2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) | 978-1-6654-6297-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927892

Emerging Simulation Frameworks for Analyzing Smart Grid Cyberattack: A Literature Review

Oscar Famous Darteh
School of Electronics and Information Engineering
Nanjing University of Information Science and Technology
Nanjing, China
dartfamous@gmail.com

Qi Liu
Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET)
Nanjing University of Information Science and Technology
Nanjing, China
qi.liu@nuist.edu.cn

Xiaodong Liu
School of Computing
Napier University organization
Edinburgh, UK
x.liu@napier.ac.uk

Ibrahima Bah
School of Computer Science and Software
Nanjing University of Information Science and Technology
Nanjing, China
20205220003@nuist.edu.cn

Francis Mawuli Nakoty
School of Computer Science and Software
Nanjing University of Information Science and Technology
Nanjing, China
francisnakoty@outlook.com

Amevi Acakpovi
Dept. of Electrical and Electronic Engineering
Accra Technical University
Accra, Ghana
acakpovia@gmail.com

***Abstract*— The transition of the conventional power grid into the Smart Grid (SG), a widely distributed energy delivery network characterized by a two-way flow of electricity and information, is key for energy sector stakeholders. Despite the SG's clear improvements, there are still certain network vulnerabilities in the power distribution and communication systems. Therefore, research into cyber security frameworks is essential to handle these security issues adequately. This paper first discussed SG's architecture, possible vulnerability, and information networking. Finally, the emerging simulation frameworks for analyzing smart grid cyberattacks were discussed, including the SG Hardware-In-the-Loop co-simulation framework (2018), GridAttackSim (2020), and GridAttackAnalyzer (2021).**

***Keywords*— Simulation Frameworks, Smart Grid, Cyberattack**

I. Introduction

The electrical grid is a network of transmission lines, substations, transformers, and other electrical and mechanical devices that transmit electricity from one power plant to the receiver (substations, utilities, consumers). The traditional electrical grid is a centralized power plant that provides electricity to receivers. According to the US Department of Energy [1], the existing electrical grid consists of about 9200 electric generating units with over 1 million megawatts of generating capacity connected to over 482803.2 kilometers of transmission lines. Faced with increasing demand, it is critical to construct and expand the electricity infrastructure, including its equipment, to maintain economic growth. This growth necessitates appropriate scheduling and monitoring of specified parameters and the network. To accomplish this, a new type of electric grid is required to accelerate the usage of digital and computerized equipment to facilitate scheduling and monitoring across the transmission line, distribution line, utilities, and consumers, hence Smart Grid (SG) technology.

The Smart Grid(SG) is an automated, widely distributed energy delivery network characterized by a two-way flow of electricity and information, capable of monitoring and responding to changes in everything from power plants to customer preferences to individual appliances [2]. In other words, controls, computers, automation, new technologies, and equipment work in tandem with the electrical grid to form the SG. The SG provides a chance to make the energy industry more reliable and efficient while contributing to economic growth. Unlike traditional grids, the SG is associated with efficient transmission of electricity, power restoration after power outages, reduced operations costs, peak demand, electricity pricing, integration of renewable energy sources, customer-owner power generation systems, and improved security. Like any other digital system, the SG suffers some vulnerabilities and complications of information which may occur both at the sending and receiving end of the power. Cyber Security is a vital component of the Smart Grid since numerous commercial and domestic devices will be connected via networks to communicate [3].

Because research on cyber security for the SG is still in its early stages, this study aims to describe the most current security frameworks developed for simulating an SG cyber attack. The remainder of this paper is structured as follows: Section 2 discusses the Smart Grid architecture and most recent cyber security threats and solutions for the Smart Grid Information security are linked to the possible vulnerability; Section 3 discusses attackers and medium of attacks; In section 4, the emerging Smart Grid cyber-attack simulating frameworks were described and Lastly, conclusions with the future works are presented in section 5.

II. Related Works

This section discusses the Smart Grid architecture and most recent cyber security threats and solutions for the Smart Grid Information security are linked to the possible vulnerability of Smart Grid technology and its information networking.

A. The Smart Grid architecture

The primary SG architecture, as shown in Fig.1, consists of secured communication interfaced and electrically interfaced primary systems (Bulk Generation Station, Transmission Station, Distribution Station, Customer) and other power players (Utilities, Markets, Operators) interfaced with only a secured communication from the primary systems.

978-1-6654-6297-6/22/$31.00 ©2022 IEEE

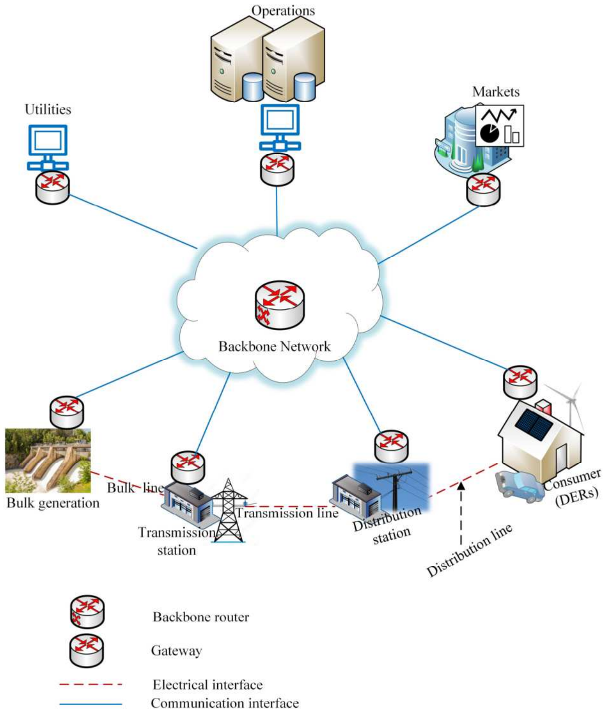

Fig. 1. The typical SG architecture

The bulk generation station houses the generating equipment such as turbines, generators, and other peripherals.

The generated power is transmitted via the bulk line to the transmission station and then to the distribution station to serve consumers. The Market involves investment and deployment of SG infrastructure. The operators ensure that as much as power generated, transmitted, and distributed is delivered to the Utilities with minimal losses [4]. The Utilities supervise the distribution and are the power service providers to the consumers, including billing. Since the main distributed energy technologies in demand response aim to optimize electricity consumption rather than generation, the consumer and distributed energy resources (DERs) side has been the most recent focus [5]. The IEC 61850 standards provide the path for deploying several digital technologies relating to the SG [6]. They deal with concerns such as integrating renewable energies and distributed energy resources (DERs) into the electrical grid.

Modern energy systems rely on an ever-expanding set of sophisticated controls and information exchanges coordinated across many operational and economic systems [7]. For this reason, the National Institute of Standards and Technology (NIST), a major SG industry player, recently drafted a framework and roadmap for SG interoperability standards [8]. Industrial, business and academic researchers are still investigating the area of SGs. [9] discussed the conceptual framework for the business model for SGs. Their concept investigated how the SG's technological aggregation may be linked with new business models based on related firms' commitment to operation and maintenance. An SG monitoring model was proposed by [10] to facilitate network management, data management, and application integration. [11] and [12] suggested a protocol for data transfer and meter data gathering in SGs using advanced metering architecture (AMI). [13] explored the capacity of a wireless backhaul for the distribution level of the smart grid. Their work sought to address the difficulty faced by bidirectional communication between the smart energy meter of customers and the Utility control center during the demand response.

B. *Smart Grid Security*

Because of the heterogeneous communication architecture of SGs, designing complex and strong security measures that can be quickly implemented to safeguard communications among different levels of the smart grid infrastructure is quite a problem [14]. However, research is rigorously being conducted to ensure SGs communication is secured from the vulnerabilities proposed by [15]-[16]. Some of these vulnerabilities are:

- Physical security: The SG network has several components, most of which are outside the Utility's facilities. This heightens the threat to numerous unsecured physical locations and renders them vulnerable to physical intrusion.

- The lifetime of power systems: Because power systems exist with relatively short-lived communication components, it is unavoidable that outdated equipment is still in use. Weak equipment might be exploited as a point of entry for security breaches

- Greater number of intelligent devices: The SG has several intelligent devices involved in managing electricity supply and demand. Attackers may use these devices as entry points, thereby causing data manipulation.

- Customer security: The advent of the AMI paved the way for smart meters to gather huge amounts of data and transfer it to the utility company and the consumers on their own. This data contains private consumer information that may be used to determine consumer activities, devices utilized, and periods spent at home.

- Internet Protocols (IP) and commercial hardware and software: Using IP standards in SGs significantly benefits since it allows for greater compatibility of the various communication components. IP-enabled devices are intrinsically vulnerable to IP-based network attacks such as teardrop, DoS, and IP spoofing.

Various works of literature have been explored on SG security. The SG security challenges, solutions, and cyber security requirements were carried out in [17]-[18]. [19] Discussed cyberattack incidents in the SG environment for critical power systems while [20] analyzed threats and their countermeasures on SG cyber security. An extensive literature review research was carried out by [21] on five categories of potential threats to SG security: process control security, smart meter security, power system state estimation security, SG communication protocol security, and SG simulation for security analysis.

III. Attackers and medium of attacks

Vulnerabilities may be exploited in various ways by attackers with varying motivations and competence, causing varying degrees of harm to the network, devices, and components.

A. *Advanced Metering Infrastructure(AMI) Attacks*

The vulnerability to AMI extends beyond the cheating consumers and vociferous persons to other organizations or nations with a vested interest. The current focus on security among utilities deploying AMI is on the well-known problem of consumers' power theft. Electricity theft is the energy consumed by a customer unaccounted for or not measured by the energy meter. Electricity theft happens due to meter tampering, meter bypassing, and service lines tapping into the customers' premises. Due to the deficiencies in the metering system and the lack of transparency and accountability in billing customers for electricity in public utilities, customers take advantage to steal electricity to avoid paying the realistic tariff. Reports cited in [22] suggest that 25 percent of Ghana's current annual average losses are due to power theft. These attacks on the smart meters include accessing configurations and modification through cyber means, as described in [23]. Other attacks on the smart meter are in the form of insider persons within the Utilities and nation or terrorist threats [24].

B. *Decryption Attacks*

This attack discovers the network's encryption key, connects to it, and accesses data. This may be accomplished by gaining access to the network's physical frames, stealing them, and storing them decrypted using tried and tested algorithms. Some decryption attackers introduce malicious data, cracks passwords, or introduce worms, replay attacks, and change messages sent or received from the SG [25] - [26], leading to a trust gap between the working entities and severe damage. In a transmission supervisory control and data acquisition (T-SCADA) [27] and distribution, supervisory control and data acquisition (D-SCADA) [28], the input and output values of line parameters such as voltages, frequencies, transformer settings, and loads can be compromised by decryption attacks.

IV. Emerging Smart Grid Cyber Attack Simulating Frameworks

The expanding penetration of monitoring and control capabilities for security breaches study in cyber attack simulation of the Smart Grid has become relevant due to the complexity of the power infrastructure and the more sophisticated nature and speed of malicious attacks. This section explores the emerging SG attack simulating frameworks.

A. *Smart Grid Hardware-In-the-Loop co-simulation framework*

[25] introduced the SG Hardware-in-the-Loop (HIL) co-simulation framework in 2018. It can simulate SG actions and reactions to targeting its power and communication components. The testbed is equipped with a real-time power grid simulator and an OpenStack-based communication network. The testbed includes a real-time power grid model and an OpenStack-based communication network. The utilized communication network emulates multitudes of attacks targeting the power system and evaluates the grid response to those attacks. It consists of the OPAL-RT technologies [26] power grid simulator responsible for interfacing control systems ranging from relays to complex AC-DC converter controllers, phasor measurement units (PMUs) that receive analog outputs and sample the measurements as a stand-alone physical unit or a functional unit within another physical unit in standards [27]. The communication network emulation and control center uses the OpenStack environment and applications that monitor the state of the grid and take decisions based on the algorithms, respectively. The attack scenarios simulated in this work are Denial of Service, Relay Attack, and Traffic Manipulation attacks.

B. *GridAttackSim: A cyber Attack Simulation Framework for Smart Grids*

The GridAttackSim, published in the electronics journal, was proposed in 2020 by Tan Duy Le based on the combination of simulation environments [28]; GridLAB-D [29], ns-3 [30], and FNCS [31] using the IEEE 13 node feeder [32]. As shown in Fig.2, the GridAttackSim is built on six components: the pre-proposing module, the attack pattern library, GridLAB-D, ns-3, the FNCS broker, and the model manager.

1) *Preprocessing Module*

The processing module preprocesses files such as the raw GridLab-D into the main GridLab-D and FNCS communication configuration in the form of .txt and ZeroMQ Property Language (zpl) to enable communication between and FNCS broker. It also configures the simulator to subscribe to the interesting issues in the form of market ID, submit bid state, market-clearing price, average price, and standard deviation of price.

2) *Attack Pattern Library*

The GridAttackSim provides for the injection of cyberattacks and evaluates their impact in a simulated environment. These attacks are created using the attack pattern library.

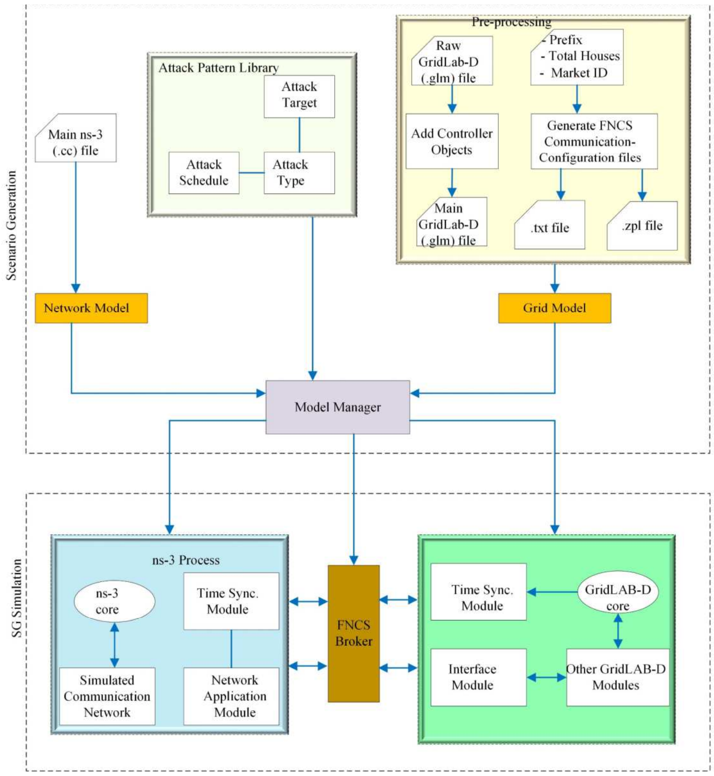

Fig.1.The SG cyberattack co-simulation framework based on the GridAttackSim Architecture

It is responsible for simulating cyberattacks on the SG system and allows the development of many sorts of attack behavior. It also provides settings for selecting attack characteristics such as attack target components, attack type, and simulation start and finish times. That is, the attack pattern library addresses the questions "what question" -what kind of attack, "where the question"-where the vulnerability parts are, "when question" – when the attack happens.

3) GidLAB-D

The GidLAB-D [29] is an open-source time-series simulation framework that can simulate all components of a power grid system in modern power distribution simulation systems, from the substation to end-user loads. The GridLAB core, time sync module, interface module, and others comprise the GidLAB-D. The combination consistently integrates advanced simulation tools and high-performance optimization strategies coupled with equipment, devices, and user models and is compatible with distributed energy resources (DERs) and storage models to enable complicated applications. It has external links with Microsoft Excel, Matlab, Microsoft Access, MySQL, and other text-based tools.

4) ns-3

The ns-3 comprises the ns-3 core, time sync nodule, simulated communicated network, and a network application module. Although it was designed using the C++ language, it supports python scripting and allows enhanced scalability and improved software integration with the support of the Python Language.

5) FNCS Broker

The FNCS broker is a framework for network co-simulation and supports integrating distribution and transmission simulators (GridLAB-D) and communication simulators (ns-3). This resource allows for the modeling and construction of more effective SG hardware and other tools, improving grid efficiency and performance [33].

6) Model Manager

The model manager is the core component of the SG cyberattack simulation system; it handles the simulation scenario composition, supervises simulation execution, and initializes both simulators. Its interface allows the selection of assaults from the attack pattern library and the selection and modification of power and network models.

C. GridAttackAnalyzer: Smart Grid Attack Analysis Framework

The GridAttackAnalyzer, developed by Cyber range Organization and Design (CROND) at the Japan Advanced Institute of Science and Technology [34], is the latest SG attack analysis tool for determining attack pathways and calculating different security metrics for a given SG architecture and cyberattack scenario. It is an upgraded version of GridAttackSim that can be extended by end-users and has three SG models, over 20 different types of SG devices, and 40 different sorts of vulnerabilities. Fig.3 depicts the GridAttackAnalyzer architecture, which includes the following components:

1) SG Model

The SG model defines the network and power grid models.

2) Attack Scenarios

Attack Scenarios define the attack scenario entry points, targets, and vulnerabilities.

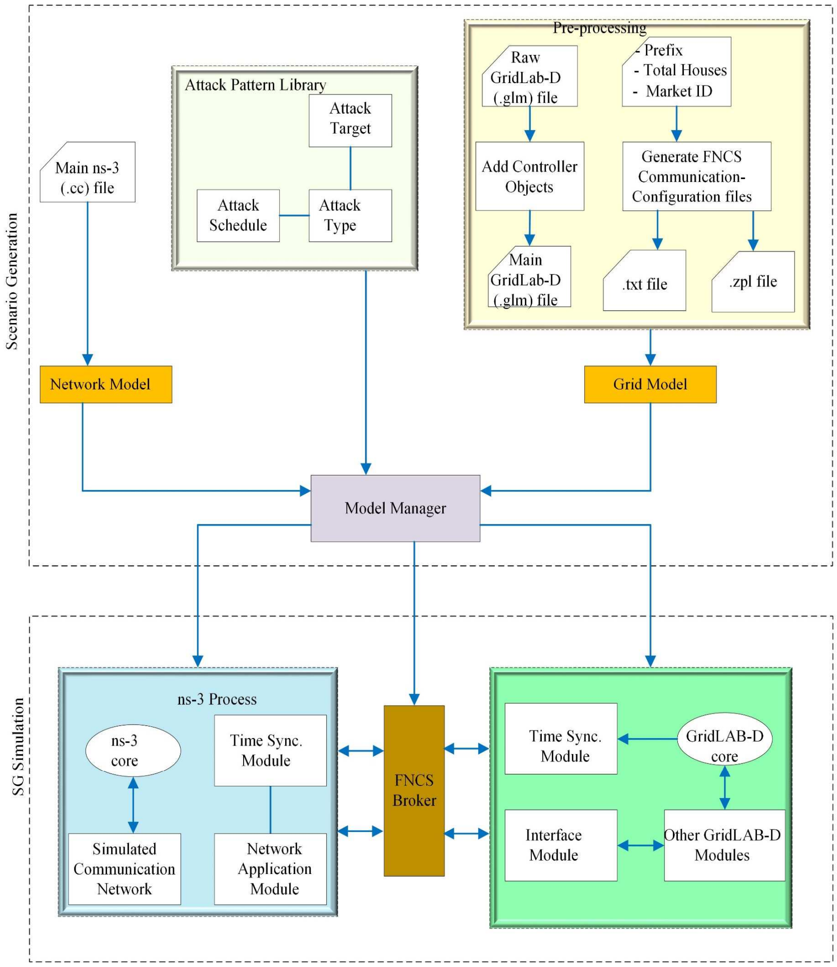

Fig. 3. GridAttackAnalyzer architecture

3) Database/ Database Manager

Database Manager accesses and maintains data on different sorts of attacks and network vulnerabilities. This interface interacts with end-users to supply the attack analysis manager with the appropriate information from the database.

4) Attack Analysis Manager

The Attack Analysis Manager is the core module that manages the entire attack analysis process.

5) Attack Model Generator

The Attack Model Generator generates an attack model based on the input parameters provided by the analysis manager.

6) Attack Module Evaluator

The Attack Module Evaluator generates the attack graph and computes the security metrics for a specific scenario.

The GridAttackAnalyzer, based on our research, is one of the pioneering frameworks for SG attack analysis. In terms of SG application and security metrics calculation, GridAttackAnalyzer is more extensive than the recent frameworks proposed during the past two years, based on the most popularly used SG metrics such as attack cost, and attack risk, attack success probability, and attack impact, and the attack types covered as shown in Table I.

V. Conclusion

This article thoroughly investigates the Smart Grid design and the potential vulnerabilities to the power grid and the communication network. We reviewed the existing literature on the topic and discussed the emerging frameworks for analyzing SG attacks. The emerging frameworks assessed are the SG Hardware-In-the-Loop co-simulation framework (2018), GridAttackSim (2020), and GridAttackAnalyzer (2021). We noticed in our review that while the SG Hardware-In-the-Loop co-simulation framework solves some vulnerability problems, GridAttackSim and GridAttackAnalyzer seem to make room for solving more SG vulnerabilities. GridAttackAnalyzer has over 20 SG devices and creates a platform for analyzing over 40 different types of vulnerabilities. We hope to validate our work in the next research by applying the simulation frameworks to tailored-made vulnerable devices.

Acknowledgment

This work has received funding from the Key Laboratory Foundation of National Defence Technology under Grant 61424010208, Natural Science Foundation of China (No. 41911530242 and 41975142), 5150 Spring Specialists (05492018012 and 05762018039), Major Program of the National Social Science Fund of China (Grant No. 17ZDA092), Royal Society of Edinburgh, UK and China Natural Science Foundation Council (RSE Reference: 62967 and Liu 2018_2) under their Joint International Projects funding scheme and basic Research Programs (Natural Science Foundation) of Jiangsu Province, China (BK20191398 and BK20180794).

REFERENCES

[1] US Department of Energy, “The Smart Grid:An introduction,” 2011. doi: 10.1002/9781119958352.ch15.

[2] B. Kroposki, “Smart Grid Overview,” 2015. doi: 10.1201/b18005-2.

[3] L. A. Maglaras et al., “Cyber security of critical infrastructures,” ICT Express, vol. 4, no. 1, pp. 42–45, 2018, doi: 10.1016/j.icte.2018.02.001.

[4] S. M. Amin, “Smart grid: Overview, issues and opportunities. Advances and challenges in sensing, modeling, simulation, optimization and control,” Eur. J. Control, vol. 17, no. 5–6, pp. 547–567, 2011, doi: 10.3166/EJC.17.547-567.

[5] IRENA (2019), “Innovation landscape brief: Market integration of distributed energy resources,” in International Renewable Energy Agency, 2020, pp. 345–372, doi: 10.1049/pbpo167e_ch14.

[6] C. Brunner, “IEC 61850 Profile for Distributed Energy Resources Supporting IEEE 1547,” 2022.

[7] US Department of Energy, “The National Opportunity for Interoperability and its Benefits for a Reliable, Robust, and Future Grid Realized Through Buildings,” 2016. doi: 10.1525/curh.2016.115.780.160.

[8] A. Gopstein, C. Nguyen, C. O’Fallon, N. Hastings, and D. Wollman, “DRAFT NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0,” 2020.

[9] I. A. Sajjad, R. Napoli, G. Chicco, and L. Martirano, “A conceptual framework for the business model of smart grids,” in EEEIC 2016 - International Conference on Environment and Electrical Engineering, 2016, pp. 1–5, doi: 10.1109/EEEIC.2016.7555684.

[10] A. Singhal and R. P. Saxena, “Software models for smart grid,” in 2012 1st International Workshop on Software Engineering Challenges for the Smart Grid, SE-SmartGrids 2012 - Proceedings, 2012, pp. 42–45, doi: 10.1109/SE4SG.2012.6225717.

[11] I. Parvez, M. Jamei, A. Sundararajan, and A. I. Sarwat, “RSS based loop-free compass routing protocol for data communication in advanced metering infrastructure (AMI) of Smart Grid,” IEEE Symp. Comput. Intell. Appl. Smart Grid, CIASG, vol. 2015-Janua, no. January, 2015, doi: 10.1109/CIASG.2014.7011570.

[12] B. Karimi, V. Namboodiri, and M. Jadliwala, “Scalable Meter Data Collection in Smart Grids Through Message Concatenation,” IEEE Trans. Smart Grid, vol. 6, no. 4, pp. 1697–1706, 2015, doi: 10.1109/TSG.2015.2426020.

[13] B. Karimi and V. Namboodiri, “On the capacity of a wireless backhaul for the distribution level of the smart grid,” IEEE Syst. J., vol. 8, no. 2, pp. 521–532, 2014, doi: 10.1109/JSYST.2013.2260701.

[14] [14] A. Zaballos, A. Vallejo, and J. M. Selga, “Heterogeneous communication architecture for the smart grid,” IEEE Netw., vol. 25, no. 5, pp. 30–37, 2011, doi: 10.1109/MNET.2011.6033033.

[15] I. L. G. Pearson, “Smart grid cyber security for Europe,” Energy Policy, vol. 39, no. 9, pp. 5211–5218, 2011, doi: 10.1016/j.enpol.2011.05.043.

[16] S. S. Wu, C. C. Liu, A. F. Shosha, and P. Gladyshev, Cyber security and information protection in a smart grid environment, vol. 44, no. 1 PART 1. IFAC, 2011.

[17] W. Wang and Z. Lu, “Cyber security in the Smart Grid: Survey and challenges,” Comput. Networks, vol. 57, no. 5, pp. 1344–1371, 2013, doi: 10.1016/j.comnet.2012.12.017.

[18] E. Pallotti and F. Mangiatordi, “Smart grid cyber security requirements,” in 2011 10th International Conference on Environment and Electrical Engineering, EEEIC.EU 2011 - Conference Proceedings, 2011, no. July 2015, pp. 1–4, doi: 10.1109/EEEIC.2011.5874822.

[19] A. Anwar and A. Mahmood, “Cyber security of smart grid infrastructure,” in The State of the Art in Intrusion Prevention and Detection, CRC Press, Taylor and Francis Group, 2014, no. January, pp. 449-472., doi: 10.1201/b16390-9.

[20] Carlos Lopez, Arman Sargolzaei, Hugo Santana, and Carlos Huerta, “Smart Grid Cyber Security: An Overview of Threats and Countermeasures,” J. Energy Power Eng., vol. 9, no. 7, pp. 632–647, 2015, doi: 10.17265/1934-8975/2015.07.005.

[21] T. Baumeister, “Literature Review on Smart Grid Cyber Security,” 2010.

[22] O. Famous Darteh, C. Oseiwah Adjei, R. Anaadumba, S. Sarker, G. TFJ Christian, and A. Samuel Blay, “Design of Internet of Things based Electricity Theft Detection using Raspberry PI,” Int. J. Eng. Res. Technol., vol. 10, no. 02, pp. 1–6, 2021, [Online]. Available: www.ijert.org.

[23] R. P. Díaz Redondo, A. Fernández-Vilas, and G. F. Dos Reis, “Security aspects in smart meters: Analysis and prevention,” Sensors (Switzerland), vol. 20, no. 14, pp. 1–19, 2020, doi: 10.3390/s20143977.

[24] K. Ardis, “BATTLING THREATS IN THE SMART GRID,” 2014.

[25] F. Diao, F. Zhang, and X. Cheng, “A privacy-preserving smart metering scheme using linkable anonymous credential,” IEEE Trans. Smart Grid, vol. 6, no. 1, pp. 461–467, 2015, doi: 10.1109/TSG.2014.2358225.

[26] W. A. I. U. D. A. A. B.-S. Kim, “A Novel Privacy Preserving Scheme for Smart Grid-Based Home Area Networks,” sensors, vol. 22, no. 2269, pp. 1–26, 2022, doi: https:// doi.org/10.3390/s22062269.

[27] E. D. Knapp and R. Samani, Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure, 1st Editio. Newnes: Elsevier Inc., 2013.

[28] D. Wang, X. Guan, T. Liu, Y. Gu, Y. Sun, and Y. Liu, “A survey on bad data injection attack in smart grid,” Asia-Pacific Power Energy Eng. Conf. APPEEC, 2013, doi: 10.1109/APPEEC.2013.6837157.

[29] A. Albarakati, B. Moussa, M. Debbabi, A. Youssef, B. L. Agba, and M. Kassouf, “OpenStack-Based Evaluation Framework for Smart Grid Cyber Security,” in 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2018, 2018, pp. 1–6, doi: 10.1109/SmartGridComm.2018.8587420.

[30] Opal-RT, “Real Time Digital Simulation Facility,” Power System Lab, Department of EE, IIT Kanpur - Webmaster. https://iitk.ac.in/rtds/opalrt.php (accessed May 28, 2022).

[31] IEEE, “IEEE Draft Standard for Synchrophasor Measurements for Power Systems for Power Systems.,” in IEEE PC37.118.1/D4.2, 2011, pp. 1–56.

[32] T. D. Le, A. Anwar, S. W. Loke, R. Beuran, and Y. Tan, “Grid attacksim: A cyber attack simulation framework for smart grids,” Electron., vol. 9, no. 8, pp. 1–21, 2020, doi: 10.3390/electronics9081218.

[33] D. P. Chassin, K. Schneider, and C. Gerkensmeyer, “GridLAB-D: An open-source power systems modeling and simulation environment,” in Transmission and Distribution Exposition Conference: 2008 IEEE PES Powering Toward the Future, PIMS 2008, 2008, pp. 1–5, doi: 10.1109/TDC.2008.4517260.

[34] G. F. Riley and T. R. Henderson, “The ns-3 network simulator,” in Modeling and Tools for Network Simulation, 2010, pp. 15–34, doi: 10.1007/978-3-642-12331-3_2.

[35] S. Ciraci, J. Daily, J. Fuller, A. Fisher, L. Marinovici, and K. Agarwal, “FNCS: A framework for power system and communication networks co-simulation,” Simul. Ser., vol. 46, no. 4, pp. 256–263, 2014.

[36] W. H. Kersting and G. Shirek, “Short circuit analysis of IEEE test feeders,” in Proceedings of the IEEE Power Engineering Society Transmission and Distribution Conference, 2012, no. 1, pp. 1–9, doi: 10.1109/TDC.2012.6281539.

[37] J. Daily, “ Project 2.5 - Framework for Network Co-Simulation (FNCS),” Control of Complex Systems Initiative, Sep. 2018. https://controls.pnnl.gov/research/project_2_5.stm (accessed May 29, 2022).

[38] Cyber range Organization and Design (CROND), “GridAttackAnalyzer: Smart Grid Attack Analysis Framework,” Cyber range Organization and Design (CROND), 2021. https://github.com/crond-jaist/GridAttackAnalyzer (accessed May 29, 2022).

[39] T. Eom, J. B. Hong, S. An, J. S. Park, and D. S. Kim, “A Framework for Real-Time Intrusion Response in Software Defined Networking Using Precomputed Graphical Security Models,” Secur. Commun. Networks, vol. 2020, 2020, doi: 10.1155/2020/7235043.

[40] [2] N. K. Singh, P. K. Gupta, V. Mahajan, A. K. Yadav, and S. Mudgal, Monitoring Cyber-Physical Layer of Smart Grid Using Graph Theory Approach, vol. 710. Springer Singapore, 2021. doi: 10.1007/978-981-15-8815-0_46.

TABLE I. EVALUATION METRICS AND FUNCTIONALITIES OF THE FRAMEWORKS (√ =APPLICABLE, ×=NOT APPLICABLE)

Framework	**Functionalities**						
	Attack Graph Generation	***Attack Graph Visualization***	***Attack Succes Probability***	***Attack Cost***	***Attack Impact***	***Attack Risk***	***Attack Type Covered***
GridAttackAnalyzer [34]	√	√	√	√	√	√	1. Channel Jamming (Distributed denial of service) 2. Malicious Code (Exploit kits, VirusWorms, Trojans, Malware) 3. Injection Attacks (Malicious code injection, Malformed data injection) 4. Replay of messages 5. Attack with local terminals for substations as entry points 6. SCADA systems
GridAttackSim [28]	√	√	×	√	√	√	1. Channel Jamming (Distributed denial of service) 2. Malicious Code (Exploit kits, VirusWorms, Trojans, Malware) 3. Injection Attacks (Malicious code injection, Malformed data injection) 4. Replay of messages
Ref [25]	×	×	×	√	√	√	Power systems validation
Ref [39]	√	×	√	√	√	√	1. Channel Jamming (Distributed denial of service) 2. Malicious Code (Exploit kits, VirusWorms, Trojans, Malware) 3. Injection Attacks (Malicious code injection, Malformed data injection)
Ref [40]	√	×	×	×	×	×	1. Channel Jamming (Physical layer and cyber layer)