CVSS Based Attack Analysis using a Graphical Security Model: Review and Smart Grid Case Study

Tan Duy Le[1], Mengmeng Ge[2], Phan The Duy[3,4], Hien Do Hoang[3,4], Adnan Anwar[2], Seng W. Loke[2], Razvan Beuran[1], and Yasuo Tan[1]

[1] Japan Advanced Institute of Science and Technology, Ishikawa, Japan
[2] School of Information Technology, Deakin University, Geelong, Australia
[3] Information Security Lab, University of Information Technology, Ho Chi Minh City, Vietnam
[4] Vietnam National University Ho Chi Minh City, Ho Chi Minh City, Vietnam
tanld@jaist.ac.jp

Abstract. Smart Grid is one of the critical technologies that provide essential services to sustain social and economic developments. There are various cyber attacks on the Smart Grid system in recent years, which resulted in various negative repercussions. Therefore, understanding the characteristics and evaluating the consequences of an attack on the Smart Grid system is essential. The combination of Graphical Security Model (GrSM), including Attack Tree (AT) and Attack Graph (AG), and the Common Vulnerability Score System (CVSS) is a potential technology to analyze attack on Smart Grid system. However, there are a few research works about Smart Grid attack analysis using GrSM and CVSS. In this research, we first conduct 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. We indicate that the framework for automating security analysis of the Internet of Things is a promising direction for Smart Grid attack analysis using GrSM and CVSS. The framework has been applied to assess security of the Smart Grid system. A case study using the PNNL Taxonomy Feeders R4-12.47-2 and Smart Grid network model with gateways was conducted to validate the utilized framework. Our research is enriched by capturing all potential attack paths and calculating values of selected security metrics during the vulnerability analysis process. Furthermore, AG can be generated automatically. The research can potentially be utilized in Smart Grid cybersecurity training.

Keywords: Smart Grid · Graphical Security Model (GrSM) · Common Vulnerability Score System (CVSS) · Attack Analysis · Attack Tree · Attack Graph

1 Introduction

Smart Grid is one of the application domains of the emerging Internet of Things (IoT). According to the US Department of Homeland Security (DHS) [1], it is one of the key technologies supporting essential services towards sustainable social and economic developments. The number of cyber attacks on the Smart Grid system has expanded in recent years. It has resulted in various negative impacts, such as blackouts, the loss of confidential data, and even physical destruction to electrical devices. Therefore, it is

essential to understand the characteristics and evaluate the consequences of an attack on the Smart Grid system.

Vulnerability scanners are widely accepted 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, is a list of a reference-method for publicly known vulnerabilities and exposures [2]. This CVE glossary investigates vulnerabilities and uses the Common Vulnerability Score System (CVSS) to evaluate the severity level of vulnerabilities [3]. CVSS offers a systematic approach to capture critical features of vulnerabilities through numerical scores reflecting their severity. To support evaluation and prioritization of organization's vulnerability management processes by IT experts, security analysts, and cybersecurity professionals, CVSS scores can be converted into a qualitative representation, ranging from low, medium, high, and critical. Besides, these numerical scores can be taken as inputs to generate the Graphical Security Model (GrSM) [4].

GrSM is a significant technology to identify the security posture of networked systems and evaluate the effectiveness of security defenses. Since it provides a visualisation 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) [5] and Attack Graph (AG) [6] 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 calculation of security metrics 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.

Several studies have proposed technologies to combine ATs and AGs in multiple layers to resolve the scalability issue of single-layered model [7, 8]. GrSM with CVSS is an emerging technology to analyze attacks on Smart Grid system. However, there has been only a few works that focuses on Smart Grid attack analysis using GrSM and CVSS. In this context, we first provide an analytical literature review in current state-of-the-art attack analysis using GrSM and CVSS for (1) Traditional Networks, (2) Emerging Technologies, and (3) Smart Grid. We indicate that the framework for automating security analysis of the Internet of Things is a promising direction for Smart Grid attack analysis using GrSM and CVSS. We apply the framework to assess the security of the Smart Gid system. A case study with various attack scenarios was conducted to validate our applied framework.

The main contributions of this research are summarized as follows:

- A comprehensive study and comparison of the existing research on attack analysis using GrSM and CVSS ranging from (1) Traditional Networks, (2) Emerging Technologies, to (3) Smart Grid;
- Application of security assessment framework with automatic generation of AG for Smart Grid;

- A case study using the PNNL Taxonomy Feeders R4-12.47-2 and a simplified Smart Grid network model with gateways to validate the utilized framework.
- Classification of attack paths based on attack success probability and matching into five levels: Rare, Unlikely, Possible, Likely, and Almost Certain.

The remainder of this paper is organized as follows. Section 2 discusses the related research on attack analysis using GrSM and CVSS. A Smart Grid case study with various attack scenarios is provided in Section 3. Conclusion and future work are finally drawn in Section 4.

2 Attack Analysis using GrSM and CVSS

In this section, we discuss the related studies on attack analysis using GrSM and CVSS based on three categories (1) Traditional Networks, (2) Emerging Technologies, to (3) Smart Grid. We examine numerous metrics of interest, including 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 (lh), and Smart Grid Application (SG) to accomplish this goal. Table 1 chronologically presents the majority of the attack analysis using GrSM and CVSS that have been studied in recent years.

2.1 Attack Analysis for Traditional Networks

Nowadays, attacks targeting information systems are getting more sophisticated gradually. Attackers can combine and exploit multiple vulnerabilities to run an attack. The research [9] 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. Besides, CVSS score, a standard that is used to evaluate the severity of security vulnerabilities of computer systems, is used to estimate the security risk.

HyunChul Joh et al. [10] indicated that a risk cannot 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 each 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 [11] drilled down 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 help maintained corresponding semantics of the individual scores.

Table 1: Attack Analysis using Graphical Security Model (GrSM) and CVSS (Y: Yes, Blank: No)

No	Research	AT	Attack Graph		Security Metrics Calculation				*lh*	SG
			AGG	AGV	*p*	*ac*	*aim*	*r*		
1	Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs [9]		Y		Y		Y	Y		
2	Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics [10]				Y		Y	Y		
3	Aggregating CVSS Base Scores for Semantics-Rich Network Security Metrics [11]		Y				Y			
4	Dynamic Security Risk Management Using Bayesian Attack Graphs [12]	Y	Y		Y	Y		Y		
5	Determining the Probability of Smart Grid Attacks by Combining Attack Tree and Attack Graph Analysis [21]	Y	Y		Y					Y
6	Attack Graph-Based Risk Assessment and Optimisation Approach [13]	Y	Y		Y			Y		
7	A Framework for Modeling and Assessing Security of the Internet of Things [15]	Y	Y		Y	Y	Y	Y		
8	Security Modelling and Analysis of Dynamic Enterprise Networks [16]				Y	Y	Y	Y		
9	A Quantitative CVSS-Based Cyber Security Risk Assessment Methodology for IT Systems [14]		Y		Y		Y	Y		
10	A Framework for Automating Security Analysis of the Internet of Things [17]	Y	Y		Y	Y	Y	Y		
11	A Comprehensive Analysis of Smart Grid Systems against Cyber-Physical Attacks [22]	Y	Y		Y		Y	Y	Y	Y
12	CloudSafe: A Tool for an Automated Security Analysis for Cloud Computing [19]		Y		Y					Y
13	Quantitative Model of Attacks on Distribution Automation Systems Based on CVSS and Attack Trees [18]	Y	Y		Y					
14	A Bayesian Attack Tree Based Approach to Assess Cyber-Physical Security of Power System [23]	Y	Y		Y		Y	Y		Y
15	A Framework for Real-Time Intrusion Response in Software Defined Networking Using Precomputed Graphical Security Models [20]		Y		Y	Y	Y	Y		

The work in [12] 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 [13] 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. The proposed genetic algorithm finds the highest risk for building a minimal attack tree. This also computed with huge graphs when very large attack paths are explored.

In a work of risk assessment for IT systems, Ugur Aksu et al. [14] 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. But the authors did not evaluate the likelihood of potential attack when analyzing the cyber security risk that may occur inside the network.

2.2 Attack Analysis for Emerging Technologies

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 work in [15] 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 ability of the framework in two cases of IoT networks in reducing impacts of possible attacks.

In the context of dynamic networks that the configuration changes over time, Simon et al. [16] 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 the attack risk were calculated based on the metrics of CVSS base score. But the authors did not use the likelihood of exploitable vulnerability in investigating the security of a dynamic network.

In the study of automating security assessment for the IoT environment, Ge et al. [17] proposed a graphical security model which is used to find the potential at-

tack before it occurs [15]. The authors conducted experiments with three different IoT networks in the context of smart home, environment sensor, 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. They analyzed the security problems of IoT devices to specific vulnerabilities on 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 network element, the CVSS is used to computed aforementioned metrics. They also supported the feature of choosing the most effective defense strategies for mitigating potential attacks. But this work neither discussed about the security likelihood nor visualized the attack graph.

Erxia Li et al. [18] 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 attackers behavior. Each step of complete attack processes is formed to calculate the node attack probability. Therein, the root tree is the ascertained component in the system while an attack which can be occurred in certain DASs is represented by each leaf node of the AT. Three metrics of CVSS, namely base, time, environment score, are used to compute the maximum probability of each potential path for intruding 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 [19], a tool for automated security assessment in cloud environment which is implemented in the Amazon AWS. It consists of two phases: information collection and HARM generation. Firstly, they built a cloud information gathering interface for further data store 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, they also provided the Attack Cost, Risk, and Impact information correlating with each cloud vulnerability. Nevertheless, the graph visualization is not supported.

Meanwhile, a work by Taehoon Eom et al. [20], focused on the computation of possible attack graphs for real-time intrusion detection and response in Software-Defined Networking (SDN). They used HARM model with security metrics depending on the information of flow table, and SDN components. All possible attack paths which 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 remedy. In detail, the authors used the base score (BS) of CVSS to measure the severity of vulnerabilities and the probability of an attack success in the network entities. 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 the 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 to be not scalable in enumerating all possible attack scenarios. By leveraging from HARM, they 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, their work lacks the support of graph attack visualization and likelihood recommendation.

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. [21] delivered a method that can show steps of attackers. This method gathers information of a system at the low-level presentation to analyze high-level probabilistic attributes. The attackers high-level aims are drawn as an attack tree and actions in low level as an attack graph. The research combined both the attack tree and attack graph for mapping 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 the power delivery systems to be easily used as well as meet the intelligence and efficiency. However, insider and outsider attacks that may harm the Smart Grid system have recently occurred in the real case. 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.

To start with, the study [21] delivered a method that can show the steps of attackers. This method gathers information of a system at the low-level presentation to analyze high-level probabilistic attributes. The attackers high-level aims are drawn as an attack tree and low-level actions as an attack graph. The research combined both the attack tree and attack graph for mapping aims of the attacker to actions. This combination was applied to a Smart Grid. This proposal helps system administrators prevent possible attacks.

Besides, Yatin et al. [22] presented the methodology of risk assessment for Cyber-physical attacks in Smart Grid system. They concentrated on one primary function which is power delivery to narrow down the number of attacks in the system. The Bayesian Attack Graph for Smart Grid (BAGS) tool is used to quantify the probability of attack success and the likelihood of attack relied on the CVSS base score when successfully exploiting vulnerabilities. The authors also considered the attack risk to help power engineers decide the security budget and patch management to protect system on which system component is being susceptible to easily get compromised by intruders. In addition, they applied reinforcement learning for resource allocation in the cyber domain of Smart Grid to generate the optimal policy which recommends whether to conduct the assessment and patching 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 their implementation.

In [23], Rounak presented a Bayesian attack tree to model CPS vulnerabilities for SCADAs security assessment. This work concentrated on the perspective of prioritizing

important vulnerabilities in SCADA to be first identified and generated attack paths to 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 on the time of compromising system which contains the vulnerability. The CVSS metric is used to calculate the probability that a vulnerability is successfully exploited. Besides, the impact on the power grid as well as the risk of cyber attack on each attack path is also assessed in the cyber-system. However, lack of attack graph visualization and likelihood is the shortcoming of this study.

2.4 Security Metrics Calculation

To compute the likelihood of compromise in a Smart Grid environment, Yatin et al. [22] used the base score of CVSS to compute the exploitability of a vulnerability. Based on the probability ranges, they matched each potential attack into the corresponding qualitative value of likelihood.

Besides, Ge et al. [17] 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 maker as its input to generate extended HARM model. Then, the graph visualization of 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. In this approach, a set of IoT 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 is the value to measure the probability of success when an attacker is attacking the target. At the level of node, attack success probability is measured 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. At the level of path, the value of attack success probability of an attack path is also measured. This value is the metric of the probability that an attacker can compromise the target over the attack path.

Attack cost 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 for each inner node and node $t \in T$ of an attack tree. At the level of path, the measure is the cost spent by an attacker to compromise the target over the attack path. At the level of network, the measure is the minimum cost for an attacker compromising the target in the company of all possible paths.

Similarly, the attack impact value of an attack path is computed by taking the sum of attack values of each node. Then, at the network-level, the attack impact is the maximum value among all potential paths.

2.5 Summary

Among the related studies, the framework for automating security analysis of IoT proposed in [17] is the most advanced in terms of coverage, ranging from Attack Tree,

Attack Graph Generation, *p*, *ac*, *aim*, *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 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. Missing research on Smart Grid Attack Graph Visualization and Likelihood creates a gap in the field. Consequently, we utilize the framework to bridge the gap of current research.

3 Smart Grid Case Study

In this section, a Smart Grid case study with various attack scenarios is conducted. We first introduce the Smart Grid model, including the power grid and network models, followed by description of attack scenarios. Finally, attack analysis results are presented.

3.1 Smart Grid Model

There are two essential components of Smart Grid, 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 the complexity, scale, and control data, are developed in recent decades. Among these test feeders, IEEE Feeders [24] and Pacific Northwest National Laboratory (PNNL) Taxonomy Feeders [25] are widely accepted in Smart Grid research community. On the other hand, numerous network architectural models were designed for the Smart Grid system [26], [27]. The IEEE Feeders have been applied in our previous research at [28] and [29]. Therefore, the selected PNNL Taxonomy Feeders for power grid and network models applied for the Smart Grid case study are discussed in the scope of this research.

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 studying the impact of attacks for such cyber-physical models.

Due to its large size and the various utilities, the existing electricity grids in the US 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, R4-12.47-2 has its advantage by representing a combination of a moderately populated urban area with a lightly populated suburban area. Besides, 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 1.

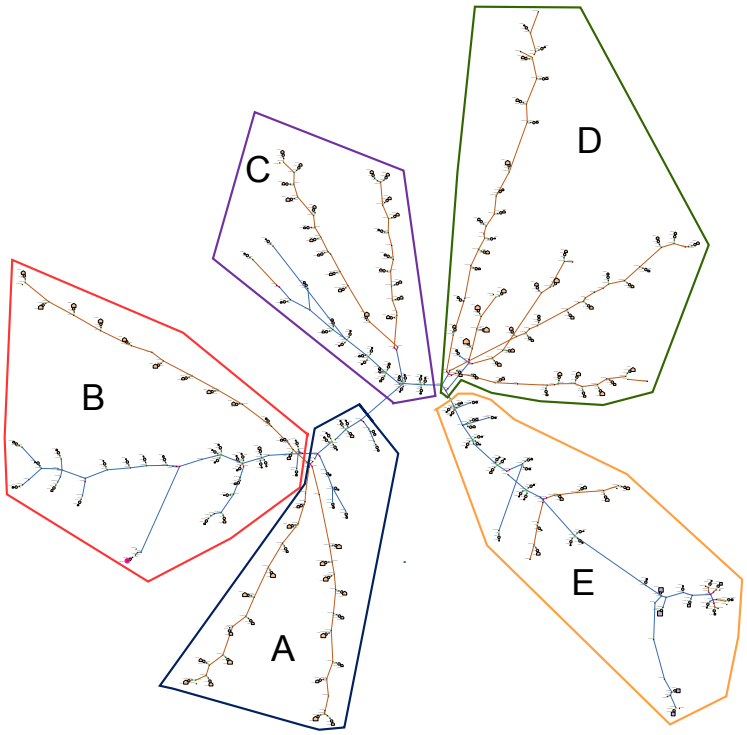

Fig. 1: The Pacific Northwest National Laboratory (PNNL) Taxonomy Feeders - R4-12.47-2 [30].

.

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 5 smaller areas, namely, A, B, C, D, and E.

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) [31]. The research at [32] 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 2. 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. Besides, these households are clustered into smaller

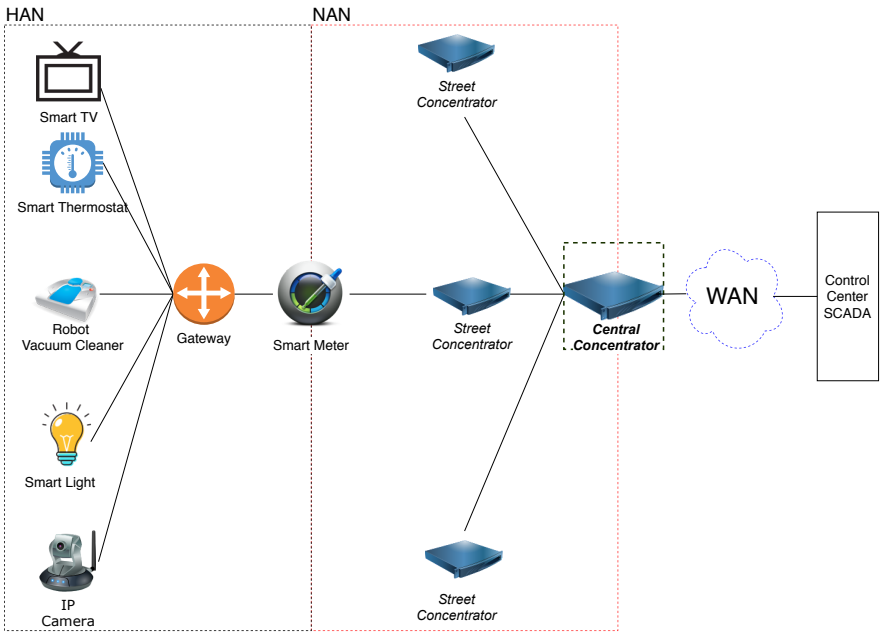

Fig. 2: Simplified network model (part of Smart Grid) with Gateway used in our case study.

areas in the same way as the residential houses are clustered in the power grid model. Each house is equipped with 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 to the central concentrator. Finally, these data are gathered at the SCADA system. In the considered scenario, the SCADA system is not covered.

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 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. Finally, $Central\_Concentrator$ serves as the ID for the central concentrator in the defined Smart Grid network model.

3.2 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

Table 2: Assumption 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

houses in each area A and B, as well as one house in each area C, D, and E, that have 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 2 was the vulnerabilities exploited by attackers. The hackers can use any HAN devices, including smart tv, smart thermostat, robot vacuum cleaner, smart light, and IP camera, one by one or even all of them as the entry points to start an attack. Three attack scenarios were considered in this research:

1. Single-entry attacker model: one type of devices has vulnerabilities in this model. 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.
2. Multiple-entry attacker model: all types of the 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.
3. Multiple-entry attacker model with patch: patching is used to fix the vulnerabilities in a specific type of devices. This scenario is the extension of the multiple-entry attacker model by integrating the patching as a defense strategy. For example, all

Table 3: Attack Analysis Results

Scenario	**Entry Point**	**Patch**	*p*	*ac*	*aim*	*r*	**Number of Paths**					
							Total	**Rare**	**Unlilkely**	**Possible**	**Likely**	**Almost Certain**
1	Smart TV	No	1	21.6	35.8	35.8	25	1	10	0	7	7
2	Smart Thermostat	No	0.65	23.6	35.8	23.27	25	0	5	14	6	0
3	Robot Vacuum Cleaner	No	0.86	21.6	32.2	27.69	25	3	12	0	8	2
4	Smart Light	No	1	23.6	35.8	35.8	25	2	10	9	0	4
5	IP Camera	No	0.8	23.6	35.8	28.64	25	2	9	5	6	3
6	All	No	1	21.6	35.8	35.8	125	8	46	28	27	16
7	All	Smart TV	1	21.6	35.8	35.8	100	7	36	28	20	9
8	All	Smart TV and Smart Light	0.86	21.6	35.8	30.8	75	5	26	19	20	5

vulnerabilities of all smart TVs inside the system have been fixed. Hence, they can not be used as the entry points by attacker to conduct the attack.

The attack goal is to control the central concentrator. If a Smart Grid device has more than one vulnerability, attackers can randomly select one vulnerability to conduct the attack. The considered attack scenarios are not the only solutions since more vulnerability rates can be selected and tested. Fortunately, the result at a 2% rate is visually significant.

3.3 Attack Analysis Results

We conducted a Smart Grid case study by applying the framework for automating IoT security analysis proposed in [17]. We calculate the security metrics values in node, attack path, and network level. These security metrics are Attack Success Probability (p), Attack Cost (ac), Attack Impact (aim), Attack Risk (r). The formulas to calculate these security metrics are extracted from Subsection 2.4. Based on the range of p adapted by the research at [22] and [33], 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. The network level analysis results are shown in Table 3. Accordingly, the scenarios from one to five denote the results for the single-entry attacker model, as well as scenario six represents the results for the multiple-entry attacker model, and the scenarios from seven to eight for results from multiple-entry attacker model with patch.

Single-entry attacker model: We can see that attacking the smart TVs and smart lights have the maximum success probability from the metrics values 1. However, the attack cost by compromising the smart lights is higher than the smart TVs. Accordingly, there are 25 attack paths, which contain 7 Almost Certain paths, for attackers to reach the central concentrator 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 central concentrator may not exist even in the single-entry attacker model. As an evidence, the path from TV_{A_1} to $Central\_Concentrator$, which is shown in the following, has the minimum attack cost at 21.6, maximum attack success probability at 1, and maximum attack risk and impact at 35.8:

- Attackers $\rightarrow TV_{A_1} \rightarrow Gateway_{A_1} \rightarrow Meter_{A_1} \rightarrow Concentrator_A \rightarrow Central\_Concentrator$

However, the following path from TV_{B_2} to $Central\_Concentrator$ has the maximum impact at 35.8:

- Attackers $\rightarrow TV_{B_2} \rightarrow Gateway_{B_2} \rightarrow Meter_{B_2} \rightarrow Concentrator_B \rightarrow Central\_Concentrator$

After analyzing the Smart Grid system, attackers can determine which paths to hack based on their intention. The knowledge can be used by security experts to protect the system against an attack. By using attack success probability metrics, the example of an attack graph generated automatically by the case study is shown in Figure 3.

Multiple-entry attacker model: By providing more entry devices, attackers possess more paths to conduct an attack. There is more likely that the Smart Gird system is hacked since among 125 paths, there are 16 Almost Certain, 27 Likely, and 28 Possible paths, respectively. In this scenario, attackers need to spend less cost at 21.6. However, the attack impact and attack risk are highest at 35.8. Similarly, smart TVs and smart lights should be protected at first in order to prevent the attackers from breaking into the system.

Multiple-entry attacker model with patch: We modify the vulnerability information for the smart TVs or both smart TVs and smart lights, separately.

Since the potential attack paths 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, attack risk remain the same with multiple-entry attacker model. However,

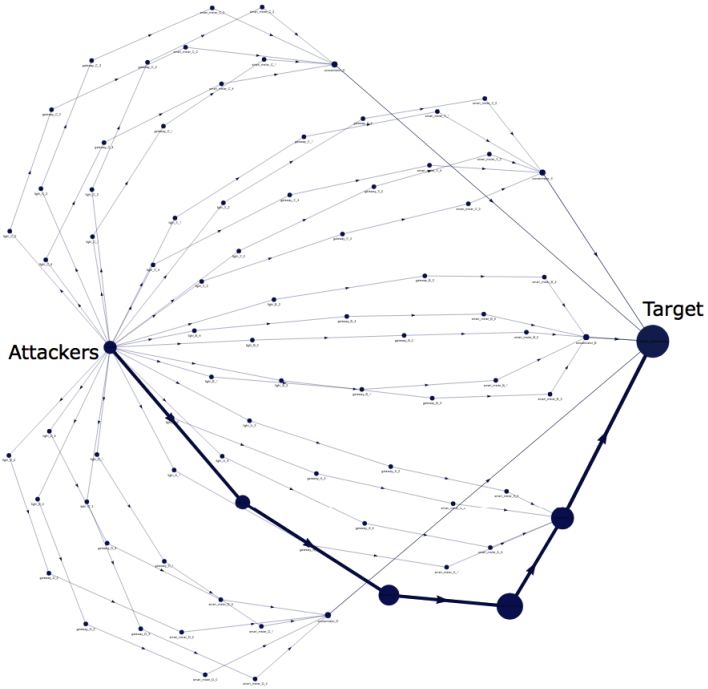

Fig. 3: An Example of Attack Graph Generated by a Case Study

the total paths have been decreased. The Almost Certain paths are modified from 16 to 9.

By eliminating the vulnerabilities of both smart TVs and smart lights, we decrease the attack success probability, attack impact, and attack risk. However, the attack cost has not changed. The reason comes from the vacuum cleaners, which costs attackers less effort to compromise. The number of Almost Certain paths has been changed 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.

4 Conclusion and Future Work

Cyber-security 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 and CVSS. We reviewed of the state-of-the-art techniques, ranging from traditional networks, emerging technologies, to Smart Grid. To accomplish this goal, numerous metrics of interest have been examined, namely, Attack Tree, Attack Graph Generation, Attack Graph Visualization, Attack Success Probability, Attack Cost, Attack Impact, Attack Risk, Likelihood, and Smart Grid Application.

As cyber attacks on the Smart Grid system can have serious issues, protecting the Smart Grid system safe 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 the Smart Grid system. However, there is few research focus on Smart Grid attack analysis using Graphical Security Model.

We indicated that the framework for automating security analysis of the Internet of Things proposed in this paper is a successful solution which can be extended to Smart Grid system. By applying the PNNL Taxonomy Feeders R4-12.47-2, Smart Grid network model with gateway, a Smart Grid case study with three attack scenarios, including a single-entry attacker model, multiple-entry attacker model, and multiple-entry attacker model with patch, 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. Besides, 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. Besides, 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.

We intend to extend our current work to a Cyber Attack Analysis Framework for Smart Grids, which integrates more power grid test feeders and network models for future work. We will also conduct case studies with the collection of various Smart Grid CVEs, different power grid and network models, to validate our extended framework.

References

1. I. Ghansah, *Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks: Interim Project Report*. California Energy Commission, 2012.
2. S. Christey and R. A. Martin, "Vulnerability type distributions in cve," 2007.
3. 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.
4. 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.
5. B. Schneier, *Secrets and lies: digital security in a networked world*. John Wiley & Sons, 2015.
6. 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.
7. J. Hong and D.-S. Kim, "Harms: Hierarchical attack representation models for network security analysis," 2012.
8. 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.

9. X. O. Anoop Singhal, "Security risk analysis of enterprise networks using probabilistic attack graphs," National Institute of Standards and Technology (NIST), Tech. Rep., 2011.
10. 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.
11. 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.
12. I. R. Nayot Poolsappasit, Rinku Dewri, "Dynamic security risk management using bayesian attack graphs," *IEEE Transactions on Dependable and Secure Computing*, 2012.
13. 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.
14. M. U. Aksu, M. H. Dilek, E. I. Tatl, K. Bicakci, H. I. Dirik, M. U. Demirezen, and T. Aykr, "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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. C. N. Yatin Wadhawan, Anas AlMajali, "A comprehensive analysis of smart grid systems against cyber-physical attacks," *Electronics*, vol. 7, 2018.
23. 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.
24. 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.
25. 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.
26. 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.

27. 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.
28. T. D. Le, A. Anwar, R. Beuran, and S. W. Loke, "Smart grid co-simulation tools: Review and cybersecurity case study," in *2019 7th International Conference on Smart Grid (icSmartGrid)*. IEEE, 2019, pp. 39–45.
29. 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.
30. M. A. Cohen, "Gridlab-d taxonomy feeder graphs," *GridLAB-D Taxonomy Feeder Graphs*, 2013.
31. 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.
32. 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.
33. R. M. Blank, "Guide for conducting risk assessments," 2011.