related to each component of the block are defined. Now a threat model is defined as any violation of DFD from the normal flow will indicate the threat. This strategy of systematically decomposing the system for better and efficient threat assessment have grater possibility to produce effective results also find a fair scope for information security of SDN-SG – as this strategy is independent of the type of networks.

B. Summary and Insights

In this subsection, threat assessment techniques implemented for evaluating the SG are reviewed and their summary is tabulated in Table. VII. We have observed that some are generalised techniques that are already also applied for SDN, however, some are SG specified assessment models. Moreover, all these techniques lack either attack categorisation, risk-based approaches, risk quantification, comprehensiveness or best practices. Nonetheless, the operation of SG in on traditional non-SDN networks with no SDN components such as SDN controller, SDN switches, SBI, NBI, EBI/WBI inter-faces, or data-control link. So these threat assessment models deployed for SG with traditional networks lacks the feasibility for the required vulnerabilities analysis of SDN components as desired in SDN-SG. Moreover, these threat assessment models are more prone towards the electrical domain threats of SG rather than the communication system threats. One more factor that is missing in SG related threat assessment methods is

that the vulnerabilities related to packets are considered, while in SDN, there are flows. All these circumstances highlight the need for SDN-SG specified comprehensive threat assessment model that categorised all SDN-SG related vulnerabilities and also provide a comprehensive risk assessment and quantification.

V. THREAT ASSESSMENT AND MODELLING OF SDN-SG

Security of SDN-SG relative to traditional networks-based SG has to observe a unique environment – vulnerabilities of both SDN and SG and combined SDN-SG infrastructure required to be addressed in threat assessment models. The above-mentioned threat assessment tools are useful for non-SDN based SG but not for SDN-SG – an open research field demanding the efforts of the research community to secure SDN-SG by developing threat assessment models that can identify the possible threats of SDN-SG. The only work found in the literature is the security risk assessment of SDN-SG [61], in which authors have proposed risk assessment model and also evaluate its effectiveness for windmill collector substation. The work focused on the security of Intelligent Electronic Devices (IEDs) - microprocessor-based power system equipment having the ability to take actions as required without any prior directions from the main control centre, and IEC 61850 protocol – SDN based substation communication network. Quantification of security risks in IEC 61850 and IEDs is performed considering the criticality of each IEDs in the SG. This paper successfully presented a security score

model that only address link flooding-based DoS attacks in which the attacker flood any particular link. Moreover, although its an SDN-SG infrastructure but SDN specified vulnerabilities are not discussed in this paper. This work does not fulfil the demand for a complete well-defined risk assessment tool for SDN-SG that has the ability to incorporate all possible known attacks and also unknown exploitable risks to SDN-SG.

A. Unique Requirements of SDN-SG for Threat Assessment

It has been concluded from the above sections that SDN-SG is unique relative to other SDN applications in terms of data plane – in which security of switches has the paramount significance because of underlying power system equipment. Currently, the literature lacks the thorough threat assessment studies of SDN-SG, so it is difficult to say whether existing threat assessment techniques are feasible for SDN-SG or not? But, a key point that needs to be considered in the threat assessment of SDN-SG is that it is the convolution of the power system and SDN paradigm — a suitable threat assessment technique or merging multiple techniques is deemed here for the comprehensive risks assessments of SDN-SG. A technique that has the ability to identify domain specified threats of SG, SDN and can also assess the vulnerabilities that will provoke as a result of their combination. For example, it might be possible that underneath power system equipment might risk the stability of SDN switches so the desired threat assessment technique also requires to indicate external as well as internal threats.

TABLE VII: Evaluation metrics for evaluating the performance of SG security.

Assessment Model	Evaluation Metrics	Features Considered	Ref
Attack Trees	Password breaches	Loss of load in power system	[158]
	Password breaches	Loss of load in power system	[165]
STRIDE	Security breaches	Access control, data integrity, repudiation, confidentiality	[157]
OWASP	Data breaches	CIA of Electric meter data	[162]
	Information security	Impacts on CIA of SG	[164]
DREAD	Network Access	Damage potential, reproducibility, means to exploit threat	[159]
CVSS	Base group,	CIA, remediation level, report confidence, damage potential,	[160],
	Environmental	exploitability,	[161]

	group, Temporal group	authentication	
OCTAVE	Economic feasibility	Business and technical sustainability	[167]
LINDDUN	Privacy	Criminal Intention, data abuse, unintended data aggregation, unclarity	[166]
Customised Models not utilising any defined assessment technique			
ISERM	Information security	Violaion from standard operation	[171]
BLITHE	Power flow, Inconsistency	Phasor angle of power flow	[170]
CPVSG	Access control, false data injection	Relays trip	[169]
INSpIRA	Threat-Cause-Effect analysis	Failure modes	[172]
EISG	Cost-benefit analysis	Economic loss caused by cyberattack	[168]
PASMT	Network Traffic	Average uplink throughput, Packet loss ratio, Delay	[173]
CEDoS	Entropy	Measuring the randomness of source traffic	[174]
SGNDB	Network Performance	Network (Availability, Integrity, Confidentiality), Attack Scope (Stealthy, Strong), Attack Target (End user, System operations, Communication network)	[175]

The unique data plane of SDN-SG also demands a unique SBI. The novel SBI designed for SDN-SG is in its infancy and yet requires a very rigorous evaluation for possible risks. Design of evaluation metrics and desired threat assessment model to evaluate the new SBI is required to assess the vulnerabilities that might lead towards outages in SG. We have also figure out the cascading failures in SDN-SG because of its interlinked design — a very crucial and emergent state for SG stability. The proposed threat assessment model needs to address threats whose influence can also propagate and influence other resources, in addition to victim resources. An efficient cyber threat model is desired here with relevant and effective metrics that can indicate such unwanted and sudden circumstances. Furthermore, SDN-SG is a time-critical infrastructure demanding strict QoS. Here again, suitable metrics need to be designed that can keep a check on the desired QoS as SG, a super CI, has a very narrow tolerance for any mal-operations. Moreover, equipment in SG undergoes a diversified range of criticality. Some are more fault-tolerant while others have a narrow margin for mal-functioning. A security score model that evaluates the criticality of each element of SDN-SG is also desired.

B. Evaluation Metrics of SDN-SG

Implementation of SDN for SG also demand such rigorous evaluation studies before its deployment for a real-world scenario. SDN-SG is the convolution of both the SG and SDN, so here a threat assessment model utilising the most suitable evaluation metrics out of these two could be a plausible solution. Articles tabulated in Table VII and Table V are reviewing various evaluating metrics utilised for the threat assessment of SG and SDN respectively. For instance, availability of the SDN controller is most crucial for normal operation of SDN-SG. It can be assessed using the evaluation criterion (bandwidth available relative to attack rate) as used in the article [142] related to SDN threat assessment in Table

V. Whereas, in article [179] of Table VII, QoS is used as an assessment criterion to ensure SG applications are meeting their specified minimum threshold of data rate and latency. These are the potential evaluation metrics utilised for the threat assessment of SG and SDN and have a fair scope for threat assessment of SDN-SG.

Moreover, certain studies have also considered the security of SDN-SG by simulating certain scenarios as shown in Table VIII. The parameters utilised in these studies can be used as the evaluation metrics for threat assessment of SDN-SG. Such as vulnerabilities related to link failures can be studied using link failure rates [176], network performance can be critiqued by switch load capacity [177], communication resources can be assessed by SDN controller utilisation, and network susceptance to attacks can be evaluated by trust, confidentiality, authentication, authorisation, availability, and integrity [185]. As these studies are employed for SDN-SG, so they have a greater probability of success.

C. Threat Assessment Model for SDN-SG

There are multiple techniques in the literature for the threat assessment of SDN and SG solely, but not for SDN-SG. In enterprise SDN architectures, when

threat assessment was performed, the switches have no underlying equipment as we have in SDN-SG; no chances of any threat from underlying the switch in enterprise SDN. The factor of interconnected components as found in SDN-SG in which attack on one component might travel to other components, is also not present in enterprise SDN. These factors limit the applicability of SDN threat assessment models for SDN-SG. Considering the SG threat assessment models, operation of SG is on traditional networks – no vulnerability assessment of SBI, NBI, EBI/WBI interfaces and SDN stitches as desired in SDN-SG. These circumstances confine the implementation of SDN and SG related threat assessment models for SDN-SG – unless these are tested and there is experimental evidence for their suitability.

TABLE VIII: Prospective evaluation metrics for evaluating the performance of SDN-SG security.

Article	Evaluation Metrics	Features Considered	Ref
RSDN-RG	Link failure rate	Ability to predict the possibility of link failure	[176]
SSDS	Network Performance	Throughput, Switch load capacity	[177]
SSDNSG	Network Traffic	Average delay in traffic during attack	[178]
SDSGA	QoS	Meeting the SG application specified minimum threshold of data rate and latency	[179]
SGCSDN	Anomaly detection	Time to detect, Resources utilisation, Accuracy (attack detection)	[98]
FFSDNSG	Fail-over	Available data rate relative to fail-over recovery rate	[97]
SMFSDSG	Network traffic	Evaluating delay of traffic at switch and controller, Recovery time	[180]
PFSNDNC	Traffic prioritisation	Available data rate and transmission delays for top priority and low priority traffic	[108]
RASDNSG	Network Traffic	Evaluation of received packets relative to sent packets to diagnose link flood attack (Packets dropped, Rate of drop)	[61]
IPSGSDN	Packet Size	Evaluation of packet size relative system efficiency, throughput, latency, and round trip time (RTT)	[181]
SDNVG	Network Resources	End-to-end delay, Network load capacity	[182]
SDRSG	Network Traffic	Packets transmission average delay, Total packet lost	[183]
ISDNMASG	Network Traffic	Data rate, Transmission delay, Round trip time (RTT)	[184]
SDSGS	QoS, Network Security	QoS (Bandwidth, Delay, Latency), Network Security (Trust, Confidentiality, Authentication, Authorisation, Availability, Integrity)	[185]
QoSSDSG	Network Resources	Utilisation of links, Throughput	[186]
SDSGIIoT	Network Traffic	Load, Throughput	[187]

SFSDSG	QoS Threshold	Throughput	[188]
SFVSDSG	Network Resources	Capacity, Bandwidth, Allocated resources, Resources occupancy rate	[189]
BGGSDSG	Security	Monitoring cost, Detection rate	[105]
SDIECDM	Network Traffic	Average packet delay	[190]
SDNRSG	Network Resources	CPU utilisation of SDN controller, End-to-end delay	[191]

Various threat assessment models target different cyber domains like STRIDE focus on spoofing, DoS, data tampering based attacks while LINDDUN targets the privacy assessment. Standalone threat assessment models or hybrid versions can be evaluated to check their feasibility for the threat assessment for SDN-SG. Whether it's any individual technique or a hybrid model like hTMM or qTMM, the main requirement is the overall security evaluation of SDN-SG covering all of its domains as specified above. To address these requirements, a very compact and comprehensive threat assessment model with the following features is desired for security evaluation of SDN-SG:

- Design of suitable evaluation metrics for the vulnerability analysis of SBI of SDN-SG.
- Assessment of internal threats that might arise from underneath power system equipment.
- Assessment of external risks that can be triggered by an attacker.
- Composition of evaluation metrics that can study the interconnected design of SDN-SG and thus can identify threats may lead to cascading failures.
- Evaluation of stability and resilience of SDN-SG under cascading failures.
- Feasibility study of exiting threats and their impact on SDN-SG
- Identification of potential and novel unknown threats to SDN-SG that can be exploited to launch a cyber attack.
- Design of risk assessment models to identify the criticality of each element of SDN-SG.

It is envisioned from the above unique threat assessment requirements of SDN-SG that a hybrid threat assessment technique convolving the required features of standalone models is desired. For instance, a threat model employing Attack Tree for attacks modelling, STRIDE for attacks categorisation, and CVSS for attack quantification. Other models can also be shaped using PnG and Security Cards for threat modelling, LINDDUN and PASTA for attack categorisation, and Trike and DREAD for attack

quantification. These are two of the possible combinations that can be checked for SDN-SG; there might be many more. Moreover, parameters utilised in the efforts to secure SDN-SG as tabulated in Table can also be carved for the threat assessment of SDN-SG – the most relatable and closely linked parameters out of given options, as they follow the same architecture of SDN-SG. This is a potential research area that needs to be investigated for the effective and reliable threat assessment of SDN-SG.

D. Summary and Insights

In this section, we have observed that the threat assessment of SDN-SG is still in its infancy state and is a prospective research venue. A comprehensive threat assessment model of SDN-SG that can address a wide spectrum of cyber attacks in SDN-SG is the dire requirement for the cyber-security of SDN-SG. This will enable the network administrators to carry out security analysis of SDN-SG elements like generating stations, transmission networks, distribution substations, utilisation network, and control centre. Furthermore, We have provided the unique requirements of SDN-SG that need to be considered in modelling the threat assessment model of SDN-SG. The vulnerabilities of SDN-SG required to be evaluated – a compact and complete package for threat assessment of SDN-SG. As SDN-SG is a consumer-based utility that undergoes great variations. The devised threat assessment model needs to distinguish between abnormal conditions and faulty conditions. Moreover, quantification of threats, in addition to their identification, is also desired in SDN i.e. a security score model that can also quantify the criticality of various SG equipment. This would highlight the elements of SDN-SG that are critical for the operations of the system so that multiple levels of security can be provided to such elements.

VI. DENIAL OF SERVICE (DOS) ATTACKS IN SDN

In this section, we will review different types of DoS attacks that can be launched in SDN and attack mitigation techniques employed to detect and mitigate these attacks. Moreover, attack vectors of SDN are also studied in reference to SDN application to SG. In the end, attack detection and mitigation techniques deployed to secure SDN are surveyed in detail. Details of these DoS attacks is elaborated in Fig. 7.

A. Flooding attacks

It is the type of cyber-attack in which the intruder flood the victim with the bulk of malware traffic, that is greater than the standard operational capacity of the switch, with an effort to overwhelm its resources. Occupancy of resources by fraudulent actors restrict the legitimate users from accessing the system resources thus resulting in a denial of service.

- (i) Event flooding attack (EFA): To enhance the reliability of the SDN architecture, distributed design with multiple SDN controllers is deployed to inject redundancy in the system [194]. These physically distributed and logically centralise SDN controllers are linked to each other under strong or eventual consistency models. An event flooding attack is a scenario in which a strong consistency model is utilised. A strong consistency model responds to any change in network state (topology, links, or hosts) of each SDN controller and synchronise the change to all other SDN controllers. During the time of synchronisation, the read / write actions remain temporarily unavailable, known as blocking time. This will also elongate the time required to read new information, known as the read time. There are also eventual consistency models which have less blocking time and read time, but all distributed SDN controllers might be not on the same status for the given time – data conflicts might arise. In EFA, an attacker just attacks premises of a single controller, but a strong consistency feature distributes it throughout the network- a distributed DoS attack.
- (ii) UDP flood attack [199]: UDP is a connection-less protocol that does not require to initiate a three-way handshake as in TCP. An attacker sends a

large number of forged UDP requests to the victim switch. System search for applications related to datagrams of UDP requests and upon not finding any application, reply with “destination unreachable”. Continuous receiving of UDP messages and corresponding replies saturates system resources.

- (iii) Internet control message protocol (ICMP) flood attack [200]: This attack overwhelms the resources of the host by flooding the bulk of echo requests.
- (iv) Link flood attack [196]: This attack aims to disrupt the services of a specified link only rather than attacking the whole network. This attack disrupts all the services associated with victim link. This type of attack usually initiated to target any crucial link that is handling control and critical information.
- (v) TCP flood attacks
 - a) SYN / ACK Flood attack [199]: TCP protocol develops a connection with the destination host/server using a three-way handshake before initiating communication. It first sends an SYN message and upon receiving the message by the intended system, the SYN/ACK message is returned. In response, ACK reply is transmitted and the connection is established. In SYN / ACK flood attack, attackers keep flooding SYN messages to the switches, for which switch replies with SYN/ACK and waits for ACK reply as shown in Fig. 8. As far as the switch receives ACK reply, the connection remains open waiting for the reply. Attack machines do not reply for SYN/ACK messages and keep sending more SYN messages, thus keeping the connections half-open - utilising the resources of the network. Exhaustion of SDN resources by the attack will limit the access for legitimate users - DoS case.
 - b) RST / FIN flood attack [17]: To terminate a TCP connection, FIN/ACK messages are exchanged between the hosts. In the said attack, bulk of FIN messages although there is no connection existing there. The attacker keeps sending FIN messages. System resources will be wasted searching for the connection. Same-like RST message is shared in response to SYN message when the host does not want to make a connection. When attacker bulk of RST messages, system resources are wasted to search for the SYN requests for which RST

requests are received. Such circumstances over-utilise system resources thus restricting the valid users

- a DoS case.
- 1) *Impacts of flooding attacks:* These are direct attacks on the switch in the SDN environment that halt the resources (memory, processing power, installation of flow rules) of the victim switches. SDN controller will neither be able to install new flow rules to route new traffic requests in the compromised switch nor it will be able to deal with the existing installed flow rules as all the resources are pre-utilised in processing the fraudulent traffic. This results in the reduced capacity of SDN architecture as victimised switches are in halt state and also the denial to the legitimate traffic.
- 2) *Solutions for flooding attacks:* Floodguard [67] detects UDP flooding, ICMP flooding, TCP flooding by installation of proactive flow rule to tackle attacks. But to install all flows that could be possible is not practical and it cannot tackle emerging attacks. Moving Target Defence (MTD) [201] detects ICMP flooding, link flood attack by

checking each link individually that might elevate the time of processing. SDNScore [202] detect UDP flooding, ICMP flooding, and TCP flooding attacks by injecting intelligence into the switches using statistical analysis of traffic so that malicious flooded traffic can be identified at the switch level. Cyberpulse [203] detects link flood attacks by classifying network traffic using deep learning techniques. Regarding TCP flooding, various techniques are discussed in the literature like SYNC Guard [204] that identifies the MAC addresses with pending syn/ack requests and block it requests cross a certain threshold while SLICOTS [205] introduces a pending list in which all syn re-quests are moved towards it rather than keeping the connection in half-open mode. OPERETTA [206] avoid TCP flooding by rejecting fake connection requests while Cusum Entropy [174], SAFETY [207], and SA-Detector [198] utilises entropy of the traffic to detect TCP flooding.

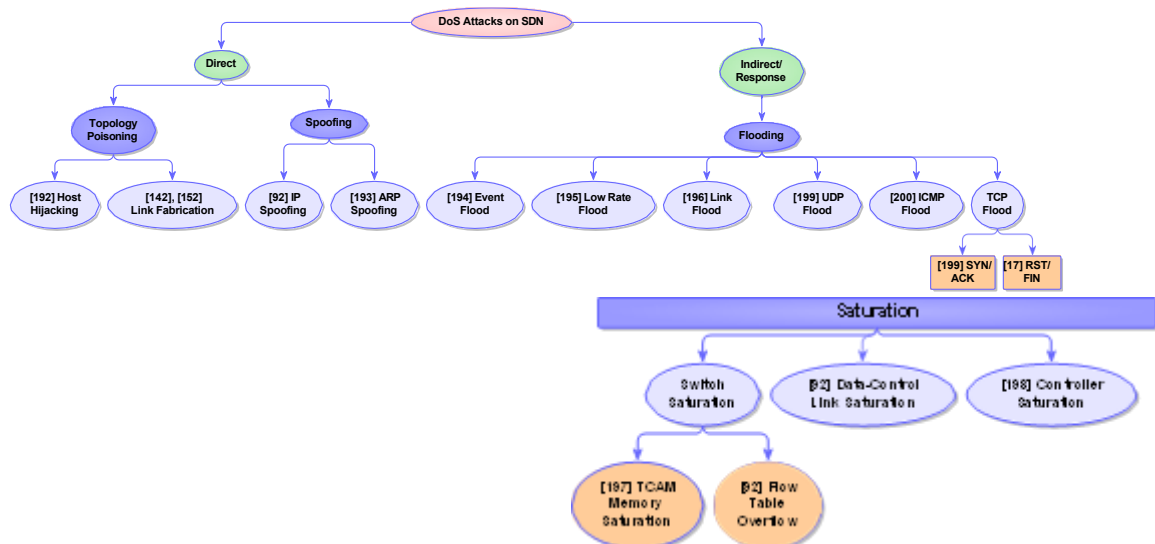


Fig. 7: DoS Attacks on SDN.

B. Topology poisoning attack

In this attack, intruder poisons the network topology by either injecting fake links in the network topology or impersonates to be the victim switch. Traffic traversing via these fake links and compromised switches will lead towards huge packet loss. Further categorisation of these attacks is as follow:

- (i) Host hijacking attack [192]: The purpose of this attack is to initiate DoS by saturating the data-control link. In SDN, the location of hosts is tracked with host tracking service (HTS), whenever a host is migrated to a different position. Upon receiving the packet_in message from the migrated host, HTS recognises the host and

updates the associate flow tables, but HTS is not able to authenticate hosts. In host hijacking attack, the attacker impersonates to be a large number of valid users that already exists in the network. This will make HTS to miss-recognise the location of valid users. SDN controller will reconfigure the flow tables of the whole network that are linked to impersonated host switches. This will greatly consume the data-control link bandwidth and may also saturate it, thus halting the whole SDN network.

- (ii) Link fabrication attacks [142], [152]: In SDN architecture, the topology of the network is determined automatically by utilising the link layer discovery protocol (LLDP) [208]. SDN controller enforces all the switches to generate LLDP packets. When these packets are received by the immediate neighbouring switches, these are directed towards the SDN controller as packet_in messages. In this way, the controller learns about the topology of the network. But, LLDP does not ensure the integrity/origin of the LLDP packets and propagation path of LLDP packets [152]. Exploiting these vulnerabilities, attackers can inject new links in the topology or can also fabricate links in-between existing switches. In this way, the legal traffic can be diverted towards forged paths - DoS case. Spanning tree protocol (STP) is used in the SDN topology mechanism to kill loops in network shortest path routing by blocking redundant ports. By leveraging this feature of STP, attacker blocks the valid ports of the networks - DoS case for that port.

- a) *Impacts of the Topology poisoning attack:* Its a direct attack in which a fabricated link is inserted in the SDN environment or a particular switch is hijacked. SDN controller assumes those fraudulent links and switches to be legal and will process traffic via them. All the routed traffic will either dropped, trapped or forged. This will greatly influence the credibility and reliability of traffic routed in the SDN architecture.

Solutions for Topology poisoning attack: Host hijacking attacks are detected by employing AuthFlow [209] that checks the authenticity of the switches and SLAMHHA [210] by verifying the legitimacy of a host using supervised machine learning. Link fabrication attacks are mitigated using Flowkeeper [142] by packet filtering and TopoGuard [152]

utilising topology update legitimacy checker mechanism.

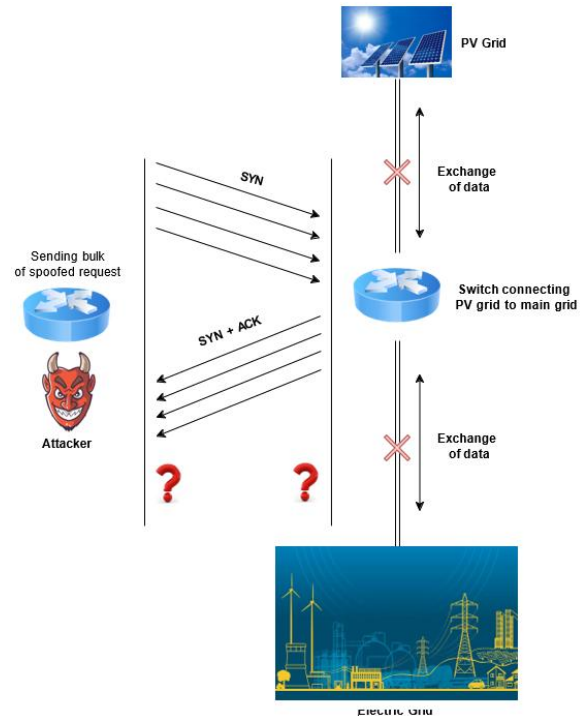


Fig. 8: Flooding Attack: Attacker enforces the switch to remain in half-open state by continuously flooding SYN request with-out replying to switch resulting in disconnecting the associated PV plant from the main grid in SDN-SG.

C. Spoofing attacks

Spoofing is the attack in which attacker impersonates to be a legal user and then access SDN architecture as shown in Fig. 9. As the attacker is impersonating a legal user, so that particular user will not be able to access the system - DoS case.

- (i) IP spoofing [92]: It is the creation of a false IP address with an intention to impersonate a targeted source to initiate DoS for that specified source.

ARP spoofing [193]: ARP protocol is defined in RFC 826 [211]. ARP protocol is used for performing communication in computer networks. ARP protocol performs IP to MAC mapping so that messages can reach from sources to destinations. ARP is a protocol used by hosts to know the MAC address of the next hop in the path to the destination. Every host also maintains an ARP cache. If host_X wants to communicate with host_Y, it will first search its ARP cache for the next-hop MAC address. If the MAC

address is found there, then it will proceed with the packets, and if a search is not successful then the ARP protocol will broadcast the ARP request to the network. Host_Y replies with an ARP reply message. Host_X then updates its ARP cache with the IP-MAC pair for future communication to host_Y.

ARP spoofing also known as ARP cache poisoning is a technique to insert forged IP-MAC mapping the victims ARP cache. ARP spoofing can either be a request or response attack. In a request attack, attacker broadcast forged IP-MAC pair request. When a victim receives this spoofed request, it will respond with ARP reply and updates its ARP cache with new IP-MAC entry. Now all the traffic sent by the victim to the forged IP address will be received by the corresponding MAC address specified by the attacker, thus intercepting the traffic of the network. In a response attack, attacker either response with spoofed ARP replies for legal ARP requests or sends ARP replies with any received ARP request.

1) *Impacts of the Spoofing attacks:* These are direct attacks in which attacker impersonates to be a legal switch in the SDN environment thus initiating DoS to the victim switch to which it is impersonating. All the legal traffic of the victim switch will now encounter DoS. Furthermore, an attacker can also insert fraudulent traffic in the SDN environment to initiate other attacks like this attack method can be implemented to perform the following attacks:

- (i) Flooding attacks: Terminating the connection between two hosts.
- (ii) Host impersonating attack: Attacker pretends to be an existing legal host and intercept the intending traffic.
- (iii) Man in the middle attack: There are multiple hops in the path to the destination. An attacker can impersonate to be a hop in between the intended host and can listen to all the communication.

2) *Solutions for Spoofing attacks:* For the security of gen-eral SDN systems, VAVE [212] detects an IP/ARP spoofing attacks by validating the source address of any request before processing it while Sgaurd [213] employ classification and authorisation of traffic flows to detect such attacks. Furthermore, BASE [214] performs cryptographic packet screening to detect IP spoofing.

D. The Low-rate DoS (LDoS) attack

These are direct attacks on the switches and links in the SDN environment that consumes a very tiny portion of to make it unnoticeable. That limited malicious traffic volume remains within the standard capacity of the SDN resources. The purpose of this attack is to shrink the throughput of the network and packet loss of a very minute extent to make it unnoticeable [195]. Attack rate (R) and attack period (T) are the parameters that define the LDoS attack. By adjusting these parameters, the attack traffic seems to be the legal traffic and is very tough to distinguish it. Such attacks initiate DoS to diminutive packets only.

Impacts of the LDoS attacks: LDoS is a direct attack on SDN architecture. In LDoS, unlike the flooding attacks in which there are bulk of malicious traffic, a limited range of fraudulent traffic is flooded in the SDN to offer DoS to a small scale. The severity of this attack is not much high, but it is difficult to detect due to lower rate of malware traffic.

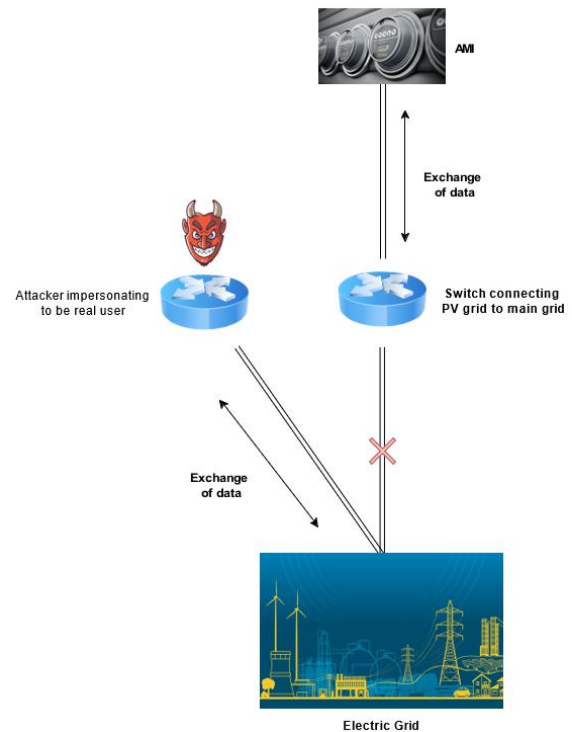


Fig. 9: Spoofing attack on SDN-SG in which a malicious switch is impersonating a switch connecting advance metering infrastructure (AMI) to main grid in SDN-SG.

2) *Solutions for LDoS attacks*: For general SDN systems, entropy of the traffic is evaluated using Generalised Entropy (GE) algorithm to check the randomness of the traffic in [215] to detect LDoS attacks.

E. Response Attacks

Impersonating to be the source address of the legal (victim) user, the attacker sends a larger number of requests and in response, the corresponding replies exhaust the victim's re-sources. These attacks can further escalate the forged response frequency by using amplification techniques.

- 1) Reflection attack [216] Exploiting the vulnerability of IP spoofing, the attacker pretends to be the source (victim). Attackers send forged requests to the servers which in return direct their massive responses towards the victim host. These bulk replies overwhelm the source resources, thus preventing access to legitimate users (DoS case). As servers are just acting as a reflector that is returning responses for forged requests, that's why such attacks are termed as reflection attacks.
- 2) Amplification attack [150] The ratio of produced re-sponses to the initiated requests are termed as amplification. The attacker tends to amplify the response factor

F. Saturation attacks

In SDN, switches are managed by the SDN controller. SDN controller install, modify, or deletes flows from switches. Whenever any packet arrives at the switch that does not match any existing flow, switch extract the packet header, encapsulate it in the packet_in message and sends it to the SDN controller. The message remains in the TCAM / buffer memory until the flow rule is assigned by the SDN controller. SDN controller processes the packet and sends a packet_out message that contains the information required to install the flow rules to the switch.

- (i) Switch Saturation: These types of attacks are also called as packet_in flooding as attacker send the bulk of fraudulent messages that are in the flow table of the switch, so switch send them to the SDN controller [92]. These malicious packets try to saturate the SDN resources.
- a) TCAM memory saturation: Under the normal operation, only the header of the packet was encapsulated in the packet_in message keeping the original packet in the TCAM memory. But,

when a large number of the malicious packets are sent by the attacker, it overflows the TCAM memory but no room for new messages even for legitimate ones. Now the whole packet is sent to the controller rather than just sending the header in the packet_in message.

- b) Flow table overflow: SDN controller upon receiving the packet_in messages, install corresponding flow rule in the flow table of the switch. Upon packet_in flooding, there are bulk of malicious messages and the SDN controller must install the flow rules for them respectively. This will exhaust the flow table of the switch thus restricting the SDN controller to further install new rules. During the course of this attack, there is a possibility that a request for flow rule installation might be from legitimate users. But, the SDN controller is now unable to install flow rules - DoS for the legitimate user.

Switch-controller channel congestion: When TCAM memory gets congested and overwhelmed, now whole packets are transferred to SDN controller [92]. This will utilise the bandwidth of data to the control channel. As the frequency of the malware message will increase, it will saturate the data-control channel resources accordingly. Under the attack, SDN will not be able to entertain the legal users as a channel is saturated and packets can no longer be transmitted to the SDN controller to be processed - a DoS attack.

- (ii) Controller saturation: SDN controller will receive a bulk quantity of attacker traffic to be processed under packet_in flooding attack [198]. This malicious traffic consumes controller processing capabilities causing wastage of energy and resources. If the frequency of the attacker traffic is to a greater extent than it can cause saturation of controller resources, then even legitimate traffic will not be processed by the controller - a DoS attack.

Conventional switches process the packets according to vendor installed switching and routing protocols like open shortest path first (OSPF) [217], Interior Gateway Routing Protocol (IGRP) [218], or Border Gateway Protocol (BGP) [219]. In case of updating any network policy, each switch has to be configured individually. Switches under conventional networks have both the data and control features. SDN

providing a logically centralised control has provided the opportunity to supervise all the switches under the single controller. SDN divides the operations into data and control devices. Data plane (switches) just relay the packets following the commands of the control plane (SDN controller).

This advancement has complemented the performance of the communication but has also highlighted some vulnerabilities of the data plane. Switches maintain rules for forwarding of packets also known as Flows in the forwarding tables stored on Ternary Content Addressable Memory (TCAM). Whenever any packet arrives, a lookup is performed at TCAM. If the flow is there, the packet proceeds accordingly. If the packet is a new entry, then it will be kept in the TCAM memory until the controller decides about its flow and install the flow in the forwarding tables. If the table is fully occupied, switch deletes old entries to enter the new flows.

Thus, saturation attacks are capable to compromise the victim's resources and suspend target and available services. In the above discussion, we have discussed several types of DoS attacks that can damage SDN. SDN paradigm promises to complement the performance of the communication system for legit users of the system. There are switches, SDN controllers, and the channels connecting the SDN premises. When any of the DoS attacks occurs, it either saturate the resources with fake traffic and making it unavailable for the legit users or impersonate to be the legit users. Under all such circumstances, valid users are compromised and face DoS.

1) *Impacts of the saturation attacks:* These are indirect attacks that occur as a result of flooding attacks in the SDN environment. Flooding attacks exhaust victim switch resources, which in return engages data-control link and overwhelming SDN controller operation capabilities like identifying new routing requests and installing specified flow rules. Saturation of the SDN controller caused by a single switch will engage SDN controller resources that cease its capability to even process the benign switches. Thus the scope of these attacks is not limited to the victimised switch only but also compromises the overall efficiency of

SDN architecture.

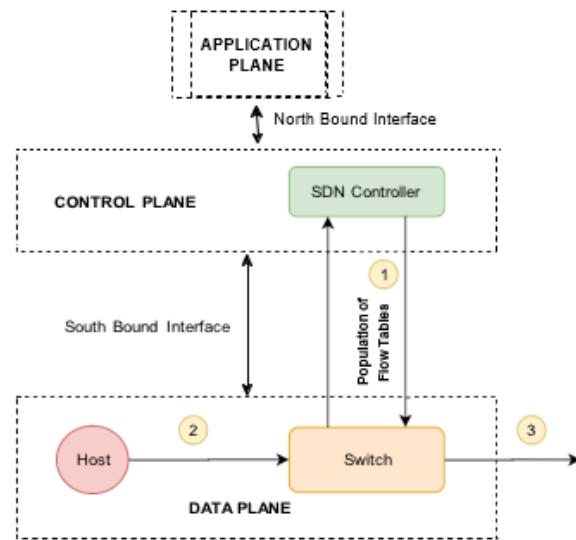


Fig. 10: Reactive defence strategy of SDN architecture.

2) *Solutions for saturation attacks:* In the SPHINX [141], controller application examines the incoming requests for each host and raises alarm if certain host exceeds defined thresholds to detect all sort of saturation attacks while Flowkeeper [142] do the same job by packet filtering. FAST [220] pre-installs flow rules and then process packets by matching them against the applied flow rules to prevent saturation attacks. Floodguard [67] detects controller saturation by the installation of a proactive flow rule to tackle attacks. WEDGETAIL [221] systematically and autonomously prioritise network policies and performs real-time updating of attacks definition to safeguard data plane against saturation attacks. Flood Shield [222] mitigate saturation attacks by filtering forged traffic using a source validation mechanism. In SDN Guard [223], SDN application identifies and prevent malicious traffic by rerouting potential malware traffic, adjusting flow timeouts and aggregating flow rules.

We have studied the detailed overview of DoS attacks. Fig. 7 is classifying these DoS attacks in terms of sub-classes. We have evaluated that DoS attacks have quite similar trends with very marginal differences. Comparative analysis has been performed in Table IX to define the unique attributes of DoS

attacks in terms of scope of the attack, specified area of influence, and nature of the attack (direct/indirect). SDN field is quite matured now and certain attack mitigation techniques have been well developed to catch various types of DoS attacks. In SDN, two types of defence mechanism are employed: Proactive and Reactive defence as shown in Fig. 11

and Fig. 10 respectively. In proactive, defence measures are pre-defined before the packet arrives, while in reactive defence SDN controller decides the security measures to be deployed for incoming packets. Existing defence mechanisms to mitigate DoS attacks on SDN are summarised in the Table X.

TABLE IX: Comparative analysis of DoS Attacks.

Feature	Flooding	Saturation	Spoofing	Topology poisoning	LDoS	Response
Scope of attack	Bulk of malicious traffic	Overwhelming of resources	Impersonating a host	fabricated links or host hijacking	Unwanted and un-noticed utilisation of resources	Sending amplified responses of attack traffic rather than direct attack
Area of influence	Switch	Switch, Controller, Data-Control path	Switch	Switch, links between switches	Switch	Switch, Controller, Data-Control path
Direct / Indirect attack	Direct	Indirect as response of flooding attack	Direct	Direct	Direct	Indirect as Botnets generated legit response to attack traffic
Impact on SG	SG equipment not connected to flooded switch will face DoS	Saturated switch will not be able to process traffic underneath SG infrastructure	SG facilities for which attacker is impersonating will face DoS and can also inject false data	When traffic is relayed to fabricated links that does not exist in reality, SG traffic will face DoS	some percentage of SG traffic not all will face DoS	Victim switch / controller will be jammed to offer services to SG

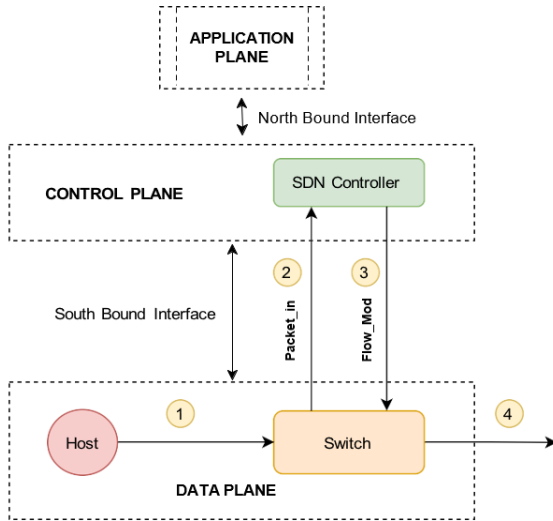


Fig. 11: Proactive defence strategy of SDN architecture.

Various attack vectors, defined as means by which attackers can gain unauthorised access to the network to exploit the vulnerabilities, are considered in this survey article for launching DoS attacks on SDN. There are multiple attack mitigation techniques available that have effectively handled these DoS attacks in SDN environments [141], [142], [174], [197], [198], [201]– [207], [209], [210], [212]– [215], [220]– [233]. Feasibility of these techniques is also further evaluated for SDN-SG in Section VII.

G. Machine Learning for DoS Attacks in SDN

ML has gained great attention in the research community across various fields. Communication networks also applied these advancements and enhancement brought in by ML. Specifically, SDN architecture with the programmable controller finds the ML very suitable candidate in refining the control plane operations related to network management or security. There is a diverse range of advantages that ML has brought to SDNs. Researches have implemented ML for traffic classification [234],

ensuring QoS [235] and QoE [236], routing optimisation [237], and resources management [238] in SDN architecture. These are various cyberattacks that might compromise the victim resources, but DoS attacks block access to the network for all legit users and subscribers. Considering the severity of these attacks, Table XI elaborates the application of ML techniques to detect and mitigate DoS attacks in the SDN environment. The ML features in an SDN architecture are listed as below:

- The data processing and learning abilities of ML enables the SDN controller to autonomously learn and adapt network dynamics.
- SDN controller is the main core of the architecture that operates and compute network services. ML applications will complement the computational capabilities of SDN making it more robust and efficient.
- Data-driven ML techniques require folds of data. Considering, an SDN controller has a global overview of the network and is enriched with granular details of data, making it a very suitable environment for ML applications.
- ML algorithms, by observing the historical and real-time network data, can learn and improve the SDN network and bring more intelligence and automation to the SDN controller.
- Programmability of the SDN controller enabled my ML will offer more optimal network services like configurations, resource allocation, and provision of network applications and services.
- ML-based SDN security enables learning capabilities, detect and mitigate known and unknown attacks. In DoS attacks, a major threat to network sustainability can be launched, using novel methods, that are previously unknown. ML with learning and evolving abilities can process and identify new attack vectors.

TABLE X: Attacks on SDN and Mitigation Techniques.

Attack	Mitigation Technique
Event flood attack	-
UDP Flood attack	Floodgaurd [67], SDNScore [202]
ICMP Flood attack	Moving Target Defence (MTD) [201], Floodgaurd [67],SDNScore [202]
TCP SYN Flood	SYNC Guard [204], SLICOTS [205], OPERETTA [206], Floodgaurd [67], Cusum Entropy [174],

	SDNScore [202], SAFETY [207]
RST/ FIN (TCP) flood	SA-Detector [198], SAFETY [207]
Link flood attack	Moving Target Defence (MTD) [201], Cyberpulse [203]
Amplification attack	-
IP Spoofing	Sgaurd [213], BASE [214], VAVE [212]
ARP Spoofing	Sgaurd [213], SPHINX [141], VAVE [212]
Switch saturation	DoS detection and mitigation [197], WEDGETAIL, SPHINX [141] [221], SDPA [227], Flood Shield [222], Flowkeeper [142], SDN Gaurd [223], FlowChecker [229], FlowVisor [231], FAST [220]
Controller saturation	SPHINX [141], Floodgaurd [67], Flood Shield [222], Flowkeeper [142], SDN Gaurd [223], VeriFlow [230], DISCO [232], VeriCon [233], FAST [220]
Data-control channel exhaustion	WEDGETAIL [221], FloodDefender [228], MultiCriteria SDN [226], Flood Shield [222], AvantGuard [225], Flowkeeper [142], SDN Gaurd [223], FlowFence [224], FAST [220]
Reflection based attack	-
Low-rate DoS	Generalized Entropy (GE) [215]
Host Hijacking	AuthFlow [209], SLAMHHA [210]
Link fabrication	Flowkeeper [142], TopoGuard [152]

H. Summary and Insights

Detailed literature related to DoS attacks in SDN is provided in this section. Various DoS attacks are studied. Attack trends of DoS attacks are analysed and then categorised according to their impact on the system. Dynamics of DoS attacks and their effect on data, control, and application layer of SDN are analysed in detail. We have analysed and discussed various SDN attacks having defined trends, i.e. spoofing attacks impersonate to be the legit user, topology poisoning attacks aim to forge the network topology while saturation and flooding attacks are launched to saturate network resources resulting in DoS to legit users. All these varying trends demand mitigation techniques that are suitable and adequate to identify the attacking trends. This is the reason all the attacks have their defined security mechanisms and the mitigation technique for one attack is not simply adaptable and viable for other attacks. Moreover, APIs used for NBI, SBI, and EBI/WBI are also vulnerable to DoS attacks. A comprehensive attack mitigation mechanism that can handle all sorts of DoS attacks in SDN is prospective research direction for securing SDN architecture. In addition, a complete defence platform could be a great contribution that can prevent cyberattacks before their occurrence, in addition to the detection/ mitigation of DoS attacks after they have

stroked the system.

VII. DENIAL OF SERVICE (DoS) ATTACKS IN SDN-SG

Cyber-attacks are the major threat for CIs as it halts the operations and also services provided to the public. There is a long history of cyber-attacks on CIs, thus demanding the concrete measures to ensure the security of CIs. In Table XII, we have accumulated various DoS attacks on CIs and discussed how these attacks affected the state machinery.

We have discussed the DoS attacks for SDN architecture in Section. VI in which we elaborated that SDN architecture infrastructure is enriched with the memory, processing capabilities, and energy resources according to the dynamics and requirements of the field of application. Here, we are employing SDN for SG systems. In SG, there are various generating stations, transmission and distribution substations, control centres, and utilisation sectors. Each of the entities is supervised by the switch that interconnects the underlying power system infrastructure with each other for better coordination and also to the grid. Some switches have to deal with less frequent data transmission requests while others could be heavily

crowded like relaying data related to real-time pricing or demand-response systems. These switches are then equipped with resources according to the requirement and also the associated SDN controllers and a channel connecting data and control planes are tuned accordingly. Under the saturation attack either on a switch, controller or data-control channel, attacker direct bulk of malicious traffic towards the SDN devices. Now, there will be dozens of extra traffic which SDN-SG have to deal with for which it is not designed for. This will saturate the available resources and SDN will not be able to entertain the SG traffic. The SG traffic that encounters such DoS might be of critical nature that can disturb the synchronisation of the power system, may damage equipment or waste energy.

It is possible that DoS compromise traffic related to protection devices that relaying tripping signals. Such circumstances can damage the SG components like transformers or generators and can cause blackouts on large. Hospitals, education institutes, industries, and state machinery will also be affected. This will cause social as well as economical loss for the state. Devising a defence framework to cater and mitigate

these attacks in SDN-SG has the paramount significance for the state. There are several related frameworks equipped with techniques already exist to address security concerns in the context of SDN, but the question arises whether these are applicable in SDN-SG? Table XIV and Table XIII are discussing various attack mitigation techniques for SDN and also highlights their potential scope for SDN-SG.

A. Flooding attacks

1) Impacts of flooding attacks: When the SDN paradigm is deployed in the SG environment, switches are responsible for the connectivity of the underlying power system equipment like sub-station or power plant to the main utility. Under the flooding attack, the victim switch will not be able to route the SG traffic - disconnecting the underlying equipment from the main utility as shown in Fig. 8 in which a PV power plant is facing DoS. Furthermore, SG traffic facing denial of service could be of critical nature like tripping signals of protection devices, that if not transmitted might cause damage to the SG equipment or even power outages.

TABLE XI: Machine Learning techniques for catering DoS attacks in SDN.

ML Technique	Algorithm	Description	Ref
Supervised	State Vector Machine	Multiple Linear SVM + SOM	Detection of DDoS attacks (97.6% accuracy) [239]
		RBF-SVM	Detection of DDoS attacks [240]
		RBF-SVM	Detection of DDoS attacks (97.6% accuracy) [241]
		SVM classifier	Detection of DDoS attacks (96% accuracy) [228]
		SVM classifier	Detection of DDoS attacks [242]
		RBF-SVM	Detection of DDoS attack (96.25% accuracy) [66]
		Linear-SVM	Flooding attacks (96.25% accuracy) [243]
	Decision Tree	ID3	Mitigating host locaton hijacking attacks [210]
		C4.5	DoS attack (Flow table saturation) [244]
		C4.5	Host hijacking attack [245]
		Enhanced C4.5	DoS attack (Prediction of TCP flooding) [246]
		XGBOOST	Prediction of TCP flooding attack [247]
	Bayes theorem	Naive bayes, KNN	Detects flooding attacks [200]

Unsupervised	Classification based clustering	k-means clustering	DDoS at application layer	[248]
		Dirichlet process mixture model (DPMM)	Mitigate DDoS attacks	[249]
		k-means, K-medoids	Detects flooding attacks	[200]
	Mapping based classification	SOM	Detects flooding attacks	[250]
		SOM	Detects DoS attacks	[251]
	Restricted Boltzmann Machine	Constrastive Divergence (CD)	Detects DDoS attack (Accuracy 92%)	[252]
Reinforcement	Deep RL	A3C, Double Q-learning	Detection poisoning attack	[253]
		A3C	Mitigating topology poisoning attach	[254]
		Q-learning	Saturation attacks	[255]
		DQSP	Detecs DoS attacks	[256]
	Actor-critic approach	Deep DPG (DDPG)	Flooding attacks	[199]
Deep Learning	Neural Network	NN + biological danger theory (95.11% accuracy)	DoS attack mitigation	[257]
	Deep Neural Network	DNN classifier	DDoS attacks	[258]
		CNN, RNN, and LSTM	DDoS attacks	[259]
	Artificial Neural Networks	SAE	DDoS detection (Accuracy 99.82%)	[260]
		CIPA	Detection of flooding attacks	[261]
		Radial basis function (RBF)	Detection of DoS attacks	[262]
		SOM	Detects flooding attacks	[250]
		SOM	Detects DoS attacks	[251]
	Feed forward neural networks	Back propagation	Impact of DoS attacks	[263]

2) Solutions for flooding attacks: Considering the security of SDN-SG, event flooding attack (EFA) is the novel attack introduced for the distributed SDN architectures. Attack modelling and analysis of the EFA attack are there in literature but mitigation techniques are still lacking. For standalone SDN architectures, authors have although generally discussed UDP and ICMP flooding but have not provided any attack modelling or mitigation technique. PYGRID, a TCP SYN/ACK flooding attack mitigation technique is proposed in the article [276]. To secure the SDN-SG against link flood attacks, research articles [150], [175] are analysing the effect of an attack on SDN-SG while authors in [61], [277] are proposing attack mitigation techniques by identifying abnormally loaded traffic.

B. Topology poisoning attack

1) Impacts of Topology poisoning attack: In the SDN-

SG environment, there is a possibility that a hijacked switch is governing any sensitive site like nuclear power station – resulting in havoc caused by denial of service to the nuclear site traffic. There is also a possibility that critical traffic containing signals and indicators for the stability of the SG might get dropped if routed via fraudulent links. The attacker might forge the SG traffic thus poisoning the real status of the SG. These false monitoring readings can manipulate operational decisions based on the monitored data.

2) Solutions for Topology poisoning attack: In SDN-SG, the effects of the Host Hijacking attack are discussed in [178] but mitigation techniques are still lacking in the literature. Regarding the link fabrication attack, authors in [176] are employing reinforcement learning to detect link failures and also shifts the traffic to benign links before traffic gets compromised.

C. Spoofing attacks

1) Impacts of the Spoofing attacks: In the SDN-SG environment, traffic of any switch that has been spoofed will face DoS like we can observe a spoofing attack on SDN-SG in Fig. 9 in which a malicious switch is impersonating a switch connecting advance metering infrastructure (AMI) to the main grid in SDN-SG. Furthermore, the other attacks that can be launched using spoofing attacks like flooding attack or host impersonating attack, whose impacts on SDN-SG

has been already discussed, can greatly risk the cybersecurity of SDN-SG if all attacks are launched simultaneously.

2) Solutions for Spoofing attacks: Talking about the security of SDN-SG, [61] has just discussed the IP spoofing attack without details like attack model, effect or solutions while authors in [178] have analysed the effect of the attack on SDN-SG in case of ARP spoofing attack.

TABLE XII: DoS attacks on critical infrastructure.

Year	Country	Description	Consequences	Ref
2007	Estonia	Large scale DDoS compromised the Internet infrastructure of the state	1 million US \$	[264], [265]
2012	UK	DoS on the hot-line of defence organisation (counter terrorism) in which telephones lines was bombarded by BotNets that repeatedly transmit a voice note "Team Poison"	Helpline for public remains suspended	[266]
2015	USA	ISIL tries to hijack the USA critical infrastructure (electrical power grid)	System sustained the attack but hints possible vulnerabilities	[267]
2015	Ukraine	DoS on power distribution control centre	200 megawatts energy loss and around 30 distribution stations went out of service	[268]–[271]
2016	Liberia	DDoS was launched using Mirai(malware that convert linux operating machines into botnets-remotely controlled). Attack was launched on the Internet sector	Majority of country went offline	[272]
2016	Ukraine	DoS was launched on transmission substation.	It cut off around 20% of the power of the Kiev city of Ukraine for one night	[271], [273]
2017	Saudi Arabia	DoS attack on national petro-chemical industrialisation or-organisation with an attempt sabotage the economy of the state as Saudi Arabia relies on petroleum export for financial sustainability	Power sector of Saudi Arabia dependant on petroleum face serious setback. It took 5 months to compensate the loss.	[274]
2019	USA	DoS attack on the power utility of Converse County, Los Angeles County and Salt Lake County of USA	Interrupts the supply of energy for about 12 million customers for about 10 hours	[275]

D. The Low-rate DoS (LDoS) attack

1) Impacts of the LDoS attacks: As mentioned previously, the effects of LDoS attack over SDN-SG are very much limited, but there is a possibility that the low-rate malicious traffic might intercept the critical

and control traffic of SDN-SG. LDoS attack traffic might create congestion on a link that is traversing critical traffic of protection to shutdown malfunction generators or transformer which otherwise could cause huge outages.

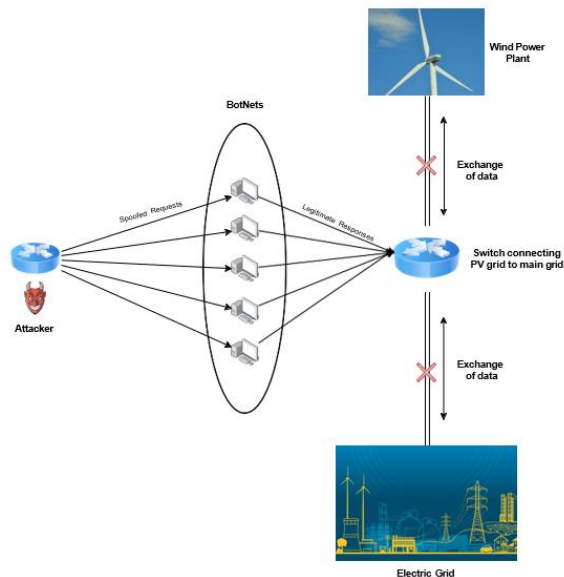
2) Solutions for LDoS attacks: In the case of SDN-SG, authors in [61] have just introduced the attack without details like attack model, effect or solution.

E. Response Attacks

1) Impacts of the Response attacks: The effect of response attacks on the SDN-SG environment is the same as in case of saturation and flooding attacks with the only difference is the nature of the attack is indirect i.e. via Botnets. Reflection attack on a switch connecting the wind power plant to the main grid in SDN-SG is shown in Fig. 12. Same like saturation and flooding attacks, not only the SG equipment under the victimised switch will face DoS, but also the progression of the effect towards SDN controller will result in DoS to the benign switches traffic causing massive level outages due to disconnectivity of the larger number of SG equipment.

2) Solutions for Response attacks: Currently, there are no solutions in the literature for detecting and mitigating response based attacks in the SDN-SG environment.

Fig. 12: Reflection attack on a switch connecting wind power plant to main grid in SDN-SG.



F. Saturation attacks

SG, a super critical infrastructure always remained focused in the research domain with efforts to further enhance its efficiency and application of SDN for SGC is the part of these efforts. In SDN-SG, switches and SDN controllers provide the communication paradigm for the underlying power system infrastructure. These switches and links connecting these switches and SDN controllers have paramount significance as they carry the SG traffic in between power system components and sub-components. Previously, we discussed the effects of DoS and saturation attacks on SDN, which hinder the services for legal users, similar applies to SDN-SG. Inherently, here the consequences are more adverse. The DoS attack will not only affect the resources, but can damage the interdependent systems. For example, a switch responsible for the supervision of a generation site, enabling a link to carry critical and control traffic related to fault operating mechanisms or observing a substation of a sensitive site is under DoS attack. Under such conditions, synchronisation of the SG will be adversely affected. Tripping signals from relays cannot reach circuit breakers will damage the faulty components and might cause cascading failures or a complete blackout. Compromised switch linked to a sensitive site such as nuclear power station might trigger catastrophic situations or a link relaying critical signals can corrupt the status of the grid to the control site. All such circumstances caused by DoS are highly critical and vital to be addressed in SDN-SG and must be catered efficiently for consistent operations.

TABLE XIII: Analysis of SDN based DoS attack mitigation techniques for SDN-SG, Part-I.

Technique Name	Attacks / Description	Application to SDN-SG	Ref
TopoGuard	Topology poisoning	Link fabrication attack and topology attacks are possible in SDN-SG. Here the topology update legitimacy checker mechanism of Topogaurd can prevent such attacks	[152]

FlowFence	Data-control link saturation	It identify congested links with flows greater than fair usage of bandwidth. This strategy is applicable to SDN-SG to tackle flooding attacks in which the attacker tries to overwhelm the resources	[224]
SDN Gaurd	Controller saturation, Data-Control link saturation, Switch saturation	SDN Application that works with IDS to identify and prevent malicious traffic. This can be applied to SDN-SG to identify attacks on switches to avoid the disconnection between sub-station and utility	[223]
Flowkeeper	Topology Poisoning, Data-Control link saturation, Switch saturation	This can be applied to make switches of SDN-SG more intelligent to empower smart traffic management at the switch level. It will save resources of communication infrastructure of SG as many of the decisions will be made at switch level thus less consumption switch-controller channel	[142]
Avant Guard	Data-Control link saturation	SDN-SG is prone to Syn ack flooding attacks which can saturate switch and also data-control path. Avantgaurd validates the legitimacy of these Syn packets and deals them at switch level to tackle attacks. Such smart switches complement the resilience of SDN-SG. Mitigate TCP-based flooding attacks but don't mitigate UDP, ICMP flooding	[225]
Cusum - Entropy	Flooding attacks	Detection of attack using signal processing technique Cumulative Sum to analyse the Entropy of traffic. This technique is effective for flooding attacks in SG-SDN as under flooding attack traffic is of diversified nature with high entropy	[174]
Flood shield	Data-Control link saturation, TCAM memory saturation, Controller saturation	This technique employed two modules: one to validate the address of the source to filter malicious traffic, and other to states of packets that belong to real addresses. All the parameters are configurable using the REST API. This adaptability is highly favoured by SG environment based on SDN	[222]
Multi-Criteria SDN	Data-Control link saturation	This technique ensures attack identification by utilising multiple criteria. When applied to SDN-SG it might demand more utilisation of resources but meanwhile, it is reliable	[226]
Flood Guard	Data-Control link saturation, SYN/ACK flood, UDP flood, ICMP flood	Floodgaurd can ensure the acceptable operation of SDN-SG even under the attack using Data Plane Cache. It protects the controller by installation proactive flow rule to tackle attacks. But to install all flows that could be possible is not practical. Not suitable for SDN-SG as it lacks the ability to tackle emerging attacks.	[67]
SDPA	Data Plane Intelligence	Application of stateful data planes to SDN-SG to make switches more intelligent.	[227]
OPERETTA	SYN/ACK flood	This technique can Detect and mitigate SYN flood attacks in SDN-SG networks by rejecting fake connection requests	[206]
SLICOTS	SYN/ACK flood	Introduces a pending list. All syn requests are moved towards it rather than keeping the connection in half-open mode. When an ack is received, syn request in the pending list is entertained and the connection is established. SDN-	[205]

		SG can utilise this technique by exploiting the programmability feature of SDN controller, no additional physical infrastructure is required	
SYN Guard	SYN/ACK flood	In Syn flooding, an attacker repeatedly sends a syn request and does not reply with syn/ack. Controller remains engaged to wait for the reply. Syn guard identifies the MAC addresses with pending syn/ack requests. When requests cross a certain threshold of a pending request, that MAC is blocked. This technique is applicable to SDN-SG as it is installed on a controller requiring no extra infrastructure to be installed on data switches	[204]
Flood-Defender	Saturation attacks	An effective technique for SDN-SG without any additional hardware modification and offering a wide range of protection against DoS attacks. It can prevent data-control path saturation, switch saturation, and controller exhaustion in SDN-SG environment	[228]
SPHINX	ARP spoofing, Topology poisoning, Controller saturation, Switch saturation	Controller application that oversees the SYN requests by each host and raises alarm if a certain host exceeds the defined threshold. It's a controller application that doesn't require any additional physical infrastructure to be installed so it is favourable by SDN-SG.	[141]
WEDGE-TAIL	Data plane flooding	It systematically and autonomously prioritise network policies. Real-time updating of attacks definition will make SDN-SG more resilient to attacks. It offers minute interference to operations of the system while running its defence mechanism against attacks: a viable approach for real-world networks like SDN-SG communication	[221]
Cyberpulse	Link flood	Targeting a specific critical link carrying crucial traffic can be triggered using link flooding attack that can be tackled using the Cyberpulse technique	[203]
SLAMHHA	Host hijacking	Hijacking a switch can compromise the underlying power system equipment in SDN-SG and its a very critical condition. Advising this technique can resolve such circumstances	[210]
SA-Detector	Flooding attacks	SDN-SG can be compromised by flooding bulk switches with the bulk of malicious traffic. SA-Detector can detect such traffic by finding the similarities between traffic to distinguish abnormal traffic	[198]
BASE	IP Spoofing	Impersonating a legal switch of SDN-SG infrastructure cause DoS for the victim that might of critical nature. BASE can inject resilience in SDN-SG for such attacks	[214]

TABLE XIV: Analysis of SDN based DoS attack mitigation techniques for SDN-SG, Part-II.

Technique Name	Attacks / Description	Application to SDN-SG	Ref
BASE	IP Spoofing	Impersonating a legal switch of SDN-SG infrastructure cause DoS for the victim that	[214]

		might of critical nature. BASE can inject resilience in SDN-SG for such attacks	
Generalized Entropy (GE)	low rate DoS	Such attacks are very tough to be detected as they employ low rate attack traffic. SDN-SG under such attacks can suffer un-noticed damage. Entropy estimation using GE can detect such attacks in SDN-SG	[215]
AuthFlow	Host hijacking	Applicable for SDN-SG to ensure the authenticity of the switches that are trying to get linked to the network	[209]
Moving Target Defence	Link flood, ICMP flood	It can be utilised to safeguard crucial links in SDN-SG	[201]
DoS detection and mitigation	TCAM memory saturation	Switch saturation attacks can be detected and mitigated using this technique in SDN-SG	[197]
SGaurd	IP spoofing ARP spoofing	Spoofing attacks can cause DoS for any critical site of SDN-SG for which spoofing attack is impersonating for. SGaurd has the capacity to block such requests	[213]
FlowChecker	Switch consistency	Switches are critical for SDN-SG as these are terminal elements that connect the underneath SG equipment. FlowChecker ensures consistency of the switches by validating the correctness of flow tables and also the reliability of intra-switch communication and implementation of new configurations by SDN controller	[229]
VeriFlow	Flow rules consistency	Routing decisions in SDN-SG are based upon the flow rules defined by the SDN controllers. Processing (insertion, modification, deletion) of these flow rules is also prone to bugs. Implementation of VeriFlow has the potential to check the consistency of these flow rules with much low latency - low overhead with no effect on SDN-SG performance due to this additional scrutiny mechanism	[230]
FlowVisor	Network Slicing for re-silience	Switch has a critical role in SDN-SG and demands adequate resilience. When an attacker gets succeeded in launching an attack, the whole switch gets compromised. FlowVisor logically separates the switch resources into slices having isolated abstraction of physical resources. If the attacker is succeeded in the attack, only the particular slice will be affected rather than the whole switch thus providing the service to SDN-SG even in the event of attack	[231]
VAVE	IP spoofing ARP spoofing	Host impersonating aka spoofing attacks not only initiate DoS for the victim elements but also can trigger man in the middles attacks in the SDN-SG. VAVE validates the source address of any request before processing it. Now spoofed request will be filtered out in SDN-SG	[212]
DISCO	Distributed SDN re-silience	Microgrid environment is highly favoured by the distributed SDN architecture in which each SDN controller can assume the functionalities of each microgrid under the interconnected SDN-SG system. DISCO is the key player to ensure the consistency and resilience of communication between the SDN controllers and also to mitigate the propagation of attacks from one controller to the other	[232]
VeriCon	Controller applications validation	SDN controller allows to model innovation in the SDN-SG by implementing policies and also formulating applications. All the routing decisions and security	[233]

		mechanisms are operated in accordance with the SDN applications. VeriCon checks the consistency of these applications as any loophole in the SDN app can compromise whole SDN-SG	
FAST	Proactive defence	FAST pre-installs flow rules and then process packets by matching them against the applied flow rules. It is an effective approach for securing SDN-SG as flooding attacks can be mitigated in advance, but it has lacked support for the run-time installation of new flowrules. Whenever any flow is be inserted to engineer a link to the new SG premises, first SDN controller has to be informed in advance rather than run-time configuration as in case of reactive operation of SDN	[220]
SDNScore	Flooding attacks (detection and mitigation)	SDNScore inject intelligence into the switches using statistical analysis of traffic so that malicious flooded traffic can be identified at switch level	[202]
SAFETY	SYN/ACK flood	Flooding attacks on SDN-SG can saturate system resources so demand extra attention for early detection. SAFETY by utilising entropy of the flow can check the randomness of the traffic. Under the random attack traffic with much greater entropy, proposed security mechanism can detect in advance the SYN flooding and safeguard SDN-SG	[207]

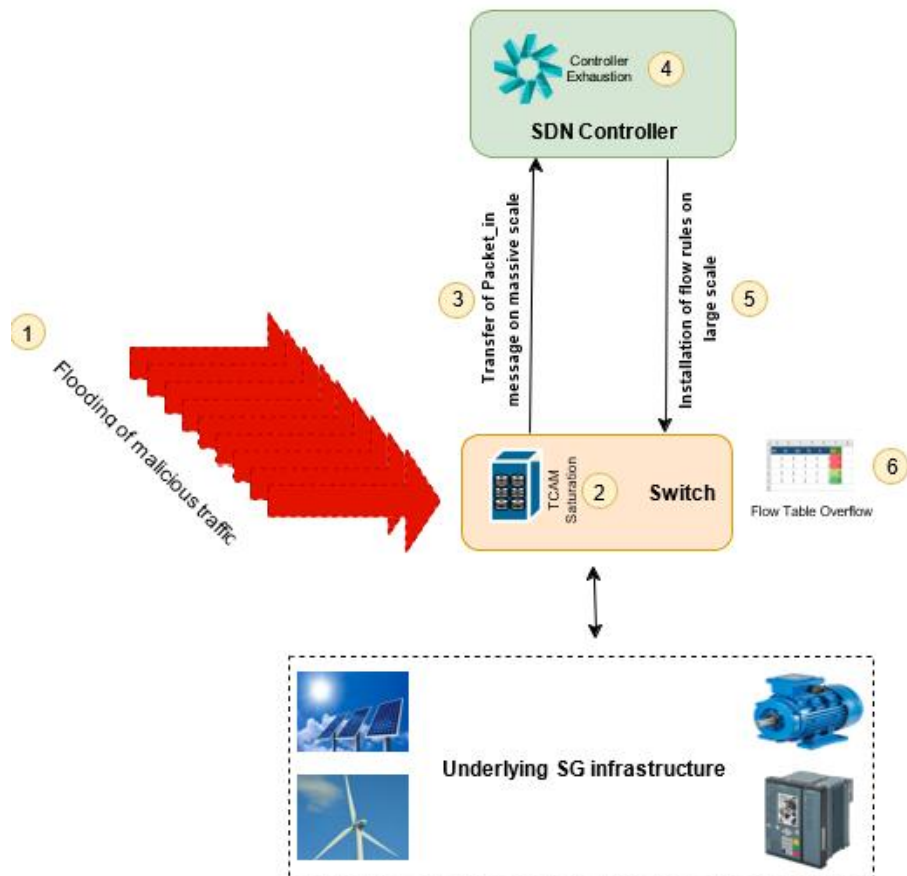


Fig. 13: SDN-SG under switch saturation, controller saturation and data-control plane saturation.

DoS attacks are launched with the primary goal of interrupting the service for legit users. Various attacks have associated effects on SDN-SG which are discussed in detail as follows:

- **Flooding Attacks:** Flooding the specified links, switches or SDN controllers may halt the underlying power system equipment under victim supervision. If a switch of a substation is under attack, then that particular substation will not be able to interact with the rest of sub-systems.
- **Spoofing Attacks:** Impersonating to be a legit switch will cease the availability of service to the victim. Supposing, an attacker attacks a particular substation and behaves as a valid and authorised switch. The attacker will have access to the SDN-SG, so these attacks can inject false energy requests, false energy supply information or false link states in the SDN-SG system.
- **Saturation Attacks:** SDN-SG has to energise the critical sites. Saturation attacks can be launched to saturate the network resources like a switch, controller or data-control channel by flooding of malicious traffic. Now those critical sites would not have access to the SDN-SG and cannot update the grid about energy supply/demand and faults status.
- **Topology Poisoning Attacks:** Attacker either hijacks a switch or fabricate any malicious links in the SDN-SG communication layers. Under both conditions, the victim domain will observe DoS and associated services like real-time monitoring, fault management, demand-response system, and real-time pricing will get suspended.

Saturation attacks are followed by flooding of malicious traffic in which the rate of flow of traffic, traffic density, and entropy of the traffic is quite high relative to benign traffic. Furthermore, due to over-utilisation of network resources by the attack traffic, legitimate traffic also has to face delay and even DoS. Considering these facts, evaluation metrics like measuring entropy [174], monitoring network resources [182], [186], [191], and ensuring QoS [179] for meeting the SG application specified minimum threshold of data rate and latency are highly favourable for SDN-SG.

1) Impacts of the saturation attacks: In the SDN-SG environment, the SDN controller resides in the control centre that aggregates the traffic from all the switches and also performs traffic routing and engineering. Under the saturation attacks, not only the SG equipment under the victimised switch will face DoS, but also the progression of the effect towards SDN controller will result in DoS to the benign switches traffic. Such circumstances can cause outages on a very huge scale as multiple SG elements are now disconnected from each other and also from the main grid. Communication layer efficiency is now compromised as the SDN controller is lacking its capability to engineer efficient traffic routing. We are considering a use case of an SDN-SG in which a switch is handling the underneath SG infrastructure by providing the communication arena to the SG. Attackers tend to initiate the saturation attack on SDN-SG by overwhelming the SDN devices as shown in Fig. 13. The attacks are launched following the sequence:

TABLE XV: DoS Attacks on SDN and SDN-SG.

Attacks			SDN	Details	SDN-SG	Details
Direct	Topology Poisoning	Host Hijacking	[192]	Attack modelling by exploiting vulnerabilities	[178]	Analysed the effect of attack on SDN-SG
		Link Fabrication	[142]	Attack modelling by exploiting vulnerabilities, Attack mitigation using variant of TopoGaurd	[11]	Attack analysis and mitigation technique using reinforcement learning
	Spoofing	IP Spoofing	[92]	Detection of attack	[61]	Just discussed without details like attack model, effect or

Direct/Response						solution
		ARP Spoofing	[193]	Detection of attack, Mitigation of attack (customized algorithm)	[178]	Analyzed the effect of attack on SDN-SG
	Flooding	TCP Flood	SYN/ACK	[199]	Possibilities of attacks Analysis of effect of attack on network	[61], [175], [276], [278] Just discussed without details like attack model, effect or solution, while [276] is assessing the effect of attack on SDN-SG
			RST/FIN	[17]	Effect of attack on network	[61], [95], [175] Just discussed without details like attack model, effect or solution
		UDP Flood		[199]	Statistics (entropy measurement) for detection of attacks	[61] Just discussed without details like attack model, effect or solution
		ICMP Flood		[200]	Machine learning algorithms such as Naive Bayes, K-Nearest neighbour, K-means and K-medoids for detection of attacks	[61] Just discussed without details like attack model, effect or solution
		Link Flood		[196]	Detection and prevention of attack	[61], [150], [175], [277] Analyzed the effect of attack on SDN-SG, Attack mitigation by identifying abnormally loaded traffic
		Event Flood		[194]	Modelling of attack on DSDN architecture. No mitigation technique provided	-
		Low Rate DoS		[195]	Effect of attack on network	[61] Just discussed without details like attack model, effect or solution
	Saturation	Switch Saturation	TCAM Memory Saturation	[197]	TCAM memory saturation	-
			Flow Table Overflow	[92]	Effect of attack and mitigation techniques	-
		Data-Control Link Saturation		[92]	Effect of attack and mitigation techniques	-
		Controller Saturation		[198]	Effect of attack and mitigation techniques	-
	Reflection based attacks			[216]	Study of attack and Defence mechanism against attack	-

Amplification attack	[150]	Possibilities of attacks analysis of effect of attack on network	-	-
----------------------	-------	--	---	---

i) Flooding of malicious traffic: Attacker direct bulk of fraudulent packets (TCP / UDP / ICMP) towards the victim switch (Step 1 in Fig. 13). As attacker impersonates to be a real legal user using ARP/IP spoofing or host hijacking attacks, so SDN controller cannot judge it that incoming bulk traffic is malicious traffic.

ii) TCAM saturation: When any new packet arrives at the switch, switch parse its header and transmit it to the controller after encapsulating it in the *packet in* message. As far as the controller decides the rule for the packet, it is kept in the TCAM. Now there are bulk of messages forwarded by the attacker that will saturate the TCAM (Step 2 in Fig. 13).

iii) Controller exhaustion: There is a bulk of attack traffic that will arrive at the SDN controller. SDN resources, such as identifying new routing requests and installing specified flow rules, will be exhausted dealing with the attack traffic (Step 4 in Fig. 13).

iv) Data-Control plane saturation: malicious traffic

arrived at the switch do not find already installed flow rules so it will be sent as *packet in* message towards SDN controller. Sending bulk of *packet in* messages corresponding to attack traffic and receiving the associated flow rules from the controller to be installed on the switch will overcrowd the data-control channel (Steps 3, 5 in Fig. 13). This saturation occurs for both cases in-band or out-of-band data-control channel.

v) Flow table overflow: When the bulk of packet in requests of malicious traffic arrived at the SDN controller, it processes them and initiates instructions to install the associated flow rules in the switch. As a result, a bulk of flow rule requests are directed towards the switch to install them at the switch. As flow table memory is limited, that bulk quantity of the flow rules will overflow the flow table memory. Switch will be even halted to install flow rule requests of legit traffic, (Step 6 in Fig. 13).

TABLE XVI: Machine learning techniques for SDN-SG security.

ML Technique	Description	Ref
Unsupervised	k-means clustering, Incremental k-means	Anomalies detection [279]
	Transfer learning	V2G security [177]
	K-means algorithm, K-modes	Privacy preserving [280]
	AutoEncoders (AE)	Anomalies detection [281]
Reinforcement	LFL-MAB	Link failure [176]
Deep Learning	DFF neural network	Anomalies detection [281]

2) Solutions for saturation attacks: For the SDN-SG modelling, analysis, mitigation techniques for saturation attacks in an open field demanding the attention of the research community. A list of DoS attacks that could occur in SDN and their potential ability to harm SDN-SG is presented in Table XV. Some attacks are well discussed and analysed in the literature for SDN-SG such as ARP spoofing [178], link flood [61], [150], [175], [277] and host hijacking [178], while others such as attack effect, risk analysis or mitigation techniques lack some details. It has been found that this leaves sufficient research gap that need to be addressed for these attacks as in UDP Flood [61], ICMP Flood [61], TCP flood (SYN, FIN, RST) [61],

[175], [278], IP Spoofing [61], and the Low-rate DoS [61]. Furthermore, there are certain attacks which are still unaddressed and demands significant attention in SDN-SG. Saturation attacks on a switch, controller and data-control channel are still not considered in SDN-SG. Other attacks like amplification, reflection, event flooding, and link fabrication attacks are some areas of SDN-SG that needs to be researched. Fig. 14 is classifying the research scope of DoS for SDN-SG. G. Machine Learning for DoS Attacks in SDN-SG

ML techniques are highly favourable for environments where uncertainty and unpredictability are quite high. SG, being a consumer utility, observes a highly

uncertain environment subject to the varying responses of the consumers. In such an environment, ML can learn about the systems and take appropriate actions accordingly. SDN-SG that inherits the uncertainty of SG finds its scope for ML for the security of SDN-SG. Learning abilities that SDN-SG acquire from the application of ML will greatly complement its security for novel DoS attacks currently unknown. Furthermore, the learning abilities of ML also supplements the decision making of the SDN controller to distinguish between normal and attack traffic, benign and poisoned topology, and legit switch and impersonating attacker switch. Table XVI presents various ML algorithms deployed for SGN-SG security. We have analysed that the application of ML for the dealing DoS attack in the security of SDN-SG is in its infancy stage. Only four articles have considered the application of ML for SDN-SG. In this work, we are also envisioning to utilise ML for the mitigation DoS attacks in SDN-SG.

H. Summary and Insights

In this section, we have observed that although the security of generalised SDN architecture is matured enough, but SDN-SG security is still a developing field in which various attacks are still unaddressed in the literature. Considering the security of SDN-SG, attacks such as UDP, ICMP, and TCP flooding, LDoS, IP spoofing are briefly discussed without details about attack models, attack effects on the SG, or defence mechanisms/ mitigation techniques due to lack of work done in the domain. Attack modelling and analysing the effects of the attack on SDN-SG has been performed in various paper for Host Hijacking and ARP spoofing attack. Link flood attacks are discussed in the paper proposing attack modelling, analysis, and mitigation technique. Regarding the link fabrication attacks and response attacks, literature needs to be developed for attack modelling, analysis, or mitigation techniques. Currently, there is not much work on the saturation attacks on SDN-SG. Neither the effects of these attacks on the SDN-SG is analysed, nor any mitigation techniques are proposed. This is an open area of research in SDN-SG to analyse the dynamics (severity, effect radius) of these attacks on SDN-SG. Furthermore, considering the SDN-SG

security requirements for stringent QoS, critical tasks execution by switches for underlying power grid equipment, and demand for highly reliable contingency services; generic SDN security techniques are not suitable for SDN-SG. Considering the unique dynamics of SDN-SG, devising novel metrics, or distinguish the network behaviour and traffic trends during an attack and benign state, is also an open area of research.

VIII. OPEN ISSUES, CHALLENGES, AND FUTURE RESEARCH DIRECTIONS

Emerging SDN-SG has attracted great attention from the research community, however, with the requirement of security and maturity in the area, its widespread implementation still demands various research challenges to be addressed. In this section, challenges, issues and potential research directions for the security of SDN-SG are discussed.

A. Threat Assessment of SDN-SG

We have observed in this survey article that SDN-SG is currently a developing domain with much room for improvements and advancements in many sectors; especially in its threat assessment. To ensure reliable and secure operations of SDN-SG, possible vulnerabilities need to be identified and managed. For this purpose, sufficient efforts are required to measure, quantify, and priorities the security threats of SDN-SG for better resilience.

1) Evaluation Metrics for SDN-SG Security: Metric, which is defined to be the standard of measurement, is the foundation of the assessment method. Metrics are utilised to measure the specified attribute of the system. These attributes when cross a certain threshold, violating benign operations, are measured by the metrics and identified as a security threat of the system. Implementation of SDN for SG has evolved a unique data plane of SDN-SG in which there is underlying SG infrastructure under the SDN switches, unlike the enterprise SDN in which SDN switches are free from such underlying infrastructures. The unique data plane of SDN-SG also demands a unique

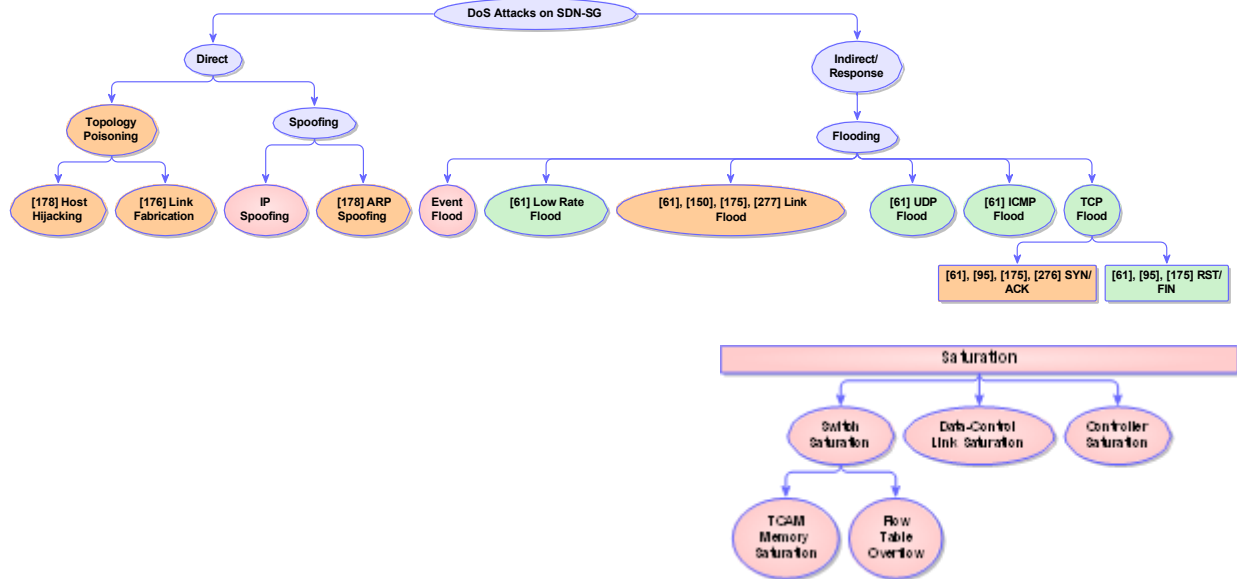


Fig. 14: Classification of DoS attacks on SDN-SG. Orange boxes represent attacks that are already addressed. Green boxes shows attacks are just discussed in the literature while Red boxes depict attacks that are not still observed in SDN-SG.

SBI. These unique data plane and SBI are possible areas that can be exploited by the attacker. Moreover, attacks can also be launched by the underlying SG equipment under the switch if in case attacker gets a chance to physically access the SG equipment.

Considering these facts, this field of SDN-SG featuring the benefits of both the SDN and SG demands suitable evaluation metrics to assess the possible threats. Metrics that can evaluate and quantify the normal operation of SBI are required, so that threats can be identified if normal operation is interrupted. Moreover, vulnerable areas of underlying SG equipment also needs to be assessed with suitable metrics. But the composition of the metrics that can distinguish between normal traffic and the attack traffic is a challenging task as traffic patterns of normal and attack traffic are quite overlapping.

Metrics deployed for assessing enterprise SDN security are presented in Table V. Furthermore, we also accumulate certain evaluation metrics in Table VII that can be utilised for assessing SDN-SG. Here two research questions demand the attention of the researchers to assess the scope of evaluation metrics for SDN-SG. Whether the metrics of enterprise SDN can be extended for SDN-SG nor not? Are potential metrics identified for assessing SDN threats, as a part

of this survey article in the Table VII, can produce reliable results or not? Furthermore, considering the unique security requirements of SDN-SG, future research work can also be modelled to present new evaluation metrics.

2) Evaluation of Risks in SDN-SG: A complete risk assessment of SDN-SG highlighting the strengths and weaknesses of SDN-SG is required. Like penetration testing, in which the internal vulnerabilities and also the possible breaches providing access to intruders, is required in SDN-SG. Risk is characterised by its impact and likelihood of occurrence, so for the case of SDN-SG, possible risks need to be get evaluated. What will be the effect of the electrical failure of any electrical equipment on the SDN switch? SG is a consumer-based utility subject to a higher degree of variations, like sudden fall of load or generator can be misinterpreted as an attack. How risk assessment model will distinguish between abnormal and attack conditions? What will be the effect on SG equipment if the associated SDN switch gets compromised? These are some of the questions that need to be addressed in the research for the overall risk evaluation of SDN-SG.

3) Characterisation of Cascading Failures: In the case of interconnected systems, cascading failures are the

major threat to system security. Same as for SDN-SG, in which operation of each equipment is dependant on the operation of one or more equipment, such that failure on one equipment also leads to failure in others, and the chain continues. The main reason for these cascading failures is the higher degree of interconnectedness of various components of SDN-SG. This highlights the need to measure and characterise this effect of cascading failures while performing the threat assessment of SDN-SG. A detailed analysis of SG equipment operations and their prior dependence on other SG equipment, and also the SDN equipment is required. This study can figure out various zones of SDN-SG, like red zone with the highest level of interconnectedness and attack on it can result in disruptions at the maximum level, or yellow or green zones with intermediate to a low level of interconnectedness and associated disruption levels respectively. The main challenge is to model the propagation of failures from one component of SG to the other, and also to introduce the effect of SDN components failures. What factors need to be considered here? Is the efficiency and reliability of current SG equipment have any role in deciding these factors? The behaviour of consumer reflects the operations of SG equipment – whether to operate the SG equipment on full, intermediate or under capacity is decided by the load demands of consumers. How to include this factor of consumer demand and the corresponding behaviour of SG equipment in threat assessment model? is another question that needs to be addressed.

4) Identification of Attack Vectors: Attack vectors by means of which attacker gains access to the system for launching the cyberattacks need to be evaluated and categorised for SDN-SG with an effort to formulate attack mitigation mechanisms. Classification of attack types and their associated effects on the system is the basics to develop the attack mitigation solutions. Such analysis is also desired for SDN-SG for developing its defence techniques.

In Fig. 4, we observe various interfaces of SDN architecture. These interfaces will also be observed for SDN-SG and these can serve as potential attack vectors. We have discussed the unique data plane of SDN-SG. Furthermore, the SDN controller operating in the Electric Control Centre with operations

followed by the SG dynamics, also have to observe changes in the NBI – a unique NBI just like the unique SBI. In the case of MGs, there will be an SDN controller for each MG. These distributed SDN controllers in SDN-SG interact with each other using EBI/WBI interfaces, but this interaction is followed by the operations of SBI and NBI interfaces, which have to face certain changes upon SDN application to SG. This means the interaction between SDN controllers that will be utilised for distributed MG architecture has to also consider unique EBI/WBI interfaces relative to enterprise SDN. These unique SBI, NBI, and EBI/WBI are in very early stages, so a rigorous evaluation is required to identify the possible attack vectors.

We also discussed about the underlying SG equipment under the switches in SDN-SG, which can be utilised as an attack vector to gain access to the SDN-SG and launch a cyberattack. This novel attack vector of SDN-SG is not studied in the literature and needs to be investigated.

5) SDN-Aware Comprehensive Threat Assessment Method: SDN application to SG also induces its domain-specific vulnerabilities, in addition to the security threats of SG and emerged SDN-SG. Various threat models deployed for enterprise SDN are discussed in Table VI. Out of these, CVSS has been implemented for SDN-SG also in [61], [277] for link flood attack only. In these articles, [61], [277], only the data plane vulnerabilities are discussed. Threat assessment model, that are aware of unique SDN-SG interface (SBI, NBI, EBI/WBI) and also the operational dynamics of SDN-SG, is required to perform the comprehensive security assessment of SDN-SG. An assessment model that can cover all the specified domains of the data plane, control plane, application plane, data-control link, SBI, NBI, EBI/WBI, known and unknown threats. This is an open research area that will lead towards a more secure SDN-SG.

Furthermore, refer to the Table VI, here we can observe that even for the enterprise SDN, not threat assessment method is covering all the specified domains of the data plane, control plane, application plane, data-control link, SBI, NBI, EBI/WBI, known and unknown threats. A comprehensive threat

assessment model for assessing the possible exploitable covering all the possible domains is also an open research area for the enterprise SDN also.

B. DoS in SDN-SG

In Section VI, we have discussed DoS in enterprise SDN and further evaluated the scope of these DoS attacks for SDN-SG in Section VII. It is evident from the Table XV that only few attacks like host hijacking [178], link fabrication [176], ARP spoofing [178], and link flood [61] attacks are addressed in literature for SDN-SG. While, other DoS attacks, are either just discussed with insufficient attack analysis/ mitigation or not addressed at all. Considering this super CI SDN-SG, the significance of these attacks is much elevated as its a direct threat to the state operations and business.

1) Event Flooding Attacks: We have discussed EFA and its associated terminologies such as strong consistency, eventual consistency, blocking time and read time in Section VI-A for distributed SDN in which attacks on one SDN controller propagates to other controllers also. Distributed SDN architecture can also be deployed for MGs based SDN-SG systems. Here question arises that whether EFA on SDN-SG will have the same consequences or not?

Attack Analysis: To evaluate the effects of EFA on SDN-SG, a detailed analysis needed to be carried out to determine the performance of all the SDN controllers and thus also the associated MGs under EFA. An article discussing EFA [194] claims that this attack leverages the strong consistency models of the distributed SDN architecture. There are multiple SDN controllers that are utilising strong consistency such as OpenDaylight, Disco, and ElasticCon. A study of SDN-SG can be carried out to evaluate these SDN controllers with associated strong consistency models to analyse the influence of EFA under each case. In this study, each SDN controller can be evaluated for the reach of EFA to figure out the number of SDN controllers it is affecting, time of propagation of fault from victim controller to other controllers and degree of DoS, victim controller, other controllers, and associated SG equipment have to bear. This will help us to determine the most stable SDN controller for SDN-SG. Currently, there is no research work in the literature regarding these issues and are open research

areas.

Attack Mitigation: Successful attack analysis can provide the researchers with the desired insights required for devising a reliable mitigation technique. Authors in article [194] have discussed EFA for SDN, but have not proposed any mitigation technique. These research gaps in literature demand the researchers to devise a suitable attack mitigation technique for EFA in SDN-SG and also for distributed enterprise SDN.

EFA is exploiting the strong consistency of the distributed SDN architecture, that can be resolved either by proposing a more secure strong consistency model or by revising the existing strong consistency models to fix the vulnerability. In either case, the main challenge is the increased blocking time and the read time offered by strong consistency models that retain any operations until all SDN controllers of distributed architecture are on the same status. But, how SG time-critical traffic will be traversed during this time duration? This issue can be resolved by the SDN controller such as ONOS with a hybrid consistency models leveraging benefits of both strong and eventual consistency, to ensure the timely operation of time-critical traffic. How these hybrid consistency models will work in SDN-SG, and what are their effects on the overall operation of SDN-SG? Can SDN-SG afford strong consistency at the cost of less availability? Is SDN-SG is immune to the conflict of data caused by eventual consistency or not? A policy can also be implemented to resolve the data conflicts of eventual consistency, but will these initiatives can help to secure SDN-SG against EFA or not? These are some of the research directions that need to be investigated.

2) Spoofing Attacks: The significance of the spoofing attack is highlighted in Section VII-C1 in which such attacks may even lead to cascading failures and also might affect other CIs. There are could be various possibilities in which this attack can be launched in SDN-SG. These possibilities and their corresponding effects are not studied in the literature for SDN-SG.

Attack Analysis: Authors in article [178] have performed attack analysis for ARP spoofing attack, but a detailed attack analysis is a need for the security of SDN-SG to evaluate various cases of spoofing attacks. Measures, intruders took for spoofing attacks,

and corresponding attacks trends, need to be analysed. This observation can help the research community to understand and distinguish the attack and benign conditions. But, the SG equipment are so huge in number and attack analysis have to be performed in each minor cases such as what happened if attacker impersonates to be:

- a relay initiating false signals to circuit breakers,
- a circuit breaker to shut down generator or transformer,
- a consumer meter sending false demand requests,
- an energy storage bank to give false storage status,
- a SDN switch to compromise the underlying SG equipment,
- an SDN controller affecting the whole system.

Performing an attack analysis for each individual case is a challenging task. All these SG equipment are operating on different protocols. In case of spoofing attack on protection devices, the SG equipment under protection may vary, such as in one case, the circuit breaker is protecting a transformer while for the other case, its implementation is for generator – attack affecting the SDN-SG uniquely in each case. Furthermore, connections could be wired or wireless, and the flow of SG traffic could be either a packet or flow level. These are the few research challenges that can be studied for performing the attack analysis of spoofing attacks.

Attack Mitigation: The challenges discussed in attack analysis of spoofing attacks also need to be considered in either testing the enterprise SDN solutions or while proposing new solutions. The biggest challenge, proposed solutions have to deal with is to achieve interoperability in such a heterogeneous environment compromising of various propriety devices operating on different protocols. This issue of interoperability can be resolved by using the inherent feature of SDN – protocol Independence. But, how much time will be required to fully transform the SG into SDN-SG? Efforts can also be done to provide a unique identifier for each SG equipment or to deploy authentication procedures like cryptography to validate the integrity

of SG equipment. But, these unique identifiers can be provided to intelligent SG devices only, while SG is still in transforming stages in which mechanical devices also exist. Either these mechanical SG devices need to be replaced with intelligent devices or methods to embed intelligence in these mechanical devices needs to be investigated.

3) Saturation Attacks: The severest DoS in which the resources of the SDN-SG get saturated to an extent that it becomes unavailable for the legit users. Now, even if the system has the attack mitigation procedures to handle attack conditions, but still SDN-SG will get compromised. As attack mitigation procedures can be applied only if the SDN-SG equipment are connected to the system, but here due to saturation, SDN-SG equipment are facing DoS – halt the defence system. In Table XV, it has been evaluated that saturation attacks are not discussed in the literature for SDN-SG in terms of attack analysis and attack mitigation. These attacks demand great attention of the research community in the effort to secure SDN-SG.

Attack Analysis: It is evident from the Section VII-F1 and Fig. 13 that saturation occurs as a result of flooding attacks. We also discussed the halt action of saturation attack in the above paragraphs. Furthermore, the various type of saturation occurring at the switch, data-control link, and the controller needs to be analysed. To detect saturation by flooding, there could be two ways; 1) validation of authentic sources of SDN-SG to reject spoofed sources, 2) monitoring and updating the benign flows so that any flow can be terminated when a certain threshold is crossed. Considering the first solution, an attacker can impersonate to be the legal user to dodge the system. Techniques to avoid such circumstances have been implemented for enterprise SDN [212]–[214], but can these techniques detect attacks when an attacker is impersonating to be any of SG equipment? This question requires further evaluation. For the second envisioned solution, this concept of observing a certain threshold is not viable for SDN-SG. As SG is a consumer-based utility that is subject to a higher degree of variations – sometimes flows can be very high or low. This randomness of traffic flows can be managed with the use of ML techniques. These are few research directions need to be considered while performing the attack analysis of SDN-SG.

Attack Mitigation: The above discussion about saturation attacks suggests that future research efforts can be directed to achieve a proactive defence system for SDN-SG. We have observed that multiple solutions using diversified technologies like ML, controller application, and IDS systems have been deployed for enterprise SDN [67], [141], [142], [221]–[223]. Firstly, there is also a need to study the application of existing SDN solutions for SDN-SG. Considering the significance of SDN-SG as super CI, can these techniques can provide an acceptable level of operations even in adversarial settings? Secondly, a new mitigation technique can be proposed for SDN-SG using the concept of injecting intelligence in SDN switches. Now the majority of traffic will be dealt at the switch level, minimising the chances of data-control link and controller saturation. Considering the unique data plane of SDN-SG, what will happen if the flooding attack is launched from the underlying SG equipment, e.g. bulk of demand requests or energy trading queries? Flooding leading towards saturation can be of any protocol such as TCP, UDP, or ICMP. There are mitigation techniques for each protocol for enterprise SDN, but a comprehensive saturation attack solution for SDN-SG have to consider all possibilities.

4) **Response Attacks:** These attacks can utilise BotNets to escalate the effect of over mentioned attacks on SDN-SG. Any type of flooding attack can be escalated using response attacks. The main challenge is, these attacks do not reveal the identity of intruders.

Attack Analysis and Mitigation: Study of attack modelling of these attacks to analyse the effects on SDN-SG is an open research area. By this analysis, the dynamics (severity, effect radius) of the attacks on SDN-SG can be observed. The main challenge here is the anonymous nature of the intruder that cannot be traced back. Even if the attack gets contained successfully, but still we have no information about the attacker to be kept in the database to avoid future attacks. Efforts can be directed to devise suitable methods that can track the intruder if in case of SDN-SG environment such attacks.

As response attacks are not analysed yet, that's why attack mitigation techniques are also not proposed for these attacks yet. The main challenge in developing a defence mechanism is the lack of information about

the attacker identity. Every time attacker attacks, it will be considered as a new attack, even though that sort of attack has been tackled by the mitigation solution before. Considering the significance of this super CI, immediate efforts are required to secure it against the specified attacks by tracing the attacker identity. As the victim switch get over-saturated due to very bulk malicious traffic, here concept of redundant switches can be utilised by terminating the victim switch and directing its traffic towards the redundant switch. What will happen to traffic in the moment of traffic transition from victim switch to redundant switch? This time will be minute, but what if SDN-SG time-critical traffic get compromised during this duration? Furthermore, redundant switches will also uphill the economics of the system. This demands a techno-economical analysis to evaluate the benefits of security at the cost of economics. All these steps can ensure a secure environment to leverage the benefits of SDN for SGC.

C. Machine Learning for SDN-SG Security

In Section VII-G, we have analysed that some authors have considered ML for SDN-SG security [176], [177], [279], [280], but the application of ML is limited to certain attacks only like link failure, V2G, anomalies detection of link failure attack. Comprehensive ML-based solution addressing all sorts of attacks in SDN-SG can be a great contribution to the research community.

1) **High-Quality Datasets:** The implementation of ML techniques is followed by training with quality datasets. These datasets are the foundation of ML operations. The same is the case of ML for SDN-SG security. Sufficient high-quality datasets are required for the deployment of ML for SDN-SG security. How to determine if the dataset is sufficient or not? If the dataset is of high quality or not? These are possible research directions to enable ML-based SDN-SG security solutions by studying the relationship among the datasets sample space, SDN-SG network unique requirements, and false positives and false negatives of ML algorithms.

Datasets like KDD99, NSLKDD [282], [283] or ISCX 2012 dataset [284] are effective for already known attacks, but here, two challenges need to be considered. First, new attack vectors emerged with the

integration of SDN and SG also introduces new attacks, that are previously unknown and are also not present in the existing datasets. This requires efforts to aggregate and maintain an all network flow data of SDN-SG platforms deployed to develop a comprehensive dataset. Acquiring and managing fine-grained quality datasets, covering all sorts of SDN-SG attacks, is the open research area of ML-based SDN-SG security. Secondly, the identity of the attacker is anonymous in response attacks as discussed in Section VII-E. Logging the complete information of such attacks in the datasets is a potential area of research. Here, ML-based classification techniques can learn about the similarities and patterns of the attack traffic to identify the attacker. However, the effectiveness of this proposed research direction can only be verified by experimentation.

2) Minimizing the Training Period: ML algorithms operate in a cognitive cycle by observing, processing, implementing, and improving the results. The training period decides the efficiency of ML techniques. Greater the training time period, the greater is the chance to improve results, and thus more efficient are the results. But, here in SDN-SG, traffic is time-sensitive and cannot bear such delays caused by the training periods. If priority is given to time-sensitive traffic over the training period, then it will result in compromised efficiency of the ML algorithm, due to lack of training. Plenty of time which later was consumed in the appropriate selection has been improved [285], but selecting the appropriate precision of the feature is challenging. Suppose that SDN-SG underwent a flooding attack. Then is it sufficient to distinguish among various type of flooding or further precision regarding the source, attack pattern, and duration of attack also needs to be considered? However, more precision demands more training time and similarly, less training can produce under fitted results with minimal precision. The challenging factor here to achieve a trade-off between the training period, ML algorithm precision, and the time-sensitive traffic of SDN-SG to enable ML-based SDN-SG security. Another issue related to training phase is the human interpretation of evidence and justifications for classification and clustering performed by ML that is necessary for decisions in policymaking and also built trust in ML algorithms.

3) Hybrid ML Solutions: Section VII-G elaborated the use of unsupervised learning [279], deep learning [281], and reinforcement learning [176] for SDN-SG security, but supervised learning and hybrid solutions leveraging benefits of multiple ML techniques is still unaddressed in the literature. Like, supervised ML is an efficient solution for already known attacks, while unsupervised and reinforcement ML can be utilised to deal with the unknown attacks that might occur in the future. Hybrid ML techniques have great potential to further complement the resilience of SDN-SG.

Availability of labelled data for training is limited in SDN-SG systems [286]. ML classification techniques can be utilised here to predict attacks, but this application is also not without challenges. First, there is a need to rely mostly on contextual information due to the unavailability of labelled data. Secondly, SDN-SG is a consumer-oriented utility with the requirement to handle an enormous amount of data, so efficient feature extraction technique need to deploy for extraction of useful information out of this bulk information. Thirdly, the degree of change and evolution is quite high in SDN-SG. A prediction model that is applicable for one time, becomes obsolete for the future. Research efforts for hybrid ML-based security solutions that can utilise supervised learning for labelled data and meanwhile also leverage unsupervised learning with efficient classification and deep learning-based robust feature extraction capabilities could be a great contribution to SDN-SG security.

4) Differentiating Abnormal and Attack Conditions: SDN-SG is a consumer-oriented utility whose operational dynamics are determined by the behaviours of the end consumers. There is a possibility that sudden rise/fall of power demand occur in SDN-SG and get misinterpreted as an attack on the generating stations or on consumption premises. Furthermore, cyber-attacks also need to be distinguished from electric failure, as they follow overlapping trends – DoS energy to consumers. Here, ML can be utilised here to differentiate abnormal and attack conditions. But, ML algorithm is required with the training of power profiles of generation, demand, and power flows of normal, abnormal, and faulty conditions of the SG of recent years. Power profiles of how many recent years are sufficient to achieve

efficient results? It is an open research question. Moreover, SG underwent changes on even hourly basis, so the power profiles also need to be updated in realtime. Concept of ML-based continuous learning can satisfactorily address both the factors and can be a contribution to the research community.

D. Other Issues and Research Directions

1) Simulators/Emulators for SDN-SG: In Section III-C3, we have surveyed various simulators/emulators that have been employed for SDN-SG. All tools are merging the EG simulators with communication simulators such as MATLAB with NS-3 or Mininet [11], [94], [104]. There are lots of issues in using these incorporated testbeds such as synchronising the power and communication simulators/emulators in realtime. Furthermore, when simulator and emulator pair of power and communication testbeds is utilised, here a difference in execution occurs as emulator use realtime system clock, while simulators depend upon the simulation virtual clock [107].

There are two simulators as Distribution System Solver network (DSSnet) [107] and SDN4SmartGrids [179] that has the built-in support for both the power and communication aspects of SDN-SG. Although, there are lots of testbeds for simulation studies of SDN [287] and SG [288], but SDN-SG specific testbed is still an open research area. A dedicated simulator/emulator with embedded power and communication components to synchronise the executions using the realtime system clock can produce more practical results to analysing attack trends and proposing associated mitigation techniques.

2) Integration of trust in SDN-SG: Trust is a context-dependent procedure with a unique trust evaluation mechanism specific to the application [289]. In the context of SDN-SG, trust is subject to the degree of security and privacy system have. Challenges related to security have been surveyed and elaborated in detail in the article, but what about privacy? SDN-SG is a consumer-oriented utility that logs the power usage patterns of residential colonies to implement SG services like demand-response and time of use pricing. This power usage pattern logging at an individual can greatly supplement the efficiency of these SG services, but meanwhile, it also raises privacy concerns. How this concern of data privacy can be resolved in SDN-

SG? Furthermore, to evaluate the overall trust offered by any particular technique, what could be various trust metrics required to be evaluated? In the literature, there is a lot of work to integrate trust in SDN [290]–[292], but SDN application to SG has now changed context. Do the trust models for enterprise SDN can work for SDN-SG?

There are plenty of privacy techniques available in the literature such as authors in article [293] have surveyed 50 privacy techniques. Differential Privacy (DP) is one of these techniques that protects personal sensitive data with the convolution of certain calculated noise in the data [294]. Application DP in SDN-SG has the potential to guarantee the trust to the consumer to share the requisite information required for the operations of SDN-SG services, while withholding the identity of SDN-SG elements. Talking about the application of any particular trust enabling technique, blockchain has a potential scope in contrast to its counterparts such as Steganographic and water marking methods. To evaluate the efficacy of trust achieved with blockchain, common trust metrics used in trust models like integrity, truthfulness, benevolence, ability, and collaborativeness can be utilised. Moreover, these trust aspects can also further extended to check the effectiveness of enterprise SDN trust models for SDN-SG.

DP is ensuring the requisite privacy in SDN-SG, but its implementation demands for the consensus among the consumers and the electric utility for the type of information that need to be shared. Furthermore, more detailed information is required for better efficiency of SDN-SG applications, but it can also reveal consumer usage patterns. Developing a mechanism to ensure this consensus and also to achieve a tradeoff between privacy and efficiency and can be studied as a future research direction. Focusing on the second identified issue of trust, blockchain was proposed. In the blockchain, to register any change in the database, it can take 10-15 minutes, while in SDN-SG, availability is the most desired feature. It means blockchain can provide privacy in SDN-SG at the cost of availability. Is this a worthwhile tradeoff or not? Furthermore, SDN-SG is a consumer-oriented utility that needs to be scalable, while blockchain is reluctant to scalability. Moreover, blockchain is desired for decentralisation, while in SDN-SG, all operations are

streamlined by a regulatory authority. Although private blockchain can provide centralised control, but considering the radius of SDN-SG, is such a gigantic private ledger of blockchain is feasible or not? If it is not feasible, then is the decentralisation of certain SDN-SG operations for the sake of security is a sound solution or not? These are some research questions that demand further evaluation. Regarding the third issue of trust metrics, the researcher can focus to provide a mathematical model to quantify the specified trust metrics in the context of SDN-SG.

3) Standardisation for SDN-SG: Standardisation is the way to ensure the standard use of procedures all over the globe. This allows us to develop a consensus over established practices. Security methods that have global applicability can be developed for the accepted standard procedures. As SDN-SG is an emerging field, so it lacks standardisation. But some of the existing standards of SG has been extended for their application in SDN-SG such as IEC 61850 for substation communication [179], [179], [183], ETSI OSGP for smart meters [295], and IEEE 802.15.4g for NAN communication in SDN-SG.

Without standards, it is very much challenging to synchronise the research activities in SDN-SG. Each researcher has to develop its algorithm of extending existing standards for SDN-SG. This restricts all the research to be on the same page. Development of standards for SDN-SG can complement its operations and also provides an accepted and standard platform for the research and development that has worldwide applicability. Furthermore, when the researchers have consensus over the standard back-end procedures, then it can assist in the development of desired security measures to secure the SDN-SG against cyberattacks. Achieving standardisation in SDN-SG is not without challenges like the deadlocks over consensus on a particular standard among research groups and industries R&D working on SDN-SG. Formation of a consortium with the coverage of all academic and industrial research groups can help in the agreement on commonly recognised standards.

4) QoE for CANs in SDN-SG: CAN is a region of SDN-SG that constitutes the maximum number of participants in the form of electric energy consumers. The Attack surface for cyberattacks and the potential

of intruders to launch attacks is at maximum in these regions. There might be a possibility that SDN-SG is under attack, but attack mitigation could not detect it. But, this attack will affect the energy output of the SDN-SG that can easily be realised by the consumers as a shortfall in energy. The inclusion of consumers by introducing the factor of QoE in the attack mitigation system can greatly complement its attack detecting capability. QoE is defined as the *degree of consumer satisfaction with service*. What QoE factors are required to be included? How these QoE will be conveyed to the SG control centre in realtime? How these QoE can be integrated into the attack mitigation algorithm? These are questions that need to be addressed in further future studies.

5) Effective Capacity for Time-Critical Traffic in SDN-SG: Communication among the remote premises of SDN-SG is performed wirelessly, but the communication within the substations and control centre can be wired. In both cases, delivery of control information, that is time-critical and latency craving in nature, needs to guarantee by mitigating possible delays. As discussed in Section VII-E2, delays in time-critical traffic might affect other SG equipment and also the end customer has to face DoS energy – igniting cascading failures; a major security threat.

To mitigate delays, first, these delays are required to be assessed. Evaluation of the delay performance of such critical traffic can be carried out by many tools such as effective capacity (EC), effective bandwidth, meta distribution, extreme value theorem. EC is the link-layer modelling of a channel to match and maximise the QoS metrics of the source rate to the given service rate; ensuring a constant rate for the wireless channel without delays [296]. The concept of EC can be utilised to keep the check on latency for the timely delivery of critical traffic of SDN-SG.

In case of any new request, SDN-SG switches transfer it to SDN controller and wait till that request is the process and associated flow rules are installed. What if the new request is followed delay-sensitive traffic? From a careful review of the literature, we have realised such delays are a routine activity in SDN architectures, and EC has a great potential to evaluate the delay performance of traffic under such circumstances.

IX. CONCLUSION

The evolving SDN-SG has enabled the programmable communication layer of SG aiming to enable various network applications to further enhance the efficiency of SDN-SG. This critical infrastructure is the potential host for intruders. In this survey article, we have highlighted the need for threat assessment of SDN-SG to explore the vulnerabilities that can be exploited by the attackers. Threat assessment models and their applications for SDN are provided. We have presented the security requirements of the SDN-SG threat assessment model. One of the known vulnerability is the DoS attack that blocks legit users. Various categories of DoS attacks and associated mitigation techniques are surveyed in the context of SDN, and also their adaptability for SDN-SG is evaluated. Multiple DoS attacks are still unaddressed in the literature for SDN-SG. One of the severe DoS attacks, saturation attack, is neither analysed nor any mitigation technique is proposed. This is an open area of research in SDN-SG. Attack mitigation techniques that can detect and mitigate these attacks will enable the researchers to further secure SDN-SG. ML-based solutions are highly favourable for SDN-SG, as they can detect both the known and unknown attack vectors using learning techniques. ML-based attack mitigation solutions are investigated in this survey article for SDN, SG, and SDN-SG. In the literature, there is not sufficient research in this domain for SDN-SG; an open research area.

REFERENCES

- [1] N. Evans and W. Horsthemke, "Regional critical infrastructure," in *Cyber Resilience of Systems and Networks*, pp. 355–380, Springer, 2019.
- [2] P. Regulagadda, I. Dincer, and G. Naterer, "Exergy analysis of a thermal power plant with measured boiler and turbine losses," *Applied Thermal Engineering*, vol. 30, no. 8-9, pp. 970–976, 2010.
- [3] R. Morello, S. C. Mukhopadhyay, Z. Liu, D. Slomovitz, and S. R. Samantaray, "Advances on sensing technologies for smart cities and power grids: A review," *IEEE Sensors Journal*, vol. 17, no. 23, pp. 7596–7610, 2017.
- [4] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid: The new and improved power grid: A survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.
- [5] K. De Craemer and G. Deconinck, "Analysis of state-of-the-art smart metering communication standards," in *Proceedings of the 5th young researchers symposium*, 2010.
- [6] A. A. Khan, M. H. Rehmani, and M. Reisslein, "Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 860–898, 2015.
- [7] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks*, vol. 55, no. 15, pp. 3604 – 3629, 2011.
- [8] H. Lin, C. Chen, J. Wang, J. Qi, D. Jin, Z. T. Kalbarczyk, and R. K. Iyer, "Self-healing attack-resilient PMU network for power system operation," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1551–1565, 2016.
- [9] W. Meng, R. Ma, and H. H. Chen, "Smart grid neighborhood area networks: a survey," *IEEE Network*, vol. 28, no. 1, pp. 24–32, 2014.
- [10] K. H. Chang, "Interoperable nan standards: a path to cost-effective smart grid solutions," *IEEE Wireless Communications*, vol. 20, no. 3, pp. 4–5, 2013.
- [11] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software defined networks-based smart grid communication: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2637–2670, 2019.
- [12] D. B. Rawat and S. R. Reddy, "Software defined networking architecture, security and energy efficiency: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 325–346, 2016.
- [13] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 355–379, 2011.
- [14] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications*

- Surveys & Tutorials, vol. 14, no. 4, pp. 998–1010, 2012.
- [15] W. Wang and Z. Lu, “Cyber security in the smart grid: Survey and challenges,” *Computer networks*, vol. 57, no. 5, pp. 1344–1371, 2013.
- [16] N. Komninos, E. Philippou, and A. Pitsillides, “Survey in smart grid and smart home security: Issues, challenges and countermeasures,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.
- [17] Q. Yan, F. R. Yu, Q. Gong, and J. Li, “Software-defined networking (sdn) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges,” *IEEE communications surveys & tutorials*, vol. 18, no. 1, pp. 602–622, 2015.
- [18] S. Scott-Hayward, S. Natarajan, and S. Sezer, “A survey of security in software defined networks,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 623–654, 2015.
- [19] S. T. Ali, V. Sivaraman, A. Radford, and S. Jha, “A survey of securing networks using software defined networking,” *IEEE transactions on reliability*, vol. 64, no. 3, pp. 1086–1097, 2015.
- [20] R. Mahmud, R. Vallakati, A. Mukherjee, P. Ranganathan, and A. Ne-jadpak, “A survey on smart grid metering infrastructures: Threats and solutions,” in *IEEE International Conference on Electro/Information Technology (EIT)*, pp. 386–391, 2015.
- [21] L. Langer and M. Kammerstetter, “The evolution of the smart grid threat landscape and cross-domain risk assessment,” in *Smart Grid Security*, pp. 49–77, Elsevier, 2015.
- [22] Y. Kabalci, “A survey on smart metering and smart grid communication,” *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 302–318, 2016.
- [23] A. S. Thyagaturu, A. Mercian, M. P. McGarry, M. Reisslein, and W. Kellerer, “Software defined optical networks (SDONs): A comprehensive survey,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2738–2786, 2016.
- [24] H. He and J. Yan, “Cyber-physical attacks and defences in the smart grid: a survey,” *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.
- [25] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, “A survey on software-defined wireless sensor networks: Challenges and design requirements,” *IEEE access*, vol. 5, pp. 1872–1899, 2017.
- [26] P. C. da Rocha Fonseca and E. S. Mota, “A survey on fault management in software-defined networks,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2284–2321, 2017.
- [27] R. Alvizu, G. Maier, N. Kukreja, A. Pattavina, R. Morro, A. Capello, and C. Cavazzoni, “Comprehensive survey on T-SDN: Software-defined networking for transport networks,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2232–2283, 2017.
- [28] T. Dargahi, A. Caponi, M. Ambrosin, G. Bianchi, and M. Conti, “A survey on the security of stateful SDN data planes,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1701–1725, 2017.
- [29] J. H. Cox, J. Chung, S. Donovan, J. Ivey, R. J. Clark, G. Riley, and H. L. Owen, “Advancing software-defined networks: A survey,” *IEEE Access*, vol. 5, pp. 25487–25526, 2017.
- [30] A. Abdou, P. C. Van Oorschot, and T. Wan, “Comparative analysis of control plane security of SDN and conventional networks,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3542–3559, 2018.
- [31] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, C. Wang, and Y. Liu, “A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 393–430, 2018.
- [32] R. Amin, M. Reisslein, and N. Shah, “Hybrid SDN networks: A survey of existing approaches,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3259–3306, 2018.
- [33] I. Stelliou, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, “A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.
- [34] S. Wang, J. Wu, W. Yang, and L.-h. Guo, “Novel architectures and security solutions of

- programmable software-defined networking: a comprehensive survey,” *Frontiers of Information Technology & Elec-tronic Engineering*, vol. 19, no. 12, pp. 1500–1521, 2018.
- [35] B. K. Tripathy, D. P. Das, S. K. Jena, and P. Bera, “Risk based security enforcement in software defined network,” *Computers & Security*, vol. 78, pp. 321–335, 2018.
- [36] Y. Wadhawan, A. AlMajali, and C. Neuman, “A comprehensive anal-ysis of smart grid systems against cyber-physical attacks,” *Electronics*, vol. 7, no. 10, p. 249, 2018.
- [37] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, “Cyber-security in smart grid: Survey and challenges,” *Computers & Electrical Engineering*, vol. 67, pp. 469–482, 2018.
- [38] P. B. Pajila and E. G. Julie, “Detection of DDoS attack using SDN in IoT: A survey,” in *Intelligent Communication Technologies and Virtual Mobile Networks*, pp. 438–452, Springer, 2019.
- [39] S. Dong, K. Abbas, and R. Jain, “A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments,” *IEEE Access*, vol. 7, pp. 80813–80828, 2019.
- [40] Y. Liu, B. Zhao, P. Zhao, P. Fan, and H. Liu, “A survey: Typical se-curity issues of software-defined networking,” *China Communications*, vol. 16, no. 7, pp. 13–31, 2019.
- [41] Y. Zhao, Y. Li, X. Zhang, G. Geng, W. Zhang, and Y. Sun, “A survey of networking applications applying the software defined networking concept based on machine learning,” *IEEE Access*, vol. 7, pp. 95385–95405, 2019.
- [42] A. Mubarakali and A. S. Alqahtani, “A survey: Security threats and countermeasures in software defined networking,” in *IEEE 2nd International Conference on Information and Computer Technologies (ICICT)*, pp. 180–185, 2019.
- [43] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, “Survey on sdn based network intrusion detection system using machine learning approaches,” *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, pp. 493–501, 2019.
- [44] R. Sahay, W. Meng, and C. D. Jensen, “The application of software defined networking on securing computer networks: A survey,” *Journal of Network and Computer Applications*, vol. 131, pp. 89–108, 2019.
- [45] S. Saraswat, V. Agarwal, H. P. Gupta, R. Mishra, A. Gupta, and T. Dutta, “Challenges and solutions in software defined networking: A survey,” *Journal of Network and Computer Applications*, vol. 141, pp. 23–58, 2019.
- [46] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, “Smart grid metering networks: A survey on security, privacy and open research issues,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2886–2927, 2019.
- [47] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, “A survey on security communication and control for smart grids under malicious cyber at-tacks,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1554–1569, 2019.
- [48] T. Han, S. R. U. Jan, Z. Tan, M. Usman, M. A. Jan, R. Khan, and Y. Xu, “A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers,” *Concurrency and Computation: Practice and Experience*, p. e5300, 2019.
- [49] S. Marksteiner, H. Vallant, and K. Nahrgang, “Cyber security require-ments engineering for low-voltage distribution smart grid architectures using threat modeling,” *Journal of Information Security and Applica-tions*, vol. 49, p. 102389, 2019.
- [50] K. S. Sahoo, S. K. Panda, S. Sahoo, B. Sahoo, and R. Dash, “Toward secure software-defined networks against distributed denial of service attack,” *The Journal of Supercomputing*, vol. 75, no. 8, pp. 4829–4874, 2019.
- [51] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, and G. Srivastava, “Security aspects of internet of things aided smart grids: A bibliometric survey,” *Internet of things*, p. 100111, 2019.
- [52] J. McCoy and D. B. Rawat, “Software-defined networking for un-manned aerial vehicular networking and security: A survey,” *Electronics*, vol. 8, no. 12, p. 1468, 2019.

- [53] J. A. Herrera and J. E. Camargo, "A survey on machine learning applications for software defined network security," in *International Conference on Applied Cryptography and Network Security*, pp. 70–93, Springer, 2019.
- [54] V. Lamba, N. Šimková, and B. Rossi, "Recommendations for smart grid security risk management," *Cyber-Physical Systems*, vol. 5, no. 2, pp. 92–118, 2019.
- [55] T. Alharbi, "Deployment of blockchain technology in software defined networks: A survey," *IEEE Access*, vol. 8, pp. 9146–9156, 2020.
- [56] J. C. C. Chica, J. C. Imbachi, and J. F. Botero, "Security in sdn: A comprehensive survey," *Journal of Network and Computer Applications*, p. 102595, 2020.
- [57] S. Lee, J. Kim, S. Woo, C. Yoon, S. Scott-Hayward, V. Yegneswaran, P. Porras, and S. Shin, "A comprehensive security assessment frame-work for software-defined networks," *Computers & Security*, vol. 91, p. 101720, 2020.
- [58] W. B. Jaballah, M. Conti, and C. Lal, "Security and design requirements for software-defined vanets," *Computer Networks*, p. 107099, 2020.
- [59] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks*, vol. 169, p. 107094, 2020.
- [60] M. Mateski, C. M. Trevino, C. K. Veitch, J. Michalski, J. M. Harris, S. Maruoka, and J. Frye, "Cyber threat metrics," *Sandia National Laboratories*, 2012.
- [61] H. Maziku, S. Shetty, and D. M. Nicol, "Security risk assessment for SDN-enabled smart grids," *Computer Communications*, vol. 133, pp. 1–11, 2019.
- [62] R. Khan, K. McLaughlin, D. Lavery, and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," in *IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pp. 1–6, 2017.
- [63] H. Attila, P. M. Erdo'si, and F. Kiss, "The Common Vulnerability Scoring System (CVSS) generations – usefulness and deficiencies," pp. 137–153, 2016.
- [64] B. Schneier, "Attack trees," *Dr. Dobb's journal*, vol. 24, no. 12, pp. 21–29, 1999.
- [65] Z. Fan, Y. Xiao, A. Nayak, and C. Tan, "An improved network security situation assessment approach in software defined networks," *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, pp. 295–309, 2019.
- [66] M. Latah and L. Toker, "A novel intelligent approach for detecting DoS flooding attacks in software-defined networks," *International Journal of Advances in Intelligent Informatics*, vol. 4, no. 1, pp. 11–20, 2018.
- [67] H. Wang, L. Xu, and G. Gu, "Floodguard: a dos attack prevention extension in software-defined networks," in *IEEE International Conference on Dependable Systems and Networks*, pp. 239–250, 2015.
- [68] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397–422, 2017.
- [69] C. Sulzberger, "Thomas edison's 1882 pearl street generating station," *IEEE Global History Network*, 2010.
- [70] S. K. Guttikunda and P. Jawahar, "Atmospheric emissions and pollution from the coal-fired thermal power plants in india," *Atmospheric Environment*, vol. 92, pp. 449–460, 2014.
- [71] A. K. Chen, Y. N. Velaga, and P. K. P. Sen, "Future electric power grid and battery storage," in *IEEE Texas Power and Energy Conference (TPEC)*, pp. 1–6, 2019.
- [72] M. R. Hossain, A. M. T. Oo, and A. S. Ali, "Evolution of smart grid and some pertinent issues," in *IEEE Australasian Universities Power Engineering Conference*, pp. 1–6, 2010.
- [73] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in Smart Grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.
- [74] Z. Fan, R. J. Haines, and P. Kulkarni, "M2M communications for e-health and smart grid: An industry and standard perspective," *IEEE Wireless Communications*, vol. 21, no. 1, pp. 62–69, 2014.
- [75] M. L. Tuballa and M. L. Abundo, "A review of

- the development of smart grid technologies,” *Renewable and Sustainable Energy Reviews*, vol. 59, pp. 710–725, 2016.
- [76] A. Yazdani, Y. Hu, A. Johnson, and D. Martinez, “Deployment of smart grid ideas - what needs enhancement?,” *IEEE Power and Energy Magazine*, vol. 10, no. 2, pp. 108–115, 2012.
- [77] E. Fadel, V. Gungor, L. Nassef, N. Akkari, M. A. Malik, S. Almasri, and I. F. Akyildiz, “A survey on wireless sensor networks for smart grid,” *Computer Communications*, vol. 71, pp. 22 – 33, 2015.
- [78] J. Pan, R. Jain, and S. Paul, “A survey of energy efficiency in buildings and microgrids using networking technologies,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1709–1731, 2014.
- [79] C. Greer, D. A. Wollman, D. E. Prochaska, P. A. Boynton, J. A. Mazer, C. T. Nguyen, G. J. FitzPatrick, T. L. Nelson, G. H. Koepke, A. R. Hefner Jr, et al., “Nist framework and roadmap for smart grid interoperability standards, release 3.0,” tech. rep., National Institute of Standards and Technology, 2014.
- [80] A. B. Birchfield, T. J. Overbye, and K. R. Davis, “Educational applications of large synthetic power grids,” *IEEE Transactions on Power Systems*, vol. 34, no. 1, pp. 765–772, 2018.
- [81] J. Lopez, J. E. Rubio, and C. Alcaraz, “A resilient architecture for the smart grid,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3745–3753, 2018.
- [82] A. Abdrabou, “A wireless communication architecture for smart grid distribution networks,” *IEEE Systems journal*, vol. 10, no. 1, pp. 251–261, 2014.
- [83] S. Samtani, S. Yu, H. Zhu, M. Patton, J. Matherly, and H. Chen, “Identifying SCADA systems and their vulnerabilities on the internet of things: A text-mining approach,” *IEEE Intelligent Systems*, vol. 33, no. 2, pp. 63–73, 2018.
- [84] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, and A. Mohammadi-Nodooshan, “A novel identity-based key establishment method for advanced metering infrastructure in smart grid,” *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2834–2842, 2016.
- [85] F. Elghitani and E. El-Saadany, “Smoothing net load demand variations using residential demand management,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 390–398, 2018.
- [86] C. M. Martinez, X. Hu, D. Cao, E. Velenis, B. Gao, and M. Wellers, “Energy management in plug-in hybrid electric vehicles: Recent progress and a connected vehicles perspective,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 4534–4549, 2016.
- [87] W. Tushar, B. Chai, C. Yuen, S. Huang, D. B. Smith, H. V. Poor, and Z. Yang, “Energy storage sharing in smart grid: A modified auction-based approach,” *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1462–1475, 2016.
- [88] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki, “Networked microgrids for enhancing the power system resilience,” *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1289–1310, 2017.
- [89] C. Vartanian, R. Bauer, L. Casey, C. Loutan, D. Narang, and V. Patel, “Ensuring system reliability: Distributed energy resources and bulk power system considerations,” *IEEE Power and Energy Magazine*, vol. 16, no. 6, pp. 52–63, 2018.
- [90] J. Zhang, B.-C. Seet, T.-T. Lie, and C. H. Foh, “Opportunities for software-defined networking in smart grid,” in *IEEE International Conference on Information, Communications & Signal Processing*, pp. 1–5, 2013.
- [91] N. Kumar and D. P. Vidyarthi, “A green routing algorithm for IoT-enabled software defined wireless sensor network,” *IEEE Sensors Journal*, vol. 18, no. 22, pp. 9449–9460, 2018.
- [92] M. Parashar, A. Poonia, and K. Satish, “A survey of attacks and their mitigations in software defined networks,” in *IEEE International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–8, 2019.
- [93] A. Sydney, J. Nutaro, C. Scoglio, D. Gruenbacher, and N. Schulz, “Simulative

- comparison of multiprotocol label switching and openflow network technologies for transmission operations,” *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 763–770, 2013.
- [94] A. Aydeger, K. Akkaya, and A. S. Uluagac, “SDN-based resilience for smart grid communications,” in *IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN)*, pp. 31–33, 2015.
- [95] U. Ghosh, P. Chatterjee, S. Shetty, C. Kamhoua, and L. Njilla, *Towards secure software-defined networking integrated cyber-physical systems: Attacks and countermeasures*. Boca Raton: CRC Press, 1 ed., 2019.
- [96] M. Cokic and I. Seskar, “Software defined network management for dynamic smart grid traffic,” *Future Generation Computer Systems*, vol. 96, pp. 270–282, 2019.
- [97] N. Dorsch, F. Kurtz, F. Girke, and C. Wietfeld, “Enhanced fast failover for software-defined smart grid communication networks,” in *IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2016.
- [98] J. Peebles and A. Zare, “Toward resilient smart grid communications using distributed SDN with ML-based anomaly detection,” in *Wired/Wireless Internet Communications (WWIC)*, vol. 10866, p. 83, Springer, 2018.
- [99] J. Kim, F. Filali, and Y.-B. Ko, “Trends and potentials of the smart grid infrastructure: From ict sub-system to SDN-enabled smart grid architecture,” *Applied Sciences*, vol. 5, no. 4, pp. 706–727, 2015.
- [100] M. Alishahi, M. H. Y. Moghaddam, and H. R. Pourreza, “Multi-class routing protocol using virtualization and SDN-enabled architecture for smart grid,” *Peer-to-Peer Networking and Applications*, vol. 11, no. 3, pp. 380–396, 2018.
- [101] D. A. Chekired, L. Khoukhi, and H. T. Mouftah, “Decentralized cloud-sdn architecture in smart grid: A dynamic pricing model,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 3, pp. 1220–1231, 2017.
- [102] T. Ubale and A. K. Jain, “Survey on DDoS attack techniques and solutions in software-defined network,” in *Handbook of Computer Networks and Cyber Security*, pp. 389–419, Springer, 2020.
- [103] N. Dorsch, F. Kurtz, and C. Wietfeld, “On the economic benefits of software-defined networking and network slicing for smart grid communications,” *NETNOMICS: Economic Research and Electronic Networking*, vol. 19, no. 1-2, pp. 1–30, 2018.
- [104] Z. Pan, Q. Xu, C. Chen, and X. Guan, “NS3-matlab co-simulator for cyber-physical systems in smart grid,” in *IEEE Chinese Control Conference (CCC)*, pp. 9831–9836, 2016.
- [105] R. A. Niazi and Y. Faheem, “A bayesian game-theoretic intrusion detection system for hypervisor-based software defined networks in smart grids,” *IEEE Access*, vol. 7, pp. 88656–88672, 2019.
- [106] K. Mets, T. Verschueren, C. Develder, T. L. Vandoorn, and L. Vande-velde, “Integrated simulation of power and communication networks for smart grid applications,” in *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pp. 61–65, 2011.
- [107] C. Hannon, J. Yan, and D. Jin, “DSSnet: A smart grid modeling platform combining electrical power distribution system simulation and software defined networking emulation,” in *ACM SIGSIM conference on principles of advanced discrete simulation*, pp. 131–142, 2016.
- [108] S. Dalhues, L. Robitzky, U. Häger, N. Dorsch, F. Kurtz, and C. Wietfeld, “Analysis of real-time coordination of distributed power flow controllers using software-defined networking communication,” in *IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pp. 1–5, 2018.
- [109] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, “Threat modeling-uncover security design flaws using the stride approach,” *MSDN Magazine-Louisville*, pp. 68–75, 2006.
- [110] J. Cleland-Huang, “How well do you know your personae non gratae?,” *IEEE software*, vol. 31, no. 4, pp. 28–31, 2014.
- [111] D. Wichers, “Owasp top-10 2013,” *OWASP Foundation*, February, 2013.
- [112] T. Denning, B. Friedman, and T. Kohno, “The security cards: A security threat brainstorming

- toolkit,” Univ. of Washington, <http://securitycards.cs.washington.edu>, 2013.
- [113] J. Hizver, “Taxonomic modeling of security threats in software defined networking,” in BlackHat Conference, pp. 1–16, 2015.
- [114] J. M. Dover, “A denial of service attack against the open Floodlight SDN controller,” Dover Networks, Tech. Rep., 2013.
- [115] J. M. Dover, “A switch table vulnerability in the open floodlight SDN controller,” Relatório técnico, 2014.
- [116] K. Benton, L. J. Camp, and C. Small, “OpenFlow vulnerability assessment,” in ACM SIGCOMM workshop on Hot topics in software defined networking, pp. 151–152, 2013.
- [117] N. R. Mead, F. Shull, K. Vemuru, and O. Villadsen, “A hybrid threat modeling method,” Carnegie Mellon University-Software Engineering Institute-Technical Report-CMU/SEI-2018-TN-002, 2018.
- [118] M. Howard and D. LeBlanc, “STB online, and SBO (firme), writing secure code,” 2003.
- [119] P. Saitta, B. Larcom, and M. Eddington, “Trike v. 1 methodology doc-ument [draft],” URL: [http://dymaxion.org/trike/Trike_v1 Methodology Documentdraft. pdf](http://dymaxion.org/trike/Trike_v1_Methodology_Documentdraft.pdf), 2005.
- [120] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, “Introduction to the octave approach,” tech. rep., Carnegie-Mellon Univ Pittsburgh Pa Software Engineering, 2003.
- [121] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, “Introduc-ing octave allegro: Improving the information security risk assessment process,” tech. rep., Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, 2007.
- [122] M. Rosenquist, “Prioritizing information security risks with threat agent risk assessment,” Intel Corporation White Paper, 2009.
- [123] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, “A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements,” Requirements Engineering, vol. 16, no. 1, pp. 3–32, 2011.
- [124] T. UcedaVelez and M. M. Morana, Risk centric threat modeling. Wiley Online Library, 2015.
- [125] M. Niemiec, P. Jaglarz, M. Jekot, P. Cholda, and P. Boryło, “Risk assessment approach to secure northbound interface of SDN networks,” in IEEE International Conference on Computing, Networking and Communications (ICNC), pp. 164–169, 2019.
- [126] C. Zhou, D. Wei, H. Cao, J. Zhang, J. Liu, and Z. Li, “Risk assessment method for host nodes in software defined networking,” in IEEE International Conference on Information Technology in Medicine and Education (ITME), pp. 738–742, 2019.
- [127] T.-H. Nguyen and M. Yoo, “Analysis of link discovery service attacks in SDN controller,” in IEEE International Conference on Information Networking (ICOIN), pp. 259–261, 2017.
- [128] C. Yoon, S. Lee, H. Kang, T. Park, S. Shin, V. Yegneswaran, P. Porras, and G. Gu, “Flow wars: Systemizing the attack surface and defenses in software-defined networks,” IEEE/ACM Transactions on Networking, vol. 25, no. 6, pp. 3514–3530, 2017.
- [129] B. Potteiger, G. Martins, and X. Koutsoukos, “Software and attack centric integrated threat modeling for quantitative risk assessment,” in Proceedings of the Symposium and Bootcamp on the Science of Security, pp. 99–108, 2016.
- [130] A. Jaquith, Security metrics: replacing fear, uncertainty, and doubt. Pearson Education, 2007.
- [131] W. Kaydos, Operational performance measurement: increasing total productivity. CRC press, 1998.
- [132] L. Woodard, C. K. Veitch, S. R. Thomas, and D. P. Duggan, “Catego-rizing threat: building and using a generic threat matrix.,” tech. rep., Sandia National Laboratories, 2007.
- [133] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodol-molky, and S. Uhlig, “Software-defined networking: A comprehensive survey,” Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, 2014.
- [134] L. Yao, P. Dong, T. Zheng, H. Zhang, X. Du, and M. Guizani, “Network security analyzing and modeling based on petri net and attack tree for sdn,” in IEEE International Conference on Computing, Networking and Communications (ICNC), pp. 1–5, 2016.
- [135] D. Z. Baker, H. Liu, and C. Roberts, “Ensuring

- flexibility and security in SDN-based spacecraft communication networks through risk assessment,” in IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1–6, 2019.
- [136] L. M. Almutairi and S. Shetty, “Generalized stochastic petri net model based security risk assessment of software defined networks,” in IEEE Military Communications Conference (MILCOM), pp. 545–550, 2017.
- [137] M. Hajizadeh, T. V. Phan, and T. Bauschert, “Probability analysis of successful cyber attacks in SDN-based networks,” in 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 1–6, IEEE, 2018.
- [138] R. Deb and S. Roy, “Dynamic vulnerability assessments of software-defined networks,” *Innovations in Systems and Software Engineering*, vol. 16, no. 1, pp. 45–51, 2020.
- [139] T. Eom, J. B. Hong, S. An, J. S. Park, and D. S. Kim, “A systematic approach to threat modeling and security analysis for software defined networking,” *IEEE Access*, vol. 7, pp. 137432–137445, 2019.
- [140] A. A. Soares, D. M. Mattos, Y. Lopes, D. S. Medeiros, N. C. Fernandes, and D. C. Muchaluat-Saade, “An efficient authentication mechanism based on software-defined networks for electric vehicles,” in IEEE 28th International Symposium on Industrial Electronics (ISIE), pp. 2471–2476, 2019.
- [141] M. Dhawan, R. Poddar, K. Mahajan, and V. Mann, “SPHINX: detecting security attacks in software-defined networks,” in *Ndss*, vol. 15, pp. 8–11, 2015.
- [142] S. Gao, Z. Li, B. Xiao, and G. Wei, “Security threats in the data plane of software-defined networks,” *IEEE network*, vol. 32, no. 4, pp. 108–113, 2018.
- [143] N. Jehan and A. M. Haneef, “Scalable ethernet architecture using sdn by suppressing broadcast traffic,” in IEEE International Conference on Advances in Computing and Communications (ICACC), pp. 24–27, 2015.
- [144] S. Kumar and S. Tapaswi, “A centralized detection and prevention technique against arp poisoning,” in IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp. 259–264, 2012.
- [145] A. Nehra, M. Tripathi, and M. Gaur, “FICUR: employing SDN programmability to secure arp,” in IEEE Annual Computing and Communication Workshop and Conference (CCWC), pp. 1–8, 2017.
- [146] A. Zaalouk, R. Khondoker, R. Marx, and K. Bayarou, “OrchSec: An orchestrator-based architecture for enhancing network-security using network monitoring and SDN control functions,” in IEEE Network Operations and Management Symposium (NOMS), pp. 1–9, 2014.
- [147] T. Xing, Z. Xiong, D. Huang, and D. Medhi, “SDNIPS: Enabling software-defined networking based intrusion prevention system in clouds,” in IEEE International Conference on Network and Service Management (CNSM) and Workshop, pp. 308–311, 2014.
- [148] L. Schehlmann, S. Abt, and H. Baier, “Blessing or curse? revisiting security aspects of software-defined networking,” in IEEE International Conference on Network and Service Management (CNSM) and Work-shop, pp. 382–387, 2014.
- [149] M. D. Hatagundi and H. Kumaraswamy, “A comprehensive survey on different attacks on SDN and approaches to mitigate,” in IEEE International Conference on Computing Methodologies and Communication (ICCMC), pp. 624–627, 2019.
- [150] N. Dayal and S. Srivastava, “Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN,” in IEEE International Conference on Communication Systems and Networks (COMSNETS), pp. 274–281, 2017.
- [151] S. Shin and G. Gu, “Attacking software-defined networks: A first feasibility study,” in ACM SIGCOMM workshop on Hot topics in software defined networking, pp. 165–166, 2013.
- [152] S. Hong, L. Xu, H. Wang, and G. Gu, “Poisoning network visibility in software-defined networks: New attacks and countermeasures,” in *NDSS*, vol. 15, pp. 8–11, 2015.
- [153] P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B.

- O'Connor, P. Radoslavov, W. Snow, et al., "ONOS: towards an open, distributed SDN OS," in Proceedings of the third workshop on Hot topics in software defined networking, pp. 1–6, 2014.
- [154] J. Medved, R. Varga, A. Tkacik, and K. Gray, "Opendaylight: Towards a model-driven SDN controller architecture," in IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, pp. 1–6, 2014.
- [155] Z. K. Khattak, M. Awais, and A. Iqbal, "Performance evaluation of OpenDaylight SDN controller," in IEEE international conference on parallel and distributed systems (ICPADS), pp. 671–676, 2014.
- [156] F. Tomonori, "Introduction to RYU SDN framework," Open Network-ing Summit, pp. 1–14, 2013.
- [157] B. Jelacic, D. Rosic, I. Lendak, M. Stanojevic, and S. Stoja, "STRIDE to a secure smart grid in a hybrid cloud," in Computer Security, pp. 77–90, Springer, 2017.
- [158] C.-W. Ten, C.-C. Liu, and M. Govindarasu, "Vulnerability assessment of cybersecurity for SCADA systems using attack trees," in IEEE Power Engineering Society General Meeting, pp. 1–8, 2007.
- [159] M. H. Haider, S. B. Saleem, J. Rafiqat, and N. Sabahat, "Threat modeling of wireless attacks on advanced metering infrastructure," in IEEE International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), pp. 1–6, 2019.
- [160] A. Hahn, "Smart grid architecture risk optimization through vulnerability scoring," in IEEE Conference on Innovative Technologies for an Efficient and Reliable Electricity Supply, pp. 36–41, 2010.
- [161] J. Ko, H. Lim, S. Lee, and T. Shon, "AVQS: attack route-based vulnerability quantification scheme for smart grid," The Scientific World Journal, vol. 2014, 2014.
- [162] R. K. Pandey and M. Misra, "Cyber security threats—smart grid infrastructure," in IEEE National Power Systems Conference (NPSC), pp. 1–6, 2016.
- [163] A. Lee and T. Brewer, "Smart grid cyber security strategy and requirements," Draft Interagency Report NISTIR, vol. 7628, 2009.
- [164] D. Yadav, A. R. Mahajan, and A. Thomas, "An ontology for risk analysis in smart grid," International Journal of Computer Science and Information Security, vol. 14, no. 12, p. 371, 2016.
- [165] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," IEEE Transactions on Power Systems, vol. 23, no. 4, pp. 1836–1846, 2008.
- [166] C. Neureiter, G. Eibl, A. Veichtlbauer, and D. Engel, "Towards a framework for engineering smart-grid-specific privacy requirements," in IEEE Conference of the Industrial Electronics Society IECON, pp. 4803–4808, 2013.
- [167] I. S. Razo-Zapata, "A method to assess the economic feasibility of new commercial services in the smart grid," in IEEE Conference on Service-Oriented Computing and Applications (SOCA), pp. 90–97, 2017.
- [168] C. C. Fung, M. A. Roumani, and K. P. Wong, "A proposed study on economic impacts due to cyber attacks in smart grid: A risk based assessment," in 2013 IEEE Power & Energy Society General Meeting, pp. 1–5, IEEE, 2013.
- [169] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 235–244, 2013.
- [170] H. Bao, R. Lu, B. Li, and R. Deng, "BLITHE: Behavior rule-based insider threat detection for smart grid," IEEE Internet of Things Journal, vol. 3, no. 2, pp. 190–205, 2015.
- [171] Y.-T. Chen, "Modeling information security threats for smart grid applications by using software engineering and risk management," in IEEE International Conference on Smart Energy Grid Engineering (SEGE), pp. 128–132, 2018.
- [172] J. Dobaj, "INSpiRA: integrating security into risk assessment: doctoral project paper," in International conference on software engineering for adaptive and self-managing systems, pp. 183–187, 2018.
- [173] A. Hematian, W. Yu, D. Griffith, and N. Golmie, "Performance assessment of smart meter traffic over lte network using sdr

- testbed,” in IEEE International Conference on Computing, Networking and Communications (ICNC), pp. 408–412, 2019.
- [174] I. Özçelik and R. R. Brooks, “Cusum-entropy: an efficient method for DDoS attack detection,” in IEEE International Istanbul Smart Grid Congress and Fair (ICSG), pp. 1–5, 2016.
- [175] H. T. Mouftah and M. Erol-Kantarci, *Smart Grid: Networking, Data Management, and Business Models*. Boca Raton: CRC Press, 1 ed., 2017.
- [176] M. H. Rehmani, F. Akhtar, A. Davy, and B. Jennings, “Achieving resilience in sdn-based smart grid: A multi-armed bandit approach,” in IEEE Conference on Network Softwarization and Workshops (NetSoft), pp. 366–371, 2018.
- [177] S. Wang, J. Wu, S. Zhang, and K. Wang, “SSDS: a smart software-defined security mechanism for vehicle-to-grid using transfer learning,” *IEEE Access*, vol. 6, pp. 63967–63975, 2018.
- [178] D. Ibdah, M. Kanani, N. Lachtar, N. Allan, and B. Al-Duwairi, “On the security of SDN-enabled smartgrid systems,” in IEEE International Conference on Electrical and Computing Technologies and Applications (ICECTA), pp. 1–5, 2017.
- [179] N. Dorsch, F. Kurtz, H. Georg, C. Hägerling, and C. Wietfeld, “Software-defined networking for smart grid communications: Applications, challenges and advantages,” in IEEE International conference on smart grid communications (SmartGridComm), pp. 422–427, 2014.
- [180] F. Kurtz, N. Dorsch, C. Bektas, and C. Wietfeld, “Synchronized measurement concept for failure handling in software-defined smart grid communications,” in IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 1–6, 2017.
- [181] S. Rinaldi, F. Bonafini, P. Ferrari, A. Flammini, E. Sisinni, D. Di Cara, N. Panzavecchia, G. Tinè, A. Cataliotti, V. Cosentino, et al., “Characterization of IP-based communication for smart grid using software-defined networking,” *IEEE Transactions on Instrumentation and Measurement*, vol. 67, no. 10, pp. 2410–2419, 2018.
- [182] S. Zhang, Q. Li, J. Wu, J. Li, and G. Li, “A security mechanism for software-defined networking based communications in vehicle-to-grid,” in IEEE Smart Energy Grid Engineering (SEGE), pp. 386–391, 2016.
- [183] A. Aydeger, K. Akkaya, M. H. Cintuglu, A. S. Uluagac, and O. Mo-hammed, “Software defined networking for resilient communications in smart grid active distribution networks,” in IEEE International Conference on Communications (ICC), pp. 1–6, 2016.
- [184] N. Dorsch, F. Kurtz, S. Dalhues, L. Robitzky, U. Häger, and C. Wietfeld, “Intertwined: Software-defined communication networks for multi-agent system-based smart grid control,” in IEEE international conference on smart grid communications (SmartGridComm), pp. 254–259, 2016.
- [185] A. Irfan, N. Taj, and S. A. Mahmud, “A novel secure SDN/LTE based architecture for smart grid security,” in IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, pp. 762–769, 2015.
- [186] F. Alharbi and Z. Fei, “Improving the quality of service for critical flows in smart grid using software-defined networking,” in IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 237–242, 2016.
- [187] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. Rodrigues, “SDN-enabled multi-attribute-based secure communication for smart grid in iiot environment,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2629–2640, 2018.
- [188] U. Ghosh, P. Chatterjee, and S. Shetty, “A security framework for sdn-enabled smart power grids,” in IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW), pp. 113–118, 2017.
- [189] G. Lin, M. Dong, K. Ota, J. Li, W. Yang, and J. Wu, “Security function virtualization based moving target defense of SDN-enabled smart grid,” in IEEE International Conference on Communications (ICC), pp. 1–6, 2019.

- [190] S. Jitnukulsiri and C. Aswakul, "Validation of SDN emulator based on Mininet and ONOS controller for iec 61850 packet delay measurement," in IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), pp. 113–117, 2019.
- [191] X. Zhang, K. Wei, L. Guo, W. Hou, and J. Wu, "SDN-based resilience solutions for smart grids," in IEEE International Conference on Software Networking (ICSN), pp. 1–5, 2016.
- [192] Y. Sim and H. Y. Lee, "Denial-of-service attack using host location hijacking in software-defined network," in IEEE European Symposium on Security and Privacy (Euro S&P), pp. 1–2, 2016.
- [193] A. M. AbdelSalam, A. B. El-Sisi, and V. Reddy, "Mitigating arp spoofing attacks in software-defined networks," in Proceedings of the International conference on Computer Theory and Applications (ICCTA), 2016.
- [194] D. Smyth, D. O'Shea, V. Cionca, and S. McSweeney, "Attacking distributed software-defined networks by leveraging network state consistency," *Computer Networks*, vol. 156, pp. 9–19, 2019.
- [195] D. Saif, A. Cormier, S. Banik, and A. Matrawy, "A review of recently emerging denial of service threats and defences in the transport layer," in IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), pp. 1–5, 2018.
- [196] S. Singh, R. Khan, and A. Agrawal, "Prevention mechanism for infrastructure based denial-of-service attack over software defined network," in IEEE International Conference on Computing, Communication & Automation, pp. 348–353, 2015.
- [197] R. Durner, C. Lorenz, M. Wiedemann, and W. Kellerer, "Detecting and mitigating denial of service attacks against the data plane in software defined networks," in IEEE Conference on Network Softwarization (NetSoft), pp. 1–6, 2017.
- [198] Z. Li, W. Xing, and D. Xu, "Detecting saturation attacks in software-defined networks," in IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 163–168, 2018.
- [199] Y. Liu, M. Dong, K. Ota, J. Li, and J. Wu, "Deep reinforcement learning based smart mitigation of DDoS flooding in software-defined networks," in IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 1–6, 2018.
- [200] L. Barki, A. Shidling, N. Meti, D. Narayan, and M. M. Mulla, "Detection of distributed denial of service attacks in software defined networks," in IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2576–2581, 2016.
- [201] A. Aydeger, N. Saputro, K. Akkaya, and M. Rahman, "Mitigating crossfire attacks using SDN-based moving target defense," in IEEE Conference on Local Computer Networks (LCN), pp. 627–630, 2016.
- [202] K. Kalkan, G. Gür, and F. Alagöz, "SDNScore: A statistical defense mechanism against DDoS attacks in SDN environment," in IEEE Symposium on Computers and Communications (ISCC), pp. 669–675, 2017.
- [203] R. U. Rasool, U. Ashraf, K. Ahmed, H. Wang, W. Rafique, and Z. Anwar, "Cyberpulse: a machine learning based link flooding attack mitigation system for software defined networks," *IEEE Access*, vol. 7, pp. 34885–34899, 2019.
- [204] R. Mohammadi, M. Conti, C. Lal, and S. C. Kulhari, "SYN-Guard: an effective counter for syn flooding attack in software-defined network-ing," *International Journal of Communication Systems*, vol. 32, no. 17, p. e4061, 2019.
- [205] R. Mohammadi, R. Javidan, and M. Conti, "Slicots: an sdn-based lightweight countermeasure for tcp syn flooding attacks," *IEEE Transactions on Network and Service Management*, vol. 14, no. 2, pp. 487–497, 2017.
- [206] S. Fichera, L. Galluccio, S. C. Grancagnolo, G. Morabito, and S. Palazzo, "OPERETTA: an openflow-based remedy to mitigate tcp synflood attacks against web servers," *Computer Networks*, vol. 92, pp. 89–100, 2015.
- [207] P. Kumar, M. Tripathi, A. Nehra, M. Conti, and C. Lal, "SAFETY: Early detection and

- mitigation of tcp syn flood utilizing entropy in SDN,” *IEEE Transactions on Network and Service Management*, vol. 15, no. 4, pp. 1545–1559, 2018.
- [208] G. Tarnaras, F. Athanasiou, and S. Denazis, “Efficient topology discovery algorithm for software-defined networks,” *IET Networks*, vol. 6, no. 6, pp. 157–161, 2017.
- [209] D. M. F. Mattos and O. C. M. B. Duarte, “AuthFlow: authentication and access control mechanism for software defined networking,” *annals of telecommunications*, vol. 71, no. 11–12, pp. 607–615, 2016.
- [210] R. Nagarathna and S. M. Shalinie, “SLAMHHA: a supervised learning approach to mitigate host location hijacking attack on SDN controllers,” in *IEEE International Conference on Signal Processing, Communication and Networking (ICSCN)*, pp. 1–7, 2017.
- [211] D. C. Plummer et al., “Ethernet address resolution protocol: Or converting network protocol addresses to 48. bit ethernet address for transmission on ethernet hardware,” *RFC*, vol. 826, pp. 1–10, 1982.
- [212] G. Yao, J. Bi, and P. Xiao, “Source address validation solution with openflow/nox architecture,” in *IEEE International Conference on Network Protocols*, pp. 7–12, 2011.
- [213] T. Wang and H. Chen, “SGuard: A lightweight SDN safe-guard architecture for DoS attacks,” *China Communications*, vol. 14, no. 6, pp. 113–125, 2017.
- [214] J. Kwon, D. Seo, M. Kwon, H. Lee, A. Perrig, and H. Kim, “An incrementally deployable anti-spoofing mechanism for software-defined networks,” *Computer Communications*, vol. 64, pp. 1–20, 2015.
- [215] K. S. Sahoo, D. Puthal, M. Tiwary, J. J. Rodrigues, B. Sahoo, and R. Dash, “An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics,” *Future Generation Computer Systems*, vol. 89, pp. 685–697, 2018.
- [216] S. Luo, J. Wu, J. Li, and B. Pei, “A defense mechanism for distributed denial of service attack in software-defined networks,” in *IEEE International Conference on Frontier of Computer Science and Technology*, pp. 325–329, 2015.
- [217] M. Pióro, Á. Szentesi, J. Harmatos, A. Jüttner, P. Gajowniczek, and S. Kozdrowski, “On open shortest path first related network optimisation problems,” *Performance evaluation*, vol. 48, no. 1–4, pp. 201–223, 2002.
- [218] J. R. Yee, “On the internet routing protocol enhanced interior gateway routing protocol: is it optimal?,” *International Transactions in Operational Research*, vol. 13, no. 3, pp. 177–194, 2006.
- [219] B. R. Smith and J. Garcia-Luna-Aceves, “Securing the border gateway routing protocol,” in *IEEE Global Telecommunications Conference*, pp. 81–85, 1996.
- [220] M. Moshref, A. Bhargava, A. Gupta, M. Yu, and R. Govindan, “Flow-level state transition as a new switch primitive for SDN,” in *Proceedings of the third workshop on Hot topics in software defined networking*, pp. 61–66, 2014.
- [221] A. Shaghghi, M. A. Kaafar, and S. Jha, “Wedgetail: an intrusion prevention system for the data plane of software defined networks,” in *ACM Asia Conference on Computer and Communications Security*, pp. 849–861, 2017.
- [222] M. Zhang, J. Bi, J. Bai, and G. Li, “Floodshield: securing the sdn infrastructure against denial-of-service attacks,” in *IEEE International Conference On Trust, Security And Privacy In Computing And Communications*, pp. 687–698, 2018.
- [223] L. Dridi and M. F. Zhani, “SDN-guard: DoS attacks mitigation in SDN networks,” in *IEEE International Conference on Cloud Networking (Cloudnet)*, pp. 212–217, 2016.
- [224] A. F. M. Piedrahita, S. Rueda, D. M. Mattos, and O. C. M. Duarte, “FlowFence: a denial of service defense system for software defined networking,” in *IEEE Global Information Infrastructure and Network-ing Symposium (GIIS)*, pp. 1–6, 2015.
- [225] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, “Avant-guard: scalable and vigilant switch flow management in software-defined networks,” in *ACM SIGSAC conference on Computer & communications security*, pp. 413–424, 2013.

- [226] P. Van Trung, T. T. Huong, D. Van Tuyen, D. M. Duc, N. H. Thanh, and A. Marshall, "A multi-criteria-based DDoS-attack prevention solution using software defined networking," in *IEEE International Conference on Advanced Technologies for Communications (ATC)*, pp. 308–313, 2015.
- [227] S. Zhu, J. Bi, C. Sun, C. Wu, and H. Hu, "Sdpa: enhancing stateful forwarding for software-defined networking," in *IEEE International Conference on Network Protocols (ICNP)*, pp. 323–333, 2015.
- [228] G. Shang, P. Zhe, X. Bin, H. Aiqun, and R. Kui, "FloodDefender: Protecting data and control plane resources under SDN-aimed DoS attacks," in *IEEE Conference on Computer Communications (INFO-COM)*, pp. 1–9, 2017.
- [229] E. Al-Shaer and S. Al-Haj, "FlowChecker: configuration analysis and verification of federated openflow infrastructures," in *Proceedings of the 3rd ACM workshop on Assurable and usable security configuration*, pp. 37–44, 2010.
- [230] A. Khurshid, X. Zou, W. Zhou, M. Caesar, and P. B. Godfrey, "Veriflow: verifying network-wide invariants in real time," in *Presented as part of the 10th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 13)*, pp. 15–27, 2013.
- [231] R. Sherwood, G. Gibb, K.-K. Yap, G. Appenzeller, M. Casado, N. McKeown, and G. Parulkar, "Flowvisor: a network virtualization layer," *OpenFlow Switch Consortium, Tech. Rep.*, vol. 1, p. 132, 2009.
- [232] K. Phemius, M. Bouet, and J. Leguay, "Disco: distributed multi-domain sdn controllers," in *IEEE Network Operations and Management Symposium (NOMS)*, pp. 1–4, 2014.
- [233] T. Ball, N. Bjørner, A. Gember, S. Itzhaky, A. Karbyshev, M. Sagiv, M. Schapira, and A. Valadarsky, "VeriCon: towards verifying controller programs in software-defined networks," in *Proceedings of the 35th ACM SIGPLAN Conference on Programming Language Design and Implementation*, pp. 282–293, 2014.
- [234] A. Nakao and P. Du, "Toward in-network deep machine learning for identifying mobile applications and enabling application specific network slicing," *IEICE Transactions on Communications*, 2018.
- [235] P. Wang, S.-C. Lin, and M. Luo, "A framework for QoS-aware traffic classification using semi-supervised machine learning in SDNs," in *IEEE International Conference on Services Computing (SCC)*, pp. 760–765, 2016.
- [236] A. B. Letaifa, "Adaptive QoE monitoring architecture in SDN net-works: Video streaming services case," in *IEEE International Wire-less Communications and Mobile Computing Conference (IWCMC)*, pp. 1383–1388, 2017.
- [237] L. Yanjun, L. Xiaobo, and Y. Osamu, "Traffic engineering framework with machine learning based meta-layer in software-defined networks," in *IEEE International Conference on Network Infrastructure and Digital Content*, pp. 121–125, 2014.
- [238] Y. He, F. R. Yu, N. Zhao, V. C. Leung, and H. Yin, "Software-defined networks with mobile edge computing and caching for smart cities: A big data deep reinforcement learning approach," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 31–37, 2017.
- [239] T. V. Phan, N. K. Bao, and M. Park, "A novel hybrid flow-based handler with DDoS attacks in software-defined networking," in *IEEE Confer-ences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, pp. 350–357, 2016.
- [240] T. V. Phan, T. Van Toan, D. Van Tuyen, T. T. Huong, and N. H. Thanh, "OpenFlowSIA: An optimized protection scheme for software-defined networks from flooding attacks," in *IEEE Sixth International Conference on Communications and Electronics (ICCE)*, pp. 13–18, 2016.
- [241] P. Wang, K.-M. Chao, H.-C. Lin, W.-H. Lin, and C.-C. Lo, "An efficient flow control approach for SDN-based network threat detection and migration using support vector machine," in *IEEE International Conference on e-Business Engineering (ICEBE)*, pp. 56–63,

- 2016.
- [242] D. Hu, P. Hong, and Y. Chen, "FADM: DDoS flooding attack detection and mitigation system in software-defined networking," in IEEE Global Communications Conference, pp. 1–7, 2017.
- [243] N. Bouacida, A. Alghadhban, S. Alalmaei, H. Mohammed, and B. Shi-hada, "Failure mitigation in software defined networking employing load type prediction," in IEEE International Conference on Communi-cations (ICC), pp. 1–7, 2017.
- [244] B. Leng, L. Huang, C. Qiao, and H. Xu, "A decision-tree-based on-line flow table compressing method in software defined networks," in IEEE/ACM 24th International Symposium on Quality of Service (IWQoS), pp. 1–2, 2016.
- [245] S. Nanda, F. Zafari, C. DeCusatis, E. Wedaa, and B. Yang, "Predicting network attack patterns in SDN using machine learning approach," in IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 167–172, 2016.
- [246] F. Tang, L. Li, L. Barolli, and C. Tang, "An efficient sampling and classification approach for flow detection in sdn-based big data centers," in IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), pp. 1106–1115, 2017.
- [247] Z. Chen, F. Jiang, Y. Cheng, X. Gu, W. Liu, and J. Peng, "XGBoost classifier for ddos attack detection and analysis in SDN-based cloud," in IEEE International Conference on Big Data and Smart Computing (BigComp), pp. 251–256, 2018.
- [248] E. Ivannikova, M. Zolotukhin, and T. Hämäläinen, "Probabilistic transition-based approach for detecting application-layer ddos attacks in encrypted software-defined networks," in International Conference on Network and System Security, pp. 531–543, Springer, 2017.
- [249] M. E. Ahmed, H. Kim, and M. Park, "Mitigating DNS query-based DDoS attacks with machine learning on software-defined networking," in MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), pp. 11–16, IEEE, 2017.
- [250] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in IEEE Local Computer Network Conference, pp. 408–415, 2010.
- [251] T. M. Nam, P. H. Phong, T. D. Khoa, T. T. Huong, P. N. Nam, N. H. Thanh, L. X. Thang, P. A. Tuan, V. D. Loi, et al., "Self-organizing map-based approaches in DDoS flooding detection using SDN," in IEEE International Conference on Information Networking (ICOIN), pp. 249–254, 2018.
- [252] P. MohanaPriya and S. M. Shalinie, "Restricted Boltzmann machine based detection system for DDoS attack in software defined networks," in IEEE Fourth International Conference on Signal Processing, Com-munication and Networking (ICSCN), pp. 1–6, 2017.
- [253] Y. Han, B. I. Rubinstein, T. Abraham, T. Alpcan, O. De Vel, S. Erfani, D. Hubczenko, C. Leckie, and P. Montague, "Reinforcement learning for autonomous defence in software-defined networking," in Interna-tional Conference on Decision and Game Theory for Security, pp. 145–165, Springer, 2018.
- [254] S. Salman, C. Streiffer, H. Chen, T. Benson, and A. Kadav, "DeepConf: Automating data center network topologies management with machine learning," in Proceedings of the 2018 Workshop on Network Meets AI & ML, pp. 8–14, 2018.
- [255] S. Kim, J. Son, A. Talukder, and C. S. Hong, "Congestion prevention mechanism based on Q-leaning for efficient routing in SDN," in IEEE International Conference on Information Networking (ICOIN), pp. 124–128, 2016.
- [256] X. Guo, H. Lin, Z. Li, and M. Peng, "Deep reinforcement learning based QoS-aware secure routing for SDN-IoT," IEEE Internet of Things Journal, 2019.
- [257] R. Kokila, S. T. Selvi, and K. Govindarajan, "DDoS detection and anal-ysis in sdn-based environment using support vector machine classifier," in IEEE International Conference on Advanced Computing (ICoAC), pp. 205–210, 2014.
- [258] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in

- software defined networking,” in IEEE International Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 258–263, 2016.
- [259] C. Li, Y. Wu, X. Yuan, Z. Sun, W. Wang, X. Li, and L. Gong, “Detection and defense of DDoS attack based on deep learning in openflow-based SDN,” *International Journal of Communication Systems*, vol. 31, no. 5, p. e3497, 2018.
- [260] Q. Niyaz, W. Sun, and A. Y. Javaid, “A deep learning based DDoS detection system in software-defined networking (SDN),” *arXiv preprint arXiv:1611.07400*, 2016.
- [261] X.-F. Chen and S.-Z. Yu, “Cipa: A collaborative intrusion prevention architecture for programmable network and sdn,” *Computers & Security*, vol. 58, pp. 1–19, 2016.
- [262] N. Dayal and S. Srivastava, “An RBF-PSO based approach for early detection of DDoS attacks in SDN,” in *IEEE International Conference on Communication Systems & Networks (COMSNETS)*, pp. 17–24, 2018.
- [263] A. Abubakar and B. Pranggono, “Machine learning based intrusion detection system for software defined networks,” in *IEEE International Conference on Emerging Security Technologies (EST)*, pp. 138–143, 2017.
- [264] A. Schmidt, “The estonian cyberattacks,” *A fierce domain: Conflict in cyberspace, 1986 to 2012*, pp. 174–193, 2013.
- [265] “Estonia DDoS.”
<https://www.nytimes.com/2007/05/29/technology/29estonia.html>, 2007.
- [266] N. Hamid, “The british hacker who became the islamic state’s chief terror cyber coach: A profile of junaid husain,” *Combating Terrorism Center*, vol. 11, no. 4, 2018.
- [267] J. Pagliery, “Isis is attacking the u.s. energy grid (and failing).” www.money.cnn.com, 2015.
- [268] “Ukraine power grid DDoS.”
<https://www.bbc.com/news/technology-38573074>, 2015.
- [269] M. Lee, M. J. Assante, and T. Conway, “TLP: White-analysis of the cyber attack on the ukrainian power grid-defense use case,” in *Electricity Information Sharing and Analysis Center (E-ISAC)*, pp. 1–29, 2016.
- [270] Z. K., “Inside the cunning, unprecedented hack of ukraine’s power grid.”
www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-powergrid, 2016.
- [271] D. Park, J. Summers, and M. Walstrom, “Cyberattack on critical infrastructure: Russia and the ukrainian power grid attacks,” *Henry M Jackson School of International Studies*, vol. 11, 2017.
- [272] “Liberia DDoS.”
<https://www.bbc.com/news/technology-37859678>, 2016.
- [273] J. Condliffe, “Ukraines power grid gets hacked again a worrying sign for infrastructure attacks,” *MIT Technol. Rev.*, 2016.
- [274] “DoS attack on saudia arbaia petro-chemical industry.”
<https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html>, 2017.
- [275] “DoS attack on usa power grid.”
<https://www.cnbc.com/2019/05/02/ddos-attack-caused-interruptions-in-power-system-operations-doe.html>, 2019.
- [276] M. Samir, M. Azab, M. R. Rizk, and N. Sadek, “PYGRID: a soft-ware development and assessment framework for grid-aware software defined networking,” *International Journal of Network Management*, vol. 28, no. 5, p. e2033, 2018.
- [277] H. Maziku and S. Shetty, “Software defined networking enabled resilience for IEC 61850-based substation communication systems,” in *IEEE International Conference on Computing, Networking and Communications (ICNC)*, pp. 690–694, 2017.
- [278] U. Ghosh, X. Dong, R. Tan, Z. Kalbarczyk, D. K. Yau, and R. K. Iyer, “A simulation study on smart grid resilience under software-defined networking controller failures,” in *ACM International Workshop on Cyber-Physical System Security*, pp. 52–58, 2016.
- [279] A. Starke, J. McNair, R. Trevizan, A. Bretas, J. Peeples, and A. Zare, “Toward resilient smart grid communications using distributed SDN with ML-based anomaly detection,” in

- International Conference on Wired/Wireless Internet Communication, pp. 83–94, Springer, 2018.
- [280] Z. Lv, L. Wang, Z. Guan, J. Wu, X. Du, H. Zhao, and M. Guizani, “An optimizing and differentially private clustering algorithm for mixed data in SDN-based smart grid,” *IEEE Access*, vol. 7, pp. 45773–45782, 2019.
- [281] L. Reuter, O. Jung, and J. Magin, “Neural network based anomaly detection for SCADA systems,” in *IEEE Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, pp. 194–201, 2020.
- [282] S. Revathi and A. Malathi, “A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection,” *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no. 12, pp. 1848–1853, 2013.
- [283] J.-H. Lee, J.-H. Lee, S.-G. Sohn, J.-H. Ryu, and T.-M. Chung, “Effective value of decision tree with KDD 99 intrusion detection datasets for intrusion detection system,” in *IEEE International Conference on Advanced Communication Technology*, vol. 2, pp. 1170–1175, 2008.
- [284] S. Soheily-Khah, P.-F. Marteau, and N. Béchet, “Intrusion detection in network systems through hybrid supervised and unsupervised machine learning process: A case study on the iscx dataset,” in *IEEE International Conference on Data Intelligence and Security (ICDIS)*, pp. 219–226, 2018.
- [285] J. Cai, J. Luo, S. Wang, and S. Yang, “Feature selection in machine learning: A new perspective,” *Neurocomputing*, vol. 300, pp. 70–79, 2018.
- [286] S. Azad, F. Sabrina, and S. Wasimi, “Transformation of smart grid using machine learning,” in *IEEE Australasian Universities Power Engineering Conference (AUPEC)*, pp. 1–6, 2019.
- [287] T. Huang, F. R. Yu, C. Zhang, J. Liu, J. Zhang, and Y. Liu, “A survey on large-scale software defined networking (SDN) testbeds: Approaches and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 891–917, 2016.
- [288] S. Tan, W.-Z. Song, S. Yothment, J. Yang, and L. Tong, “Scoreplus: A software-hardware hybrid and federated experiment environment for smart grid,” *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 16, no. 1, pp. 1–25, 2016.
- [289] D. Artz and Y. Gil, “A survey of trust in computer science and the semantic web,” *Journal of Web Semantics*, vol. 5, no. 2, pp. 58–71, 2007.
- [290] Z. Yao and Z. Yan, “A trust management framework for software-defined network applications,” *Concurrency and Computation: Practice and Experience*, p. e4518, 2018.
- [291] A. L. Aliyu, P. Bull, and A. Abdallah, “A trust management framework for network applications within an SDN environment,” in *IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pp. 93–98, 2017.
- [292] D. Kreutz, F. M. Ramos, and P. Verissimo, “Towards secure and dependable software-defined networks,” in *ACM SIGCOMM workshop on Hot topics in software defined networking*, pp. 55–60, 2013.
- [293] D. Desfontaines and B. Pejo, “Sok: Differential privacies,” *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, pp. 288–313, 2020.
- [294] C. Dwork, “Differential privacy: A survey of results,” in *International conference on theory and applications of models of computation*, pp. 1–19, Springer, 2008.
- [295] M. Bräuning and R. Khondoker, “Analysis of SDN applications for smart grid infrastructures,” in *SDN and NFV Security*, pp. 99–110, Springer, 2018.
- [296] M. Amjad, L. Musavian, and M. H. Rehmani, “Effective capacity in wireless networks: A comprehensive survey,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3007–3038, 2019.