Doctoral Dissertation

Smart Grid Cybersecurity Experimentation: Architecture and Methodology

LE Duy Tan

Supervisor: Razvan BEURAN

Graduate School of Advanced Science and Technology
Japan Advanced Institute of Science and Technology
[Information Science]
March, 2021

Abstract

The smart grid is a vital part of the Japanese initiative named “Society 5.0”. It is also one of the core technologies enabling sustainable economic and social developments. This next-generation electrical power system integrates the traditional electrical grid and computer technology to enhance the automation, connectivity, and communication of the different power network components. In recent years, various attacks have been made on the smart grid system, which lead to serious harmful consequences.

The smart grid structure is complex and includes two essential parts: network communication and the power grid. Researchers need to consider the relationship between these components for further system investigation and improvement. Moreover, it is not a trivial activity to implement a real smart grid system for the cybersecurity experiment and validation process, since it entails high risk of destroying the electrical infrastructure and equipment, resulting in enormous economic consequences and even in danger regarding human lives. As a result, in this critical domain where testing on a real system is so hazardous, simulation and analysis techniques can be considered as an effective solution to make smart grid cybersecurity experimentation possible.

The attack simulation and analysis tools are mainly applied to simulate attacks and emulate the actual circumstances in which these attacks occur, particularly system settings and network topologies. The application of real incident simulation tools to cybersecurity experimentation is a primary factor for enhancing the efficacy of the experimentation process. Due to its pioneering characteristics, not many research studies currently exist on practical cybersecurity experimentation for the smart grid. To the best of our knowledge, this is one of the first research works that thoroughly addresses this important issue.

This dissertation identifies the need for realistic cybersecurity experimentation for the smart grid and formulates the corresponding system design requirements. A general architecture for smart grid cybersecurity experimentation, which fulfills these specifications, is also introduced. To deal with the great system complexity but still achieve our goal, we divided smart grid cybersecurity experimentation into two parts: the co-simulation approach and the analytical modeling approach. The specifications, general architectures and methodologies of both are determined and detailed herein.

In the co-simulation approach, we introduced and implemented GridAttackSim. This novel co-simulation framework enables the simulation of smart grid infrastructure characteristics, allows various cybersecurity attacks to be simulated, and evaluates their consequences. A case study was performed with two different test feeders to validate the functionality of GridAttackSim.

In the analytical modeling approach, we first provided a literature review on the current state-of-the-art for smart grid attack analysis. The most promising directions were then applied to design and implement GridAttackAnalyzer (Cyber Attack Analysis Framework for Smart Grids). A case study with various attack scenarios was conducted to validate this framework.

This dissertation's main contribution is a methodology that can effectively support realistic cybersecurity experimentation for the smart grid. This methodology was implemented in the form of the two frameworks mentioned above, GridAttackSim and GridAttackAnalyzer. Using these frameworks, researchers can determine the consequences of various attack types, thus making possible the early development and evaluation of new anomaly detection methods and mitigation even before their actual implementation. Moreover, the frameworks can also be used to define effective approaches for the implementation of smart grid technology, for instance, to determine efficient communication requirements for device operation.

In addition, the systems can be used for cybersecurity training of IT experts and cybersecurity professionals. For example, based on evaluating various security metrics, IT experts and cybersecurity professionals can discover all the possible attack paths, and determine which vulnerable devices on those paths should be protected in advance to prevent the most significant damage. It also becomes possible to compare the effectiveness of specific device-level strategies deployed for different devices. For the network level, the performance of various defense strategies for smart grid systems can be assessed. Furthermore, our work can help system planners to estimate the attack damage cost on a smart grid system.

Keywords: smart grid, cybersecurity experimentation, simulation, co-simulation, attack analysis.

Acknowledgment

Along the way on this journey, I have received a great deal of support and assistance.

First, I would like to acknowledge my supervisor, Research Associate Professor Razvan Beuran. Thank you for accepting me to your laboratory. If your answer had been “No” when I made by request three years ago, I would not have achieved this goal. I appreciate all of the words of your advice and encouragement. Thank you for your patient support and the opportunities I was given to further my academic career.

I would also like to thank Professor Yasuo Tan, Professor Yoichi Shinoda, Associate Professor Yuto Lim, and Professor Seng W. Loke. As the members of my dissertation committee, their suggestions brought in threads of thought that made my research much richer and my dissertation something I can be proud of having written.

I also want to express my sincere thanks to my colleagues from my internship at Deakin University, Australia, especially Dr. Mengmeng and Dr. Adnan, for their extraordinary collaboration. Thanks to Dr. Tuan Nguyen for his continuous support and for introducing me to this internship opportunity. Thanks to Matsumoto from the International Student Section of JAIST for her invaluable assistance. Again, I would like to single out my internship supervisor at Deakin University, Professor Seng W. Loke. Your insightful feedback pushed me to sharpen my thinking and brought my research to a higher level.

I would also like to thank NIFA teachers, Sushiro Komatsu, and Roast Beef Hoshi Komatsu, especially Takebe-sensei and Yoshida-san, for their great support. Thank you for teaching me Japanese and taking care of me when I was in Japan. My life there would be boring without you guys.

In addition, I want to express special thanks to my soulmates, Lac Si Le, Quynh Dao, and Thanh Quynh, for their support and understanding that helped me through the dark times. Without you, I never would have made it. Completing this dissertation would have been more difficult without the support and friendship I received from the other lecturers, friends at JAIST, and friends in Melbourne, especially Tuyen Nguyen, Thuy Nguyen, Giang Trinh's family, Tuan-Thao's family, etc.

Finally, I would like to thank my family for their endless support. All of you have sacrificed a great deal so that I can accomplish this personal goal. We can all be proud of it; you earned this degree right along with me.

List of Figures

List of Tables

Contents

Abbreviation

AG	Attack Graph
AMI	Advanced Metering Infrastructure
APTs	Advanced Persistent Threats
ASTORIA	Attack Simulation Toolset for Smart Grid Infrastructures
AT	Attack Tree
BAG	Bayesian Attack Graph
BAGS	Bayesian Attack Graph for Smart Grid
CPP	Critical Peak Price
CPS	Cyber-Physical System
CSMA	Carrier Sense Multiple Access
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSV	Comma-Separated Values
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Score System
DASs	Distribution Automation Systems
DDoS	Distributed Denial of Service
DoS	Denial of Service
DP	Dynamic Pricing
DR	Demand Response
EMS	Energy Management System
ENISA	European Union Agency for Cybersecurity
EPOCHS	Electric Power and Communication Synchronizing Simulator
FEP	Front End Processor

FNCS	Framework for Network Co-Simulation
GrSM	Graphical Security Model
GUI	Graphical User Interface
HAN	Home Area Network
HARM	Hierarchical Attack Representation Model
HPC	High-Performance Computing
HVAC	Heating, Air Conditioning
IoT	Internet of Things
MOOP	Multiobjective Optimization Problem
NAN	Neighbor Area Network
NIST	National Institute of Standards and Technology
NSRDB	National Solar Radiation Database
NVD	National Vulnerability Database
PMU	Phasor Measurement Units
PNNL	Pacific Northwest National Laboratory
RG	Reachability Graph
RTP	Real-Time Price
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SINR	Signal-to-Inference-Plus-Noise Ratio
SUS	System Usability Scale
T-HARM	Temporal-Hierarchical Attack Representation Model
TASSCS	Testbed for Analyzing Security of SCADA Control Systems
TCP	Transmission Control Protocol
TOU	Time-of-Use

UDP	User Datagram Protocol
WAMPAC	Wide-Area Monitoring, Protection, and Control
WAN	Wide Area Network
ZPL	ZeroMQ Property Language

Chapter 1

Introduction

1.1 Overview

Conventional electrical grids are defined as central power stations that generate and supply electricity to the consumers. Traditionally, electricity was distributed without much energy consumption management and monitoring. Currently, both developed and developing nations want to construct vast electricity infrastructures to ensure economic development. Thanks to developments in technology, the management process of loads and equipment has been improved. These loads and devices are programmed to track particular parameters or to run according to schedules. A new and smart power system is currently being facilitated by the integration of information technologies and communications into the conventional electricity grids. This trendy power grid system is known as the smart grid—a term that incorporates information technology, two-way communication, and security application to electrical grids. Interestingly, there are a variety of ways in which the definition of a smart grid can be clarified. However, the most commonly acknowledged is the interoperability of electricity, information technology, and communication, to improve the electrical power system serving loads and ensure end-use applications development.

In 2016, the Japanese Cabinet launched its "Society 5.0" initiative [5] to design new strategies for economic and social development. This program envisions a future super-intelligent society that will benefit humanity with a better quality of life and a shift in social norms. The smart grid is described as one of the keys supporting Society 5.0. Furthermore, the

U.S. Department of Homeland Security (DHS) [6] defined the smart grid as a “special” critical infrastructure supporting necessary services to sustain society and ensure economic development since it is essential to many of the 18 critical infrastructures.

A recent report conducted by the Center for Strategic and International Studies (CSIS) surveyed Information Technology (IT) decision-makers in eight countries. The study indicated that 82% of organizations addressed a lack of cybersecurity abilities, and 71% agreed that this skill shortage results in direct and determinable consequences to their institutions [7]. As of January 2019, the USA faced a shortage of nearly 314,000 cybersecurity professionals among 716,000 current total employed cybersecurity professionals, according to the National Initiative for Cybersecurity Education (NICE) [8]. Organizations are still facing significant difficulties in the recruitment of cybersecurity experts. Data obtained from recruitment websites showed that there had been an increase in the number of unfilled cybersecurity positions by over 50% since 2015 [9]. Therefore, there is an urgent need for highly-skilled technical cybersecurity staff.

1.2 Motivation

Cybersecurity has become a major challenge for smart grid systems. In 2014, almost one-third of the cybersecurity incidents reported by the U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) was targeted the energy sector [10].

In 2007, an attack on Iran’s nuclear power plant slowed down the country’s critical nuclear power development [11]. This attack was conducted using Stuxnet, a powerful and organized virus designed to penetrate the programmable industrial system. A substantial part of the uranium enrichment cycle activity could also be slowed down and completely blocked.

By 2014, more than 1000 energy firms [12] had been targeted by a professional hacker team called Dragonfly. The group had successfully broken into the core systems that control energy companies in North America and Europe. Dragonfly gained access to these systems mainly through malware in emails, websites, and third-party programs. The attackers' intention was cyber espionage, but the intrusion was fortunately detected before it could interrupt or damage electricity supplies in the affected areas.

On 25 December 2015, during the Ukrainian civil war in Donbass, 80,000 civilians were forced into the dark [13] due to a cyber attack targeting an electrical power station in Ivano-Frankivsk. This assault was triggered by the use of a BlackEnergy Trojan horse and spear-phishing. Created by a hostile actor, BlackEnergy can destroy hard drives, remove data, and control infected computers. Furthermore, after attacking the companies, a concerted denial of service attack was carried out on the telephone numbers of the firm operating the power station. Correspondingly, it was impossible for users to either get help or notify the companies of the collapse.

The DHS reported that 2017 saw a considerable increase in the number of cyberattacks, further expanding in 2018, ranging from more than 4,300 French network cyberattacks to intrusion into the US electricity companies.

These security incidents prove that cyberattacks can happen and that actual, tangible consequences exist in the real world. This sparked a period of intense cyberattacks that spread through isolated viruses and radical hacker groups. These attacks on smart grid networks can be conducted by governments and coordinated groups, and can lead to blackouts and even infrastructure destruction.

In [14], various studies on the competence profiles of cybersecurity experts are analyzed. The researchers concluded that success at individual and team levels could only be achieved by a proper combination of technical knowledge and soft skills. Utilizing attack simulation tools is considered as a solution to reach the goal. The tools are mainly applied to simulate attacks and emulate the actual circumstances in which these attacks take place, particularly system settings and network topologies. The application of the real incidents simulation tools for cybersecurity training is believed to be the primary factor in enhancing the efficacy of the training process [15].

Co-simulation refers to the simultaneous execution of two or more simulation models, depending on the interfaces and required runtime. In addition, the smart grid is a complex power grid and network interconnected system.

Co-simulation technology is, therefore, proposed as a potential approach to overcome these complexities. Although there has been a rapid increase in consideration of the benefits of smart grid vulnerability assessment, to our best knowledge, research has been limited and not thoroughly investigated in this area. Very little effort has been put into investigating the potential damage of attacks and evaluating their impact on the system. Therefore, a new framework should be developed to support smart grid attack co-simulations fully.

In addition, several studies have proposed technologies to combine the attack tree and attack graph in multiple layers to resolve the scalability issue of the single-layered model [16,17]. Graphical Security Models (GrSM) based on the Common Vulnerability Scoring System (CVSS) are an emerging technology to analyze attacks on the smart grid system. However, there have been only a few works that focus on smart grid attack analysis using GrSM and CVSS.

1.3 Aims and Approach

The objective of this research is to develop a methodology that can effectively support realistic smart grid cybersecurity experimentation. Using the top-down model, we first determine the design requirements for this system. Then, we design the general architecture for the smart grid realistic cyber-security experimentation. Then, the requirement for each component of the general architecture is defined. Finally, the target system can be built. The research questions are:

- RQ1. What are the requirements for cybersecurity experimentation for smart grids? How can we design and implement a system that fulfills these requirements?

  We identify the need for realistic cybersecurity experimentation for smart grid and system design requirements by investigating the related research in the field. To deal with the system complication but still achieve our goal, we divide the smart grid cybersecurity experimentation into two components: the co-simulation approach and the analytical modeling approach. We figure out their specifications and general architectures.

- RQ2. Is it possible to jointly simulate the cyber network and the physical system?

  We propose a new co-simulation architecture to allow simulations of smart grid infrastructure properties and communication networks to answer this issue. A more detailed discussion is presented in Chapter 4.
- RQ3. How can we include cyber attack simulation in a smart grid environment for experimentation purposes?

  To address this question, our proposed co-simulation framework can simulate various cybersecurity attacks and evaluate their consequences. Our methodology is illustrated in Chapter 4.
- RQ4. Is it possible to develop an analytical model that analyzes the attack propagation path?

  To address this question, we propose an analytical modeling approach. First, we provide an analytical literature review of current state-of-the-art attack analysis. We aim to indicate the promising direction for smart grid attack analysis. We apply this finding to assess the security of the smart grid system. Finally, we not only highlight the advantages of the promising direction for smart grid attack analysis but also illustrate its applicability and validation by analyzing a real case with attack scenarios.

1.4 Main Contributions

The main contributions of this research are:

1. We determined the requirements that need to be fulfilled to design realistic cybersecurity experimentation for smart grids. We designed a general architecture for a realistic smart grid cybersecurity experimentation that fulfills these requirements. We divided the structure into

two approaches: co-simulation and analytical modeling.

2. We conducted a comprehensive study of the existing research on smart grid attack co-simulation and analysis.
3. We proposed GridAttackSim, the co-simulation framework that facilitates the simulation of the various customized smart grid system topologies that involve both power grid and network components. We also introduced GridAttackAnalyzer, one of the first smart grid attack analysis frameworks. Both of these frameworks are designed to enable researchers to easily create, modify the experimentation content, and facilitate their interaction with the system.
4. We conducted several case studies using various power grid test feeders, network models, and attack types to validate the proposed frameworks.

1.5 Outline

The remainder of this dissertation is organized as follows:

- Chapter 2 provides the conceptual model of the smart grid. The background of smart grid co-simulation and smart grid attack analysis are introduced. A comprehensive study of the existing research on smart grid attack co-simulation is described. Moreover, a comprehensive study of the existing research on attack analysis using GrSM and CVSS, ranging from (1) traditional networks, (2) emerging technologies, to (3) smart grid, is summarized. Finally, the security metrics calculation method is briefly described.
- Chapter 3 identifies the necessity and the requirements for realistic cybersecurity experimentation for smart grid. By using the requirements, an architecture of a realistic smart grid cybersecurity experimentation is designed. Its components, including co-simulation and analytical modeling approaches, are discussed.
- Chapter 4 discusses in detail the architecture of GridAttackSim - a Cyber Attack Simulation for Smart Grids. Its components, including preprocessing module, attack pattern library, GridLAB-D, ns-3, FNCS

broker, and model manager, are addressed. Further, chapter 4 introduces the implementation of GridAttackSim. A case study with the simple test feeder and IEEE 13 node test feeder is represented.

- Chapter 5 explains the architecture of GridAttackAnalyzer - a Cyber Attack Analysis on Smart Grids. Its components, including input, processing, and output, are addressed. Besides, the last section of this chapter mainly introduces the implementation of GridAttackAnalyzer. A case study with the PNNL test feeder and simplified network model is represented.
- Chapter 6 presents the evaluation of GridAttackSim and GridAttack-Analyzer from several perspectives.
- Chapter 7 discusses the potential applications of GridAttackSim and GridAttackAnalyzer for cybersecurity research and training.
- Finally, chapter 8 summarizes the results and outlines future research directions.

Chapter 2

Background and Related Work

2.1 Background

2.1.1 Smart Grid Conceptual Model

The smart grid conceptual model, which was introduced by the National Institute of Standards and Technology (NIST) [1], provides a descriptive overview of the development of smart grid. It presents a visualized diagram illustrating how seven smart grid domains, including Bulk Generation, Transmission and Distribution, Operations, Service Providers, Markets, and Customers, can be incorporated. Each domain and its sub-domains constitute the conceptual roles and services of the smart grid. Further, it also concentrates on application integration, cybersecurity, data management, and network connection. Figure 2.1 shows a high-level, overarching logical architecture representing several significant relationships between current applications of the seven domains. It is a practical model to define which current applications can be an appropriate candidate for a specific smart grid function as well as determine the proper communications paths between these applications. Additionally, the diagram helps to detect possible interactions between the intra-domain and inter-domain applications as well as their potential interactions. In this research, the smart grid conceptual model is used as the standard model to develop our cybersecurity experimentation framework, which aims to cover almost all of the smart grid domains.

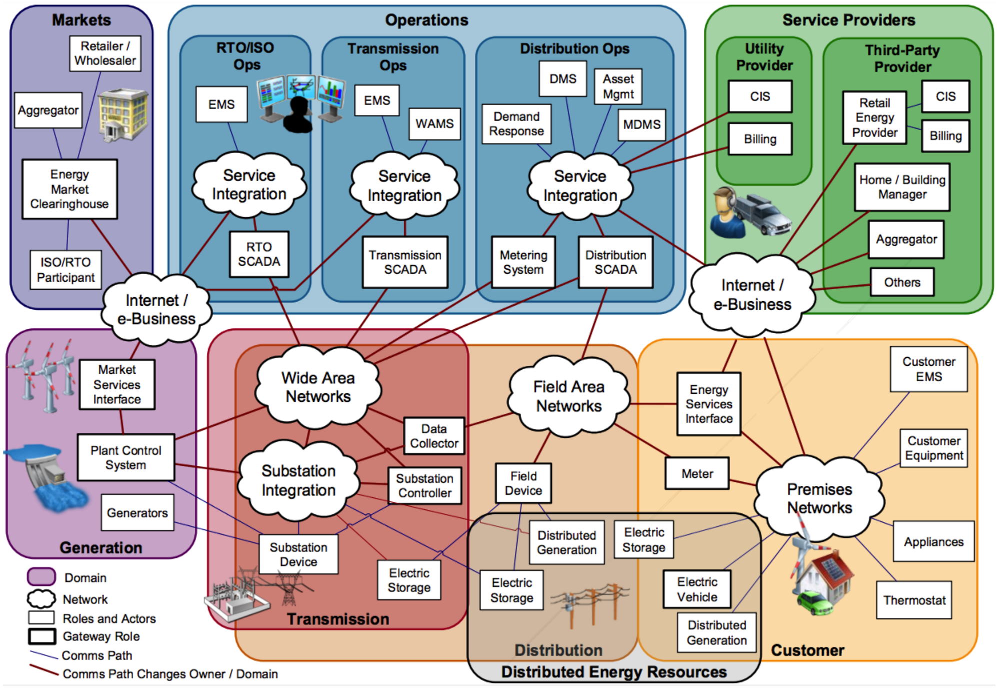


Figure 2.1: Logical model of legacy systems mapped onto conceptual domains for smart grid information networks [1].

2.1.2 Smart Grid Co-simulation

Co-simulation is defined as the incorporation of several simulation models to improve the overall efficiency and accuracy of the simulation. It is an efficient method to capture the interaction between communication and electricity grid components. Numerous systematic research efforts regarding smart grid modeling and simulation and the concept of attack patterns have been undertaken in recent years. A thorough overview of the most current simulation tools and their smart grid applications has been provided in our previous study [18]. The GridLAB-D, ns-3, and FCNS combination is suggested as a potential approach for smart grid research. Two basic case studies have been carried out using the IEEE 13 node feeder model to verify that the combination can simulate security threats in the smart grid environment. There are technical limitations on the number of attack types, smart grid models, and power grid models. Also, the result visualization function was omitted. The framework design, GUI application, and attack schedule function have not been taken into account. Consequently, the study provides a starting point for the current investigation. In other words, this research attempts to extend our previous research by addressing the limitations mentioned earlier.

2.1.3 Smart Grid Attack Analysis

Vulnerability scanners are widely understood to assess security threats by identifying the number, type, and location of the vulnerabilities within the network. Common Vulnerabilities and Exposures (CVE), maintained by MITRE Corporation, provides an up-to-date list of publicly-known vulnerabilities and exposures [19]. This CVE glossary explores the vulnerabilities and utilizes the Common Vulnerability Score System (CVSS) to assess vulnerabilities level [20]. CVSS provides a systems approach to capture critical vulnerability characteristics through quantitative scores that represent their severity. To support evaluation and prioritization of organizations' vulnerability management processes by IT experts, security analysts, and cybersecurity professionals, CVSS scores can be converted into a qualitative representation, ranging from low to medium, high, or critical. These numerical scores can also be taken as inputs to generate the Graphical Security Model (GrSM) [21].

GrSM is a significant technology to identify the security posture of networked systems and evaluate the effectiveness of security defenses. Since it provides a visualization of how a system can be hacked through attack paths, countermeasures to prevent the attacks from reaching the target can be developed. Attack Tree (AT) [22] and Attack Graph (AG) [23] are two essential components of GrSM. The structure of an AT contains a root node as the attack goal and leaf nodes to represent different ways of achieving that goal. Each node represents a sub-target, and children of the node form the paths to accomplish this sub-target. There are two types of nodes, namely, AND nodes and OR nodes. Once an AT is built, CVSS values can be assigned to the leaf nodes; then, the security metrics calculation can be conducted. An AG visualizes all paths through a system that results in a circumstance where attackers can successfully achieve their target. Cybersecurity professionals can utilize attack graphs for detection, defense, and forensics.

2.2 Related Work

2.2.1 Co-simulation Technology

EPOCHS (Electric Power and Communication Synchronizing Simulator) [24] is one of the first simulation models developed for smart grid systems. EPOCHS is built on top of PSLF, a commercial electric simulator, and ns-2, an open-source network simulator. This partial open-source project was developed to investigate the impacts of communication networks on electromechanical conditions. EPOCHS consists of a wide variety of applications, including wide-area monitoring and management. However, the EPOCHS plan does not include a cyberattack simulation function.

Testbed for Analyzing Security of SCADA Control Systems (TASSCS) [25] intends to enhance cyberattack detection and recovery techniques, especially for SCADA-based control systems. Several simulation technologies were integrated into TASSCS, consisting of OPNET simulation, PowerWorld simulation, and hardware. Modbus, which is a type of SCADA system architecture and communications methodology, supports a simulation-based control system. Further, the simulation results detail how ASPS is useful in detecting and solving DoS and HMI attacks' consequences.

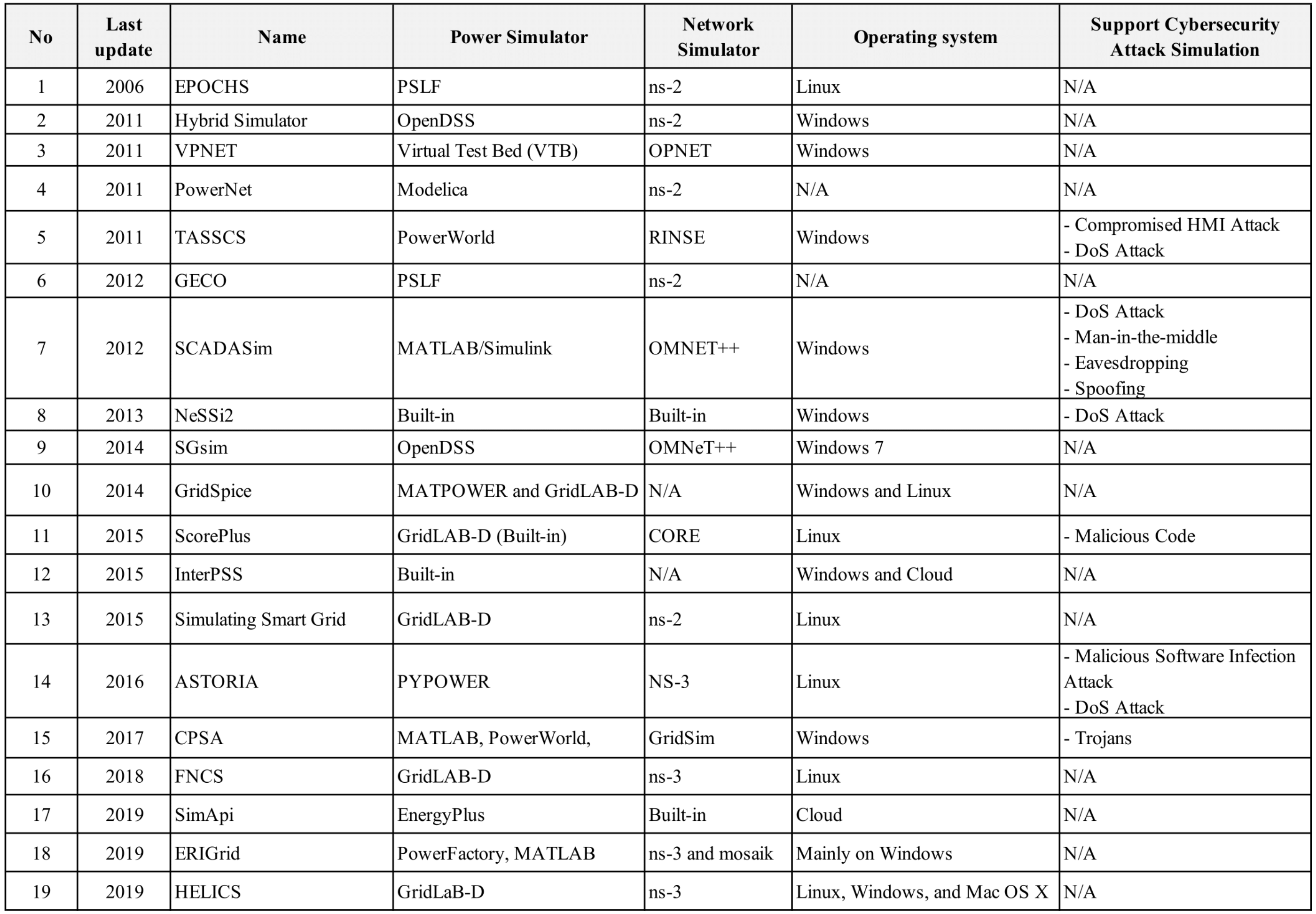
SGsim [26] is a simulation framework that can be used to simulate different smart grid applications in real-time. It consists of OMNET++, the backend for communication, and OpenDSS, a power simulation. Furthermore, SGsim supports smart grid communication-related standards, such as IEEE C37.118, and the standard smart grid tools, including openPDC. The primary purpose of SGsim is to monitor how communication affects control actions. In the smart grid research community, it has been considered the premier simulation tool. Unfortunately, the supported standards, smart grid components, and case studies for this framework are currently limited. Similar to EPOCHS, the cybersecurity attack simulation feature is omitted.

NeSSi2 [27] is a network simulation application built on the interface of a JIAC service agent. The framework focuses on protection scenarios; for instance, attack analysis and assessment of countermeasures. The study in [28] inherited the architecture of NeSSi2 and extended it with a safety model, as well as demonstrating the effect of attacks on AMIs' network. For communication and power networks, an open ring topology, which is usually deployed in the big cities in Germany, is defined. NeSSi2, however, is only able to model and determine the effects of the DDoS attacks on critical infrastructure.

SCADASim [29] is a SCADA simulation that allows the integration of external devices and applications. The architecture of SCADASim is designed by using a discrete event simulation engine (OMNET++) and modules that communicate with each other by transferring messages. Furthermore, this discrete event simulation engine permits the incorporation of external programs such as sockets, source code, and shared libraries into SCADASim. Even though SCADASim is a virtual tool, it can estimate the effect of attacks on real applications and devices. It is possible to simulate four attack categories on a smart grid system, consisting of eavesdropping, spoofing, man-in-the-middle, and DDoS.

The Attack Simulation Toolset for Smart Grid Infrastructures (ASTORIA) [30] is a framework for smart grid attack simulation and evaluation. ns-3 and PY-POWER were used as network and power flow simulators at the core of ASTORIA, respectively. As a broker, Mosaik was introduced to allow for the integration between these simulators. Through a simulated environment, ASTORIA enables the injection of attacks and the evaluation of their consequences. These attacks are instantiated by the Attack Profiles, consisting of generic formatted configuration files. They enable multiple attack parameters, such as attack schedule, attack type, intensity/frequency, and target and source components, to be configured. Denial of Service (DoS) and malicious software infection attacks, which are the two familiar cyberattacks on the SCADA system, were simulated. The research does not, however, identify clear security assessment metrics. In addition, only the vulnerabilities are highlighted in the system by presenting sampled data.

Table 2.1: Smart grid co-simulation tools



No	Last update	Name	Power Simulator	Network Simulator	Operating system	Support Cybersecurity Attack Simulation
1	2006	EPOCHS	PSLF	ns-2	Linux	N/A
2	2011	Hybrid Simulator	OpenDSS	ns-2	Windows	N/A
3	2011	VPNET	Virtual Test Bed (VTB)	OPNET	Windows	N/A
4	2011	PowerNet	Modelica	ns-2	N/A	N/A
5	2011	TASSCS	PowerWorld	RINSE	Windows	- Compromised HMI Attack - DoS Attack
6	2012	GECO	PSLF	ns-2	N/A	N/A
7	2012	SCADASim	MATLAB/Simulink	OMNET++	Windows	- DoS Attack - Man-in-the-middle - Eavesdropping - Spoofing
8	2013	NeSSi2	Built-in	Built-in	Windows	- DoS Attack
9	2014	SGsim	OpenDSS	OMNeT++	Windows 7	N/A
10	2014	GridSpice	MATPOWER and GridLAB-D	N/A	Windows and Linux	N/A
11	2015	ScorePlus	GridLAB-D (Built-in)	CORE	Linux	- Malicious Code
12	2015	InterPSS	Built-in	N/A	Windows and Cloud	N/A
13	2015	Simulating Smart Grid	GridLAB-D	ns-2	Linux	N/A
14	2016	ASTORIA	PYPOWER	NS-3	Linux	- Malicious Software Infection Attack - DoS Attack
15	2017	CPSA	MATLAB, PowerWorld,	GridSim	Windows	- Trojans
16	2018	FNCS	GridLAB-D	ns-3	Linux	N/A
17	2019	SimApi	EnergyPlus	Built-in	Cloud	N/A
18	2019	ERIGrid	PowerFactory, MATLAB	ns-3 and mosaik	Mainly on Windows	N/A
19	2019	HELICS	GridLaB-D	ns-3	Linux, Windows, and Mac OS X	N/A

Although both electricity grid and communication network simulations are capable of these simulation techniques, they are typically used in small, limited networks. The simulation approaches are designed in particular for certain circumstances that are difficult to expand. Furthermore, implementing and using the present architecture for co-simulation is very complicated. IT specialists, managers, and researchers are required to build a network model or incorporate proprietary software in an unusual environment. Further, there is little research on simulating smart grid cybersecurity attacks. Moreover, in the current co-simulation tool, attack schedule ability is usually omitted. Furthermore, recent studies integrate only a few attack types.

FNCS (Framework for Network Co-Simulation) [31] is a High-Performance Computing (HPC) simulation platform. The FNCS broker maintains the communication between ns-3 and GridLAB-D, which are the network and power grid simulators, respectively. Certainly, it facilitates a synchronized simulation in configurable time steps.

Table 2.1 illustrates the development of various simulation tools in the energy domain over time.

2.2.2 Attack Analysis Technology

A thorough overview of the most current analysis tools and their smart grid applications has been provided in our previous study [32].

2.2.2.1 Attack Analysis for Traditional Networks

Today, attacks targeting information systems are becoming gradually more sophisticated. Attackers can combine and exploit multiple vulnerabilities to run an attack. The research in [33] pointed out that probabilistic attack graphs can be used to analyze and draw all attack paths. This method can help mitigate risks and maximize the security of enterprise systems. The authors use available tools for generating attack graphs in enterprise networks to indicate potential steps that allow attackers to hit their targets. Additionally, the CVSS score, a standard used to evaluate the severity of computer systems' security vulnerabilities, is used to estimate the security risk.

Hyun Chul Joh et al. [34] indicated that risk could not be evaluated by a single cause. Independent multiple causes need to be considered to estimate the overall risk. Based on likelihood and impact values, a risk matrix is built to classify causes. The risk matrix is used to rate risks, and therefore, serious risks can be recognized and mitigated. Their study also addressed the software vulnerability life cycle. From the method of risk evaluation for every single vulnerability using stochastic modeling, the authors defined conditional risk measures to evaluate risk by combining both the essence and accessibility of the vulnerability. They provided the mathematical basis and demonstrated this approach by experimental validation.

The existing approaches to assess a network security metric using aggregation of CVSS scores can result in valuable semantics of individual scores to be lost. The research [35] drilled down into the basic metric levels to get dependency relationships in order to obtain better semantics. These relationships are signified by an attack graph. This approach used three separate aspects of the CVSS score to explain and aggregate the basic metrics. This helped maintain the corresponding semantics of the individual scores.

The work in [36] used Bayesian networks to propose a risk management framework, called Bayesian Attack Graph (BAG). This framework allows administrators to estimate the possibility of network compromise at various levels. Security risk management with BAG comprises threat analysis, risk assessment, loss expectancy, potential safeguards, and risk mitigation analysis. This component enables administrators to execute static and dynamic risk assessments, and risk mitigation analysis. Security risk mitigation with BAG is formulated as a Multiobjective Optimization Problem (MOOP), having a low complexity for optimization.

In approaches of attack graph-based risk management, a study [37] proposed a framework of risk assessment and optimization to generate a graph using a genetic algorithm for drawing attack paths. The framework was presented by six steps: attack graph generation, likelihood determination, loss estimation, risk determination, optimization, and high-risk attack paths.

Table 2.2: Attack analysis using GrSM and CVSS (Y: Yes, Blank: No)

No	Year	Research	Attack Tree	Attack Graph		Security Metrics Calculation				Likelihood	Apply to Smart Grid
				Attack Graph Generation	Attack Graph Visualization	Attack Success Probability	Attack Cost	Attack Impact	Attack Risk		
1	2011	Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs		Y		Y		Y	Y		
2	2011	Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics				Y		Y	Y		
3	2012	Aggregating CVSS Base Scores for Semantics-Rich Network Security Metrics		Y				Y			
4	2012	Dynamic Security Risk Management Using Bayesian Attack Graphs	Y	Y		Y	Y		Y		
5	2014	Determining the Probability of Smart Grid Attacks by Combining Attack Tree and Attack Graph Analysis	Y	Y		Y					Y
6	2014	Attack Graph-Based Risk Assessment and Optimisation Approach	Y	Y		Y			Y		
7	2015	A Framework for Modeling and Assessing Security of the Internet of Things	Y	Y		Y	Y	Y	Y		
8	2016	Security Modelling and Analysis of Dynamic Enterprise Networks				Y	Y	Y	Y		
9	2017	A Quantitative CVSS-Based Cyber Security Risk Assessment Methodology For IT Systems		Y		Y		Y	Y		
10	***2017***	***A framework for automating security analysis of the internet of things***	***Y***	***Y***		***Y***	***Y***	***Y***	***Y***		
11	2018	A Comprehensive Analysis of Smart Grid Systems against Cyber-Physical Attacks	Y	Y		Y		Y	Y	Y	Y
12	2019	CloudSafe: A Tool for an Automated Security Analysis for Cloud Computing		Y		Y					Y
13	2019	Quantitative Model of Attacks on Distribution Automation Systems Based on CVSS and Attack Trees	Y	Y		Y					
14	2020	A Bayesian Attack Tree Based Approach to Assess Cyber-Physical Security of Power System	Y	Y		Y		Y	Y		Y
15	2020	A Framework for Real-Time Intrusion Response in Software Defined Networking Using Precomputed Graphical Security Models		Y		Y	Y	Y	Y		

The proposed genetic algorithm finds the highest risk for building a minimal attack tree. This is also computed with huge graphs when very large attack paths are explored.

In their research into risk assessment for IT systems, Ugur Aksu et al. [38] proposed a quantitative methodology for evaluating the vulnerability in the system. Like other approaches, in this study, the CVSS metrics (base and temporal scores) are used to calculate the probability of attack success, attack risk, and the attack impact. The attack paths can be determined corresponding to the generation of the attack graph-based risk of a CVE on an asset. They measure risks not for only single CVEs but also for a collection of CVEs on the assets, elements, and attack paths in each IT system. Nevertheless, the authors did not evaluate the likelihood of a potential attack when analyzing the cybersecurity risk that may occur inside the network.

2.2.2.2 Attack Analysis for Emerging Technologies

The Internet of Things (IoT) brings many innovations in numerous domains; however, its security is a challenge. In order to analyze and address security issues in IoT, the research in [39] proposed a framework for security modeling and assessment, building graphs of security models, evaluating security levels, and recommending defense strategies. The framework can find attack scenarios in five stages: preprocessing, security model generation, visualization and storage, security analysis, and alterations and updates. This research demonstrated the framework's ability to reduce the impacts of possible attacks in cases studies of two IoT networks.

In the context of dynamic networks in which the configuration changes over time, Simon et al. [40] presented the Temporal-Hierarchical Attack Representation Model (T-HARM) with two layers for analyzing the security problems in the network. Therein, the upper layer contains the temporal hosts' reachability information, whereas the lower layer shows the changes of vulnerabilities correlating with each host by defining AT and AG. The attack paths, attack cost, attack success probability, and attack risk were calculated based on the metrics of the CVSS base score. However, the authors did not explore the likelihood of exploitable vulnerability in investigating a dynamic network's security.

In a study on automating security assessment for the IoT environment, Ge et al. [41] proposed a graphical security model used to find the potential attack before it occurs [39]. The authors conducted experiments with three different IoT networks in the context of smart home, environment sensor, and healthcare wearable device monitoring. The 3-layer Hierarchical Attack Representation Model (HARM), an extended version of HARM, is used to find all potential attack paths. This extended one consists of an attack tree (AT) for each node in the network topology. The authors analyzed the security problems of IoT devices regarding specific vulnerabilities according to various metrics like attack success probability, attack cost spent by hackers, attack impact, and the time to compromise these vulnerabilities. To quantify the severity of vulnerabilities for a network element, the CVSS is used to compute the aforementioned metrics. They also supported the feature of choosing the most effective defense strategies for mitigating potential attacks. Nevertheless, this work neither discussed the security likelihood nor visualized the attack graph.

Erxia Li et al. [42] presented a quantitative model in Distribution Automation Systems (DASs) for attack analysis based on CVSS and ATs. To be more specific, their modeling method is considered from the perspective of the attacker's behavior. Each step of the complete attack process is considered to calculate the node attack probability. Therein, the root tree is the ascertained component in the system, while an attack that can occur in certain DASs is represented by each leaf node of the AT. Three metrics of CVSS, namely, base, time, and environment score, are used to compute the maximum probability of each potential path for intruding on the network. The max score indicates the most vulnerable path to be patched with the most defense strategies. Although this framework can generate the quantitative attack graph, it does not support the feature of graph visualization.

Seongmo et al. proposed CloudSafe [43], a tool for automated security assessment in a cloud environment, which is implemented in the Amazon

AWS. It consists of two phases: information collection and HARM generation. Firstly, the researchers built a cloud information gathering interface for further data storage and security analysis. Then, this module is integrated with HARM by modifying the security information retrieved from the first phase. In quantifying security, the probability of successfully exploiting a vulnerability is calculated by the metrics of CVSS on the Reachability Graph (RG), which is saved in a database after mapping inter-VM connections in cloud targets. Moreover, the researchers also provided attack cost, risk, and impact information correlating with each cloud vulnerability. Nevertheless, graph visualization is not supported.

Meanwhile, a study by Taehoon Eom et al. [44], focused on the computation of possible attack graphs for real-time intrusion detection and response in Software-Defined Networking (SDN). They used the HARM model with security metrics depending on the information of the flow table and SDN components. All possible attack paths that are pre-computed by HARM and full AG can evaluate the security issues of the network system prior to an attack detected. It is useful to estimate possible attack paths from the point of detection to formulate effective remedies. The authors used the base score of CVSS to measure the severity of vulnerabilities and the probability of attack success in the network entities in detail. The impact attack metric was directly inherited from CVSS. Additionally, in accordance with the reduction of scalability complexity, the authors also built attack graphs based on modeling network nodes and their vulnerabilities onto multiple layers. The main reason for this is that the SDN consists of many components and network elements, causing security assessment not to be scalable in enumerating all possible attack scenarios. By leveraging from HARM, the authors generate 2-layer HARM, where each host in the higher layer has a corresponding AT in the lower layer. The lower layer is a collection of ATs, where each AT is the representative of the vulnerability information for each upper layer node, i.e., SDN network node. Nonetheless, this study lacks the support of graph attack visualization and likelihood recommendation.

2.2.2.3 Attack Analysis for Smart Grid

An attacker collects information from the high-level aim of a target and then takes low-level actions. Kristian Beckers et al. [45] delivered a method that can show the attackers' steps. This method gathers information of a system at the low-level presentation to analyze high-level probabilistic attributes. The attacker's high-level aims are drawn as an attack tree and actions at a low level are drawn as an attack graph. The research combined both the attack tree and attack graph for mapping the aims of the attacker to actions. This combination was applied to a smart grid. This proposal helps system administrators prevent possible attacks.

The acceleration of the smart grid technologies makes power delivery systems easy to use as well as meet the needs of intelligence and efficiency. However, insider and outsider attacks that may harm to the smart grid system have recently occurred in real cases. Hence, there is more attention from researchers to deeply understand security levels in these systems in order to implement defense methods for disaster prevention to avoid the consequences of intrusion attacks.

Besides, Yatin et al. [3] presented the methodology of risk assessment for cyber-physical attacks in the smart grid system. They concentrated on one primary function, power delivery, to narrow down the system's number of attacks. The Bayesian Attack Graph for Smart Grid (BAGS) tool is used to quantify the probability of attack success, and the likelihood of attack relying on the CVSS base score when successfully exploiting vulnerabilities. The authors also considered the attack risk to help power engineers decide on the security budget and patch management to protect the system in which system components are susceptible to easy compromise by intruders. They also applied reinforcement learning for resource allocation in the cyber domain of smart grid to generate the optimal policy that recommends whether to conduct the assessment and patching of the vulnerability in the network. However, this work did not take into account the attack cost for hackers when attempting to compromise the cyber system. Graph visualization is also ignored in its implementation.

In [46], Rounak presented a Bayesian attack tree to model CPS vulnerabilities for SCADA's security assessment. This work concentrated on the perspective of prioritizing important vulnerabilities in SCADA that are likely to be first identified and generate attack paths to the target element. This is to avoid comprehensive modeling of every element in the CPS. For each type of vulnerability, the probability of successfully exploiting is considered in accordance with the skill level of the intruder. Also, their skill level reflects the time it takes to compromise the system that contains the vulnerability. The CVSS metric is used to calculate the probability that a vulnerability is successfully exploited. Further, the impact on the power grid as well as the risk of the cyber attack on each attack path is also assessed in the cyber-system. However, the lack of attack graph visualization and likelihood are shortcomings of this study.

2.2.2.4 Security Metrics Calculation

To compute the likelihood of compromise in a smart grid environment, Yatin et al. [3] used the base score of CVSS to compute the exploitability of a vulnerability. Based on the probability ranges, they matched each potential attack with the corresponding qualitative value of likelihood.

Besides, Ge et al. [41] proposed some metrics to analyze the security problems for an IoT-enabled system. In general, this framework takes IoT topology, vulnerability information, and security metrics from security decision-makers as its input to generate an extended HARM model. Then, the graph visualization of the IoT network topology with attack paths is produced. Subsequently, the security analysis is conducted, relying on the set of IoT nodes, vulnerabilities, and potential attack path information. The analysis result is then used to determine the most appropriate defense strategies for vulnerable nodes in the network.

2.3 Summary

For smart grid attack co-simulation, our previous research [18] argued that it is possible to co-simulate with ns-3, FNCS, and GridLAB-D. Furthermore, the co-simulation performance was improved by 20%. Unfortunately, few studies have evaluated the implications of cyber attacks against the smart grid system based on this combination. Consequently, our research was carried out to fill the FNCS study gap by introducing a robust and extendable attack pattern library with an attack schedule, a friendly GUI, and a result visualization function.

For smart grid attack analysis, the framework for automating security analysis of IoT proposed in [41] is the most advanced in terms of coverage, ranging from Attack Tree (AT), Attack Graph Generation (AGG), attack success probability (p), attack cost (ac), attack impact (aim), and attack risk (r). Furthermore, the formulae to calculate security metrics were explained in detail. However, the scope of the framework focuses on the general IoT system. Therefore, there are still limitations in attack graph visualization, likelihood, and smart grid application. Attack graph visualization is a practical method for cybersecurity experts and even novices to examine the system's activities and investigate all potential cyber attacks. By using likelihood, the possibility of an attack can be ranked, which strongly supports the risk assessment process. The lack of research on smart grid attack graph visualization and likelihood creates a gap in the field. Consequently, we utilize the framework to bridge the gap in the current research.

Chapter 3

General Architecture for Smart Grid Cybersecurity Experimentation

3.1 Design Requirements

The smart grid structure is complicated with two essential parts: network communication and the power grid. Researchers need to consider the relationship between these components for further system investigation and improvement. Unfortunately, it is usually impossible to implement a real smart grid system for the cybersecurity experiment and validation process because of their potentially dangerous consequences. Accordingly, system-level modeling and simulation tools are necessary for a smart grid cybersecurity experimentation system. Therefore, a cybersecurity experimentation system for smart grid should meet the following specifications, which are summarized in Figure 3.1.

- Power grid component: the experimentation system should be able to reproduce the behavior of a power grid network and the interaction between its components.
- Network component: the experimentation system should be able to reproduce a smart grid network's behavior by calculating and simulating interactions between various network entities.
- Security component: the experimentation system should be able to simulate, emulate, and analyze various types of attacks on the smart

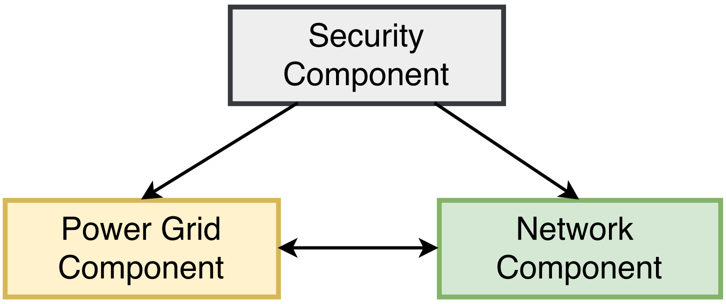


Figure 3.1: Cybersecurity experimentation for smart grids in general

grid system. The security component is a set of databases and configurations to start an attack on the system.

3.2 Concern in Smart Grid Cybersecurity Research

These requirements should be fulfilled to create realistic cybersecurity experimentation for smart grids. Due to its structure being complicated, it is inefficient to design a single, smart grid cybersecurity experimentation system that meets all of the requirements above. Therefore, to simplify the system but still accomplish our goal, we break down the smart grid cybersecurity experimentation into two components: simulation approach and analytical modeling approach.

The intention of simulation and analytical modeling approaches is to enhance understanding of the system's performance under various conditions.

On the one hand, through certain assumptions about how a method progresses, an analytical model is a mathematical abstraction that can be generalized to deal with different working conditions. In some instances, it is possible to determine a solution, and a result can be obtained in a wide variety of situations. The analytical model's strength is that it provides a generalized method for obtaining performance results by using a mathematical formulation under different conditions. The model's accuracy must be taken into account through the validity of the assumption that the

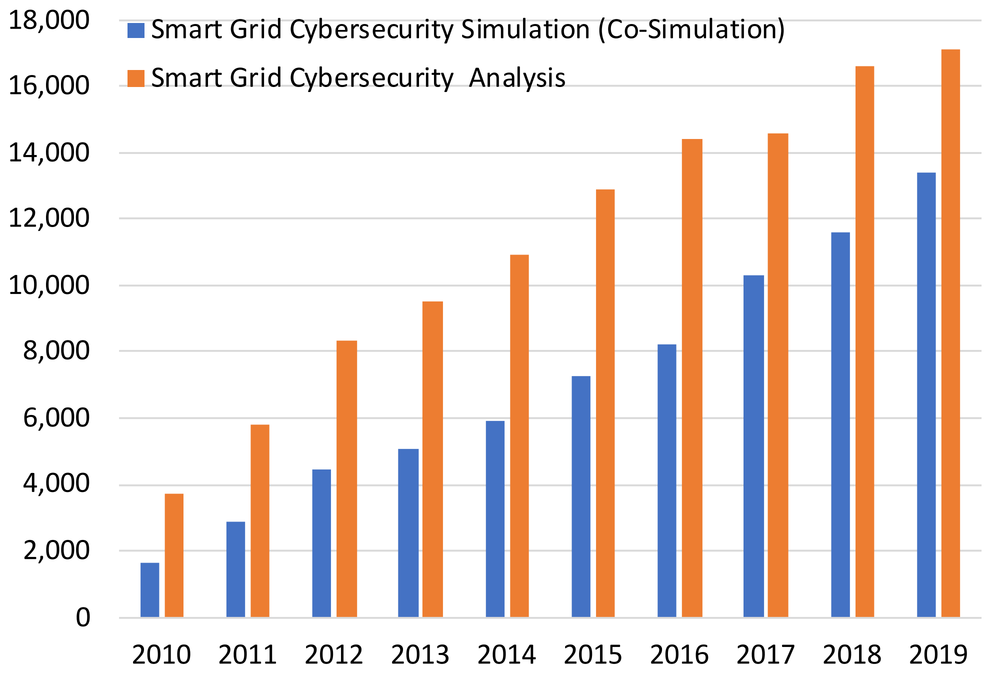


Figure 3.2: Number of publications related to smart grid attack simulation and analysis from 2010 to 2019.

mathematical formula is derived. To estimate the modeling and measurement model, some uncertainties can be addressed with a stochastic model.

On the other hand, a simulation model also makes assumptions of the model and the process's behavior that it is simulating. A simulation model is applied when it is impossible to derive the result using the analytical formulation since the model is too large, or the exact solution cannot be obtained. It is only useful for specific applications and should be executed multiple times to compensate for the influence of numerical calculations. For several application scenarios, the simulation should be re-executed to confirm the findings. A simulation model can be recognized as useful when it has been shown to operate under numerous circumstances and is not dependent on a single case study.

The analytical approach should be preferred when the two methods are available, and simulation can be applied to verify the assumptions and models' validity. When the two approaches can be used, preference should be given to the analytical approach, and simulation can be used to validate the assumptions and the models. Since the simulation aims not to verify the model but to validate the reality of the modeling process, the assumptions applied by the simulation model could be slightly different from the analytical model for better analysis.

Therefore, using the simulation approach is one possible direction take to conduct cybersecurity experimentation for smart grids. On the one hand, the power grid and the network should be simulated independently. On the other hand, the interaction between them should be captured. Consequently, these specifications not only complicate the system architecture but also reduce its performance. Co-simulation is an emerging technology to deal with this issue.

The application of simulation (co-simulation) and analysis for smart grid cybersecurity experimentation research has been increasing in recent years. Figure 3.2 shows the number of publications related to smart grid simulation and analysis from 2010 to 2019. The data on the table were acquired from Google Scholar by searching the keywords. The search pattern for smart grid attack co-simulation is (“Smart Grid” OR “Smart Grids”) AND (“Simulation” OR “Co-simulation”) AND (“cybersecurity” OR “cyber security” OR “security”); while the keywords for smart grid attack analysis searching are (“Smart Grid” OR “Smart Grids”) AND (“Analysis”) AND (“cybersecurity” OR “cyber security” OR “security”).

The relationship between the general cybersecurity experimentation for smart grids and the two approaches is shown in Figure 3.3. The co-simulation approach and analytical modeling approach are discussed in the following.

3.3 Co-simulation Approach

Co-simulation is the coordination of two or more simulation models, which differ in their runtime and representation. It can simulate the network and the power grid separately. Moreover, co-simulation enables the reciprocal relationship between the physical power grid and the communication network to be monitored. Instead of developing and constructing a new combined simulation environment, multiple specialized simulation environments are

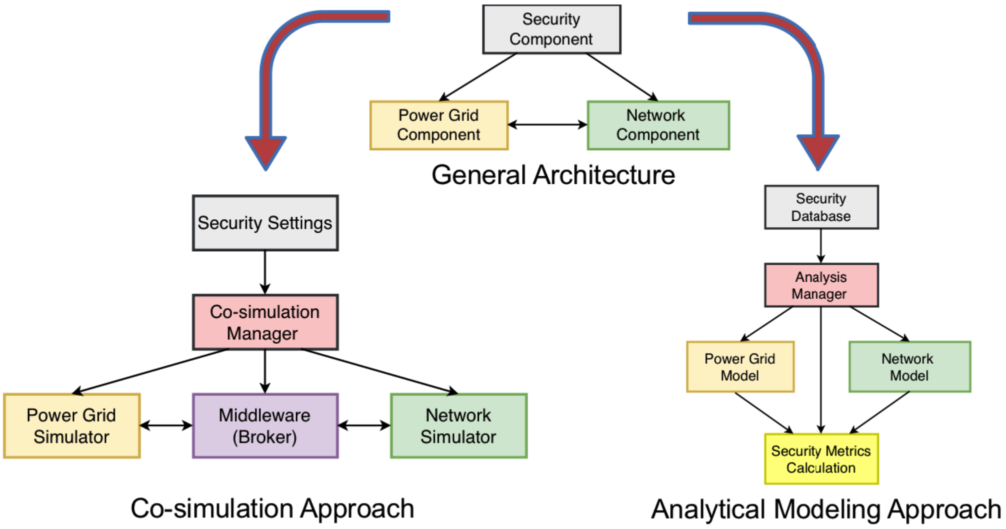


Figure 3.3: The two approaches of smart grid cybersecurity experimentation

connected into a single distributed environment.

Reuse and separation are two critical criteria for the incorporation of smart grid components. The objective is to make the different simulators' modules available for combined simulations, which run independently and only exchange data when needed. The combination allows users to implement and examine different communication and power hardware/protocol integration. Fortunately, there are various robust network simulations as well as power grid simulation tools. Therefore, one of the advantages of this integration is reusing existing models and frameworks and their well-validated libraries.

Unfortunately, the aforementioned integration commonly complicates the simulators' codebase, introduces bugs, and sometimes replicates work that has already been completed. The adaptation also poses numerous difficulties that need to be overcome, such as differences in time scales, time synchronization, communications delays, and appropriate model reuse. To overcome these challenges, a reliable middleware or broker should be placed in the middle of the co-simulation approach's architecture to monitor and control the two smart grid components' communication.

Further, to manage the co-simulation activity, a general manager is

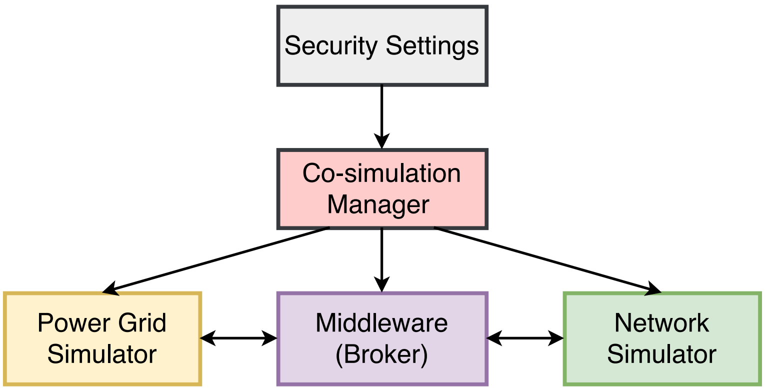


Figure 3.4: The general architecture of the co-simulation approach for smart grid cybersecurity experimentation.

needed. It receives attack data and configuration from the security component then transfers to the power grid simulation and network simulation as well as awakes the middleware to conduct a simulation session.

Therefore, the design requirements for co-simulation space should contain five components:

- Security Component
- General Manager
- Power Grid Simulation
- Middleware (Broker)
- Network Simulation

The general architecture of the co-simulation approach for smart grid cybersecurity experimentation is illustrated in Figure 3.4.

3.4 Analytical Modeling Approach

Another possible direction to take to conduct cybersecurity experimentation for smart grids is by utilizing the analytical modeling approach, which aims to create a model for smart grid attack analysis.

An attacker may launch various attacks, such as DoS attacks, eavesdropping, node controlling, and node capture, by exploiting the system vulnerabilities. Attack analysis focuses on all possible attack paths where the system

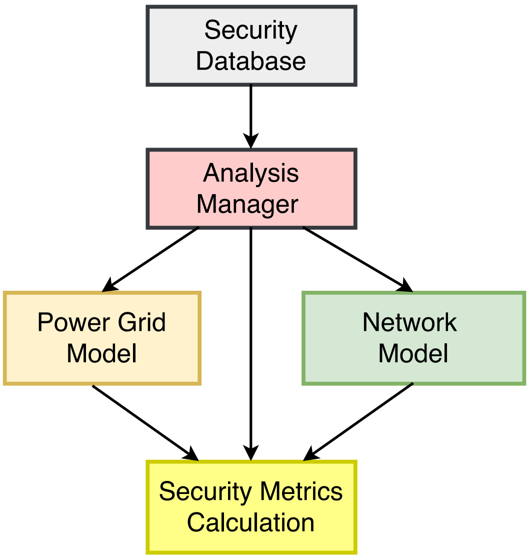


Figure 3.5: The general architecture of the analytical modeling approach for smart grid cybersecurity experimentation

(or network) is accessed or compromised by utilizing technical capabilities to exploit a vulnerability. With the existence of several complicated threats, the ability to discover possible attack scenarios and minimize the effect of malicious attacks is becoming a significant problem. The attack analytical results allow the researchers or security decision-makers to determine which part of the network is the most vulnerable, evaluate the various defenses' efficacy, and decide how to secure the network most effectively; hence, minimizing the potential attacks' impact.

Securing a network involves an in-depth analysis of regular operations and vulnerabilities. Such analysis is tiresome and error-prone. The conventional attack analysis classifies attacks based on information of reported attacks. Hence, such an approach can not be extended to new (unknown) incidents. The concern is even more severe in emerging environments where very few reported threats are available, such as the smart grid. The study on modeling the security of the smart grid is also limited due to its pioneering nature.

Researchers can gain several benefits by using attack analysis:

- Firstly, the model provides the ability for researchers to capture all potential attack paths, meaning it is no longer limited to the protection of particular attacks.

- Second, it enables researchers to analyze the security of different smart grid attack scenarios.
- Finally, it offers an intuitive way of analyzing security flaws in systems and assessing possible counteractions since the sequences of the attackers' measures are captured in the model.

The main challenge in attack analysis is the security metrics calculation, for instance, how to correctly compute all possible attack paths. Therefore, security metrics calculation is one of the requirements for the analytical modeling approach.

Additionally, to control the attack analysis activity, a general manager is required. Attack data and configuration from the security component are acquired, then transferred to the power grid model and network model. The security metrics calculation component receives attack data from the security component as well as the smart grid model from the power grid model and network model. Finally, the security metrics are calculated and analyzed.

Figure 3.5 shows the requirements to design the architecture of the analytical modeling approach for smart grid cybersecurity experimentation, including:

- Security components
- General manager
- Power grid model
- Network model
- Security metrics calculation

3.5 Approaches Comparison

Despite their similarities, the co-simulation approach and analytical modeling approach are implemented with different intentions.

The co-simulation approach makes assumptions of the model and the process's behavior that it is simulating. The approach enables analysts to simulate different attack types on the smart grid system. Additionally, these security metrics can be compared against normal operation and attack scenarios. Therefore, the co-simulation approach advances the experience of recreating vulnerability manipulation strategies and involves exercises, for instance, using the same methods and technologies adopted by attackers. Further, it enables the design and implementation of cybersecurity defense methodologies to anticipate similar future attacks.

Analytical modeling is a mathematical abstraction under different conditions. It allows researchers to determine all possible attack paths and calculate the selected security metrics. Plus, the attack graph can be generated. Therefore, this approach gives researchers a deeper understanding of the phenomena relevant to exploitation and patching of vulnerabilities.

3.6 Summary

In this chapter, we identify the need for realistic cybersecurity experimentation for smart grid. The design requirements of the system are outlined. To deal with the system complication but still achieve our goal, we divide the smart grid cybersecurity experimentation into two components, including the co-simulation approach and analytical modeling approach, and offer their specifications and general architectures.

This research aims to design and develop a smart grid cybersecurity experimentation system for smart grids that fulfills the aforementioned requirements. The core technologies of this research are GridAttackSim - Cyber Attack Simulation on Smart Grids and GridAttackAnalyzer - Cyber Attack Analysis on Smart Grids. GridAttackSim follows the conceptual model of the co-simulation approach, while GridAttackAnalyzer inherits the architecture of the analytical modeling approach.

The developed frameworks can be used to understand the power and network system monitoring, analyze the nature of cyber-attacks, and investigate their impact on the smart grid's operation. GridAttackSim and GridAttackAnalyzer are discussed in the next chapters.

Chapter 4

GridAttackSim: Cyber Attack Simulation for Smart Grids

4.1 GridAttackSim Architecture

In this section, we proposed GridAttackSim, the Smart Grid Attack Co-Simulation framework, which is shown in Figure 4.1. The architecture of GridAttackSim is based on the co-simulation approach, where the power grid and communication network components are integrated. The ability to perform different attack simulations is also provided. GridAttackSim is comprised of six core modules, including the preprocessing module, attack pattern library, GridLAB-D, FNCS broker, ns-3, and model manager.

4.1.1 Preprocessing Module

There are two components of the preprocessing module, including communication configuration files generation and GLM append. The purpose of this module is to prepare the environment and configure the FNCS simulator properly to connect the FNCS broker applications. An appropriate configuration requires at least a global unique simulator term. Additionally, the simulator should specify the topics for which the broker is subscribed.

The GLM append function's input is a raw IEEE test feeder file in GridLAB-D format (.glm), created initially by PNNL (Pacific Northwest National Laboratory), U.S. Department of Energy. It adds the fncs_msg and auction objects into the input file to configure the GridLAB-D process connection and FNCS broker.

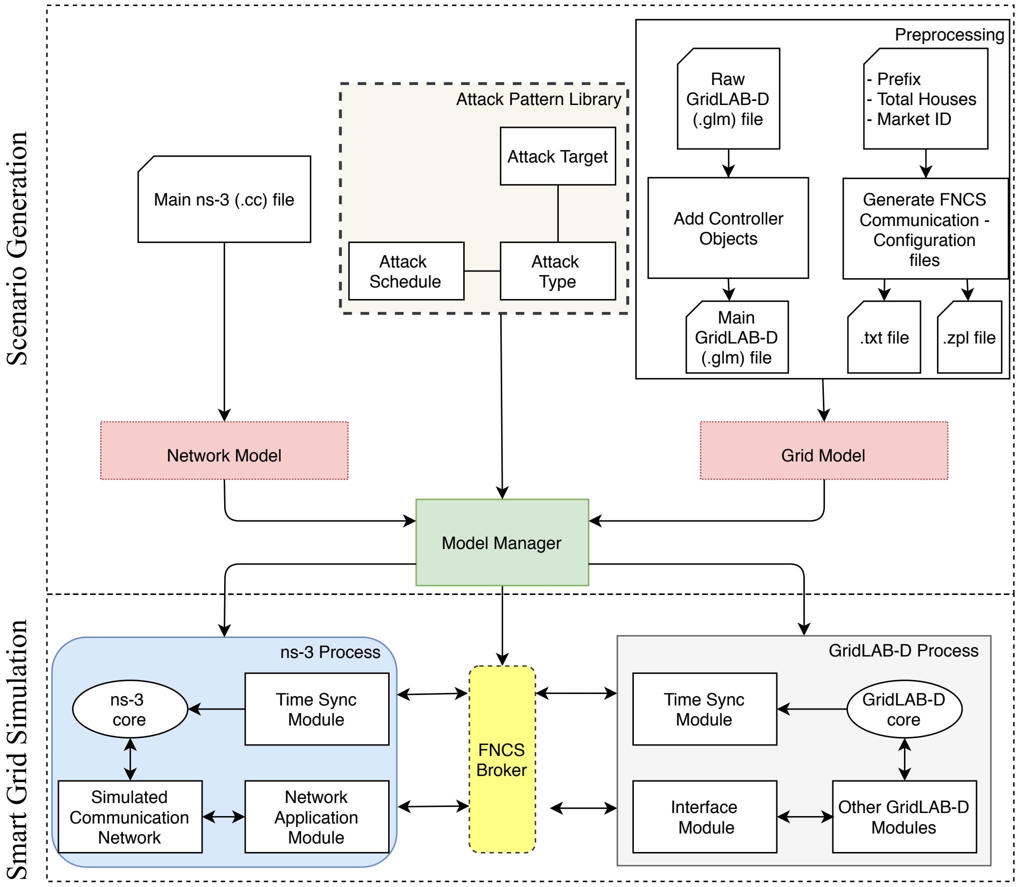


Figure 4.1: The architecture of GridAttackSim.

The communication configuration files generation function obtains the total number of houses, market ID, and prefix of the controller inside each house as the input. The generated files are a .txt file and a .zpl file. The txt-formatted file's aim is to configure the communication between the FNCS broker and the ns-3 process. The zpl-formatted file or FNCS ZPL (ZeroMQ Property Language) configure file, which is based on the ZPL structure, configures the simulator to subscribe to the topic of interests, such as market ID, market-clearing price, submit bid state, the price's standard deviation, and average price.

For each simulator, a corresponding "fncs.zpl" file should be available. This fncs.zpl is expected to be in the actual working directory that awakes the simulator by default. An example of a fncs.zpl format file is shown in

```
name = GLD1
# required; across the co-simulation, all names must be unique
time_delta = 1s
# optional; format is <number><unit>; smallest time step supported by the simulator;
# defaults to 1s
broker = tcp://localhost:5570
# optional; broker location; defaults to tcp://localhost:5570
values
  # optional; list of exact-string-matching topic subscriptions
  lookup_key
    # required; lookup key, which is what you pass to fncs::get_value() in the code
    topic = some_topic
    # required; format is any reasonable string (not a regex)
    default = 50
    # optional; default value
    type = int
    # optional; currently unused; data type
    list = false
    # optional; defaults to "false"; whether incoming values queue up (true)
    # or overwrite the last value (false)
```

Figure 4.2: The fncs.zpl format example.

Figure 4.2.

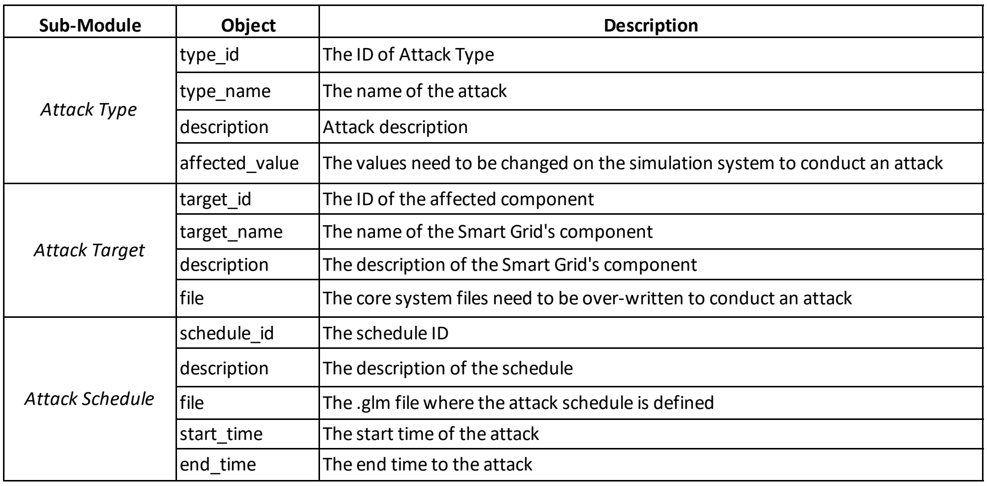
4.1.2 Attack Pattern Library

GridAttackSim makes it possible to inject attacks and evaluate their consequences in a simulated environment. These attacks are instantiated through the attack pattern library. It helps model the nature, intensity, and schedule of an attack on the smart grid infrastructure. The attack pattern library contains a standardized JSON configuration format file to enable behaviors of various attack types to be defined.

During the simulation process, different attack parameters settings are allowed, such as the target components, attack type, and the start time and end time. Table 4.1 shows the attack pattern library structure. The library enables the run-time reconfiguration to explore a wide variety of attacks against the same smart grid architecture.

The combination of three sub-modules introduced by research in [47], including attack type, attack schedule, and attack target, can attain different attacks. By extending the aforementioned approaches, it is possible to model an attack's behavior, including the type of attack that may be carried out (what question), when the attack may occur (when question), and which

Table 4.1: The structure of attack pattern library



Sub-Module	Object	Description
Attack Type	type_id	The ID of Attack Type
	type_name	The name of the attack
	description	Attack description
	affected_value	The values need to be changed on the simulation system to conduct an attack
Attack Target	target_id	The ID of the affected component
	target_name	The name of the Smart Grid's component
	description	The description of the Smart Grid's component
	file	The core system files need to be over-written to conduct an attack
Attack Schedule	schedule_id	The schedule ID
	description	The description of the schedule
	file	The .glm file where the attack schedule is defined
	start_time	The start time of the attack
	end_time	The end time to the attack

parts of the system may be targeted (where question).

The attack type sub-module is employed to address the "what" question. It is utilized to characterize specific types and categories of attacks. Indeed, the sub-module is responsible for different types of malicious actions to be executed on the system.

Along with defining a particular type of attack, it is necessary to specify the targeted device. The attack target sub-module aims to answer the "where" question. It sets the vulnerable parts of the smart grid system that are affected in a specific attack circumstance. The type of target can be very different such as nodes, networks, end-point regularities, and control systems.

The attack schedule sub-module represents the times when a particular attack type is conducted. Its goal is to solve the "when" question. The schedule decides when to conduct a particular attack type.

4.1.3 Ns-3

ns-3 [48], a successor of ns-2, is an open-source network simulation framework specifically designed for simulation, networking studies, and training. First released in 2008, this powerful network simulator has been widely accepted in the network research community. A robust network model library with IP-based applications (TCP, UDP), routing, protocols for multicasting, and wired and wireless networks is provided at the top of the tool's architecture. An ns-3 process consists of four principal modules, including an ns-3 core, simulated communication network, time sync module, and network application module. These components aim to sustain all other simulator components. Although the core of ns-3 is developed using the C++ language, both CMDENV, Python scripting, the OTcl interface, and TKENV are supported. Consequently, developers can continue to develop and modify simulations without understanding the C++ language or recompiling ns-3. Furthermore, with the Python language support, the tool enables improved scalability and enhanced software integration.

4.1.4 GridLAB-D

GridLAB-D [49], which is an open-source, time-series simulation developed by PNNL, is the pioneer of modern power distribution simulation systems. GridLAB-D can simulate all of a power grid system's features from substation to the end-users' power consumption. A GridLAB-D process has four central modules, consisting of the GridLAB-D core, interface module, time sync module, and other modules. In order to enhance sophisticated applications, the combination consistently incorporates high-level simulation methods as well as high-performance optimization methods. GridLAB-D has several important features. For example, its end-use models, including devices, equipment, and user models, are combined with the modern agent-based simulation methods. In addition, GridLAB-D is driven by energy resources distributed models, such as the distributed generator and storage models, and load shedding infrastructure. GridLAB-D also enables the retail market modeling services, including selecting contracts, metering technologies, SCADA modeling, and businesses and transactions simulation. Furthermore, it allows external connections with different other tools, such as Matlab, MySQL, SynerGEE, Microsoft Excel, and Microsoft Access. Also, GridLAB-D can be combined with a range of third party data management and analysis tools. The tool was validated by applying the standard analysis methods of distribution as well as the existing simulation approaches. Therefore, GridLAB-D is invaluable for regulators, stakeholders, service managers, and even consumers.

4.1.5 FNCS Broker

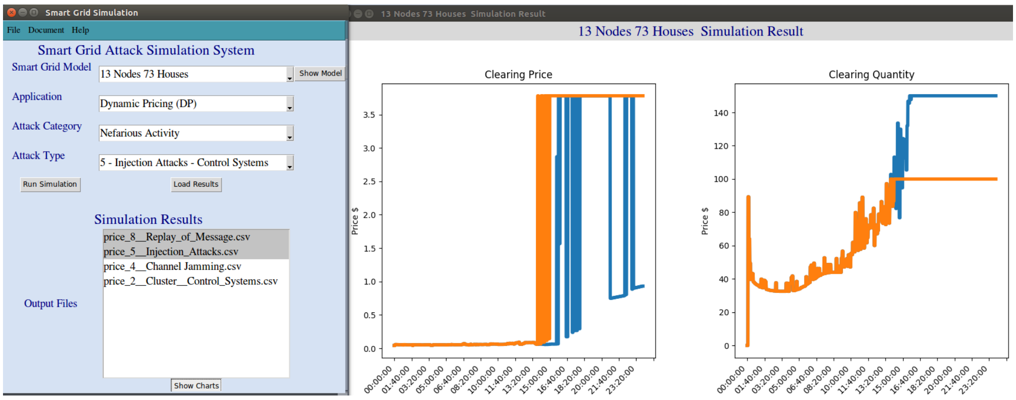
The FNCS broker assists the communication between ns-3 and GridLAB-D simulators. It facilitates co-simulation with multiple platforms such as single, multiple, cluster, and cloud nodes. On one side, ns-3 is designed to simulate data communication networks and monitor the operation of the system. On the other side, the power grid is simulated by GridLAB-D. In the core of the architecture, the FNCS broker is installed to maintain the communication between ns-3 and GridLAB-D. However, all FNCS-federated simulators are required to register with the FNCS broker, which enables the simulator's centralized process control. Moreover, the FNCS' design intention is to reuse existing simulators to enable a real-time co-simulation environment. The time synchronization steps are calculated in conjunction with the next time steps in the simulators and depending on whether there are messages in transit.

4.1.6 Model Manager

The model manager serves as the smart grid attack simulation engine, which is in the central component GridAttackSim. By implementing this module, the combination of simulation scenarios is managed, and the execution of the simulations is controlled. Further, the model manager also implements both simulators' initialization, configuring the power grid topology, the simulators' parameters, and the network model. It wakes up the preprocessing module to prepare the simulation environment when the simulation of a scenario is initiated. Firstly, the resource models, consisting of the network and power grid models, are loaded. Then, if the user selects an attack type, the attack pattern library will be called. Consequently, the power grid and the network models' cores are updated. Then, the model manager executes both the three main components of GridAttackSim, including GridLAB-D, ns-3, and FNCS broker. Finally, the simulation results are loaded and visualized.

4.2 Implementation and Selected Results

We discuss the proof-of-concept prototype of GridAttackSim in this section. A smart grid co-simulation application using the Python programming language was developed based on the architecture presented in the previous chapter. The GridAttackSim desk application (GUI) shown in Figure 4.3 was created by Tkinter [50], a binding Python to the Tk GUI toolkit.



Smart Grid Simulation

Smart Grid Attack Simulation System

Smart Grid Model: 13 Nodes 73 Houses

Application: Dynamic Pricing (DP)

Attack Category: Nefarious Activity

Attack Type: 5 - Injection Attacks - Control Systems

Simulation Results

Output Files:

price_8__Replay_of_Message.csv
price_5__Injection_Attacks.csv
price_4__Channel Jamming.csv
price_2__Cluster__Control_Systems.csv

13 Nodes 73 Houses Simulation Result

Figure 4.3: Desktop application (GUI) of GridAttackSim.

This section is organized as follows. Firstly, the smart grid model overview is described. Then, the specifics of two smart grid applications are presented, including demand response and dynamic pricing. Later, we describe the supported attack types. Finally, the detail of running the simulation and visualizing the results is discussed in the last subsection.

4.2.1 Smart Grid Model

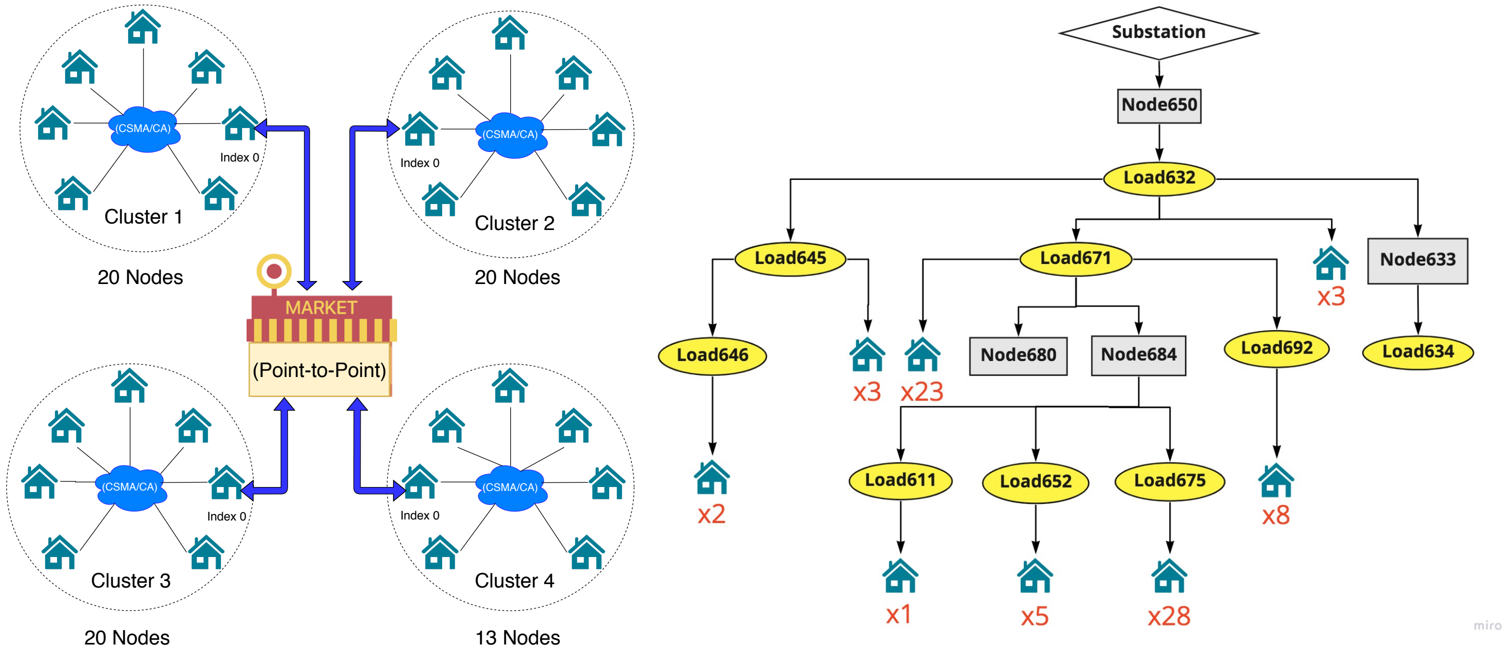
The smart grid model consists of two critical parts: the communication network and the power grid models. Hence, to model a smart grid system, both ns-3 and GridLAB-D are required. There are a particular number of houses in each smart grid model that act as dynamic power consumption or residential loads. Each of the residential loads is equipped with a Heating, Air Conditioning (HVAC) system, and ventilation, which are managed by a specific passive controller. Figure 4.4 shows an example of a smart grid model with 73 houses and an IEEE 13 node test feeder.

4.2.1.1 Network Model

An ns-3 network model with several nodes representing smart meters installed in the residential load was developed for the communication networks. These smart meters are organized into small groups forming local networks. An IP address was also provided for each smart meter; then, it was mapped to the given name for each GridLAB-D model's residential load. Each group's collected data are routed to a data aggregator by an edge network node through a point-to-point communication connection. UDP has been used as the communication protocol since it is a connection-free protocol that results in a lower transmission delay than TCP. The ns-3 CSMA (Carrier Sense Multiple Access) device models a simple Ethernet bus network, which is the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) transmission protocol. The ns-3 CSMA/CD model was utilized to define data rates and delay values in this study. Ns-3 is a powerful simulator for network modeling. Consequently, it is possible to apply it to more complicated network models in the future.

4.2.1.2 Power Grid Model

A GridLAB-D power grid model was developed based on the simple test feeder, the 4 node and 13 node IEEE test feeders [51]. These test feeders' objective is to present a distribution system model that represents a broad class of analytical and design difficulties. Initially, these test feeders were created to test new methods of power flow. However, due to their convenience and accessibility, the test feeders have been utilized for various studies. These test feeders' general structure involves (1) substations represented as the energy provider, (2) transformers to adjust the voltage levels, (3) meters to measure the power consumption, (4) loads to consume energy,



(a) (b)

Figure 4.4: Smart grid model: (**a**) The network model and (**b**) the power grid model of IEEE 13 node test feeder with 73 houses.

and (5) transmission lines.

The simple test feeder [52] is a tiny test feeder created by PNNL to test the FNCS function. It comprises a substation swing bus and residential loads. This substation consists of a swing bus with a nominal voltage of 7200 V and a power rating of 1500 kW each phase (4500 kW in total). A total load meter to measures power consumption is installed between the transformer substation and residential loads. In addition, the collected data enable the substation to adjust the supply of power to the system. Through triplex meters, the residential loads link to the power line.

IEEE 4 node test feeder, or the 4-bus feeder [53], was originally created in 2001, ten years after the original 1991 IEEE test feeders were released. By providing a simple model, the test feeder has the capability of a program to analyze all the possible three-phase transformer connections. Additionally, it steps up and steps down operations in various balanced and unbalanced load scenarios. Due to their small size, the test feeder error rate is expected to be less than 0.05%. Thus, the 4-bus feeder is widely used in distributed energy resources research and power flow analysis.

The IEEE 13 node test feeder, or the 13-bus feeder [54], was first introduced in 1992. During the Power and Energy Society Summer Meeting in 2000, this small and highly loaded test feeder was approved. It features many of the standard technologies employed in current grids, such as shunt capacitor banks, voltage regulators, underground and overhead lines, and unbalanced loads. Operating at 4.16 kV, the 13-bus feeder aims to experiment with common features of distribution analysis applications. It is the starting point for power-flow convergence problems in highly unbalanced systems research.

4.2.2 Smart Grid Applications

A range of smart grid applications is available, including Demand Response (DR), Dynamic Pricing (DP), Advanced Metering Infrastructure (AMI), Wide-Area Monitoring, Protection, and Control (WAMPAC), and Phasor Measurement Units (PMU). High bandwidth communications are necessary for several smart grid applications, such as DR and DP, to facilitate high-speed, cybersecurity, wide-area monitoring. Nevertheless, these standards do not apply to all smart grid applications; for example, AMI only has to update billing once every 24 hours.

Peak demand is when the power consumed by the network is highest, which can strain the electricity grid and cause power outages. Hence, reducing peak demand is an emerging difficulty for the energy industry. The construction of the electrical system should receive more financial investment to tackle this problem. Unfortunately, this expense will contribute to rising electricity costs. However, research has shown that demand for 25% of the distribution and 10% of the generation and transmission assets, which is worth more than 100 billion dollars, is less than 400 hours a year. Fortunately, the smart grid system can reduce peak demand by applying DP and DR. Accordingly, we have implemented DR and DP as models to prove results.

DR refers to adjustments in a consumer's power usage to balance supply with demand. During periods of high demand, DR endeavors to ensure a reliable power supply by enabling consumers to minimize or adjust their energy consumption dynamically. It aims to adjust the end-users' power usage instead of adjusting the energy supply to the system. As a result, users can play an active role in electric grids' operation, unlike most conventional power grid systems. Accordingly, the service provider has numerous benefits, for example, emergency operations, control services, and a reduction in peak load.

DP is a price model that allows utility companies to create flexible electricity prices based on current market demands. DP is a proper technology to enhance the DR function. Critical Peak Price (CPP), Time-of-Use (TOU), and Real-Time Price (RTP) are the three methods for DP price determination. RTP has successfully allowed price elasticity to be estimated at different times. Therefore, this form of DP is currently utilized in developed countries.

In this research, the dynamic residential loads or the houses participated in a transitive energy market and submitted the quantity and price bids to the auction system to enable DR and DP function. In response to current demand, the substation determines the maximum power provided to the end-users and energy cost for the market. The reference bids price and control signals are transmitted to the market controller by both demanders and the supplier in a finite time interval. On the one hand, the supplier bids the maximum power and the price that it can supply to the system at a given time. On the other hand, demanders bid power they can forgo at a given price. To realistically delay communications between components, all bids and price signals are transmitted via the aforementioned ns-3 model. The bidding process is stopped after the specified time cycle, typically from 5 to 15 min. Then, the market-clearing process is started. In this process, both supply and demand bids have been sorted. Supply bids are sorted from lowest to highest. In contrast, demand bids are sorted from highest to lowest. The curves are then generated by the total quantities of these values. The intersection of curves is essentially the clearing price and the demand quantity. The passive controller in the HVAC system adjusts the thermostat control band by moving the temperature band or increasing the hysteresis after receiving the clearing quantity from the market for each time interval. This cycle continues for each interval.

4.2.3 Supported Attacks

The attack categories of GridAttackSim were constructed based on a cybersecurity guideline created by the European Union Agency for Cybersecurity (ENISA) [55]. To cover all the threats that threaten the smart grid system directly, ENISA has classified the threats into six categories based on the summarization of advanced guidelines from NISTIR 7628 [56], enhancing security throughout the supply chain (IBM Center) [57], and smart grid information assurance and security technology assessment (Sacramento State) [58], and others. The six high-level attack categories are (1) nefarious activity, (2) eavesdropping, interception, and hijacking, (3) outages, (4) unintentional data damage, (5) deliberate data damage, and (6) other threats. In the scope of this research, we focused on two well-known categories: (1) nefarious activity and (2) eavesdropping, interception, and hijacking.

A nefarious activity is defined as a deliberate action targeting the core infrastructure and the network of the smart grid system by conducting malicious activities with the intention of either stealing, altering, or destroying a specified target. It categorizes the most common threats on the smart grid system, including Advanced Persistent Threats (APTs), DNS attacks, channel jamming, generation and use of rogue certificates, identity theft, injection attacks, malicious code, social engineering, unauthorized access to systems, and web-based attacks.

Eavesdropping/interception/hijacking is the set of actions that aims to listen to, modify, interrupt, seize control, or delete the transmitted data of a smart grid communication without permission. It contains the main network-related threats, such as information theft, man-in-the-middle, network reconnaissance, routing attacks, replay of messages, smart meter connection hijacking, and wardriving.

Based on the two well-known attack categories mentioned earlier, the nine typical attack types are selected. They are organized into four groups, comprising channel jamming, malicious code, injection attacks, and replay of messages.

Channel jamming is the term used to describe the intentional actions of jamming, blocking, disrupting, or interfering with the transmission of authorized wireless communications by decreasing the Signal-to-Inference-Plus-Noise Ratio (SINR). Channel jamming is a kind of DoS attack. These attacks aim to make smart grid resources inaccessible for internal and external users. The attack targets are various layers of the network and applications, such as physical and data links.

Injection attacks are a wide range of attack vectors that enable an adversary to inject untrusted input data or code to a software system, mainly in the end-point systems. Such an attack is actualized by an interpreter as part of a command or query that changes the way the program is executed. The two variants of injection attacks are malicious code injection and malformed data injection.

Malicious code means any code in any component of a program or script that has an adverse impact, security violation, or causes destruction of a smart grid system. Depending on the installed software, these can threaten a smart grid in the functioning of all associated IT segments. Malicious code consists of numerous threats, such as exploit kits, worms, trojans, backdoor/trapdoor, service spoofing, and ICMP-flooding attacks.

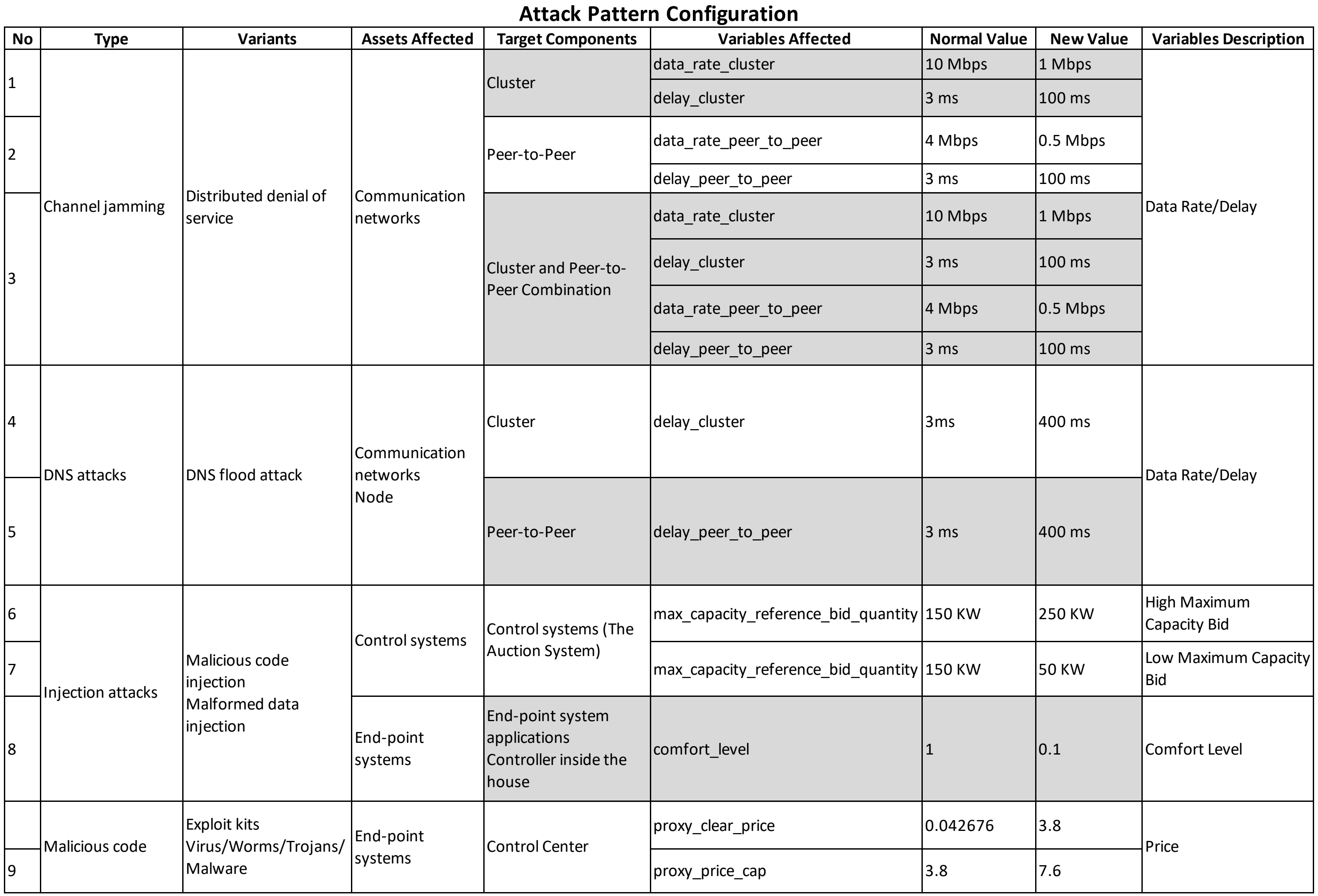
For the framework implementation, the attack simulations on a smart grid system have been conducted by altering the input values of GridLAB-D and ns-3 simulators. The configuration of the attack pattern library with the variables that need to be changed to simulate an attack is summarized in Table 4.2. Note that different types of attacks might affect the same variables, yielding multiple possibilities for diagnosis.

4.2.4 Co-simulation Management

The simulation is ready to run after the smart grid model, application, attack category, and type of attack have been selected. The model manager module calls the preprocessing module, and accesses the attack pattern library and network model. At this time, the environment is configured, and the simulation can be executed. Three terminal windows are opened, one for the ns-3 process, one for the GridLAB-D operation, and the last for the fncs_broker. Once the simulation finishes, it is possible to track what occurred in the system, how the attacks disrupted the network activity, which components were compromised, and what the consequences of the attack are, all in the same application, which is a key contribution of our GridAttackSim approach.

Data input and output are an essential part of any simulation, and simulations with the combination of FNCS, GridLAB-D, and ns-3 are no exception. After finishing the simulation, the outputs in the CSV (Comma-Separated Values) format can be loaded. It is a basic file format used mostly for storing tabular data, for example, a database or spreadsheet. Furthermore, they are the primary method for recording simulation results. The framework uses the recorder and collector objects of the GridLAB-D tape module to create aggregated values over the entire model or a time-series of selected values. The outputs can include but are not limited to

Table 4.2: The configuration of the attack pattern library



Attack Pattern Configuration

No	Type	Variants	Assets Affected	Target Components	Variables Affected	Normal Value	New Value	Variables Description
1	Channel jamming	Distributed denial of service	Communication networks	Cluster	data_rate_cluster	10 Mbps	1 Mbps	Data Rate/Delay
					delay_cluster	3 ms	100 ms	
2				Peer-to-Peer	data_rate_peer_to_peer	4 Mbps	0.5 Mbps	
					delay_peer_to_peer	3 ms	100 ms	
3				Cluster and Peer-to-Peer Combination	data_rate_cluster	10 Mbps	1 Mbps	
					delay_cluster	3 ms	100 ms	
					data_rate_peer_to_peer	4 Mbps	0.5 Mbps	
					delay_peer_to_peer	3 ms	100 ms	
4	DNS attacks	DNS flood attack	Communication networks Node	Cluster	delay_cluster	3ms	400 ms	Data Rate/Delay
5				Peer-to-Peer	delay_peer_to_peer	3 ms	400 ms	
6	Injection attacks	Malicious code injection Malformed data injection	Control systems	Control systems (The Auction System)	max_capacity_reference_bid_quantity	150 KW	250 KW	High Maximum Capacity Bid
7					max_capacity_reference_bid_quantity	150 KW	50 KW	Low Maximum Capacity Bid
8			End-point systems	End-point system applications Controller inside the house	comfort_level	1	0.1	Comfort Level
	Malicious code	Exploit kits Virus/Worms/Trojans/ Malware	End-point systems	Control Center	proxy_clear_price	0.042676	3.8	Price
9					proxy_price_cap	3.8	7.6	

the power load, clearing price, clearing quantity, and the voltages of a single node or the whole system. By using the friendly GUI, users can select the simulation outputs and then visualize the results. This function enables the users to quickly make a visual comparison between the regular operation and attack scenarios. Therefore, the behavior, impact, and consequence of the attacks can be easily recognized. Currently, line graphs and bar graphs are supported.

4.2.5 Selected Results

In this section, the results achieved in our experiments are demonstrated. The study analyzed the consequences of the simulated cyber-attacks on the energy providers and their customers in terms of financial and operational losses, total loads, clearing price, and clearing quantity. The principal objective of our research is to introduce a smart grid co-simulation environment that can be extended to simulate and analyze the various type of attacks and analyze their impact. Note that developers and smart grid researchers interested in attack simulation can easily extend the proposed framework with additional attack pattern libraries and simulation scenarios. However, only some selected results are discussed in this paper due to the scope of this study. In addition, the results of the simple test feeder, which is the smallest in this study, and the IEEE 13 node test feeder, which is the largest, are shown. The attack types selected, channel jamming and injection attack, are two of the most common attack types on the smart grid system defined by ENISA. Indeed, the co-simulation results in both metrics, including the total real-time load, current market-clearing price, current market-clearing quantity, and economic impact, are visually significant, which strongly supports cyber-security training for IT experts, cyber-security professionals, and even advanced/interested end-users.

In our study, the co-simulator uses FNCS, GridLAB-D, and ns-3 on Intel Core i7 CPU 3.1 GHz with a Linux 64-bit operating system and 16 GB DDR3 RAM to carry out the simulation. Based on the models mentioned in Section 4.2.1, we consider two typical case studies with the simple test feeder and IEEE 13 Node. In these models, the default data rate for point-to-point connectivity and local area networks are 4 Mbps and 10 Gbps, respectively. Additionally, the default transmission delays are set as three milliseconds for both. According to the available climate databases, a one-day simulation period from 00:00:00 21 July 2009 until 00:00:00 22 July 2009 was run through, using the weather information from the National Solar Radiation Database (NSRDB) of Seattle, WA, USA.

4.2.5.1 Channel Jamming Attack

The simple test feeder model is used in this case study. The GridLAB-D model comprises 255 houses participating in a transactive market. Accordingly, the ns-3 model contains a 250-node network divided into groups of 20. The default price cap and maximum capacity bid quantity are set as $3.78 and 1500 kW, respectively.

In this circumstance, we assumed that, by directly transmitting an interference signal, an adversary could completely block wireless communications, disturbing the normal operation, leading to execution problems, or even disrupting the control system. The attack was simulated by increasing the communication delays until the total load, cleared market price, and cleared quantity had been significantly affected. Eventually, the data rate of point-to-point connectivity and local area networks were sequentially adjusted from 4 Mbps and 10 Gbps to 0.5 Mbps and 1 Gbps, while the delay values were increased from 3 ms to 100 ms. The purpose of this scenario is not only to demonstrate the consequences of a chanel jamming attack but also to illustrate how a dysfunctional network system affects the energy market.

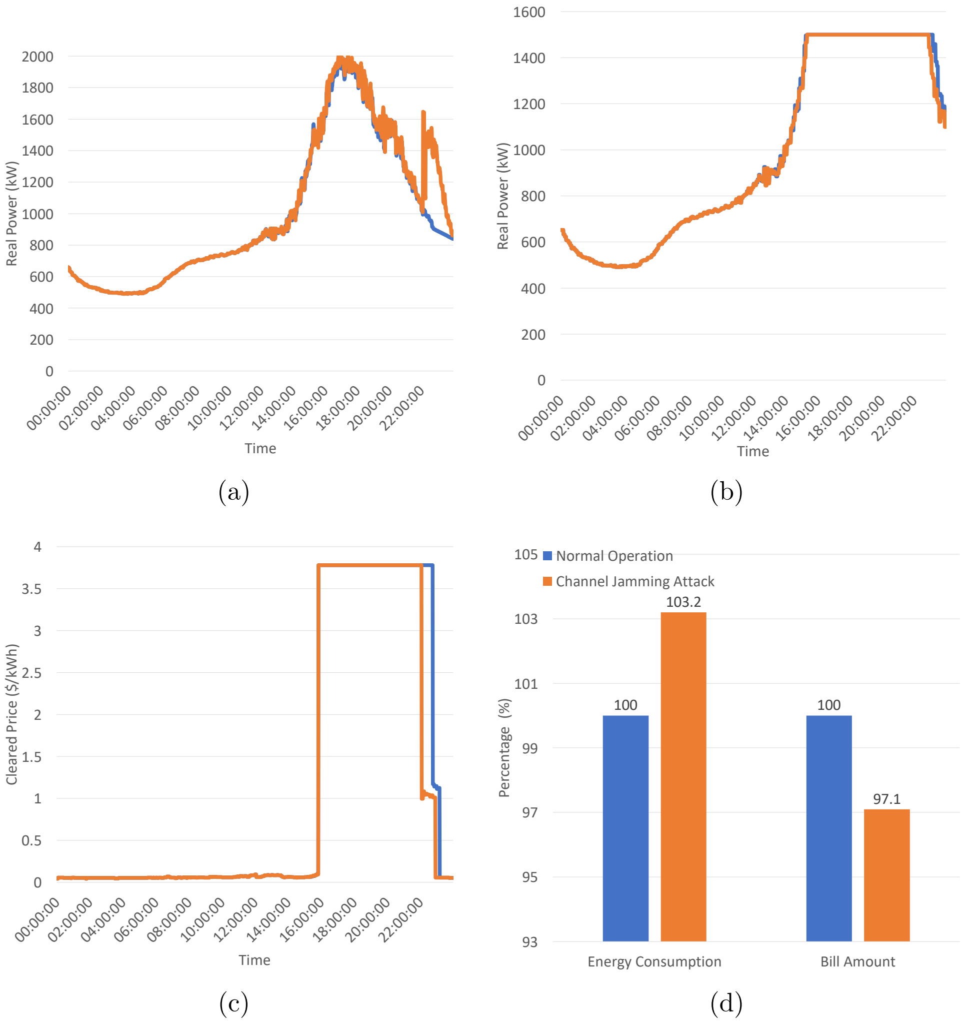
Figure 4.5 shows the results obtained in a one-day simulation for normal operation and the channel jamming attack scenarios. In Figure 4.5a, we can see the total real-time load of the system collected at the substation's meter. Figure 4.5b presents the current market-clearing quantity, while the current market-clearing price is demonstrated in Figure 4.5c. Figure 4.5d presents the economic impact of the attack. Although the clearing quantity curves are identical, the clearing price and the total load curves are partly distinct from normal and attack situations. The peak hours are noticed from around 16:00 until around midnight. At approximately 16:00, the total feeder load exceeds the market's pre-defined maximum capacity bid quantity. As a result, the market-clearing price has been increased to flatten energy consumption at the capacity limit as well as encourage more DR. Since there is more energy demand, the market-clearing price jumps to the price cap 3.8$/kWh, significantly affecting the cleared price for nearly 5 hours. At around 22:00, the clearing price curve under the channel jamming attack suddenly dropped to around $1, then slowly decreased to low prices. These low prices encouraged customers to purchase more energy. Consequently, the total load curve due to the channel jamming attack fluctuated and reached over 1600 kW. Note that, in a normal operation scenario, the clearing price and total load curves only decrease after the peak period.

These differences are caused by a significant number of delayed bids, especially re-bids later in the market interval. Since more packets have been lost under the simulated channel jamming attack, the delivery ratio of packets is statistically insignificant. If the average package delivery ratio in the normal scenario is 100%, this channel jamming attack decreases 20.14% of the typical package delivery ratio. The lack of real-time data transmission between end-users and market controllers leads to a market malfunction. Because the interval re-bids do not fully arrive at the auction system before the clearing market process, the system uses out-of-date data to calculate the bid curve. While this failure does not affect the result in most market clearings, at 22:00, the issue is sufficiently large to influence the results due to the continuously stressed system and high price. Thus, the performance of DR and DP is not obvious.

As shown in Figure 4.5d, this circumstance affords end-users significant profit; nevertheless, energy suppliers suffer considerable losses. Considering that the energy consumption and bill amount in normal operation are 100%, this attack can provoke more than 3.2% of energy consumption and a financial loss of 2.9% to the electric utility in a short period of only 24 h.

A promising option to avoid channel jamming attacks is the use of jamming mitigation technologies, for instance, the identification of trigger

Figure 4.5: Channel jamming attack with the simple test feeder: **(a)** total load, **(b)** current market-clearing quantity, **(c)** current market-clearing price, and **(d)** economic impact of the attack.



(a)

(b)

(c)

(d)

nodes, as discussed in [59].

4.2.5.2 Injection Attack

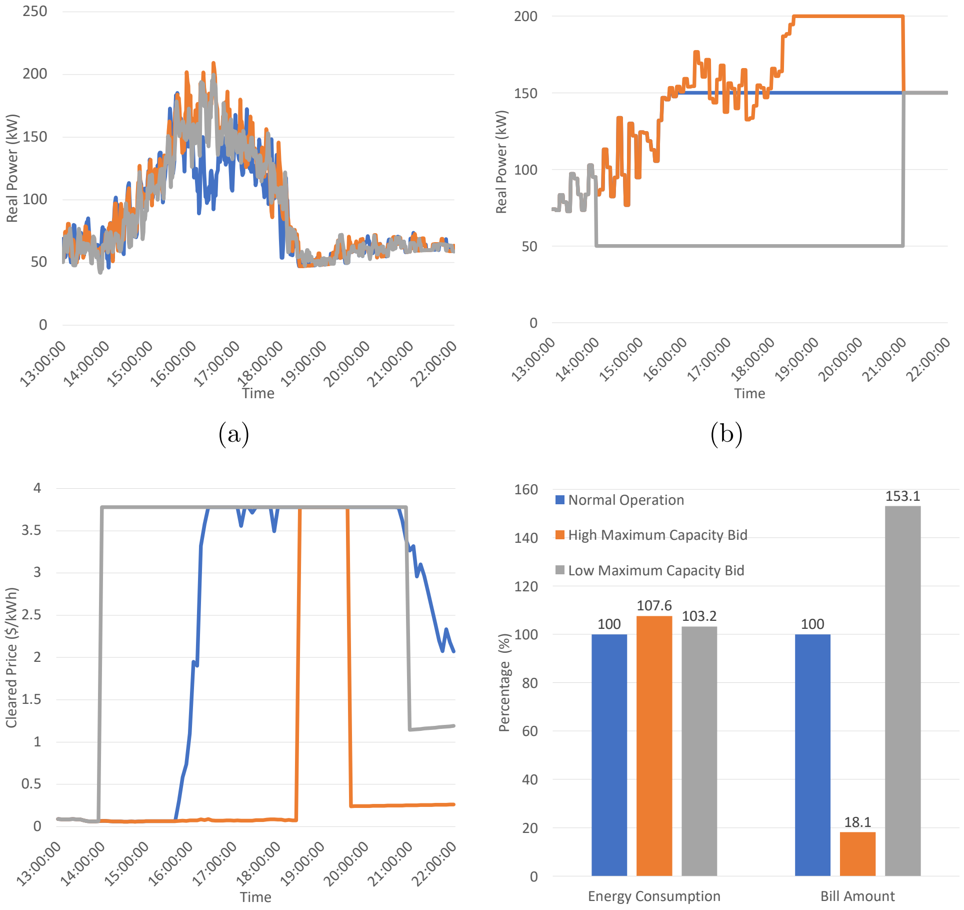
The IEEE 13 node test feeder model is applied in this case study. For the GridLAB-D model, there are 73 houses participating in a transactive market. Therefore, there are also 73 network nodes in the ns-3 model. These nodes are divided into groups of 20. The pre-defined price cap is \$3.78, and the maximum capacity bid quantity is set as 150 kW.

The false data injection attack was recently identified as a notable type of cyber attack against large-scale smart grid measurement and monitoring systems. To support their final goal of misleading the system operation and control centers, the adversaries exploit system vulnerabilities then inject malicious code to manipulate the data collected from the network. In this simulation, we assumed that the injected malicious code in the control center of the auction system could modify the maximum bid quantity from 150 kW to lower (50 kW) or higher (200 kW) values. In contrast, the default data rate and delay values are not affected in this scenario. By analyzing the total energy used, market-clearing quantity, and market-clearing price, the experiment aimed to evaluate the efficiency of the dynamic pricing as well as the performance of the DR application under the cybersecurity attack.

The results of normal operation and injection attack in a 24 h simulation, including (a) the total load, (b) market-clearing quantity, (c) market-clearing price, and (d) economic impact, are presented in Figure 4.6. The attack schedule was set as specified by the peak hours, which are from 14:00 to 21:00. Only the window of interest, including one hour before and after the attack period, is shown.

More electricity is supplied to the market by injecting a fake 200 kW maximum capacity bid. Hence, the price is comfortable most of the time except for the two-hour rush period starting from 18:00 when the clearing price suddenly jumped up to the price cap. As a result, consumers can afford to use more energy even during the rush period without being overly concerned about their monthly bills. If the energy consumption and bill

Figure 4.6: Injection attack with IEEE 13 node: **(a)** total load, **(b)** current market-clearing quantity, **(c)** current market-clearing price, and **(d)** economic impact of the attack.



(a)

(b)

(c)

(d)

amount in the normal scenario are 100%, as shown in Figure 4.6d, 107.6% of energy was consumed in this attack. Consequently, the highest total load was 210 kW in this scenario. However, the end-users paid just 18.1% of the bill amount, which means the power company dropped 81.9% of their profit in only a 9-hour period of the window of interest, from 13:00 to 22:00. This is the most profitable scenario for the end-user.

By injecting a false, small maximum capacity bid at 50 kW, less electricity is provided to the auction market. Consequently, the clearing price immediately hit the price cap at the beginning of the attack period and maintained the $3.78 value until it finished. Unfortunately, the efforts of end-users to adapt their electricity usage have limited impact, and DR function is less efficient. Therefore, the total energy consumption in this attack is 3.2% higher than the normal scenario, as depicted in Figure 4.6d. The highest total load is nearly 200 kW. This is the most severe economic impact for the end-user, with a 153.1% bill amount increase when compared to the normal scenario.

Therefore, to achieve a win-win situation between the energy suppliers and end-users, injection attacks should be considered and prevented. Various technologies to detect and prevent injection attacks are discussed in [60–65].

4.3 Summary

Based on the general smart grid cybersecurity experimentation's co-simulation approach, we designed the architecture of GridAttackSim (Cyber Attack Simulation for Smart Grids). The details of GridAttackSim's six components, consisting of the preprocessing module, attack pattern library, ns-3, GridLAB-D, FNCS broker, and model manager, were described. Both the communication network and power grid components are integrated into the designed architecture of GridAttackSim. Moreover, it enables the simulation of various attack types.

We carried out a comprehensive survey of the current approaches in this area and then introduced GridAttackSim, a smart grid cybersecurity co-simulation framework. Our approach features a stable, user-friendly interface (GUI), an extendable set of attack patterns, and a powerful attack simulation tool with an attack schedule resulting in visualization functions. Moreover, case studies with and IEEE 13 node and the simple test feeders were performed to validate GridAttackSim. Our proposed framework allows different smart grid metrics to be compared between normal operation and attack scenarios, such as the energy consumption, current market-clearing quantity, current market-clearing price, economic impact of an attack, and bill amount. Therefore, we expect that GridAttackSim can be utilized by both cybersecurity professionals and IT experts to analyze the smart grid attack consequences. In addition, it can be applied for cybersecurity training.

The network model design is the primary issue faced in GridAttackSim. The basic network model applied in our case study should not be treated as the only solution that can be created using ns-3 since it is a robust network simulator. The current framework also supports three types of test feeder, including a test system of the IEEE 13 node test feeder model. The maximum number of houses (or dynamic loads) can be up to 1000 houses. GridAttackSim simulates a combined CPS model where both the communication and power system models are jointly solved and synchronized at every iteration. Hence, for this 1000-house model, the proposed framework is doing an adequate amount of computational tasks. Since GridAttackSim is quite flexible; extending the work with a bigger network is also possible.

Chapter 5

GridAttackAnalyzer: Cyber Attack Analysis for Smart Grids

5.1 GridAttackAnalyzer Architecture

Based on an attack analysis approach where it is possible to intercorporate the different smart grid components and enable the ability to analyze different cyberattack scenarios, we introduce GridAttackAnalyzer - Cyber Attack Analysis Framework for Smart Grids, which is illustrated in Figure 5.1. GridAttackAnalyzer is centered on eight primary components: the database, smart grid model, security settings, database manager, attack analysis manager, security model generator, security model evaluator, and output.

5.1.1 Input

GridAttackAnalyzer allows attacks to be investigated and their impact to be evaluated. By using the smart grid database, these attacks are instantiated. The database structure is provided in Table 5.1. It is organized by using a structured JSON-format file. Such a database is the input to enable reconfiguration to examine a wide variety of attacks on the same smart grid architecture. This searchable database comprises three sub-modules, including the smart grid model, smart grid devices, and CVE list.

There are two essential components of a smart grid system, including the power grid and network models. Various research has been completed to model each smart grid component. On the one hand, several distribution test feeders, which vary in complexity, scale, and control data, are developed

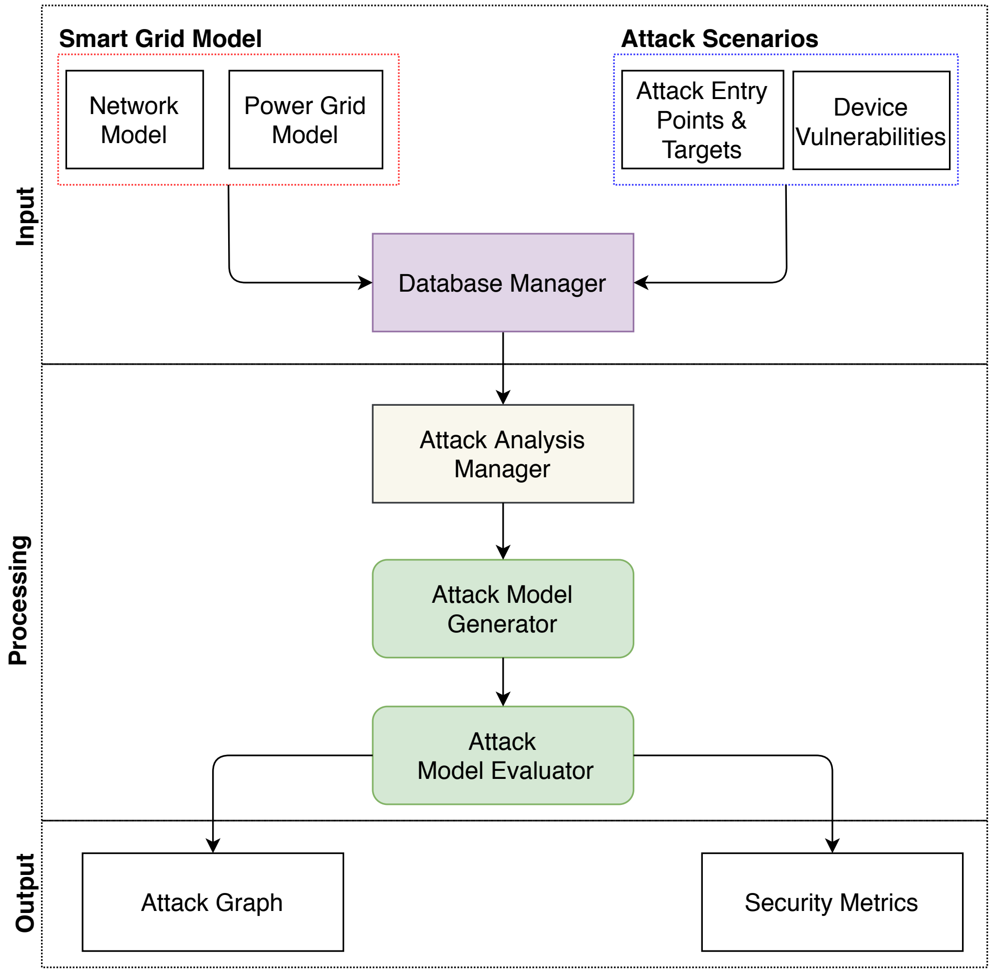
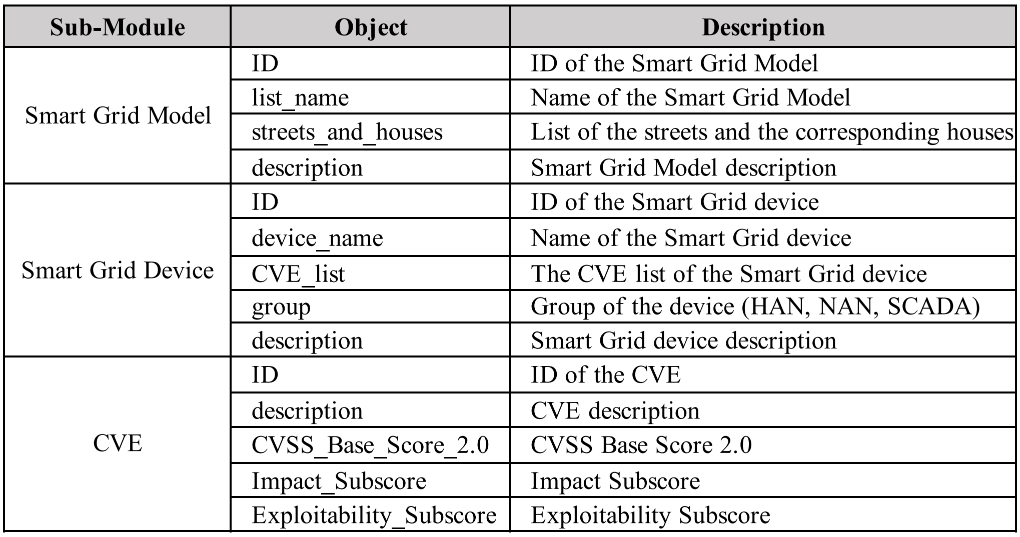


Figure 5.1: The architecture of GridAttackAnalyzer.

in recent decades. Each test feeder contains several residential loads or houses. In order to enhance the attack analysis, these houses are clustered into smaller areas. This information is stored in the database. On the other hand, numerous network architectural models were designed for the smart grid system. The connections between smart grid devices form the network model. Since GridAttackAnalyzer aims to allow the users to optimize the network model, these connections are not physically stored in the database. The network model is configured later by users.

Smart grids involve various energy measures and operations, for instance,

Table 5.1: The database structure of GridAttackAnalyzer.



Sub-Module	Object	Description
Smart Grid Model	ID	ID of the Smart Grid Model
	list_name	Name of the Smart Grid Model
	streets_and_houses	List of the streets and the corresponding houses
	description	Smart Grid Model description
Smart Grid Device	ID	ID of the Smart Grid device
	device_name	Name of the Smart Grid device
	CVE_list	The CVE list of the Smart Grid device
	group	Group of the device (HAN, NAN, SCADA)
	description	Smart Grid device description
CVE	ID	ID of the CVE
	description	CVE description
	CVSS_Base_Score_2.0	CVSS Base Score 2.0
	Impact_Subscore	Impact Subscore
	Exploitability_Subscore	Exploitability Subscore

smart meters, smart appliances, and Supervisory Control and Data Acquisition (SCADA). A smart meter or a smart electric energy meter is an equipment that measures electrical data, for example, current, electricity consumption, power factor, and voltage levels. Smart meters enhance the visibility of energy usage, power consumption behavior, and customer billing. Besides, it enables various smart grid applications, for instance, dynamic pricing and demand response. Smart appliances have the ability to respond to the dynamic pricing and demand response signals. These applications add additional value for smart grid appliances through intelligent control, power management, and network technologies. In addition, one feature of designing the smart grid's capability is incorporating SCADA systems to allow the utilities to track and control network equipment remotely. The information of these smart meters, smart appliances, and SCADA devices are organized in the database. The structure includes ID, name of the device, the CVE list of the device, group, and description.

5.1.2 Processing

Each of the smart grid devices has a corresponding CVE List. The list is collected from the National Vulnerability Database (NVD) website [66] by searching the smart grid device's name. Each CVE is stored in the database under the components of the CVE List sub-module.

The database manager module is the interface that interacts with the end-users, attack analysis manager, and database to capture and analyze an attack. It first obtains data from the database, then enables the users to select the power grid and network model from the smart grid model module, attack entry point, attack target, and vulnerability scores from the security settings module. The information is then transmitted to the attack analysis manager module to start the processing stage.

5.1.2.1 Attack Analysis Manager

The attack analysis manager, which is in the central part of the smart grid attack analysis system, serves as the engine of GridAttackAnalyzer. On the one hand, it implements the attack analysis's initialization, configuring the network model, the power grid topology, and the security setting. On the other hand, it manages the composition of the attack analysis scenarios and controls the attack model generator and attack model evaluator's execution.

When analyzing a scenario, the attack analysis manager module uses the data from the data manager module to prepare the analysis environment. Then, the data are transferred to the attack model generator for the next steps.

5.1.2.2 Security Metrics Calculation

The security metrics are calculated using the security model generator and security model evaluator modules inherited from the research in [41]. When the network is constructed, the security model generator module takes the network topology and vulnerability information as inputs to compute all possible attack paths in the smart grid network.

In this approach, a set of nodes is defined as T. There is an attack tree $at_t = (A, B, c, g, root)$ for each node $t \in T$. Attack success probability (p) is the value to measure the probability of success when an attacker is attacking the target. At the level of the node, p is measured by Eq. (5.1) for each inner node of an attack tree. The value of attack success probability at the node $t \in T$ is the attack success probability value of the root of the attack tree corresponding to the node by Eq. (5.2)

At the path level, the value of attack success probability of an attack path is also measured by Eq. (5.3). This value is the metric of the probability that an attacker can compromise the target over the attack path.

$$p_b = \begin{cases} \Pi_{a \in c(b)} p_a;\ b \in B, g(b) \in AND \\ 1 - \Pi_{a \in c(b)}(1 - p_a);\ b \in B, g(b) = OR \end{cases} \tag{5.1}$$

$$p_t = p_{root} \tag{5.2}$$

$$p_{ap} = \prod_{t \in ap} p_t;\ ap \in AP \tag{5.3}$$

Attack cost (ac) is the value of measuring the cost of an attack spent for successfully attacking a target. At the level of node, the values of attack cost are calculated by Eq. (5.4) and Eq. (5.5) for each inner node and node $t \in T$ of an attack tree. At the path level, the measure is the cost spent by an attacker to compromise the target over the attack path. This cost is calculated by Eq. (5.6).

At the network level, the measure is the minimum cost for an attacker compromising the target in the company of all possible paths. The cost of network level is given by Eq. (5.7).

$$ac_b = \begin{cases} \sum\limits_{a \in c(b)} ac_a;\ b \in B, g(b) \in AND \\ \min\limits_{a \in c(b)} ac_a;\ b \in B, g(b) = OR \end{cases} \tag{5.4}$$

$$ac_t = ac_{root} \tag{5.5}$$

$$ac_{ap} = \sum_{t \in ap} ac_t,\ ap \in AP \tag{5.6}$$

$$AC = \min_{ap \in AP} ac_{ap} \tag{5.7}$$

Similarly, the attack impact (aim) value of an attack path is computed by taking the sum of the attack values of each node. Then, at the network-level, the attack impact is the maximum value among all potential paths. The aim values are calculated by the following formulas:

$$aim_b = \begin{cases} \sum\limits_{a \in c(b)} aim_a; \ b \in B, g(b) \in AND \\ \max\limits_{a \in c(b)} aim_a; \ b \in B, g(b) = OR \end{cases} \tag{5.8}$$

$$aim_t = aim_{root} \tag{5.9}$$

$$aim_{ap} = \sum_{t \in ap} aim_t, \ ap \in AP \tag{5.10}$$

$$AIM = \max_{ap \in AP} aim_{ap} \tag{5.11}$$

The risk on attack paths (r) is defined as the expected value of the impact on an attack path. It is computed as the summation of the product of the probability of attack success pr_t and the amount of damage aim_t h belonging to an attack path ap, as following:

$$r_b = \begin{cases} \sum\limits_{a \in c(b)} pr_a \times aim_a; \ b \in B, g(b) \in AND \\ \max\limits_{a \in c(b)} pr_a \times aim_a; \ b \in B, g(b) = OR \end{cases} \tag{5.12}$$

$$r_t = r_{root} \tag{5.13}$$

$$r_{ap} = \sum_{t \in ap} pr_t \times aim_t, \ ap \in AP \tag{5.14}$$

$$R = \max_{ap \in AP} r_{ap} \tag{5.15}$$

By using the security metrics, the security evaluator can perform three functions. The first one is to output the analysis results directly. The second one is to the other to generate and export a CSV-format output file. The final function is to generate the AG automatically. In addition, attack paths are classified based on attack success probability and matching into five-level:

rare, unlikely, possible, likely, and almost certain.

5.1.3 Output

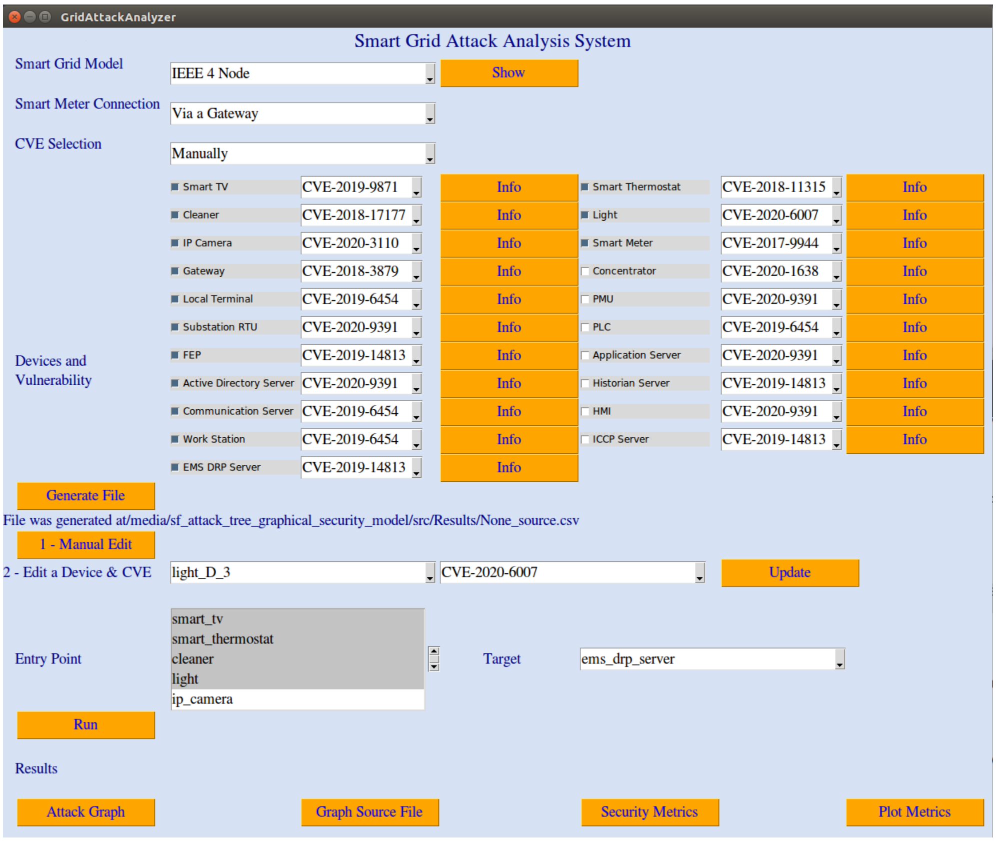
Data input and output are essential parts of any analysis system, and our attack analysis on the smart grid is no exception. AG and security metrics, including attack success probability, attack cost, attack impact, attack risk, likelihood, are the outputs of GridAttackAnalyzer. After finishing the attack analysis process, the outputs in the CSV format can be loaded. It is a simple file format used mainly to store tabular data, for instance, a spreadsheet or a database. By using the user-friendly GUI, the analytical outputs can be selected and visualized. GridAttackAnalyzer allows users to generate AG automatically. In addition, the number of attack paths is visualized based on the likelihood classification. This function facilitates the users to make a visual comparison between the attack scenarios quickly. Consequently, the characteristics of the attacks can be easily distinguished. Currently, bar graphs are supported.

5.2 Implementation and Selected Results

We discuss the proposed framework's proof-of-concept prototype in this section. Using a Python binding to the Tk GUI toolkit named Tkinter [50], the previous section's architecture has been applied to develop a smart grid attack analysis desktop application. The interface GridAttackAnalyzer is depicted in Figure 5.2.

5.2.1 Smart Grid Model

Among these test feeders, IEEE feeders [67] and PNNL taxonomy feeders [68] are widely accepted in the smart grid research community. On the other hand, numerous network architectural models were designed for the smart grid system [69], [70]. The IEEE feeders have been applied in our previous research in [18] and [71]. Therefore, the selected PNNL taxonomy feeders for


GridAttackAnalyzer

Smart Grid Attack Analysis System

Smart Grid Model: IEEE 4 Node

Smart Meter Connection: Via a Gateway

CVE Selection: Manually

Devices and Vulnerability

■ Smart TV	CVE-2019-9871	Info	■ Smart Thermostat	CVE-2018-11315	Info
■ Cleaner	CVE-2018-17177	Info	■ Light	CVE-2020-6007	Info
■ IP Camera	CVE-2020-3110	Info	■ Smart Meter	CVE-2017-9944	Info
■ Gateway	CVE-2018-3879	Info	□ Concentrator	CVE-2020-1638	Info
■ Local Terminal	CVE-2019-6454	Info	□ PMU	CVE-2020-9391	Info
■ Substation RTU	CVE-2020-9391	Info	□ PLC	CVE-2019-6454	Info
■ FEP	CVE-2019-14813	Info	□ Application Server	CVE-2020-9391	Info
■ Active Directory Server	CVE-2020-9391	Info	□ Historian Server	CVE-2019-14813	Info
■ Communication Server	CVE-2019-6454	Info	□ HMI	CVE-2020-9391	Info
■ Work Station	CVE-2019-6454	Info	□ ICCP Server	CVE-2019-14813	Info
■ EMS DRP Server	CVE-2019-14813	Info			

File was generated at/media/sf_attack_tree_graphical_security_model/src/Results/None_source.csv

2 - Edit a Device & CVE: light_D_3 CVE-2020-6007

Entry Point: smart_tv, smart_thermostat, cleaner, light, ip_camera

Target: ems_drp_server

Figure 5.2: GridAttackAnalyzer desktop application (GUI)

.

the power grid and network models applied for the smart grid case study are discussed in the scope of this research.

5.2.1.1 Power Grid Model

The increasing integration of smart grid technologies in the U.S. electricity networks highlights the significance of test feeders' availability, which allows us to study the impact of attacks for such cyber-physical models.

Due to its large size and the various utilities, the existing electricity grids in the U.S. present a wide range of topologies and equipment. Therefore, test feeders should reflect these differences based on factors, for instance, the voltage level and climate region. To respond to this demand, PNNL introduced a set of 24-node radial distribution test feeders for taxonomy representing the continental region of the U.S. in 2009. These distribution test feeders have been developed with a clustering algorithm comprising of 17 different utilities and their 575 current feeders. The continental region was divided into five climate zones to perform this categorization, where 35 associated statistical and electrical characteristics were investigated.

Among 24 prototypical feeders, the advantage of R4-12.47-2 is that it represents a combination of a moderately populated urban area with a lightly populated suburban area. Further, the less populous area is mainly comprised of single-family residences, which is ideal for our case study. The power grid infrastructure is shown in Figure 5.3. There are 352 residential houses in the system. Each house was extended by a smart meter to collect electricity consumption data. In order to enhance the performance control, these houses are clustered into five smaller areas, namely, A, B, C, D, and E.

5.2.1.2 Network Model

The infrastructure of smart grid is divided into three major communication networks, namely Home Area Network (HAN), Neighbor Area Network (NAN), and Wide Area Network (WAN) [72]. The research in [73] introduced two distinct types of HAN architecture to represent its relationship with the utility. In the first architecture, the smart meter monitors all the house appliances to manage the grid. The disadvantage of this architecture is that all devices have to communicate through the same networking protocol. Therefore, the second architecture in which all the devices connect to the smart meter through a gateway is introduced to deal with the difficulty of multiple communication protocols.

We show the smart grid communication network with the gateway based on the selected structure of the power grid in Figure 5.4. Note that the model was simplified for the purposes of our case study. The household in the network model reflects each house in the power grid model. Moreover, these households are clustered into smaller areas in the same way as the residential houses are clustered in the power grid model. Each house is equipped with

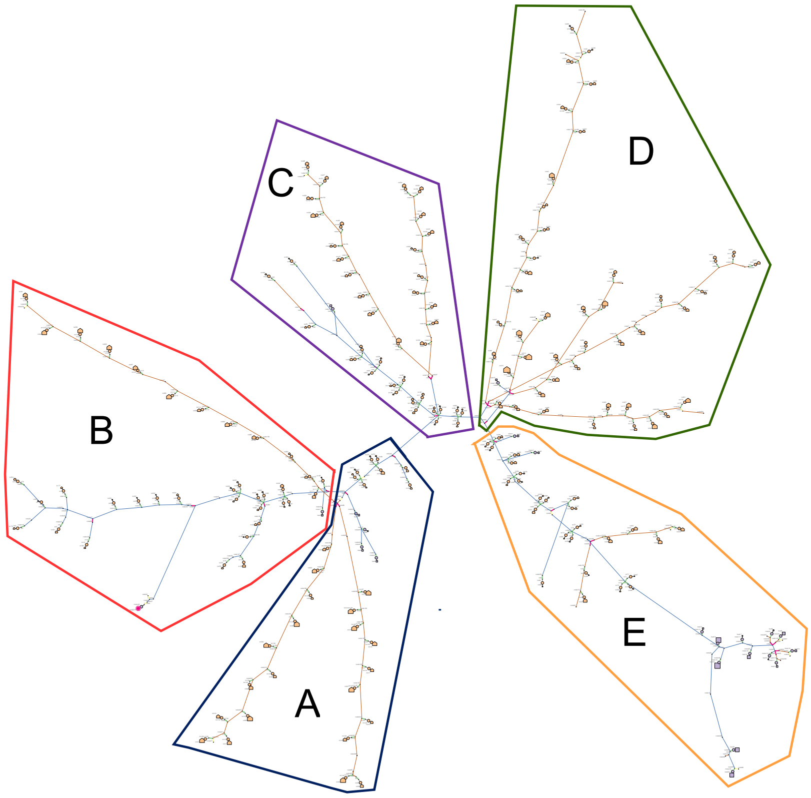


Figure 5.3: The Pacific Northwest National Laboratory (PNNL) taxonomy feeders - R4-12.47-2 [2].

.

five smart appliances, including a smart TV, a smart thermostat, a robot vacuum cleaner, a smart light, and an IP camera. The gateway handles incoming messages from the smart devices and forwards those relevant to the smart meter. Then, these data are transmitted from the smart meter to the area concentrator. Five area concentrators are corresponding with five areas A, B, C, D, E. They receive the data, then transfers it to the central concentrator. Finally, these data are gathered at the SCADA system.

Each device or node in the system is given an ID that follows a regular pattern including device name, area, and house ID. For instance, the ID of a smart TV belongs to house number 1 of area A is denoted as TV_{A_1}. Similarly, we have $Thermostat_{A_1}$, $Cleaner_{A_1}$, $Light_{A_1}$, Cam_{A_1}, $Gateway_{A_1}$, and $Meter_{A_1}$ as the IDs of the smart appliances of the area A's first house. In

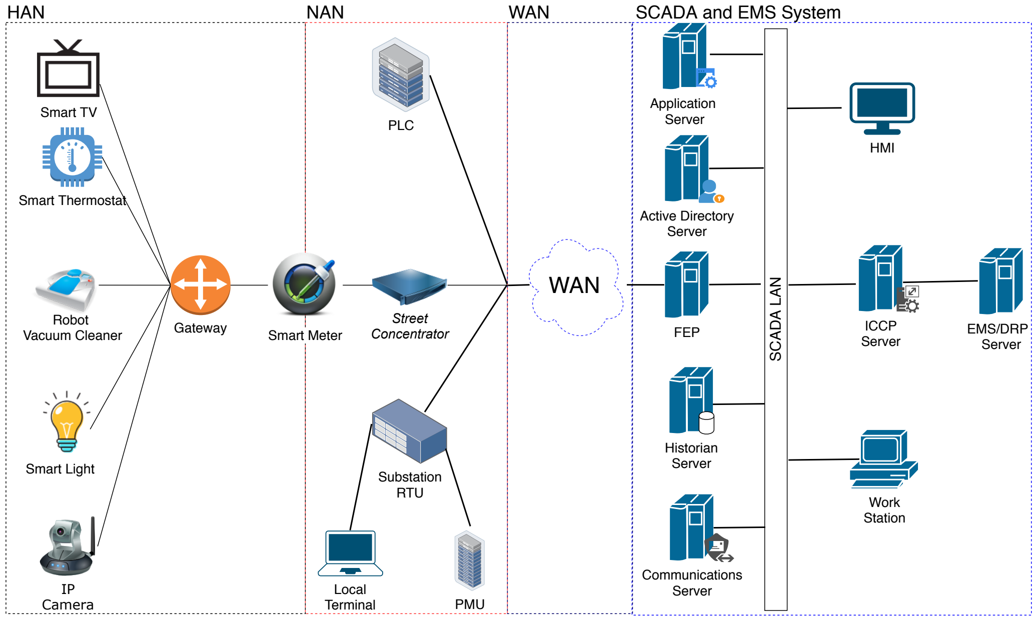


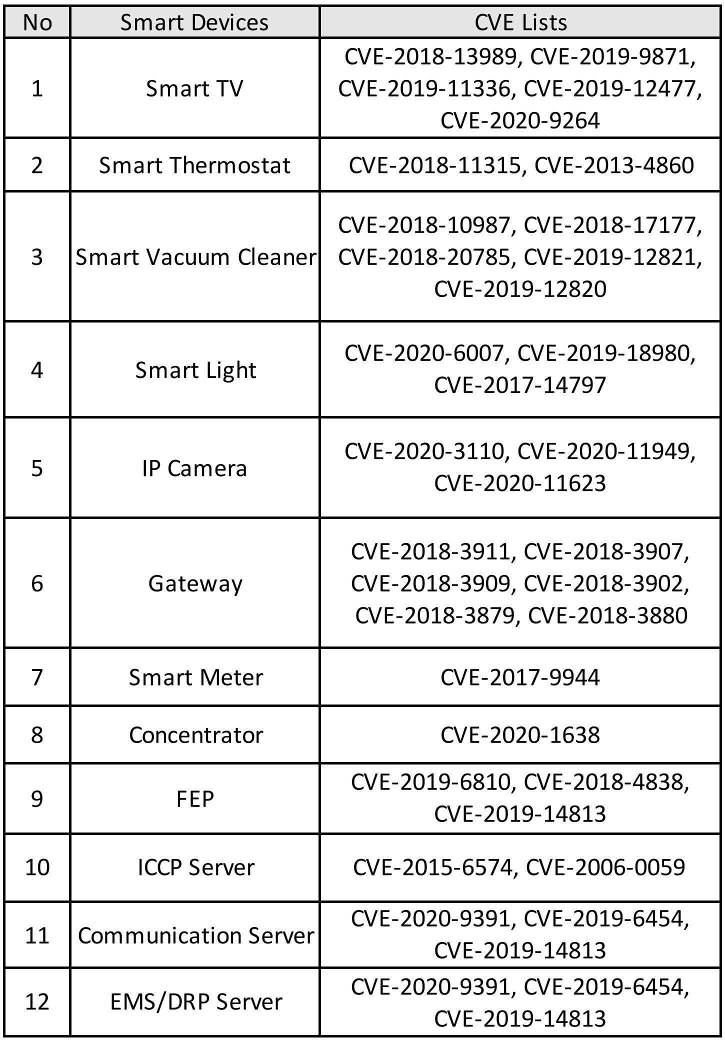
Figure 5.4: Simplified network model (part of smart grid) with gateway used in our case study.

addition, $Concentrator_A$, $Concentrator_B$, $Concentrator_C$, $Concentrator_D$, and $Concentrator_E$ represent the concentrators for each area A, B, C, D, and E, respectively. FEP, $Communication\_Server$, $ICCP$, EMS/DRP serve as the IDs for the FEP, Communications, ICCP, and EMS/DRP servers in the defined smart grid network model.

5.2.2 Devices and Vulnerabilities

A vulnerability is a weakness, flaw, or error detected inside a security system that can be taken advantage of by nefarious actors to compromise a secure network. By using sequences of commands, pieces of software, or even open-source exploit kits, hackers can exploit which vulnerabilities can be leveraged for malicious activity. In the considered circumstance, we assume that the CVE list shown in Table 5.2 was the vulnerabilities exploited by attackers. The hackers can use any HAN device, including smart tv, smart thermostats, robot vacuum cleaners, smart lights, and IP cameras, one by one or even all of them as the entry points to start an attack. Additionally, some smart grid

Table 5.2: Short CVE list for smart grid devices



No	Smart Devices	CVE Lists
1	Smart TV	CVE-2018-13989, CVE-2019-9871, CVE-2019-11336, CVE-2019-12477, CVE-2020-9264
2	Smart Thermostat	CVE-2018-11315, CVE-2013-4860
3	Smart Vacuum Cleaner	CVE-2018-10987, CVE-2018-17177, CVE-2018-20785, CVE-2019-12821, CVE-2019-12820
4	Smart Light	CVE-2020-6007, CVE-2019-18980, CVE-2017-14797
5	IP Camera	CVE-2020-3110, CVE-2020-11949, CVE-2020-11623
6	Gateway	CVE-2018-3911, CVE-2018-3907, CVE-2018-3909, CVE-2018-3902, CVE-2018-3879, CVE-2018-3880
7	Smart Meter	CVE-2017-9944
8	Concentrator	CVE-2020-1638
9	FEP	CVE-2019-6810, CVE-2018-4838, CVE-2019-14813
10	ICCP Server	CVE-2015-6574, CVE-2006-0059
11	Communication Server	CVE-2020-9391, CVE-2019-6454, CVE-2019-14813
12	EMS/DRP Server	CVE-2020-9391, CVE-2019-6454, CVE-2019-14813

devices in the substations and the SCADA system can be used as the entry points for an attack.

5.2.3 Attack Scenarios

We assumed that nearly 2% of 352 residential houses in the system, which are all of the smart devices inside seven households, contain vulnerabilities. In detail, there are two houses in each area A and B, as well as one house in each area C, D, and E, that have vulnerabilities.

Four attack scenarios were considered in this research:

1. Single-entry attack model: in this model, one type of device has vulnerabilities. Therefore, attackers can only exploit this kind of device inside the infected houses to conduct an attack. For instance, all smart TVs of seven selected houses contain different types of CVEs. Consequently, these smart TVs can be exploited by attackers as the entry points and compromised to perform further attacks. This basic scenario is used to introduce the users to the system's functions.
2. Multiple-entry attack model: in this model, all types of devices in the seven selected houses have vulnerabilities. Accordingly, attackers can potentially exploit all of these devices to carry out an intrusion. This scenario can be considered as combining all available devices in the aforementioned single-entry attacker model. This scenario aims to equip the researchers with attack analysis ability.
3. Multiple-entry attack model with patch: in this model, patching is used to fix the vulnerabilities in a specific type of device. This scenario extends the multiple-entry attacker model by integrating the patching as a defense strategy. For example, all vulnerabilities of all smart TVs inside the system have been fixed. Hence, they can not be used as the entry points by the attacker to conduct the attack. This scenario is applied to introduce the users about the patching function.
4. Massive attack model: this circumstance extends the multiple-entry attacker model by expanding the attack target to the SCADA system's core. This scenario aims to demonstrate the massive attack analysis ability of the system. The users can learn how a massive attack happens and what the consequences are.

A Front End Processor (FEP) is a computing device that interfaces to SCADA system a number of networks. For practical reasons such as avoiding the necessity for a new pair of modems, FEP can be considered a central node in the network model. On the one hand, its function is to establish a solid communication link from HAN and NAN devices, for instance, the street concentrators and substations. On the other hand, it ensures the connection with the SCADA system. FEP aims to offload the SCADA system from transmitting and receiving data, managing the peripheral devices, error correction and error detection, and packet assembly and disassembly.

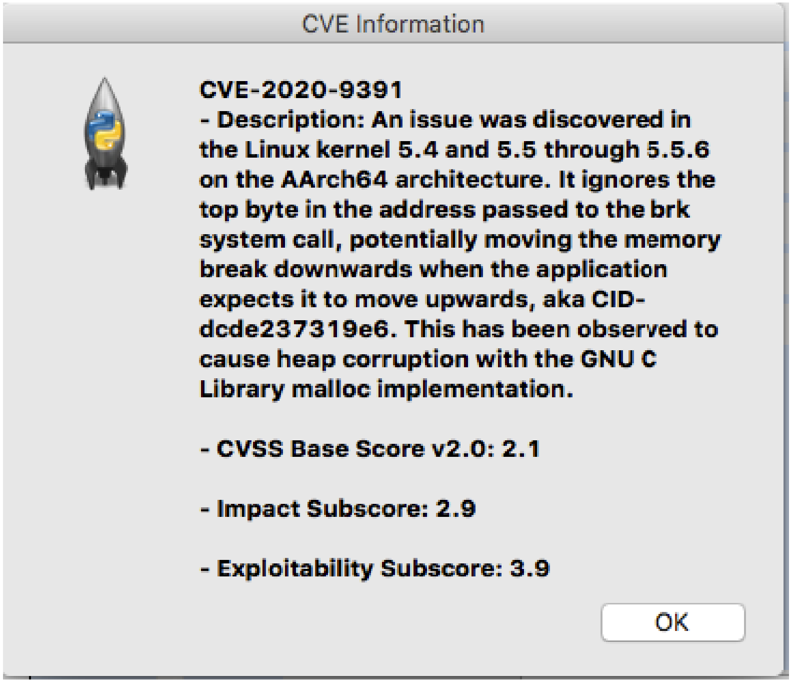
Since the power system goes through numerous operating states such as normal, alert, emergency, and restorative, EMS (Energy Management System) is designed to maintain the capability of the system by monitoring its behavior and making decisions to get it back to normal operation. Further, EMS also supports the demand response (DRP) application. The operation of EMS relies on data acquired by SCADA. It is on the top level of our applied network model.

The attack goal of scenarios from 1 to 3 is to control the FEP, while EMS/DRP is targeted in the final circumstance. If a smart grid device has more than one vulnerability, attackers can randomly select one vulnerability to conduct the attack.

Note that GridAttackAnalyzer enables users to select the smart grid devices to form a network model, as well as decide entry points and targets freely. Therefore, considered attack scenarios are not the only solutions. The system allows researchers to create new experimentation content, add and modify CVE values easily. Hence, more attack scenarios can be analyzed. Additionally, more vulnerability rates can be selected and tested. Fortunately, the result at a 2% rate is visually significant.

5.2.4 Attack Analysis Running and Results Visualization

To start an attack analysis session, a user selects a smart grid model. There is a “Show” button next to the smart grid model dropbox to visualize the smart grid model structure. Next, smart grid connection and CVE selection types should be selected. Currently, two smart meter connection types, including “via a gateway” and “direct connection”, as well as two CVE selection types, namely, “manually” and “automatically”, are supported. Devices and the corresponding vulnerability should be selected by clicking



CVE-2020-9391
- Description: An issue was discovered in the Linux kernel 5.4 and 5.5 through 5.5.6 on the AArch64 architecture. It ignores the top byte in the address passed to the brk system call, potentially moving the memory break downwards when the application expects it to move upwards, aka CID-dcde237319e6. This has been observed to cause heap corruption with the GNU C Library malloc implementation.

- CVSS Base Score v2.0: 2.1

- Impact Subscore: 2.9

- Exploitability Subscore: 3.9

Figure 5.5: An example of CVE information.

on their checkboxes. An "Info" button is located next to a corresponding CVE to show the CVE information, including CVE description, CVSS Base Score v2.0, Impact Subscore, and Exploitability Subscore. An example of CVE information is shown in Figure 5.5.

After the smart grid model, smart meter connection, CVE selection type, and devices and vulnerability are defined, the system is ready to create the source file by clicking on the "Generate File" button. This source file is a CSV-format file that contains all of the necessary data for an attack analysis session. GridAttackAnalyzer enables users to modify this source file before starting an analysis session by two options. The first option is to open the CSV-format file and manually to change the data. This option allows users to modify the source file freely. However, it is sometimes time-consuming and error-prone. Another option is selecting a specific IoT device, then update its CVE information. By using this option, the error-prone issue can be eliminated.

When the source file is ready and the entry points and targets are selected, the attack analysis session is ready to be started by clicking on the "Run" button. After finishing the attack analysis process, the outputs are stored in the CSV-format files. On the one hand, the attack graph source file, which contains the information of all attack paths, can be accessed by clicking on the "Graph Source File" button. Plus, all paths can be gathered to form an attack graph and visualized by selecting "Attack Graph" button. On the other hand, the calculated security metrics are also archived in a CSV-format file. It can be accessed by selecting the "Security Metrics" button. Finally, these security metrics can be visualized for the result comparison between different attack scenarios. Currently, bar charts are supported. Visualization examples are discussed in the next section.

5.2.5 Selected Results

By applying the mathematical formulas discussed in subsection 5.1.2.2, we calculate the security metrics values in node, attack path, and network level. These security metrics are the attack success probability (p), attack cost (ac), attack impact (aim), and attack risk (r). Based on the range of p adapted from the research at [3] and [4], the attack paths are classified into five categories, including rare ($0.0 \leq p \leq 0.19$), unlikely ($0.2 \leq p \leq 0.39$), possible ($0.4 \leq p \leq 0.59$), likely ($0.6 \leq p \leq 0.79$), and almost certain ($0.8 \leq p \leq 1$) paths. These categories are summarized in Table 5.4. The network level analysis results are shown in Table 5.3. Accordingly, the scenarios from one to five denote the results for the single-entry attack model, scenario six represents the results for the multiple-entry attack model, the scenarios from seven to eight for results from multiple-entry attack model with patch, and the last scenario represents the massive attack on the smart grid system.

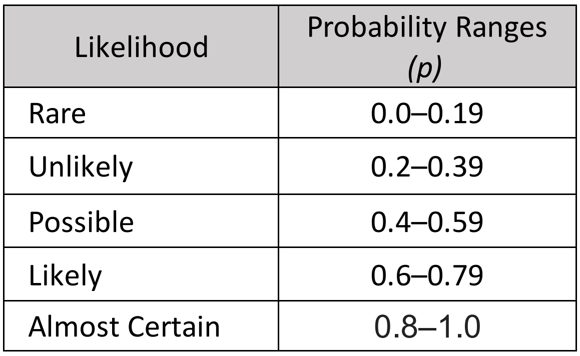
5.2.5.1 Single-entry Attack Model

We can see that attacking the smart TVs and smart lights have the maximum success probability (p) from the metrics values 1. However, the attack cost (ac) caused by compromising the smart lights is higher than for the smart TVs. Accordingly, there are 16 attack paths, which contain 8 almost certain

Table 5.3: Attack analysis results

Scenario	Entry Point	Patch	Security Metrics				Number of Paths					
			p	*c*	*aim*	*r*	**Total**	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
1	Smart TV	No	1	21.7	33.9	33.9	16	0	3	0	5	8
2	Smart Thermostat	No	0.65	19.7	33.9	22.035	16	0	2	8	6	0
3	Robot Vacuum Cleaner	No	0.86	21.7	33.9	29.154	16	1	6	2	4	3
4	Smart Light	No	1	21.7	30.3	30.3	16	1	9	2	0	4
5	IP Camera	No	0.8	19.7	33.9	27.12	16	0	7	2	5	2
6	All	No	1	19.7	33.9	33.9	80	2	27	14	20	17
7	All	Smart TV	1	19.7	33.9	33.9	64	2	24	14	15	9
8	All	Smart TV and Smart Light	0.86	19.7	33.9	29.154	48	1	15	12	15	5
9*	All	No	0.39	22.09	36.29	14.153	125	66	59	0	0	0

* Massive Attack



Likelihood	Probability Ranges *(p)*
Rare	0.0–0.19
Unlikely	0.2–0.39
Possible	0.4–0.59
Likely	0.6–0.79
Almost Certain	0.8–1.0

Table 5.4: The classification of attack paths based on the probability ranges adapted from [3] and [4].

paths, for attackers to reach the FEP via the smart TVs' entry points. Consequently, intruders are more likely to choose smart TVs as entry points.

At the network level, attack cost is the minimum cost, while attack impact is the maximum loss caused by an intruder to compromise the target among all potential paths. Therefore, an ideal path for attackers to compromise the target may not exist even in the single-entry attacker model. As an evidence, the path from TV_{A_2} to FEP, which is shown in the following, has the minimum attack cost at 21.7, maximum attack success probability at 1, and maximum attack risk (r) and impact (aim) at 33.9:

- Attackers $\rightarrow TV_{A_2} \rightarrow Gateway_{A_2} \rightarrow Meter_{A_2} \rightarrow Concentrator_A \rightarrow FEP$

However, the following path from TV_{B_1} to FEP has the maximum impact at 33.9 but lower attack success probability:

- Attackers $\rightarrow TV_{B_1} \rightarrow Gateway_{B_1} \rightarrow Meter_{B_1} \rightarrow Concentrator_B \rightarrow FEP$

After analyzing the smart grid system, attackers can determine which paths to hack based on their intention. This knowledge can be used by security experts to protect the system against an attack.

5.2.5.2 Multiple-entry Attack Model

By providing more entry devices, attackers possess more paths to conduct an attack. It is more likely that the smart grid system will be hacked since among 80 paths, there are 17 almost certain, 20 likely, and 14 possible paths, respectively. In this scenario, attackers need to spend less cost at 19.7. However, the attack impact and attack risk are highest at 33.9. Similarly, smart TVs and smart lights should be protected first in order to prevent the attackers from breaking into the system.

5.2.5.3 Multiple-entry Attack Model with Patch

We modify the vulnerability information for smart TVs or both smart TVs and smart lights separately.

Since the potential attack paths are caused by both smart TVs and smart lights, the impact of patch function on smart TVs is not obvious. The attack success probability, attack impact, and attack risk remain the same as the multiple-entry attacker model. However, the total paths have been decreased. The almost certain paths are modified from 17 to 9.

By eliminating the vulnerabilities of both smart TVs and smart lights, we decrease the attack success probability and attack risk. However, the attack cost and attack impact have not changed. This is due to the smart thermostats and IP cameras, which cost attackers less effort to compromise but can cause more significant consequences. The number of almost certain paths has been reduced to 5. Therefore, based on the analysis results, it is evident that protecting both smart TVs and smart lights is more effective than protecting either of them.

5.2.5.4 Massive Attack Model

In this scenario, attackers can use all of the HAN devices to start an attack. The target is the EMS/DRP server. Since more entry devices are provided, there are more paths to conduct an attack. There are a few serious vulnerabilities in this scenario. Therefore, the attack success probability is just 0.33, and the attack risk is just 14.15. Among 125 attack paths, there are

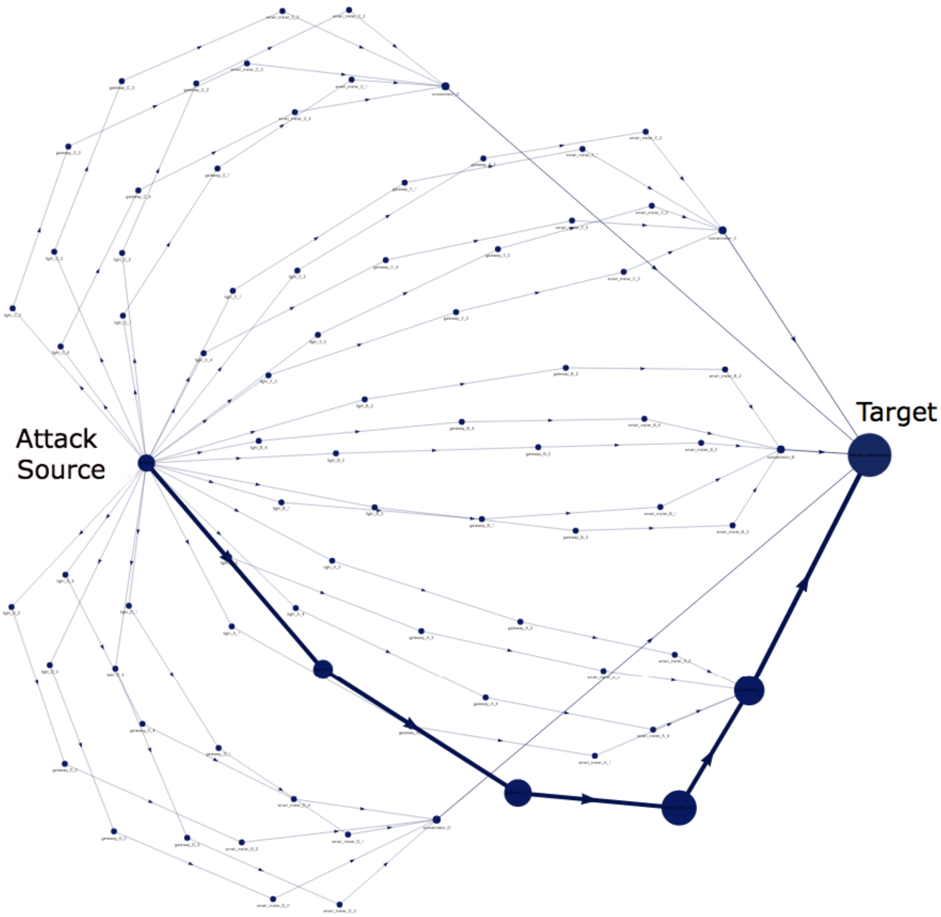


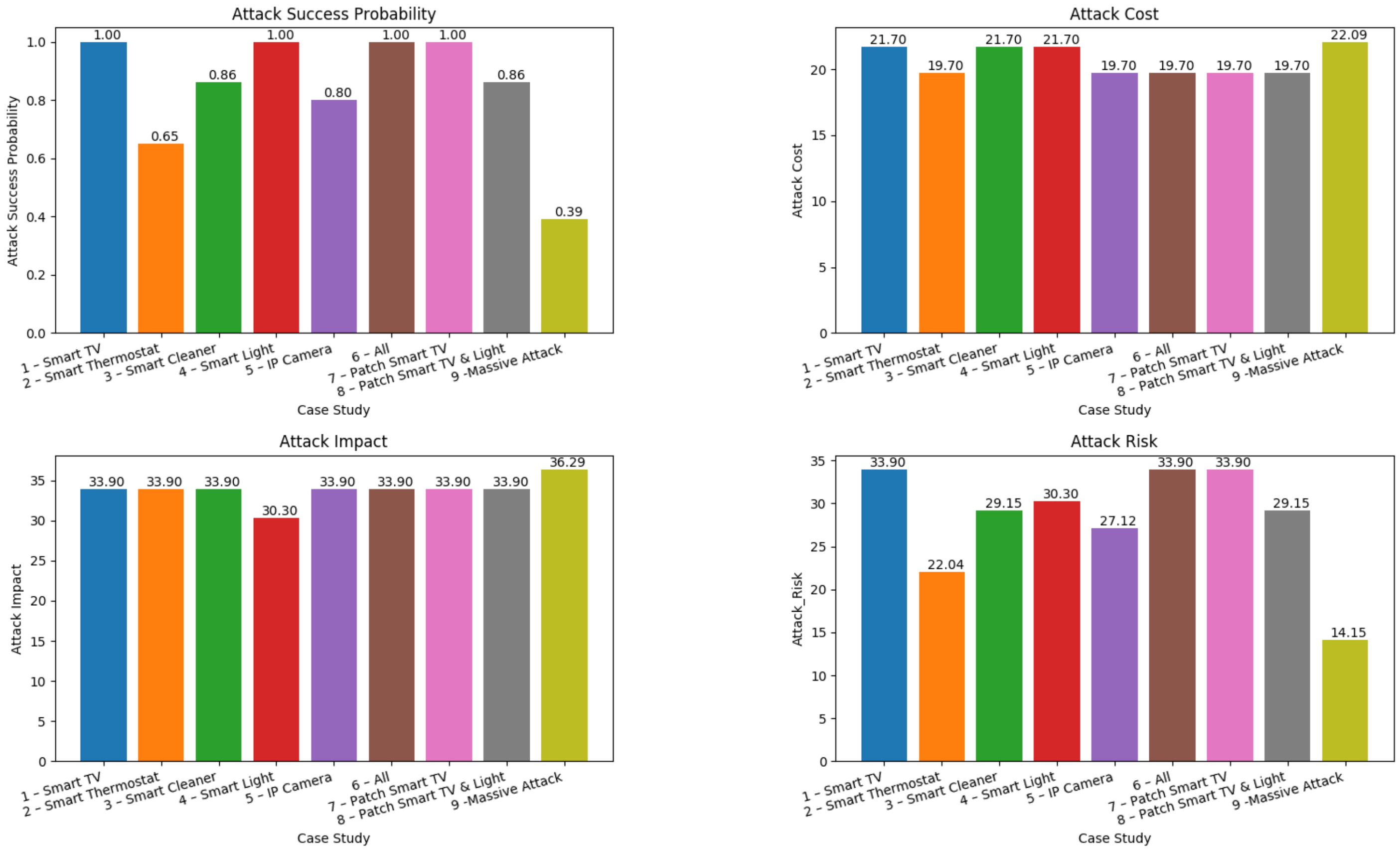
Figure 5.6: An example of attack graph generated by a case study

59 unlikely paths and 66 rare paths. However, attackers need to spend more effort since they have to compromise more devices to reach the target. The attack cost is 22.09, which is the highest in all scenarios studied. Similarly, the attack impact is high at 36.29. Therefore, more effort is required to conduct this attack. However, there is an enormous consequence if attackers achieve the target.

5.2.6 Result Visualization Example

One of the main functions of GridAttackAnalyzer is to analyze the attacks on the smart grid system. To enable users to understand the attack graph easily,

Figure 5.7: Attack analysis result visualization



GridAttackAnalyzer automatically generates the attack graphs. Using attack graphs, all of the possible attack paths for attackers to reach the targets are obvious. Plus, an attack graph that needs to be considered, for instance, the highest attack success probability, is highlighted. The automatic attack graph generation is one of our key contributions to fill the gap in the current research. An example of an attack graph generated automatically by GridAttackAnalyzer using attack success probability metrics is shown in Figure 5.6.

Along with the CSV format output files, GridAttackAnalyzer allows users to visualize the results. The security metrics, including attack success probability, attack impact, attack cost, and attack risk, can be visualized. Moreover, the number of attack paths, classified from rare, unlikely, possible, likely, and almost certain, can be highlighted in charts. The CSV-format output files' data are too numerous or complex to be represented appropriately in the text and without using substantial space. This function gives the user the ability to compare the result of different attack scenarios. Using charts, data can be displayed, and further exploration of an analysis result can be invited. An example of attack analysis result visualization is shown in Figure 5.7. Currently, the bar chart type is supported.

5.3 Summary

The architecture of GridAttackAnalyzer (Cyber Attack Analysis for Smart Grids) is designed based on the general smart grid cybersecurity experimentation's analytical modeling approach. In this chapter, the details of GridAttackAnalyzer's key components were described. The input is the combination of the smart grid model, security settings, and database to prepare the analysis session's environment. Also, the preprocessing components are employed to calculate the security metric. GridAttackAnalyzer enables the analysis of various attack types. The implementation of GridAttackAnalyzer is discussed in the next chapter.

To facilitate its use, a user-friendly GUI was developed for GridAttack-Analyzer using the Python Tkinter. To validate GridAttackAnalyzer, a case study using the smart grid network model with gateways and R4-12.47-2 PNNL taxonomy feeders was conducted.

In the vulnerability analysis process, GridAttackAnalyzer is enriched by determining all possible attack paths and calculating the selected security metrics. Crucially, our proposed framework can generate the attack graph automatically.

Chapter 6

Evaluation

In this chapter, we conduct an evaluation of GridAttackSim and GridAttackAnalyzer in terms of functionality and user evaluations, as follows:

- Functionality evaluation: the surpassing functions of both frameworks were compared with the related studies.
- User evaluation: cybersecurity researchers were invited to employ the frameworks in practice, then give feedback by filling in the System Usability Scale (SUS) evaluation forms.

6.1 Functionality Evaluation

6.1.1 Evaluation Method

Both GridAttackSim and GridAttackAnalyzer have integrated the power grid model, network model, and security components. Therefore, the two frameworks meet the requirement for cybersecurity experimentation, as discussed in Chapter 3. To highlight the surpassing functions of GridAttackSim and GridAttackAnalyzer, we compare their functionalities with the related research.

On the one hand, the comparison criteria of GridAttacksim are focused on the extendable ability of the power grid model, network model, attack type, and attack schedule, which are considered essential functions of an attack co-simulation framework. On the other hand, GridAttackAnalyzer is evaluated by comparing the ability to calculate various interest metrics, including attack success probability, attack impact, attack cost, attack risk,

Table 6.1: Functionality evaluation of GridAttackSim (Y: Yes, Blank: No)

No	Last update	Name	Extendable			Attack Schedule
			Power Grid Model	Network Model	Attack Type	
1	2011	TASSCS	Y	Y	Y	
2	2012	SCADASim			Y	
3	2014	SGsim	Y	Y		
4	2014	GridSpice	Y	Y		
5	2015	ScorePlus	Y	Y		
6	2016	ASTORIA		Y	Y	Y
7	2017	CPSA	Y	Y		
8	2018	FNCS	Y	Y		
9	2019	SimApi	Y			
10	2019	ERIGrid	Y	Y		
11	2019	HELICS	Y	Y		
12	**2021**	**GridAttackSim**	**Y**	**Y**	**Y**	**Y**

and likelihood.

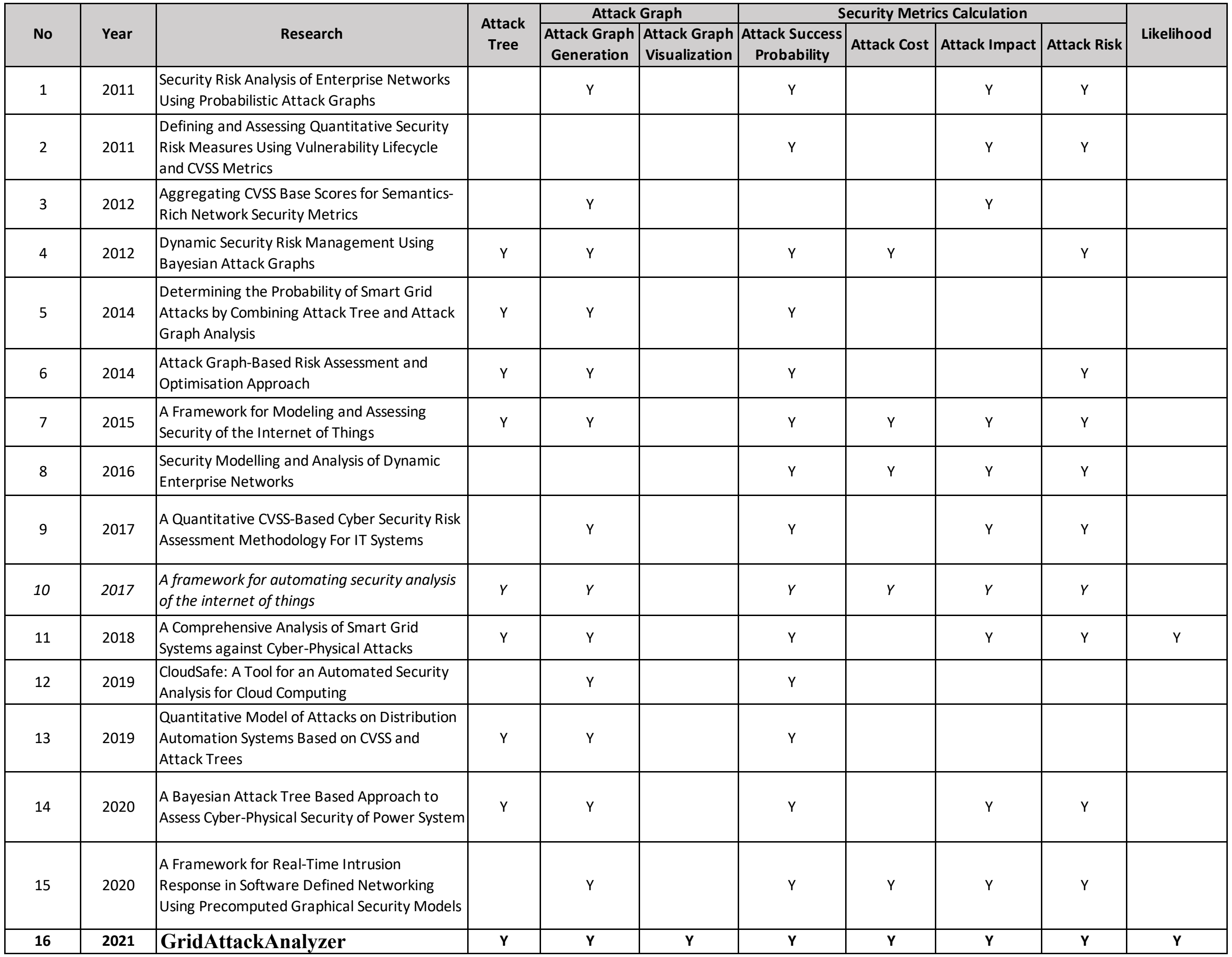
The comparison results are shown in Table 6.1 and Table 6.2, respectively.

6.1.2 Evaluation Results

The current smart grid co-simulation approaches are mainly designed for specific scenarios that are too complicated to expand. Additionally, these studies usually omit the attack schedule functionality of the co-simulation system. Further, few frameworks allow to integrate or develop a new attack type on their current system. Since many projects have been finished, the current software update and technical support are not available. Therefore, GridAttackSim is more prosperous than other related frameworks in terms of the ability to extend the power grid model, network model, attack type, and attack schedule, as shown in Table 6.1.

For smart grid attack analysis, many research did not consider the full attack metric calculation when hackers attempt to compromise the cyber system. Moreover, attack graph visualization and likelihood are also ignored in the implementation. Additionally, smart grid attack analysis is still a new area of research. GridAttackAnalyzer is one of the pioneering frame-

Table 6.2: Evaluation of GridAttackAnalyzer (Y: Yes, Blank: No)



No	Year	Research	Attack Tree	Attack Graph		Security Metrics Calculation				Likelihood
				Attack Graph Generation	Attack Graph Visualization	Attack Success Probability	Attack Cost	Attack Impact	Attack Risk	
1	2011	Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs		Y		Y		Y	Y	
2	2011	Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics				Y		Y	Y	
3	2012	Aggregating CVSS Base Scores for Semantics-Rich Network Security Metrics		Y				Y		
4	2012	Dynamic Security Risk Management Using Bayesian Attack Graphs	Y	Y		Y	Y		Y	
5	2014	Determining the Probability of Smart Grid Attacks by Combining Attack Tree and Attack Graph Analysis	Y	Y		Y				
6	2014	Attack Graph-Based Risk Assessment and Optimisation Approach	Y	Y		Y			Y	
7	2015	A Framework for Modeling and Assessing Security of the Internet of Things	Y	Y		Y	Y	Y	Y	
8	2016	Security Modelling and Analysis of Dynamic Enterprise Networks				Y	Y	Y	Y	
9	2017	A Quantitative CVSS-Based Cyber Security Risk Assessment Methodology For IT Systems		Y		Y		Y	Y	
10	*2017*	*A framework for automating security analysis of the internet of things*	*Y*	*Y*		*Y*	*Y*	*Y*	*Y*	
11	2018	A Comprehensive Analysis of Smart Grid Systems against Cyber-Physical Attacks	Y	Y		Y		Y	Y	Y
12	2019	CloudSafe: A Tool for an Automated Security Analysis for Cloud Computing		Y		Y				
13	2019	Quantitative Model of Attacks on Distribution Automation Systems Based on CVSS and Attack Trees	Y	Y		Y				
14	2020	A Bayesian Attack Tree Based Approach to Assess Cyber-Physical Security of Power System	Y	Y		Y		Y	Y	
15	2020	A Framework for Real-Time Intrusion Response in Software Defined Networking Using Precomputed Graphical Security Models		Y		Y	Y	Y	Y	
16	**2021**	**GridAttackAnalyzer**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**

works for smart grid attack analysis to the best of our knowledge. Hence, GridAttackAnalyzer is more useful than other related frameworks in smart grid application and security metrics calculation, including attack success probability, attack cost, attack impact, attack risk, as well as likelihood, as shown in Table 6.2.

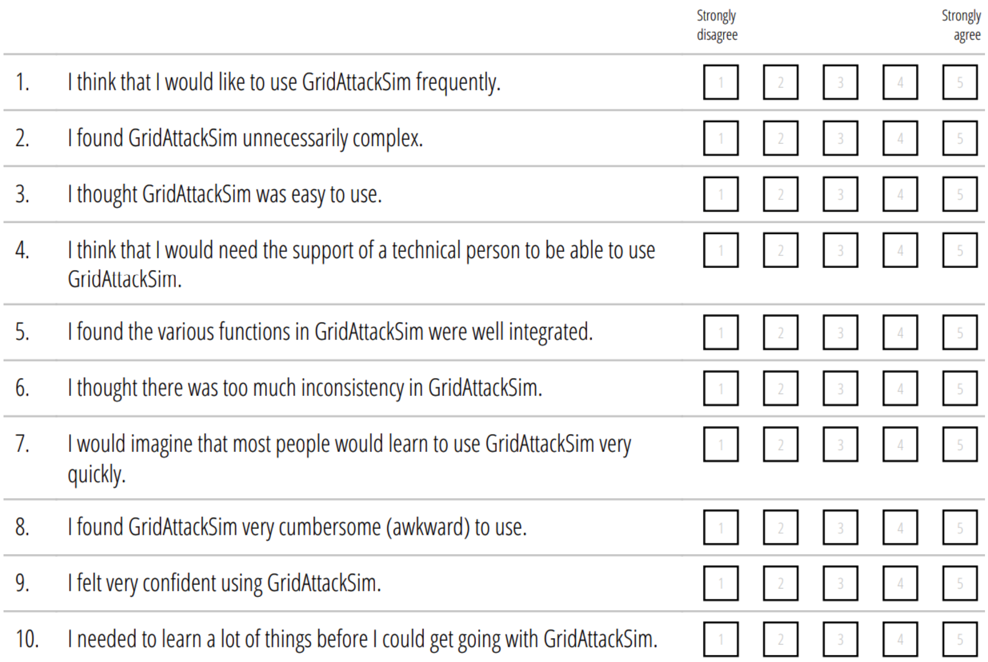
6.2 User Evaluation

6.2.1 Evaluation Method

Along with the functionality evaluation, we also conducted an external user evaluation. Particularly, ten participants, who are Ph.D. candidates in cybersecurity or related topics, were invited to use GridAttackSim and GridAttackAnalyzer. There are five participants from JAIST and five from other institutions.

We held a session to introduce the functions of GridAttackSim and GridAttackAnalyzer to each participant. After this session, a user guide was provided to the participants. Each of the 10 Ph.D. students attempted to conduct the case studies introduced in section 4.2 and 5.2. As a result, all the participants succeeded in reproducing the case studies results. Further, they were encouraged to use the frameworks to simulate and analyze new case studies. After completing the experiment, participants were asked to complete a usability questionnaire to measure their satisfaction with the frameworks' cognitive-load.

A reliable tool for measuring usability, System Usability Scale (SUS), was applied to measure users' experiences. First introduced in 1996 by Brooke [74], this well-known standardized questionnaire accounts for more than 40% of post-test questionnaire usage [75]. The structure of SUS is simple with a 10-item attitude Likert scale, ranging from 1 for "strongly disagree" to 5 for "strongly agree". Even for a small sample of participants, it has been proved to produce very reliable results compared to alternatives [76]. The outcome of SUS is a single score on a scale from 0 to 100. The qualitative interpretation of SUS scores is defined by research in [77] as follows:



		Strongly disagree				Strongly agree
1.	I think that I would like to use GridAttackSim frequently.	□ 1	□ 2	□ 3	□ 4	□ 5
2.	I found GridAttackSim unnecessarily complex.	□ 1	□ 2	□ 3	□ 4	□ 5
3.	I thought GridAttackSim was easy to use.	□ 1	□ 2	□ 3	□ 4	□ 5
4.	I think that I would need the support of a technical person to be able to use GridAttackSim.	□ 1	□ 2	□ 3	□ 4	□ 5
5.	I found the various functions in GridAttackSim were well integrated.	□ 1	□ 2	□ 3	□ 4	□ 5
6.	I thought there was too much inconsistency in GridAttackSim.	□ 1	□ 2	□ 3	□ 4	□ 5
7.	I would imagine that most people would learn to use GridAttackSim very quickly.	□ 1	□ 2	□ 3	□ 4	□ 5
8.	I found GridAttackSim very cumbersome (awkward) to use.	□ 1	□ 2	□ 3	□ 4	□ 5
9.	I felt very confident using GridAttackSim.	□ 1	□ 2	□ 3	□ 4	□ 5
10.	I needed to learn a lot of things before I could get going with GridAttackSim.	□ 1	□ 2	□ 3	□ 4	□ 5

Figure 6.1: SUS questionnaire for GridAttackSim

- $0 \leq$ SUS Score < 36: Poor
- $36 \leq$ SUS Score < 51: OK
- $51 \leq$ SUS Score < 72: Acceptable
- $72 \leq$ SUS Score < 85: Good
- SUS Score ≥ 85: Excellent

The questions used in the questionnaire for GridAttackSim is shown in Figure 6.1, and is the same as the GridAttackAnalyzer's SUS questionnaire. Among the 10 questions, five are positive and five are negative, whereby a negative item alternates each positive. By alternating these negative and positive statements, the participant is made to read every question and try to think whether they agree with it or not.

The score contributions from each question, ranging from 1 to 5, were used to calculate the SUS score as follows:

- The score contributions from the odd items: the scale position minus 1.

Table 6.3: SUS Results for GridAttackSim and GridAttackAnalyzer

No	Frameworks	Maximum Value	Minimum Value	Mean	Standard Deviation
1	**GridAttackSim**	87.5	55	74.3	9.5
2	**GridAttackAnalyzer**	90	60	72.2	10.2

- The score contributions from the even items: 5 minus the scale position.

$$Score_i = \begin{cases} a_i - 1, & \text{if } i\%2 \neq 0 \\ 5 - a_i, & \text{if } i\%2 = 0 \end{cases} \tag{6.1}$$

- The overall SUS value in the range of 0 to 100: the 10 question's total score is multiplied by 2.5.

$$SUS_j = 2.5 \times \sum_{i=1}^{10} Score_i \tag{6.2}$$

The average SUS score was calculated by the 6.3 equation where n is the number of participants.

$$\overline{SUS} = \frac{\sum_{j=1}^{n} SUS_j}{n}, n \in \mathbb{N} \tag{6.3}$$

6.2.2 Evaluation Results

The analysis reflects the result values of SUS for GridAttackSim and GridAttackAnalyzer, which are shown in Table 6.3. Standard deviation, which is the dispersion measure of a data set from its average, was calculated by the 6.4 equation where σ is the data standard deviation, N is the data set size, x_i is defined for each value, and μ is the mean of the data set.

$$\sigma = \sqrt{\frac{\sum(x_i - \mu)^2}{N}} \tag{6.4}$$

The SUS mean score is 74.3 for GridAttackSim and 72.2 for GridAttack-

Analyzer, respectively. These mean scores can be considered as acceptable (SUS $>$ 70) for both frameworks. The standard deviation are 9.5 and 10.2 for GridAttackSim and GridAttackAnalyzer. Also, the minimum scores are above 51, which is acceptable for both frameworks. Comparing these usability values, we can see that the users were satisfied with the frameworks' usability.

6.3 Summary

In this section, the functionality and user evaluations of GridAttackSim and GridAttackAnalyzer were conducted.

For the functionality evaluation, the surpassing functions of GridAttackSim and GridAttackAnalyzer were compared with the related research. The results show that our frameworks are more useful than other related frameworks in terms of comparison criteria.

For the user evaluation, ten cybersecurity researchers were invited to use GridAttackSim and GridAttackAnalyzer and then gave feedback based on the System Usability Scale (SUS) questionnaire. The SUS scores were calculated. The results show that users were satisfied with the usability of GridAttackSim and GridAttackAnalyzer.

Chapter 7

Discussion

7.1 Physical Attack Simulation and Analysis

As evidenced in the actual smart grid incidents mentioned in Section 1.2, cyber-attacks can lead to disturbances that transcend the virtual world and damage the physical system. In other words, physical attacks on the smart grid can affect the system's stability, leading to loss of load. As a result, power stakeholders, including utility companies, transmission system operators, and distribution system operators, may face severe economic pressures. Therefore, it is essential to undestand the consequence of a physical attack on the smart grid system.

Compromising the availability, integrity, or confidentiality of a part of cyberinfrastructure is the first step that an attacker needs to conduct before attempting to damage the physical smart grid system. GridAttackAnalyzer is mainly designed to analyze an attack's characteristics in terms of attack tree, attack graphs, and security metrics. Therefore, utilizing GridAttackAnalyzer is a preliminary approach to understanding the effect of a physical attack on smart grid systems.

In GridAttackSim, various metrics, including the total load, current market-clearing quantity, current market-clearing price, economic impact of an attack, and bill amount, can be measured and compared both in normal operation and attack scenarios. At the core of GridAttackSim, GridLAB-D can simulate and monitor the characteristics of substations, meters, power lines, and residential and devices inside these loads, including clothes washer, dishwasher, dryer, microwave, occupant load, plug load, refrigerator, and water heater. These characteristics can include the voltages, phases, real and imaginary components of a specific smart grid device. Moreover, these values can be aggregated as a maximum, minimum, average, count, mean, standard deviation, mean bias error (1st moment), variance (2nd moment), or kurtosis (3rd moment) [78]. Therefore, while we have not conducted such experiments, by leveraging the functionality of GridLAB-D, GridAttackSim potentially has the ability to simulate the consequences of a physical attack on the smart grid system.

By combining the functionalities of both GridAttackSim and GridAttack-Analyzer, the characteristics and consequences of an attack on the smart grid physical system can be simulated and analyzed.

7.2 Potential Applications

7.2.1 Application for Research

The conceptualization and realization of engineered systems, of which the smart grid is one of the most prominent cyber-physical systems, have often needed significant consideration in all the development process stages, from the requirement analysis, design and validation, to the implementation.

Testing a smart grid system is not a trivial activity since it entails high risk of destroying the electrical infrastructure and equipment, resulting in enormous economic consequences or even danger to human lives. As a result, in this critical domain, where testing on a real system is prohibited, simulation techniques can be considered an effective solution. With the combination of the power grid and network models, GridAttackSim can be employed for the animation and assessment of smart grid behavior, to identify device vulnerabilities and corrective strategy in various attack scenarios before its implementation. Therefore, for smart grid system developers, GridAttackSim can be used not only to assess the consequences of various attack types but also to enable early development and evaluation of new anomaly detection and mitigation methods before their implementation. Since GridAttackSim enables researchers to create new attack models freely, it allows the experimentation and validation of the proposed attack modeling approach in a realistic case study. Moreover, the framework can be used to determine the most effective approaches to implementing smart grid technology, particularly for communicating specifications for effective system operation.

Conventional planning and management of information security starts with risk evaluation, which identifies risks to critical components and the corresponding loss expectation. Several researchers have suggested risk management approaches by constructing network protection models, utilizing paradigms such as attack trees and attack graphs, and then defining attack paths in these models. Unfortunately, most of these models fail to consider the capabilities of the attackers; for instance, the likelihood of a specific attack being conducted. Without the factors mentioned above, security threats and their consequences might be misjudged. Therefore, by examing security metrics, smart grid researchers can use GridAttackAnalyzer to investigate all potential attack paths, then determine which device included in the paths should be protected first. Additionally, the effectiveness of device-specific management strategies can be compared. The performance of the smart grid system's defense strategies can be measured at the network level. Moreover, GridAttackAnalyzer can help researchers estimate the attack's damage cost on the proposed smart grid system.

7.2.2 Application for Training

7.2.2.1 Overview

The Japanese National Center of Incident Readiness and Strategy for Cybersecurity (NISC) reported that cybersecurity personnel are not adequately trained and is insufficient [79]. The CSIS 2016 survey found that only 23% of educational programs in the USA adequately train graduates to enter the cybersecurity industry [80]. In 2018, the professional association ISACA found that 61% of companies participating in a survey believed that less than half of the candidates for cybersecurity jobs were qualified for the position [81]. These problems are caused by the current competence gap between knowledge, practical experience, and essential soft skills acquired from the cybersecurity training programs and the actual demands from the organizations.

IT professionals, cybersecurity specialists, and end-users must acquire a thorough knowledge of preventing and responding to these security incidents. However, Information and Communications Technology (ITC) issues, such as integrating renewables, computer networks, and cybersecurity, are usually not fully covered in conventional training and education approaches. There is a need for realistic cybersecurity training for smart grids. To fill the gap in the current research, the smart grid realistic cybersecurity training design requirements should be clarified. Furthermore, realistic cybersecurity training for smart grids should be implemented by applying these design requirements. To the best of our knowledge, this is one of the first studies aimed at addressing this current issue in the field.

The research in [82] identified three main components for a typical cybersecurity training system:

- Attack-oriented training: including practical activities on penetration testing, using the same tools and methodologies applied by real attackers.
- Defense-oriented training: focusing on the vulnerability protection mechanisms to strengthen system security.
- Analysis/forensics-oriented training: providing a deeper understanding of the vulnerability exploitation and patching.

These categories are not mutually independent, and cybersecurity professionals can only accomplish the readiness required to resolve cybersecurity incidents effectively through their combination. All training exercises should be conducted based on real-world situations. Complex network environments are typically required to simulate attacks in real circumstances, particularly the system settings and network topologies.

The prior research from [83] also indicated the requirements that should be met to conduct training exercises that prepare trainees for realistic incidents:

1. All three aspects of cybersecurity training, including attack, defense, and forensics, should be combined in the training activity.
2. The system should have the ability to actively "respond" to the activities of trainees, for instance, via appropriate defense strategy for attack training and suitable attacks for defense practice.
3. Trainers should adequately manage the hands-on exercises, both in scenario reproducibility and training content.
4. To enhance the effectiveness and reach, there should be a low entrance barrier for participating in the training.

By integrating a training content component in the smart grid cybersecurity experimentation general architecture, as shown in Figure 7.1, our proposed framework can support cybersecurity training activity.

7.2.2.2 Training Content

Training content is an essential part of any training system. It includes all resources and information given to trainees to develop their cybersecurity awareness and abilities. Training content can be in various forms, for instance, text, static video and visual, audio, and interactive factors. What content should be included in the training course depends on the objective and desired outcome. A realistic smart grid cybersecurity training system should be designed to convey the training contents to the learners effectively. This training content should be organized and stored in the database properly. Further, there should be no barrier for trainers to create new training content or modify the existing training content. There are various smart grid cybersecurity guidelines from renowned institutions, such as NIST [56], the European Union Agency for Cybersecurity (ENISA) [55], Smart Grid Information Assurance and Security Technology Assessment (Sacramento State) [58], and IBM Center [57]. Many common attack types, which should be considered, are identified and classified in these guidelines. Moreover, various case studies that can be used for cybersecurity training are shown. Therefore, the designed system should be able to support the application of the training content extracted from these guidelines.

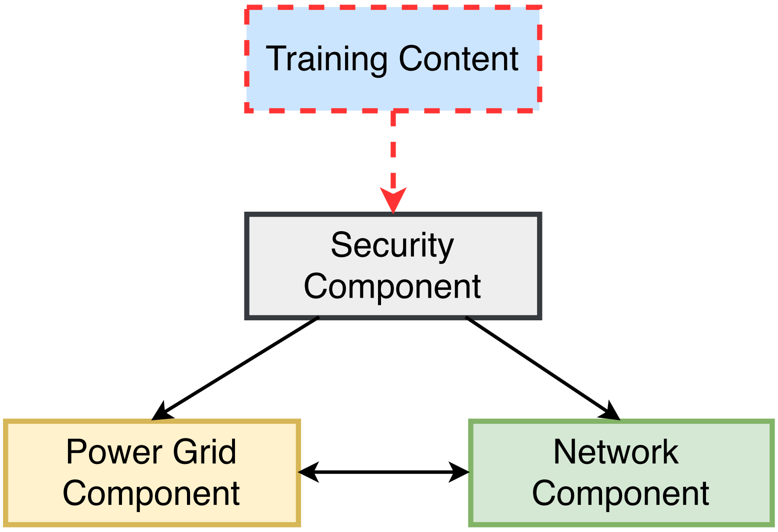


Figure 7.1: Cybersecurity training for smart grids in general

The co-simulation approach should be able to simulate the various types of attacks on the smart grid. Therefore, its training content should be designed to educate trainees on the attack characteristics. Additionally, the training content should include knowledge about the power grid and network communication, which are the smart grid's two primary components. A more in-depth understanding of these systems is essential to appreciating the smart grid system's complexity.

The analytical modeling approach should be able to analyze different types of smart grid attacks. The publicly known information-security vulnerabilities and exposures database should be used to form the training content. Hence, the attacks' consequences can be highlighted in the training content. Moreover, the attack path should be included in the training content to inform trainees on how the hacking attempt is successful.

The reciprocal relationship between our proposed requirements for a realistic smart grid cybersecurity training and the general realistic cybersecurity training is clarified as:

1. The combination of power grid, network, and security components provides the ability to conduct both three aspects of cybersecurity training, including attack, defense, and forensics.

2. The system can actively respond to trainees' activities when carrying out a power grid and network simulation or analysis.
3. Trainers can modify the security component to adjust the hands-on exercises, both in training content and scenario reproducibility. The structure, architecture, and model of the power grid and network components can be easily modified to accommodate the training demand.
4. Since there are just three main components, the system's complex can be mitigated. Therefore, a low entrance barrier for participating in the training can be satisfied.

GridAttackSim advances the recreating vulnerability manipulation strategies experience and involves exercises, for example, using the same techniques used by attackers. Furthermore, it allows the cybersecurity defense methodologies design and implementation to anticipate similar future attacks. Hence, it can support (1) attack-oriented training and (2) defense-oriented training.

GridAttackAnalyzer enhances trainees' more in-depth knowledge of the phenomenon relevant to exploitation and patching of vulnerabilities. Hence, it can support analysis/forensics-oriented training.

7.3 Summary

In this section, we introduced the ability to simulate and analyze the physical attack of GridAttackSim and GridAttackAnalyzer. The characteristics and effects of an attack on the smart grid physical structure can be simulated and evaluated by integrating the two frameworks' functionalities.

In addition, the potential applications of GridAttackSim and GridAttack-Analyzer for research and training activities have been discussed.

On the one hand, experimenting with a smart grid system is not trivial because it carries a high risk of electrical infrastructure and equipment destruction, which has enormous economic implications or harmful effects on our lives. Therefore, GridAttackSim and GridAttackAnalyzer can be considered as an effective solution for smart grid research activity.

On the other hand, cybersecurity personnel are not adequately trained and the training provided is insufficient. Our proposed framework can enhance the cybersecurity training activity by combining the training content component with the smart grid cybersecurity experimentation general architecture. Hence, GridAttackSim and GridAttackAnalyzer can be seen as practical applications for smart grid training activities.

Chapter 8

Conclusion and Future Work

8.1 Summary and Contributions

We are in the Society 5.0 era, when technology is transforming the way people live, communicate, and interact with each other. One of the critical elements of Society 5.0 is the smart grid, which includes the network and power grid components. In recent years, there have been several cyber attacks on smart grid systems that have caused significant repercussions, such as loss of confidential data, blackouts, power equipment destruction. Therefore, it is essential to protect smart grid systems against cybersecurity attacks.

The smart grid structure is complex, having two essential parts: network communication and the power grid. Researchers need to consider the relationship between these components for further system investigation and improvement. Evidently, it is not a trivial activity to implement a real smart grid system for the cybersecurity experiment and validation process since it entails high risks for destroying the electrical infrastructure and equipment, resulting in enormous economic consequences or even potential loss of for human lives. As a result, in this critical domain, where testing on a real system is prohibited, simulation and analysis techniques can be considered an effective solution to reach the goal.

The attack simulation and analysis tools are mainly applied to simulate attacks and emulate the actual circumstances in which these attacks occur, particularly system settings and network topologies. The application of the real incidents simulation tools for cybersecurity experimentation is believed to be the primary factor in enhancing the efficacy of the experimentation process. Due to its novel status, few research studies have focused on practical cybersecurity experimentation for smart grids. To the best of our knowledge, the present research is one of the first works to address this current issue in the field.

This dissertation identified the need for practical cybersecurity experimentation for the smart grid. We indicated the system design specifications as one of the key contributions. Furthermore, a general smart grid cybersecurity architecture that satisfies these requirements was implemented. To deal with the complications of the system but still accomplish our objective, the smart grid cybersecurity experimentation is divided into two parts: co-simulation and analytical modeling approaches. Their requirements and general architectures were defined.

Although both communication networks and power grids can be simulated by current technologies, they are usually designed for small and limited networks. Therefore, we implemented ns-3, a robust network simulator, and GridLAB-D, a feature-rich power grid simulator, to tackle this issue. In addition, as they support different programming languages, external libraries, and APIs, our GridLAB-D and ns-3 can be extended easily. However, this interoperation introduces numerous challenges, such as time synchronization, differences in time scales, flexible model reuse, and data transmission delays. One promising direction to deal with this problem is applying the FNCS broker to efficiently control and handle this combination.

One of our contributions is the introduction of GridAttackSim, a framework that reproduces a real smart grid environment with different cybersecurity attacks and then assesses their effects, all in one place. In addition, built-in attack profiles and the user-friendly GUI enable users to execute simulations and analyze the results automatically without a thorough knowledge of software technology, abstracting the underlying complexity of the integration tools. While most related studies support a few types of attacks, more types of attacks can be included in GridAttackSim due to the extensive pattern library for IT experts and electrical utilities interested in enhancing smart grid security. Although the attack schedule function has been omitted by most of the current research, GridAttackSim fills this gap by introducing the attack schedule capability.

It is possible to implement the framework for cybersecurity training for customers. For example, visualizing graphics allows end-users to understand the economic consequences of attacking smart grid systems. For system operators, the framework can be used to evaluate the effects of different types of attacks and enable the early development and assessment of new methods for the detection and mitigation of anomalies prior to their implementation. The framework can also be applied to identify the most efficient smart grid technology implementation strategies, particularly for communicating specifications for effective system operation.

Significantly, cybersecurity is at the core of modern technologies. In this research, we conducted a comprehensive and systematic survey of various attack analysis studies using the combination of Graphical Security Model (GrSM) and CVSS. We reviewed the state-of-the-art techniques, ranging from traditional networks to emerging technologies for the smart grid. Numerous metrics of interest have been examined to accomplish this goal, namely, Attack Tree (AT), Attack Graph Generation (AGG), Attack Graph Visualization (AGV), attack success probability (p), attack cost (ac), attack impact (aim), attack risk (r), likelihood, and smart grid application.

As cyber attacks on the smart grid systems can cause serious issues, protecting the smart grid system from attackers is extremely important. Attack analysis is one of the advanced technologies to investigate and evaluate attackers' activities. This information is invaluable to defense of the smart grid system. However, there is little research focus on smart grid attack analysis using GrSM.

We introduced GridAttackAnalyzer, a smart grid attack analysis framework. By applying the PNNL Taxonomy Feeders R4-12.47-2, smart grid network model with the gateway, a smart grid case study with four attack scenarios, including a single-entry attack model, multiple-entry attack model, multiple-entry attack model with patch, and massive attack model, has been carried out. All potential attack paths have been determined, and the values of the selected security metrics have been calculated during the vulnerability analysis process. Further, our research is enriched by the automated Attack

Graph generation capacity.

This knowledge can be used for cybersecurity training of IT experts and cybersecurity professionals. Based on evaluating various security metrics, IT experts and cybersecurity professionals can determine all possible attack paths, then decide which devices included in the paths should be protected at first. Plus, the effectiveness of specific device-level strategies deployed for different devices can be compared. For the network-level, the performance of the smart grid system's defense strategies can be measured. Furthermore, our work can help system planners estimate the attack's damage cost on the proposed smart grid system.

The source code of GridAttackSim and GridAttackAnalyzer have been uploaded on Github and can be found at [84] and [85].

8.2 Future Work

As future work, GridAttackSim and GriAttackAnalyzer can be extended to integrate more power grid test feeders and network models. For example, there are various other test feeders available, such as EPRI Representative Feeders [86], PG&E Prototypical Feeders, Benchmark Models for Low-Voltage Distribution Feeders [87], Agent-Based Distribution Test Feeder with Smart-Grid Functionality [88], Test Feeder for DG Protection Analysis [89].

More case studies could also be conducted in the future, for instance by collecting various smart grid attack types and CVEs to further validate our GriAttackAnalyzer framework.

References

[1] C. Greer, D. A. Wollman, D. E. Prochaska, P. A. Boynton, J. A. Mazer, C. T. Nguyen, G. J. FitzPatrick, T. L. Nelson, G. H. Koepke, A. R. Hefner Jr *et al.*, "Nist framework and roadmap for smart grid interoperability standards, release 3.0," National Institute of Standards and Technology (NIST), Tech. Rep., 2014.

[2] M. A. Cohen, "Gridlab-d taxonomy feeder graphs," *GridLAB-D Taxonomy Feeder Graphs*, 2013.

[3] C. N. Yatin Wadhawan, Anas AlMajali, "A comprehensive analysis of smart grid systems against cyber-physical attacks," *Electronics*, vol. 7, 2018.

[4] R. M. Blank, "Guide for conducting risk assessments," National Institute of Standards and Technology (NIST), Tech. Rep., 2011.

[5] M. Fukuyama, "Society 5.0: Aiming for a new human-centered society," *Japan Spotlight*, vol. 27, pp. 47–50, 2018.

[6] I. Ghansah, *Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks: Interim Project Report.* California Energy Commission, 2012.

[7] C. Worley, "Hacking the skills shortage a study of the international shortage in cybersecurity skills," in *JA Lewis (Chair), Hacking the skills shortage A study of the International shortage in Cybersecurity skills [Video file]. Symposium conducted at the meeting of Center for Strategic & International Studies, Washington, DC. Retrieved from https://www. csis. org/events/hacking-skills-shortage*, 2016.

[8] C. Seek, "Cybersecurity supply/demand heat map," *Cyber Seek Website*, 2019.

[9] A. Setalvad, “Demand to fill cybersecurity jobs booming,” *Retrieved from*, 2015.

[10] ICS-CERT, *Incident response/vulnerability coordination in 2014*, available online: https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf (accessed on 30 June 2020). [Online]. Available: https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

[11] T. M. Chen and S. Abu-Nimeh, “Lessons from stuxnet,” *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[12] J. T. Langill, “Defending against the dragonfly cyber security attacks,” *Retrieved*, vol. 11, p. 2015, 2014.

[13] T. FoxBrewster, “Ukraine claims hackers caused christmas power outage,” *Forbes Security*, 2016.

[14] J. Dawson and R. Thomson, “The future cybersecurity workforce: Going beyond technical skills for successful cyber performance,” *Frontiers in psychology*, vol. 9, p. 744, 2018.

[15] C.-N. Bodea, M.-I. Dascalu, and M. Cazacu, “Increasing the effectiveness of the cybersecurity teaching and learning by applying activity theory and narrative research.” *Issues in Information Systems*, vol. 20, no. 3, 2019.

[16] J. Hong and D.-S. Kim, “Harms: Hierarchical attack representation models for network security analysis,” *10th Australian Information Security Management Conference*, 2012.

[17] J. B. Hong and D. S. Kim, “Towards scalable security analysis using multi-layered security models,” *Journal of Network and Computer Applications*, vol. 75, pp. 156–168, 2016.

[18] T. D. Le, A. Adnan, R. Beuran, and W. L. Seng, “Smart grid co-simulation tools: Review and cybersecurity case study,” in *7th Inter-*

national Conference on Smart Grid (icSmartGrid2019). IEEE, 2019, pp. 273–280.

[19] S. Christey and R. A. Martin, "Vulnerability type distributions in cve," *Mitre report, May*, 2007.

[20] K. Scarfone and P. Mell, "An analysis of cvss version 2 vulnerability scoring," in *2009 3rd International Symposium on Empirical Software Engineering and Measurement.* IEEE, 2009, pp. 516–525.

[21] J. B. Hong, D. S. Kim, C.-J. Chung, and D. Huang, "A survey on the usability and practical applications of graphical security models," *Computer Science Review*, vol. 26, pp. 1–16, 2017.

[22] B. Schneier, *Secrets and lies: digital security in a networked world.* John Wiley & Sons, 2015.

[23] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in *Proceedings 2002 IEEE Symposium on Security and Privacy.* IEEE, 2002, pp. 273–284.

[24] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, "Epochs: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components," *IEEE Transactions on Power Systems*, vol. 21, no. 2, pp. 548–558, 2006.

[25] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of scada control systems (tasscs)," in *ISGT 2011.* IEEE, 2011, pp. 1–7.

[26] Awad, Abdalkarim, Bazan, Peter, German, and Reinhard, "Sgsim: A simulation framework for smart grid applications," in *2014 IEEE International Energy Conference (ENERGYCON).* IEEE, 2014, pp. 730–736.

[27] D. Grunewald, M. Lützenberger, J. Chinnow, R. Bye, K. Bsufka, and S. Albayrak, "Agent-based network security simulation," in *The*

10th International Conference on Autonomous Agents and Multiagent Systems-Volume 3. Citeseer, 2011, pp. 1325–1326.

[28] J. Chinnow, K. Bsufka, A.-D. Schmidt, R. Bye, A. Camtepe, and S. Albayrak, "A simulation framework for smart meter security evaluation," in *2011 IEEE International Conference on Smart Measurements of Future Grids (SMFG) Proceedings.* IEEE, 2011, pp. 1–9.

[29] C. Queiroz, A. Mahmood, and Z. Tari, "Scadasim—a framework for building scada simulations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 589–597, 2011.

[30] A. G. Wermann, M. C. Bortolozzo, E. G. da Silva, A. Schaeffer-Filho, L. P. Gaspary, and M. Barcellos, "Astoria: A framework for attack simulation and evaluation in smart grids," in *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium.* IEEE, 2016, pp. 273–280.

[31] S. Ciraci, J. Daily, J. Fuller, A. Fisher, L. Marinovici, and K. Agarwal, "Fncs: a framework for power system and communication networks co-simulation," in *Proceedings of the symposium on theory of modeling & simulation-DEVS integrative.* Society for Computer Simulation International, 2014, p. 36.

[32] T. D. Le, G. Mengmeng, T. D. Phan, D. H. Hien, A. Adnan, R. Beuran, W. L. Seng, and T. Yasuo, "Cvss based attack analysis using a graphical security model: Review and smart grid case study," in *4th EAI International Conference on Smart Grid and Internet of Things (SGIoT 2020).* Springer, 2020.

[33] X. O. Anoop Singhal, "Security risk analysis of enterprise networks using probabilistic attack graphs," National Institute of Standards and Technology (NIST), Tech. Rep., 2011.

[34] Y. K. M. Hyunchul Joh, "Defining and assessing quantitative security risk measures using vulnerability lifecycle and cvss metrics," *The 2011 International Conference on Security and Management (SAM'11)*, 2011.

[35] P. Cheng, L. Wang, S. Jajodia, and A. Singhal, "Aggregating cvss base scores for semantics-rich network security metrics," *International Symposium on Reliable Distributed Systems*, 2012.

[36] I. R. Nayot Poolsappasit, Rinku Dewri, "Dynamic security risk management using bayesian attack graphs," *IEEE Transactions on Dependable and Secure Computing*, 2012.

[37] M. Alhomidi and M. Reed, "Attack graph-based risk assessment and optimisation approach," *International Journal of Network Security & Its Applications*, vol. 6, no. 3, p. 31, 2014.

[38] M. U. Aksu, M. H. Dilek, E. I. TatlÄ±, K. Bicakci, H. I. Dirik, M. U. Demirezen, and T. AykÄ±r, "A quantitative cvss-based cyber security risk assessment methodology for it systems," in *2017 International Carnahan Conference on Security Technology (ICCST)*, 2017, pp. 1–8.

[39] M. Ge and D. S. Kim, "A framework for modeling and assessing security of the internet of things," *IEEE 21st International Conference on Parallel and Distributed Systems*, 2015.

[40] S. E. Yusuf, M. Ge, J. B. Hong, H. K. Kim, P. Kim, and D. S. Kim, "Security modelling and analysis of dynamic enterprise networks," in *2016 IEEE International Conference on Computer and Information Technology (CIT)*, 2016, pp. 249–256.

[41] M. Ge, J. B.Hong, and W. G. D. SeongKim, "A framework for automating security analysis of the internet of things," *Journal of Network and Computer Applications*, vol. 83, pp. 12–27, 2017.

[42] Erxia Li, Chaoqun Kang, Deyu Huang, Modi Hu, Fangyuan Chang, Lianjie He, and Xiaoyong Li 0003, "Quantitative model of attacks on distribution automation systems based on cvss and attack trees." *Information.*, 2019.

[43] S. An, T. Eom, J. S. Park, J. B. Hong, A. Nhlabatsi, N. Fetais, K. M. Khan, and D. S. Kim, "Cloudsafe: A tool for an automated

security analysis for cloud computing," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2019, pp. 602–609.

[44] T. Eom, J. B. Hong, S. An, and J. S. P. D. S. Kim, "A framework for real-time intrusion response in software defined networking using precomputed graphical security models," *Security and Communication Networks*, 2020.

[45] K. Beckers, M. Heisel, L. Krautsevich, F. Martinelli, R. Meis, and A. Yautsiukhin, "Determining the probability of smart grid attacks by combining attack tree and attack graph analysis," *International Workshop on Smart Grid Security*, 2014.

[46] R. Meyur, "A bayesian attack tree based approach to assess cyber-physical security of power system," in *2020 IEEE Texas Power and Energy Conference (TPEC)*, 2020, pp. 1–6.

[47] A. Tundis, R. Egert, and M. Mühlhäuser, "Attack scenario modeling for smart grids assessment through simulation," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1–10.

[48] T. R. Henderson, M. Lacage, G. F. Riley, C. Dowell, and J. Kopena, "Network simulations with the ns-3 simulator," *SIGCOMM demonstration*, vol. 14, no. 14, p. 527, 2008.

[49] D. P. Chassin, K. Schneider, and C. Gerkensmeyer, "Gridlab-d: An open-source power systems modeling and simulation environment," in *2008 IEEE/PES Transmission and Distribution Conference and Exposition.* IEEE, 2008, pp. 1–5.

[50] J. W. Shipman, "Tkinter 8.4 reference: a gui for python," *New Mexico Tech Computer Center*, 2013.

[51] P. Marcos, E. Fernando, C. Mateo Domingo, T. Gómez San Román, B. Palmintier, B.-M. Hodge, V. Krishnan, F. De Cuadra García, and B. Mather, "A review of power distribution test feeders in the united states and the need for synthetic representative networks," *Energies*, vol. 10, no. 11, p. 1896, 2017.

[52] S. Ciraci, J. Daily, K. Agarwal, J. Fuller, L. Marinovici, and A. Fisher, "Synchronization algorithms for co-simulation of power grid and communication networks," in *2014 IEEE 22nd International Symposium on Modelling, Analysis Simulation of Computer and Telecommunication Systems*, 2014, pp. 355–364.

[53] W. H. Kersting, "Radial distribution test feeders distribution system analysis subcommittee report," in *Proc. 2001 IEEE Power Eng. Soc. Winter Meeting*, 2000, pp. 908–912.

[54] H. Kersting William, "Radial distribution test feeders," *IEEE Transactions on Power Systems*, vol. 6, no. 3, pp. 975–985, 1991.

[55] R. Mattioli and K. Moulinos, "Communication network interdependencies in smart grids," *EUA FNAI Security, Ed., ed. EU: ENISA*, 2015.

[56] V. Y. Pillitteri and T. L. Brewer, "Guidelines for smart grid cybersecurity," National Institute of Standards and Technology (NIST), Tech. Rep., 2014.

[57] D. J. Closs and E. F. McGarrell, *Enhancing security throughout the supply chain.* IBM Center for the Business of Government, Washington, DC, 2004.

[58] I. Ghansah, *Smart Grid Information Assurance and Security Technology Assessment: Final Project Report.* California Energy Commission, 2010.

[59] I. Shin and M. Cho, "On localized countermeasure against reactive jamming attacks in smart grid wireless mesh networks," *Applied Sciences*, vol. 8, no. 12, p. 2340, 2018.

[60] M. Ganjkhani, S. N. Fallah, S. Badakhshan, S. Shamshirband, and K.-w. Chau, "A novel detection algorithm to identify false data injection attacks on power system state estimation," *Energies*, vol. 12, no. 11, p. 2209, 2019.

[61] D. Wang, X. Guan, T. Liu, Y. Gu, C. Shen, and Z. Xu, "Extended distributed state estimation: A detection method against tolerable false data injection attacks in smart grids," *Energies*, vol. 7, no. 3, pp. 1517–1538, 2014.

[62] A. Anwar, A. N. Mahmood, and M. Pickering, "Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements," *Journal of Computer and System Sciences*, vol. 83, no. 1, pp. 58–72, 2017.

[63] A. Anwar, A. N. Mahmood, and Z. Tari, "Identification of vulnerable node clusters against false data injection attack in an ami based smart grid," *Information Systems*, vol. 53, pp. 201–212, 2015.

[64] A. Anwar and A. N. Mahmood, "Vulnerabilities of smart grid state estimation against false data injection attack," in *Renewable energy integration*. Springer, 2014, pp. 411–428.

[65] A. Anwar, A. N. Mahmood, and M. Pickering, "Data-driven stealthy injection attacks on smart grid with incomplete measurements," in *Pacific-Asia Workshop on Intelligence and Security Informatics*. Springer, 2016, pp. 180–192.

[66] NVD, *National Vulnerability Database (NVD)*, available online: https://nvd.nist.gov/ (accessed on 30 October 2020). [Online]. Available: https://nvd.nist.gov/

[67] K. Schneider, B. Mather, B. Pal, C.-W. Ten, G. Shirek, H. Zhu, J. Fuller, J. L. R. Pereira, L. F. Ochoa, L. R. de Araujo *et al.*, "Analytic considerations and design basis for the ieee distribution test feeders," *IEEE Transactions on power systems*, vol. 33, no. 3, pp. 3181–3188, 2017.

[68] K. P. Schneider, Y. Chen, D. P. Chassin, R. G. Pratt, D. W. Engel, and S. E. Thompson, "Modern grid initiative distribution taxonomy final report," Pacific Northwest National Lab.(PNNL), Richland, WA (United States), Tech. Rep., 2008.

[69] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," *Computer Networks*, vol. 56, no. 11, pp. 2742–2771, 2012.

[70] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, and C.-F. Covrig, "A survey on the critical issues in smart grid technologies," *Renewable and Sustainable Energy Reviews*, vol. 54, pp. 396–405, 2016.

[71] T. D. Le, A. Anwar, S. W. Loke, R. Beuran, and Y. Tan, "Gridattacksim: A cyber attack simulation framework for smart grids," *Electronics*, vol. 9, no. 8, p. 1218, 2020.

[72] N. Raza, M. Q. Akbar, A. A. Soofi, and S. Akbar, "Study of smart grid communication network architectures and technologies," *Journal of Computer and Communications*, vol. 7, no. 3, pp. 19–29, 2019.

[73] S. L. Clements, T. E. Carroll, and M. D. Hadley, "Home area networks and the smart grid," Pacific Northwest National Lab.(PNNL), Richland, WA (United States), Tech. Rep., 2011.

[74] J. Brooke, "Sus: a retrospective," *Journal of usability studies*, vol. 8, no. 2, pp. 29–40, 2013.

[75] J. Sauro and J. R. Lewis, "Correlations among prototypical usability metrics: evidence for the construct of usability," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2009, pp. 1609–1618.

[76] T. S. Tullis and J. N. Stetson, "A comparison of questionnaires for assessing website usability," in *Usability professional association conference*, vol. 1. Minneapolis, USA, 2004.

[77] A. Bangor, P. T. Kortum, and J. T. Miller, "An empirical evaluation of the system usability scale," *Intl. Journal of Human–Computer Interaction*, vol. 24, no. 6, pp. 574–594, 2008.

[78] D. Chassin, "Gridlab-d technical support document tape modules version 1.0. eng," *Washington, DC: Oak Ridge, Tenn.: United States. Dept. of Energy*, 2008.

[79] NISC, *National center of Incident readiness and Strategy for Cybersecurity (NISC)*, available online: https://www.nisc.go.jp/eng/ (accessed on 30 October 2020). [Online]. Available: https://www.nisc.go.jp/eng/

[80] W. Crumpler and J. A. Lewis, *Cybersecurity Workforce Gap.* Center for Strategic and International Studies (CSIS), 2019.

[81] C. Keith Price and C. CGEIT, "State of cybersecurity 2018 part 1: Workforce development," *ISACA*, 2018.

[82] R. Beuran, K.-i. Chinen, Y. Tan, and Y. Shinoda, "Towards effective cybersecurity education and training," *Research report*, vol. IS-RR-2016-003, 2016.

[83] R. Beuran, T. Inoue, Y. Tan, and Y. Shinoda, "Realistic cybersecurity training via scenario progression management," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).* IEEE, 2019, pp. 67–76.

[84] T. D. Le and R. Beuran, "Gridattacksim: Smart grid attack simulation framework," https://github.com/crond-jaist/GridAttackSim, 2021.

[85] T. D. Le, R. Beuran, M. Ge, and J. B. Hong, "Gridattackanalyzer: Smart grid attack analysis framework," https://github.com/crond-jaist/GridAttackAnalyzer, 2021.

[86] D. Sarajlić and C. Rehtanz, "Overview of distribution grid test systems for benchmarking of power system analyses," in *2020 AEIT International Annual Conference (AEIT).* IEEE, 2020, pp. 1–6.

[87] PG&E, *Pacific gas and electric prototypical feeder models*. [Online]. Available: http://gridlab-d.shoutwiki.com/wiki/PGE_Prototypical_Models

[88] P. Jahangiri, D. Wu, W. Li, D. C. Aliprantis, and L. Tesfatsion, "Development of an agent-based distribution test feeder with smart-grid functionality," in *2012 IEEE Power and Energy Society General Meeting*. IEEE, 2012, pp. 1–7.

[89] T. McDermott, "A test feeder for dg protection analysis," in *2011 IEEE/PES Power Systems Conference and Exposition*. IEEE, 2011, pp. 1–7.

Publications and Awards

International Journals

- **T. D. Le**, A. Anwar, S. W. Loke, R. Beuran, Y. Tan, "GridAttackSim: Cyber Attack Simulation Framework for Smart Grids", MDPI Electronics, Special Issue on Applications of IoT for Microgrids, vol. 9, no. 8, August 2020, 1218.
- **T. D. Le**, M. Ge, A. Anwar, S. W. Loke, R. Beuran, Y. Tan, "GridAttackAnalyzer: Cyber Attack Analysis Framework for Smart Grids", Elsevier Sustainable Energy, Grids and Networks [Under Review].

Related International Conferences

- **T. D. Le**, M. Ge, P. T. Duy, H. D. Hoang, A. Anwar, S. W. Loke, R. Beuran, Y. Tan, "CVSS Based Attack Analysis using a Graphical Security Model: Review and Smart Grid Case Study", 4th EAI International Conference on Smart Grid and Internet of Things (SGIoT 2020), TaiChung, Taiwan, December 5-6, 2020.
- **T. D. Le**, A. Anwar, R. Beuran, S. W. Loke, "Smart Grid Co-Simulation Tools: Review and Cybersecurity Case Study", 7th International Conference on Smart Grid (icSmartGrid 2019), Newcastle, Australia, December 9-11, 2019, pp. 39-45.

Non-related International Conferences

- **T. D. Le**, R. Beuran, Y. Tan, "Comparison of the Most Influential Missing Data Imputation Algorithms for Healthcare", 10th International Conference on Knowledge and Systems Engineering (KSE 2018), Ho Chi Minh, Vietnam, November 1-3, 2018, pp. 247-251.

- **T. D. Le**, R. Beuran, “Cybersecurity Training Framework for Smart House System”, Verbal/Poster, Smart Information/Smart Knowledge/Smart Material Workshop 2019 (SKSISM 2019), Thailand, January 2019.

Awards

- JAIST President Award 2019