Analysing Smart Power Grid against different Cyber Attacks on SCADA System

Garvit Gupta[1], Rahul Meena[2], Raghuveer Meena[3], Pulkit Yadav[4], Rintam Singh Shekhawat[5],

Department of Electrical Engineering,

Swami Keshvanand Institute of Technology, Management &Gramothan, Jaipur

garvit.gupta@skit.ac.in[1], rahulmeena4437@gmail.com[2], meenaraghuveer7557@gmail.com[3], pulkityadav156@gmail.com [4], rintamshekhawat@gmail.com[5]

Abstract- The integration of information and communications technology (ICT) with traditional power grid is transforming the power grid into a more reliable and smarter cyber physical system. A supervisory control and data acquisition (SCADA) system is used to implement the cyber layer for power grid, which is responsible for real-time monitoring and control of power grid and power delivery network. A SCADA system combined with other devices creates smart power grid environment, but it also makes power grid vulnerable against different cyber-attacks as it requires connection with various kinds of open networks. Smart power grids are a extremely critical infrastructure and attack of any kind can affect socio-economical condition of the region. In this paper we present a non-complex co-simulation environment for analysing smart power grid and also includes two different cyber-attack scenarios.

Index Terms- co-simulation; smart power grid; SCADA system; cyber-attack scenarios.

I. INTRODUCTION

The traditional power grid is no longer a practical solution for power delivery and distribution due to several shortcomings including: chronic blackouts, energy storage issues, high cost of assets, and high carbon emissions. Briefly, several cases prove that there is a serious need to improve the functionality of the traditional power system.

For example, in February 2020, the storm Ciara caused a power cut for around 130,000 homes in France. In March 2016, at least 70 million people in Turkey were impacted by a power blackout. These examples are the obvious reasons why using a traditional power grid is no longer considered an effective power system. To address the limitations of the traditional grid, a new approach, microgrid, was introduced.

A microgrid can be defined as a local and small distribution system that consists of sets of micro sources, namely micro turbines, fuel cells, photovoltaic arrays wind turbines, and some storage systems like energy capacitors. It can be connected to a main grid or work independently. Microgrids provide some benefits, such as a higher efficiency, reduction of emissions, and cheaper and cleaner energy. Also, this technology deals with some challenges, including the resynchronization with the main grid, which can be problematic to the network, due to the network inconsistency. To address these challenges and limitations, a holistic solution, smart grid, was proposed in 2007. This new electrical grid (smart grid) includes a variety of operations and energy measures, including smart meters, smart appliances, renewable energy resources, and energy-efficient resources. It utilizes information technology to deliver energy to end-users through a two-way flow of communications, which changes the power infrastructure in terms of efficiency, scalability, reliability, and interoperability. The National Institute of Standard and Technology (NIST) state that smart grids consist of seven logical domains, namely bulk generation, transmission, distribution, customer, markets, service provider, and operations. These logical domains have actors and applications that are presented as smart grid’s conceptual model. Actors are defined as programs and systems, while applications are considered as tasks.

DOI: 10.55041/IJSREM28566

These tasks are conducted by a single or multiple actors in every domain.

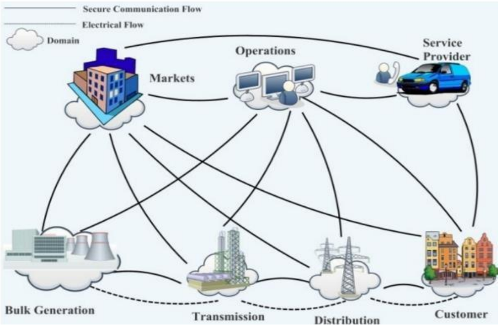

Fig:1 NIST Framework and Roadmap for Smart Grid

Over the last decade, several surveys provided an overview of smart grid's cyber-security, the main cyber-attacks that can damage the smart grid infrastructure, the detection techniques, and the countermeasures. They classify cyber-attacks in smart home/smart grid networks according to confidentiality, integrity, availability, authorization, and authenticity.

II. RESEARCH MOTIVATION

The ever-growing reliance on interconnected technologies in modern power systems has led to the emergence of smart grids, promising enhanced efficiency and sustainability to combat the impacts of climate change. However, this increased complexity also exposes these critical infrastructures to a myriad of cyber threats. In light of the escalating frequency and sophistication of cyberattacks on smart grids, a comprehensive understanding of their components, vulnerabilities, and potential impacts becomes imperative. It aims to unravel the intricate interplay between smart-grid components and cyber vulnerabilities, analyze the diverse spectrum of cyber threats and their short-term and long-term consequences, investigate cascading effects on grid components, draw insights from real-world case studies, and develop quantitative models to assess cyberattack impacts. By exploring the techno–economic–safety–social implications of cybersecurity measures and delving into the application of artificial intelligence (AI) techniques, this study aspires to contribute valuable insights to the field of smart-grid cybersecurity, ultimately fortifying the resilience of critical energy infrastructure.

III. SMART GRID AND CYBER-SECURITY

A smart grid is an electricity network based on digital technology that is used to supply electricity to consumers via two-way digital communication. This system allows for monitoring, analysis, control and communication within the supply chain to help improve efficiency, reduce energy consumption and cost, and maximize the transparency and reliability of the energy supply chain. The smart grid was introduced with the aim of overcoming the weaknesses of conventional electrical grids by using smart net meters. Smart grid technology is an extended form of analog technology that has also been introduced for controlling the use of appliances by employing two-way communication. However, the prevalence of Internet access in most homes has made the smart grid more practically reliable to implement. Smart grid devices transmit information in such a way that enables ordinary users, operators and automated devices to quickly respond to changes in smart grid condition systems.

Cybersecurity measures protect users against viruses, malware, ransomware and other threats that cause outages or data breaches. When applied correctly, these measures can help smart grid operators quickly identify potential vulnerabilities within their networks and take corrective action before any damage occurs.

IV. INTRODUCTION OF SCADA

SCADA stands for "Supervisory Control and Data Acquisition". SCADA is a process control system architecture that uses computers, networked data communications, and graphical Human Machine Interfaces (HMIs) to enable high level process supervisory management and control. SCADA systems communicate with other devices such as programmable logic controllers (PLCs) and PID controllers to interact with industrial process plants and equipment. SCADA systems form a large part of control systems engineering. SCADA systems gather pieces of information and data from a process that is analyzed in real-time (the "DA" in SCADA). It records and logs the data, as well as representing the collected data on various HMIs. This enables process control operators to supervise (the "S" in SCADA) what is going on in the field, even from a distant

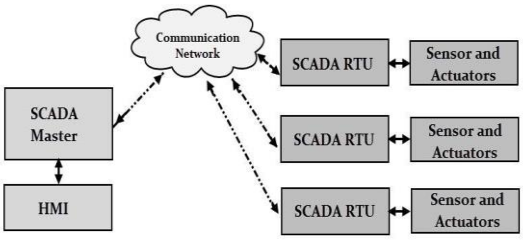

Fig:2 Genric SCADA System

location. It also enables operators to control (the “C” in SCADA) these processes by interacting with the HMI. Supervisory Control and Data Acquisition systems are essential to a wide range of industries and are broadly used for the controlling and monitoring of a process. SCADA systems are prominently used as they have the power to control, monitor, and transmit data in a smart and seamless way.

V. OBJECTIVES OF SCADA SYSTEM

• **Monitor**: SCADA systems continuously monitor the physical parameters

• **Measure**: It measures the parameter for processing

• **Data Acquisition**: It acquires data from RTUs (Remote Terminal Units), data loggers, etc.

• **Data Communication:** It helps to communicate and transmit a large amount of data between MTU and RTU units

• **Controlling**: Online real-time monitoring and controlling of the process

• **Automation**: It helps for automatic transmission and functionality

The SCADA systems consist of hardware units and software units. SCADA applications are run using a server. Desktop computers and screens act as an HMI which are connected to the server. The major components of a SCADA system include:

• Master Terminal Unit (MTU).

• Remote Terminal Unit (RTU).

• Communication Network.

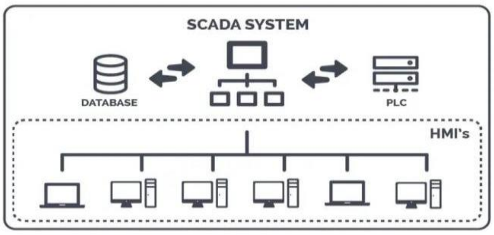

Fig:3 Functional units of SCADA

VI. SCADA IN DIFFERENT ATTACKING SITUATIONS

Flooding attack

Attacker gets the access of SCADA system and perform flooding attack, (i.e., DoS attack) on two sensor units. And as a result of attack, the victim PMU units were not able to transfer the data to their collector module. The sensors are overwhelmed by the attack traffic and transfer of fetched data from power simulator by these sensors were stopped resulting in no reception of data to their respective DC which will assume the failure of these units. Therefore, the fetched data from victim sensors is not transferred to master unit via DC and gateways. For this experiment, only sensors unit are targeted for flooding attack which is shown and results are stored, although similar kinds of result were observed while attacking the other units with flooding attack.

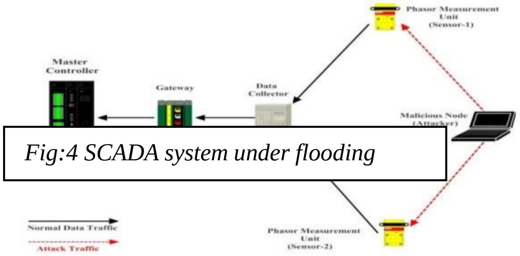
Phasor Measurement Unit (Sensor-1)
Master Controller
Gateway
Data Collector
Malicious Node (Attacker)
Normal Data Traffic
Attack Traffic
Phasor Measurement Unit (Sensor-2)

Fig:4 SCADA system under flooding

Sink hole attack

Attacker gets the access of SCADA system and perform sink hole attack, i.e., man in-middle (MITM) attack] on one of the DC units which results in transfer the data to attacker module rather than its connected gateway from victim DC units. As the gateway is connected to victim DC and not receive the respective data, it assumes that the DC is failed. Therefore, the fetched data from sensors is not transferred to master unit as DC suffer from the MITM attack. The attacker receives the data from DC and can use this data to launch other attacks as well. For this experiment only DC units are targeted for sink hole attack and outcomes are observed.

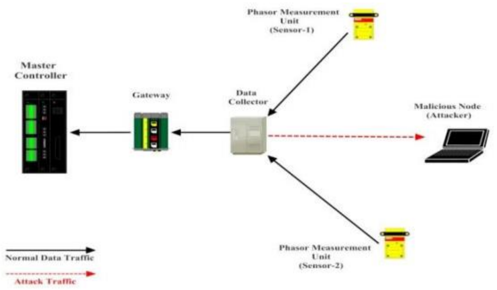
Phasor Measurement Unit (Sensor-1)
Master Controller
Gateway
Data Collector
Malicious Node (Attacker)
Phasor Measurement Unit (Sensor-2)
Normal Data Traffic
Attack Traffic

Fig: 5 SCADA system under sink hole attack

VII. CONCLUSION

The security of smart grid networks is of paramount importance and plays a pivotal role in the implementation of smart grid systems. However, prior studies have shown a constrained role in evaluating cyber-security solutions for smart grid networks. Therefore, this paper considers the shortcomings of the existing surveys and provides an in-depth description of potential attacks that target smart grids and an evaluation of different security solutions.

In this paper, we propose a benchmarking of cyber-attacks in terms of the integrity, availability, confidentiality, and accountability and a classification based on OSI communication layers. Moreover, we present a new classification for the existing detection techniques, which is mainly divided into localization-based, AI-based, prediction models, filtering techniques, and intrusion detection systems. We also classify the countermeasure techniques into preventive and protective techniques. In the preventive countermeasures, we describe secure protocols and standards, cryptographic and authentication, intrusion prevention, education, access control, and required cyber-security policies approaches. For the protective countermeasure category, we discuss spread spectrum techniques and game theory in the smart grid. Finally, we describe the existing challenges that can guide future research directions. This survey has highlighted the requirements of new solutions, which can collectively resolve the problems related to security challenges in the smart grid infrastructures without compromising the performance and Functionalities of this type of network.

VIII. REFRENCES

1. https://www.scirp.org/journal/paperinformation?paperid=121421

2. https://www.researchgate.net/publication/331418396_Analysis_of_cyber-attacks_on_smart_grid_applications

3. https://en.wikipedia.org/wiki/Cyberattack

4. https://www.inderscienceonline.com/doi/abs/10.1504/IJICA.2021.116656