IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

Pillars of Power System and Security of Smart Grid

Ujas Bhadani

Cybersecurity Expert, Northeastern University, Boston MA

ABSTRACT: When a complex physical network system and a cyber network are combined to form a smart grid, numerous technical challenges arise. The electric power grid's basic structure hasn't evolved in the last century. It has been demonstrated that the needs of the twenty-first century cannot be met by a hierarchical, centralized organization. While the information and communication infrastructure that supports present electricity systems is strong, the new smart grid requires a separate, much more complicated infrastructure due to its much larger size. Smart grids are electric networks that use cutting-edge monitoring, controlling, and communication technology to deliver a safe and stable energy supply, improve the efficiency of operation for generators and distributors, and offer consumers various options. A multipurpose electric power grid system, the smart grid offers improved efficiency, dependability, and other advantages. This power system will be improved in order to increase efficiency and safety, lessen its impact on the environment, and give customers more control over the network. In this survey report, we will gain a better understanding and a comprehensive overview of the concept of the smart grid.

KEYWORDS: Smart Grid, Reliability, Interconnected Power System, Security, Distributed Generation

I. INTRODUCTION

The invention of electricity, which revolutionized our culture and economy, was the biggest discovery of the 19th century. Considering electricity is capable of traveling over great distances more easily than any other form of energy carrier, it has become important to our economic and social functioning. Electric grids, which are essentially huge, interconnected physical networks, serve as the foundation of today's energy supply and consumption systems [1].

The term" smart grids" (SGs) has been used frequently and has been given various definitions. The integration of enabling ICT and other cutting-edge technologies with large-scale power networks is extremely important to the SG definitions because it makes it possible for electric energy generation, transmission, distribution, and usage to be more effective, efficient, affordable, and environmentally sustainable. Seven crucial domains are defined under the U.S. NIST conceptual model, which includes bulk generation, transmission, distribution, customers, service providers, operations, and markets [2]. Different nations have their own interpretations of what the SGs mean. In China, SGs refers to a more physical-network- based strategy to ensure energy supply is safe, reliable, responsive, and cost-effective while also being environmentally sustainable [3].

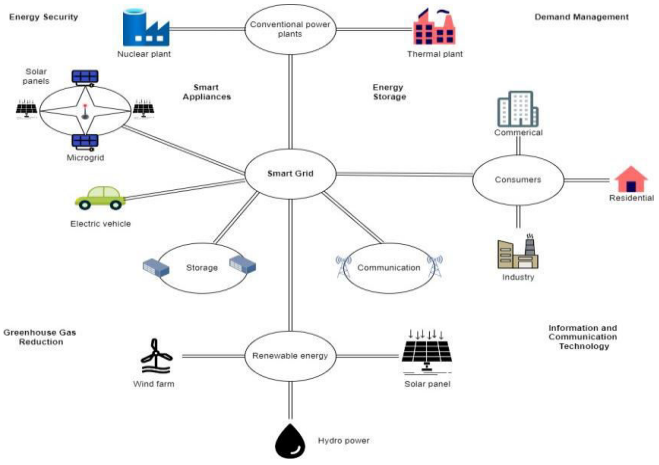

Fig. 1. Smart Grid Network

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

The smart grid is shown as a complex and highly linked system that encompasses a wide range of stakeholders and players, in accordance with the organizational structure shown in Figure 1 [1]. This broad framework includes organizations that range from conventional utilities to cutting-edge technology suppliers, regulators, and end users, all of whom are vital to the operation and development of the smart grid.

According to IEEE Grid Vision 2050 [4], the decentralization of operations and control throughout the whole power system is a key component of the smart grid idea. In order to enable effective bidirectional power flows, this strategy integrates a variety of power generation sources, including both established technology and cutting-edge alternatives like distributed generation and renewable energy. The smart grid intends to improve resilience, optimize energy usage, and more effectively handle varying demand and supply patterns by distributing operational capabilities throughout the grid.

Future energy supply and consumption via smart grids will require more mobility, security, safety, and flexibility. These goals need a fundamental rethinking of the way power networks are organized and controlled, how cyber systems support grid operations, and how consumers engage with energy systems.

Paper is organized as follows. Section II describes automatic text detection using morphological operations, connected component analysis and set of selection or rejection criteria. The flow diagram represents the step of the algorithm. After detection of text, how text region is filled using an Inpainting technique that is given in Section III. Section IV presents experimental results showing results of images tested. Finally, Section V presents conclusion.

The technical difficulties that must be addressed include the intermittent nature of renewable energy generation, massive networks of small, distributed generation systems, and the uncertainty imposed by the implementation of an energy market mechanism. The stark contrast between the peak and average electricity demand is one of the fundamental characteristics of power usage. Increasing the capacity of the energy supply with greater capacity to satisfy rising energy needs without constructing additional power generation facilities would derive from reducing peak usage. Another concern is how to employ ICT and other cutting-edge technology, like smart meters and telecommunications technologies, for sensing, transmitting, and processing data about grid conditions, to improve energy consumption efficiency. Several significant technological improvements are needed to address the problems, such as

•To create a more effective grid, peak demand should be decreased through techniques like load shedding, intelligent load mnagement, and dynamic pricing.
•If grid components like sources, loads, and storage units can be controlled locally or can make some decisions on their own, control methods need to be decentralized in order to reduce communication requirements.
•Energy production from RE sources like solar cells and wind turbines should also be accurately estimated.
•Demand at the distribution level should be rather accurately predicted, with demand in any area of the grid estimated a few hours or days in advance.
•Innovative energy storage technology is also required to reduce energy demand peaks.

Smart grid integrates the advantages of digital communications with the conventional electrical grid to deliver real-time information and enable a nearly instant supply and demand management balance. Mobile sensor networks and wireless networks are two examples of smart grid technologies that have already been employed in various industrial applications and are being developed for use in contemporary smart linked systems [5]. The elements of this communications system are complex units, estimation, and perception-enhanced user interfaces and support for decision-making, standards and classes, and integrated contact.

An integral element of a smart grid is the ability to connect to a network of organizations and communicate with them (e.g., intelligent appliances, specialized applications, systems, a control centre, etc.). As a result, creating a reliable and all-encompassing connectivity network is crucial to the creation of the Smart Grid Communication Networks Service. A crucial goal in support of this assertion is creating a reliable communications network to provide strong relevant information distribution across WAN's (wide area networks) to the distribution feeder and client level. This has been a key area of study for a while. The key differences between the traditional electric system and the smart grid are displayed in Table 1 [6].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

Traditional electric system	Smart grid
Electromechanical	Digital
One-way communication	Two-way communication
Centralized generation	Distributed generation
Few sensors	Sensors throughout
Failures and blackouts	Adaptive and is landing
Limited control	Pervasive control
Manual restoration	Self-healing

Table I: Comparison between the old electric grid and smart grid

The Smart Grid implementation in the traditional electric power grid infrastructure will [7]:
•Guarantee grid stability at a degree that was never imagined
•Pressuring power costs to decline
•Allow for innovations and efficiencies that are yet to be imagined
•Keep the cost of electricity affordable for customers and offer more information and give options to consumers
•Take into consideration both conventional and renewable energy sources and increase the penetration of sources of inconsistent power generation
•Integrating electric vehicles as generation and storage devices will revolutionize both the utilities and transportation sectors
•Finally, the smart grid will support a more equitable distribution of renewable energy sources, enable access to more environmentally friendly central station generation, and enable users to purchase cleaner, lower-carbon-emitting electricity. Additionally, the smart grid will enable more effective consumer pricing responsiveness, which will lessen the demand for additional fossil fuel-fired generation capacity and cut CO2 and other pollutant emissions

II. SMART GRID

A. Characteristics of Smart Grid
Smart Grid uses cutting-edge products and services, as well as intelligent control, communication, monitoring, and self-healing technology [7]. The following characteristics of the Smart Grid are suggested in this section.

- Smart Grid gives customers more information and supply options while allowing them to contribute to system operation optimization. Through the integration of smart meters, smart consumer loads, micro generation, and electricity storage (hybrid cars), it enables demand response and demand-side management. Additionally, it informs customers about energy use and costs. Customers should receive information and incentives to change their usage habits in order to get around some of the limitations of the power system.
- It better supports intermittent generation and storage choices, and significantly enables the connection and operation of generators of different sizes and technologies. All renewable energy sources, distributed generation, household micro-generation, and storage alternatives are supported and made possible by it, which considerably lessens the overall environmental effect of the electrical supply system. It will facilitate connecting in a manner comparable to 'plug-and-play.'
- By intelligently operating the delivery system (rerouting power, operating independently, and pursuing efficient asset management), it optimizes and operates assets efficiently. This includes using resources in accordance with what is required and when it is required.
- It offers increased levels of energy supply reliability and security while operating resiliently in the face of natural disasters, physical threats, and cyberattacks. Predicting problems and taking self-healing action when they arise, it ensures and enhances reliability and the security of supply. It also increases supply security through improved transfer capabilities.
- In order to accommodate sensitive technology that is improved by the digital economy, it provides power quality of the electrical supply.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

- Through expanded transmission routes, consolidated sup- ply and demand response programs, and additional service offerings, it expands market access.

B. Functions of smart grid

Functions performed by the smart grid are as follows,

•Using information technology, exchange data on power producers, users, and grids over the Internet.

•Integrate a number of new, more compact power- producing facilities.

•To counteract changes in electricity production brought on by the usage of renewable energy sources.

•The utility can adjust the system to stop fault currents from reaching harmful levels by using sensors, communications, information processing, and actuators that enable a higher level of network coordination.

•Analysing electrical and environmental factors in real- time to determine an element's capacity to transport load (such as a line, transformer, etc.).

•Utilizing phase angle regulating transformers (PARs), series capacitors, very low impedance superconductors, and flexible AC transmission systems (FACTS).

•Settings for protective relays that can be changed in real-time in response to signals from nearby sensors or a centralized control system, such as current, voltage, feeders, and equipment.

•An independently operated section of the transmission and distribution (TD) system is automatically disconnected and then connected again as per need.

•Integrating the functioning of reactive power resources with sensors, controllers, and communication systems, such as capacitor banks, voltage regulators, transformer load-tap changers, and distributed generation (DG).

•Equipment performance and operational environment are tracked and analyzed online in order to spot abnormalities. With coordinated measurement across many devices, fault location and type can be distinguished with greater precision.

•By providing clients with real-time price signals, time- of-use (TOU) rates, and service alternatives, advanced metering infrastructure (AMI) systems, and embedded appliance controllers may assess customer usage in real-time and manage load.

•Reconfiguring and optimizing feeders in real-time to reduce the strain on machinery, increase asset utilization, boost system performance, and improve distribution system efficiency.

•Customers are given information so they can choose wisely how much electricity they use.

C. Classification of smart grid

In this survey report, we divided the smart grid into three major systems: smart infrastructure, smart management, and smart protection systems [6].

•Smart infrastructure system: The energy, information, and communication infrastructure that supports the SG is known as the smart infrastructure system. Both information and power can move in both directions. Note that the idea of a "two-way flow of information" is simple to comprehend. "Tw–way flow of electricity" suggests that the delivery of electric energy is no longer one-way.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

Smart infrastructure system	Smart management system	Smart protection system
Smart energy subsystem • Power generation • Transmission grid • Distribution grid • Microgrid	**Management objectives** • Energy efficiency and demand profile • Utility, cost and price • Emission	**System reliability and failure protection** • System reliability • Failure protection mechanism
Smart information subsystem • Information metering and measurement • Information management	**Management methods and tools** • Optimization • Machine learning • Game theory • Auction	**Security and Privacy** • Information metering and measurement • Information transmission
Smart communication subsystem • Wireless • Wired • End-to-end communication management		

Fig. 2. The Detailed Classification of the Smart Infrastructure System, the Smart Management System, and the Smart Protection System

Subsystems for the purposes of this survey: the smart energy subsystem, the smart information subsystem, and the smart communication subsystem. The advanced generation, transmission, and consumption of electricity are controlled by the smart energy subsystem. Advanced information metering, monitoring, and administration within the smart grid are part of the smart information subsystem. Among systems, devices, and applications in the smart grid framework, the smart communication subsystem is in charge of communication connectivity and information transmission.

Smart management system: The SG subsystem that offers sophisticated management and control services and functionalities is known as the smart management system. The proliferation of functionality based on SG's smart infrastructure is the primary factor that can transform the grid. The grid will continue to become smarter as new management tools and services are created that can make use of the advancements in technology and capability made possible by this cutting- edge infrastructure. To achieve numerous advanced management goals, the smart management system makes use of smart infrastructure. So far, the majority of these goals have to do with increasing energy efficiency, balancing supply and demand, reducing operation costs, and maximizing utility.

Smart protection system: The SG component known as the "smart protection system" offers services for advanced grid reliability analysis, failure protection, and security and privacy protection. The SG must use the smart infrastructure to create a better management system as well as a smarter protection system that can support failure protection mechanisms more consistently and efficiently, solve cyber security concerns, and safeguard privacy.

III. PROBLEM STATEMENT AND CHALLENGES

A. Adaptive CUSUM Algorithm

The Smart Grid has an enormous physical infrastructure and vast cybersecurity requirements due to which maintaining and getting constant output out of it is a challenging task. Transmission lines, generation, and distribution are the significant conventional parts of the smart grid. Moreover, it can be integrated with sensors, intelligent devices, renewable energy resources, distribution automation, electric vehicles, etc. Due to technological advancement, the transfers of files, data, records, etc are done through the cloud which is a very effective and fast way to communicate from one grid to another. However, there were a significant rather noticeable amount of cyber-attack incidents noticed in the past on the smart grid causing blackouts, inaccurate state estimation which results in incorrect billing decisions, etc. The challenges posed by unpredictable attacks include affecting the smart grid's stability and the statistical

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

behavior change of the state estimation process. In this paper, we will be discussing a few of the proposed algorithms to handle different kinds of issues or attacks related to the Smart grid.

There are various parts of the smart grid that controls the different functions of the system. The Energy Management System (EMS) is the control center of the smart grid which performs all the important tasks of the grid. Primar- ily task includes, maintaining the record of the system states by collecting the required data from the remote meter periodically. The attacker can inject malicious data into the system causing the system to produce a false output and causing disruption in the grid. To secure the smart grid against the injection of malicious data, an adaptive CUSUM algorithm is proposed. This algorithm detects the false data injection data in real time which protect the grid from any major blackout. The proposed algorithm is recursive, and every recursion involves two steps.

- Unknown Variable solver based on Rao Test.
- Multithread CUSUM test.

The statistic of the Rao test detection can be modified and written as [1]:

$$I(R_n) = \frac{\partial Ln}{\partial a_n}\Big|_{a_{n=0}} \left[J^{-1}(a_n)|_{a_n=0}\right] \frac{\partial Ln}{\partial a_n}\Big|_{a_{n=0}}$$

The Multithreaded CUSUM-based statistic after recursion can be written as:

$Sn = \max\{0, Sn-1 + I(Rn)\}$

The above equation is independent of the unknown variable. The monitoring of the CUSUM statistic is done by the control centre in real-time against false data injection. If the CUSUM statistic (Sn) exceeds the set threshold, then the system raised the alarms alerting the necessary individuals.

Adaptive CUSUM Algorithm
n ← (1, 2, 3 • • •)
Rn ← compute the difference between ˆZ and Z.repeat
Update of: n ← n + 1 continues the observation
Unknown solver based on Rao test:
eliminate an by taking derivative of Ln withrespect an evaluated at 0
Multithread CUSUM test:
compute recursively Sn for all m measurements at current n as shown in (19)
until Th = infn 1—Sn ¿ h is determined Terminate the adaptive CUSUM process Report the determined hypothesis and ARL

B.Markov-Chain-Based Analytical Model
In order to examine the quantitative performance of the system and receive guidance on the required system configuration, the Markov-chain-based analytical model is proposed. There are three fundamental metrics: FAR expectation, missing- detection rate expectation, and detection delay expectation.
•The FAR Expectation is defined as the probability of the system reaching Uf from the proposed CUSUM statistic Sn when there is no attacker. As per [16] the TPM P will have a special eigenvector with =1 and the rest are 0. The FAR Expectation can be determined by:
•The Expectation of Missing Detection ratio is defined as the probability that the detection delay is greater than or equal to the detection delay constraint.
•The Expected Detection Delay is calculated by taking the weighted average of the expected number of transitions from the initial stage to the state, which is based on P.

The observation variation index is shown in Fig 3. On the X-axis, while CUSUM Statistic Sn is shown on the Y-axis. Plotting two distinct cases, Case 1 and Case 2, with FAR values of 1 and 0.1 percent, respectively, corresponds to h1 and h2.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

C. Performance

The performances of the proposed scheme are presented for both analytical and numerical simulations.

Simulation Results with Simulated Data:

The Fig 4. Displays the performance analysis of the proposed algorithm by comparing it with CUSUM GLRT by varying the FAR for accuracy and expected E(Td) of detection delay. We can also see that better accuracy is obtained as FAR decreases. If we drop the FAR to its significantly lowest point then the proposed algorithm reached an accuracy of above 95 percent.

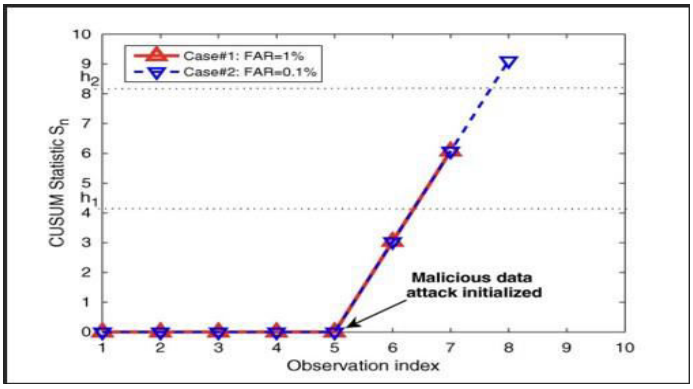

Fig. 3. Simulation of the adaptive CUSUM algorithm

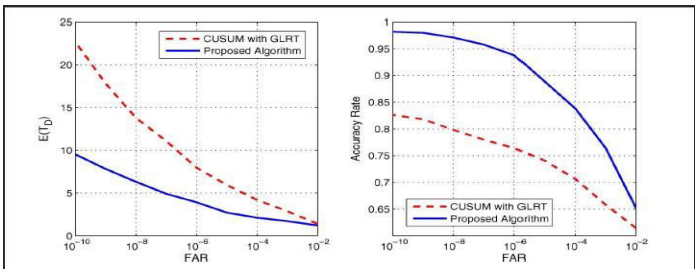

Fig. 4. Performance analysis of the adaptive CUSUM algorithm in comparison with CUSUM GLRT

Simulations Results with MATPOWER 4.0:

The Fig 5. Displays the graph is plotted with CUSUM Statistic S(n) on the y-axis and the Observation index on the x-axis. The observation index is taken for the IEEE bus-4, bus-57, and bus-118 test systems.

D. Subset Selection Algorithm

Another algorithm [17] that is used to provide protection against specific attacking strategies is Subset Selection Algorithm.

It begins by simulating an attack under security subset S, which is initially empty. The main aim of this algorithm is to keep track of the array of counters known as Measurer, which counts the number of times the attacker manipulates each measurement. After determining the most modified measurement, it moves that entity to security subset S, forcing the attacker to investigate alternative solutions due to a lack of measurements. To get the most out of this algorithm,

	Alarmed	Threshold detection	Detection Delay
Bus-4	24 observations	34.51	9
Bus-57	37 observations	133.52	22
Bus-118	45 observations	283.14	30

Fig. 5. The Below mentioned are observations from Fig 6.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

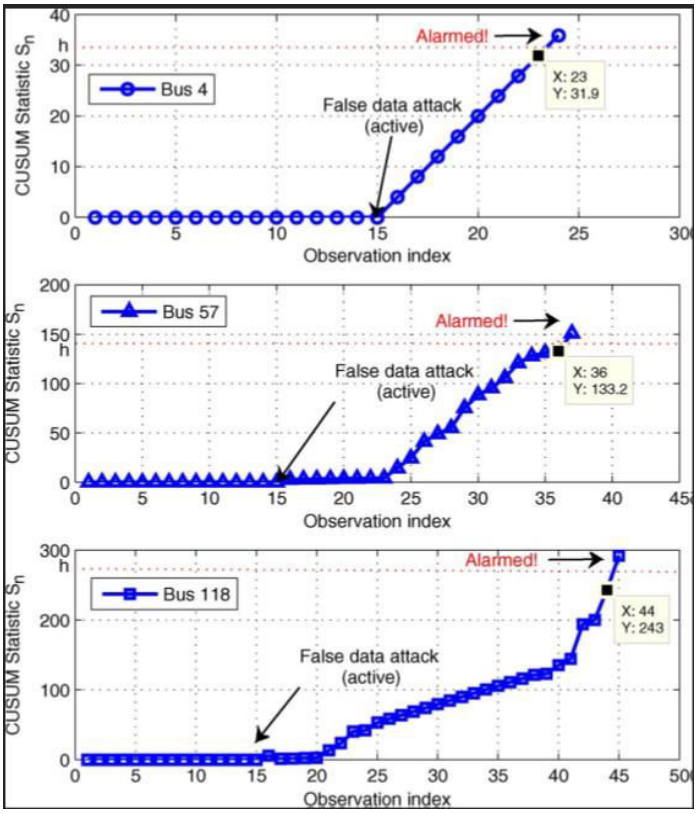

Fig. 6. Detection simulation of the adaptive CUSUM algorithm with MAT- POWER 4.0 power flow measurements for the IEEE 4-bus test system, IEEE 57-bus test system, and IEEE 118-bus test system

It can be modified as considered necessary. In respect to complexity, it is equivalent to N * Ns linear program, solving linear programs in an exhaustive search.

Subset Selection Algorithm
$S = \phi$;
Repeat
MeasyreArr($\{1,\ldots,M\}$) = 0;
For I = 1 to N do, Find s_i and N_{Ai};
If $N_{Ai} < N_A$ then, MeasureArr (s_i) <= MeasyreArr(s_i) + 1
End if, End for
K* = argmax MeasureArr(k);
Add k* to S:
Until N_Ai≥ N_A,∀i

IV. DENIAL OF SERVICE ATTACK

The general form of DDOS attack is when the attackers or group of attackers attempt to make a computing service or a network service unavailable for the legitimate user. It can be seen in the image that on the leftmost part of the image the attacker is present and will launch the malicious traffic through the handlers and the compromised devices to the targeted device and make it inaccessible.

NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report This report said that 87 percent of total attacks on any server are DOS attacks and in the 14th report, this number reached 95 percent [8].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

A. Methods of attacking different layers of a system

•Physical layer: At this layer, the attack is totally dependent on altering the physical properties of the communication channel. It can be done by two different methods: Jamming: It relies upon the modification of signals which are transmitted during the communication between the sender and receiver. Altering: It depends upon the physical tempering of devices.

•Data link layer: It depends on finding the bugs and exploiting media access protocols in the target network

•IP layer: It depends on spoofing the IP protocol fields, such as falsifying routing information.

•Transport layer: Dos attacks find the vulnerabilities to exploit the computing or the network resources.

•Application layer: DoS attacks send fake malicious traffic on the target resources and servers to make them unavailable for legitimate users.

V. SMART GRID DDOS ATTACKS

Structure flaws causing DDOS attack: The hierarchical structure having multiple layers includes the data collection devices present at the bottom layer like smart ap- plications, smart meters, data aggregators, PMUs, IEDs, RTUs, etc. as seen in the figure below. To sense the environment, generate data, and transmit it towards the middle layer or intermediate levels which take data from all aggregators and marks as DCs. Furthermore, the data is transferred to the above layer which acts as the data centre of the system and is marked as PO (power operators).

This whole set of levels for sensing and managing the data act as small units like internet infrastructure affected with the same vulnerabilities that may be exploited to deploy the DDOS attack on the system. The smart grid also faces similar types of attack vectors, vulnerabilities, and threats. Also, the security part for the smart grid was thought after the whole process which leads to a lot of flaws in the cybersecurity of the SG.

An example of DDOS attack: The attacker may somehow spoof the victim's address and sent it to a different number of destinations which may present at the same or different place of the world as a source address and these destinations may flood the victim with malicious fake traffic and make it out of service for the legitimate users. The main controller of the system named as Distribution Management system oversees the monitoring, protection, control, and optimization of distribution assets and DdoS attacks may disrupt it to produce disturbance in the whole system and its normal working [9].

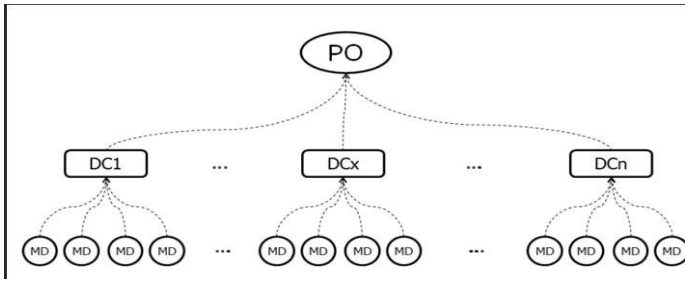

Fig. 7. A simple representation of data collection subsystems in the SG, where MD represents a measurement device, DC a data concentrator, and POa centralized power operator.

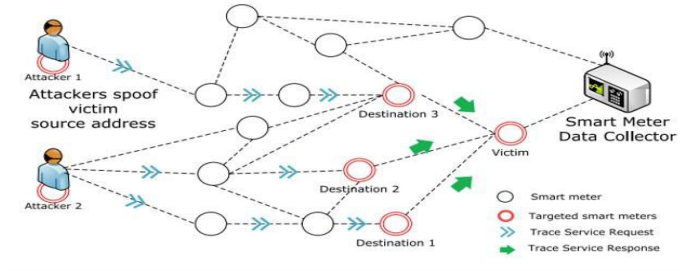

Fig. 8. An attack scenario on the AMI

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

- Taxonomy of the DDOS attack techniques: There are seven main categories that the DoS attack may use to launch the DoS attack on the system.
- Jamming: Jamming refers to the delay or denial of a signal on the physical layer to stop or disturb the information or electricity service.
- Resource Exhaustion: In resource exhaustion, some specific device or network is targeted.

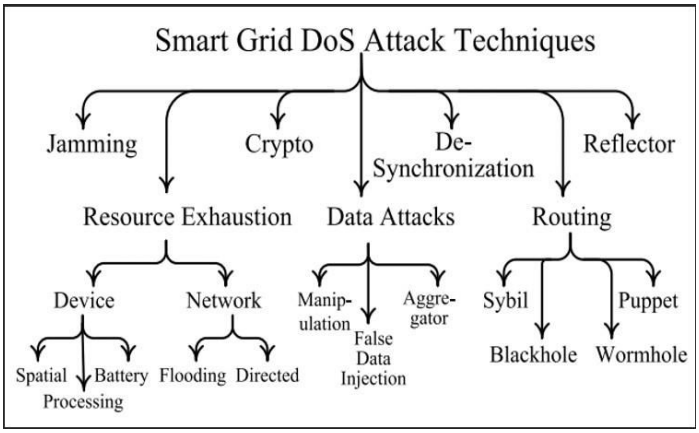

Fig. 9. A taxonomy of the DoS attack techniques in the smart grid

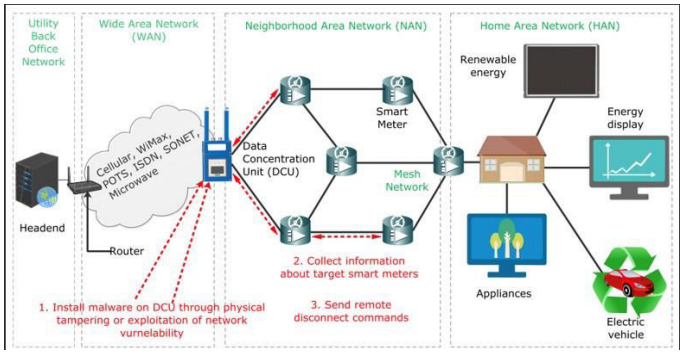

Fig. 10. A compromised data collection unit might be used to knock off SGdevices, such as smart meters, to deny power to consumers

•Crypto: The scenario is explained when the data manipu- lation is used as the pivot of the DoS attack during which the message authentication code which prevents the cor- rupted data may be exploited to launch the attack.[10]
•Data Attack: The data is manipulated and injected into the single meter which leads it to infect several other networks causing the entrance for several other attacks in Neighborhood Area Network including Dos attacks as seen in the figure below.[11]
•De-synchronization attacks: De-synchronization attacks can be utilized as another form of DoS. Devices using GPS synchronization may be vulnerable to well-known GPS spoofing attacks. In authors present a poisoning attack on the Smart Grid's load forecasting system, while authors provide a summary of load forecasting attack types
•Routing based attack: The Smart Grid allows bidirec- tional data transfer and routing, this mechanism attracts a lot of attacks including DoS attacks. The routing- based attacks also act as a base for other attacks Sybil, wormhole, blackhole, and puppet attacks
•Reflector attacks: It involves the attacker may spoof some of the servers to send requests again and again to the target node.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

VI. COUNTERMEASURES

As attackers have a number of methods to attack different layers of the system and they tried to disrupt the service or completely shut down it. We do not have any single concrete solution to defend against all these different types, but we must carefully bring together all the solutions to stop the attacks.

•Non-technical Controls: "Security is a process, not a product" and it is relevant for the solutions to SG DoS solutions. Some of the physical security protocols must be followed to ensure the availability of service. Only authorized people must be allowed to enter the space of important or sensitive areas to prevent malicious infection to the system by direct injection like a USB- attached master control system to insert some malicious code.

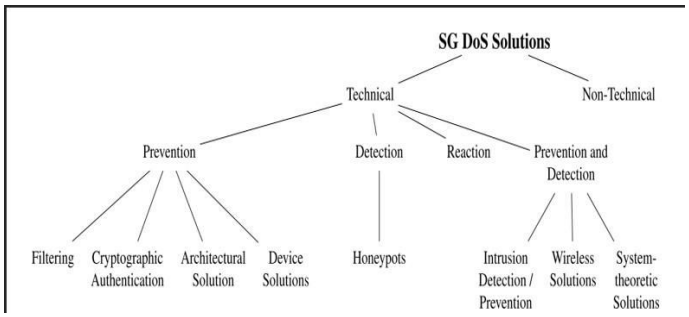

Fig. 11. Solution approaches to the SG DoS attacks

- Filtering: The main motive of filtering is to drop the packets or requests which seem to be not legitimate out of the normal pattern. Packet filtering technique is used at the perimeters like firewalls having some strict policies to detect and drop malicious packets. Filtering is applied at a place like a gateway in which the SG is connected to the internet through it and all policies and rules must be followed and only trusted hosts are allowed to enter and access the internal system and subsystems in SB. The design presented by Wang and Yi for the firewall to secure the SG communication with the multi-hop wireless network. The idea is that the node may inform his neighbouring nodes about the intruder so they either blacklist or grey list the intruder [12].
- Intrusion Detection system: The firewall or filtering refers to the blocking or permitting of packets or data based on its policies. On the other hand, the system or software which analyses the packets or data allowed to enter, its header, and the payload that is searched for ant malicious code or injection is called an intrusion detection system.
- Rate limiting: An intermediate phase in the attack response process is the identification of the attack source. If this is carried out successfully, the subsequent step may be to stop the DoS flow. In Ipv4 networks, however, there are two fundamental obstacles to accurate source identification.[13] First off, source addresses are readily falsified since they lack cryptographic security. Second, because routers only know the next hop when forwarding a packet, it is challenging to track the packet's true source.

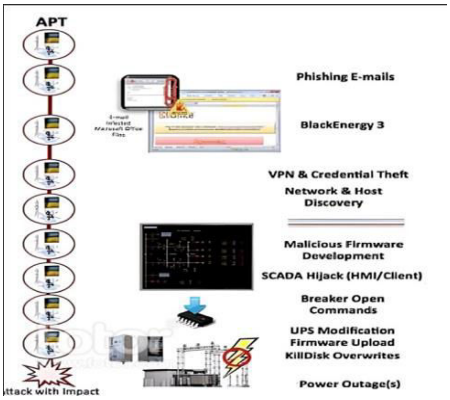

Fig. 12. Industrial Control System Kill Chain Mapping Chart

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

•Cryptographic Authentication: We take the example of a perfect world in which two communication parties that are sharing data must be encrypted then most of the DoS-like attacks can be protected. The possibility that a DoS attack may be directed at the usage of encryption itself is an important consideration in this case. In other words, if verifying a packet's validity requires a lot of resources, an attacker may be able to conduct a s successful attack using fake packets [13].

•Honeypot solutions: The use of honeypots as a component of SG systems is advised. Honeypots are purpose-built gadgets that replicate the target of malicious assaults. They are utilized to identify, deflect, and evaluate assaults. Buza identified a honeypot that, from an attacker's perspective, looks like a Siemens PLC (programmable logic controller).

VII. USECASE

•Ukrainian Smart grid attack Breakdown: A team from the USA was sent to the Ukrainian power plant to work openly on the attacks which were launched by the attackers in 2015. This team was composed of the e National Cybersecurity and Communications Integration Center (NCCIC)/Industrial Control Systems Cyber Emergency Response Team (ICSCERT), U.S. Computer Emergency Readiness Team (US-CERT), Department of Energy, Federal Bureau of Investigation [14].
•Attack time frame March 2015 – December 23, 2015: Please refer to Fig 12.

•March 2015: The extremely calculated attack was launched this month when attacks start the initial stage by sending spearphishing emails that have the Microsoft Office documents which were opened by the user in the system, as soon as the document was opened, a popup was displayed that asking the user to enable the Macros in the document. As the user allowed these Macros malware named as Blackenergy3 was installed into the system. The most important fact over here is that the malicious code was installed not due to any vulnerability in the system code but due to the huge loophole inside Microsoft office. As this malicious code was injected and made a communication channel to the adversary system. The adversary stayed in the system for more than 6 months before the attack happened. During this period the adversary observed deeply the whole system using credential theft and was able to access the pivot of the whole system which is SCADA and its servers. As the SCADA system was installed with the firewall but somehow attackers managed to bypass the firewall and were able to access the user management credentials to reach the Windows Domain Controller attackers also became successful to use VPN so to access Into SCADA remotely. Once got all the things they started planning the attack [14]. The control centers were also taken down by the attackers by reconfiguring the UPS (Uninterruptible power supply) which was responsible to supply the backup power the control centers because they not only want the power outage for the costumers but also make it hard to recover from the outage for the management. The firewall also coded maliciously so the SCADA cannot access to its Substations during the period of outage. As the attackers have credential access to the system so they changed the user id and password for the most of systems so the legitimate users cannot access them during the recovery phase.

•December 23, 2015: On this date, the attackers tap the SCADA system of the power system and hijacked the network through VPN and send Commands to deactivate the UPS system. At the same time, the system's whole communication system was hacked so no can call out- side or the regional office. They also launched a power shutdown of the main data centres that would occur a few hours later. The Killdisk approach was used to completely delete the data from the disk during the period of the reboot session [14]. Attackers also launched the telephony Denial of service attack at the all-customer care centres. The hacker used the flood of fake requests on the system servers so that legitimate users should be prevented to report the power outage. When the hackers open the breakers and took a lineup and take control of the dozens of substations, they overwrote the firmware on some of the substation serial-to-ethernet converters, as well as injecting the malicious firmware in place of legitimate firmware leading the converters to be- come inoperable and uncoverable. Once the firmware was injected with the malicious code it cannot be recovered even with the help of the manufacturer [14]. Once the attackers were almost near to the attack, at- tackers used the software Killdisk to completely wipe off the files from the operator station making their working nonefficient. The Killdisk is a process that makes the computer crash. The infected computer is unable to reboot as the system as it completely overtook the master boot record of the system. Killdisk doesn't infect the whole system but some of the specific systems like management, HR, finance, and ICS operation staff systems are compromised for the success of this attack. reports that the Black Energy malware was used to download and launch the KillDisk malware. There were also reports that there was at least one instance where a Remote Terminal Unit (RTU) product with an embedded Windows HMI card (ABBRTU 560 CMU-02 – PLC Daughter Card) was overwritten with KillDisk.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

•December 23, 2015: At 5 pm, Prykar Pattya posted a note to its website acknowledging the power outage and reassuring customers that they were working to find the source of the problem. At 5:30 pm they posted a second note saying the cause of the outage was hackers; making it the first publicly acknowledge cyberattack that caused a power outage [14].

VIII. FEDERAL FUNDING FOR SMART GRID

The given figure shows the funding given by federals in Canada to the smart grid advancement. TRL denoted the technology maturity. The Natural Sciences and Engineering Research Council (NSERC), an organization that supports academic creative research, including areas linked to smart grids, is not included in the funding mentioned in this summary. Depending on the amount of technology preparedness, certain federal programs have restrictions on the kind of projects they may fund (TRL). The Energy Innovation Program expedites clean energy technology research and development (RD) in the areas of studying renewable, smart grid, and storage systems; reducing diesel usage by industrial operators in northern and remote communities; lowering methane and volatile organic compound emissions; lowering GHG emissions in the build- ing sector; advancing carbon capture, use, and storage; and enhancing industrial efficiency. This initiative receives support from both internal and external governments.

Internal energy RD initiatives with a focus on creating a sustainable energy future for Canada's economy and environment are funded through the Program of Energy Research and Development. Only federal departments and agencies or non- federal groups who collaborate closely with one are supported by this fun

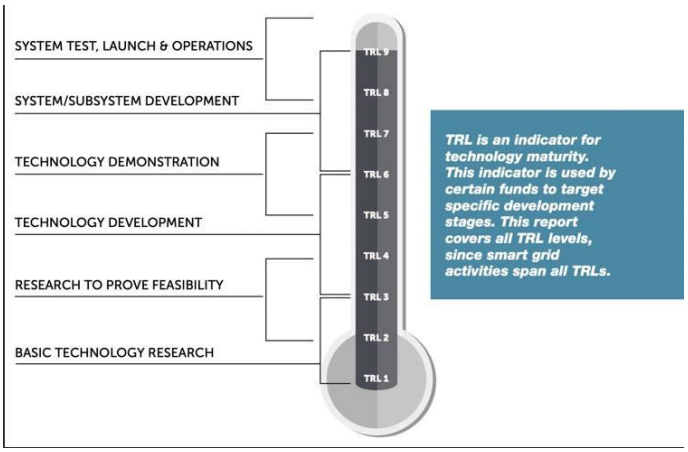

Fig. 13. Technology readiness level scale

Through a number of initiatives, the Green Infrastructure Phase II (GI2) fund hastens the implementation and market entry of next-generation sustainable energy infrastructure. GI2 is made up of a number of initiatives that concentrate on specific infrastructure streams, as explained below. This fund is only for outside funding.

The GI2's Smart Grid Program supports the adoption of smart grid technology from utility-led projects in order to lower greenhouse gas emissions, make better use of current power resources, promote innovation, and create clean jobs. The GI2 Emerging Renewable Energy Program supports the deployment of offshore wind, tidal, geothermal, concentrated solar power and other emerging RE technologies.

The Clean Growth Hub is a federal government resource that supports companies and projects, coordinates programs, and tracks results in the cleantech sector. This team of experts helps businesses of all sizes and levels better understand government programs and services. A six-month nationwide open and inclusive discourse called Generation Energy was started by the Canadian government in 2017 to encourage discussion about what a low-carbon energy future for Canadians might entail. More than 380,000 Canadians attended this project, including subject matter experts, and Indigenous and community leaders. In June 2018, a report describing the energy future that Canadians envisioned was published. Despite a wide range of interests, everyone agreed that everyone should have access to cheap, dependable,

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

and clean energy. Four complementary transitional routes were identified by the report's findings: energy efficiency, clean power, renewable fuels, and cleaner oil and gas.

The economic and environmental advantages for all customers were a key emphasis of Quebec's Energy Plan 2030, which was published in 2016 [49]. The strategy includes a 25 increase in RE generation as one of its goals. As a project stated in the Energy Policy 2030 for a public business, Transition Quebec (TEQ) was established to enable a smooth transition to meet the energy targets set by the Government of Quebec. Every five years, plans are developed with input from partners to make sure that the necessary steps are taken to reach government targets. The first plan, the 2018-2023 Master Plan, was unveiled as a short-term strategy for achieving 2030 targets through energy innovation, transition, and efficiency. In order to gradually roll out dynamic pricing alternatives on a voluntary basis for the summer of 2019 [50], Hydro-Quebec made a request to regulators. Customers would be encouraged to cut back on consumption during off-peak times when the system is less stressed by higher prices during morning and evening peak hours.

IX. FUTURE SCOPE

In a future smart grid, technology should be advanced so that consumption of energy could be managed so as to make the delivery of energy more efficient. It could be achieved by making use of machine learning via the cloud and big data. Grid security could also be improved by using this technology. Plug-and-play technology could be also implemented in order to redistribute energy made by wind turbines, solar cells, etc. Automation should be done in smart grids in order to make the smart grids self-healing in which with the help of certain algorithms malicious patterns could be detected. The smart grids need to be completely automated. The power generation to distribution and service management needs to be automated.

1. Standardization of smart grids: There are agencies that are working on the standardization and regulation of smart grids.
- IEEE Power and energy society (PES)
- IEC smart grid standardization - National institute of standards and technology (NIST)

2. Smart grid in electric vehicles: As pollution is increasing day by day, the world is slowly coming towards electric vehicles. As far as now it is difficult for electric vehicles to communicate with smart grids.
- Smart meters, communication, and control are examples of advanced technology, and so are smart grids. As a result, it has the ability to offer electric vehicles as both a load and a flexible energy supply.
- There has been a lot of research done on this charging and discharging. A similar study carried out in Portugal demonstrates effective coordination between solar energy and the charging of electric vehicles [21].
- Understanding the electric grid's dynamic behaviour is necessary to forecast its dependability and efficiency when using V2G. Although very few cases of weak grids are reported while using V2G.

X. CONCLUSION

The smart grid is a very advanced electricity supply network system that is used effectively and efficiently to supply electricity. It should also be combined with smart cars and many more advanced devices. To increase the security in smart grids various algorithms like CSM should be integrated so that any malicious data injection could be detected. There is work going on in making the advancement in the smart grids. Many organizations are working to standardize and regulate the smart grid. Work on plug-n-play, self-healing and total automation of the smart grid is going on which will help to make the smart grid an effective technology.

REFERENCES

1. X. Yu, C. Cecati, T. Dillon, and M. G. Simoes, "New frontier of smart grids," IEEE Ind. Electron. Mag., vol. 5, no. 3, pp. 49–63, 2011.
2. Department of Energy, "The future of the grid: Evolving to meet America's needs," Dec. 2014.
3. S. Xiao, "Consideration of technology for constructing Chinese smart grid," Autom. Electric Power Syst., vol. 33, no. 9, May 2009.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307178|

4. IEEE Grid Vision 2050 Reference Model, New York, NY, USA: IEEE, 2013.
5. Fazili, S., Grover, J. (2022). Smart Grid: A Survey. In: Agarwal, P., Mittal, M., Ahmed, J., Idrees, S.M. (eds) Smart Technologies for Energy and Environmental Sustainability. Green Energy and Technology. Springer, Cham.
6. X. Fang, S. Misra, G. Xue and D. Yang, "Smart Grid — The New and Improved Power Grid: A Survey," in IEEE Communications Surveys Tutorials, vol. 14, no. 4, pp. 944-980, Fourth Quarter 2012.
7. Hossain, Rahat Maung, Amanullah Than Oo, Aman Ali, Shawkat. (2013). Smart Grid.
8. P. Alcoy, P. Bowen, C. Chui, S. Bjarnason, K. Kasavchenko, G. Sockrider, and D. Anstee, (2018). Arbor's 13th Annual Worldwide Infrastructure Security Report.
9. Jin, Y. Zheng, H. Zhu, D. M. Nicol, and L. Winterrowd, "Virtual time integration of emulation and parallel simulation," in Proc. ACM/IEEE/SCS 26th Workshop Princ. Adv. Distrib. Simul., Jul. 2012, pp. 201–210. [Online]. Available: http://dl.acm.org/citation. cfm?id=2372596.2372597
10. V. Kolesnikov and W. Lee, "MAC aggregation protocols re- silient to DoS attacks," IEEE SmartGridComm, vol. 7, no. 2, pp. 226–231, 2011. [Online]. Available: http://inderscience.metapress. com/index/XW8541375106697V.pdf
11. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A.
12. Cardenas, and J. G. Jetcheva, "AMI threats, intrusion detection requirements and deployment recommendations," in Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm), Nov. 2012, pp. 395–400.
13. X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 809–818, Dec. 2011.
14. Huseinovic´, S. Mrdovic´, K. Bicakci, and S. Uludag, "A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid," in IEEE Access, vol. 8, pp. 177447-177470, 2020, doi: 10.1109/AC-CESS.2020.3026923.
15. Ukraine power grid cyberattack and US susceptibility: Cybersecurity Im- plications of Smart Grid Advancements in the US. Retrieved December 9, 2022, from https://web.mit.edu/smadnick/www/wp/2016-22.pdf
16. D. Maio, "Rao test for adaptive detection in Gaussian interference with unknown covariance matrix," IEEE Trans. Signal Process., vol. 55, no. 7, pp. 3577–3584, Jul. 2007.
17. D. Gamerman and H. F. Lopes, Markov Chain Monte Carlo: Stochastic Simulation for Bayesian Inference. Boca Raton, FL, USA: CRC, 2006.
18. Tu`ng T. Kim, H. Vincent Poor (2011). Strategic Protection Against Data Injection Attacks on Power Grids.
19. Yi Huang, Jin Tang, Yu Cheng, Husheng Li, Kristy A. and Zhu Han (2016). Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis.
20. Challenges, Trends, and Solutions for Communication Networks and Cyber-Security in Smart Grid
21. Natural Resources Canada: Smart Grid in Canada
22. The Future of Smart Grid Technologies.
23. Osama Majeed Butt, Muhammad Zulkarnain and Tallal Majeed Butt. Recent advancement in smart grid technology: Future prospects in the electrical power network Ain Shamas: Recent advancement in smart grid technology

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details