Impact Analysis of Cyber Attacks on Smart Grid: A Review and Case Study

Temitayo O. Olowu, Shamini Dharmasena, Alexandar Hernandez, and Arif Sarwat

1 Introduction

Cyber physical systems is a term that applies to engineered systems that find their use in a variety of domains. Often these systems are a collection of sensors, actuators, and embedded devices that act as an interface with the real world. In addition, these devices communicate through short- or long-range communication channels to share data and create a seamlessly integrated network (Sundararajan et al. 2018, 2019). Cyber physical architecture can be used to improve existing traditional systems, as well as improve the quality of service provided by these systems. For example, one application of a CPS is wide-scale deployment of sensors and actuators that will be used to monitor key environmental changes in the world. The data can be aggregated to a database and used to make better decisions concerning the environment. This ties closely with disaster response, which is another area where the use of CPS can reduce the chaos caused by natural disasters or other large-scale emergencies. These systems can be implemented to manage evacuations and create scheduled departures that will reduce congestion and accidents that would further delay evacuations (Sundararajan et al. 2018; Gunes et al. 2014). Various other applications find promise in cyber physical systems. These include smart manufacturing, air transportation, robotics for service, and health care/medicine which includes anything from assistive devices to smart operating rooms (Gunes et al. 2014; Dharmasena et al. 2019). They create a

This work is funded by NSF under the grant numbers CNS-1553494 and CNS-1446570.

T. O. Olowu (✉) · S. Dharmasena · A. Hernandez · A. Sarwat
Energy, Power and Sustainability Group, Florida International University, Miami, USA
e-mail: tolow003@fiu.edu
URL: https://www.eps.fiu.edu

S. Dharmasena
e-mail: ikona001@fiu.edu

A. Hernandez
e-mail: ahern373@fiu.edu

A. Sarwat
e-mail: asarwat@fiu.edu

H. Tyagi et al. (eds.), *New Research Directions in Solar Energy Technologies*,
Energy, Environment, and Sustainability,
https://doi.org/10.1007/978-981-16-0594-9_3

highly monitored and controlled environments where human interaction is reduced. However, with any new technology, there are always a variety of challenges that must be overcome in order to realize widespread cyber physical system implementation. In order to ensure the systems are robust, several factors must be accounted for. These are inter-operability, predictability, security, reliability, dependability, and sustainability (Gunes et al. 2014). There is an ongoing drive by power utility companies to achieve smart distribution systems or the smart grid (Wadhawan et al. 2017; Chen et al. 2011; Sundararajan et al. 2019; Dharmasena et al. 2019). This typically involves the deployment of communication and control devices and integration of localized generations, distributions, and energy management systems to allow the physical grid become more autonomous, intelligent, and controllable (Sarwat et al. 2017; Hawrylak et al. 2012; Stefanov and Liu 2012; He and Yan 2016; Wei et al. 2014; Olowu et al. 2019a, b). As part of the smart grid architecture, the deployment of distributed energy resources (DERs) such as photovoltaic (PV) systems is becoming a good alternative to the conventional power generators (Olowu et al. 2018, 2019; Rahman et al. 2018; Jafari et al. 2018; Olowu et al. 2018, 2019; Debnath et al. 2020). The drive to achieve a smart distribution system has opened up new set of challenges for the utility companies (Zhaoyang 2014; Srivastava et al. 2013; Dagle 2012). Data communication and control between the physical systems and the cyber network have made the smart grid prone to cyber physical attacks (Parvez et al. 2016, 2017; Mekonnen et al. 2018; Odeyomi et al. 2020). In this paper, cyber physical attacks that occur in smart grid and their mitigation techniques are extensively reviewed under the three domains: device level, communication level, and application level in Sect. 2. In Sect. 3, a case study of fault data injection (FDI) in a production meter of a standard IEEE 34 test feeder with three PVs has is simulated, analyzed, and presented. Section 4 presents a proposed machine learning based protection architecture that can be used to mitigate the severe impact of FDI attack. Finally, Sect. 5 concludes the paper together with proposals for the future work.

2 Cyber Attacks on Smart Grid

This section discusses the features of the smart grid architecture and various level of cyber attacks that can be executed within it.

2.1 Smart Grid and Its Architecture

According to the definition by national institute of standard and technology (NIST), smart grid is a network that provides electricity efficiently, reliably, and securely. In other words, it is delivering electricity with brain (Smart grid 2019). Smart grid comprises of generation (including DERs), transmission, distribution, service providers, customers, and markets. Each of these components interacts with others which means

that there is a bi-directional flow of power and communication in between. In order to facilitate the required functionalities, smart grid comprises of heterogeneous systems such as supervisory control and data acquisition (SCADA), advanced metering infrastructure (AMI), intelligent electronic devices (IEDs), human–machine interface (HMI), building management systems (BMS), DERs, and many more. Furthermore, there are different network protocols for the communication of these different systems. While these technologies make the grid smarter, it increases the system's vulnerability to cyber attacks. Smart grid and its cyber threats can be analyzed across three layers: device layer, communication layer, and application layer. In smart grid, there are many physical devices and their interfaces that falls into device layer. This includes smart meters, monitoring, and measuring units such as phasor measurement units (PMU), relays, and other protection devices. Communication layer incorporates the communication network between theses devices in generation, distribution, and consumer ends in the smart grid. It is very important to secure the data packet transfer between these devices. The processing and analytical platforms deliver high-end insights to analysts and operators which is listed as the application layer in this study (Saleem et al. 2019). Supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS) are such examples for the application layer of smart grid.

2.2 Layers of Cyber Attacks

As discussed in Sect. 1, there is a growing concern as regards cyber attacks on the smart grid architecture. These attacks have wide ranging effects on the dynamics of the grid which include loss of generator synchronism, voltage collapse, frequency issues, prolong outages, and power quality issues among others. There are various possible attacks on a smart grid. These attacks can be categorized on the basis of what exactly is being compromised. As discussed in Sect. 2.1, smart grid can be classified into three domains, and so, the attacks can also categorize into these three levels. The attack happens in device level, communication level, and in application level. The authors of Li et al. (2012) proposed a different categorization for cyber attack, which are: device attack, data attack, privacy attack, and network availability attack. But the taxonomy of attacks used in this paper is simpler and shows a direct connection with the end target compared to the taxonomy proposed in Li et al. (2012). There are many other attacks that fall into above categories. In addition, there are many possible entry points for attackers. These include, but are not limited to, infected devices where an employee may inadvertently, or intentionally, plug in an infected USB. Attacking the network through vulnerabilities is another possibility if the IT infrastructure has holes or backdoors that can be accessed by hackers. Equipment preloaded with malware is another common entry point and is known as a supply chain attack. Phishing emails or social engineering also present a problem. Here, a hacker can obtain personal information and access the system as a valid user. This becomes difficult to detect as the intrusion does not appear as a threat to the system

(Conteh et al. 2016). Often, the addition of humans to the loop makes a system much more vulnerable to outside attack (Haack et al. 2009).

2.2.1 Device Layer

The device layer attack as its name connotes occurs when an attacker targets a grid device and seizes control of it. This could be used to wreak havoc by shutting off power or to gain control of communications, and mostly this level of attack can lead into another level. The puppet attack which is a variant of of denial of service (DoS) is a plausible attack type in AMI. AMI creates the bidirectional communication interface between smart meters (Wei et al. 2017) and utilities to share power consumption, outage, and electricity rate data. The attacker compromises several normal nodes in AMI and keep as puppet nodes to exhaust the system through flooding data packets. Attacks like puppet or time delay switch (TDS) attack only target one security parameter, availability, to affect AMI (El Mrabet et al. 2018).

2.2.2 Communications Layer

Attacks at communication level can be either data attacks or a network availability attack. The data attack involves either removing, adding, changing, or stealing the data being communicated. An example of this would be an attacker sending false price and meter information. This will lead to power shortages and overall cause a loss in the power companies' revenue (Mo et al. 2011). Privacy attacks can also be categorized under this type which involves stealing confidential information, which could be consumers electric bill or their daily energy usage. The network availability attack involves reducing or eliminating the functionality of the network that the devices are communicating on. A commonly seen example of this is a DOS attack. Based on previous statistics, momentary or prolonged shutdown of the grid can have devastating consequences. The distributed denial of service (DDOS) attacks that occur in networks overwhelm the Internet bandwidths and reduces the network performance through multiple compromised devices. There are several types of DDOS attacks: Slowloris, SYN flood, Ping of Death, ICMP flood, UDP flood, etc., which operates in different speeds (Ozgur et al. 2017). Slammer worm is another malware that attacked a nuclear power plant in Ohio in 2003. It disabled the plant's safety monitoring system for nearly 5 h. Slammer was one of the fastest worms at that period and had the capability to spread workwide in 15 min. Slammer sends a UDP datagram to the port 1434 of target computer, and it makes use of the buffer overflow vulnerability in the SQL server monitor for the execution.

2.2.3 Applications Layer

There are a variety of well-known attacks on the application level of the smart grid, and these include Stuxnet, Duqu, BlackEnergy3, etc. These attacks have become sophisticated and multifaceted making them harder to detect and prevent (Eder-Neuhauser et al. 2017). For example, Stuxnet compromised confidentiality, integrity, availability, and the accountability of a system, and it targeted SCADA and control devices (PLCs). Stuxnet was a multilayered attack that first infected a Windows computer through an infected USB and began replicating itself. Once it had integrated itself into the system, it found a certain program created by Siemens called Step7, and eventually found its way to the PLCs. Not only could the attacker spy on the systems, but they could also control the PLCs and in that way control the connected machinery (Kushner 2013). Stuxnet utilized four zero-day vulnerabilities of the system. It had a rootkit to hide the malicious files and processes from users and anti-malware software. There are several other Stuxnet related malware: Duqu, Flame, Triton. Similar to Stuxnet, Duqu uses a kernel driver to decrypt the dynamic load library (DLL) files, and it mainly targets the SCADA. The way the above attacks function vary greatly on what their specific target is. The Duqu and Flame attacks were slightly different than Stuxnet whose purpose was to cause physical damage to equipment. The Duqu attack was created to steal information about industrial control systems. DDOS type attacks occur in application level too. DDOS exhaust SCADA like systems by striking with simultaneous data requests and crash down the system. BlackEnergy-3 is a Trojan that is used for DDOS attacks. In 2015, a SCADA related industrial control system in a electricity distribution system in Ukraine was subjected to a BlackEnrgy-3 attack which caused power outages for around 225,000 customers for several hours. In this incident, the access to the network is gained through spear phishing and used a KillDisk to erase the master boot record and the logs of the impacted system (Sharing and Center 2016). A summary of reported cyber attacks in smart grid is given in Table 1.

2.3 Cyber Attacks on DERs in a Smart Grid

With the increase in utility- and small-scale DERs (particularly PV systems) in the grid, there is an increase in the vulnerability of the entire system. Figure 1 shows the different attack points in a DER integrated grid. There are two basic networks layers in a grid-tied DER system. These are the power layer (that allows the energy generated by the DER to be sent to the grid bidirectionally) and the communication and control layer (which allows remote monitoring, data logging, and remote controlling of the DERs).

Usually, DER devices have their individual energy management systems (EMSs) that control their power electronic converters such as smart inverters (SIs) (Qi et al. 2016). SIs typically have IP addresses that allow for a remote control of their operations. This makes them vulnerable to man-in-the-middle (MITM) attacks. The

Table 1 Reported cyber attacks in smart grid

Name of attack	Target of attack	Year	Attack details
Device layer			
Trojan.Laziok reconnaissance malware	Devices of energy companies	2015	Collected data from compromised devices, i.e., installed antivirus software, installed applications, CPU and GPU details, etc.
BlackEnergy	General Electric's HMI	2011	HMI of utility grid control systems
Communication layer			
Spear phishing, Havex malware for watering hole attack	ICS/ SCADA	2014	Espionage using OPC protocol to map devices on ICS network
Dragonfly 2.0	Western energy sector	2015–2017	Spear-phishing, Trojan-ware, watering hole attacks
Exploitation of vulnerabilities in firewall firmware	Power grid of Western US	2019	Outside party rebooting the company's firewalls to cause periodic "blind spots" for grid operators losing communication with multiple remote power generation sites for minutes at a time that lasted for around 10 h
Application layer			
Stuxnet worm	Programmable logic controllers of SCADA	2010	Travels via a USB stick. Exploits zero-day vulnerabilities of PLCs
Duqu worm	SCADA	2011	Designed to steal information about ICS (digital certificates, private keys)
Remote access Trojan; watering-hole attack	ICS/ SCADA	2014	Conducted by dragonfly, energetic bear
BlackEnergy3	Ukrainian grid control center	2015	Left 220000+ customers without power
Industroyer or crash override malware	Pivnichna substation ICS, Ukraine	2016	Power outage to one-fifth of Kiev

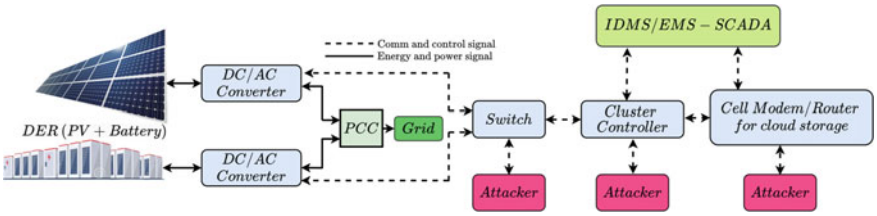

Fig. 1 Potential attack points on a grid-connected DER

knowledge of the SI's IP enables the attacker to gain a direct control of the SI and could potentially alter its SI settings. Depending on the level of DER penetration on the feeder where the DER is connected, altering the SI settings by an attacker could lead to severe changes in the grid's voltage and frequency (Teymouri et al. 2018) Another level of attack can be executed by compromising the utility's wide area network. This will allow the attacker send malicious and false commands to the DERs. This include sending false messages to enable the DERs make unnecessary control actions and operation. The false command messages to the DERs from the utility SCADA system could also be as a result of the attacker compromising the power systems data from the point of common coupling (PCC) being sent by the SIs. For example, if the voltage and frequency values coming from a DER's SI are compromised, this could cause the integrated distribution management system (IDMS) or energy management system (EMS) to send false control actions to other DER SIs.

2.4 Detection and Mitigation Techniques for Cyber Attacks in Smart Grid

Different ways in which the attacker infect and propagate through a system makes it difficult to detect and mitigate these attacks. These attacks all have different purposes depending on the goals of the hacker. They range from disrupting the normal operation of a system to stealing information from the local utility or its consumers. In addition, the way these systems breach the security of a smart grid vary from removable drives to client-to-server access. Nimda, an attack that occurred in 2003 for disrupting the smart grid, has several access points including email, client-to-server, server-to-client, and host-to-network sharing (Eder-Neuhauser et al. 2017; El Mrabet et al. 2018). All the different points of entry, attack methods, and different targets make attack detection, prevention, and elimination very difficult. Various detection and mitigation techniques are proposed in literature, and they are mostly specific to the type of the attack. And most of the time rather than using a single solution, several security measures are deployed together to mitigate attacks at every progression stage.

2.4.1 Detection Techniques

During pre-attack atmosphere, it is mainly monitoring and detection schemes applied at vulnerable locations. In this case, different detection techniques are introduced to get early warnings and prepare with proper counter measures. Intrusion detection system (IDS) is such major mechanism and can be found as anomaly-based detection, specification-based, and signature-based IDS. Currently, many anomaly-detection-based IDS are developed using machine learning techniques. The authors of (Ozay et al. 2016) present a review on different machine learning techniques to develop

learning algorithms that can be employed to classify secure and attacked datasets. In Ozay et al. (2016), a statistical correlation-based scalable unsupervised anomaly detection engine for large-scale smart grids is proposed. The proposed scheme has reduced computational complexity by exploiting feature extraction through symbolic dynamic filtering. An IDS framework using blockchain for multimicrogrid (MMG) system is presented in Hu et al. (2019). This paper investigates that the vulnerability of MMGs for cyber attacks proposes a novel corroborative IDS that adopts a multipattern proposal generation method to reduce the false negative rate of intrusion detection.

False data injection is another common attack in smart grid. Therefore, many studies are carried out on false data injection detection (FDID). The paper (Wei et al. 2018) proposes a FDID technique that uses deep belief networks, and it uses unsupervised learning from the bottom of the restricted Boltzmann machine to have initial weights. Another recent study on FDID is presented in Ameli et al. (2020) which is focused on line current differential relays. It has been learnt that attacks on multiple relay can create catastrophic failures in the system, and therefore, this paper investigates coordinated attack scenario on line current differential relays and its consequences. Then, a FDID is proposed which uses the state space model of the faulty line together with positive and negative sequences of voltage to detect the attack. With specific reference to DER, some of the detection technique is proposed in literature. These include security information and event management (SIEM), data loss prevention (DLP) technology, and IDS (El Mrabet et al. 2018). The use of data-driven techniques can be used to implement real-time intrusion detection. This requires the use of machine learning algorithms to forecast accurate PV power generation and prediction of dynamic states of the network based of historical and extensive simulation data. Another detection approach specific to the power electronic converters is by regularly sampling the voltage and frequency at the PCC in other detect the rate of change of these parameters. A sudden change beyond the set tolerance could indicate a potential cyber attack on the SIs. The tolerance values of the detection algorithms are set based on the learning performance of the SIs.

2.4.2 Mitigation Techniques

The severity of cyber attacks on smart calls for the development of adequate and effective mitigation strategies. These techniques can be made proactively or reactively. This implies that steps can be taken to address a cyber physical threats before attack, during at or after an attack has been executed. Several approaches to addressing different types of attacks on cyber physical assets on smart grid has been proposed in literature. Authors of Srikantha and Kundur (2016), Farraj et al. (2016) proposed the use of game theoretic framework to mitigate cyber attacks on switching and control of physical assets in smart grid. In Srikantha and Kundur (2016), the authors demonstrated that power utility companies can devise a counter measure vectors against an attacker using the 2PZS (two-player zero sum) differential game formulation. A new iterative algorithm to solve the nonlinear 2PZS game was proposed. Their

results showed that by applying the countermeasure vector, the utility company can successfully prevent the attack and keep the system stable. Also their formulation is able to determine the safety margin that will enable a proactive measures to be taken. In Farraj et al. (2016), a simplified model of a switching attacked is presented. The position and sign of the rotor speed is used to initiate a local control action (with resource constraints) to provide a counter measure against an attack n the generator. A game theoretic formulation is proposed to make this interaction between the attack switching action as well as the counterattack control mechanism. Their results shows that the proposed resource-constraint controller can effectively be called to action only when needed as well as meet the requirement of stabilizing the system. To prevent FDI attacks in smart grids, authors of Wang et al. (2017) proposed a data analytical technique to detect FDI attacks. The data-centric technique is based in margin-setting algorithm (MSA). MSA is a machine learning algorithm based on data analytics. The authors used a six-bus feeder for simulation and experimental validation of the proposed MSA algorithm on tho FDI attack scenarios. Their results showed that the proposed MSA algorithm performed better for FDI attack mitigation when compared with other machine learning algorithms such as support vector machine (SVM) and artificial neural network (ANN). Deep learning models have also been proposed to capture anomalies due to FDI attacks with validations showing high level of accuracy (He et al. 2017). One detection approach specific to the power electronic converters is by regularly updating the firmware of the SIs to minimize their vulnerabilities. Authors of McLaughlin et al. (2010) proposed the use of a firmware diversity approach that prevents or limits the possibility of a large-scale cyber attack on smart meters. This approach can also be deployed on SIs. The diversity in the SIs firmware of various DERs will make simultaneous large-scale attack difficult to achieve by the attacker since the vulnerabilities of these SI firmware will differ. An inverter internal anomaly (such as switch faults) detection and mitigation algorithm which adjusts the inverter voltage output using model predictive control technique was proposed by Fard et al. (2019). This control method prevents a complete shut down of the inverter which may lead to cascading shut down of other DERs in the network due to sudden increase in load seen by other DERs as a result of the sudden loss of power generation from the attacked DER's SI.

3 Case Study of FDI Attack on IEEE 34 Bus System

In order to visualize and quantify the potential impacts of an FDI attack on the grid, an IEEE 34 distribution feeder is developed by the IEEE PES test feeder working group. Its parameters are based on an actual distribution feeder located in Arizona in USA.

3.1 System Model and Simulation Setup

The IEEE 34 bus network (used as a case study) is integrated with three PV systems, a synchronous generator, and a battery energy storage system (BESS) as shown in Fig. 2. The nominal voltage rating of the feeder is 24.9 kV. The feeder has two voltage regulators between nodes 814–850 and 852–832. The substation transformer upstream of node 850 is a 2.5 MVA, 69/24.9 kV, Δ Y . The combined rating of the load (modified) on the feeder is approximately 3.1 MW (active) and 0.689 MVAr (reactive). Node 838 is the farthest distance and its approximately 59km away from the substation transformer The specifications of the sources integrated into the feeder is as given in Table 2.

The IEEE 34 node test feeder, PVs, synchronous generator, and the battery energy storage are modeled using OpenDSS and MATLAB.

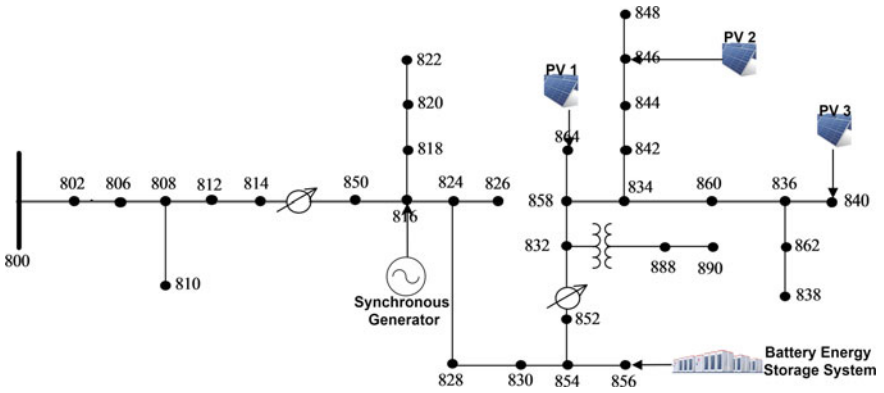

Fig. 2 IEEE 34 node distribution feeder with three PVs, a synchronous generator, and one battery energy storage system

Table 2 Generation specifications

Generation power (kW)	Maximum (kWh)	Inverter	Phases	Default PF	Energy
PV1	200	300	1	1	–
PV2	2050	3000	3	1	–
PV3	200	300	3	1	–
Synchronous generator	5000	5000	3	1	–
Battery energy storage	1000		1	1	12,000

3.2 Data Gathering, Cleaning, and Preprocessing

According to Sundararajan et al. (2019), the power generation from photovoltaic systems mainly depends the global horizontal irradiance (GHI) and the ambient temperature (consequently the module temperature).

$$P_{\mathrm{PV}^{\mathrm{gen}}}(t) = P_{\mathrm{DC}} \times \frac{\mathrm{GHI}(t)}{1000} \times G \times M \tag{1}$$

$$G = 1 + \frac{\%\mathrm{temp}_{-\mathrm{coeff}}}{100}[T(t) - 25] \tag{2}$$

$$M = b_{\mathrm{d}} \times b_{\mathrm{m}} \times b_{\mathrm{c}} \times b_{\mathrm{inv}} \tag{3}$$

where P_{dc} is the DC name plate capacity of the PV system, GHI(t) is the instantaneous value of the irradiance, b_{d} is the dirt/soil de-rate factor, b_{m} is the PV mismatch de-rate factor , b_{c} is the DC cable wiring de-rate factor, b_{inv} is the inverter plus transformer de-rate factor. The simulation software used to investigate this attack uses the instantaneous values of GHI, ambient temperature profiles, inverter, and PV efficiency-temperature de-rating factors in order to estimate the PV generation. A one-minute resolution (GHI) and temperature profile (as shown in Figs. 3 and 4) used for the PVs are actual data from the data acquisition system of a 1.4 MW PV plant located on the engineering Campus of Florida International University.

The GHI and temperature were acquired on the February 24, 2019 which was a typical cloudy day in Miami. Based on the method proposed by authors of Sundararajan et al. (2020), some of the missing data from measurements taken by the site data acquisition system were extrapolated. The production meter of the PV

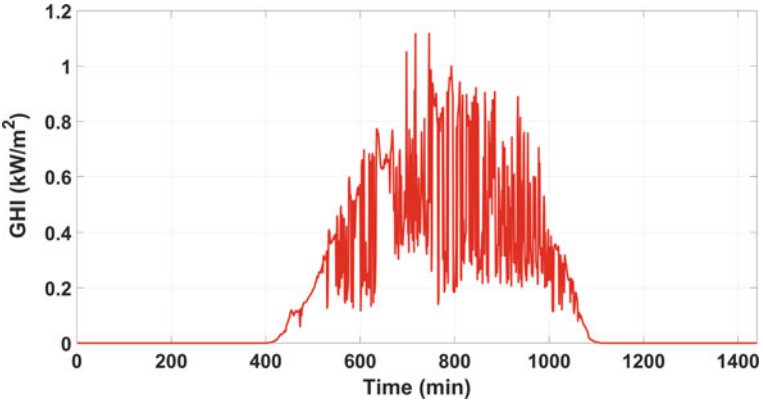

Fig. 3 One-minute resolution global horizontal irradiance profile of the location used for the simulation

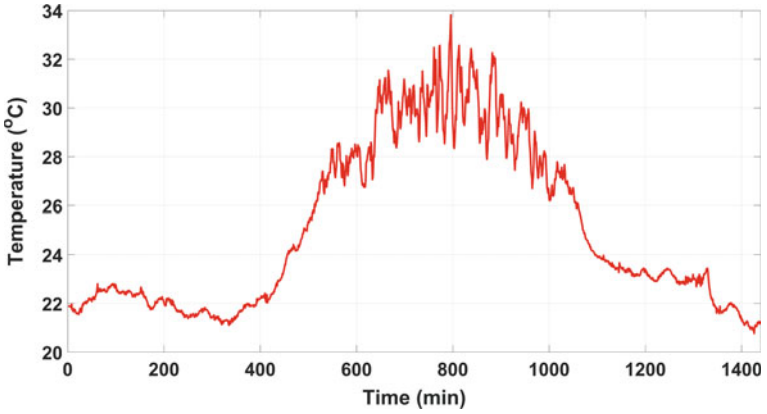

Fig. 4 PV ambient temperature profile

system is located the point of common coupling with the grid which measures the aggregation of the 46 string inverters installed on the PV site. Since the simulation software only takes the GHI measurements, temperature measurements, inverter, and PV efficiency-temperature de-rating factors as input, it is therefore imperative to verify the accuracy of the PV production generated by the software during the simulation with the actual data acquired from the production meter by the data acquisition system. The production meter values were correlated with the output if the simulation software for to verify the accuracy of the PV generation being simulated using the software. The correlation results shows a high level of accuracy between the actual PV generation and the values estimated by the software used for the simulation. For the power generation from the three PVs used in the simulation (200 kW, 2.05 MW, and 200 kW), the same weather parameters were used. Since the expression in (1) depends on the DC name plate rating of the PV, the individual power generation depends (or is directly proportional) to their respective name plate capacity.

3.3 Attack Scenario Construction

In order to implement the FDI attack in the production meter of the PV plant (PV 2), the power production data for a time window of 10 and 30 min is considered. The time resolution of the power generation data is one-minute. The attacks were synthetically generated by introducing error signals to the production estimations at time t. The attack can be modeled as expressed in Eq. 4, where P_{attack} and P_{actual} represent the tampered production measurements and real production measurements, respectively, for the attack scenario considered. $e(t)$is also a time series data which gives rise to the injected false data by the attacker.

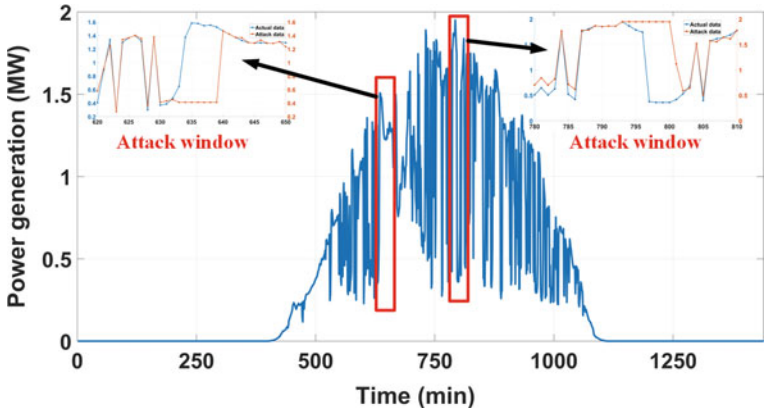

Fig. 5 Power generation profile showing the attack window

$$P_{\text{attack}}(t) = P_{\text{actual}}(t) + e(t) \tag{4}$$
$$P_{\text{attack}}\{P_1\},\ P_{\text{actual}}\{p_1\},\ e\{e_1\}$$

The FDI attack emulated within the time window between 620 and 650 min shows an error of 1.2 MW in the production meter measurement between 630 and 640 min. This drop as seen by the distribution command and control center will necessitate the need to ramp up the synchronous generator connected to bus 816 by the same amount. This will potentially cause excess generation in the network. Conversely, with time window of 780 and 810, the erroneous production meter measurements show an error of approximately 1.5 MW between 795 and 801 min. Consequently, this will lead to ramping down of the synchronous generator in order to maintain the stability of the system. The introduction of error values in the production meter measurement is as shown in Fig. 5. The impact of this attack on the power system network is analyzed and discussed in Sect. 3.4.

3.4 Simulation Results

Following the attack as described in Sect. 3.3, the synchronous generator was ramped up between 630 and 640 and ramped down 795 and 801 based on the false data received from the production meter of $PV2$. The nodal voltages of some buses in the network is as shown in Figs. 6 and 7. The result shows that there is a significant impact of the generator ramping on the voltage profile on almost all the buses in the network. Buses with close proximity to the synchronous generator were the most affected. For example, the voltage profile of nodes 850, 812, and 806 shows some spikes in their node voltages during the attack periods. The nodal voltage during the

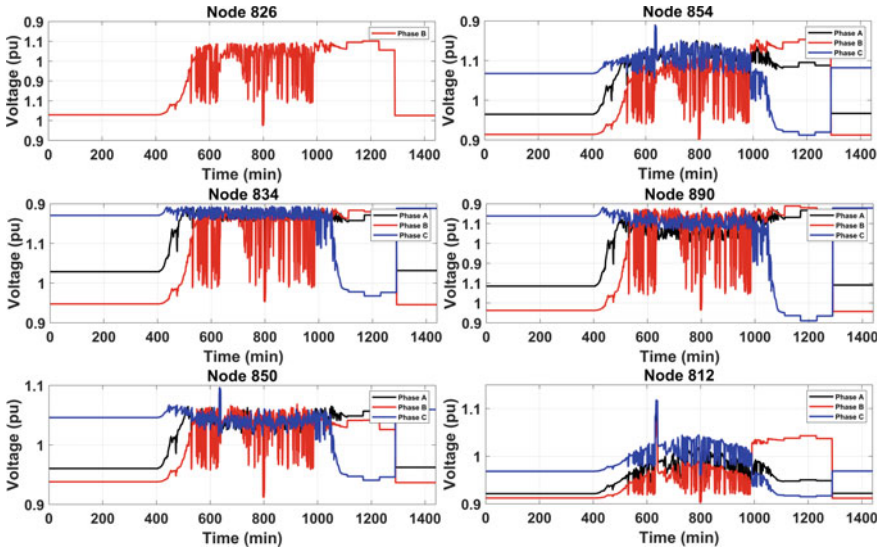

Fig. 6 Nodal voltage profile before, during, and after the attack

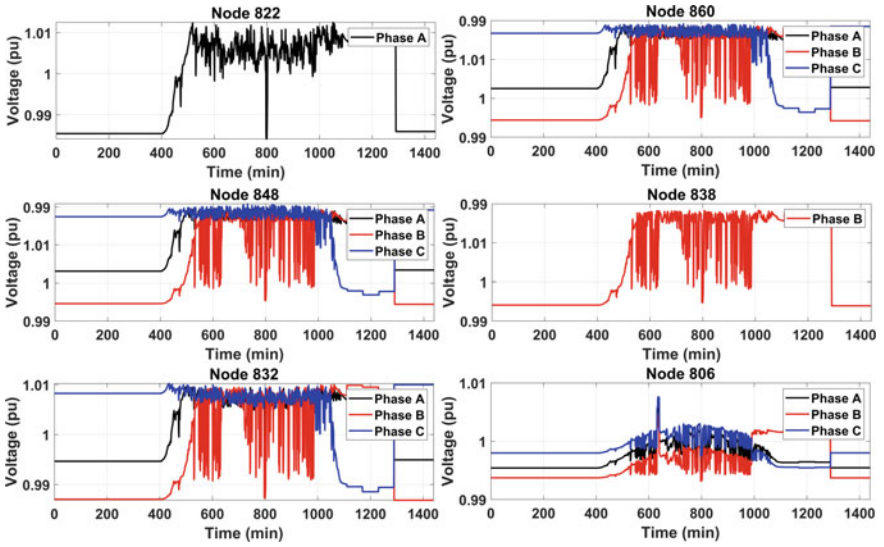

Fig. 7 Nodal voltage profile during before, during, and after the attack

first attack period went to 1.12 pu which is beyond the 1.05 pu threshold. This is an indication of a voltage collapse. For nodes close to the PVs, the fluctuations in the PV generation cause a severe variation in the nodal voltages.

It is worthy of note that the SI settings of the PVs is unity power factor. This means that the PVs does not carry out any voltage regulation in the network. For example, using SI settings of Volt-VAR will allow the PVs inject/absorb some reactive power which could potentially allow some voltage regulation in some of the nodes especially those closer to the location of the PVs. The impact of the BESS system can been seen in the nodal voltages at periods (beyond 1001 min time stamp) when the PV generation is no longer available. The current profile across some of the branches in the network is as shown in Figs. 8 and 9. Similar to the impact of the attack on the nodal voltage profiles, the branches close to the synchronous generator were the most impacted by the attack. Branches 810–808, 822–820, and 802–806 show significant spikes in their current profile. In practice, this could lead to erroneous tripping of the over-current relays and cause instability in the system. For branches close to the PVs, their current profiles is significantly impacted by the current injection by the PVs as seen in branches 832–852, 864–858, and 834–860. Branch 854–856 where the BESS is connected shows its current injection based on the charge and discharge profile attached to the BESS. This current injection allowed the some of the nodal voltages to be stabilized when the power generation from the PV ramps to zero (Fig. 10).

The total system's loss (which includes the line line loss and the transformer loss) is as shown in Fig. 11. The total network loss is also impacted by the attack. As it can be seen from Fig. 11, the second attack window caused a sharp increase in the network losses during this period which significantly affects the overall efficiency of the system

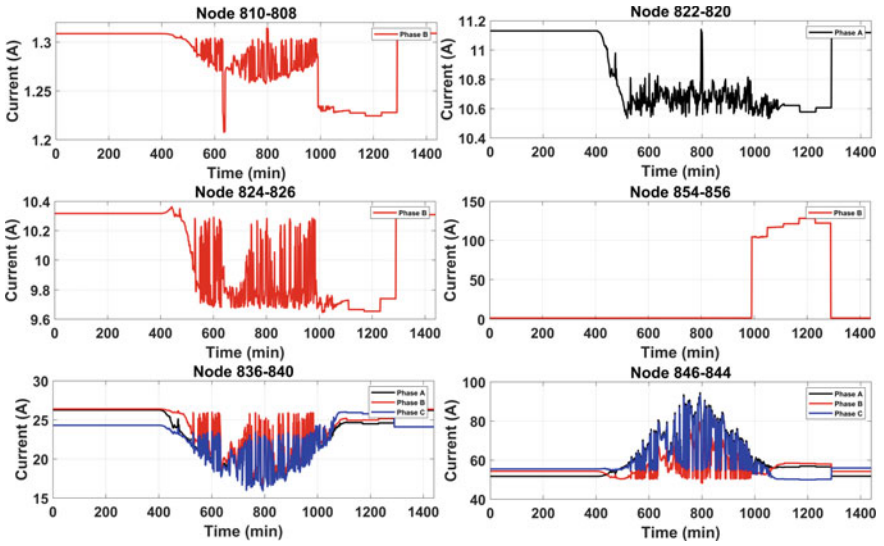

Fig. 8 Branch current profile before, during, and after the attack

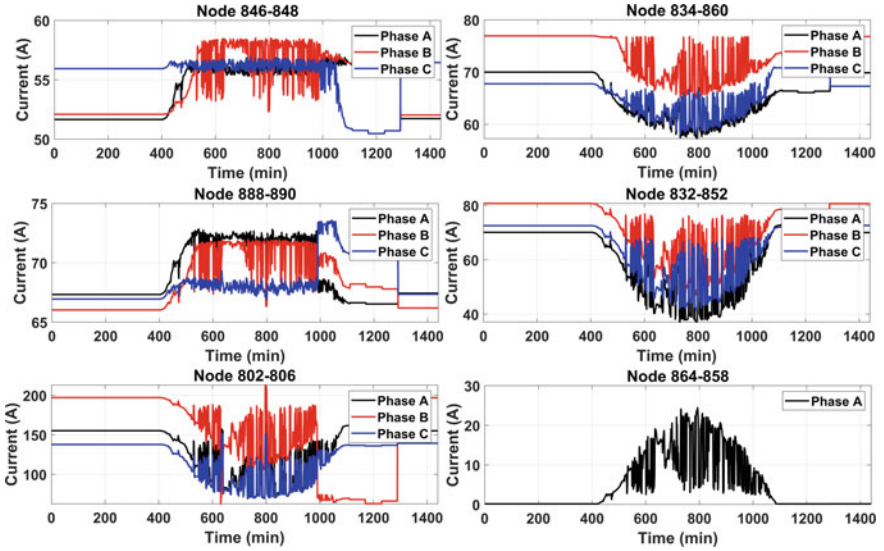

Fig. 9 Branch current profile before, during, and after the attack

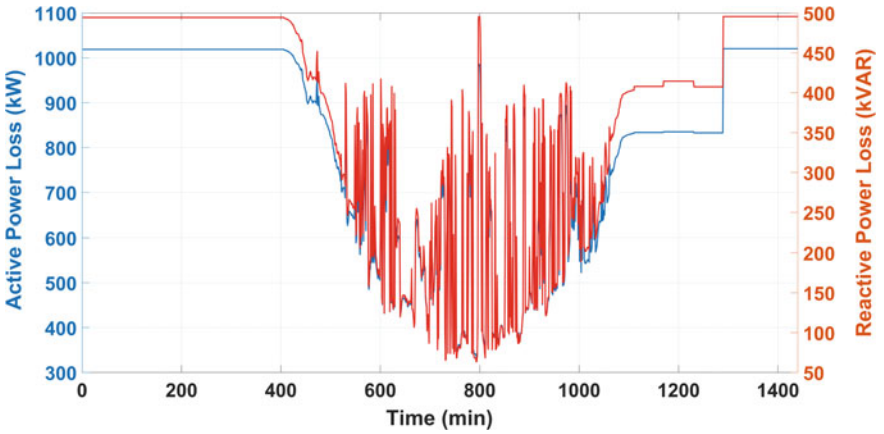

Fig. 10 Active and reactive power loss profile before, during, and after the attack

4 Machine Learning-Based Adaptive Protection Scheme

Figure 11 shows a proposed solution (under development) for smart grid protection with high PV penetration. This solution provides a multi-layer protection system using an machine learning-based protection device for isolation of fault currents from one cluster of PV systems to another. Each PV with SI is controlled by a PV control hub with an integrated WDAS. The weather forecast subsequent prediction

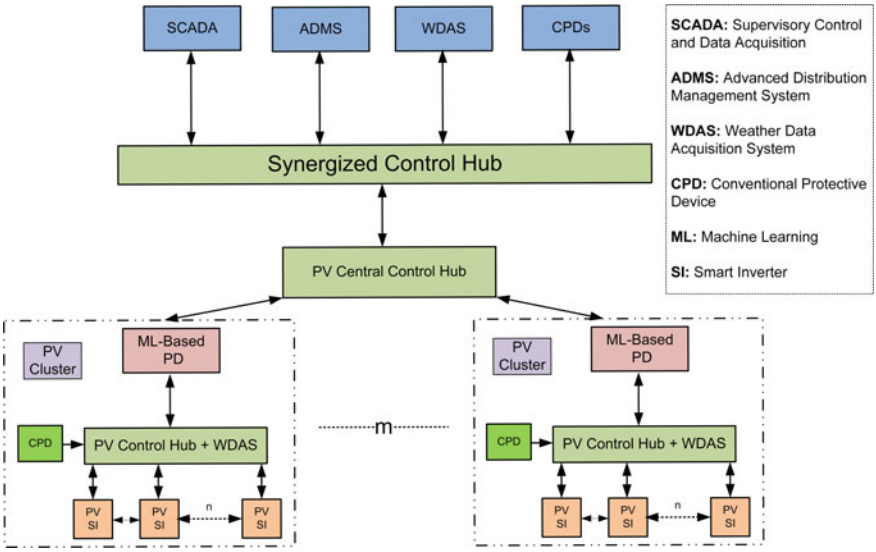

Fig. 11 Proposed machine learning adaptive protection scheme

of energy profile generation allows the PV control hub to determine the right settings for the PV SIs.

The settings of this SIs are dynamically controlled from the PV control hub. Within each PV cluster, the CPD continually sends in real-time current, voltage, and frequency parameters of the system to the PV control hub. This data is fed into the ML-based PD. The historical data of the network under normal and fault conditions are used to develop a classification model which is programmed into the ML-based PD. The fault parameters of the system are derided from extensive simulations carried out using the ADMS which allows various types of faults (such as single-to-ground, line-to-line-, line-to-line-to-ground, line-to-line-to-line, line-to-line-to-line-to-ground, and open circuit faults) to be simulated and their respective fault current values captured. The classification algorithm already programmed into the ML-based PD classifies if the system is system parameters normal, abnormal, or fault condition. Whenever the system is attacked and the conventional generator is wrongly ramped up, the new system parameters measured by the CPD will be classified as an abnormal and the ML-based PD disconnects this cluster of PV from the others. This would prevent other PV clusters from contributing to the abnormal system parameters. The PV central control hub is a wide area control that connects to the synergized control hub. The synergized control hub is located at the substation. This control hub is integrated with the SCADA, ADMS, and WDAS and controls the CPD at the substation level. The SCADA integrated ADMS has the fault location isolation and service restoration algorithm. This helps the systems to quickly located the abnormal section of the network and isolate it while restoring power to the normal section of the system as soon as possible. This is part of the self-healing process of the smart grid.

5 Conclusions and Future Work

With obvious increase in DER integration and the drive toward achieving smart distribution systems, there is an increase possibility of cyber attacks. As DERs continues to form a network with communications and control layers, the vulnerability and susceptibility to attacks consequently increase. This implies that smart grid systems can be simply regarded as a cyber physical network. This chapter presents a comprehensive review of vulnerabilities in smart grids and the impacts of cyber attacks. This chapter presented real-world case studies of successful attack on on multiple grid assets, including networks with high-penetration of distributed energy resources (DERs), and their impacts on the system. A specific case study of one of the prevalent attacks called FDI is presented. A real-world scenario of an FDI attack was done using an IEEE 34 bus system with three PVs, one synchronous generator, and one energy storage. A false command was sent to the synchronous generator based on false data received from the production meter by the command and control center. The eventual ramping up and down to dispatch the deficit or surplus of power from the PV lead to some severe impacts on the system's grid voltages, currents, and total system's power loss. The nodal voltage shows some voltage collapse with values going beyond and also below the $0.95 - 1.05 pu$ thresholds . The current values also significantly increased in some branches in the network. The system power loss was also impacted by this attacks. This abnormal system parameters could potentially lead to erroneous tripping of the protective devices which will cause cascading failures and possible system collapse. A machine learning-based protection system was also proposed in this chapter which can be effective way of dealing wit FDI attacks by comparing the new system dynamic parameters using a classification model developed from historical data and fault simulation studies. The proposed holistic protection framework can help prevent a total system collapse during an FDI attack on grid assets especially at high DER penetration scenarios.

References

Ameli A, Hooshyar A, El-Saadany EF, Youssef AM (2020) An intrusion detection method for line current differential relays. IEEE Trans Inf Forens Secu 15:329–344

Chen TM, Sanchez-Aarnoutse JC, Buford J (2011) Petri net modeling of cyber-physical attacks on smart grid. IEEE Trans Smart Grid 2(4):741–749

Conteh NY, Schmick PJ (2016) Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. Int J Adv Comput Res 6(23):31

Dagle JE (2012) Cyber-physical system security of smart grids. In: IEEE PES innovative smart grid technologies (ISGT) 2012, pp 1–2

Debnath A, Olowu TO, Parvez I, Dastgir MG, Sarwat A (2020) A novel module independent straight line-based fast maximum power point tracking algorithm for photovoltaic systems. Energies 13(12):3233

Dharmasena S, Choi S (2019) Model predictive control of five-phase permanent magnet assisted synchronous reluctance motor. In: IEEE Applied power electronics conference and exposition (APEC), 2019, pp 1885–1890

Dharmasena S, Olowu TO, Sarwat AI (2019) Bidirectional ac/dc converter topologies: a review. In. SoutheastCon 2019, pp 1–5

Eder-Neuhauser P, Zseby T, Fabini J, Vormayr G (2017) Cyber attack models for smart grid environments. Sustain Energy, Grids Networks 12:10–29

El Mrabet Z, Kaabouch N, El Ghazi H, El Ghazi H (2018) Cyber-security in smart grid: survey and challenges. Comput Electr Eng 67:469–482

Fard AY, Easley M, Amariucai GT, Shadmand MB, Abu-Rub H (2019) Cybersecurity analytics using smart inverters in power distribution system: Proactive intrusion detection and corrective control framework. In: IEEE International symposium on technologies for homeland security (HST). IEEE 2019, pp 1–6

Farraj A, Hammad E, Daoud AA, Kundur D (2016) A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems. IEEE Trans Smart Grid 7(4):1846–1855

Gunes V, Peter S, Givargis T, Vahid F (2014) A survey on concepts, applications, and challenges in cyber-physical systems. KSII Trans Internet Inf Syst 8(12):

Haack JN, Fink GA, Maiden WM, McKinnon D, Fulp EW (2009) Mixed-initiative cyber security: putting humans in the right loop. In: The first international workshop on mixed-initiative multiagent systems (MIMS) at AAMAS

Hawrylak PJ, Haney M, Papa M, Hale J (2012) Using hybrid attack graphs to model cyber-physical attacks in the smart grid. In: 2012 5th international symposium on resilient control systems, pp 161–164

He H, Yan J (2016) Cyber-physical attacks and defences in the smart grid: a survey. IET Cyber-Phys Syst: Theo Appl 1(1):13–27

He Y, Mendis GJ, Wei J (2017) Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Trans Smart Grid 8(5):2505–2516

Hu B, Zhou C, Tian Y, Qin Y, Junping X (2019) A collaborative intrusion detection approach using blockchain for multimicrogrid systems. IEEE Trans Syst Man, and Cybern Syst 49(8):1720–1730

Jafari M, Olowu TO, Sarwat AI (2018) Optimal smart inverters volt-var curve selection with a multi-objective volt-var optimization using evolutionary algorithm approach. In: North American Power Symposium (NAPS) 2018, pp 1–6

Kushner D (2013) The real story of stuxnet. IEEE Spect 3(50):48–53

Li X, Liang X, Lu R, Shen X, Lin X, Zhu H (2012) Securing smart grid: cyber attacks, countermeasures, and challenges. IEEE Commun Magaz 50(8):38–45

McLaughlin SE, Podkuiko D, Delozier A, Miadzvezhanka S, McDaniel PD (2010) Embedded firmware diversity for smart electric meters. In: HotSec

Mekonnen Y, Haque M, Parvez I, Moghadasi A, Sarwat A (2018) Lte and wifi coexistence in unlicensed spectrum with application to smart grid: a review. In: IEEE/PES Transmission and Distribution Conference and Exposition (T D) pp 1–5

Mo Y, Kim TH-J, Brancik K, Dickinson D, Lee H, Perrig A, Sinopoli B (2011) Cyber-physical security of a smart grid infrastructure. Proceedings of the IEEE 100(1):195–209

Odeyomi O, Kwon HM, Murrell DA (2020) Time-varying truth prediction in social networks using online learning. In: 2020 International Conference on Computing, Networking and Communications (ICNC), pp 1–5

Olowu TO, Jafari M, Sarwat AI (2018) A multi-objective optimization technique for volt-var control with high pv penetration using genetic algorithm. In: North American power symposium (NAPS) 2018, pp 1–6

Olowu TO, Sundararajan A, Moghaddami M, Sarwat A (2019) Fleet aggregation of photovoltaic systems: a survey and case study. In: 2019 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)

Olowu T, Sundararajan A, Moghaddami M, Sarwat A (2018) Future challenges and mitigation methods for high photovoltaic penetration: a survey. Energies 11(7):1782

Olowu TO, Jafari H, Moghaddami M, Sarwat AI (2019) Physics-based design optimization of high frequency transformers for solid state transformer applications. IEEE Ind Appl Soc Ann Meet 2019:1–6

Olowu T, Jafari H, Dharmasena S, Sarwat AI (2019) Photovoltaic fleet aggregation and high penetration: a feeder test case. SoutheastCon 2019:1–6
Olowu TO, Jafari M, Sarwat A (2019) A multi-objective voltage optimization technique in distribution feeders with high photovoltaic penetration. Adv Sci Tech Eng Syst J 4(6):377–385
Ozay M, Esnaola I, Yarman Vural FT, Kulkarni SR, Poor HV (2016) Machine learning methods for attack detection in the smart grid. IEEE Trans Neu Networks Learn Syst 27(8):1773–1786
Ozgur U, Nair HT, Sundararajan A, Akkaya K, Sarwat AI (2017) An efficient mqtt framework for control and protection of networked cyber-physical systems. In: IEEE Conference on Communications and Network Security (CNS) 2017, pp 421–426
Parvez I, Islam N, Rupasinghe N, Sarwat AI, Güvenç I (2016) LAA-based LTE and Zigbee coexistence for unlicensed-band smart grid communications. SoutheastCon 2016:1–6
Parvez I, Sarwat AI, Pinto J, Parvez Z, Khandaker MA (2017) A gossip algorithm based clock synchronization scheme for smart grid applications. In: North American Power Symposium (NAPS) 2017, pp 1–6
Qi J, Hahn A, Lu X, Wang J, Liu C-C (2016) Cybersecurity for distributed energy resources and smart inverters. IET Cyber-Phys Syst Theo Appl 1(1):28–39
Rahman S, Moghaddami M, Sarwat AI, Olowu T, Jafaritalarposhti M (2018) Flicker estimation associated with pv integrated distribution network. SoutheastCon 2018:1–6
Saleem D, Sundararajan A, Sanghvi A, Rivera J, Sarwat AI, Kroposki B (2019) A multidimensional holistic framework for the security of distributed energy and control systems. IEEE Syst J 1–11
Sarwat AI, Sundararajan A, Parvez I (2017) Trends and future directions of research for smart grid iot sensor networks. In: International symposium on sensor networks, systems and security. Springer, pp 45–61
Sharing EI, Center A (2016) Analysis of the cyber attack on the Ukrainian power grid: defense use case pp 1–5
Smart grid 2019. [Online]. Available: https://www.nist.gov/el/smart-grid
Srikantha P, Kundur D (2016) A der attack-mitigation differential game for smart grid security analysis. IEEE Trans Smart Grid 7(3):1476–1485
Srivastava A, Morris T, Ernster T, Vellaithurai C, Pan S, Adhikari U (2013) Modeling cyber-physical vulnerability of the smart grid with incomplete information. IEEE Trans Smart Grid 4(1):235–244
Stefanov A, Liu C (2012) Cyber-power system security in a smart grid environment. In: IEEE PES Innovative Smart Grid Technologies (ISGT) 2012, pp 1–3
Sundararajan A, Chavan A, Saleem D, Sarwat AI (2018) A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security. MDPI Energ 9:2360
Sundararajan A, Sarwat AI, Pons A (2019) A survey on modality characteristics, performance evaluation metrics, and security for traditional and wearable biometric systems. ACM Comput Surv 52(2):1–35
Sundararajan A, Hernandez AS, Sarwat A (2020) Adapting big data standards, maturity models to smart grid distributed generation: critical review. IET Smart Grid (2020)
Sundararajan A, Khan T, Moghadasi A, Sarwat AI (2018) Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies. J Mod Power Syst Clean Energy 1–19
Sundararajan A, Olowu TO, Wei L, Rahman S, Sarwat AI (2019) Case study on the effects of partial solar eclipse on distributed pv systems and management areas. IET Smart Grid (2019)
Teymouri A, Mehrizi-Sani A, Liu C-C (2018) Cyber security risk assessment of solar pv units with reactive power capability. In: IECON 2018–44th Annual Conference of the IEEE Industrial Electronics Society. IEEE, pp 2872–2877
Wadhawan Y, Neuman C, AlMajali A (2017) Analyzing cyber-physical attacks on smart grid systems. In: Workshop on modeling and simulation of cyber-physical energy systems (MSCPES) 2017, pp 1–6
Wang Y, Amin MM, Fu J, Moussa HB (2017) A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids. IEEE Access 5, 26-022–26-033

Wei J, Kundur D, Zourntos T, Butler-Purry KL (2014) A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control. IEEE Trans Smart Grid 5(6):2687–2700
Wei L, Sundararajan A, Sarwat AI, Biswas S, Ibrahim E (2017) A distributed intelligent framework for electricity theft detection using Benford's law and Stackelberg game. Resilience week (RWS) 2017:5–11
Wei L, Gao D, Luo C (2018) False data injection attacks detection with deep belief networks in smart grid. In: Chinese Automation Congress (CAC) 2018, pp 2621–2625
Zhaoyang D (2014) Smart grid cyber security. In: 2014 13th International Conference on Control Automation Robotics Vision (ICARCV), pp 1–2 (2014)