Chapter 1

Cyber Attack Detection and Mitigation in Smart Power Systems

Joshua Chibuike Sopuru[1]

Abstract

The security of modern power systems is a pressing concern due to their real-time requirements and the integration of various technologies. Recent cyber incidents have highlighted the limitations of traditional security measures based on information and communications technology (ICT). To address these challenges, this chapter makes significant contribution in the field of cybersecurity for smart grids. By developing innovative methods based on machine learning algorithms, dynamic analysis, and belief propagation techniques, this chapter aims to enhance the detection, prevention, and mitigation of cyber attacks in power systems. One key contribution of the chapter is the development of a methodology that utilizes machine learning algorithms for the detection of false data injection attacks (FDIAs) during power system state estimation. By leveraging the power of machine learning, this approach enhances the ability to identify and mitigate FDIAs effectively. Additionally, this chapter investigates the emergence of stealthy FDIAs, improving the understanding and detection capabilities of modern machine learning algorithms. Furthermore, this chapter emphasizes dynamic analysis over steady-state analysis, addressing the limitations of traditional approaches. By considering the dynamic behaviors of power systems, this chapter enhances the understanding and detection of cyber threats. This approach provides a more comprehensive assessment of system behavior, particularly in the context of cyber attacks, thereby strengthening the overall security of smart grids.

1. Introduction

An explosion in the expected demand for electricity delivery is being driven by the use of cutting-edge technology in our everyday lives, which has been followed by some technological improvements inside the industrial

1 Girne American University, https://orcid.org/0000-0001-7049-0058, joshuasopuru@gau.edu.tr

https://doi.org/10.58830/ozgur.pub250.c1200

zone. Industry 4.0, additionally known as the fourth industrial revolution, makes use of modern technologies like synthetic intelligence, the internet of things, high-tech communications, and plenty of others to create cyber-bodily-oriented networks among humans and gadget mastering (L. M. Zawra, H. A. Mansour, and N. W. Messiha 2019, pp. 1-7). This revolution is converting electric-powered energy device architectures from physically remote electricity systems to extraordinarily interconnected cyber-bodily smart grids. This change has many advantages (Y. Lu, 2017, pp. 1-10).

Because the smart grid is a complex aggregate of the legacy physical grid, smart electronic devices, and embedded ICT, improvements include physical and cyber protection, technological development, standards, regulations, regulatory activities, and others. Power system stakeholders and policymakers globally have targeted cyber safety troubles due to the developing importance of conversation and cyber layers. This trend should persist. For instance, the American President's Council of Advisers on Science and Technology (PCAST) prioritizes cyber-physical electricity gadget protection studies (P. C., 2007), (G. Erbach & J. O'shea, 2019)

1.1 Background and motivation

It is essential to construct a defense against cyber assaults in an effort to assure the protection, dependability, and financial viability of the operations of the clever grid, which is the strongest area of the following technology. The term "clever grid" refers to a complicated cyber-physical network wherein electricity technology, transmission, and distribution structures are interconnected through the usage of modern, bidirectional data and communications generation-based networks as well as shrewd management algorithms (I.Xyngi, 2011).

The term "cyber protection" is used to explain the secure flow of information, the processing of facts, and the execution of manipulative actions amongst a huge number of interdependent entities in a smart electricity system ("What is a Smart Grid?", n.d.). The terms "generation," "transmission," and "distribution," as well as "market pricing," "control," and "operations," are protected among those entities. On the other hand, malicious cyber attacks are sizable disruptive occasions that produce unsatisfactory behaviors in smart grids and lead to the maloperation of computers and electronic controllers, which in turn ends in the tripping of cars and mills, load dropping, and complete black-out of the machine (Smart Grids European Technology Platform, n.d.).

Cyberattacks are becoming an increasingly common form of struggle. Malicious cyberattacks are one example of these unacceptable styles of conduct. A cyberattack can be launched against a power infrastructure both with the aid of insiders, inclusive of vengeful personnel, or by means of outsiders, inclusive of expert hackers, prepared criminals, or others of their kind. Either group might be responsible for the assault ("ICS Vulnerabilities Key Findings," n.d.).

By taking advantage of bugs and loopholes in software programs and communication protocols, cybercriminals can infiltrate the operational networks of energy structures and cause disruptions (G. Liang, al., 2017, pp. 3317-3318). This could bring about the disclosure of exclusive information, the disruption or blocking of communication and control signals, or the creation of incorrect or malicious measurements and commands in the gadget. This can damage the grid's bodily infrastructure, prevent strong transport, and begin system-huge cascading failures that could cripple a financial system (M. Zeller, 2011, pp. 130-136). Figure 1 shows the number of disclosed vulnerabilities targeting ICS.

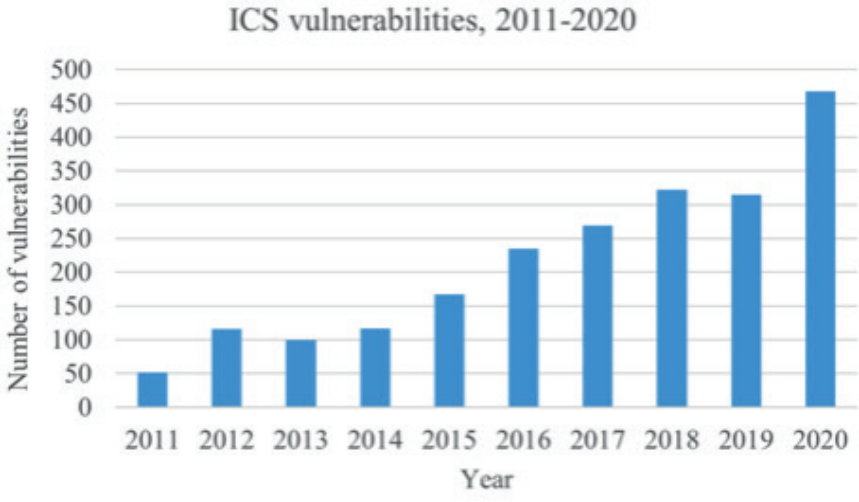


Figure 1: Number of disclosed vulnerabilities targeting ICS, 2011-2020 (Source: IBM Security X-Force).

The following is a condensed model of the cyber safety issues related to the efficient and reliable operation of clever electricity systems, as outlined in the aforementioned conversations:

- In light of the fact that the clever grid is a complex important infrastructure that has acquired a wonderful deal greater attention than the conventional strength grid, the advent of a choice aid device that is both stable and intelligent could seem as a treasured contribution.
- At the moment, the generation, transmission, and distribution of smart power systems are extremely interconnected with each other via verbal exchange networks that span huge geographical areas. Making decisions that can be suitable is extraordinarily reliant on the manipulated middle's capacity to as it should determine the nation of the gadget. The stability and dependability of strength systems can be jeopardized through managed responses that might be inaccurate or deceptive.
- Every asset of a clever energy grid is at risk of cyber assaults, and insufficient security features can lead to the manipulation of confidential statistics, which can have disastrous results in the manipulation and operations of the strength system.
- It is hard for a human operator to correctly differentiate between herbal disturbances along with faults and man-made disturbances together with cyber assaults in a strength device due to the fact disturbances in an electrical device are inherently complicated and might be because of both herbal occurrences or by using human pastime. To supplement the selections that human beings make while reacting to disturbances in strength structures, it is important for gadget learning algorithms to be able to differentiate between errors and cyberattacks.
- An adversary can take advantage of a machine's vulnerability to scouse borrow touchy facts and craft misleading size alerts in the sort of way as to avoid detection by traditional strategies of improper facts and to throw off the EMS's capability to accurately decide the gadget's present-day country. Attacks of the covert, fake facts injection variety are extra hard to come across and manipulate when they have been released. Additionally, because of the constrained wide variety of times of cyberattacks and the issues concerning their security, they may be uncommon.
- Intelligent protection devices are extremely reliant on digital information analysis, coordination, and control strategies, all of which are recognized as introducing today's forms of vulnerability into electricity systems. Because conversation networks are used for safety relay coordination and faraway upkeep options, it's very feasible for nefarious intruders to manipulate the operations of the device.

- The effect that credible contingencies and cyber-attacks have on a smart grid needs to be simulated, and the dynamic behaviors that occur at some stage in each scenario have to be thoroughly analyzed. This will allow one to better recognize the resiliency and vulnerabilities of the whole system.
- Due to the high computational burdens that may disrupt time-critical operations in actual-time strength systems, traditional ICT-based detection techniques aren't continually powerful at protecting against cyber assaults. It is viable to conduct an in-intensity analysis of the behavior of the machine at some point of unexpected occasions and cyber assaults. With these facts, it's far viable to design cyber assault countermeasure strategies with the intention to prevent instability and system-extensive cascading disasters.
- It is recommended that, following the detection of cyberattacks, suitable control instructions be carried out in order to mitigate the poor consequences of the assaults on system performance and improve gadget stability.

1.2 Research Objectives

This study proposes and investigates detection and mitigation strategies to guard against cyber assaults on strength system EMS, protecting gadgets, and AMI-based totally primary control mechanisms while making sure clever energy system reliability, protection, and stability. The essential research question is:

How exactly can one make use of an electric device's physical characteristics and dynamic behaviors?

Enhance the cyber safety of a SCADA-primarily based EMS, shielding devices like relays and circuit breakers (CBs), and a device-level controller in a powerful manner via detecting spurious cyber injections and mitigating the results of cyber attacks with the aid of both sending an optimized control sign or doing away with the malicious element from the gadget, all at the same time as retaining the protection, security, and balance of electricity networks.

The following goals have been described for you to take a look at in order for you to accomplish the primary cause of this study and provide answers to the research questions that have been posed as a part of this study:

1. The creation of false records injection attacks within the state estimation technique of a SCADA-based totally smart EMS, in addition to the

diploma to which these assaults are stealthy, can be investigated in this observe.

2. One of the targets of this assignment is to create and positioned into practice modern algorithms for machine learning in order to differentiate between natural disturbances and cyber assaults, inclusive of faults in a power network.
3. Developing a cyber-attack detection set of rules for a SCADA-based smart EMS this is primarily based on belief propagation and the handiest analysis of lengthy historic records that have not been compromised by using cyber attacks;
4. The manner of growing a set of rules that is primarily based on dynamic physical residences to be able to hit upon cyber assaults on a device-level controller by way of utilizing the distinction among the envisioned device state and the actual machine nation.
5. The development of a cyber-resilient decentralized controller that is able to generate an optimized management signal to mitigate the effects of cyber attacks on the device-level controller of the power system and keep apart the malicious unit so as to keep the system's stability at some stage in each regular-kingdom and the transient condition is something that needs to be worked on.

2. Literature Review

In this Section, a comprehensive literature survey is presented on a smart grid infrastructure, along with associated cyber-vulnerable nodes, cyber security requirements, cyber defense, and countermeasures, as well as other topics. After a quick introduction to the requirements for cyber security in a smart grid, conventional and non-conventional countermeasures are discussed.

2.1 Introduction

The discovery of energy has been extensively cited as one of the greatest contributions to human progress (M. H. Rehmani et al., 2015, pp. 3114-3118). Nearly all the technological endeavors that cutting-edge human beings partake in are made viable by the life of the electric energy device. Since the start of the improvement of the energy industry, studies, evaluation, and improvement of energy structures that might be reliable, steady, and value-powerful have been absolutely vital steps closer to enhancing human beings' standard of living ("Electricity Retains Power as Greatest Invention," n.d.).

In addition to this, there is an ever-increasing demand for the delivery of electricity, which is leading to the incorporation of several types of smooth and sustainable power sources into the power grid. Additionally, new forms of hundreds and garage devices are appearing in the marketplace thanks to clients. In order to reveal and exert control over such a difficult and ever-changing community of energy structures, state-of-the-art, and versatile devices are required. In addition, crucial enhancements to the growing older power grid are required in order that modern-day societal and environmental challenges may be effectively addressed.

In addition, the toolkits, abilities, and stages of cyber adversaries are continuously evolving, and it's miles from predicted that new types of cyber threats will emerge (M. Zeller, 2011, pp. 130-136). Additionally, state-of-the-art artificial intelligence has the potential to increase the competencies of cyber attackers. Because of the interconnected nature of the electric machine, an intense disruption in a single part of the gadget can also cause a whole blackout throughout the entirety of the device, which influences a huge part of the United States territory. Attacks finished through the net have the functionality of jeopardizing not only the safety of the nation as a whole but additionally the economic system and even the protection of its homes (R. McMillan, 2010). It is feasible for cyberattacks in the energy sector to have a cascading impact on different essential industries, including the financial area, the transportation area, and the healthcare industry. If they are not averted now, cyberattacks on Destiny's smart structures have the ability to halt an economy for several hours, intervene with verbal exchange, and disrupt operations (T. Chen and S. Abu-Nimeh, 2011, pp. 91-93).

2.2 Cybersecurity necessities

When it involves protecting the cyber-bodily energy grid infrastructure from malicious actors, the three most important necessities for cyber protection are normally considered to be the confidentiality of statistics, the integrity of information, and the availability of statistics (Y. Mo, T. H. Kim, 2012, pp. 195-209). Data from the meters, commands for controlling them, and pricing data are the top forms of records in an effort to be traded in the cyber infrastructure. The following is an outline of the significance of protective core information on the subject of the various requirements for cyber safety:

2.2.1 Confidentiality

Because the records saved in clever meters can reveal essential data about the consumption patterns of individuals or groups of customers, keeping

information confidential is a critical component of effective cyber protection. This touchy data may be utilized by a cyber attacker to construct harmful cyber injections, that can then be used to misinform the device's present-day states in addition to its future manipulation commands (Anwar & Mahmood, 2016, pp. 8-12). The privacy of the program, the accessibility of the control instructions, and the confidentiality of the pricing information are not important. The handiest aspect that ensures the privacy of the software is retaining the important thing as a mystery, which is something that may be executed by replacing encrypted messages among special machines (D. Thanos, Voloh, & Udren, 2012, pp. 335-357).

2.2.2 Integrity

Due to the fact that the software program, management instructions, and meter data are all critical to the operation of the grid, integrity is an important requirement for cyber security. If you convert the fee statistics, it can bring about errors in billing for the consumer, and if you inject a poor fee, it can cause a utilization spike that could bring about a loss of revenue. By tampering with the meter readings, an attacker can send out instructions that are either false or misleading and immediately affect the operation of the grid. On the other hand, maintaining the software's integrity intact is really important because malware that is present in compromised software programs may be used to control any gadgets or grid additives (Y. Mo, T. H. Kim, 2012, pp. 195-209).

2.2.3 Availability

It is essential to have access to the facts asked with the intention of arriving at vital decisions regarding management or manipulation within the allocated amount of time. Distributed denial-of-service attacks (also known as DDoS assaults) involve sending false or delayed facts to a server or network by way of meters or home equipment that has been compromised. As an instantaneous consequence of this, crucial records will either no longer be on hand or will not be on time when manipulation selections are being made, which will result in the instability of the machine (D. Kundur et al., 2010, pp. 244-249). The accessibility of both machines and electricity is an important element of smart grids. To be more precise, the inability to access up-to-date statistics regarding charges could have intense monetary or even legal repercussions, and using information that is out of date can have a terrible effect on the quantity of strength that is required (Y. Mo, T. H. Kim, 2012, pp. 195-209).

2.3 Overview of the Smart Cyber-Physical Grid Model

An electricity gadget is a complex network of physical additives that generate and transmit electricity from a remote geographical area to homes and industrial utilities. These additives include electricity flowers, transmission strains, and distribution substation.

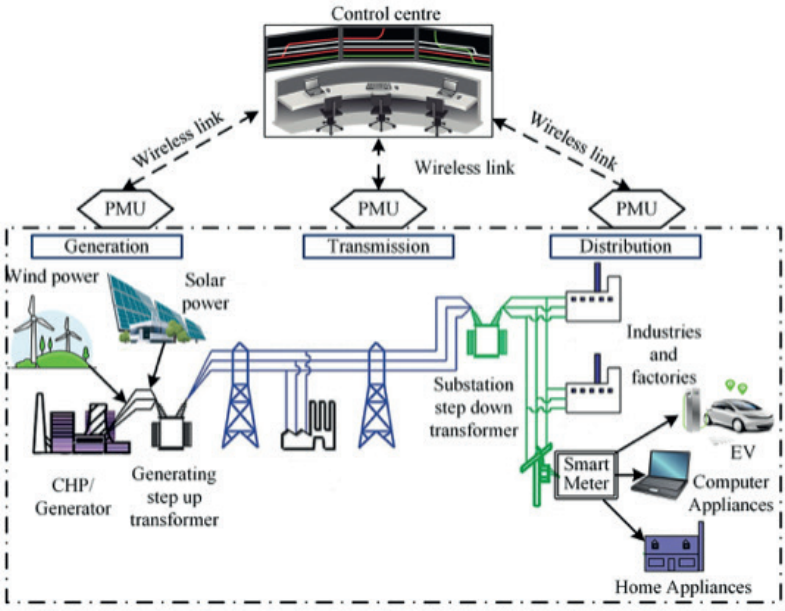


Figure 2: The ICT-based cyber-physical smart power system (Source: Amin, Ruhul 2021).

Continuous monitoring of the device states, making important manipulation selections during emergencies and changing running conditions, and executing control choices within a vital time frame are the steps that want to be taken in an effort to ensure the secure operation of an energy gadget. In the modern-day, significant demanding situations include the set up of larger energy stations to fulfill the higher demand for strength; the integration of dispensed renewable power resources for economic and environmental reasons; the rapid conversion of appliances that rely on fossil fuels to packages that depend upon energy, which includes electric cars; and a fantastically wide variety of different problems. As a result, current clever strength structures are starting to include record processing and communication infrastructure, which is based on ICT and further enhanced by superior control devices (A. Abur & Expósito, 2004).

2.4 Cyber Vulnerabilities within the Smart Grid

In this phase, we will be discussing the probable cyber-inclined areas that are embedded inside the cyber-physical device (CPS). The SCADA-primarily based manipulation middle is one instance of a cyber-vulnerable point. Other examples of cyber-susceptible factors include advanced metering along with PMUs, conversation networks, virtual protection gadgets in substations, and manipulating structures primarily based on AMI.

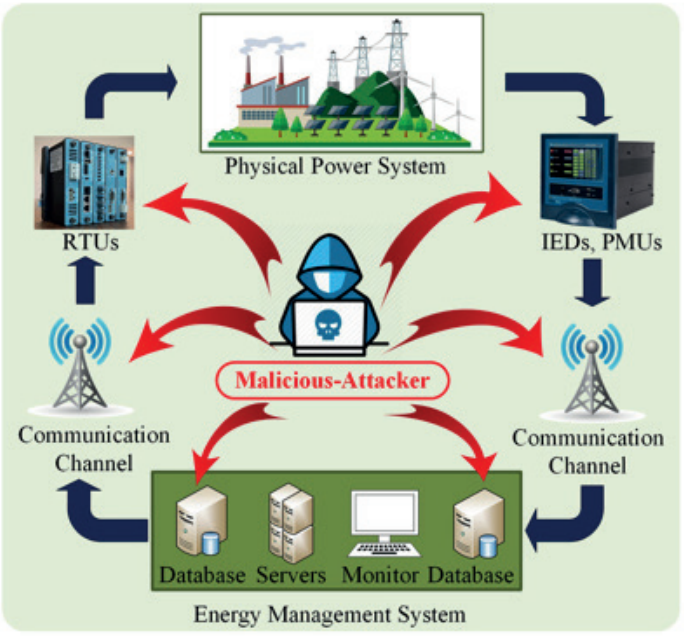


Figure 2.1: Cyber-vulnerable nodes in a power system EMS (Source: ResearchGate, n.d.)

2.5 Cyber Attack Countermeasures

The transition from conventional strength grids to smart cyber-physical grids is followed by an increase in the number of cyber vulnerabilities, in addition to a boom in the degree of complexity and capability of damage(G. Liang, et al., 2017, pp. 3317-3318). The fast deployment of allotted renewable resources, virtual dimensions, and control devices, facts and communication generation-based totally communique networks, and far-flung tracking and control with high processing capabilities all present new demanding situations for the strength quarter. In addition, the tight integration that exists between bodily and virtual structures makes it even more vital to pick out and discover cyber threats inside the clever grid infrastructure. The

process of detecting anomalies in reference to cyberattacks continues to be in its early stages.(The Industrial Control Systems Cyber Emergency Response Team, n.d.).

In order to effectively shield against cyberattacks, answers are required on multiple levels. For instance, end-to-end verbal exchange protocols need to be secured, smart gadgets need to be tampered with, numerous detection techniques need to be carried out, smart-meter and analyzing software want to be trojan horse-unfastened, and there are many other examples (P. McDaniel & McLaughlin, 2009, pp. 75-77). Developing a gadget that strikes a wholesome balance between performance and safety is another one of the challenges that must be overcome. Within the EMS, in addition to the other management gadgets, there ought to be particularly evolved techniques for the detection and mitigation of cyberattacks (Z. Fan et al., 2013, pp. 21-38).

2.5.1 IT-primarily based Defense Techniques

Atypical adversaries search for loopholes and vulnerabilities inside the communication community and protection protocols, control middle databases and software programs and manipulate devices for you to launch important cyber attacks with the aim of seizing control of the electricity device management and operations or taking them off track. Authentication, authorization, integrity, key control, and intrusion detection are the traits and attributes that make up the smart grid's cyber protection capabilities and attributes (Z. Fan et al., 2013, pp. 21-38). Several cyber vulnerabilities have been the subject of widespread research within the discipline of facts, and several safety and detection solutions have been proposed as a result. These answers include network/host intrusion detection systems (IDSs), firewalls, getting entry to control regulations, database security, cryptographic answers, and many others.

However, due to the huge scale, dispersed nature, and fluid nature of the clever grid infrastructure, it possesses a high level of complexity, which makes cryptography-based total key control a difficult problem to clear up (J. Hu, et al., 2014, pp. 1886-1895). Traditional mechanisms for imposing cryptography, including passwords, PINs, and tokens, are not able to determine whether or not a user is proper. Emerging bio-crypto mechanisms offer the opportunity of a way out of this hassle; however, the issue of encryption and decryption remains a huge impediment that wishes to be triumphantly overcome before this hassle may be solved (K. Xi & Hu, 2010, pp. 129-157).

2.5.2 Protection-based Totally Approach

Several studies of research were performed that allow you to determine the viable cyber vulnerabilities that can be found in electricity systems, in addition to the construction and stealthiness of the assaults, as well as ability protection mechanisms. In the context of SCADA-primarily based industrial manipulation systems, the FDIA is a good-sized cyber anomaly that happens for the duration of the kingdom estimation technique (X. Liu et al., 2015, pp. 1686-1696). Hacking the bodily meter or getting access to the conversation channels are both access factors. Protecting all the virtual meters from being corrupted is a straightforward method that can be used to push back attacks of this nature. On the other hand, all the digital devices in a large-scale and complex energy machine won't be economically or practically feasible. Instead of protecting all sensor measurements, it's miles possible to guard both a critical subset of measurements or a hard and fast list of state variables that have been carefully decided on. The safety of digital devices can be accomplished in some one-of-a-kind ways: by enclosing traditional meters in a more impregnable box, by improving the safety of communication, or by replacing conventional meters with more advanced meters that employ current technologies, including PMUs (R. Bobba et al., 2010, pp. 1-9).

2.5.3 Detection and Mitigation-based Approach

In addition to the improvement of safety schemes, a widespread variety of detection strategies have additionally been evolved as a protection mechanism in opposition to assaults that contain the injection of false data into an organization control gadget (EMS) for a smart grid (A. S. Musleh et al., 2020, pp. 2218-2234). A Kalman filter state observer and neural community anomaly detector are used in a networked management device (NCS) to hit upon fact integrity attacks on shared statistics. False fact detection in a kingdom estimator is a matrix separation problem, and nuclear norm minimization and occasional-rank matrix factorization are cautioned (A. Sargolzaei et al., 2020, pp. 4281-4292). Smart grid cyber anomaly injections are detected using an adaptive cumulative sum (CUSUM) technique.

3. Distinguishing between false information injection assaults and faults the use of machine studying algorithms

FDIAs can harm smart grid networks and result in blackouts. Cleverly crafted, stealthy bogus dimension vectors can fool the power control machine's BDD unit and mislead state estimation. This chapter proposes a device for gaining knowledge of an algorithm (MLA)-a primarily based

technique for detecting stealthy FDIAs in nation estimators and strength device troubles.(X. Liu et al., 2011, pp. 1-33). At first, the random and stealthy FDIAs goal was SCADA-based total electricity control structures. Stealthy assaults can steer clear of the same old chi-square test-primarily based BDD in strength system nation estimation and generate misleading and malicious manipulation movements. Then, advanced devices gaining knowledge of algorithms like Random Forest, OneR, Naive Bayes, SVM, and AdaBoost stumble on FDIAs in the SCADA database. The gadget's conduct amid external disruptions, including faults, complicates FDIA's identity (A. Abur & Expósito, 2004). Several case studies in simulated surroundings on an IEEE benchmark device reveal the justification and efficacy of the proposed technique.

The steady availability of a good enough supply of electrical power became a critical driving force behind the upward thrust of cutting-edge civilization. For the functions of strength management, the majority of trendy strength structures employ business management systems (ICS) that are totally based on SCADA. In the power management system (EMS) for the electricity grid, the state estimator (SE) is charged with the essential job of estimating the subsequent operational states. Additionally, the country estimator (SE) gives economic dispatch, foremost power waft, and contingency evaluation for the given time instance (Dan & Sandberg, 2010, pp. 214-219). This SE module is liable to cyber assaults, and compromising this module ought to lead to disastrous repercussions on the electricity machine, together with the robbery of power, cascade disasters, and blackouts.

3.1 Power System EMS Model

The maintenance-free and dependable operation of power systems necessitates the existence of a control mechanism that is both effective and well-coordinated. Incomplete or inaccurate monitoring of the system status and measurements can cause the EMS to take control measures that are not in the best interest of the system. In order to maintain consistent, dependable, and safe working conditions, an electrical management system (EMS) for the power system continuously monitors and manages the power grid. Two distinct types of data sets are gathered by the EMS control center in order to ensure accurate monitoring and control of the system. The settings for the transformer, the impedance of the line, and the condition of the circuit breakers and switches are examples of the topological and configuration data that make up one category of a data set. Measurement data collected at various nodes and branches constitute another category of data. In order to make an accurate assessment of the current state of the system, data of both

sorts is gathered and processed. Cyberattacks can target intelligent remote terminal units (RTUs), digital communication lines, and software-based control centers. When the meter readings are tampered with in a particular way, it is possible for them to remain unnoticed in the BDD and stealthy within the system. Figure 3 illustrates the cyber-vulnerable nodes that are present in FDIAs (X. Liu et al., 2011, pp. 1-33).

The procedure for estimating the state as well as the functionalities of the BDD module is outlined below. The protection-free and reliable operation of energy structures necessitates the lifestyles of a manipulation mechanism that is both powerful and well-coordinated. Incomplete or misguided monitoring of the system status and measurements can cause the EMS to take control measures that are not in the best interest of the device. In order to maintain consistent, reliable, and secure running conditions, an electrical control device (EMS) for the power system continuously video displays units and manages the strength grid. Two wonderful sorts of statistics units are accumulated via the EMS manipulation middle so that you can make certain correct monitoring and manipulation of the machine. The settings for the transformer, the impedance of the line, and the circumstances of the circuit breakers and switches are examples of the topological and configuration data that make up one class of statistics set. Measurement records accumulated at numerous nodes and branches constitute any other category of data. In order to make an accurate assessment of the present-day state of the system, facts of both types are collected and processed. Cyberattacks target clever faraway terminal units (RTUs), digital communication strains, and software-based control centers. When the meter readings are tampered with in a specific way, it's very possible for them to remain left out inside the BDD and stealthy inside the device. Figure 3 illustrates the cyber-prone nodes that might be found in FDIAs. The technique for estimating the nation as well as the functionalities of the BDD module are mentioned under.

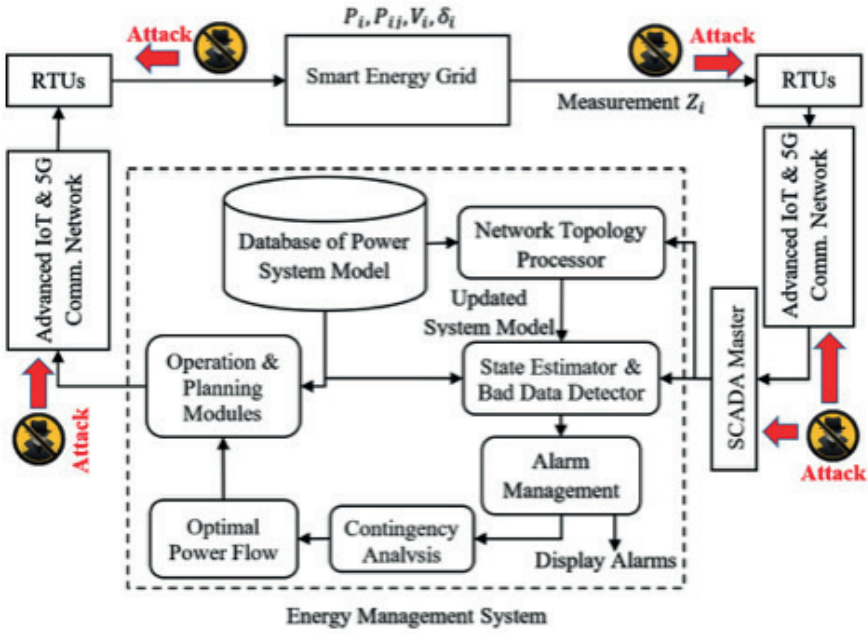


Figure 3: Cyber-vulnerable nodes in SCADA-based EMS subject to malicious data injection attacks (Source: Amin, Ruhul 2021)

3.1.1 State Estimation

The redundant measurements are processed by the kingdom estimator in order to become aware of the ideal kingdom of the contemporary running gadget. These measurements include bus voltages, currents, angles, and many more (A. Abur & Expósito, 2004). The kingdom estimator does an evaluation of the potential results and makes a decision about which manipulation moves are necessary, primarily based on facts that are correct and modern. In this chapter, a weighted least squares (WLS) static kingdom estimation version is studied to estimate voltage phasors at a given factor in time. This is because fixing nonlinear energy wave equations requires a tremendous amount of computational effort on the part of an attacker.

When trying to decide the WLS kingdom, it's often assumed that the network topology and parameters are completely recognized. In addition, it's often assumed that the device states that are most effective consist of bus-voltage phasors. Because of this, it's miles viable to explicit the contemporary state of the network as

$$\boldsymbol{\theta} = [\theta_1, \theta_2, \ldots \theta_{N-1}]^T \tag{3.1}$$

Where θ represents the kingdom vector. In addition, θi is a machine kingdom wherein i = 1, 2, 3, ..., N, and N is the full variety of states. T represents the transposition of the vector matrix for the rest of the thing. The obtained dimension vector z can be represented as:

$$z = h(\theta) + e \quad (3.2)$$

wherein h(θ) is equivalent to [h1(θ), h2(θ), ..., hm(θ)] T is a feature of the kingdom variables as well as the size errors delivered via the noise in the conversation channel, wherein e = [e1, e2,..., em] is a Gaussian vector with a recognized covariance R. During the DC nation estimation technique, it is permissible to disregard any and all branch resistances and shunt factors; however, the only way to acquire correct power glide figures is to carry out a DC load float evaluation. The equation that describes electricity going with the flow may be written as:

$$Pkm = \theta k - \theta m + v \quad (3.3)$$

$$xkm$$

where Pkm is the energy float from bus okay to bus m, θk, and θm are phase angles associated with bus k and m, xkm represents the branch reactance, and v is taken into consideration as measurement errors. Similar to how the energy injection at bus I may be defined as a sum of all the incident branches to that bus:

$$Pi = \sum j \in Nj \; Pij + w \quad (3.4)$$

$$j \in Nj$$

wherein Nj represents the gathering of buses that can be connected to bus J. Pi represents the quantity of strength that is injected onto bus I, while w stands for the measurement errors (A. Abur & Expósito, 2004). As an effect of this, the measurement vector for the DC country estimation version may be represented as

$$z = H\theta + e \quad (3.5)$$

wherein the actual power flows (inside and outside) via branches and the actual electricity injections into buses are taken into consideration, and in which the Jacobian matrix H is the most effective function of the department reactance.

3.1.2 Bad Data Detection

The information from the measurements might be distorted or misleading if the meter isn't functioning well or if the communication

networks do not have exceptional overall performance. The negative quality of the statistics will have a terrible impact on the method of estimating the kingdom's wishes, which can also cause beside-the-point choices to be made regarding management. A chi-rectangular ($\chi 2$) test is typically achieved at the dimension residue that remains after comparing particular and expected measurements. This is a non-unusual exercise. A chi-square ($\chi 2$) test is commonly completed at the dimension residue that remains after evaluating unique and anticipated measurements. This is the procedure that is used as the standard. It is assumed that the noise in the verbal exchange channel isn't always dependent on whatever else and that it follows a regular distribution with a zero mean. This is the assumption that we're handling. Therefore, the primary function of the goal J (θ) will be allocated constant with the chi-square components with $\psi = (m - n)$ varying stages of independence. A minimal level is needed for the detection $\tau = \chi 2$ chi-square distribution desk. If the objective feature is correct, then the measurement vector is suspected of holding the incorrect size. , J (θ) $\geq \tau$; A loss of defective measurements does no longer have an effect on the measurement vector in any other manner. Following that, the biggest normalized residual take a look at, also called the LNR test, is a good way to find and remove erroneous records from the scale vector.

3.2 Stealthy FDIA Construction

The conventional BDD is capable of understanding the times of random statistics injections in the length facts set, but this does not motivate the manner of United States estimation to converge. However, if attackers are successful in accumulating complete or partial tool information, they're capable of injecting malicious information in such a manner that the dominion estimation gadget converges and the malicious or compromised statistics circumvent the EMS's BDD (X. Liu et al., 2015, pp. 1686-1696). This is possible only if the attackers effectively gather whole or partial device statistics. Utilizing only size signs, it's also feasible to perform an FDIA even without previous knowledge of the gadget topology or the impedance of the transmission line. In the following subsections, we can examine the precise tactics of every variety of attacks in extra detail (J. Kim et al., 2015, pp. 1102-1114)

3.3 Attack Detection Method

In this chapter, system learning strategies are utilized to come across every random and stealthy type of FDIA. This is critical due to the reality that properly crafted assault vectors might be concealed inside the length

dataset as a way to stay far from the conventional BDD. Both the studies and industry sectors are making slow progress toward boosting their usage of machine learning strategies for the purpose of anomaly detection. The purpose of studying algorithms is to analyze existing statistical samples and assemble a mathematical version so you can make predictions or judgments based on the dataset that is furnished. Fig. 3.1 is a smooth-to-understand diagram that explains the essential jogging precept of MLAs.

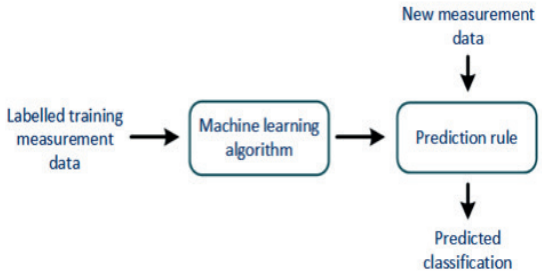


Figure 3.1: Working principle of MLAs for detecting cyberattacks (Source: Liakos, K.G., 2018)

It is essential to have a sufficient amount of historical records in order to successfully teach a gadget and gain knowledge of algorithms to be able to discover cyberattacks and malfunctions in the SCADA dimension system. Because of the many regulations placed on security, past assault statistics are rarely made available to the general public. An IEEE benchmark strength system version is used to perform randomized and covert assaults that are then used to generate attack data within the context of this study effort. In addition, the statistics for regular operational methods and fault statistics are accumulated with the help of the same benchmark version. The amassed records are then segmented into schooling and check datasets at the following level so that the effectiveness of machine learning algorithms may be evaluated in terms of their ability to distinguish between cyberattacks and malfunctions.

3.3.1 Performance Metrics for Machine Learning Algorithms

In this chapter, five well-known cutting-edge MLAs, namely Random Forests, OneR, Naive Bayes, SVM, and AdaBoost, are chosen from five separate categories to be able to determine how properly they stumble on

cyberattacks and flaws. Table 3.1 provides an outline of the MLAs along with the types that best describe them.

Table 1: Selected machine learning algorithms and their respective categories (Source: Y. Freund & R.E. Schapire, 1997)

Name	**Category**
Random Forests	Decision tree learning
OneR	Rules induction
AdaBoost	Boosting a meta algorithm for learning
Naive Bayes	Probabilistic classification
SVM	Non-probabilistic binary classification

Depending on the data that might be available, an MLA's overall performance may be measured by a whole lot of diverse overall performance signs. By utilizing the subsequent formulae, one can also calculate an MLA's detection price as well as its rate of fake wonderful consequences:

xta − xfn

Detection Rate = 100 (3.13)

xta

xfp

False Positive Rate = a hundred (3.14)

xt

in which xta = the full amount of anomalies; xfp = the number of normal facts that are considered anomalous records; xfn = the number of anomalies that are considered everyday data; and xt = the whole amount of records. The detection charge isn't always a correct reflection of the algorithm's performance because it depends on how its miles get used. For this reason, there is a great deal of different overall performance standards, such as precision, recall, and F measure. The ability of a classifier to make correct predictions may be determined by the precision parameter. Values that are typically taken into consideration to be superb and can be said as

xtp Precision = xtp + xfp (3.15)

where the variety of proper positives, xtp, equals the range of everyday facts that became incorrectly labeled as odd facts. "Don't forget is a metric that measures the true positive rate, and its value may be expressed as

xtp Recall = xtp + xfn

where xtp and xfn are of the same significance as Eq. (3.3, 3.14, and 3.15).

(3.16)

The F-degree parameter is the imply of the precision and does not forget measurements, in addition to the ex-

when you press as

F-degree = 2 × Precision × Recall

Precision + Recall (3.17)

The performance parameters of a device, together with precision, consideration, and f-measures, are ratios of extraordinary numbers, and the performance score can vary anywhere from zero to one based on how robust an MLA is.

3.4 Test System and Dataset Preparation

In this chapter, the IEEE benchmark 14-bus electricity system is considered a check device. In this device, cyber assaults and fault situations are simulated using twelve months' worth of actual-time load to go with the flow statistics from NYISO with the intention to generate the essential training and take a look at record units. These facts are used to generate essential education and take a look at information units (NYISO, 2018).

3.4.1 The Test System

The 14-bus testing machine consists of five generators, fourteen node buses, and twenty interconnecting branches. Together, those make up the device. IEDs are mounted in a number of distinctive places so that electricity injections and strength flows may be measured at a lot of unique nodes and buses. The readings from the meters are wirelessly communicated to the management center with the purpose of facilitating chance evaluation and a lot of different EMS-associated duties. In order to generate training and test statistics sets for MLAs, the manipulation center uses the meter readings it receives for the duration of various case scenarios, which include when there is verbal exchange noise when there are cyber attacks, and when there are faults. After that, the performances of various MLAs that can be taken into consideration to be trendy are evaluated for some of the exclusive case eventualities that allow you to differentiate between facts regarding faults and statistics regarding cyber-assaults within the SCADA-EMS.

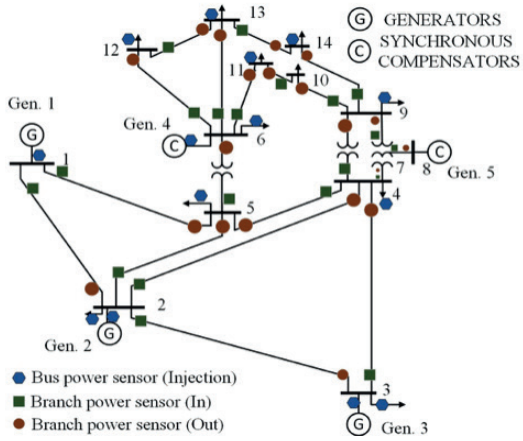


Figure 3.3: The IEEE 14-Bus system with sensors in different locations. (Source: Bawayan & H.Younis, 2021)

3.4.2 Original and With-Noise Measurements

The preliminary measurement becomes totally based on the true strength output, which can be measured in nodes or buses. In contrast, Gaussian noise with a signal-to-noise ratio (SNR) ranging from 20 to 35 DB seems to be conversational and sensor noise, and it's far removed from the initial measurement so that it will reflect realistic dimension facts. As an example of a probable state of affairs, the calculation of the dimension residue of a perfect size vector is supplied right here as eight.6e26.

3.4.3 Random and Stealthy-Attack Measurements

On the other hand, if an adversary injects faux indicators that have been randomly produced into the size dataset, the dimension residue will be better than the detection threshold fee. As a result, the BDD module could be capable of picking out the intrusion. An illustration of a randomly generated FDIA state of affairs is proven in parent three.4 (c), and in this case, the projected measurements have an enormous amount of variance in evaluation compared to the actual measurements. The size residue for this specific instance of faulty records dimension is three.21 e5, which is also quite massive in comparison to the brink value for the chi-square take a look at. However, if the adversary is cunning enough to craft covertly injected false records, you then don't have anything to fear approximately.

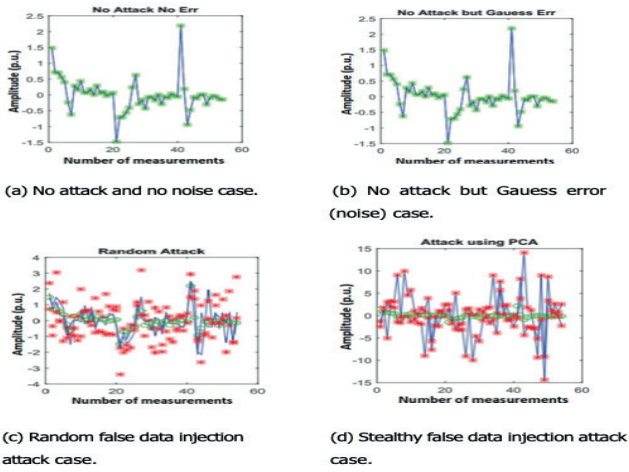


Figure 3.4: Original and estimated measurements for different scenarios (Source: (ResearchGate, n.d.)

The utilization of the device structure or the size records will cause the dimension residue to drop below the threshold value, causing it to go undetected by the BDD module. In that scenario, the expected size will now not stick to the measurements from the beginning; as an alternative, it's going to stick with the measurements that have been tampered with. An example of a hit stealth attack scenario on the system is proven in Fig. 3.4 (d), and it includes an assault that makes use of the PCA technique. For the purposes of schooling and trying out device-based total algorithms, units of records, one representing a random attack and the other representing a stealthy attack, are generated.

3.4.4 Overview of the Complete Dataset

The NYISO conducts size sample series at everyday intervals of 5 minutes apart. Because of this, a total of 290 occurrences of dimension data are recorded for every day, and a total of 212,338 sets of measurement statistics are generated all through the course of a year for every no-noise, with-noise, random attack, stealthy assault, and fault situation. Table 3.5 consists of an accounting of the full quantity of facts and factors generated for eventualities without using an attack, assault, or fault. Both original statistics and noise information are used in the no-attack statistics set. Random assaults are attack indicators that have been generated in a random style, while stealthy assaults are assault alerts that might be able to efficaciously evade detection by means of the BDD.

Table 2: Data for no-attack, cyberattack, and fault scenarios (Source: Z. H. Yu & W. L. Chin, 2015)

Situation	**No of records**
No-attach / Normal Operation	424,676
Randomly generated attacks	212,338
Stealthy Attacks (PCA, SVD and unknown H	212,338
Fault	212,338

3.5 Results and Discussion

This Section examines distinct types of cyberattacks: those that might be random and those that are stealthy. Random attacks spark off the BDD module because of the high dimension residue value they go away in the back of, but diffused attacks are capable of effectively eluding its detection. Therefore, with a view to examining the overall cyber assault detection performance of MLAs, two extraordinary case eventualities are considered: stealthy cyber attacks inside the historical information, in addition to synthesized stealthy assaults within the historic statistics. Cyberattacks that can be completed efficaciously in stealth steer clear of the BDD and are categorized as "ordinary information." On the other hand, synthesized information is categorized as attack information to educate MLA classifiers after it has been generated by the precise mathematical version (E. Frank, M. A. Hall, & I. H. Witten, 2016).

3.5.1 CASE A: Considering the success of stealthy cyber assaults within the historical statistics

In this particular investigation, attacks that have been cleverly built are regarded as hidden and are avoided via the use of the BDD module. Both the authentic facts and the statistics that have been subjected to Gaussian noise are regarded as normal operational records. Attack statistics are randomly generated and stealthy attack information that is generated via employing an acknowledged device Jacobian matrix and using algorithms that include PCA and SVD, which seem to be varieties of cyberattack facts. In addition, the measurement residue of a number of the statistics that changed into being subjected to a random assault can fall below the detection threshold, due to the information being classified as regular.

3.5.2 CASE B: Considering synthesized stealthy assaults in the ancient facts

Synthesized stealthy attacks are advanced for the motive of educating the classifiers in this situation study. These assaults are considered historical assault statistics. In the evaluation of the situation presented in Case A, stealthy statistics are not known as regular statistics; rather, they may be called assault information. 3.6 and 3.7 showcase the detection prices and the rates of fake positives for a lot of modern-day classifiers. The detection price of everyday facts is case A and case B due to the fact that MLA classifiers are trained on the same form of everyday data. On the other hand, in CASE A, assault records are regarded as stealthy. As an end result, the detection rate of every classifier is lower than 75%, but the rate of false positives is significantly greater than zero.25%. On the other hand, MLA classifiers are trained to use synthetic stealthy information for CASE B. As an end result, very excessive detection quotes are attained by classifiers, even as fake fantastic quotes are stored to a minimum. The effectiveness of MLAs depends basically on the kinds of educational information that they use and the availability of those records. This is tested by using the reality that CASE A had a lower detection price than CASE B, which had a higher detection price. On the other hand, as may be shown in Tables 1 and 2, the incorporation of applicable historic or synthesized records results in a considerable growth in detection costs and a reduction in the probability of manufacturing false positives.

4. Cyber Attacks in Smart Grids - Dynamic Impacts, Analyses, and Recommendations

Disturbances in strength structures are essentially complicated and might arise from an entire lot of sources, collectively with natural sources such as faults and man-made ones that encompass cyberattacks. Natural causes are more likely to get you up. Malicious cyber assaults are essential disruptive events that produce unsatisfactory behavior in smart grids and lead to the maloperation of PC systems and digital controllers, tripping of motors and turbines, load dropping, and cascading disintegration of the system (H. He & J. Yan, 2016). These problems may be averted by taking precautions to avoid malicious cyberattacks. In this bankruptcy, we can discuss approximately some critical worries regarding everyday safety dangers that might possibly have an effect on the right of entry to elements of digital protective relays. In an important structure that incorporates a power grid, the most trendy forms of cyber assaults are fake or spurious records injection into a laptop-aided system operating gadgets, denial of provider activities at

the device-to-device verbal exchange centers, malicious switching conduct of CBs/isolators, and different comparable behaviors.

Cyberattacks that target a smart grid encompass password theft, denial-of-service (DoS) assaults, guy-in-the-middle (MITM) attacks, replay, jamming channels, popping the human-device interface (HMI), integrity violations, privacy breaches, and a superbly extensive variety of other types of assaults. In a smart grid, the impact of cyberattacks can cause quite some intense effects, starting from the theft of strength to a massive blackout or the destruction of crucial infrastructure, along with high movers or mills. In modern years, there have been a couple of high-profile assaults on essential infrastructure in addition to commercial control structures (ICSs). These attacks were published. Different varieties of denial-of-service assaults, collectively with jamming, spoofing, and fact flooding, may be brought about through delaying time-vital messages all the way up to complete denial-of-service, which may be completed via the usage of rendering communication with a tool now not viable or by causing the device to crash or reset itself (AEMO, 2018). The disruptive switching executions and denial of service attacks that have been completed on the virtual safety gadgets of power systems were brought to light with the aid of the Aurora generator test, in addition to the coordinated cyber attacks that were finished at the electricity station in Ukraine (G. Liang et al., 2017).

Following the dialogue of the four sorts of not unusual cyber assaults that have been said in advance, the dynamic outcomes of these assaults are proven using the IEEE benchmark model of the Western System Coordinating Council (WSCC) device that was implemented in MATLAB Simulink. The following is a listing of the most vital contributions that have been made because of this dynamic evaluation of an interconnected power system at some point due to credible contingencies and cyberattacks. The physical parameters of the power device, together with current, voltage, rotor attitude, frequency, and power, are assessed for each practicable contingency, including faults, and man-made contingencies, such as cyber-attacks. These analyses are necessary to be able to prepare for both varieties of potential disruptions. The dynamic effect that was modified into completion changed into a hit in overcoming the limits of the constant-kingdom evaluation, which included non-linearities, the put-up-disturbance walking component, and the behaviors of the system. After intensive studies on the consequences of faults and cyberattacks, fresh strategies for detection and prevention have been developed.

4.1 Attack Models

According to the reports compiled through the safety system misoperation assignment stress (PSMTF) of the North American Electric Reliability Corporation (NERC), over twenty percent of safety misoperations are caused by a fault inside the relay or CB (NERC, 2013). Malicious cyber assaults because of the breach of protection flaws and vulnerabilities within the software and statistics channels were critically highlighted as one of the possible reasons for the protection misoperation. Due to inclined standards for authentication, successful cyber attacks against protective systems bring about the relays running in a bizarre way (Rahman et al., 2017). In a state of affairs like this, it's crucial to have a strong knowledge of the results that malicious operations have on the operational behavior of the electricity tool.

A records and verbal exchange (ICT)-based totally digital protection device is one of the most critical varieties of infrastructure. In this sort of machine, an attacker sends predetermined thresholds to a relay or, straight away or circuitously, tampers with a relay's commands so that it will intrude with the relay's operation and decrease its availability. The majority of attacks on a relay encompass the following steps: (i) compromising the relay trip indicators; (ii) sending spurious instructions to the relay through a compromised channel to cause a wrong operation; and (iii) manipulating the relay settings to cause volatile operation for the duration of fault events. (i) Compromising the relay adventure alerts (ii) Sending spurious instructions to the relay via a compromised channel to motivate the wrong operation Power outages can be delivered through a series of planned screw-ups in the relays. In this piece of research, a conceivable situation is used to model cyberattacks. In this situation, the adversary is able to get the right of entry to a subsystem and exchange statistics while sitting at a far-off computer.

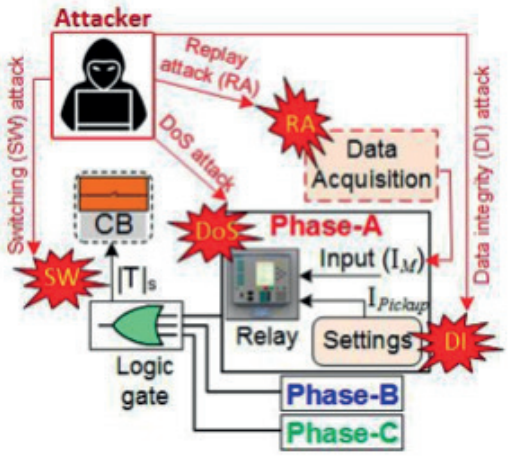


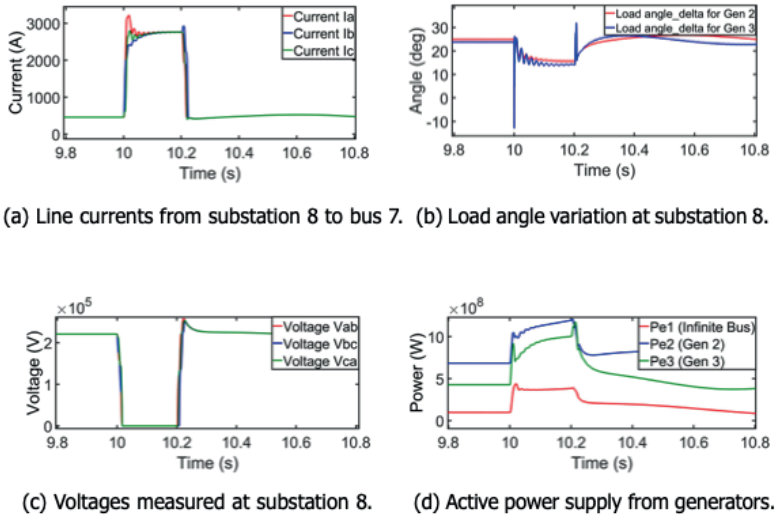
Figure 4: Attacks on digital overcurrent relay (Source: ISSN 2398-3396)

4.2 Dynamic Impact Analyses and Recommendations

As stated within the preceding paragraph, the cyber attackers take control of the relays that are positioned in essential channels in substations that are prone to attack. Because of a hassle with the substation relays, the strength device in query reports unanticipated dynamic behavior, which may result in a chain reaction of failures and power outages throughout the affected region. In order to comply with the nearly unlimited amount of system records available to the attacker, it's been assumed for the purpose of the dynamic conduct evaluation that the attacker has the functionality to compromise the operation of a single substation. The subsequent subsections will deal with the results that the 3-phase-to-floor fault as well as the numerous kinds of cyberattacks have on the dynamic performance of the system.

4.2.1 Impact Analyses of Credible Contingency

By monitoring the modifications in voltage and current, protective relays are capable of detecting oddities inside the device and communicating these records to circuit breakers (CBs), permitting them to rectify the hassle. In this observation, a three-phase-to-floor fault is added at bus eight at the ten-second mark, and it is rectified at the 10.2-second mark. When an inappropriate stage of currents and voltages is detected at substation 8, the relay R 8-7 journeys the circuit breaker (CB) BR eight-7 by sending a journey order to it. In Figure 4, you can see a presentation of the dynamic parameters that have been measured earlier than, during, and after the fault.



(a) Line currents from substation 8 to bus 7. (b) Load angle variation at substation 8.

(c) Voltages measured at substation 8. (d) Active power supply from generators.

Figure 4.1: Dynamic parameters measured at substation 8 subject to 3-phase fault at bus 8 (Source: Amin, B.M.R, 2021)

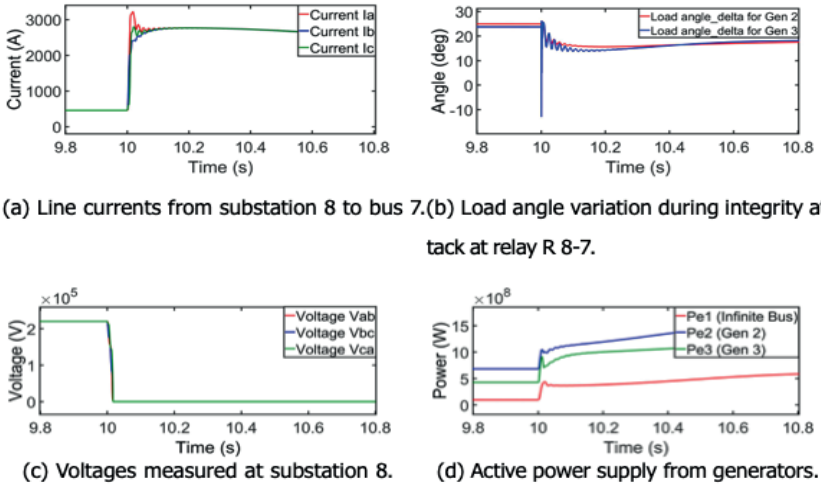
4.2.2 Impact Analyses of Random Switching Attacks

Through diverse communication channels, machine operators are able to control the community of a strength gadget from a faraway location. It is viable for an adversary to gain the right of entry to the laptop that controls the relays of a substation or to enter the conversation channels that allow you to insert direct ON/OFF instructions to a defensive device such as a CB. The switching frequency of the CBs is determined after considering the processing time delay of the relay and the relay response time. This selection is made in accordance with the amount of the cutting-edge and the chosen curve (Rahman et al., 2017). In order to maintain accurate synchronization of the system, the protecting machine of an average synchronous generator will postpone the reclosing operation by 15 cycles. By compromising the communication channels, the attacker has the potential to modify this system and release an assault that entails random switching (M. Zeller, 2011).

4.2.3 Impact Analyses of Integrity Attacks

In order to discover fault situations inside the system and successfully ship an experience instruction to the CB, you will need to make certain that the relay threshold is nicely set. An assault on the device's integrity may be the result of tampering with the threshold placement. Because the brink is too excessive, the relay may not come across an overcurrent fault caused by

an overload or a quick circuit, and the circuit breaker might not ride while a peculiar situation occurs that ought to cause it to.



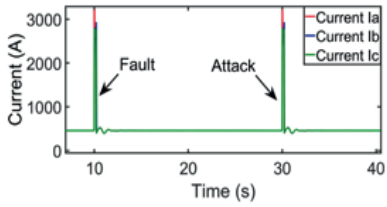
(a) Line currents from substation 8 to bus 7.(b) Load angle variation during integrity attack at relay R 8-7.

(c) Voltages measured at substation 8. (d) Active power supply from generators.

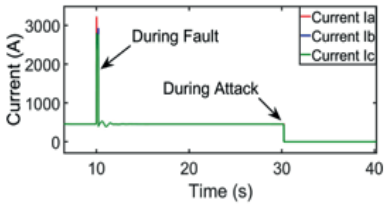
Figure 4.2: Dynamic parameters measured at substation 8 subject to the integrity attack at substation protection relay R 8-7 ((Source: Chen T. Pan, Y. Xiong., 2020)

4.2.4 Impact Analyses of DoS Attacks

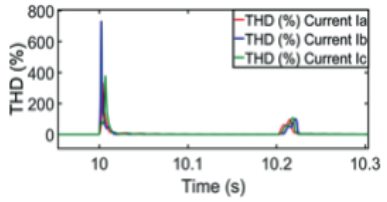
A denial of carrier assault will start with the aid of delaying or preventing the switching command from being dispatched from a relay to the CB. It is viable that the execution method of a relay's command inside a protection algorithm could be halted, delayed, or refused while a DoS assault is in progress. If a denial of carrier attack is a hit, the outcomes might be catastrophic for the gadget's overall performance and the dynamic behaviors it exhibits.



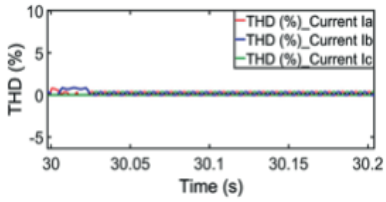
(a) Attacker current signal to the relay R 8-7



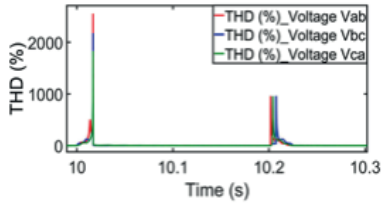
(b) Actual line currents from bus 8 to bus 7.



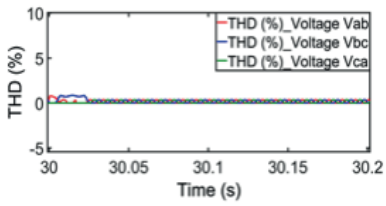
(c) THD of the line current during fault at bus 8.



(d) THD of the line current during replay attack to the relay R 8-7.



(e) THD off the bus voltage during fault at bus 8.



(f) THD of the bus voltage during replay attack at the relay R 8-7.

Figure 4.3: Dynamic parameters measured at substation 8 subject to the replay attack at protection relay R 8-7 (Source: Chen T. Pan, Y. Xiong., 2020).

Alternatives based on THD are strongly endorsed. The general harmonic distortion (THD) of the modern road modern-day could be very different from the THD of the contemporary road, which is present at some point of an assault, as may be visible in Figures 4.2 and 4.3. This can also serve as a useful indicator to differentiate between vulnerabilities and assaults. It's viable that the relay gets a new actual-time observer as additional work that is truly linked to this subject matter is executed in the future. As a result, the relay could have the ability to research the state of affairs and determine the true harmonic distortion (THD) of the road modern and/or voltage in actual time. As a result of this, if an erroneous fault command is obtained

from the adversary at the same time that the line current and/or voltage are displaying a regular THD condition, the assault can be quickly recognized, the most suitable actions can be taken, the reports can be transmitted to the manipulation center, and therefore capability damages or blackouts can be prevented.

5. Cyber Resilient Decentralized Non-linear Controller for Smart Power Systems

The developing tiers of power demand that are available in conjunction with business automation at several levels of the electricity grid's actual-time operation make the management and operation of a complicated cyber-bodily electricity community by means of the usage of turbines in reality critical. This is because the elements are intertwined. If they are no longer stopped, cyberattacks can generate a large amount of instability inside the tool, which may in the long run result in a failure that cascades at some stage in the entire device and brings about vital financial harm to a financial system.

The intricacy and immoderate computing weight of this manner make it impossible for it to decide the right authentication channel, that's one of the biggest drawbacks of the gadget. In addition, the quantity of time spent encrypting and decrypting facts is a different essential problem for the real-time operation of energy systems (M. Velciu & V. Patriciu, 2014). Because modern-day cyber-physical power systems are tightly coupled among cyber and bodily techniques, a solution that is primarily based on physical residences and can simultaneously hit upon and mitigate the effects of cyber attacks might be the first-rate alternative for dealing with this hassle (Amin, Ruhul 2020).

5.1 Cyber-assault Detection and Mitigation Technique

The purpose of this observational work is to offer a method for the identification of cyber attacks that is predicated on the residual mismatch that exists amongst received and anticipated measurements. In addition to this, an optimization method based totally on GA is established as a terrific way to reduce the bad effect that cyberattacks have on the overall performance of the tool. The strategies for detection and prevention are broken down into their elemental components as follows.

5.1.1 Detection Technique

In order to discover any disturbances or cyberattacks that can be detected inside the generator by manipulating measurement alerts, a detection index,

referred to as DI, has been set up. The detection index is the difference between the expected observer state fee and the reference price that turns out to be obtained from the PMU. This difference can be explained by predetermined threshold stages of the detection index being utilized so that noise and attacks may be differentiated from each other. The length residual fee might be higher than the allowable errors price If there is noise present inside the study, what is referred to as noise signs and symptoms are disturbance signs and symptoms that have been created randomly. A very advanced level so that you can differentiate many of the assault diplomas from the noise diplomas. Lower-degree attacks al, which can be mitigated through the manage parameter optimization machine, and excessive-degree/ extreme attacks au, which necessitate termination of the producing unit if you want to defend the network from excessive instability, are all taken into consideration in this study. Lower-degree attacks can be mitigated via the manage parameter optimization method. If the detection index DI is higher than the most noisy stage, then it is effectively expected that there may be some form of cyberattack. Only if the detection index is immoderate enough will the cyber intrusion in the sensor be greater than or identical to the most noise threshold, DIa ≥ then. Now, signs and symptoms could be dispatched to the controller in an effort to provoke the approach of mitigation on the occasion that the DI > than attack is found.

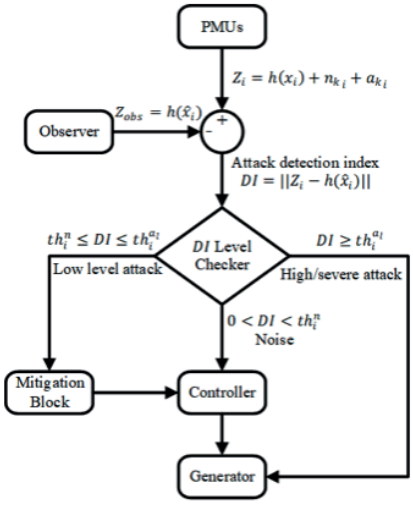


Figure 5: Cyber attack detection and mitigation flowchart (Source: Sadi, Zheng, & Ali, 2017)

5.1.2 Mitigation Technique

Following the invention of cyberattacks, appropriate preventative measures ought to be taken to reduce the impact of bad outcomes on the dynamics of the energy machine. First, if a lower-level assault signal is introduced to the PMU dimension after which an attack is done, the PMU might be compromised than ≤ DI ≤ than, when an assault is detected, the attack detector will ship a sign to the operator, after which it will transfer to the best controller operation. This will remain until the operator approves the trade and returns to the standard mode of operation. During the decrease-level attack, a set of rules based on a genetic set of rules (GA) is used to develop optimal control settings. The GA is chosen due to the fact that it is dependable in finding solutions in a good-sized search space and is capable of avoiding becoming mired in a state of affairs wherein its miles are caught in a local minimal. The following is an explanation of the goal characteristic in order to be applied in the procedure uf1(t) − uf1(0uf2(t) − uf2(0

+ 0δ2(t) − δ2(zero)phase explains what the everyday meanings of the symbols and notations are for each one.

Algorithm: 6.4 Detection and mitigation towards cyber-assaults

1: Initialize

2: PMU dimension acquired, zi = h(xi) + nki + aki

3: The predicted states xˆi is received

4: zi − h(xˆi)

5: if 0 < DI < thn, Noise exist

6: Continue nonlinear controller operation.

7: else, if thn ≤ DI ≤ thal , Low-degree attack indicators exist.

8: Initiate optimized controller operation.

9: else if DI ≥ thal , severe cyber assault detected

10: Send termination commands to CBs

11: If the put up-assault gadget is risky Re-optimize the healthy machine

12: stop

Additionally, if the attack detection index DI ≥ than , is to thal, the controller will pressure the circuit breaker (CB) to ride, with the intention of closing down the generating unit. Figure 6.3 and Algorithm 6.4 both offer

a visual illustration of the whole system's float for detection and mitigation, respectively.

5.2 Results and Discussion

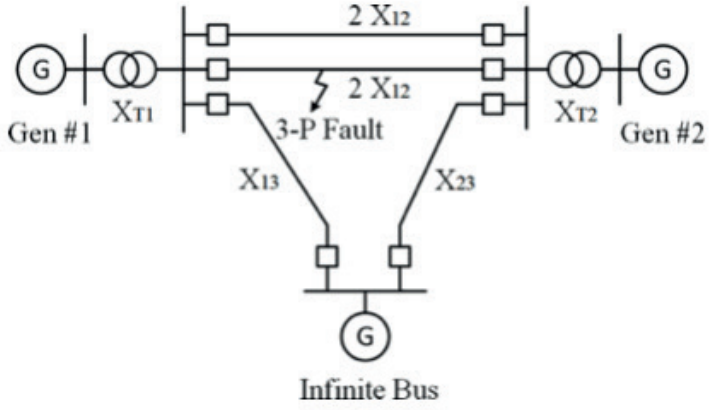


Figure 5.1: The two-machine infinite bus power system model. (Source: Mohammed, Roknuzzaman, Biswas, & Tanjimuddin, 2015)

As an illustration of a multimachine electricity gadget, this research takes into consideration a version of an energy machine with machines and countless buses. As may be seen in Figure 5.1, the energy system being mentioned consists of two synchronous turbines that might be connected together and an endless bus that is linked to each of the mills' terminals. The specification information of the endless bus and turbines are furnished in Table 5. The dynamic behaviors of the machine, both with and without fault eventualities, are analyzed while it is subjected to noise and cyber assaults. The fault conditions for the exams are those defined in Section 5.1.Three; especially, a symmetric three-section fault to the floor will occur at time t0 = zero.1 sec, and it will likely be cleared at time t1 = zero.22 sec. At this factor, it'll be assumed that the device has been fully restored at t2 = 0.3 seconds.

Table 3: Power system model parameters (Source: Amin, 2021).

	Generator # 1	**Generator # 2**
x_d (p.u.) x' (p.u.)	1.863 0.257	2.36 0.319
x_T (p.u)	0.129	0.11
$x_q d$ (p.u)	1.712	1.712
$T'0$ (p.u)	6.9	7.96
H (s)	4	5.1
D (p.u)	5	3
T_m (s)	0.35	0.35
T_e (s)	0.1	0.1
R (s)	0.05	0.05
K_m (s)	1.0	1.0
K_e (s)	1.0	1.0
K_c (s)	1	1

$x12$	(p.u.)	0.55
$x13$	(p.u.)	0.53
$x23$	(p.u.)	0.60
ω_0	(rad/s)	314.159

The decentralized controllers are developed via using all of the important device information-

$$vf1 = a1(\delta 1 - \delta 10) + b1\omega 1 - c1(Pe1 - Pm10),$$

$$vf2 = a2(\delta 2 - \delta 20) + b2\omega 2 - c2(Pe2 - Pm20) \quad (6.30)$$

in which a1 = 19.68, b1 = 20.60, c1 = 93.81, a2 = 19.69, b2 = 21.45 and c2 = 73.95 [87].

The reference signals δ10 and δ20 are derived from the measurements taken by using the PMU, and they may be liable to cyberattacks.

Now, the unique excitation controllers for the generators that were part of the previously stated multi-system power machine have evolved into -

$$uf\,1 = 1\,kc1Iq1\,\{vf\,1 + Pm10 - (xd1 - x'\,d1)Iq1Id1 + T'\,d01Qe1\omega 1\},$$

$$uf\,2 = 1kc2Iq2\,\{vf\,2 + Pm20 - (xd2 - x'd2)Iq2Id2 + T'd02Qe2\omega 2\}$$

When figuring out the excitation manipulation, the subsequent boundary conditions are taken into consideration: $-3 \leq Efi = kciufi \geq 6, i = 1, 2.$

It is assumed that both of the mills are vulnerable to some kind of cyberattack, and the performances of the controllers are analyzed for each of the no-fault and fault-susceptible eventualities.

5.2.1 CASE I: Noise and Low-level Attack Scenarios

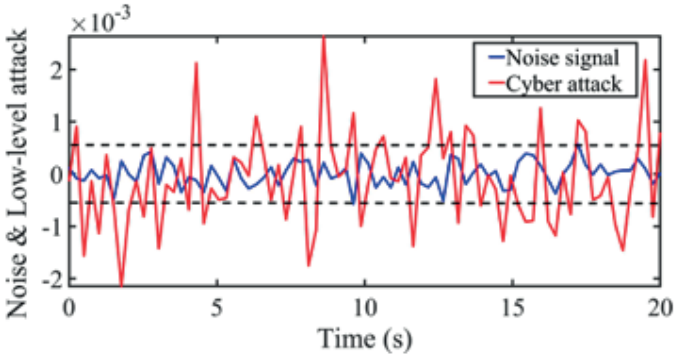


Figure 5.3: Noise and attack signals over time (Source: Amin, 2021)

In this precise case study, an examination of the repercussions of a low-level cyber attack on the dynamic behaviors of plants 1 and 2 is carried out, with attention given to both the absence and presence of faults within the structures. On the PMU measurement signal, it's far more presumable that there is a signal such as random additive white Gaussian noise (AWGN) (δref) fUse both plants as an example of a herbal incidence. At this point, a hacker compromises the PMU measurement with the aid of inserting arbitrary indicators, (δref) for each flower in the form of an attack on their integrity. A low-degree attack is one in which the signal of the assault is only marginally greater than the sign of the noise. Whenever there may be an alternate within the normal load or a fluctuation within the mechanical input electricity, the simulation method takes into consideration a disturbance of thirty percent. In Figure 5.4, we have an illustration of a noise pattern together with an instance of a cyberattack sign over the years.

Without Fault

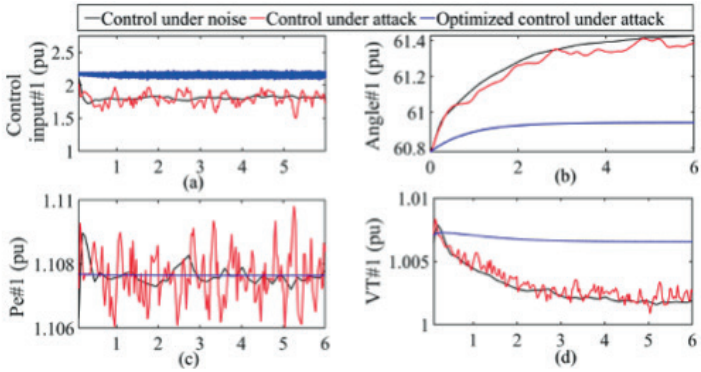


Figure 5.4: Dynamic behaviors of plant-1 for noise and low-level attack scenarios without fault (Source: Amin, 2021)

It may be observed in Fig. 5.4(a) that each noise and cyberattack have an effect on the AVR excitation control sign of plant-1. As a result, oscillatory control indicators are subsequently produced, which are then dispatched into the right management system. Now, looking at Fig. 5.4, we will see that the rotor perspective of plant-1 exhibits a piece of oscillation while subjected to noisy signals. Furthermore, the oscillations turn out to be more stated while cyberattack indicators are introduced to noise indicators. In addition, the energy dispatch as well as the device terminal voltage of plant-1 have both emerged as oscillatory as a result of noise and cyber assaults, and they diverge from the strong operational price of consistent country situations, as indicated inside the graph.

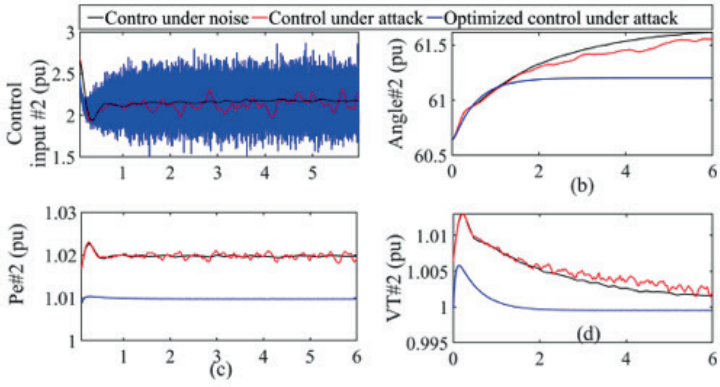


Figure 5.5: Dynamic behaviors of plant-2 for noise and low-level attack scenarios without fault (Source: Amin B.M.R, 2021)

Figs. 5.4 and 5.5. The cyber intrusion detection method is used to perceive both the noise and the attack that are present inside the manipulated signals. As can be seen in Figure 5.3, the detection threshold is able to pick out the border between the noise and the cyberattacks. As an end result, the newly designed GA-based controller is able to correctly reduce the oscillation on the rotor angle at some point of noise and decrease-importance cyber attacks on PMU records. This can be seen in Fig. 5.4. In spite of the noise and cyber attacks on PMU-based management measures, it is apparent from Figs. 5.4 and 5.5 that plant-1 maintains a consistent terminal voltage and electricity dispatch. In this bankruptcy, we check out the possibility that the control measurements at plant-1 and plant-2 have each been hacked one after the other with the aid of cyber intruders. The presence of AWGN noise on the manipulable dimension alerts plant-2 to having minor oscillations in its control enter, rotor attitude, electricity dispatch, and terminal voltage, as may be visible in Figure 5.5. These oscillations are caused by the presence of AWGN noise on manipulated size indicators. Because the quantity of cyber attack indicators is extensively greater than that of noise indicators, the outcomes of cyber attacks at the dynamic overall performance of plant-2 are likewise appreciably greater than the ones of noise alerts.

The recommended controller is applied on the way to discover both the noise and the attacks, and the GA-primarily based optimization approach is put into practice in an effort to dampen the oscillations. It has been found that the suggested controller is able to boom dynamic performances consisting of plant-2's rotor perspective, electricity dispatch, and terminal voltage even in the presence of noise and decrease-significance cyber attacks on manipulating measurements. **With Fault**

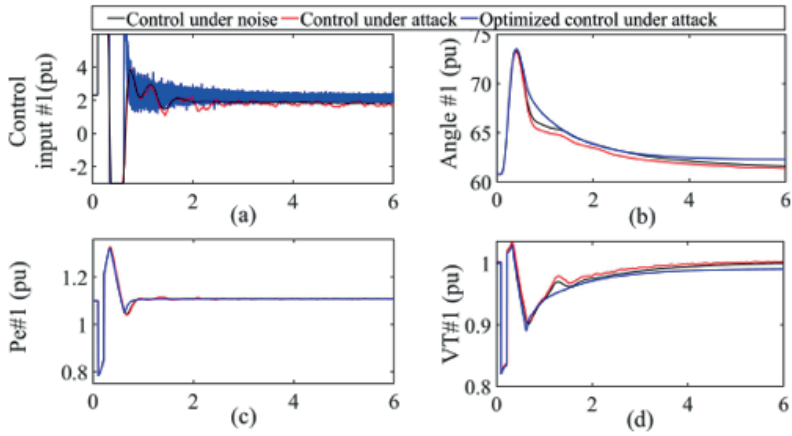


Figure 5.6: Dynamic behaviors of plant-1 for noise and low-level attack scenarios with fault (Source: Amin, B.M.R, 2021)

A fault from three degrees to the floor is imposed at 0.1 second durations at one of the transmission lines that join plant 1 and plant 2 in this hypothetical situation. Noise and cyberattacks have an effect on each plant's AVR excitation manage signals, which leads to oscillating manage signals being provided to the relevant control gadget. This can be decided in Figs. 5.6 and 5.7, respectively. Because the primary AVR control sign is being affected by noise and attack, the rotor angle of every machine is also growing oscillations in all throughput up-fault situations in advance of achieving a regular-nation situation. This is the case because the hassle will subsequently ease up. Although the superior management movement lowers the oscillation and settles the rotor perspective inside a shorter time body, it could be seen in Fig. 5.6 that the effect of assault on the rotor attitude oscillation is a chunk greater than that of noise. Figure 5.7(b) depicts an effect that is very analogous to this one while being achieved by the rotor mindset of the plant-2 generator. Noise and cyberattacks have an impact on strength dispatches from each vegetation; but, extra oscillations are observed in plant-2 as shown in Fig. 5.7, and in plant-1 as confirmed in Fig. 5.6, which suggests that plant-2 is extra prone to the elements. On the other hand, as seen in Figures 5.6 and 5.7, the gadget terminal voltages at every flora are growing because of the cyber assault that became finished at the device while it emerged in the put-up-fault situation. However, the correct and most fulfilling control motion brings both flowers' strength dispatch and gadget terminal voltage to a consistent-country rate once a malfunction takes place in the machine.

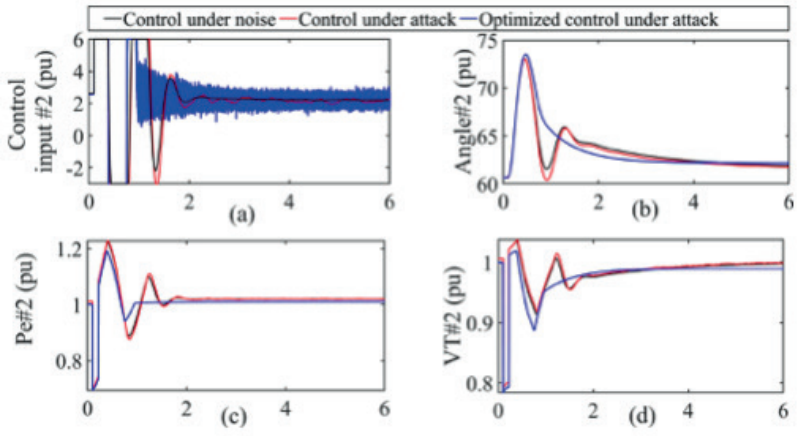


Figure 5.7: Dynamic behaviors of plant-2 for noise and low-level attack scenarios with fault (Source: Amin B.M.R, 2021)

5.2.2 CASE II: Noise and High-level Attack Scenario

A high-degree attack is defined as one that entails the injection of a random signal into the size signals at an extra amplitude. An adversary would possibly insert a high-degree assault at some point in the instant that the fault became active, which would have serious repercussions for the dynamic behaviors that happened at some stage in transients.

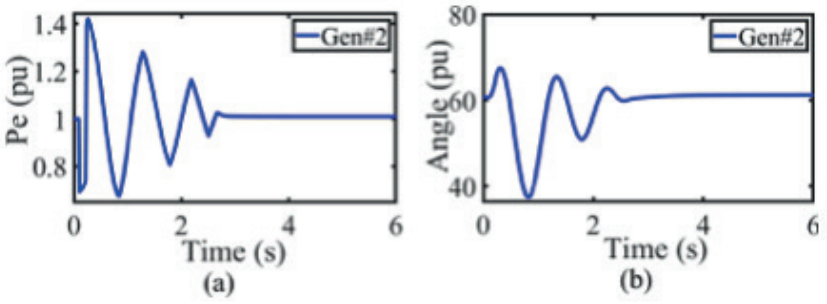


Figure 5.8: Dynamic behaviors of plant no. 2 while plant no. 1 is under high-level cyber attack (Source: Amin, B.M.R, 2021)

When high or intense assaults are taking place, the managed inputs will sooner or later attain their boundary values, and the dynamic responses will go through oscillations for longer than the important time. As a result of this, termination orders will be transmitted to the severely compromised producing unit as soon as the detection of high-level or excessive-degree assaults has taken place. In this painting, it is assumed that the attacker gains the capacity to inject an excessive-level assault into plant 1. As a response to this, the controller kills the compromised unit 0.12 seconds after the assault is detected. Figure 5.8 illustrates the rotor attitude and power dispatch of plant-2 when compared to plant-1, which is experiencing a severe cyber assault at the same time. After the malicious device was removed from the strength device, the gadget has not been affected in any way.

6. Conclusions and Recommendations for Future Works

At this time, the antique energy device is transitioning properly into a greater interactive, green, and related clever strength system that uses a complicated cyber community of digital metering, automation, sophisticated management, and verbal exchange structures that may be primarily based on records and conversation technology. Attacks at the physical layer would possibly have repercussions at the cyber layer, and vice versa. This is the case

notwithstanding the reality that several ICT-based total safety mechanisms are being developed at the moment to strengthen the cyber network.

Protection and detection strategies, which can be primarily based totally on the physical houses of energy systems, make it possible to run the device in a more regular and dependable manner. The manipulation of meter measurements, the deft creation of covert length information, and the advent of misguided or faulty indicators into the virtual safety machine are all procedures by which operators might be misled and their control measures compromised. In addition, the adversary has the functionality of fooling the operators of the energy machine by simulating natural disruptions in conjunction with failures. During the course of this observation, the behaviors of power structures at some point in everyday operations, in addition to cyber assaults, are investigated. Additionally, suitable detection algorithms are hooked up if you need to understand and differentiate between cyberattacks and troubles.

The proposed decentralized controller is put through its paces in an electricity system with machines and an unlimited bus, all through consistent state and contingency checking out, all while the controller reference size signals are exposed to conversation noise and cyberattacks.

The following inferences and interpretations are tenable in light of the findings of this research:

- In an energy machine state estimator, it is viable to get around the bad facts detector by craftily building false size facts using both partial or complete gadget data or measured sensor statistics. These false measurements will then be stored hidden inside the measurement database.
- The most superior gadget gaining knowledge of algorithms is capable of efficiently locating cyber assaults with a significant detection price. However, those algorithms have a lower detection charge when it comes to differentiating between cyber assaults and mistakes. In addition, which will gain a greater detection charge, a huge amount of records on previously launched cyberattacks is necessary.
- An technique this is based on perception propagation has the potential to effectively discover FDIAs of both the random and stealthy types. These FDIAs are constructed and deployed with the goal of fooling the bad records detector that is part of the strength machine country estimator.

- The BP-based totally algorithm demonstrates its robustness and effectiveness via achieving a higher detection rate and higher performances in parameters which includes ROC curve, precision, remember, and F-measures than the present-day machine learning algorithms inclusive of Naive Bayes, Support-Vector Machines (SVM), RandomForest, OneR, and AdaBoost. This suggests that the BP-based totally set of rules is greater powerful and more robust than those other systems gaining knowledge of algorithms.
- It isn't always important to have any beyond assault facts as a good way to observe the BP-primarily based method; as an alternative, it uses prolonged history actual-time load drift facts.
- During cyberattacks and malfunctions, dynamic gadget parameters like generator rotor angle, frequency, dispatch, voltage, and current display unique capabilities. This can open opens up a tremendous horizon for the development of novel cyberattack detection and mitigation strategies.
- The approach that is based totally on dynamic evaluation describes the pre- and put-up-contingency situations for faults and different key cyber assaults on protection devices. Some examples of those kinds of assaults are random switching assaults, integrity attacks, DoS attacks, and replay attacks.
- The variance that exists between the calculated perspective-country and the acquired PMU measurement for the controller reference sign can be used so one can perceive sensor and conversation noise, as well as various levels of cyber assaults directed at the controller.
- The cyber-resilient decentralized controller that we have provided uses an optimization approach this is based totally on GA, and it can successfully provide a manage sign that will lessen the bad consequences that cyber attacks have on the gadget.
- In the occasion that the controller reference size signal of the infected unit is being subjected to an intense cyber assault, the proposed controller is capable of trouble a termination coaching and sending it to the malicious unit.
- The sturdy decentralized controller that changed into created improves the system's stability in steady-country in addition to contingency instances, whilst being at risk of communique noise and chronic disturbances which include fluctuations in mechanical enter and frequent load shifts.

6.1 Recommendation for Future Works

Because the grid of the future can be extra dispersed, interdependent, and notably interactive from the technology layer all the way down to the distribution layer, the entities that make up the energy system could be more susceptible to cyber assaults. Because of this, extra research and improvement will want to be carried out so that it can cope with a range of new challenges regarding the cyber defense of smart security systems. The following is a listing of some of the capabilities and subsequent steps for studies related to this dissertation:

- The use of electrical gadget bodily traits in a nonlinear system offers an opportunity for an added investigation into the differentiation between cyberattacks and screw-ups.
- The BP algorithm that become suggested has the ability to be accelerated such that it could become aware of cyberattacks in an interconnected HVDC grid.
- It is feasible to expand and put in force within the relays a real-time observer-based totally detector for the motive of staring at the non-fault repute of the line modern-day, voltage, and/or frequency. This will allow the relay to distinguish between assaults and faults at some point of random switching attacks.
- The dynamic effect reviews of replay assaults reveal that the THD of the line present day is notably awesome from the THD of the cutting-edge all through an attack. This is validated by means of the fact that the THD of the road modern-day is extensively lower. It is possible to plot a reliable detection method that uses present-day and/or voltage harmonics as a way to identify replay attacks within the shielding devices used for power structures.
- Under the conditions of a severe cyber assault, the overall performance of the strong decentralized non-linear controller that has been supplied has been evaluated for an unmarried unit. When designing the controller, it's far viable to don't forget several gadgets that are underneath heavy attack.
- A supply call for imbalance can be brought on in the smart grid when an adversary efficaciously compromises the strong electronic control machine that is integrated inside the newly growing disbursed renewable energy resources. It is necessary to conduct studies into the strength gadget dynamics that take vicinity throughout fluctuations in renewable power sources within the event of a cyber attack, in

addition to studies into the improvement of detection and mitigation techniques.

- The examined work that changed into performed demonstrates that the methods that have been set up have a splendid amount of resilience against the various forms of cyber-assaults. However, there is a more need for engagement with the industry on the demand for resources and the software of methodologies. Since the mounted techniques are established with the aid of utilizing simulated facts on a whole lot of benchmark structures, extra research on sensible structures and the usage of real energy gadget statistics is necessary so one can tweak the numerous control parameters before the methodologies may be used in real power networks.

References

A. Abur and A. G. Exp´osito, Power System State Estimation: Theory and Imple-mentation. Boca Raton, FL, USA:CRC, 2004.

A. Anwar and A. N. Mahmood, "Stealthy and Blind False Injection Attacks on SCADA EMS in the Presence of Gross Errors," IEEE Power and Energy Society General Meeting, vol. 2016-Novem, pp. 8–12, 2016.

Amin, B.M.R.; Hossain, M.J.; Anwar, A.; Zaman, S. Cyber Attacks and Faults Discrimination in Intelligent Electronic Device-Based Energy Management Systems. Electronics 2021, 10, 650. https://doi.org/10.3390/electronics10060650

A. S. Musleh, G. Chen, and Z. Y. Dong, "A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids," IEEE Transactions on Smart Grid, vol. 11, no. 3, pp. 2218–2234, 2020.

A. Sargolzaei, K. Yazdani, A. Abbaspour, C. D. Crane, and W. E. Dixon, "Detection and Mitigation of False Data Injection Attacks in Networked Control Systems," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4281–4292, 2020.

Amin, Ruhul (2021). Cyber attack detection and mitigation in smart power systems. Macquarie University. Available on. https://doi.org/10.25949/21375957.v1

AEMO, "Australian Energy Sector Cyber Security Framework Education Workshop," no. October, 2018.

B. R. Amin, S. Taghizadeh, M. S. Rahman, M. J. Hossain, V. Varadharajan, andZ. Chen, "Cyber Attacks in Smart Grid – Dynamic Impacts, Analyses and Recommendations," IET Cyber-Physical Systems: Theory & Applications, vol. 5, pp.321–329, 2020.

Bawayan, H.; Younis, M. Microgrid Protection through Adaptive Overcurrent Relay Coordination. Electricity 2021, 2, 524–553. https://doi.org/10.3390/electricity2040031

Chen, T.; Pan, Y.; Xiong, Z. A Hybrid System Model-Based Open-Circuit Fault Diagnosis Method of Three-Phase Voltage-Source Inverters for PMSM Drive Systems. Electronics 2020, 9, 1251. https://doi.org/10.3390

D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid," in 2010

First IEEE International Conference on Smart Grid Communications, 2010, pp. 244–249.

D. Thanos, I. Voloh, and E. A. Udren, "P C Engineering Concepts Applied to Cyber Security of the Power Grid," in 2012 65th Annual Conference for Protective Relay Engineers, 2012, pp. 335–357.

Electricity Retains Power as Greatest Invention. [Online]. Available: http: // www.gallup.com/poll/17881/electricity-retains-power-greatestinvention. aspx.

E. Frank, M. A. Hall, and I. H. Witten, The WEKA Workbench. Online Appendix for "Data Mining: Practical Machine Learning Tools and Techniques". Morgan Kaufmann, Fourth Edition, 2016.

G. Dan and H. Sandberg, "Stealth Attacks and Protection Schemes for State Estimators in Power Systems," First IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 214–219, 2010.

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. on Power Systems, vol. 32, no. 4, pp. 3317–3318, July 2017.

G. Erbach and J. O'shea, "Cybersecurity of Critical Energy Infrastructure," October 2019

H. He and J. Yan, "Cyber-physical Attacks and Defences in the Smart Grid: A Survey," IET Cyber-Physical Systems: Theory Applications, vol. 1, no. 1, pp. 13– 27, 2016.

I.Xyngi, "An Intelligent Algorithm for Smart Grid Protection Applications," Ph.D. dissertation, Delft University of Technology, 2011.

ISSN 2398-3396, Received on 17th December 2019, Revised 11th April 2020, Accepted on 28th July 2020, E-First on 2nd October 2020, doi: 10.1049/iet-cps.2019.0103, available at www.ietdl.org

ICS Vulnerabilities Key Findings. [Online]. Available: https://www.dragos. com/ review/2019-ics-year-in-review-ics-vulnerabilities/

J. Kim, L. Tong, and R. J. Thomas, "Subspace Methods for Data Attack on State Estimation: A Data Driven Approach," IEEE Transactions on Signal Processing, vol. 63, no. 5, pp. 1102–1114, 2015.

J. Hu, H. R. Pota, and S. Guo, "Taxonomy of Attacks for Agent-Based Smart Grids," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, pp. 1886–1895, 2014.

K. Xi and J. Hu, Bio-Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 129–157.

L. M. Zawra, H. A. Mansour, and N. W. Messiha, "Migration of Legacy Industrial Automation Systems in the Context of Industry 4.0- A Comparative Study," in 2019 International Conference on Fourth Industrial Revolution (ICFIR), 2019, pp. 1–7.

Liakos, K.G.; Busato, P.; Moshou, D.; Pearson, S.; Bochtis, D. Machine Learning in Agriculture: A Review. Sensors 2018, 18, 2674. https://doi. org/10.3390/s18082674.

Mohammed Mynuddin, K. M. Roknuzzaman, Prodip Biswas, Mohammad Tanjimuddin. Stability Study of Power System. International Journal of Energy and Power Engineering. Vol. 4, No. 2, 2015, pp. 43-50. doi: 10.11648/j.ijepe.20150402.15.

M. Zeller, "Myth or Reality — Does the Aurora Vulnerability Pose a Risk to My Generator?" in 2011 64th Annual Conference for Protective Relay Engineers, April 2011, pp. 130–136.

M. H. Rehmani, M. Erol Kantarci, A. Rachedi, M. Radenkovic, and M. Reisslein, "IEEE Access Special Section Editorial Smart Grids: a Hub of Interdisciplinary Research," IEEE Access, vol. 3, pp. 3114–3118, 2015.

M. S. Rahman, M. A. Mahmud, A. M. T. Oo, and H. R. Pota, "Multi-Agent Approach for Enhancing Security of Protection Schemes in Cyber-Physical Energy Systems," IEEE Transactions on Industrial Informatics, vol. 13, no. 2, pp. 436–447, 2017.

M. Velciu and V. Patriciu, "Methods of Reducing Bio-cryptographic Algorithms Computational Complexity," in 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), 2014, pp. 153–158.

NERC, "Misoperations Report," Protection System Misoperations Task Force-NERC Planning Committee, Tech. Rep., 2013.

New York Independent System Operator (NYISO) Real-time Actual Load Data-2018. [Online]. Available: http://mis.nyiso.com/public/P-58Blist.html.

P. C. of Advisers on Science and Technology. (2007, August) Leadership under Challenge: Information Technology R & D in a Competitive World. An Assessment of The Federal Networking and Information Technology R & D Program. [Online]. Available: http://www.nsf.gov/geo/geo-data-policies/pcast-nit-final.pdf.

P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," IEEE Security Privacy, vol. 7, no. 3, pp. 75–77, 2009.

R. Bobba, K. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting False Data Injection Attacks on DC State Estimation," First Workshop on Secure Control Systems, vol. 6, no. 5, pp. 1–9, 2010.

R. McMillan, "Siemens: Stuxnet Worm Hit Industrial Systems," COMPUTER-World, 2010.

Smart Grid Security Enhancement by Using Belief Propagation - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Cyber-vulnerable-nodes-in-the-SCADA-based-EMS-subject-to-malicious-data-injection-attacks_fig1_342536207.

Smart Grids European Technology Platform. [Online]. Available: www. smartgrids. Eu.T. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," Computer, vol. 44, no. 4, pp.91–93, April 2011.

The Industrial Control Systems Cyber Emergency Response Team: Incident-reported by sector (FY 2016) and Onsite assessments by sector (FY 2014-2016).[Online]. Available: https://ics-cert.us-cert.gov/Year-Review-2016.What is a Smart Grid? [Online]. Available: www.smartgridsmartcity.com.au.X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of Local False Data Injection Attackswith Reduced Requirement on Network Information," IEEE Transactions on SmartGrid, vol. 6, no. 4, pp. 1686–1696, 2015.

Y. Lu, "Industry 4.0: A Survey on Technologies, Applications and Open ResearchIssues," Journal of Industrial Information Integration, vol. 6, pp. 1–10, 2017.

Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli,"Cyber–Physical Security of a Smart Grid Infrastructure," Proceedings of the IEEE,vol. 100, no. 1, pp. 195–209, 2012.

Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids," ACM Trans. on Information and System Security, vol. 14, no. 1, pp. 1–33, 2011.

Y. Freund and R. E. Schapire, "A Decision-Theoretic Generalization of On-Line Learning and an Application to Boosting," Journal of Computer and System Sci- ences, vol. 55, no. 1, pp. 119 – 139, 1997.

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 Communications Surveys Tutorials, vol. 15, no. 1, pp. 21–38, 2013.

Z. H. Yu and W. L. Chin, "Blind False Data Injection Attack Using PCA Approx- imation Method in Smart Grid," IEEE Transactions on Smart Grid, vol. 6, no. 3, pp. 1219–1226, May 2015.