Cyber Vulnerabilities in Smart Grid: A Review

Barnali Kundu
Department of Electrical Engineering,
Guru Nanak Institute of Technology
Sodepur, India

Neha Gupta
Department of Information Technology
Guru Nanak Institute of Technology
Sodepur, India

Raunak Seal
Department of Information Technology
Guru Nanak Institute of Technology
Sodepur, India

***Abstract*— Information technology solutions modernize the traditional power grids transformed into Smart Grid. Smart Grid is a power network consisting of digital communications technology facing challenges of increasing load demands along with problems like blackouts, overloads, and voltage sags foremost dealing with cyber-attacks. In recent years, internet driven equipments of smart grid are suffering from different cyber vulnerabilities. In this research paper, an extensive review work has been carried out which includes occurrence history in smart grid scenario. Different heuristic detection and estimation techniques have also been reviewed in this paper. Using these techniques, cyber vulnerabilities in smart grid like relay protection, power flow control; grid security and reliability can be modeled and analyzed.**

Keyword:- Smart Grid, SCADA, Cyber attacks, Cyber security

I. INTRODUCTION

Recent revolution in modern power industry evolves normal power system network into Smart grid governed by information and communication technology. Internet technology and digital communication helps smart grids to respond intelligently and communicate among user of the grid. Integration of new generation energy sources, sensors, smart meters and control devices in the smart grid provide a lot of benefits in a modern ecosystem. New generation sources like geothermal heat, waterfalls, solar radiation, wind, fuel cell, and nuclear fission generates green energy which are attached to the electricity distribution structure to meet the required electricity demand. Instead of the grid modernization, energy users still require to obtain the reliable power delivery at their end ensuring stability of the grid [1]. Energy Storage systems and renewable energy based distributed energy resources (DERs) are bought in the new age grid though Energy Management System (EMS). This EMS proves smart grid a new opportunity in energy assets [2]. EMS with intelligent control technologies require to provide extra attention against cyber vulnerabilities. These vulnerabilities affect internet governed instruments in the smart grids comprising of Supervisory control and data acquisition (SCADA), Phasor Measurement Unit (PMU), Remote terminal units (RTU) etc. So, it is vital to provide the security and prepare a safe smart grid infrastructure incorporated with intelligent technologies. Cyber rackets initiate cybercrimes for their financial gain which causes a widespread effect on economical state of a nation [3]. In the electric grid, several unpredictable attack are continuously occurred which are need to discover for the solution of cyber vulnerability issues [4]. Internet technologies are being used by energy users can also direct cyber vulnerabilities. So, it is very much required to examine potential cyber security threats, analyzed them in terms of the security objectives. This paper gives a spotlight on several past worldwide cyber attacks and the need of cyber security for smart grid. It also presents potential components of smart grid through which cyber vulnerabilities can be encountered. Several artificial intelligence based methods for identification and estimation of cyber vulnerabilities have enlisted and reviewed in this paper which will direct a path for smart grid protection. Using these different methods cyber vulnerabilities like relay protection, power flow control; grid security and reliability can be modeled and analyzed. In this investigation, cyber security objectives have been set up firstly (Section II) with detailed past history of several cyber attacks (Section III). In section III, internet driven potential equipments in smart grid infrastructure have been discussed. Next, in Section IV various protective measures and detection techniques have been presented, and finally, the paper is concluded in section V.

II. CYBER SECURITY OBJECTIVES

Cyber Security is the security which provides the protection of computer systems from information or data leak, theft of the data, important files, important passwords, confidential documents, and acts as a shield for the hardware as well as software [4-9]. At Digital Equipment Corporation, computers used for operating systems were hacked in 1979. After that various hackers used to hack many servers of U.S countries. Even NASA couldn't get rid of it. Sometimes credit cards of popular companies, govt. servers, and they become a headache to the computer programmers and specialists. The year 1985 used to be denoted as the proper beginning of Cyber security. The first antivirus support was first invented in 1987 [4]. Most of the countries have smart technology to run the power grid which uses computer based advanced technology to run a power grid. The smart grid has to be build with strong cyber security arrangements become one of the most important priorities for all the countries. In smart grid infrastructure, energy transfers from source to customer end through generation, transmission, distribution, and consumption as presented in Fig 1.

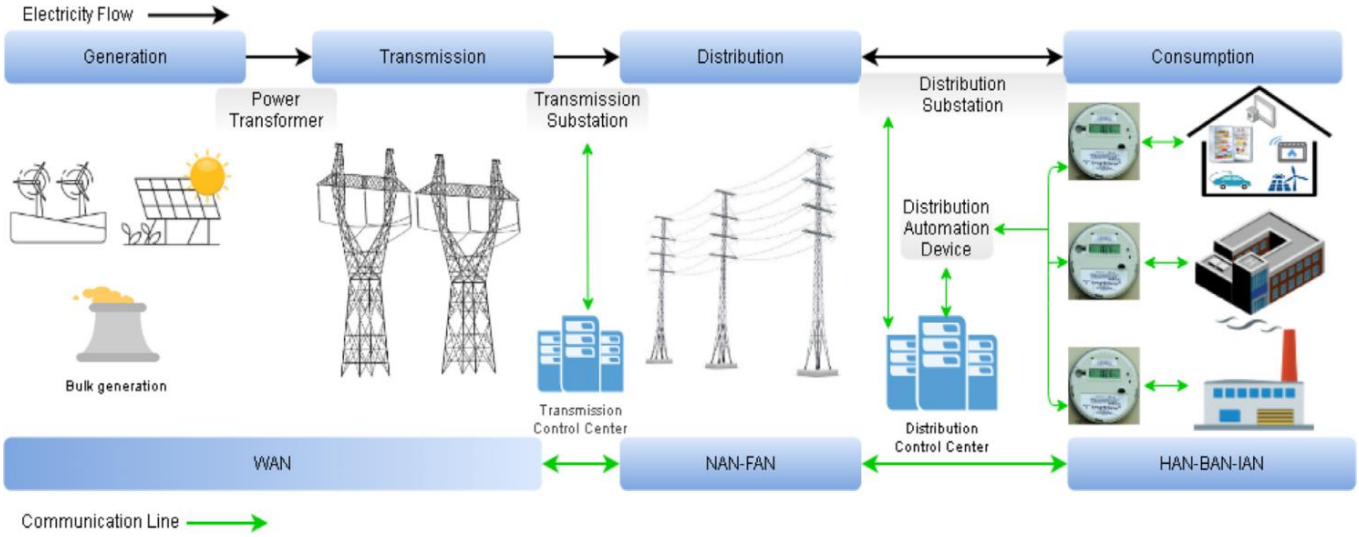

Fig 1. Smart grid structures

III. HISTORY OF CYBER ATTACK

During the last three years, the Power Industry has been affected by high profile attacks. Internet technology driven equipments such as webcams, and smart home appliances like smart washing machine, smart TV, smart refrigerator are used
for cyber attack. Mirai IoT botnet , a malware code has been developed by the cyber racket rigorously scan the internet for the IP address of the internet connected device to get default passwords by their developed code[4]. The attackers The cyber crimes occurred with the hacker's command and control server by sending out malformed packets. Bricker Bot malware caused the 2 millions IoT devices to become permanently disabled. Windows operating system protocol has been used by hacker with a ransomware Wanna Cry ransomware. There were listed many cyber-attacks on power grids all over the world. Most of the notable cyber-attacks used to happen during 2014 to now. Security of smart grid has faced questions many times in history. During this time period US, Russia, Korea had faced cyber-attacks thousands of times. In 2020 India also enlisted its name in affected countries. Here are few of the most dangerous cyber-attacks on smart grids.

2014: -In the year of 2014 the most horrible 79 incidents of hacking the power grids. According to the report, in energy sector, 37% companies have been smashed. It was found that 50 types of malwares were used to target the energy farms and energy companies only in 2013. One of a energy industry in U.S, has broken down due to insertion of a spy malware in the software which was being used to run dozens of turbines, controllers and other industrial machinery. This malware insertion has been taken place due to clicked on a bad link in an email [5] by one employee. Again in the month of December, in South Korea nuclear and hydroelectric company Korea Hydro and Nuclear Power (KHNP) was hacked and theft all layout and instruction manuals of two nuclear reactors.

December, 2015: - It has been almost one year since Korea's incident. In December of 2015 a new incident of cyber attack came into the limelight in Western Ukraine. On December 23, 2015, at the Prykarpattyaoblenergo power plant, all circuit breaker one after another has been opened causing a blackout in large areas of Ukrainians. Blackout has been occurred to 225000 households by shutting down the plant and backup generators.

December 2016:- In kyiv, Ukraine, a blackout was happened for an hour, after disabling an electricity substation. The attacker was attributed to Russian hackers, suggesting that the attack aimed to physically damage the power grid.

August 2017: - In Saudi Aramco, cyber attacks were aimed to the safety system in petrochemical plants [7].

12 October, 2020: -In Mumbai, India, a malware was inserted by the cyber attacker into the ventilation system and ICU system results the city has faced a power cut for more than 12 hours. The situation became more dangerous during Covid situation due to power cut [8].

IV. CYBER INFRASTRUCTURE OF SMART GRID

The smart grid employs internet technology to the communication devices which is intensively prompt to cyber attacks. Ethernet, Internet Protocol (IP) and other operating systems used for transmitting and receiving signals in smart grid structure plays a source of cyber vulnerabilities to the grid. Cyber Security has been employed in the Smart Grid to provide numerous benefits in sense of reliable operation and service to their customers. The functions of basic cyber Infrastructure of smart grid are to process, store, and communicate information through a control system (SCADA) [9].

A. SCADA System

In smart grid, centralized control system Supervisory control and data acquisition (SCADA) is used in power distribution system to monitor and control the power flow [9]. The main components as presented in Fig 2 which includes are the
(i) HMI (human machine interface), (ii) Remote Terminal Units (RTUs),(iii) Programmable Logic Controller (PLC), (iv) Network for Communication

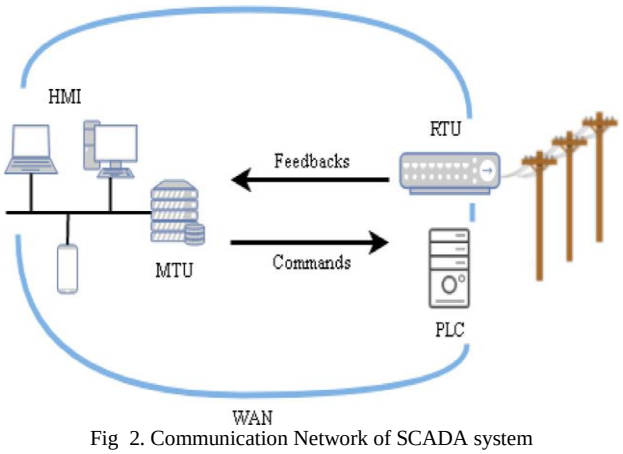

Fig 2. Communication Network of SCADA system

B. Advanced Metering Infrastructure (AMI)

It connects the central control system and smart meters by integrating various technologies. AMI can forecast the energy demand; manage congestion and the real-time price of electricity. It consists of different hardware and software components to measure energy consumption and power transmission between utility and customers [10] includes measuring equipments, communication devices and centralized systems for data analysis. It records energy consumption data through the communication between the central system and smart meters [11]. In smart grid infrastructure, data communication happens through Broadband over Power Line (BPL), Power Line Communications, Fiber Optic Communication, Fixed Radio Frequency or public networks (e.g., landline, cellular, paging).

TABLE 1: DIFFERENT CYBER ATTACK IDENTIFICATION TECHNIQUES

Objectives	Detection & Estimation Method	Ref. no	Accuracy	Computational Burden
Cyber Attack Vulnerability Analysis	Power Flow Analysis through State Estimation	[13]	Yes	Yes
Cyber Attack Vulnerability Analysis	State Estimation	[14]	Yes	No
Analysis Cyber Vulnerability	Zero Sum Static Game Theory	[15]	Yes	No
Cyber Attack Detection	Game Theory	[16]	Yes	Yes
Cyber Attack Detection and Vulnerability Analysis	Dynamic Game Theory	[17]	Yes	No
Detection and Identification of Cyber Attack	Unsupervised learning	[18]	Yes	No
Online Cyber Attack Identification	Reinforcement Learning based Algorithm	[19]	Yes	Yes
Vulnerability Analysis and Intrusion	Markov Decision Process based Method	[20]	No	Yes
Cyber Attack Detection	Multivariate Gaussian based Method	[21]	Yes	No

C. Home Area Network (HAN)

It provide better control in energy demand for both utility and consumer deploying at their premises to build the communication of home appliances with AMI and hence enable a better control of loads by both utility and consumer[12].

D. Internet of Things based Sensors

Smart home appliances could be efficiently sensed and managed via the internet driven IoT sensors. Different Internet Protocols (IP), the set of rules governing the format of data is used to control the devices through the local network. Communication between the different smart grid components is made by transfer of large data with the help of specific IP addresses.

It is very complex to protect each smart grid components from cyber vulnerabilities. It is necessary to detect and identify unusual states during the communication between IoT devices and SCADA system. The traffic status of communication network can be monitored through profiling, testing, and comparison [22]. In this context, it is vital to initiate a solution that make the energy systems free from attack. Design a control system combine with Information Communication Technology (ICT) to provide secure communication between sensors, actuators, and controllers in a smart grid infrastructure enabling detection of potential threats [23]. With the application of mathematical tools, game theory can be modeled a rule for the player's interaction between attacker and a defender in smart grid and able to defense the grid [24]. Probability based techniques have been also used to assess cyber vulnerabilities for EMS security and associated energy loss [25]. Graph theory is also used to demonstrate the connection between different components of smart grid network and scrutinize the transmission of cyber vulnerabilities in smart grid prospects. In small scale energy sector, Security-metric-based techniques can be utilized to identify cyber-threats. Among all the above methods, graph theory may be considered as a useful one connecting all the equipments in smart grid network through links, nodes and, the vertices i.e. smart meters, loads, transformers, generators, routers.

V. CYBER SECURITY CHALLENGES

The mixed communication architecture of smart grids impose a challenge to design efficient and robust security arrangements that can be implemented to protect communications of the smart grid-infrastructure. Cyber security support is deployed to face various cyber vulnerability issues of smart grid. The hackers use malware in the smart grid system, which leads the system towards black out, energy theft or customer privacy britches. There is also a challenge which is more important for Cyber security support. It is natural disasters. This causes data leaks, energy consumptions as well as power cuts. Another notable challenge is physical attacks. To destroy security systems people use to break security servers or make changes in the electric circuits of the servers. This can cause the destruction of servers. Nowadays the security providers use to provide a backup server, which can recover the lost data. It can be denoted as a nice step to overcome the challenges.

A. Protective measures for Cyber attack

Several numerical methods have been initiated by the researchers as given in Table 1 for identifying and estimating the cyber attacks. Protective measures can be adopted into two broad ways. Safe internet protocol, resource share & accounting, firewalls, etc. provide the solution for cyber attack prevention whereas heuristic techniques are employed to detect the attack and analyze its response [22].

B. Intrusion Detection System (IDS) Technology

To control the operation of SCADA systems and detect threats, IDS technology has been implemented by the researcher [25]. IDSs include several statistical methods to detect unusual network traffic in SCADA systems. Statistical models have been developed with the help regression analysis, artificial neural networks, and Bayesian networks as mentioned in Table 1. SCADA-specific IDSs employ critical state, model, and rule-based approaches for SCADA systems. Researcher has also found that Modbus protocol, rule-based IDS based on IEC 61850, etc can be deployed for SCADA system in power station,.

C. Encryption Mechanisms

The cryptographic technique includes encryption to ensure secure communication and implement encryption to maintain data veracity and privacy in a smart grid. Encryption diminishes repeat and snooping attacks considerably [26]. Cryptography plays an important role in developing privacy and reliability in smart grid. To get better solution many encryption algorithms like Symmetric cryptography, such as symmetric ciphers, DES, AES, and 3DES or public key cryptography known as asymmetric cryptography has been implemented to block potential cyber-threats in smart grid.

D. IP Fast Hopping mechanism

IP Fast Hopping [25] is applied to filter malicious streams. It can hide key data and also hide users' communication period to counteract malwares kicked off by cyber attacks. During each communication period any kind of real time change of any kind of imaginary unwanted protocol can be possible into the real IP address. It limits access of the cyber attacker and only the legitimate user is able to access to the information of schedule changing to send a request to a real IP address.

VI. CONCLUSIONS

In smart grid applications, cyber-security is a challenging issue for data acquisition systems, and different control units such as supervisory control system, smart meters, IEDs, RTU, and PMUs. In this context, this study has been focused on the latest research on the cyber security of smart grid. Histories of different cyber attacks have been discussed in this paper which will be helpful to identify the reasons for the attacks. A summary of a few mathematical and artificial

intelligence based techniques has been presented to identify and estimate the vulnerabilities in the communication structure of Smart grid. To ensure secure communication within smart grid infrastructure need to form global standardization frameworks. Big data analytics, Data mining, rule based detection, information, theory-based and machine learning algorithm have been implemented to assess cyber vulnerabilities and build smart grid more reliable to the energy users. Development of dynamic IDS/IPs can prevent and make alert the smart grid users about the unexpected malware in AMI and smart meters Furthermore, a compact review of countermeasures of cyber-security threats such as encryption, intrusion analysis and forensic analysis for smart grid infrastructure preserve the next step of research in this field.

REFERENCES

[1] C.W. Gellings, The Smart Grid: Enabling Energy Efficiency and Demand Response, The Fairmont Press, 2009.
[2] Cybercrime costs quadrupled from 2013 to 2015 to $400 billion and are projected to quadruple again between 2015 and 2019 to reach $2 trillion
[3] https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/https://blog.avast.com/history-of-cybersecurity-avast#:~:text=In%201979%2C%2016%2Dyear%2D,over%20the%20next%20 few%20decades.
[4] A. F. Aloul, A.R. Al-Ali, R. Al-Dalky, M. Al-Mardini, W. El-Hajj, Smart grid security: threats, vulnerabilities and solutions, Int. J. Smart Grid Clean Energy (2012).
[5] https://en.wikipedia.org/wiki/December 2015 Ukraine power grid cybe rattack
[6] https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html
[7] https://www.thehindu.com/news/cities/mumbai/cyber-sabotage-led-to-october-2020-outage-in-mumbai-minister/article33964939.ece
[8] https://en.wikipedia.org/wiki/Computer_security
[9] Margossian, H.; Sayed, M.A.; Fawaz, W.; Nakad, Z. Partial Grid False Data Injection Attacks Against State Estimation. Int. J.Electr. Power Energy Syst., 110, 623–629, 2019.
[10] Y. Yan, Y. Qian, H. Sharif, D. Tipper, A survey on cyber security for smart grid communications, IEEE Commun Surv. Tutor. 14 (4) (2012) 998–1010
[11] Sreeram, T.S.; Krishna, S. Managing False Data Injection Attacks during Contingency of Secured Meters. IEEE Trans. Smart Grid 2019, 10, 6945–6953.
[12] Wang, Q.; Tai, W.; Tang, Y.; Ni, M.; You, S. A Two-Layer Game Theoretical Attack-Defense Model for a False Data Injection Attack against Power Systems. Int. J. Electr. Power Energy Syst. 2019, 104, 169–177.
[13] Hasan, S.; Dubey, A.; Karsai, G.; Koutsoukos, X. A Game-Theoretic Approach for Power Systems Defense against Dynamic Cyber-Attacks. Int. J. Electr. Power Energy Syst. 2020, 115, 105432.
[14] Gao, B.; Shi, L. Modeling an Attack-Mitigation Dynamic Game-Theoretic Scheme for Security Vulnerability Analysis in a Cyber-Physical Power System. IEEE Access 2020, 8, 30322–30331.
[15] Wang, D.;Wang, X.; Zhang, Y.; Jin, L. Detection of Power Grid Disturbances and Cyber-Attacks Based on Machine Learning. J.Inf. Secur. Appl. 2019, 46, 42–52.
[16] Kurt, M.N.; Ogundijo, O.; Li, C.;Wang, X. Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach. IEEE Trans. Smart Grid 2019, 10, 5174–5185.
[17] Hao, Y.;Wang, M.; Chow, J.H. Likelihood Analysis of Cyber Data Attacks to Power Systems with Markov Decision Processes. IEEE Trans. Smart Grid 2018, 9, 3191–3202.
[18] An, Y.; Liu, D. Multivariate Gaussian-Based False Data Detection against Cyber-Attacks. IEEE Access 2019, 7, 119804–119812.
[19] Y. Guo, C. W. Ten, S. Hu, and W. W. Weaver, "Modeling distributed denial of service attack in advanced metering infrastructure," in 2015 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5, Feb 2015.
[20] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, and H. F. Wang, "Multiattribute scada-specific intrusion detection system for power networks," IEEE Transactions on Power Delivery, vol. 29, no. 3, pp. 1092–1102, June 2014.
[21] T. Liu, Y. Liu, Y. Mao, Y. Sun, X. Guan, W. Gong, and S. Xiao, "A dynamic secret-based encryption scheme for smart grid wireless communication," IEEE Transactions on Smart Grid, vol. 5, no. 3, pp.1175–1182, May 2014.
[22] V. Krylov, K. Kravtsov, E. Sokolova, and D. Lyakhmanov, "Sdi defense against ddos attacks based on ip fast hopping method," in 2014 International Science and Technology Conference (Modern Networking Technologies) (MoNeTeC), pp. 1–5, Oct 2014.
[23] R. Kaur, A.L. Sangal, K. Kumar, Modeling and simulation of DDoS attack us- ing Omnet++, in: 2014 International Conference on Signal Processing and Inte- grated Networks (SPIN), pp. 220–225, 2014.
[24] C. Peng, H. Sun, M. Yang, Y. Wang, A survey on security communication and control for smart grids under malicious cyber attacks, IEEE Trans. Syst. Man Cybernet. 1–16, 2019.
[25] H. Wei, Z. Ling, G. Yajuan, C. Hao, Research on information security test- ing technology for smart Substations, in: 2014 International Conference on Power System Technology, pp. 24 92–24 97, 2014.
[26] B. C. Alcaraz, L. Cazorla, G. Fernandez, Context-awareness using anomaly based detectors for smart grid domains, in: International Conference on Risks and Security of Internet and Systems, pp. 17–34, 2014.