Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

DETECTION AND MITIGATION OF CYBERATTACKS ON SMART GRID VOLTAGE STABILITY MONITORING

[#1]SAMREEN FATHIMA, ***M.Tech Student,***
[#2]Dr. GULAB SINGH, ***Associate Professor,***
[#3]Dr. N.CHANDRAMOULI, ***Associate Professor& HOD,***
Department of Computer Science & Engineering,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR.

ABSTRACT: Specifically, the goal of this investigation is to determine whether voltage stability monitoring for a power transmission system is vulnerable to cyber-physical attacks. Traditional voltage stability monitoring systems, which employ voltage stability indices, will be able to defeat these systems since the adversary will not be able to recognize when there is an instability in the system. If the computer senses a problem, it may induce the power system operator (PSO) to take unproductive steps, which could be dangerous. In order to avoid and battle this devastating attack, an unique intrusion detection indication as well as a novel mitigation method are given. This proposal makes use of the multi-port equivalent circuit of the power system to aid in the calculation of the TE parameters in the transmission system. The attack on the data from the Phasor Measurement Unit (PMU) is discovered by this TE parameter analysis. By implementing the proposed mitigation technique, the power distribution system (PSO) is able to identify which PMU is under attack, while the other PSOs are only notified of the attack as it occurs. The number of compromised PMUs is used to estimate the number of injection attack vectors. The effectiveness of the solutions presented is proved through the use of real-world situations.

***Index Terms*—**Cyber-physical attack, voltage stability, Wide Area Measurement System, Phasor Measurement Unit.

---

1. INTRODUCTION

This is because they are critical to society since they have a substantial impact on individuals and the economy. When selecting different examples, take into consideration the flow of energy, the production of telecommunications, and the provision of water. These cyber-physical systems make use of two-way communication and distributed intelligence to improve efficiency, dependability, and stability while reducing costs. A further problem is that these systems are more prone to cyber attacks because there is a relationship between virtual and physical activity. At this point, attacks that take advantage of vulnerabilities in physical and cyber systems are possible, and as a result, additional security measures are needed.

The electric grid has undergone significant transformation over the last century, evolving from a collection of disparate local community-based systems to something that may be the world's largest and most intricate cyber-physical system, according to some estimates. The development of smart grids has occurred as a result of the increased demand for dependable energy. In order to meet future electricity

demands, the smart grid will incorporate distributed generation, renewable energy sources, electric vehicles, and demand-side regulation of electricity generation and consumption. Complex smart grids are vulnerable to assaults from adversaries all over the world because of the high levels of cyber infrastructure in place. For another example, when a group of hackers targeted electrical power plants in the country in 2015, it is estimated that between 80,000 and 100,000 Ukrainians were left without energy. As a result of this incident, the Metcalf substation of Pacific Gas & Electric experienced damage in the amount of about $15 million (PG&E). The two attacks both purposefully targeted sensors in order to prevent control centres from functioning, even if doing so resulted in collateral damage to other systems.

Control loops that accept sensor data as input and offer control decisions as output are critically necessary for the operation of sophisticated cyber-physical systems. When a large-scale attack is launched, the operator control loop is abused in order to conceal or magnify the magnitude of the attack. Operators keep a close eye on the situation and make decisions based on what they observe and learn. Even if there is no physical harm done to the gadget, the consequences of this loop could be widespread and devastating in nature. All of these assaults have one thing in common: they all cause sensor data to be distorted.

Due to the fact that sensors are frequently the most vulnerable components to cyber attacks, it is critical to maintain them insulated or to reinforce them in some other way. Smart grid scenarios including SCADA sensors, PMUs, or smart metres are possible (AMI). The implementation of a system that monitors sensor activity in real time is required in order to accommodate the additional sensors and to allow for prompt response to inaccurate sensor data when it occurs.

Due to the fact that existing methodologies were developed with a specific goal in mind, detecting cyber-attacks on sensor data is extremely difficult (e.g., system reliability). Sensors may sound an alarm if they detect that they are "out of boundaries." The presence of subtle integrity assaults can be detected, however identifying obvious attacks is challenging. When performing replay assaults, all the attacker needs to do is copy the sensor signals exactly and then play them again past the sensor to get access to the system. Therefore, their measurements will never be outside of the prescribed range, which prevents an alert from being produced in the first place. To more effectively detect multiple integrity violations over a wide range of operating conditions, it is vital that a novel multi-sensor approach be developed and implemented.

A more advanced sort of attack detection has been implemented in order to contribute to the overall safety of smart grids. Today's bad data detection techniques are inadequate against sophisticated data injection assaults that are well-versed in the power network's structure and may exploit this knowledge. Secure devices were put across the system in order to raise the overall system security index. After a significant amount of research, a computationally efficient technique for detecting and localising assaults was developed after rigorous testing. A graph theoretic strategy based on safe PMU is offered as a means of protecting against cyber attacks that compromise data integrity. On the basis of the time-varying network topologies provided by PMUs and smart metres in real time, a revolutionary novel approach to network security monitoring for large-scale changing energy systems is presented. This approach allows for on-demand, constant network security monitoring for large-scale changing energy systems. Recently, it has been discovered that detection speed and detection performance are mutually incompatible in nature.

The majority of the technologies on this list are unable to do so because the physical laws of the electric grid have not yet been included into the technology's operation. The sensors monitor

physical activities that are governed by rules of physics that are unchangeable in their nature. Although the values of current and voltage are proportional to one another when measuring them, a variable that is dependent on circuit resistance must also be taken into account when measuring current and voltage. It is far easier to make a complex physical system more complicated than it is to make a simple physical system more complicated. Each succeeding sensor reading will demonstrate how utterly reliant we are on one another in the long run. If there are any deviations from the sensor requirements, data integrity problems will be detected and reported.

2. CYBER ATTACK CLASSIFICATION

A. Vulnerabilities of Smart Grid Sensor Networks

An inoperable system can be attacked in order to cause damage or loss to the system. Smart grids are susceptible to manipulation due to problems with hardware, software, and network connections. Utility operation centres and system operation centres have been brought together through the use of a variety of data communication protocols. SCADA systems are one of the most vulnerable places in most current protocols. Substation components such as circuit breakers, capacitors, and measurement equipment are all contained within the substation and may therefore be managed remotely. It is feasible to make smart grid vulnerabilities more exploitable in the event of a cyberattack by utilising these remote-controlled functionalities. There is also a possibility that the programmes and apps that are placed on the computers of utility companies will be vulnerable to attack from outside sources. The exploit would present itself as a result of this vulnerability when approached from the top-down.

B. Classification

The CIA triad, which stands for Confidentiality, Integrity, and Availability, is one of the fundamental concepts of information security (Confidentiality, Integrity, and Availability). A cyber attack can be classified and classified into one of three categories, which are as follows: Throughout the remainder of this section, we will cover four basic types of cyber attacks.

- **Interception**

Attacks on concealment, whether overt or covert, are included in this category of activities. However, utilising cryptography, this attack can be prevented from being detected and launched. These are the five most common types of interception attacks: eaves dropping, wiretapping, tapping into fibre optics, packet sniffing, and keystroke logging, to name a few.

- **Interruption**

The availability of a cyber asset is interrupted by an unauthorised person, resulting in an interruption. In order to achieve the ultimate purpose, the systems must be able to detect and respond to a Denial-of-Service attack. Precautions such as blocking communications signals, preventing software from functioning properly, and wiping data are all possibilities.

- **Modification**

Making changes to anything on a computer can be classified as either a failed attack in which the invader obtains something or an attempted attack in which the attacker attempts to damage something but fails. In the case of information security, integrity is jeopardised due to the vulnerability to modification assaults. The problem can be avoided with the use of cryptography. Typically, an assault has the following three effects: interference with the control signal, data corruption that affects sensor readings, and reduced energy use.

- **Fabrication**

The term fabrication refers to the act of an unauthorised third party inserting fictitious objects

into an existing system. Authentication is not a target of this attack. In order to locate it, encryption is required. In order to aid in the break-in, an attacker floods the system with fictitious control signals or fictitious money transactions in order to make the profits appear as if they came from within the system. It is feasible to target a cyber device that is a component of a smart grid by employing any of the attack categories listed above. This study will cover grid transients as well as how modification attacks can have an impact on grid stability.

3. CYBER-PHYSICAL ATTACKS IN SMART GRID

Man-in-the-Middle Attack: Man-in-the-Middle (MITM) attacks are eavesdropping tactics in which the adversary attempts to establish multiple connections and interacts with the victim in between. Man-in-the-Middle (MITM) attacks are a type of eavesdropping tactic in which the adversary attempts to establish multiple connections and interacts with the victim in between. Finally, end users have the impression that they are directly communicating with one another. When transferring data measured by the Phasor Measurement Unit, some programmes still use UDP rather than TCP/IP, which is a legacy of the 1990s (PMU). This feature aids in the prevention of Man in the Middle (MITM) attacks. However, utility businesses may also communicate via public lines, which are vulnerable to network attacks. Private lines are significantly more secure, and they are used by a much larger number of companies. As a result, MITM attacks are frequently used to initiate attacks by gaining access to crucial system components. This is because MITM attacks can be used to distort information included in delivered packets, such as price signals, measurement data, and control commands, among other things.

Distributed Denial of Service Attack (DDoS): in When connecting to the PMU communication network over a wide area network (WAN), there is an increased risk of PMU-related problems. Malicious software can be placed on the router that is connected to the communications network at the substation, and if the new password for the devices is discovered, access to the devices can be achieved through the router.

A distributed denial of service (DDoS) attack seeks to deny authorised users access to a crucial resource when that resource is required in large quantities. When the electricity system is on the verge of becoming unstable, communication channels should be made available to all parties involved. A successful denial-of-service attack would jeopardise the reliability of the power grid.

When a distributed denial of service (DDoS) attack is launched, the attack is referred to as a DDoS attack because it is often triggered by a computer infected system or by a Trojan that targets only one system. In a "epidemic of hackers," there are two phases: the recruitment phase and the actual attack phase. The recruitment phase is the first part of the epidemic.

Aents Recruitment Phase: In order to launch an AMI DDoS attack, the attacker must identify the metre locations that he will use in his attack. Due to the fact that the numerous AMI metres have characteristics that are similar, it is possible that a security weakness in a single metre might be replicated across several additional metres. Once the attacker has made contact with a large number of infected IP-based smart metres, he or she contacts the IP-based smart metres and causes a service outage. When a connection is in the middle of an attack, an attacker can exploit the vulnerability by introducing a malicious application (or, in certain cases, a hardware or software fault), or they can use a whole other sort of attack entirely. By choosing an appropriate propagation model, malicious code can be disseminated more easily. Attackers can insert malicious code into a source file that they have created. As a result, each and every agent

becomes infected (repository model). Alternatives include using malware to distribute it to several customers, with each client downloading the malicious code from the infected server (back-chaining model). Alternatively, malware can be distributed as part of a source file, with each agent downloading code from the source file (the repository approach) (The Autonomous model). Furthermore, IP spoofing can be used to mask infected agents, making it more difficult to determine the source of an attack in a case when there are thousands of potential sources of attack.

Actual Attack Phase: The launch of a distributed denial of service (DDOS) attack through the deployment of three different attack methods:

Attacks on protocol: If these vulnerabilities are exploited, it is possible that users' resources would be abused. A specific AMI service, such as the head end or data collection unit, can be rendered non-responsive in this manner by increasing the number of TCP SYN requests issued to the specified port or network device, as seen below (TCP).

Attacks on infrastructure: Attackers could deliberately disrupt the routing tables of AMI packet exchange networks in order to magnify the effect of packet distribution on the network.

Attacks on bandwidth: It is feasible to send a large amount of data by using a large number of agents. With increased traffic, real packets will have a lower likelihood of being dropped (the drop ratio can be considerable).

False data injection attack: The term "false data injection attack" refers to an integrity attack when the attacker is able to inject bogus data into sensors that can be utilised to replace authentic data. When attackers inject wrong data into random vectors, they have the ability to launch an attack or to disrupt specific variables by calibrating them with specific units, among other things.

When one looks at the network from the attacker's point of view, it becomes clear that they have complete knowledge of the topology and are able to manipulate a large number of system variables. In the event that sensitive information has been compromised, detecting dangerous data attacks becomes more difficult. Traditional processes protect critical sensors in the power system, so it is necessary to employ them in order to avoid false data injection attacks. Attack vectors such as load quantity manipulation (for load relocation attacks) and load quantity change are only a few examples of what could be used (for load quantity manipulation).

Jamming attack : Distributed Denial of Service (DDoS) attacks are a type of attack that targets the ability to interact in real time and is carried out by using a verifier. Because of the jamming, erroneous estimates of the system's present operational state may be produced, resulting in inaccurate electricity costs. One of the primary purposes of starting a battle is to gain control of the electricity market, while the other is to cause a worldwide economic catastrophe. A jam causes the pricing system to be dependent on estimations that are not received by the control centre.

The use of discrete time is a common assault tactic in jamming. Consequently, the attack is divided into intervals of time. A small number of sensors are prone to jamming because of the impact that it has on power distribution; yet, the inaccuracies caused by these sensors can cause widespread power outages and higher energy expenses. Because of this jamming attack, everyone in the vicinity has a greater probability of being identified. Finally, in order to launch a jamming attack, you must follow the steps outlined below:

In order to prevent measurements from being available when a time period begins, jammed signals are used. It is as a result of this that real-time fare estimations are inaccurate.

In the event that measurements are not available, the control centre will rely on default values from the DC optimal power flow model to compensate.

These measurements and forecasts have long been regarded as highly suspect, and they have been used to follow the electrical market over an extended period of time.

If the jamming is stopped, the opponent should expect to be able to obtain real-time measurements of prices.

While engaged in network jamming, the adversary is able to purchase electricity at a cheaper price and sell it at a higher price in order to profit from the difference in real-time pricing.

4. COUNTER MEASURES AND PROTECTIVE ACTIONS AGAINST CYBER ATTACKS

A. IP Fast Hopping mechanism

Many measures are in place to help prevent DDoS assaults from taking place. Authentication, authorization, and accounting (AAA), access control lists (ACLs), and network firewalls are examples of countermeasures that are classified as either blocking or discovering attacks. Identifying the source of an attack and taking appropriate action are examples of countermeasures that are classified as either blocking or discovering attacks.

One method of avoiding unwanted activity is known as IP Fast Hopping, which allows even the most powerful hostile streams to instantly adapt to changing network conditions. Despite the fact that it is a beneficial means of disguising communications information and targeting servers to withstand DDoS attacks, the technology has not gained widespread adoption yet. The technique makes use of IP address overlap to make it appear as though the server's IP address is actually spread across a large number of other IP addresses, so concealing the host's true location from the client. Every time a communication takes place, two fictitious IP addresses are matched with an actual IP address, and this process continues indefinitely. As long as a user with a schedule-changing capability has access to the entire IP address range, it limits an attacker's ability to bring down a server by overburdening it. Using an approach that is divided into different streams, network stress can be reduced by reducing the load on the overall network.

B. Encryption Mechanisms

The different standard encryption algorithms and authentication systems are in place to protect the confidentiality and integrity of the data stored on the system. This has been demonstrated in previous studies, in which researchers developed their own cryptographic systems while keeping the cost and energy consumption of the device in mind. In actuality, there are many different types of encryption available. One of the most well-known symmetric encryption schemes is the DES (Data Encryption Standard), which was created by IBM in 1977. the most technologically advanced encryption algorithm Another example is the use of 128-bit AES encryption by Zig Bee, which is another illustration of this. Another type of encryption technique has been mentioned in previous work: asymmetric encryption systems.

In comparison to asymmetric cypher, which has a longer lifespan, symmetric code is capable of storing and processing massive amounts of data quickly and efficiently. Because there are so many things that are publicly broadcast, it is strongly advised that you use a specific method to modify the symmetric encryption. When employing cryptographic methods, the most important problem to consider is how to manage the encryption key, which is something that the SG is actively discussing. The Public Key Infrastructure (PKI) serves as the foundation of a successful key management system. Increased communication traffic as well as the addition of new equipment may raise the overall cost. A new generation of technologies is being created to better protect the home network (HAN) through the use of creative metering strategies, such as those that optimise the metering architecture, increase data security, and reduce data aggregation.

C. IDS-based Technologies

It will be necessary to expose SCADA systems to security threats, such as SCADA systems lacking built-in security and SCADA systems with outmoded computing resources, in order to successfully implement the SG. As a result, it is critical that we develop Intrusion Detection Systems (IDS) that can monitor system operation and detect threats, such as unauthorised user activity or attacks that have been orchestrated. For example, intrusion detection technologies that analyse statistical patterns and those that employ SCADA (supervisory control and data acquisition) for the first time are frequently developed.

Network traffic for SCADA systems is classified into two categories using IDSs, which apply statistical methodologies to categorise network traffic into two groups, namely normal and abnormal behaviour. In addition to regression models, neural networks, and Bayesian networks, statistical models constructed with the help of these methods are referred to as regression models, neural networks, and Bayesian networks. While the vast majority of intrusions are ultimately rejected, most intrusion detection methods are prone to producing false positives, which creates unnecessary alarms while also causing actual security alarms to be slowed down.

An intrusion detection system (and the components that make it up) nearly always includes a monitoring agent, a server, and a graphical user interface. Centralised, embedded, and committed Internet Dissemination Strategies are the three fundamental forms of Internet Dissemination Strategies that can be found. Several characteristics of a given client can be examined to determine if a specific user or group has engaged in suspicious or damaging behaviour. These characteristics include an unplanned power outage, unexpected log data, unusual communication traffic, and a lack of communication on a regular basis. Anomaly-based monitoring, stateless specification-based monitoring, and full specification-based monitoring are three of the most prominent monitoring strategies now being used in the information technology sector. The guardian is responsible for ensuring that all security elements in the system are operational. Patching software, updating firmware, and configuring protocols, as well as identifying and correcting software errors, are all covered.

Dedicated SCADA-specific IDSs implement critical detection approaches for SCADA systems, particularly for those that rely on state, model, and rule-based methods of detecting anomalies in data. While there are just a few SCADA protocols and apps available at this moment, the overall number of available protocols and applications is still very small. This comprises rule-based intrusion detection systems for SCADA systems that take advantage of IEC 61850, as well as an intrusion detection system that relies on critical state-based monitoring.

5. MACHINE LEARNING BASED ATTACK MITIGATION

A system's overall function must be maintained while the severity of malicious activity is kept to a minimum. This is called mitigation of an attack's impact. Hillsborough (the name of a soccer team) serves as a great example of how the ML-based attack mitigation method was put into practise. A cyber-physical model based on a deep belief network (DBfN) is developed to identify and neutralise foreign direct investment threats while maintaining the transient stability of wide-area monitoring systems, according to the authors (WAMSs). Researchers in the field of alternating current power systems ran a DQN detection scheme simulation and compared the results to baseline DQN detection schemes. The accuracy and speed of the DQN detection method were higher than those of the baseline approaches, indicating that it was superior.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

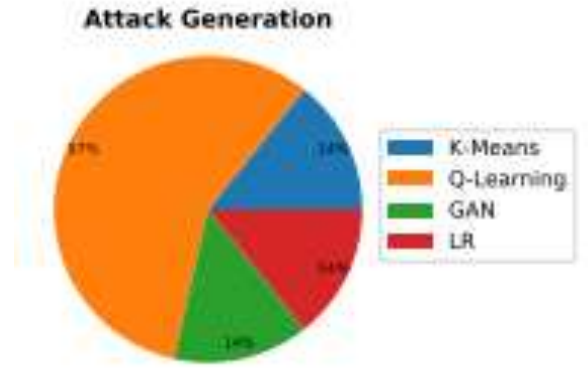
Chen et al. [24] presented a voltage controller for an autonomous voltage regulator that is based on Q-learning and has been demonstrated. They replaced the estimated values for problematic data with maximum likelihood estimation (MLE) values in order to ensure that OPF-based controls are trusted by all parties involved in the process. To address the issue of data unavailability, Maharjan et al. proposed an SVM-based robust SG network that incorporates DERs to battle the problem (DUA).

The KNN algorithm was used in the development of the localization-based key management system for AMI network node/meter authentication created by Parvez et al. for AMI network node/meter authentication. As a result of using the KNN approach, it was discovered that it is feasible to distinguish between two metres with respect to their transmission frequency, packet size, and distance between two metres.

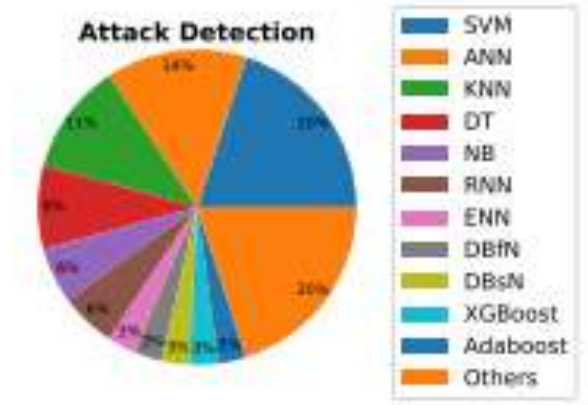
Using an unknown and unknowable network topology, the GAN model developed by Ren et al. forecasted PMU data that was either absent or inaccessible. This research study describes a GAN (genetic autoencoder) strategy to synthesise a false attack dataset from the current one using genetic autoencoders. By utilising smart grid technologies, they were able to get 91 percent of their F1 score for identifying a variety of cyber-attacks. According to researchers Ying and colleagues, another another study has been discovered, which shows that using a GAN-based technique can increase attack detection accuracy by 4 percent. Li et al. suggested a GAN-based model that incorporates anticipated measurement variance and detects and recovers sensors that have been compromised in order to combat foreign direct investment (FDI) attacks.

CLASSIFICATION OF ML-BASED ATTACK MITIGATION TECHNIQUES IN SMART GRID

Reference	Institution	Publication Year	Attack	ML Model Type	ML Algorithm	Testbed
Chen et al. [24]	Tsinghua University Beijing, China	2019	FDI	Reinforcement	Q-learning	IEEE 39 bus
Li et al. [48]	North China Electric Power University, China	2019		Unsupervised	GAN	IEEE 30, and 118 bus
Wei et al. [49]	University of Akron, USA	2016			DBN	New England 39 bus power system
An et al. [50]	Xian Jiaotong University, China	2019	DIA	Reinforcement	Q-learning	IEEE 9, 14, and 30 bus system
Parvez et al. [51]	Florida International University, USA	2016		Supervised	KNN	AMI network
Maharjan et al. [52]	University of Texas at Dallas, USA	2019	DUA	Unsupervised	SVM	MPEI
Ren et al. [53]	Nanyang Technological University, Singapore	2019			GAN	New England 39 bus
Shahriar et al. [54]	Florida International University	2020	LAD		GAN	KDD-99
Ying et al. [55]	Zhejiang University, China	2019			GAN	Synthetic

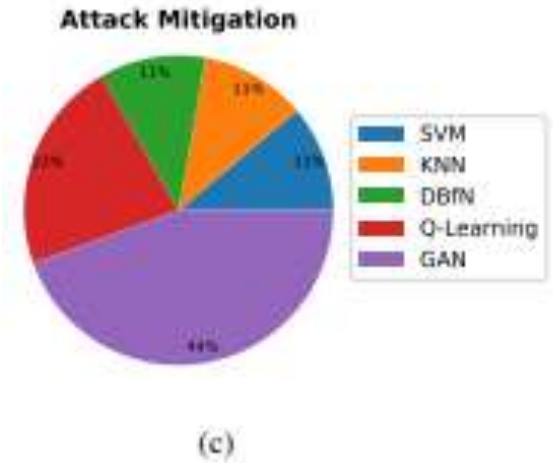


(a)



(b)

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023



(c)

Fig. Pie-chart of mostly used ML techniques in a) generation, b) detection, and c) mitigation of cyber attacks in smart grid

6. CONCLUSION

Specifically, the purpose of this paper is to evaluate the security concerns associated with voltage monitoring systems in power plants that have been penetrated by cyber-physical attacks. The first half of the paper provides an overview of voltage stability monitoring in smart grids, followed by a description of a strategy for creating assaults that will be used to demonstrate that voltage stability attacks are technically viable. It is proposed that a novel indicator be used to identify attacks. With the new indication, you may identify attacks and collect the collection of under-attack PMUs that is relevant to the present attacks only, according to the indicator. System-based attack detection and mitigation is presented, which gathers the set of under-attack PMUs and estimates the amount of injected false data or false data injection, both of which can be achieved without the requirement for historical information. Numerous advantages will accrue as a result of the detection and mitigation approaches that are now being investigated. Attackers attempting to cause damage to the measurements that are needed to determine whether or not a problem exists in the grid would be an example of an attack on the grid's power flow equations. However, the new technique has additional benefits that go beyond those provided by data-driven approaches, and it is also more straightforward to adopt (neither data of the system in normal operation nor the data in various under-attack conditions). When applied in a simulation environment, our proposed solutions were tested in near real time on a realistic set of test systems and were successful. A significant portion of this research's future will be devoted to the study of frequency instability assaults and the development of improved estimators to be employed in these attacks.

REFERENCES

- Anjan Debnath, Temitayo O Olowu, Imtiaz Parvez, Md Golam Dastgir, and Arif Sarwat. A novel module independent straight line-based fast maximum power point tracking algorithm for photovoltaic systems. Energies, 13(12):3233, 2020.
- Chitta Ranjan Saha, M Nazmul Huda, Asim Mumtaz, Anjan Debnath, Sanju Thomas, and Robert Jinks. Photovoltaic (pv) and thermo-electric energy harvesters for charging applications. Microelectronics Journal, 96:104685, 2020
- Mohamadsaleh Jafari, Temitayo O Olowu, Arif I Sarwat, and Mohammad Ashiqur Rahman. Study of smart grid protection challenges with high photovoltaic penetration. In 2019 North American Power Symposium (NAPS), pages 1–6. IEEE, 2019.
- Anjan Debnath, Sukanta Roy, M Nazmul Huda, and M Ziaur Rahman Khan. Fast maximum power point tracker for photovoltaic arrays. In 2012 7th International Conference on Electrical and Computer Engineering, pages 912–915. IEEE, 2012.
- N. Akbar, M. Islam, S. S. Ahmed, and A. A. Hye. Dynamic model of battery charging. In TENCON 2015 - 2015 IEEE Region 10 Conference, pages 1–4, Nov 2015.

- Inga, R. Hincapie, C. Paida, and S. Espinosa, "Optimal geographic ′ placement of PMU for wide area measurement system," in Ecuador Technical Chapters Meeting (ETCM), pp. 1–6, 2016.
- P. Kundur, N. J. Balu, and M. G. Lauby, Power system stability and control, vol. 7. McGraw-hill New York, 1994.
- M. Kamel, A. Karrar, and A. H. Eltom, "Development and application of a new voltage stability index for on-line monitoring and shedding," IEEE Trans. Power Syst., 2017.
- Atputharajah and T. K. Saha, "Power system blackouts - literature review," in 2009 International Conference on Industrial and Information Systems (ICIIS), pp. 460–465, Dec 2009.
- Anzalchi and A. Sarwat, "A survey on security assessment of metering infrastructure in smart grid systems," in SoutheastCon 2015, April 2015, pp. 1–4.
- M. A. Salmani, A. Anzalchi, and S. Salmani, "Virtual power plant: New solution for managing distributed generations in decentralized power systems," in 2010 International Conference on Management and Service Science, Aug 2010, pp. 1–6.