IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 30, 2020, accepted September 10, 2020, date of publication September 25, 2020, date of current version October 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3026923

A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid

ALVIN HUSEINOVI [1], SA A MRDOVI [1], (Member, IEEE),
KEMAL BICAKCI[2], (Member, IEEE), AND SULEYMAN ULUDAG[3], (Member, IEEE)
[1]Faculty of Electrical Engineering, University of Sarajevo, Sarajevo 71000, Bosnia and Herzegovina
[2]Department of Computer Engineering, TOBB University of Economics and Technology, 06510 Çankaya/Ankara, Turkey
[3]Department of Computer Science, Engineering, and Physics, University of Michigan-Flint, Flint, MI 48502, USA

Corresponding author: Alvin Huseinović (ahuseinovic@etf.unsa.ba)

The work of Suleyman Uludag was supported in part by the Fulbright Core Award under Grant PS00271012.

ABSTRACT The scope, scale, and intensity of real, as well as potential attacks, on the Smart Grid have been increasing and thus gaining more attention. An important component of Smart Grid cybersecurity efforts addresses the *availability* and *access* to the power and related information and communications infrastructures. We overload the term, Denial-of-Service (DoS), to refer to these attacks in the Smart Grid. In this paper, we provide a holistic and methodical presentation of the DoS attack taxonomies as well as a survey of potential solution techniques to help draw a more concerted and coordinated research into this area, lack of which may have profound consequences. To the best of our knowledge, the literature does not have such a comprehensive survey study of the DoS attacks and solutions for the Smart Grid.

INDEX TERMS Denial-of-service attacks, smart grid security, cybersecurity.

I. ACRONYMS

In order to make the paper more clear and easier to read, we provide a table of acronyms in Table 1.

II. INTRODUCTION

Many utilities worldwide have embarked on a transformational process to enhance the over-a-century-old power grid under an overall term of the Smart Grid (SG) [1]–[4]. Worldwide SG value is expected to more than double from $15 billion in 2017 to $35 billion by the year 2023, as shown in Figure 1.

The immense SG upgrade involves integration of a variety of digital computing, communications and industrial control systems and technologies into a modernized and advanced power grid of the future. A key element of the SG effort is in the incorporation of the bidirectional flow of power (for distributed and renewable energy sources) as well as the two-way communications and control capabilities. Simultaneously, with the intensified efforts for computing, communications and control dimensions of the SG, a critical need emerges to address a variety of security and privacy related challenges. The general term to refer to the aforementioned dimensions of the SG is *cybersecurity* [5]–[15].

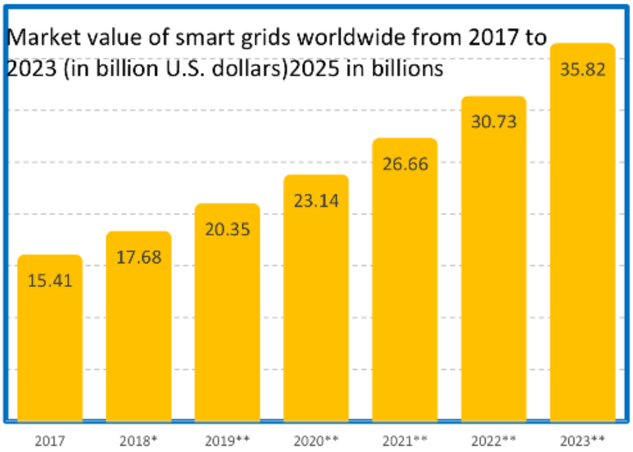


FIGURE 1. Global smart grid market value from 2017 to 2023, accumulated (in billion U.S. dollars). https://www.statista.com/statistics/246154/global-smart-grid-market-size-by-region/.

Even before the SG initiatives, the power grid was vulnerable to malfunction that could disturb its precarious equilibrium and lead to cascading failures, real world examples of which have already left hundreds of millions of people without power for extensive periods of time and with huge financial loss. Both top-down governmental and bottom-up societal trends to incorporate more distributed resources,

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

TABLE 1. List of acronyms.

Acronym	Explanation
AGC	A Automatic Generation Control
AMI	Advanced Metering Infrastructure
CAPTCHA	Completely Automated Public Turing Test To Tell Computers and Humans Apart
CPU	Central Processing Unit
DC	Data Concentrator
DCU	Data Concentration Unit
DDoS	Distributed Denial of Service
DMS	Distribution Management System
DoS Attack	Denial of Service Attack
EDP	Economic Dispatch Problem
ESS	Energy Storage System
EV	Electric Vehicle
FACTS	Flexible Alternating Current Transmission System
GPS	Global Positioning System
HAN	Home Area Network
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems – Cyber Emergency Response Team
IDS	Intrusion Detection System
IED	Intelligent Electronic Devices
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISDN	Integrated Services Digital Network
LMP	Locational Marginal Pricing
MD	Measurement Device
NAN	Neighborhood Area Network
NERC	North American Electric Reliability Corporation
NERC-CIP	North American Electric Reliability Corporation – Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology - Interagency or Internal Report
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
PO	Power Operator
POTS	Plain Old Telephone Service
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SG	Smart Grid
SOA	Service Oriented Architecture
SOC	State-of-Charge
SONET	Synchronous Optical Networking
TCP	Transmission Control Protocol
UCP	Unit Commitment Problem
UDP	User Datagram Protocol
WAMPAC	Wide Area Monitoring, Protection and Control System
WAN	Wide Area Network

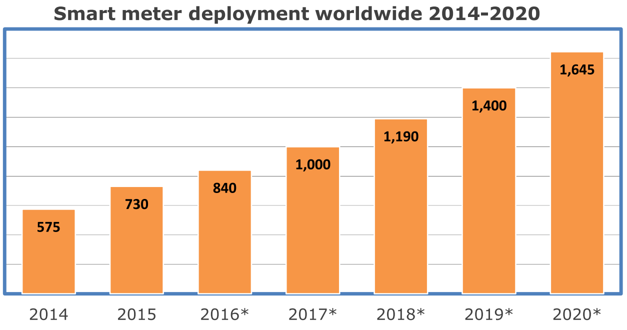


FIGURE 2. Number of smart meters (electricity, gas & water) worldwide from 2014 to 2020 (in millions), real data up to 2015, and then forecast thereafter. https://www.statista.com/statistics/625890/worldwide-smart-meter-deployment/.

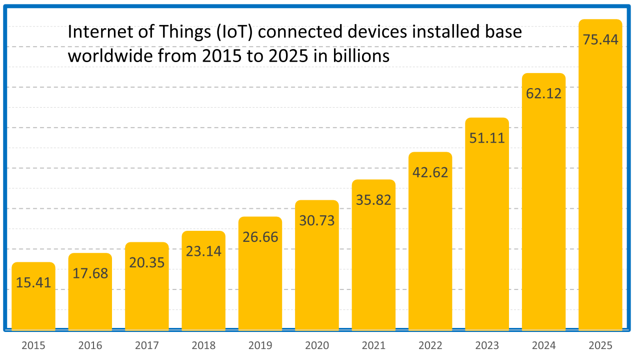


FIGURE 3. Number of connected devices IoT worldwide from 2015 to 2025 in billions. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

including renewables, exacerbate the known power grid deficiencies and make it more vulnerable to deliberate attacks. For example, the number of smart meters shows (Figure 2) almost a quadratic increase in worldwide deployment, which in turn increases the attack vectors with the same proportion.

The increase in IoT and the connected devices, as shown in Figure 3 also contributes to the overall problem by providing for more attack points. That was recently exemplified by the potent destructive potential of Internet-of-Things devices in Mirai attack [16] and its variants [17], [18].

Cybersecurity, as a consequence, becomes an indispensable component and a key enabler for the successful transformation from the electric power grid of yesterday into the SG of the future. Power grid infrastructure has become an attractive target [19] with lethal and vital economic and social consequences by means of disruption to electricity delivery [20]. World Economic Forum's 2018 report [21] emphasizes the increasing cyberattacks on the critical and strategic infrastructure that may result in disrupting the society. It is obvious that the power grid falls into the aforementioned definition of critical infrastructure [22]. Out of so many other real incidents, in December 2015 in Ukraine, cyber attacks were directly responsible for power outages [23], [24]. There is definitely an imperative to implement and adopt cybersecurity technology, both within the SG and beyond.

Conventionally, *availability*, the target of Denial-of-Service (DoS) attacks, is defined as "ensuring timely and reliable access to and use of information" [13]. However in the context of SG "ensuring access to enough power" should also be considered as part of the definition. In this regard, we expand the definition of DoS attacks for the Smart Grid with a broader scope. We believe that DoS attacks in the SG deserve a more fine-grained and a more holistic definition involving the following dimensions: (1) Denial-of-Service in the classical usage attacking *availability*,(2) Denial-of-Control, computing, communications, or the power itself, (3) DoS by means of compromising data *integrity* (such as misleading state estimation and situational awareness), (4) Denial-of-Electric-Service even when ample power is available. The catastrophic outcome of any of these DoS attacks in the Smart Grid domain is a cascading blackout that may leave thousands, if not millions, of customers without power for long time periods [19]. A recent report by University of Cambridge details a severe but plausible cyberattack against the US grid where about 100M people may be left without power with up to $1 trillion of monetary loss [25]. With this expanded definition, availability is regarded as a crucial security objective for the SG as clearly stated in NIST's Guidelines for Smart Grid Cybersecurity [13]. DoS attacks disrupting the Internet traffic have already cost billions of dollars world-wide. With the increasing connectedness of grid systems, a DoS attack to the infrastructure causing a major power failure becomes quite possible and could be undoubtedly more harmful and costly. This is because in modern society electricity is a utility we depend mightly not only on communication but also for many other life-critical functions.

In this work, we present a structured, methodical, holistic, and comprehensive view of the *availability* dimension (spanning both the computational and the electric service realms) of the SG cybersecurity by presenting classifications and discussions of DoS attacks and solutions. To the best of our knowledge, a comprehensive survey study about DoS attacks and solutions on the SG does not exist in the literature, except for the abridged version of this study in 4 pages in [26]. Hereby, we would like to draw the various research communities' attentions to these important cybersecurity issues so that more concerted efforts may be exerted towards more viable and readily available solutions. he rest of this paper is organized as follows: Section III provides the relevant background information about the underlying power grid infrastructure to contextualize the DoS attacks and the solutions of the following sections. A brief introductory material about the SG is presented in Section IV to highlight the exacerbating changes. The existing literature about the Internet DoS attacks and solutions are briefly reviewed in Section V to compare with and contrast to the SG DoS attacks. We provide a taxonomy of DoS attacks on the SG from multiple perspectives in Section VI with brief discussions of each. Section VII follows up the DoS attack classifications with the state-of-the-art solution approaches as well as a taxonomy for an easier presentation. A comparative table of the solutions and attacks is provided in a tabular format together with a discussion in Section VIII. Concluding remarks are in Section IX.

III. POWER GRID BACKGROUND

The power grid is considered to be the largest man-made machine in the world and an engineering marvel. An overall, simplified view of the power grid is depicted in Figure 4. A relatively small of number centralized power plants are responsible for generating the power. Then, the transmission takes the power to longer distances over its connected network of substations, lines, and transformers in high voltage. Distribution reduces the high-voltage power through step-down transformers before feeding it to the commercial, business, industrial, and residential consumption. The focus has always been on the reliability and stability of the power delivery with minimal disruptions. As a result, changes in the power grid are usually implemented with great caution in a conservative approach in order to avoid introducing any instabilities to the system.

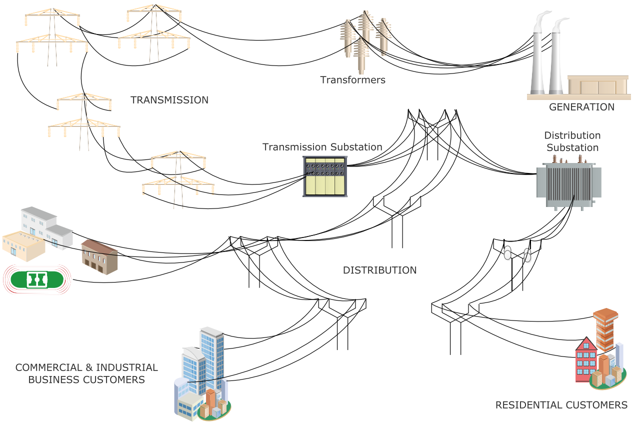
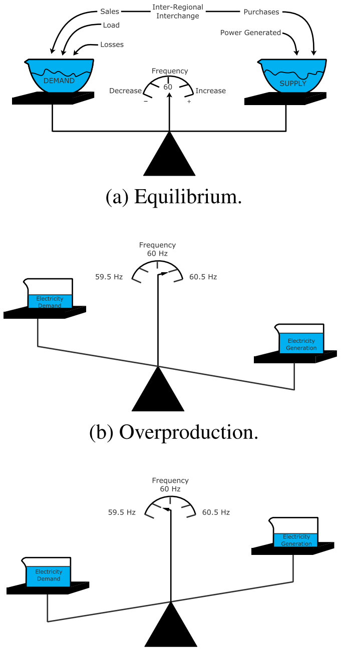


FIGURE 4. **A simplified view of the traditional power grid.**

Due to the peculiarities of electrical power, any generation must be consumed in a relatively short period of time. Large-scale electricity storage is considered to be practically unfeasible, even though many recent promising technologies have been introduced and under constant improvement. On the other hand, overproduction is also problematic that can disrupt the delicate frequency equilibrium of the grid system. shows a representation of the precarious equilibrium between power generation and the demand with the corresponding frequency value, 60 Hz for the US, for example. Any disequilibrium, either overproduction (larger production than demand or load), as shown in Figure 5b, or underproduction



(a) Equilibrium.

(b) Overproduction.

(c) Underproduction.

FIGURE 5. **Delicate frequency equilibrium of the power grid.**

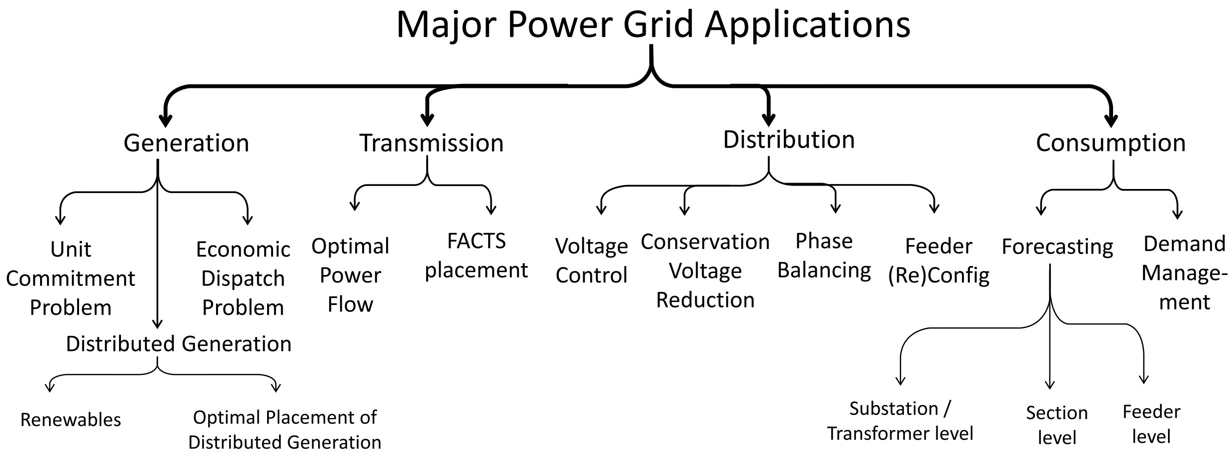


FIGURE 6. Major power grid applications by the segment.

TABLE 2. Communications protocols used in the power grid.

Protocol	Description
Modbus	Simplest, master-slave protocol
IEC 61850	IED Communications
ANSI C12	Metering Protocol
IEEE C37.118	Synchrophasor Measurements
IEC 60870	Umbrella Name for SCADA protocols
IEC 62351	Power Grid Automation Security
DNP3/IEC 60870-5	Data Acquisition in SCADA
ICCP (IEC 60870-6/TASE.2)	Control Center (CC) to CC communications
ETSI TS 104 001 Open Smart Grid Protocol	Application Layer Protocol for Smart Devices
ISO/IEC 14908-1:2012	Control Networking Layer
DLSM/COSEM (IEC 62056)	Smart Meter Data Exchange
Open Automated Demand Response (OpenADR)	Energy Management
Streaming Telemetry Transport Protocol (STTP)	PMU data transfer

TABLE 3. Comparing communications in the internet and in the power grid.

Criteria	Computer Networks	Power Grid
Delay	Maybe delay-sensitive	Stringent
Jitter	Some sensitivity	Very sensitive
Data Rate	Important	Not as much
Availability	Important but may be tolerated	Critical
Confidentiality	Critical	Important
Integrity	Critical	Important
Devices	Less Resource Constrained	Many resource constrained devices
Communications	Standard	Mostly Proprietary
Economic Lifetime	3-5 years	15-30 years
Span	Physically more tightly coupled	Remote and isolated

(lower generation than demand), as shown in Figure 5c, leads to a disturbance in the system in terms of lower or higher frequency, respectively.

Major communications protocols used in the power grid [27]–[30] are given in Table 2. Some of these protocols are proprietary with minimal or no original security provisioning. Except for the newer Open Smart Grid Protocol (OSGP) (ETSI TS 104 001 and IEC 14908), all have the option to run over TCP/IP networks that brings in the possibility of all the DoS attack techniques from the Internet into the SG domain.

NIST's Guide to Industrial Control Systems (ICS) Security (SP 800-82) [31] notes the major differences between traditional computer networks and the power grid communications [32] as summarized in Table 3. With such stringent and tight constraints for a critical infrastructure like power grid [22], the significance of reliability and availability are challenging and vital.

Some of these differences make the power grid more vulnerable to attacks, especially in conjunction with the physical dimension of the attack impact.

A. POWER GRID APPLICATIONS

Figure 6 shows the main power grid applications for its operations in terms of the sections: Generation, Transmission, Distribution, and Consumption. The Unit Commitment Problem (UCP) is an optimization problem to decide which ones of the generation sources should be activated (committed) to meet the demand while the Economic Dispatch Problem (EDP) is concerned with determining the actual amount of power from each active resource; both with the objective of cost minimization or revenue maximization. The output of EDP also includes the Locational Marginal Pricing (LMP), the cost of optimally generating an incremental load while satisfying all the constraints. The Optimal Power Flow is a set of operational problems to achieve and maintain the reliability of the grid. A set of devices, referred to as Flexible Alternating Current Transmission System (FACTS) devices, are used to control and optimize power transmission efficiency and their optimal placement is a critical problem.

In the distribution, various aspects of the power (voltage control, phase balancing, feeder configuration) as well as the devices must be addressed in different applications. Finally, in the consumption domain, forecasting and demand side management applications are used to ensure the precarious equilibrium between load and supply is maintained at all

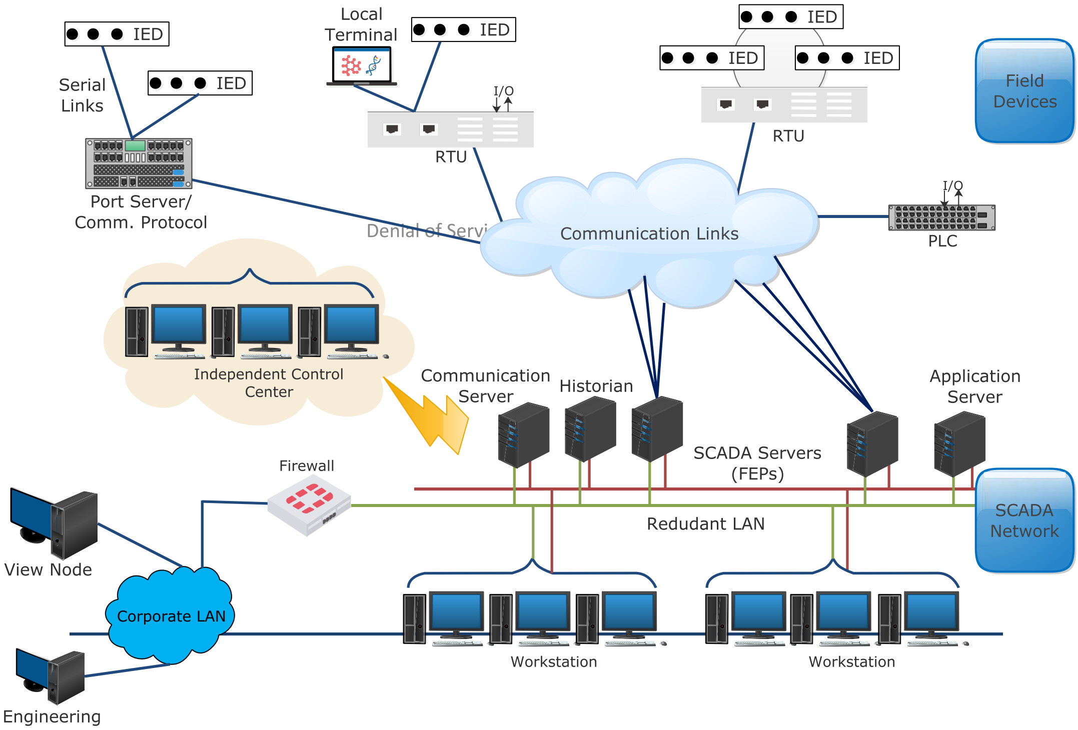


FIGURE 7. Power Grid's Supervisory control and data acquisition (SCADA) subsystem. https://eioc.pnnl.gov/research/cybersecurity.stm.

times. Note that these applications are vital for the proper functioning of the grid and thus they are themselves the potential targets of cyberattacks, especially DoS variants.

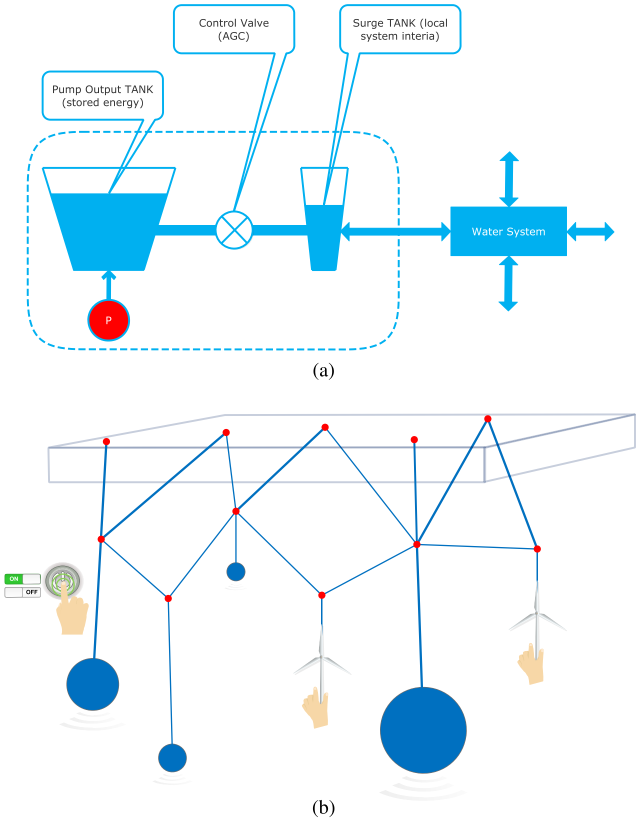
The communications and networking infrastructure of the power grid is usually represented by means of the Supervisory Control And Data Acquisition (SCADA) subsystem, as shown in Figure 7. SCADA comprises of many telemetry, sensing, and measurement devices coupled with networking infrastructure linking them to provide the basic mechanism for data collection, communications, storage, processing, and analysis. Specific devices of SCADA in the power grid context include Remote Terminal Units (RTU), Programmable Logic Controller (PLC), and Intelligent Electronic Devices (IED).

As mentioned earlier, immediate consumption requirement mandates a demand-supply equilibrium to be maintained at all times and any imbalance in either direction leads to serious repercussions. Besides maintaining the load-supply equilibrium at all times, the power grid operators must also have the capability of restoring the stability of the grid in short intervals (in 10-20 seconds) after disturbances. The aforementioned capability is referred to as *transient stability*, as typically visualized in a diagram like Figure 8b [33], where masses represent generators, strings transmission lines, power button the disturbances, and hands with windmills the volatile renewable and distributed resources to depict the delicate balance the power grid must achieve and maintain. Automatic Generation Control (AGC), as depicted in Figure 8 [34] with a water distribution analogy, adjusts the power production levels of generators automatically in response to load changes or disturbances. AGC is a ripe target for attack that may result in a significant operational damage and instability [35]. In [36] authors implemented device that on physical level causes smart meter to read consumption values that are near zero.This on larger scale can lead to false load attack. In [37] authors propose control switching unit as a countermeasure to cyber attacks on control parameters of AGC and automatic voltage regulator.

The delicate and precarious balance and operating conditions of the power grid, as shown at a high level analogy in Figure 8b, may easily lead to activation of a series of protection mechanisms with cascading failures and large-scale blackouts [38], [39], such as the blackouts of 1965 in Northeast America, 1978 in France, 1999 in Brazil, 2003 in northeastern US and Canada [40], 2012 in India [41], etc. In addition to the accidental disruption to power, there have been intentional disruptions as a result of general cyberattacks, as summarized in Table 4 [20]. Note that it is quite likely that there have been many more cyberattacks, either undetected or not reported in public documents, for obvious security reasons.

IV. SMART GRID PARADIGM

Smart Grid [42]–[44] is a vision for the next generation power grid to address the aforementioned deficiencies and improve its performance by taking the full advantage of the latest information and communications technology approaches. NIST considers it as a system of systems [45]. A holistic


Control Valve (AGC)
Surge TANK (local system interia)
Pump Output TANK (stored energy)
Water System
P
ON
OFF

(a)

(b)

FIGURE 8. (a) A simplified representation of the automatic generation control (AGC) in the power grid [34], (b) A metaphorical illustration of the concept of transient stability in the power grid [33].

TABLE 4. Some recent major cyberattacks on the power grid.

Date	Cyberattack
2003	A nuclear power plant was compromised in Ohio
Feb. 2011	Brazilian power plant management system
June 2011	Brazilian energy company Petrobras website attack
2012	German power utility hit by DoS attack
2012-13	US public utilities were breached
2013-2014	Stuxnet-like attack against more than 1000 energy companies in 84 countries
2014	A Large US Power Company's Automatic Voltage Regulator was compromised
Dec. 2015	BlackEnergy malware attack against Ukrainian regional power companies, knocking power off for about 225K people
Dec. 2016	Another Ukraine attack using Industroyer malware
May 2017	Ransomware against India's West Bengal State Electricity Distribution Company
2017	Dragonfly 2.0 attack against many Western energy companies
2017	Cyber attack in Saudi Arabia petrochemical power plant
2019	Power grid cyberattack in western United states
2020	European Network of Transmission System Operators for Electricity hit by cyberattack

definition of the Smart Grid is provided in [42]: *The Smart Grid can be regarded as an electric system that uses information, two-way, cyber-secure communication technologies, and computational intelligence in an integrated fashion across electricity generation, transmission, substations, distribution and consumption to achieve a system that is clean, safe, secure, reliable, resilient, efficient, and sustainable.*

The coverage is the entire power grid, from the generation all the way to the consumption [43]. A seven-domain Smart Grid Architectural Model [45] by NIST is shown in Figure 9.

An important enabler of the Smart Grid initiatives is the enhanced use of sensing and measurement capabilities. Phasor Measurement Units (PMUs) are the advanced, accurate, and synchronized measurement devices to take the situational awareness to a new level. While the traditional SCADA measurements are taken every 2-4 seconds, PMU reports them 30-60 times per second with GPS time stamps. As compared to SCADA, PMU-enabled conceptual model of wide-area monitoring, protection, and control subsystem is illustrated in Figure 10 [46].

V. DENIAL-OF-SERVICE ATTACKS AND SOLUTIONS IN THE INTERNET

In this section, we provide a brief overview of the state-of-the-art DoS attacks and solutions in the Internet [47]–[54] as a prelude to our discussion in the SG domain. Naturally, there are overlapping topics and areas between the Internet DoS and SG DoS. However, the unique characteristics of the SG, as elaborated in Section III, require a dedicated and closer look to adopt existing DoS solution techniques, and more importantly develop new ones. Figure 11 shows a high-level of taxonomy for our discussion in terms of the attacks and the defense mechanisms in Internet against DoS.

A. INTERNET DoS ATTACKS

Denial of Service (DoS) are the type of attacks in which the attacker or a group of attackers attempt to make a service or computing/networking resource unavailable for its intended users. Figure 12 shows a simple DoS attack, where an attacker on the leftmost initiates transmission of malicious traffic through the handlers and a set of compromised machines (zombies, or bots) to make a set of target servers inaccessible.[1] Nowadays, network security companies claim that DoS attacks are one of the greatest concerns for the service providers. NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report [55] states that 87% of the actual threats experienced on service providers are DoS attacks, while the 14th Annual Report from March 2019 [56] stated it as 95%! Akamai's State of The Internet, Summer 2018 report [57] states that in the first half of 2018 relative to the first half of 2017 DoS attacks on their content distribution networks have increased by 16%. Amazon claimed that during the first quarter of 2020 they experienced DoS attack 2.3Tbps [58].

Physical layer attacks rely on changing physical properties of the communication media. There are two major categories of attacks on this layer as described in the literature: jamming and tampering. Jamming attacks rely on modification of signals transmitted between communicating devices which may, on receiver/sender side, result in a malfunction due to

[1] We note that we do not differentiate between DoS and its distributed variant for the rest of the paper.

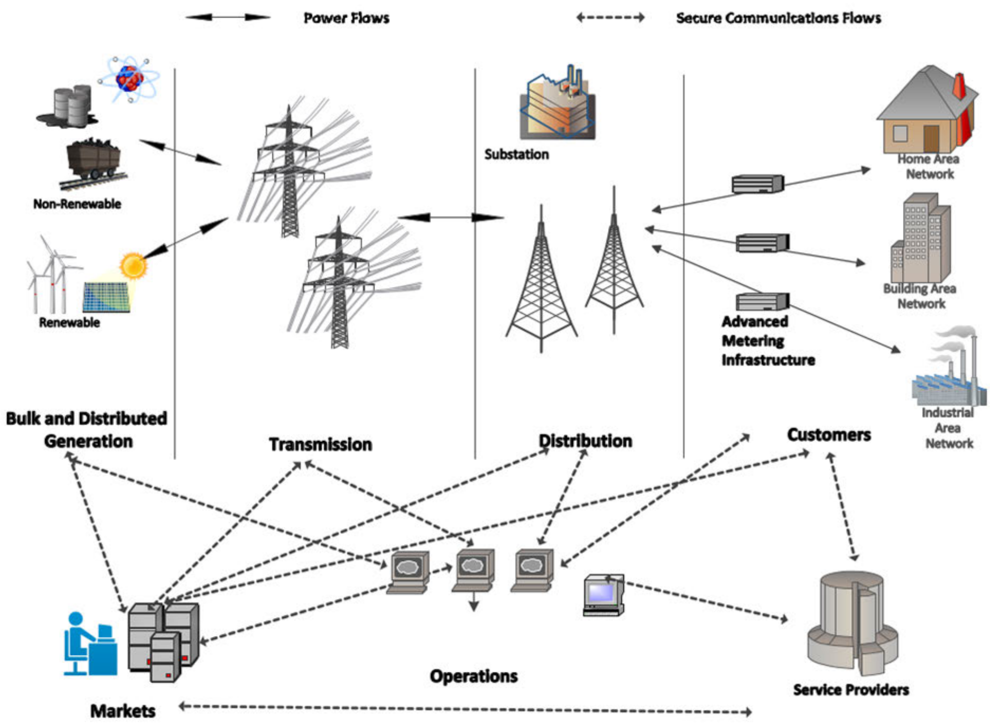


FIGURE 9. 7 domains of the NIST's smart grid architecture model [45].

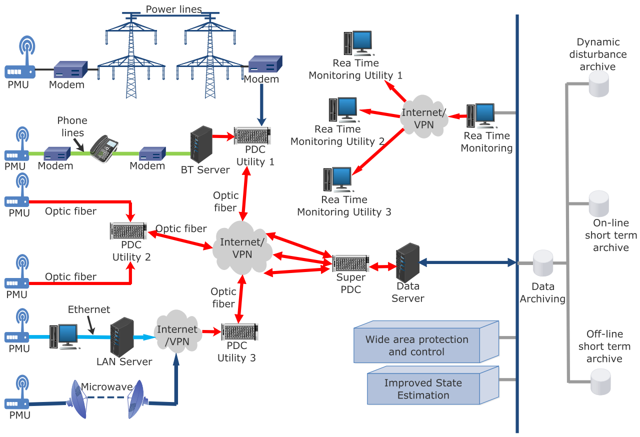


FIGURE 10. A conceptual framework for a wide-area monitoring, protection, and control system for the smart grid made possible by PMUs [46].

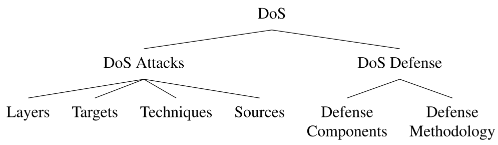


FIGURE 11. A high-level summary of the Internet DoS attack and defense approaches.

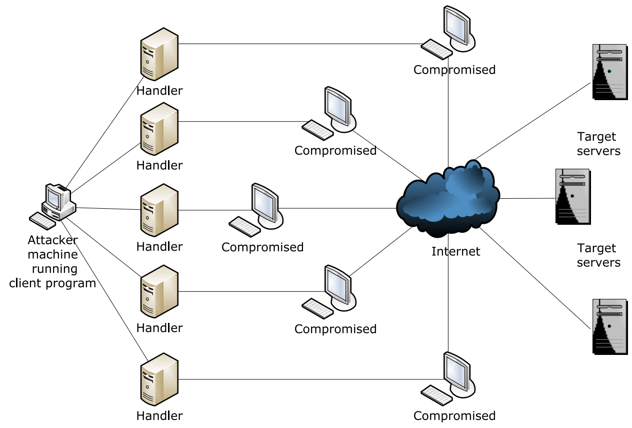


FIGURE 12. A simple illustration of a DoS attack.

false interpretation of signals. Tampering relies on physical modification of devices. Data link layer DoS attacks rely on exploiting design flaws of media access protocols in target networks. IP layer DoS attacks rely on spoofing IP protocol fields, such as falsifying routing information and altering assignment of IP addresses. At the transport layer, DoS attacks exploit vulnerabilities in order to exhaust some computing and/or networking resource. Application layer DoS attacks rely on overloading resources on target system by making target processes or servers unable to serve legitimate requests.

Another classification may be presented by means of the attack target as shown in Figure 13: Devices, Links and Power infrastructure. Devices group consists of computing end-nodes, network end-nodes and communication devices.

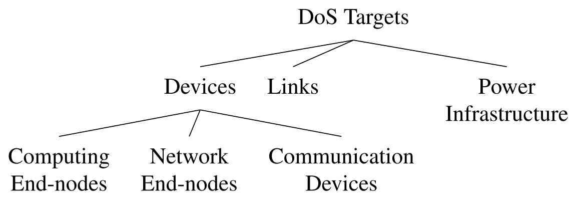


FIGURE 13. Types of Internet DoS in terms of the attack targets.

Computing end-nodes refer to personal computers and servers that provide computing resources in network. Network end-nodes refer to devices providing various network services such as firewalls, load balancers and local DNS servers. Communication devices refer to devices that provide network connectivity such as routers, switches and access points. Due to physical restrictions and available bandwidth links used for interconnection between network devices are easily congested which in the end results in DoS.

At a coarse granularity, we categorize the techniques used in the Internet DoS attacks into three, as displayed in Figure 14: spoofing, resource exhaustion and vulnerability exploitation.

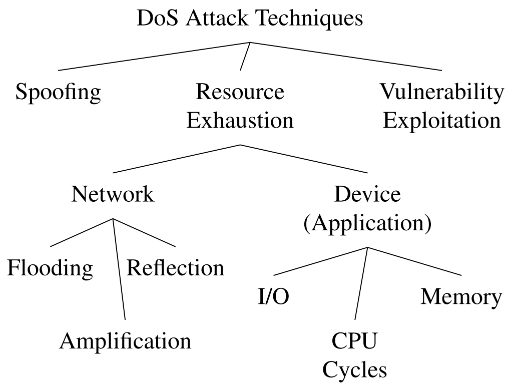


FIGURE 14. A high-level categorization of the Internet DoS attack techniques.

The IP spoofing technique is widely used in performing DoS attacks. The most simple explanation of IP spoofing is that the attacker specifies a false source IP address in the IP header when sending a request to the target. This is possible because one can assign any desired IP address to nodes. The spoofing technique is the basis of flooding, amplification and reflection attacks on network. Flooding attacks mostly exploit TCP three-way handshake mechanism by sending many SYN messages with false source IP addresses to attack server. The server then tries to send ACK messages to these non-existing IP addresses. This results in exhaustion of server resources needed to serve legitimate connection requests.

Amplification and reflection attacks usually rely on applications that use UDP protocol. The attacker sends small UDP packets with spoofed source IP addresses to vulnerable UDP servers which in return send response messages to a victim at the spoofed IP address. This method is called a *reflection* attack. When the triggered response is verbose and much higher in volume than the original bogus request then we have the *amplification* attack.

We would like to note while some of the resource exhaustion attacks may use spoofing we separate the two techniques as not all resource exhaustion attacks make use of spoofing and not all spoofing are for resource exhaustion. That is, techniques of resource exhaustion rely not only on spoofing, but also on any technique that may lead to saturation of available bandwidth, CPU throughput, memory throughput, system buses throughput on end devices. This may involve techniques of overloading regular applications and services on devices. Vulnerability exploitation can be observed from protocol design side, but in our taxonomy we consider it by means of flaws or holes in application binaries. Source of a DoS attack might involve a single device or multiple devices with spoofed or real IP addresses.

Figure 15 depicts DoS attacks from the source perspective. Nowadays, most DoS attacks are performed from multiple sources combining spoofing and real IP addresses. Those attacks are usually referred to as Distributed Denial of Service Attacks (DDoS). These are the most fatal and damaging attacks in the Internet [55], [57], [59].

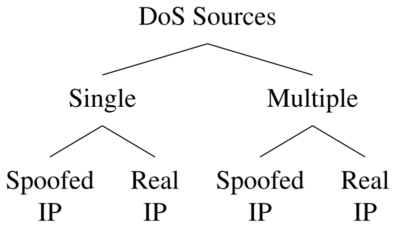


FIGURE 15. DoS Sources.

B. DEFENSE AGAINST INTERNET DoS ATTACKS

Figure 16 depicts DoS defense methodologies with main groups: Prevention, Detection and Reaction. Reaction then includes two more sub-categories as isolation and mitigation techniques. DoS prevention mechanisms [52] include different techniques from filtering spoofed IP addresses to validating IP addresses and hosts.

Figure 17 displays DoS target defense mechanisms or components. Defense mechanisms can be deployed at Hosts, Network, Application, or Algorithms. Network appliances, such as firewalls and Intrusion Prevention Systems (IPSs), can be used to prevent DoS by creating customized rules in access control lists. Intrusion Detection Systems (IDSs) as defense mechanism can be used to reconfigure firewalls in order to stop ongoing and detected attacks. Traffic monitoring system could be used to track bandwidth usage and throttle requests when they consume critical predefined values of available bandwidth. Detection mechanisms may use different algorithmic approaches, such as anomaly detection, probability density function, or distribution-free approaches. Signature-based IDS collects signatures, or a distinguishing pattern of known DoS attacks and compare network traffic

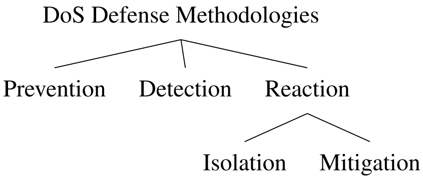


FIGURE 16. Defense methodologies against Internet DoS attacks.

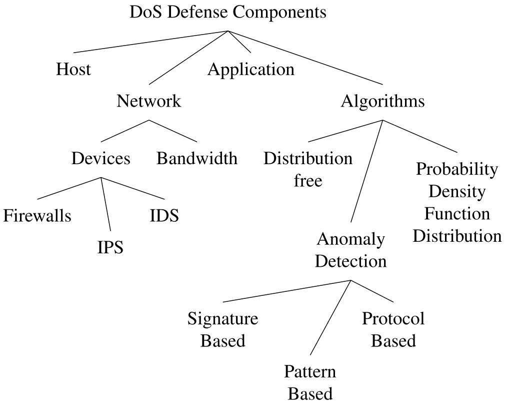


FIGURE 17. DoS defense components.

with these in order to differentiate normal traffic from the malicious. Pattern-based IDS maintains knowledge base of legitimate traffic patterns by means of statistical properties, or the good behavior, to label any data deviating form that as malicious. Protocol-based IDS is similar to the pattern-based except that the acceptable behavior is defined in terms of the logical specifications, such as the expected pattern of data transfer for a specific communications protocol [60].

VI. SMART GRID DoS ATTACKS

A. PRELIMINARIES AND FUNDAMENTAL VULNERABILITIES

The SG has many subsystems that involve some notion of hierarchical data collection, as generically depicted in Figure 18. A set of measurement devices (MDs in Figure 18), such as smart appliances, smart meters, data aggregators, PMUs, IEDs, RTUs, PLCs, etc., sense the environment, generate data, and transmit them towards a centralized data center, denoted as PO or power operator in Figure 18, via one or more levels of intermediary data aggregators, marked generically as DC (data concentrator). These general data collection subsystems are quite similar to the Internet's infrastructure, which have been plagued by a variety of vulnerabilities that were exploited for clever and devastating DoS attacks. Thus, the SG bears similar set of attack vectors, vulnerabilities, and threats, especially with the adoption of the Internet's fundamental protocols. Further, in the SG domain, the security has mostly been an afterthought or overlay, that is usually added after-the-fact, which leads to many weaknesses in cybersecurity approaches. For example, many power companies do not currently classify PMU networks as critical cyber assets [61] that may be contributing structural and inherent lack of preparedness against cyberattacks, especially DoS variants.

Potential cyberattacks leading to power service interruption in one of the SG subsystems, Advanced Metering Infrastructure (AMI), are depicted in Figure 19 [62]. Potential sequences of events leading to a disruption of the electric service triggered by a breached single smart meter [62] are displayed in this high-level diagram. In recent paper [63] a summary of threat to system level security in SG metering network are given. The effect of DoS attack can scale from low to severe, compromising availability and integrity of the service. In [64] DoS attacks impact is described twofold: financial loss and power lines failure. In [65] authors give detailed explanation of threats and potential solutions of IoT based smart grids.

B. ATTACK TAXONOMIES

In this section, we introduce different classifications of the actual and potential Smart Grid (SG) DoS attacks from five different perspectives. The first classification may be stated

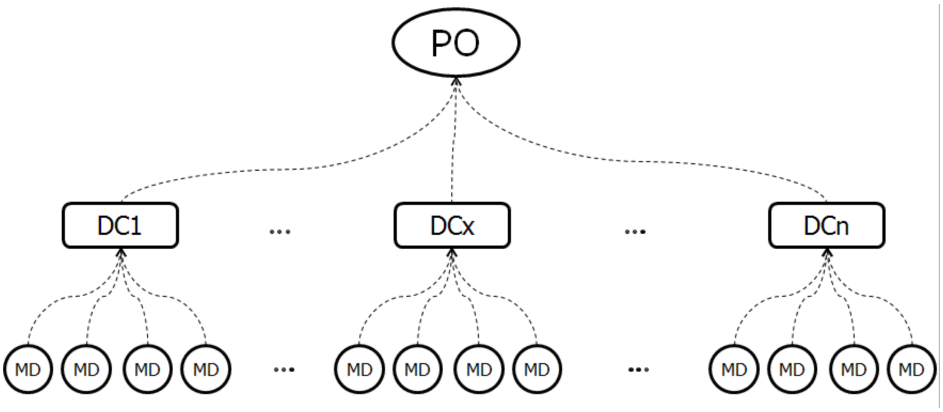


FIGURE 18. A simple representation of data collection subsystems in the SG, where MD represents a measurement device, DC a data concentrator, and PO a centralized power operator.

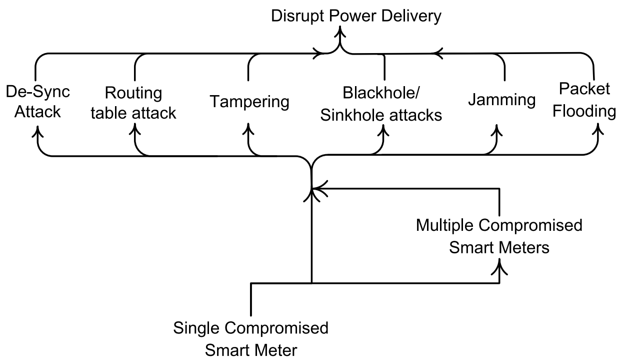

Disrupt Power Delivery
De-Sync Attack
Routing table attack
Tampering
Blackhole/ Sinkhole attacks
Jamming
Packet Flooding
Multiple Compromised Smart Meters
Single Compromised Smart Meter

FIGURE 19. Some potential sequence of events leading to power delivery interruption in advanced metering infrastructure (AMI) of the SG after a single smart meter is compromised.

in the terms of the spatial dimension. DoS attacks may target all the segments of the SG, from generation, transmission, distribution, and consumption to control centers and Electric Vehicles (EVs) charging/discharging infrastructure, which is quickly becoming a growing attack vector for cyberattacks [66], [67]. The SG comprises bidirectional transmission of both power and information.

A DoS attack may exploit vulnerabilities with respect to the commonly used communications protocols peculiar to the utility companies, as shown in Figure 20. IEC 61850 is a networking protocol for substation automation. Besides running on top of TCP/IP, and hence inheriting all the DoS vulnerabilities from the Internet domain, possible DoS attacks exploiting two of IEC 61850's protocols (GOOSE and SV) are reported in [68]. A general discussion of security threats with DoS focus can be found in [8], [9]. ANSI C12.22/IEEE 1703 defines a communications protocol for Advanced Metering Infrastructure (AMI). A distributed DoS attack scenario is presented in [69], [70] for C12.22 service. IEEE C37.118 is the networking protocol for the Phasor Measurement Unit (PMU) data. DoS attacks on C37.118 are studied in [71], [72]. State-estimation in case of DoS in the smart grid PMUs is studied in [73]. The IEC 60870 family of standards covers communications for SCADA (supervisory control and data acquisition). Simulation-based analysis of DoS attacks from the IEC 62351's perspective is presented in [74]. Finally, DNP3, an alternative protocol for SCADA used by utility companies, has its own set of DoS related problems, as detailed in [75]. Simulation-based evaluation of DoS against SCADA is given in [76]. Authors analize the effect of DoS attacks launched from compromised Remote Terminal Units.

From the communications perspective [27]–[30], [77]–[79], the attacks may originate at different layers, from the physical and data link layers all the way to the network, transport, and application layers, as shown in Figure 20b.

Another taxonomy may be presented by means of the major power grid applications, as depicted in Figure 20c. As the crucial application of the SG, Advanced Metering Infrastructure (AMI) is the last mile where smart meter to the utility bidirectional communication and data transfers take place. Several studies highlight the DoS attacks in AMI [35], [60], [62], [69], [70], [80]–[82]. An example DoS attack on an AMI network is depicted in Figure 21 [69]. Attackers spoof the victim's address; send packets to several unsuspecting destinations with the victim's address as the source address; and destinations simply flood the victim with lots of unwanted traffic, rendering it unavailable for legitimate traffic. This is an example of a reflection attack. An integral component of SG is the Distribution Management System (DMS) that is in charge of monitoring, protection, control, and optimization of distribution assets. [80], [83], [84] introduce load frequency disturbance as a result of a DoS attack and load altering attack is discussed in [85]. DoS attacks to energy

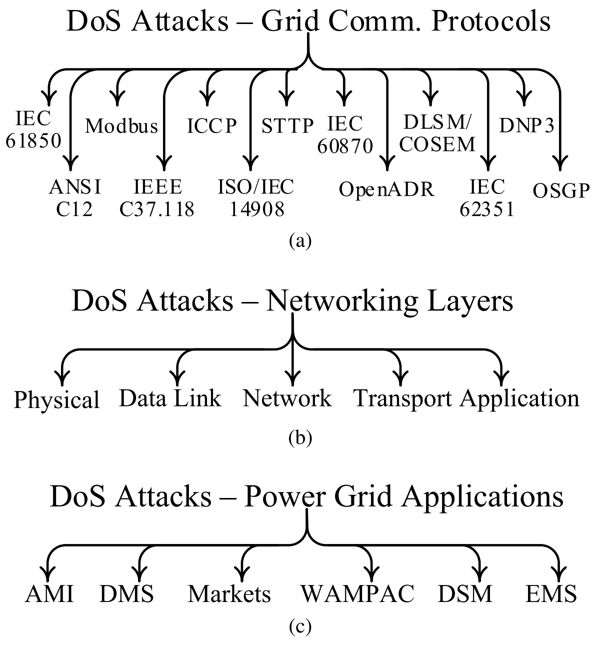


FIGURE 20. (a) SG DoS attacks in terms of the major power grid communications protocols, (b) SG DoS attacks in terms of communications layers, (c) SG DoS attacks in terms of the major power grid applications.

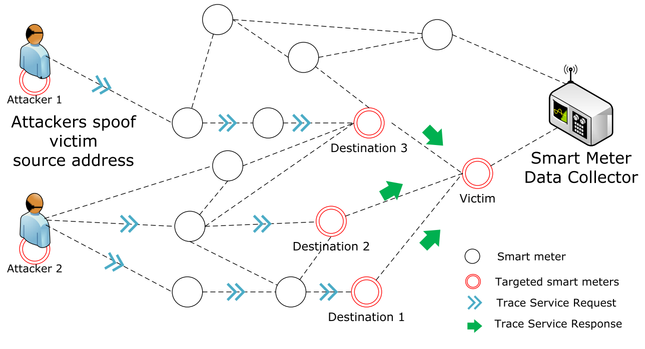


FIGURE 21. An attack scenario on the AMI [69].

markets, especially pricing, are covered in [9], [64], [86]. Wide Area Monitoring, Protection, and Control Systems (WAMPAC) [46] are also prone to DoS attacks, as described in [72], [84], [87], [88]. Demand Side Management (DSM) involves techniques to maintain the load and supply equilibrium from the demand side. DoS potentials are presented in [9], [85]. A large-scale coordinated demand manipulating attack that can be launched by compromised high wattage IoT devices is shown in [89]. The North American Electric Reliability Corporation (NERC)'s Cyber Attack Task Force from 2012 outlines the risk of DoS on Energy Management System (EMS) with targeted attacks is detailed in [90].

A final taxonomy of the DoS attacks in terms of the *techniques* employed is given in Figure 22. We posit seven different main categories of techniques that a DoS attack may utilize: Signal jamming at the physical layer may be initiated to deny, delay, or degrade information or electricity service [8], [80], [91]–[93]. Resource exhaustion DoS attacks may target a device or a network. For the former [74], [75], [94], spatial types are for depleting some dimension of memory while processing and battery target the computing and power resources, respectively. For the latter [9], [81], [95], flooding is an indiscriminate transmission of traffic to saturate the bandwidth while the directed is a more targeted transfer of deluge of data. One cryptographic DoS attack scenario is explained in [96] where a Message Authentication Code used to prevent data corruption may be exploited to trigger a DoS attack. Data manipulation may be used as a stepping stone to launch DoS attacks [35], [85], [86]. A single smart meter compromise may inject malicious data for a variety of different attacks in a Neighborhood Area Network (NAN) [97], as shown in Figure 23 [62], including DoS attacks.

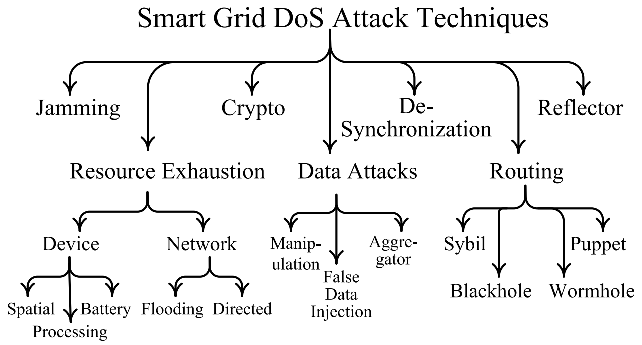


FIGURE 22. **A taxonomy of the DoS attack techniques in the smart grid.**

While the goal of the false data injection attacks [9], [98]–[103] may be on integrity, and even covert [104], it may also be easily used as a DoS tool [24], [35], [90]. A false data injection attack scenario to distrub Automatic Voltage Control (AVR) is evaluated in [105]. Data aggregation is an important part of the data collection subsystem of the SG. A typical hierarchical data collection by means of data aggregators is a boon for initiating a DoS attack [9], [62], [75], [80], [106]. Many applications of the SG are highly sensitive to the timeliness of the data and the transactions. De-synchronization attacks [107]–[115] can be utilized as another form of DoS, as illustrated in Figure 24. GPS synchronized devices may be subject to well-known GPS spoofing attacks. In [116] authors describe poisoning attack on load forecasting mechanism in Smart Grid, while authors in [117] give brief overview of attacks on load forecasting.

The right-most time synchronized measurement is compromised through a GPS spoofing attack and thus the Smart Grid control center will be fed with incorrect data or even malicious code. In [118] authors describe and simulate Denial of Sleep attack on Open Metering System with battery powered metering devices. The attack is based on manipulating control messages in TLS-like handshake used for securing communication between metering devices. In [119] authors describe attacks on test system involving Siemens and Schneider PLCs. The test scenario showed that selected PLCs are vulnerable to DoS and Man in The Middle attacks which can lead to exposure of sensitive data.

SG involves bidirectional data transfers and routing, in this respect, it becomes an important mechanism and attractive target for DoS attacks. Typical routing-based DoS attacks are directly applicable for the SG domain, such as the sybil, wormhole, blackhole, and puppet attacks. Reflector attack involves spoofed requests to a set of servers that will in return send their replies to the target node having the spoofed address. In [69], ANSI C12.22 protocol is shown to be vulnerable to a distributed DoS attack in which a number of compromised smart meters generate trace requests carrying the source address of a victim machine.

VII. SOLUTIONS

We have seen that attackers have many options to conduct a successful attack to disrupt the service of the SG or a part of it thereof. Unfortunately, there is no single bullet-proof solution that can prevent all forms of DoS attacks [49]. DoS attacks should be dealt with carefully by bringing together various solution approaches considering the specific requirements and risk priorities.

In this section, instead of targeting each attack type separately, we first introduce the tools available in the toolbox of the DoS-resilient SG system designer. Then, in the next section we discuss, compare, and contrast the suitability and strength of these tools against the concerned attacks. By this way, our goal is to identify previously unidentified or unexplored solution options.

It is also worth to mention that we try to be as comprehensive as possible in this section. For instance, among the criteria for including a tool in the following discussion, a publication of a previous work specifically using it in a SG environment may not exist. A SG network inherits many of its properties from the already available network technologies, like the Internet. Hence, there is no reason not to benefit from the rich literature which do not target smart grids specifically.

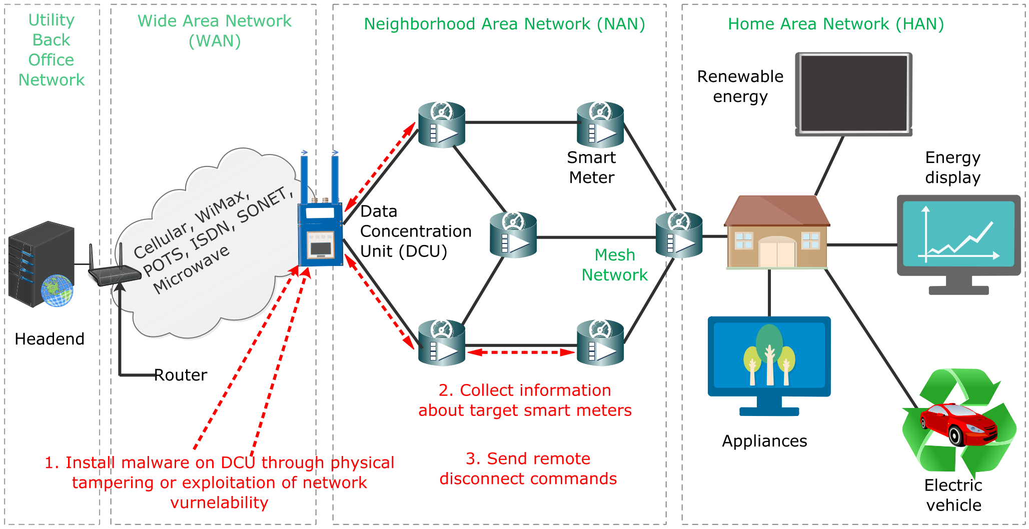

Utility Back Office Network
Wide Area Network (WAN)
Neighborhood Area Network (NAN)
Home Area Network (HAN)
Renewable energy
Energy display
Smart Meter
Cellular, WiMax, POTS, ISDN, SONET, Microwave
Data Concentration Unit (DCU)
Mesh Network
Headend
Router
2. Collect information about target smart meters
1. Install malware on DCU through physical tampering or exploitation of network vurnelability
3. Send remote disconnect commands
Appliances
Electric vehicle

FIGURE 23. A compromised data collection unit might be used to knock off SG devices, such as smart meters, to deny power to consumers [62].

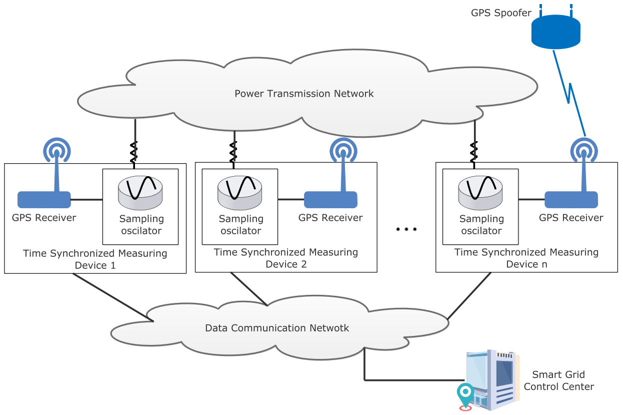

GPS Spoofer
Power Transmission Network
GPS Receiver
Sampling oscilator
Time Synchronized Measuring Device 1
Sampling oscilator
GPS Receiver
Time Synchronized Measuring Device 2
...
Sampling oscilator
GPS Receiver
Time Synchronized Measuring Device n
Data Communication Netwotk
Smart Grid Control Center

FIGURE 24. A simple representation of time de-synchronization attack [107].

On the other hand, we add SG specifics to our discussion at the end of each following subsection.

We note that all DoS countermeasures involve at least one of the three common security functions[2]; prevention, detection and reaction. A high-level classification of solution approaches for SG DoS attacks is given in Figure 25.[3]

We emphasize that prevention is the first line of defense but not always possible and detection without proper reaction is meaningless.

A. NON-TECHNICAL SECURITY CONTROLS

The observation that ''security is a process, not a product'' is also relevant for our discussion on SG DoS solutions. To ensure that availability requirements are satisfied, it is a recommended practice to implement security controls (e.g., NISTIR 7628 [13], NIST 800-53 [120], ICS-CERT Recommended Practices [121], [122], NIST Framework for Improving Critical Infrastructure Cybersecurity [22], NIST Guide to Industrial Control Systems (ICS) Security [123]). However these controls do not necessarily consist of only technical ones. For instance, physical controls to deter or prevent unauthorized access to sensitive areas is effective against certain types of DoS attacks. We should also never underestimate the importance of experienced network administrators in the attack identification efforts [124].

Maintaining a working set of security controls require careful risk assessment [125] and threat analysis [62]. Implementing security controls in a scalable manner could be facilitated with a formal framework and automated analysis tools [126].

What is different in SG? The driving force to implement security controls is usually the compliance requirements. Since security focus in SG is quite different than in traditional information systems, sector-specific standards have emerged. For instance, NERC-CIP 002-009 has been mandated for the electrical sector in USA [121] and NISTIR 7628 Guidelines for Smart Grid Cybersecurity [13] provides an analytic framework to develop cybersecurity strategies.

B. FILTERING

Filtering means dropping packets on a network device if identified as being not legitimate. Traditionally, packet filtering is implemented on perimeter devices, such as firewalls. With a carefully crafted security policy, filtering could help to prevent DoS attacks. Consider a common scenario where through a gateway the SG is connected to the Internet. Notice that the gateway is the perimeter on which you can implement filtering easily. For instance, a firewall, configured with a whitelist of trusted hosts, could serve as a simple, yet effective layer of protection against simple DoS attacks.

[2] To reduce the clutter, we have chosen this taxonomy but we note that it is not always possible to consider a countermeasure performing only a single function. For instance, there is a thin line that separates IDS and IPS devices.

[3] For the sake of readability, simple reaction techniques are omitted.

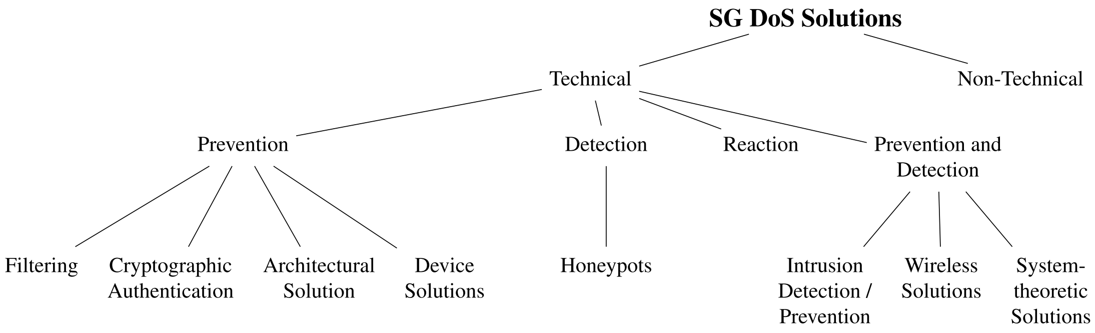


FIGURE 25. Solution approaches to the SG DoS attacks.

The attackers could penetrate inside the SG network by malicious devices inadvertently deployed inside the trusted perimeter by an organization's own personnel [127]. Against such attacks, perimeter defense is not a viable option. However, filtering could be implemented in multiple locations along the network path and the one in the local host (host-based firewall) could also protect against threats from insiders. On the other hand, in principle, filtering is most effective when implemented close to the attack source. This is due to the ability to minimize the bandwidth consumption of the DoS traffic in the network.

Wang and Yi present the design of a firewall to secure SG communication in a multihop wireless network in [128]. The key idea of their proposal is the ability of a node to report the intruder to its neighbors by sending a prealarm message. These messages trigger other nodes to move the intruder either to a graylist or a blacklist.

What is different in SG? Host-based firewall is not a viable option for legacy and/or low-end endpoint devices common in a SG. Many legacy devices are running operating systems not properly patched, therefore bump-in-the-wire firewall, a separate device providing security services for a single host, should be considered in a SG environment.

C. INTRUSION DETECTION/PREVENTION

To avoid the use of a confusing terminology, we use the terms "firewall" and "filtering" only to refer to blocking or allowing network traffic without looking at that traffic in close detail. Firewalls analyze packet headers and enforce a security policy. On the other hand, we call the device or the application that analyzes whole packets, both header and payload, and sends alerts upon detecting suspicious network event as intrusion detection systems (IDSs).

Exthe case of sophisticated attacks *e.g.,* fluctuating or increasing rate attacks [124], that cannot be differentiated from an accident or a flash event, DoS attacks are not something that could be kept secret forever. Therefore, the aim for detection usually is to shorten the time needed to detect so that proper reaction countermeasures could immediately be employed. When combined with automatic responses e.g., blocking malicious packets of the detected intrusion attempt, IDSs become IPSs (Intrusion Prevention Systems). Manual processing of IDS alerts may be preferred when the number of false positives is high.

There are three broad IDS categories: (1) Signature-based (misuse) detection: relies on an available database of signatures (patterns that identify attacks), (2) Anomaly-based detection: It involves two steps; train the system with the normal behavior and then detect any deviations, and (3) Specification-based detection: based on specifications that capture legitimate behavior.

A DoS attack is an anomaly expected to lead to a deviation of statistics of the monitored traffic. Therefore, in theory with a suitable choice of statistics a detector with low rate of false positives could be built. However, it is not clear whether malicious flooding could be reliably discriminated from a legitimate flash event (large amount of traffic from legitimate clients) [124].

The difference between anomaly-based detection and specification-based detection is subtle but important. While the former depends on statistical or machine learning techniques to identify attacks, the latter is based on manually developed specifications. Berthier and Sanders show how device-level state machine for smart meters could guide the set of valid behaviors monitored by the IDS sensors [129]. Hong *et al.* apply the idea of specification-based detection to multicast messages (GOOSE and SV) in a substation network [68]. They report a low false negative ratio. Kemal *et al.* [130] describe DoS, Integrity and Replay attack scenarios on voltage control in distribution network in the smart grid. For DoS scenario they developed anomaly detection based on offline data. Firewalls and IDS/IPS functionality sometimes can be combined into a single device. This option was studied by Yang *et al.* for synchrophasor systems [72]. IDS for different DoS scenarios related to IoT devices in SG are presented in [131].

IDSs collect the information required from devices called sensors. How and where these sensors are deployed in the network determines the IDS architecture. Grochocki *et al.* present four different alternatives; centralized IDS, embedded sensing, dedicated sensing and hybrid sensing for an SG deployment [62]. Recent paper [132] explains IDS implementation with deep learning anomaly detection for

PMU data. In [133] authors propose anomaly based detection of cyber attacks on load forecasting.

One of the challenges to make packet-level inspection with IDSs is the presence of encryption. Analysis of encrypted traffic is an active research area. It is also investigated for SG application scenarios, such as smart meter communications [134].

What is different in SG? In the literature, it was reported that signature-based approaches have limited effectiveness in SG deployments due to difficulty in designing accurate signatures for DoS attacks [129]. For applications involving homogeneous behavior such as those using smart meters, the development of the specification is relatively an easy task [129]. When the networks carry traffic for a limited number of applications, precise specification is shown to be a tractable problem [60]. In [135] authors present distributed attack detector that can based on estimated values detect false data injections that can lead to DoS attacks on smart meters. Delay-sensitive and time-critical operation requirement is another reason to consider employing an IDS/IPS specifically designed for the SG. In [136] authors gave brief overview on IDS/IPS systems that aim to secure AMI, SCADA, substations and synchrophasors.

A recent survey paper [137] provides a good summary of the machine learning techniques from the literature specifically addressing the false data attack detection in the Smart Grid in three categories: non-technical losses, state estimation, and load forecasting, where the non-technical loss is defined as the unauthorized and not billed energy consumption [138].

D. RATE LIMITING

The identification of the attack source is an intermediate step in the attack reaction process. If this is successfully performed, the next step could be to block the DoS traffic at its source [51]. However, there are two main challenges in IPv4 networks for reliable source identification. First, having no cryptographic protection, source addresses can be forged easily. Second, routers only know the next hop while forwarding a packet hence it is difficult to trace packet back to its real source [51].

A naive but widespread reaction to a DoS attack is to increase host and network resources. Smarter resource management strategies also do exist. For instance, by carefully analyzing whether the host or the network is the bottleneck, additional resources could be allocated more effectively.

If it is not possible to reliably distinguish DoS traffic from the legitimate one, rate limiting and fair scheduling could be an option as a DoS mitigation strategy.

Rate limiting could be implemented physically on a perimeter device, such as a reverse firewall for the egress traffic. We can also enforce rate limiting logically on the server machines.

Given the powerful server machines, traditionally, resource consumption on the client and the server side in a communication protocol is adjusted so that server undertakes a larger portion of the load. The DoS attack threat challenges this view. Client puzzles provide a relatively easy way for doing a readjustment so that the clients and thus attackers require more effort to interact with the server. They force the client to do a significant amount of work, and prove it has done so, before server will allocate resources for the client's request.

In a sense, well-known CAPTCHAs could also be considered as a rate-limiting tool for the applications which involve human interaction. Also known as Human Interaction Proofs, these simple tests aim at avoiding bot-generated automatic attacks. However, buying human computation to conduct a DoS attack against a CAPTCHA-protected site is not expensive.

The main disadvantage of rate limiting techniques is that attack traffic is still allowed although in a limited amount [49].

What is different in SG? Any arbitrary communication flow is possible on the Internet, whereas SG has two major directional flows (bottom-up and top-down [9]). As a result, rate-limiting (as well as filtering) is easier to implement. More intelligent rate limiting strategies could also exploit the fact that data transmission in SG applications is periodic. For instance, the frequency of metering reporting is less than 1 Hz [9] thus a higher rate is suspicious and could be limited without any side effect.

E. CRYPTOGRAPHIC AUTHENTICATION

In traditional cyber security view, availability and integrity are regarded as two distinct objectives. On the other hand, when cyber-physical systems are of concern, an attacker could indirectly disrupt the service by injecting erroneous messages and commands. Although we do not cover standard tools for integrity protection such as digital signatures here, we note that cryptography is a strong tool to detect and reject unauthorized messages injected by outsiders.

In a perfect world with the assumption that nodes are not compromised and where all communicating parties and their packets are cryptographically authenticated, many DoS attacks could be avoided. A crucial point here is the fact that the use of cryptography itself could be a target for a DoS attack. In other words, if the verification of the authenticity of a packet consumes a significant amount of resources, then an attacker could launch a successful attack by bogus packets. Designing cryptographic protocols to resist resource exhaustion attacks is not trivial [96]. Its efficiency is important even if it only expends a modest amount of resources in normal operation.

He *et al.* consider the case of PKI supported entity authentication in the SG. Since certificate verification and signature verification could be subject to a DoS attack, they propose the use of lightweight polynomial-based verification mechanism [139].

An example of previous studies which suggest the use of authentication against SG DoS attacks is the work by Anderson and Fuloria [140]. They warn against a scenario where an attacker remotely switches off residential power supply. The solution relies on cryptography to authenticate messages in the communication between the meter and headend. In their proposal, authentication is performed on the destination end. It is also possible to implement authentication in intermediate nodes, i.e., routers, but this might require a major change in the infrastructure.

What is different in SG? A notable challenge in employing cryptographic solutions in the SG is scalability of the key management. The standard PKI-based solutions designed for the Internet communication should be tailored to suit the needs of the SG environment [141]. A hybrid approach combining public and symmetric key techniques by forming interconnected trust realms could offer the desirable scalability properties [142].

Low-power devices in SG require the use of lightweight crypto primitives such as one-time signatures and hash chains. Long-lived devices, typical in power applications, demand the crypto to remain secure for a long period of time *e.g.,* 20 years. There is a more stringent performance requirement for cryptographic verification of delay-sensitive SG control messages.

F. PROTOCOL SOLUTIONS

The fact that Internet protocols such as IP and UDP/TCP were not designed with security in mind is the main reason why we have SG security problems today.[4] For instance, IEC 61580 has adopted TCP/IP as a part of its protocol stack. On the other hand, the communication protocols used in SG applications not inherited from the Internet such as DNP3 do not score much better. Secure versions such as IPv6 exist but transition is not straightforward due to the prevalence of systems that support only older versions.

There are SG security standards under development, such as IEC 62351 which deal with detecting DoS attacks among other security requirements [143].

In the literature, many new protocols, involving cryptographic authentication of communication partners, were proposed. Some of these pay particular attention to the efficiency requirements and use lightweight primitives [144]. There are also clever solutions to resist some specific DoS attacks while staying compatible to the standard. For instance, SYN cookies provide a solution to TCP SYN flood attacks using cryptographic hashing techniques.

What is different in SG? Unlike for the Internet, the future SG could have a heterogeneous protocol stack, which brings both risks as well as opportunities with respect to protocol solutions [9]. Since devices typically have a long lifetime, there is a need to design the SG protocols for evolvability, the ability to be updated or modified so that continued secure operation is ensured for a long period of time [6].

G. ARCHITECTURAL SOLUTIONS

Network topology affects the performance of networks and their survivability when they are under a DoS attack [145]. Other than the physical elements constituting the network, it is also possible to combat DoS attacks through a logical re-architecture. In 2004, Handley and Greenhalph proposed a set of architectural changes to the Internet which would greatly limit the scope of a DoS attack [146]. Specifically, they proposed IP addresses to be divided into a set of client addresses and a set of server addresses so that some of the reflector DoS attacks on servers are prevented. Although the proposed architecture has many merits, it was not adopted for the Internet, probably due to the difficulty of making a change to such a big infrastructure. One can argue that it could be much easier to consider such a radical solution for the upcoming SG networks. A fundamental redesign of routing infrastructure is another opportunity to design from the grounds up [13]. w The resilience of a SG network against DoS attacks could also be improved with Peer-to-Peer technologies which allow for the constructiwon of self-organizing, dependable and large-scale overlays on top of the existing physical networks [147].

Architectural solutions could provide redundancy; a well-known availability solution. As a potential example, we envisage a future scenario where power line communication is used when wireless communication is under a jamming attack.

What is different in SG? Users expect the Internet to provide the capability for end-to-end communication between any two points without any service disruption. However in a SG, in case of an external attack a subnetwork can automatically isolate itself and continue to operate as an *island* [148]. Islanding is a reliable and secure architectural solution matching especially well for requirements of power distribution networks [148]. In this regards, microgrids [149]–[152], defined as autonomous energy management systems under the control of a single administration authority that is capable of operating it in parallel to, or in intentional or accidental islanded mode from, the existing power grid, as a low voltage distribution power network [153], may provide a synergistic and powerful approach in isolating and islanding against DoS attacks.

H. HONEYPOTS

It is a recommended practice to have honeypots as part of SG systems. Honyepots are specifically designed devices that mimic the target of malicious attacks. They are used for the purpose of detecting, deflecting and analyzing attacks [13]. There are only a few honeypot implementations for SG environments. Buza *et al.* realized a honeypot that appears to be a Siemens PLC (programmable logic controller) from attackers point of view. Although their work is a worthy contribution to the literature, the inability to deploy it within an industrial control system's IP range limited its real-life data collection to evaluate the true potential [154]. Deployment of honeypots

[4] A simulation study is given in [95] which illustrates that a UDP flood attack could break down the whole electrical grid system.

into the AMI network as a decoy system is proposed with a game theoretic analysis of the interaction between the attackers and the defenders in [82]. Another honeypot approach was proposed in [154] as a realistic Programmable Logic Controller to guard and control industrial processes in conjunction with the control center.

What is different in SG? Although more work needs to be done to be conclusive, we argue that it is a challenging task to mimic real-world SG behavior which puts a limit on the benefits of SG honeypot deployments.

I. DEVICE SOLUTIONS

Many system software were developed without security considerations [35]. Exploitation of software vulnerabilities allows the control of large numbers of compromised SG devices. If sufficient number of compromised hosts can mimic legitimate traffic, then there is little that can be done against such a distributed attack, as the recent Mirai attack and its copy-cats showed [16]–[18]. Therefore, improving the security of the devices is essential for an effective DoS protection strategy. The following list incorporates relatively untapped promising new solutions useful in this regard for the SG applications: (1) Trusted computing: Among other features, trusted computing technology protects private keys stored on SG devices used for device authentication. It was argued that other key protection methods do not perform well for the SG due to the requirement of interaction with the user [155]. (2) Attestation: It is possible to verify remotely that the software installed on a SG device is not modified. It is more challenging to design such a protocol securely without using a dedicated hardware [156]. (3) Diversity: Homogeneity is arguably a mixed blessing. Standardization might lead to a greater homogeneity which make it an ideal target for DoS attacks [35]. Changing the device software to make it unique could prevent common failure modes exploitable to conduct a large scale distributed DoS attack [157]. (4) Secure bootstrapping: Secure initialization of a newly installed device is essential to avoid rogue devices in the network [148]. (5) Secure patching: Validating the integrity and authenticity of a software patch before installation can thwart attacks injecting malware through software patches [148].

What is different in SG? The following list presents the device-specific challenges in a SG environment: (1) Unattended operation: We cannot assume physical security for the SG devices deployed in the field, (2) Difficulty of patching: It is difficult if not impossible to patch legacy SG devices, (3) Low-end devices: Device solutions need to suit well with the limited computational capabilities of SG devices, (4) Economical factors: SG contains millions of devices hence it is certain that cost-efficiency will play a major role for security decisions.

J. WIRELESS-SPECIFIC SOLUTIONS

There are a number of advantages for using wireless communication in the SG [9]. However, as stated above, DoS attacks, especially when targeting lower layers, are particularly effective against wireless networks. These attacks are more harmful for distribution and transmission use cases where message delivery has stringent timing requirements. Solutions against these attacks fall into one of the following two categories [9]: (1) Efficient and robust detection: Presence of an attack could be detected by passive listening (e.g., RSSI measurements, packet loss). Proactively sending probe packets is also possible. (2) DoS-resilient schemes: These can be designed in either coordinated (using a shared secret between communicating parties) or uncoordinated (not requiring a pre-known secret) fashion.

What is different in SG? In SG applications (e.g., monitoring and control of devices in substations), where message delivery has strict delay requirements on the order of a few milliseconds, standard metrics quantifying the impact of jamming attacks are not sufficient.

Zhou *et al.* introduced a new metric called message invalidation ratio [92]. Using this new metric, they analyze a variety of different of attack scenarios together with a design and implementation of a jamming detection system.

K. SYSTEM-THEORETIC SOLUTIONS

Cyber attacks to SG networks may have physical consequences. Up to this point, we have seen many types of countermeasures against DoS attacks. However none of them consider physical aspects. System-theoretic approaches carry a big potential to take physical aspects also into account. They could model the attacks as component failures, external inputs or noises [127]. Security requirements, such as continuity of power delivery and accuracy of dynamic pricing, could be related to the models and states of the system [127].

There is a growing body of literature on system-theoretic approaches and could easily be the topic of a separate survey study. For brevity, we only cover a subset of these studies below.

It was discovered that if the configuration of the power system is known by the attacker all standard techniques for bad measurement detection can be bypassed because these techniques depend on the assumption that ‘‘when bad measurements take place, the squares of differences between the observed measurements and their corresponding estimates often become significant’’ [98], [158]. The seminal paper on this topic by Liu *et al.* indicates that this assumption is not true in case there is an attack. With the knowledge of the power system configuration information, one can systematically generate bad data measurements while bypassing the detection [98].

A hybrid control system could be built by combining the traditional cyber view with the consideration of physical operation for potentially damaging commands [159].

Vukovic and Dan propose an algorithm to detect a false injection attack to distributed power state estimation that has DoS consequences by identifying discrepancies in the temporal evolution of the exchanged data between regions [90]. They also propose a distributed algorithm to mitigate the attack which identifies the region with the compromised

TABLE 5. DoS solutions and their SG specific properties.

Non-technical	sector-specific standards
Filtering	bump-in-the-wire firewall required for legacy devices
IDS/IPS	specification-based approaches suitable
Rate Limit	predictable periodic flows
Crypto. Auth.	scalability of key mngt., lightweight crypto to remain secure for long time
Protocol	design for evolvability
Architectural	islanding option available
Honeypots	difficult to mimic real-world SG behavior
Device	unattended operation, difficulty of patching, low-end devices, economical factors
Wireless-specific	strict delay req., need for new metrics
System-theoretic	N/A

TABLE 6. A comparison of DoS attacks versus proposed solutions. ○: not viable, ◐: partially viable, ◗: complementary, ●: viable.

Solutions	**DoS Attacks**						
	Jamming	Res. Exhaus.	Crypto	Data	De-Synch.	Routing	Reflector
Filtering	[128]	[72], [128]	○	[128]	●	[128]	◐
IDS/IPS	[60]	[60], [68], [74], [129]	○	[68], [72], [129]	[68], [72]	[60]	●
Rate Limit	◗	●	◗	◗	◗	○	◗
Crypto. Auth.	○	[139], [142], [143]	◐	[85], [140]	◐	◐	◐
Protocol	●	[143], [144]	[96]	[80], [106], [143], [144], [167]	●	[81], [87]	●
Architectural	●	[147], [148]	○	[148]	[148]	[148]	◐
Honeypots	◗	[154]	◗	◗	◗	◗	◗
Device	○	[155], [157]	○	[155]	◗	◗	◗
Wireless-specific	[92]	[92], [128]	○	[128]	[92]	◐	◐
System-theoretic	[91], [93], [168]	[159]	◐	[85], [86], [90], [127], [159], [162]	[46], [159]	[159]	◐

control center by consolidating the beliefs of the individual regions about the origin of the attack.

Du *et al.* modified IEEE 118-bus test system in order to present their method ADMM based method for state estimation to ensure resilient SG state estimation [160] under combined DoS and Data Deception attacks. Pan et. al give the risk analysis of combined attacks against power system state estimation [161].

Li *et al.* proposed a sequential detector based on the generalized likelihood ratio to address the challenge of robust and efficient detection of malicious data injection to the monitoring meters to manipulate the state estimation [162].

Wang and Govindarasu proposed multi-agent based solution that could help mitigate DoS attacks directed to load shedding. The proposed solution is decentralized and every agent makes its own decision using anomaly detection while final decision depends on the consensus of all connected agents [163].

Against voltage control availability, [164] proposes a self-organizing multi-agent Service Oriented Architecture (SOA) with a decision making rule-set in order to mitigate DoS attacks.

A fallback control strategy is introduced in [165] to mitigate Dos attacks targeting the Energy Storage System (ESS) frequency through a decentralized state-of-charge (SOC) management algorithm in islanded microgrids.

Kumari and Shankar propose Euclidian based detector of cyber attack on AGC. Kalman filter is used to estimate values of measurements in AGC. Estimated values are compared with true measurements. The threshold is defined to be higher than value of Euclidian distance. If deviation between is greater than threshold than possible attack is detected [166].

Table 5 summarizes SG specifics of DoS solutions.

VIII. DISCUSSION

Table 6 shows the comparison of DoS attacks versus DoS solutions, as a birds-eye-view synopsis of our work. Below, we briefly discuss details of this table.

We first note that although we tried our best while filling this table a perfect distinction was not always possible. Hence, there is a good deal of subjectivity in the table.

Filtering could be used against certain jamming attacks [55] as demonstrated in [128]. Filtering is the de-facto standard mechanism against resource exhaustion attacks. Crypto attacks could not be avoided by filtering since firewalls do not have the capability to inspect packets based on their cryptographic properties. Although not specifically discussed in the literature, filtering could be used against de-synchronization attacks. Suppose the time source for the network is in the local network, a perimeter firewall could easily block fake timing packets coming from outside. Perimeter defense is helpless against most routing attacks but host-based filtering combined with exchanged alarm messages [128] could prevent malicious nodes to participate in the routing protocol. Finally, reflector attacks could be blocked by egress filtering implemented on a perimeter firewall if the attacker and the victim are not in the same network.

Previously, we have distinguished the meanings and functionality of firewalls and IDS/IPS. Although IDS/IPS is regarded as a more sophisticated defense mechanism, it is similar to firewalls in the sense that the kind of DoS attacks it could be used against are broadly similar. The key difference is the fact that some attacks could be avoided by an IDS/IPS but not by firewalls. For instance suppose the attacker conducts a reflector attack to a victim machine and the server is reached through an IDS/IPS. If the number of packets sent to the server reaches a threshold value, an alarm could easily be triggered.

As mentioned, if DoS traffic could not be distinguished from the legitimate one, rate limiting is left as the mitigation option. Although, not specifically proposed in the literature, rate limiting can be used in support of filtering and IDS/IPS devices by defining additional policy rules. Among all the other types of DoS attacks, its potential is the biggest against resource exhaustion attacks. However, rate limiting is not applicable against routing attacks, such as the blackhole attacks.

We consider "jamming" as attacks only in the physical layer. Therefore, cryptographic authentication is not useful against jamming attacks. Crypto-attacks could not be totally avoided by cryptographic authentication but can be mitigated using lightweight crypto primitives. Most of the time, de-synchronization, routing and reflector attacks are possible due to spoofing. Cryptographic authentication is the de-facto solution against spoofing. It works unless the devices are compromised. Although not specifically designed for the SG, coordinated and uncoordinated protocols can be used against jamming [128]. Protocol solutions could be applied against all SG DoS attacks. However, designing a secure communication protocol is not an easy task. We should first consider using already available proven solutions unless coming up with a special design for SG is a necessity. We should also learn from previous mistakes [6]. Against jamming attacks, use of wired instead of wireless communication is an extreme example for an architectural solution. The network architecture is not relevant against crypto attacks. Some of the reflector attacks could be addressed by a logical re-architecture [146]. In [169] authors propose wireless specific solution that determines packet drop ratio in order to detect compromised nodes during the routing attacks. Confusing the target, honeypots are generic DoS countermeasures. However, it could not be the single solution against any of the attack since the attacker could always attack the real target at the same time. Upon detection by the honeypots, it is important to take proper actions at the right time.

Device solutions prevent the attackers to compromise the SG devices. They are not effective against jamming and crypto attacks since these attacks could be performed using external devices. Device solutions and cryptographic authentication complement each other and provide a perfect solution against many different kinds of DoS attacks. In other words, if the devices are authenticated and uncompromised, then we could always distinguish between real and DoS traffic.

Jamming attacks are the natural target for wireless-specific solutions. However, the ability to listen nearby wireless communication by special "watchdog" nodes is proven useful against some other types of DoS attacks including routing and reflector attacks.

If we could model the effects of crypto attacks and reflector attacks at a system level, system-theoretic solutions could even be applied to these sophisticated cyber attacks.

IX. CONCLUSION AND FUTURE WORK

In this review study, we have focused on an important dimension of the SG cybersecurity: DoS attacks and solutions. As a critical infrastructure, the SG is emerging as a prime target for attack and DoS vulnerabilities are raising serious concerns. To the best of our knowledge, the literature does not seem to have any other study like ours in terms of the scope and coverage. In order to make this survey paper self-contained, we provide the necessary and the most relevant coverage of the power grid characteristics to set the stage for, and contextualize, the SG DoS attacks. We also bring in a synopsis of the state-of-the-art Dos from the Internet domain as a prelude to potential solutions to DoS attacks in the SG.

We provide a synopsis of high-level key insights from Table 6 and previous discussion here again:

1) Filtering and IDS/IPS systems are powerful tools against Smart Grid DoS attacks. Rate limiting, not explicitly discussed for SG in the literature, could be integrated into these solutions to comply with the "defense-in-depth" principle.
2) Cryptographic, communications protocol-based and architectural solutions carry an immense potential. However, their true potential could only be realized after the standardization efforts succeed.
3) The underlying reason for many security vulnerabilities, including DoS attacks, boils down to the inherent insecure behavior of the system software; especially at the OS kernel level.
4) While there are brilliant approaches to tackle the challenges, neither cyber security professionals nor system and power researchers alone have the expertise to address all availability challenges posed by the SG. There is definitely a need to bring interdisciplinary teams together to have a structured, methodical, holistic, and comprehensive view of the DoS problem.

Finally, we elaborate below on challenges faced and future opportunities for research directions:

- Communications and networking infrastructure should be enhanced with additional or new security mechanisms regarding data collection and interchange.
- Most of standards defined for power grid are proprietary. Open standards could be helpful in replacing security implemented through obscurity principle.
- Because of the economical aspects, it should also be accounted that existing low power processing devices participating in the Smart Grid should be replaced in

small steps, rather than being replaced at once. These evolutionary steps could also be implemented in a way to upgrade existing infrastructure by introducing new nodes that have more processing power.

- Upgrades to the current Smart Grid implementation should include distributed data collection and interchange mechanisms. This could potentially decrease DoS effect by localizing it in specific part(s) of the Smart Grid.
- DoS attacks on the Smart Grid may result in physical consequences. Most of the solutions that have been presented in this study do not consider physical aspects of the Smart Grid. This could be a good starting point in developing new security mechanisms.
- Devices that run in the Smart Grid in most cases have software that were not designed to be secure. Since upgrade of the applications is not always possible, researchers might propose new solutions that add security layer on the top of already deployed devices.
- Implementing security measures, as noted in earlier sections, is more a process of implementing various methods that include not only a technical solution but rather interdisciplinary approaches. The focus for future research could be the analysis of measures applied in this process, and creating as much as possible technical solution that minimize the non-technical influence.
- An exponentially expanding threat vector from IoT devices poses a formidable challenge in cybersecurity, especially for critical infrastructure like the Smart Grid. Various factors make securing these inexpensive IoT devices quite hard. First, the thin profit margins do not provide enough incentives for the manufacturers to invest in effective strategies and approaches. The consumers, even the technically sophisticated ones, to a large extent do not put an effort to harden IoT security at the edge of the networks. Economical and financial incentives for both the manufacturers as well as the end users should be developed to address these challenges; some of these may be technical, and some may be more of policy-based.
- Computationally limited and resource-constrained IoT devices require new paradigms and approaches that would be feasible within the low complexity capabilities of these IoT devices. Memory, processing, as well as the communications complexities of the approaches must take the device capabilities, especially the IoT devices, into considerations for feasible solutions.
- Cyberwarfare has already become a very powerful tool for some nation states. As mentioned the Smart Grid is a top and very attractive target. More concerted efforts and funding to secure these critical infrastructures are in the best interest of the policy-makers.
- Machine learning techniques, as noted in a very recent survey in [137] in a rather limited scope, provide promising solution potential. However, it is critical to consider the peculiarities of the Smart Grid when adopting the machine learning techniques, rather than applying in an agnostic manner with likely limited success.
- While the techniques developed over the past few decades against cyber attacks in the Internet are applicable to a certain extent as noted throughout our survey, we note one more time with a strong emphasis that SG has differing characteristics that must be meticulously considered when adopting as well as developing solutions.
- Again especially in light of the proliferating IoT devices and the computational upgrade of the Smart Grid, a deluge of data is being generated. It is not surprising to have the mentioning of the Smart Grid as one of the pinnacle domains for big data. As a result, many of the big data techniques and research developed for other domains may have immediate and direct application to the Smart Grid. Or, they may serve as excellent stepping stones for developing more customized solutions with some additional effort.

REFERENCES

[1] (2008). *The Smart Grid: An Introduction*. [Online]. Available: https://www.energy.gov/oe/downloads/smart-grid-introduction-0

[2] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, Jan. 2010. [Online]. Available: http://ieeexplore.ieee.org/document/5357331/

[3] M. Amin, "Smart grid," *Public Utilities Fortnightly*, Mar. 2015. [Online]. Available: https://www.fortnightly.com/fortnightly/2015/03/case-smart-grid

[4] S. F. Bush, *Smart Grid: Communication-Enabled Intelligence for the Electric Power Grid*. Hoboken, NJ, USA: Wiley, 2014. [Online]. Available: http://books.google.com/books?id=bUSMAgAAQBAJ

[5] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May/Jun. 2009.

[6] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine, "Design principles for power grid cyber-infrastructure authentication protocols," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, 2010, pp. 1–10.

[7] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010. [Online]. Available: http://ieeexplore.ieee.org/document/5460903/

[8] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.

[9] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128613000042

[10] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, 4th Quart., 2012.

[11] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: Cyber attacks, countermeasures, and challenges," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 38–45, Aug. 2012.

[12] Y. Xiao, *Security Privacy Smart Grids*. New Delhi, India: Taylor & Francis, 2013. [Online]. Available: http://books.google.com/books?id=QQ2oY0IrRM8C

[13] Y. Victoria Pillitteri and L. Tanya Brewer, "NISTIR 7628 revision 1, guidelines for smart grid cybersecurity," in *Proc. Smart Grid Interoperability Panel (SGIP)*, Sep. 2014, p. 668. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[14] A. Abdallah, "Security and privacy in smart grid," Ph.D. dissertation, Elect. Comput. Eng., Univ. Waterloo, Waterloo, CA, USA, 2016. [Online]. Available: http://hdl.handle.net/10012/10636

[15] E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*. Amsterdam, The Netherlands: Elsevier, 2013. [Online]. Available: http://books.google.com/books?id=_9GzAzehLLUC

[16] M. Antonakakis, ''Understanding the mirai botnet,'' in *Proc. USENIX Secur. Symp.*, 2017, pp. 1092–1110.

[17] N. Vlajic and D. Zhou, ''IoT as a land of opportunity for DDoS hackers,'' *Computer*, vol. 51, no. 7, pp. 26–34, Jul. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8423144/

[18] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ''DDoS in the IoT: Mirai and other botnets,'' *Computer*, vol. 50, no. 7, pp. 80–84, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7971869/

[19] The President's National Infrastructure Advisory Council. (Dec. 2018). *Surviving a Catastrophic Power Outage*. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/NIAC%20 Catastrophi%c%20Power%20Outage%20Study_508%20FINAL.pdf

[20] N. Kshetri and J. Voas, ''Hacking power grids: A current problem,'' *Computer*, vol. 50, no. 12, pp. 91–95, Dec. 2017. [Online]. Available: http://ieeexplore.ieee.org/document/8220480/

[21] World Economic Forum. (2018). *The Global Risks Report 2018 13th Edition*. [Online]. Available: http://wef.ch/risks2018

[22] M. P. Barrett, ''Framework for improving critical infrastructure cybersecurity version 1.1,'' Nat. Inst. Standards Technol. (NIST), Gaithersburg, MD, USA, Tech. Rep. NIST.CSWP.04162018, Apr. 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[23] M. J. Assante. (Jan. 2016). *Confirmation of a Coordinated Attack on the Ukrainian Power Grid*. [Online]. Available: https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on%-the-ukrainian-power-grid

[24] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, ''The 2015 ukraine blackout: Implications for false data injection attacks,'' *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7752958/

[25] T. Maynard and N. Beecroft. (May 2015). *Business Blackout*. [Online]. Available: https://www.lloyds.com/news-and-insight/risk-insight/library/society-an%d-security/business-blackout

[26] A. Huseinovic, S. Mrdovic, K. Bicakci, and S. Uludag, ''A taxonomy of the emerging Denial-of-Service attacks in the smart grid and countermeasures,'' in *Proc. 26th Telecommun. Forum (TELFOR)*, Nov. 2018, pp. 1–4.

[27] E. Hossain, Z. Han, and H. V. Poor, *Smart Grid Communication Networks* (Smart Grid Communications and Networking). Cambridge, U.K.: Cambridge Univ. Press, 2012. [Online]. Available: http://books.google.com/books?id=C7yI1cn1trwC

[28] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, ''A survey on smart grid communication infrastructures: Motivations, requirements and challenges,'' *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 5–20, 1st Quart., 2013.

[29] W. Wang, Y. Xu, and M. Khanna, ''A survey on the communication architectures in smart grid,'' *Comput. Netw.*, vol. 55, no. 15, pp. 3604–3629, Oct. 2011.

[30] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen, ''A survey of communication/networking in smart grids,'' *Future Gener. Comput. Syst.*, vol. 28, no. 2, pp. 391–404, Feb. 2012.

[31] K. A. Stouffer, J. A. Falco, and K. A. Scarfone. (2011). *SP 800-82. Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC)*. [Online]. Available: https://dl.acm.org/citation.cfm?id=2206293

[32] K. C. Budka, J. G. Deshpande, and M. Thottan, *Communication Networks for Smart Grids: Making Smart Grid Real*. Cham, Switzerland: Springer, 2014.

[33] N. W. Miller, B. Leonardi, R. D'Aquila, and K. Clark, ''Western Wind and Solar Integration Study Phase 3A: Low Levels of Synchronous Generation,'' National Renewable Energy Laboratory, Gaithersburg, MD, USA, Tech. Rep. NREL/TP-5D00-64822, 2015.

[34] The North American Electric Reliability Corporation (NERC). (Jan. 2011). *NERC Balancing and Frequency Control*. [Online]. Available: https://www.nerc.com/comm/OC/RS_Related_Resources/NERC%20Balancing%20an%d%20Frequency%20Control%20040520111.pdf

[35] S. Goel and Y. Hong, *Smart Grid Security*. London, U.K.: Springer, 2015, pp. 1–39. [Online]. Available: http://dx.doi.org/10.1007/978-1-4471-6663-4_1

[36] Y. Wu, B. Chen, J. Weng, Z. Wei, X. Li, B. Qiu, and N. Liu, ''False load attack to smart meters by synchronously switching power circuits,'' *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2641–2649, May 2019.

[37] M. A. Rahman, M. S. Rana, and H. R. Pota, ''Mitigation of frequency and voltage disruptions in smart grid during cyber-attack,'' *J. Control, Autom. Electr. Syst.*, vol. 31, no. 2, pp. 412–421, Apr. 2020.

[38] B. A. Carreras, D. E. Newman, and I. Dobson, ''North American blackout time series statistics and implications for blackout risk,'' *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4406–4414, Nov. 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7378330/

[39] P. Pourbeik, P. S. Kundur, and C. W. Taylor, ''The anatomy of a power grid blackout–Root causes and dynamics of recent major blackouts,'' *IEEE Power Energy Mag.*, vol. 4, no. 5, pp. 22–29, Sep. 2006. [Online]. Available: http://ieeexplore.ieee.org/document/1687814/

[40] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal, ''Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance,'' *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005. [Online]. Available: http://ieeexplore.ieee.org/document/1525122/

[41] J. Romero, ''Blackouts illuminate India's power problems,'' *IEEE Spectr.*, vol. 49, no. 10, pp. 11–12, Oct. 2012. [Online]. Available: http://ieeexplore.ieee.org/document/6309237/

[42] X. Fang, S. Misra, G. Xue, and D. Yang, ''Smart grid — The new and improved power grid: A survey,'' *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, Qua. 2012. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6099519

[43] H. Gharavi and R. Ghafurian, ''Smart grid: The electric energy system of the future [Scanning the Issue],'' *Proc. IEEE*, vol. 99, no. 6, pp. 917–921, Jun. 2011, doi: 10.1109/jproc.2011.2124210.

[44] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, and C.-F. Covrig, ''A survey on the critical issues in smart grid technologies,'' *Renew. Sustain. Energy Rev.*, vol. 54, pp. 396–405, Feb. 2016.

[45] (Sep. 2014). *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.1108r3

[46] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. M. Begovic, and A. Phadke, ''Wide-area monitoring, protection, and control of future electric power networks,'' *Proc. IEEE*, vol. 99, no. 1, pp. 80–93, Jan. 2011. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5549870

[47] R. K. C. Chang, ''Defending against flooding-based distributed denial-of-service attacks: A tutorial,'' *IEEE Commun. Mag.*, vol. 40, no. 10, pp. 42–51, Oct. 2002.

[48] A. D. Wood and J. A. Stankovic, ''Denial of service in sensor networks,'' *Comput.*, vol. 35, no. 10, pp. 54–62, Dec. 2002.

[49] J. Mirkovic and P. Reiher, ''A taxonomy of DDoS attack and DDoS defense mechanisms,'' *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, Apr. 2004.

[50] J. Mölsä, ''Mitigating denial of service attacks: A tutorial,'' *J. Comput. Secur.*, vol. 13, no. 6, pp. 807–837, Dec. 2005. [Online]. Available: http://dl.acm.org/citation.cfm?id=1140814.1140815

[51] T. Peng, C. Leckie, and K. Ramamohanarao, ''Survey of network-based defense mechanisms countering the DoS and DDoS problems,'' *ACM Comput. Surveys*, vol. 39, no. 1, p. 3, Apr. 2007.

[52] M. Abliz, ''Internet denial of service attacks and defense mechanisms,'' Dept. Comput. Sci., Univ. Pittsburgh, Pittsburgh, PA, USA, Tech. Rep. TR-11-178, Marc. 2011. [Online]. Available: https://people.cs.pitt.edu/ mehmud/docs/abliz11-TR-11-178.pdf

[53] S. T. Zargar, J. Joshi, and D. Tipper, ''A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks,'' *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2046–2069, 4th Quart., 2013.

[54] M. Masdari and M. Jalali, ''A survey and taxonomy of DoS attacks in cloud computing,'' *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3724–3751, Nov. 2016. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1539

[55] P. Alcoy, P. Bowen, C. Chui, S. Bjarnason, K. Kasavchenko, G. Sockrider, and D. Anstee, (2018). *Arbor's 13th Annual Worldwide Infrastructure Security Report*. [Online]. Available: https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_In%frastructure_Security_Report.pdf

[56] Netscout. (2019). *Arbor's 14th Annual Worldwide Infrastructure Security Report*. [Online]. Available: https://www.netscout.com/report

[57] Akamai Security Research. (2018). *State of The Internet, Summer 2018*. [Online]. Available: http://www.akamai.com/stateoftheinternet-security

[58] *Threat Landscape Report—Q1 2020*, A. inc. New Delhi, India, 2020.

[59] J. Pescatore, "Ddos attacks advancing and enduring: A sans survey," SANS, Boston, MA, USA, Tech. Rep. 8856130, 2014.

[60] R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 350–355. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5622068

[61] J. D. Taft, "Assessment of Existing Synchrophasor Networks (PNNL-27557)," Pacific Northwest Nat. Lab. (PNNL), Richland, WA, USA, Tech. Rep. PNNL-27557, Apr. 2018. [Online]. Available: https://www.naspi.org/node/723

[62] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. Cardenas, and J. G. Jetcheva, "AMI threats, intrusion detection requirements and deployment recommendations," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2012, pp. 395–400.

[63] 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 Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2886–2927, 3rd Quart., 2019.

[64] M. Attia, S. M. Senouci, H. Sedjelmaci, E.-H. Aglzim, and D. Chrenko, "An efficient intrusion detection system against cyber-physical attacks in the smart grid," *Comput. Electr. Eng.*, vol. 68, pp. 499–512, May 2018.

[65] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128619311235

[66] S. Ahmed and F. M. Dow, "Electric vehicle technology as an exploit for cyber attacks on the next generation of electric power systems," in *Proc. 4th Int. Conf. Control Eng. Inf. Technol. (CEIT)*, Dec. 2016, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/document/7929019/

[67] S. N. Islam, Z. Baig, and S. Zeadally, "Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6522–6530, Dec. 2019.

[68] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in *Proc. ISGT*, Feb. 2014, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6816375

[69] D. Jin, Y. Zheng, H. Zhu, D. M. Nicol, and L. Winterrowd, "Virtual time integration of emulation and parallel simulation," in *Proc. ACM/IEEE/SCS 26th Workshop Princ. Adv. Distrib. Simul.*, Jul. 2012, pp. 201–210. [Online]. Available: http://dl.acm.org/citation.cfm?id=2372596.2372597

[70] S. Rana, H. Zhu, C. W. Lee, D. M. Nicol, and I. Shin, "The Not-So-Smart grid: Preliminary work on identifying vulnerabilities in ANSI C12.22," in *Proc. IEEE Globecom Workshops*, Dec. 2012, pp. 1514–1519. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6477810

[71] T. H. Morris, S. Pan, and U. Adhikari, "Cyber security recommendations for wide area monitoring, protection, and control systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2012, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6345127

[72] Y. Yang, H. F. Wang, B. Pranggono, K. McLaughlin, S. Sezer, P. Brogan, and T. Littler, "Intrusion detection system for network security in synchrophasor systems," in *Proc. IET Int. Conf. Inf. Commun. Technol. (IETICT)*, 2013, pp. 246–252.

[73] M. A. Hasnat and M. Rahnamay-Naeini, "A data-driven dynamic state estimation for smart grids under DoS attack using state correlations," in *Proc. North Amer. Power Symp. (NAPS)*, Oct. 2019, pp. 1–6.

[74] K. Choi, X. Chen, S. Li, M. Kim, K. Chae, and J. Na, "Intrusion detection of NSM based DoS attacks using data mining in smart grid," *Energies*, vol. 5, no. 10, pp. 4091–4109, Oct. 2012.

[75] D. Jin, D. M. Nicol, and G. Yan, "An event buffer flooding attack in DNP3 controlled SCADA systems," in *Proc. Winter Simul. Conf. (WSC)*, Dec. 2011, pp. 2614–2626.

[76] D. Gogic, B. Jelacic, and I. Lendak, "Simulation-based evaluation of DDOs against smart grid scadas," in *Computer Security*. Cham, Switzerland: Springer, 2019, pp. 86–97.

[77] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2013. [Online]. Available: http://ieeexplore.ieee.org/document/6298960/

[78] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," *Comput. Netw.*, vol. 56, no. 11, pp. 2741–2771, Jul. 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128612001429

[79] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. H. Chin, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 21–38, 1st Quart., 2013.

[80] W. G. Temple, B. Chen, and N. O. Tippenhauer, "Delay makes a difference: Smart grid resilience under remote meter disconnect attack," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Oct. 2013, pp. 462–467. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6688001

[81] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and L. Pan, "Puppet attack: A denial of service attack in advanced metering infrastructure network," *J. Netw. Comput. Appl.*, vol. 59, pp. 325–332, May 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804515000880

[82] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic honeypot game model for distributed denial of service attacks in the smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2474–2482, Sep. 2017.

[83] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-Service (dos) attacks on load frequency control in smart grids," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2013, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6497846

[84] Y. Li, P. Zhang, and L. Ma, "Denial of service attack and defense method on load frequency control system," *J. Franklin Inst.*, vol. 356, no. 15, pp. 8625–8645, Oct. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0016003219306106

[85] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-based load altering attacks against smart power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec. 2011. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5976424

[86] Y. Li, R. Wang, P. Wang, D. Niyato, W. Saad, and Z. Han, "Resilient PHEV charging policies under price information attacks," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2012, pp. 389–394.

[87] J. Wei and D. Kundur, "A flocking-based model for DoS-resilient communication routing in smart grid," in *Proc. IEEE Global Commun. Conf.*, Dec. 2012, pp. 3519–3524. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6503660

[88] K. Demir and N. Suri, "Towards ddos attack resilient wide area monitoring systems," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, New York, NY, USA, 2017, pp. 1–7. [Online]. Available: https://doi.org/10.1145/3098954.3103164

[89] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT Botnet of high wattage devices can disrupt the power grid," in *Proc. 27th Secur. Symp.*, 2018, pp. 15–32.

[90] O. Vukovic and G. Dan, "Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1500–1508, Jul. 2014. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6840318

[91] J. Ma, Y. Liu, L. Song, and Z. Han, "Multiact dynamic game strategy for jamming attack in electricity market," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2273–2282, 2015.

[92] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1746–1759, Aug. 2014. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6654149

[93] H. Li, L. Lai, and R. C. Qiu, "A denial-of-service jamming game for remote state monitoring in smart grid," in *Proc. 45th Annu. Conf. Inf. Sci. Syst.*, Mar. 2011, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5766137

[94] F. M. Cleveland, "Cyber security issues for advanced metering infrasttructure (AMI)," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2008, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4596535

[95] S. Asri and B. Pranggono, "Impact of distributed denial-of-service attack on advanced metering infrastructure," *Wireless Pers. Commun.*, vol. 83, pp. 2211–2223, Mar. 2015. [Online]. Available: http://link.springer.com/10.1007/s11277-015-2510-3

[96] V. Kolesnikov and W. Lee, "MAC aggregation protocols resilient to DoS attacks," *IEEE SmartGridComm*, vol. 7, no. 2, pp. 226–231, 2011. [Online]. Available: http://inderscience.metapress.com/index/XW8541375106697V.pdf

[97] W. Meng, R. Ma, and H.-H. Chen, "Smart grid neighborhood area networks: A survey," *IEEE Netw.*, vol. 28, no. 1, pp. 24–32, Jan. 2014. [Online]. Available: http://ieeexplore.ieee.org/document/6724103/

[98] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inform. System Secur.*, vol. 14, no. 1, p. 13, 2011.

[99] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011. [Online]. Available: http://ieeexplore.ieee.org/document/6032057/

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

[101] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power Systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[102] M. Zhou, Y. Wang, A. K. Srivastava, Y. Wu, and P. Banerjee, "Ensemble-based algorithm for synchrophasor data anomaly detection," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2979–2988, May 2019.

[103] Y. Li, Y. Wang, and S. Hu, "Online generative adversary network based measurement recovery in false data injection attacks: A cyber-physical approach," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2031–2043, Mar. 2020.

[104] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest," *IEEE Trans. Inf. Forensics Securtiy*, vol. 14, no. 10, pp. 2765–2777, Oct. 2019.

[105] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2158–2169, Mar. 2019.

[106] I. Doh, J. Lim, and K. Chae, "Secure aggregation and attack detection for smart grid system," in *Proc. 16th Int. Conf. Network-Based Inf. Syst.*, Sep. 2013, pp. 270–275. [Online]. Available: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6685408

[107] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6400273

[108] B. Moussa, M. Debbabi, and C. Assi, "A detection and mitigation model for PTP delay attack in an IEC 61850 substation," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 3954–3965, Sep. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/7797198/

[109] M. S. Almas, L. Vanfretti, R. S. Singh, and G. M. Jonsdottir, "Vulnerability of synchrophasor-based WAMPAC Applications' to time synchronization spoofing," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4601–4612, Sep. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/7845713/

[110] S. B. Andrade, J.-Y. Le Boudec, E. Shereen, G. Dan, M. Pignati, and M. Paolone, "A continuum of undetectable timing-attacks on PMU-based linear state-estimation," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Oct. 2017, pp. 473–479. [Online]. Available: http://ieeexplore.ieee.org/document/8340673/

[111] B. Moussa, M. Debbabi, and C. Assi, "Security assessment of time synchronization mechanisms for the smart grid," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1952–1973, 3rd Quart., 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7397831/

[112] P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore, and R. S. Blum, "GPS spoofing attack characterization and detection in smart grids," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2016, pp. 391–395. [Online]. Available: http://ieeexplore.ieee.org/document/7860525/

[113] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2659–2668, Nov. 2015. [Online]. Available: http://ieeexplore.ieee.org/document/6887343/

[114] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Dominguez-Garcia, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3253–3262, Aug. 2013. [Online]. Available: http://ieeexplore.ieee.org/document/6451170/

[115] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability analysis of smart grids to GPS spoofing," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3535–3548, Jul. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8347144/

[116] Y. Liang, D. He, and D. Chen, "Poisoning attack on load forecasting," in *Proc. IEEE Innov. Smart Grid Technol.*, May 2019, pp. 1230–1235.

[117] Y. Chen, Y. Tan, and B. Zhang, "Exploiting vulnerabilities of load forecasting through adversarial attacks," in *Proc. 10th ACM Int. Conf. Future Energy Syst.*, New York, NY, USA, Jun. 2019, pp. 1–11, doi: 10.1145/3307772.3328314.

[118] S. Hoffmann and G. Bumiller, "Identification and simulation of a denial-of-sleep attack on open metering system," in *Proc. IEEE PES Innov. Smart Grid Technol. Eur.*, Sep. 2019, pp. 1–5.

[119] E. N. Yrlmaz, H. H. Sayan, F. Ustunsoy, S. Gonen, and G. Karacayilmaz, "Cyber security analysis of DoS and MitM attacks against PLCs used in smart grids," in *Proc. 7th Int. Istanbul Smart Grids Cities Congr. Fair (ICSG)*, Apr. 2019, pp. 36–40.

[120] E. Aroms, "Nist special publication 800-53 revision 3 recommended security controls for federal information systems and organizations," U.S. Dept. Homeland Secur., Washington, DC, USA, Tech. Rep. 2016-09, 2012.

[121] *Recommended Practice: Improving Industrial Control Systems Cybersecurity With Defense-In-Depth Strategies*, US-CERT Defense In Depth, Washington, DC, USA, 2009.

[122] (Sep. 2016). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)*.[Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/recommended_practic%es/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[123] M. A. Keith Stouffer, V. Pillitteri, S. Lightman, and A. Hahn. (May 2005). *National Institute of Standards and Technology Special Publication 800-82, Revision 2, Guide to Industrial Control Systems (ICS) Security*. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-82r2

[124] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet Comput.*, vol. 10, no. 1, pp. 82–89, Jan. 2006.

[125] T. Shawly, J. Liu, N. Burow, S. Bagchi, R. Berthier, and R. B. Bobba, "A risk assessment tool for advanced metering infrastructures," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Nov. 2014, pp. 989–994. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7007777

[126] M. A. Rahman, E. Al-Shaer, and P. Bera, "A noninvasive threat analyzer for advanced metering infrastructure in smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 273–287, Mar. 2013.

[127] Y. Mo, T. Hyun-Jin Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–Physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[128] X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 809–818, Dec. 2011.

[129] R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *Proc. IEEE 17th Pacific Rim Int. Symp. Dependable Comput.*, Dec. 2011, pp. 184–193. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6133080

[130] M. S. Kemal, W. Aoudi, R. L. Olsen, M. Almgren, and H.-P. Schwefel, ''Model-free detection of cyberattacks on voltage control in distribution grids,'' in *Proc. 15th Eur. Dependable Comput. Conf. (EDCC)*, Sep. 2019, pp. 171–176.

[131] Y. Yälmaz and S. Uludag, ''Timely detection and mitigation of IoT-based cyberattacks in the smart grid,'' *J. Franklin Inst.*, 2019, [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0016003219301413, doi: 10.1016/j.jfranklin.2019.02.011.

[132] J. Wang, D. Shi, Y. Li, J. Chen, H. Ding, and X. Duan, ''Distributed framework for detecting PMU data manipulation attacks with deep autoencoders,'' *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4401–4410, Jul. 2019.

[133] M. Cui, J. Wang, and M. Yue, ''Machine learning-based anomaly detection for load forecasting under cyberattacks,'' *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5724–5734, Sep. 2019.

[134] R. Berthier, D. I. Urbina, A. A. Cardenas, M. Guerrero, U. Herberg, J. G. Jetcheva, D. Mashima, J. H. Huh, and R. B. Bobba, ''On the practicality of detecting anomalies with encrypted traffic in AMI,'' in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2014, pp. 890–895. [Online]. Available: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=7007761

[135] M. N. Kurt, Y. Yilmaz, and X. Wang, ''Distributed quickest detection of cyber-attacks in smart grid,'' *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2015–2030, Aug. 2018.

[136] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, ''Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems,'' *IEEE Access*, vol. 7, pp. 46595–46620, 2019.

[137] L. Cui, Y. Qu, L. Gao, G. Xie, and S. Yu, ''Detecting false data attacks using machine learning techniques in smart grid: A survey,'' *J. Netw. Comput. Appl.*, vol. 170, Nov. 2020, Art. no. 102808. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804520302769

[138] J. Y. Kim, Y. M. Hwang, Y. G. Sun, I. Sim, D. I. Kim, and X. Wang, ''Detection for non-technical loss by smart energy theft with intermediate monitor meter in smart grid,'' *IEEE Access*, vol. 7, pp. 129043–129053, 2019.

[139] D. He, S. Chan, Y. Zhang, M. Guizani, C. Chen, and J. Bu, ''An enhanced public key infrastructure to secure smart grid wireless communication networks,'' *IEEE Netw.*, vol. 28, no. 1, pp. 10–16, Jan. 2014.

[140] R. Anderson and S. Fuloria, ''Who controls the off switch?'' in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 96–101. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5622026

[141] S. W. Smith, ''Cryptographic scalability challenges in the smart grid,'' in *Proc. Innov. Smart Grid Technol. (ISGT)*, 2012, pp. 1–3.

[142] D. Wu and C. Zhou, ''Fault-tolerant and scalable key management for smart grid,'' *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 375–381, Jun. 2011.

[143] C. Rosinger and M. Uslar, ''Smart grid security: Iec 62351 and other relevant standards,'' in *Standardization Smart Grids*. Berlin, Germany: Springer, 2013, pp. 129–146.

[144] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, ''Time valid one-time signature for time-critical multicast data authentication,'' in *Proc. 28th Conf. Comput. Commun.*, Apr. 2009, pp. 1233–1241.

[145] H. Lee, J. Kim, and W. Y. Lee, ''Resiliency of network topologies under path-based attacks,'' *IEICE Trans. Commun.*, vols. E89–B, no. 10, pp. 2878–2884, Oct. 2006.

[146] M. Handley and A. Greenhalgh, ''Steps towards a DoS-resistant Internet architecture,'' in *Proc. ACM SIGCOMM workshop Future directions Netw. Archit.*, 2004, pp. 49–56.

[147] A. Khelil, S. Jeckel, D. Germanus, and N. Suri, ''Towards benchmarking of p2p technologies from a scada systems protection perspective,'' in *Mobile Lightweight Wireless Systerm*. Berlin, Germany: Springer, 2010, pp. 400–414.

[148] T. T. Tesfay, J.-P. Hubaux, J.-Y. Le Boudec, and P. Oechslin, ''Cyber-secure communication architecture for active power distribution networks,'' in *Proc. 29th Annu. ACM Symp. Appl. Comput.*, 2014, pp. 545–552.

[149] R. H. Lasseter, ''MicroGrids,'' in *Proc. IEEE Power Eng. Soc. Winter Meeting*, vol. 1. Jan. 2002, pp. 305–308.

[150] B. Kroposki, C. Pink, T. Basso, and R. DeBlasio, ''Microgrid standards and technology development,'' in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jun. 2007, pp. 1–4.

[151] Y. Yoldas, A. Önen, S. M. Muyeen, A. V. Vasilakos, and . Alan, ''Enhancing smart grid with microgrids: Challenges and opportunities,'' *Renew. Sustain. Energy Rev.*, vol. 72, pp. 205–214, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032117300746, doi: 10.1016/j.rser.2017.01.064.

[152] A. Vaccaro, M. Popov, D. Villacci, and V. Terzija, ''An integrated framework for smart microgrids modeling, monitoring, control, communication, and verification,'' *Proc. IEEE*, vol. 99, no. 1, pp. 119–132, Jan. 2011.

[153] A. O. Isikman, C. Altun, S. Uludag, and B. Tavli, ''Power scheduling in privacy enhanced microgrid networks with renewables and storage,'' in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2016, pp. 405–410.

[154] D. I. Buza, F. Juhász, G. Miru, M. Félegyházi, and T. Holczer, ''CryPLH: Protecting smart energy systems from targeted attacks with a PLC honeypot,'' in *Proc. Int. Workshop Smart Grid Secur.*, 2014, pp. 181–192.

[155] A. J. Paverd and A. P. Martin, ''Hardware security for device authentication in the smart grid,'' in *Smart Grid Security*. Berlin, Germany: Springer, 2013, pp. 72–84.

[156] C. Castelluccia, A. Francillon, D. Perito, and C. Soriente, ''On the difficulty of software-based attestation of embedded devices,'' in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, 2009, pp. 400–409.

[157] S. E. McLaughlin, D. Podkuiko, A. Delozier, S. Miadzvezhanka, and P. McDaniel, ''Embedded firmware diversity for smart electric meters,'' in *Proc. HotSec*, 2010, pp. 1–2.

[158] J.-M. Lin and H.-Y. Pan, ''A static state estimation approach including bad data detection and identification in power systems,'' in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jun. 2007, pp. 1–7.

[159] M. Parvania, G. Koutsandria, V. Muthukumary, S. Peisert, C. McParland, and A. Scaglione, ''Hybrid control network intrusion detection systems for automated power distribution systems,'' in *Proc. 44th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, Jun. 2014, pp. 774–779.

[160] D. Du, X. Li, W. Li, R. Chen, M. Fei, and L. Wu, ''ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks,'' *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 8, pp. 1698–1711, Aug. 2019.

[161] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, ''Cyber risk analysis of combined data attacks against power system state estimation,'' *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3044–3056, May 2019.

[162] S. Li, Y. Yilmaz, and X. Wang, ''Quickest detection of false data injection attack in wide-area smart grids,'' *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov. 2015.

[163] P. Wang and M. Govindarasu, ''Multi-agent based attack-resilient system integrity protection for smart grid,'' *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3447–3456, Jul. 2020.

[164] C. Cameron, C. Patsios, P. C. Taylor, and Z. Pourmirza, ''Using self-organizing architectures to mitigate the impacts of Denial-of-Service attacks on voltage control schemes,'' *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3010–3019, May 2019.

[165] M. Chlela, D. Mascarella, G. Joos, and M. Kassouf, ''Fallback control for isochronous energy storage systems in autonomous microgrids under Denial-of-Service cyber-attacks,'' *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702–4711, Sep. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/7849190/

[166] N. Kumari and G. Shankar, ''Euclidean detector based cyber attack detection in automatic generation control,'' in *Proc. Int. Conf. Comput., Power Commun. Technol. (GUCON)*, 2019, pp. 871–875.

[167] O. Vukovic and G. Dan, ''Detection and localization of targeted attacks on fully distributed power system state estimation,'' in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2013, pp. 390–395. [Online]. Available: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6687989

[168] H. Li and Z. Han, ''Manipulating the electricity power market via jamming the price signaling in smart grid,'' in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Dec. 2011, pp. 1168–1172. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6162363

[169] G. Lee, Y.-S. Kim, and J. Kang, ''An adaptive dos attack mitigation measure for field networks in smart grids,'' in *Advances on Broad-BandWireless Computing, Communication and Applications*, L. Barolli, F. Xhafa, and K. Yim, Eds. Cham, Switzerland: Springer, 2017, pp. 419–428.

ALVIN HUSEINOVI is currently pursuing the Ph.D. degree with the Faculty of Electrical Engineering, University of Sarajevo, Sarajevo. He is a Chief Information Security Officer at the University of Sarajevo–University Tele-Informatics Centre. His research area is focused on computer forensics, data security, parallel computing, and smart grid security.

SA A MRDOVI (Member, IEEE) is an Associate Professor with the Faculty of Electrical Engineering, University of Sarajevo. He teaches computer networks and security courses. He defended his Ph.D. thesis on intrusion detection systems at the Department for Computing and Informatics in 2009. He has published three books on networks and security and a number of papers in scientific journals and conference proceedings. His main research interests include digital information security, digital forensics, and next generation networks. He has been reviewing papers for various journals and conferences. He also works on projects with industry and government in the area of information security. He holds a certified information system security professional (CISSP) certificate.

KEMAL BICAKCI (Member, IEEE) received the Ph.D. degree from the Department of Information Systems, Informatics Institute, Middle East Technical University, Ankara, Turkey, in 2003. He is currently a Professor with the Department of Computer Engineering, TOBB University of Economics and Technology, Ankara. His research interests include wireless and sensor networks, information security, and applied cryptography and usability.

SULEYMAN ULUDAG (Member, IEEE) is an Associate Professor of computer science with the University of Michigan-Flint. His research interests include secure data collection, smart grid communications, smart grid privacy, smart grid optimization, demand response bidding privacy, the denial-of-service in the smart grid, cybersecurity education, curriculum development, routing and channel assignment in wireless mesh networks, the quality-of-service (QoS) routing in wired and wireless networks, and topology aggregation. More recently, his research focus has been on the Internet-of-Things devices, especially on developing intrusion detection systems against DDoS attacks against the smart grid using machine learning techniques. He has received the Teaching Excellence Award in 2010 and the Research Excellence Award from the University of Michigan-Flint. He received the Fulbright Core Award twice in 2012 and 2018.