Smart Grid Security: Attack Modeling from a CPS Perspective

Bo Luo
Department of EECS
University of Kansas
Lawrence, KS, USA

Razvan Beuran
School of Information Science
Japan Advanced Institute of Science and Technology
Nomi, Ishikawa, Japan

Yasuo Tan
School of Information Science
Japan Advanced Institute of Science and Technology
Nomi, Ishikawa, Japan

***Abstract*—With the development of smart grid technologies and the fast adoption of household IoT devices in recent years, new threats, attacks, and security challenges arise. While a large number of vulnerabilities, threats, attacks and controls have been discussed in the literature, there lacks an abstract and generalizable framework that can be used to model the cyber-physical interactions of attacks and guide the design of defense mechanisms. In this paper, we propose a new modeling approach for security attacks in smart grids and IoT devices using a Cyber-Physical Systems (CPS) perspective. The model considers both the cyber and physical aspects of the core components of the smart grid system and the household IoT devices, as well as the interactions between the components. In particular, our model recognizes the two parallel attack channels via the cyber world and the physical world, and identifies the potential crossing routes between these two attack channels. We further discuss all possible attack surfaces, attack objectives, and attack paths in this newly proposed model. As case studies, we examine from the perspective of this new model three representative attacks proposed in the literature. The analysis demonstrates the applicability of the model, for instance, to assist the design of detection and defense mechanisms against smart grid cyber-attacks.**

I. Introduction

The smart grid, which integrates advanced computing and telecommunication capabilities with the conventional electric grid infrastructure, is envisioned to revolutionize power generation, transmission, delivery, and consumption. While some supporting and value-added technologies for the smart grid are still evolving, the core concepts, such as the advanced metering infrastructure (AMI), large-scale load balancing, dynamic pricing, and demand response, have been widely adopted across continents. Cybersecurity is a major concern for the smart grid, since the added "smart" capacities and the connected peripheral devices are exploitable to adversaries.

Existing attack modeling frameworks for smart grids mostly follow the conventional system or network attack models. They fall short in capturing the essential cyber-physical (C-P) properties and the interactions among cyber and physical components for smart grids, which carry insightful and significant implications to the design of control mechanisms. In particular, we observed that attacks only propagate within the cyber world or within the physical world during the majority of their life-cycles, and they only cross the C-P boundary at certain components of the smart grid system. It is beneficial to examine these two attack channels independently, and identify the possible crossing points via attack modeling. In addition, with the exponential growth of IoT devices that are connected to the grid, new attack surfaces and attack paths are being introduced that are not captured in most of the existing models.

In this paper, we propose an attack model for the smart grid systems that: (i) captures the specificity of and the interactions between the cyber and physical aspects of attacks against smart grid systems; (ii) is abstract and general enough so that it could be used to analyze a variety of cyber-attacks; (iii) covers the core concepts and the security-critical components of the smart grid system, and highlights the possible attack surfaces and attack paths among the components; and (iv) also captures the interactions and the corresponding security implications between IoT devices and the smart grid system.

The main contributions of the present paper are:
•We present a novel CPS model for the security analysis of the smart grid from both cyber and physical perspectives.
•With the proposed model, we investigate the possible attack surfaces and attack paths for security attacks on smart grids.
•We examine case studies to illustrate how the proposed model can be used to analyze real-world security attacks and assist, for instance, in designing defense mechanisms against them.

The remainder of this paper is organized as follows. We first present the CPS model for smart grid systems in Section II. We then review all the possible attack surfaces and attack paths by using the new model, and present three case studies in Section III. We discuss the implications of the proposed model in Section IV, followed by a brief summarizing of the literature in Section V, and then we finally conclude the paper.

II. CPS Model for Smart Grid Systems

A. CPS Components of Smart Grid Systems

Unlike [1] that coarsely models CPS components into cyber, cyber-physical, and physical aspects, we study the smart grid at a fine granularity. We examine the cyber and physical aspects for each smart grid component, and analyze how such components interact during smart grid operations, and how such interactions affect the security of the grid. We model the smart grid into four main components: meters, communication infrastructure, control system, and the power grid (Figure 1). We also include IoT devices and home hubs. Inspired by [1],

we model the cyber aspect (C) and the physical aspect (P) in each component, where the cyber aspect refers to computing and communication modules, and the physical aspect refers to sensors, actuators, electricity distribution modules.

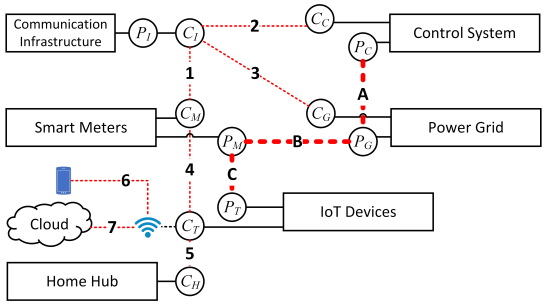

Fig. 1. Overview of the CPS model for smart grid systems.

Smart Meters: The smart meters are terminals of the energy distribution pipeline that are distributed in every household. We consider the communication channel with the smart grid infrastructure (C_M in Figure 1) as the *cyber aspect* of the smart meters, and the power line (P_M) as their *physical aspect*. C_M is used to report consumption data, and receive electricity prices and instructions. Meters are also envisioned to have a consumer-facing cyber module that directly connects to the cloud, possibly through local Wi-Fi or mobile network. P_M monitors and controls local electricity consumption in the household. Although the smart meters are usually proprietary closed-source devices owned by the utilities, they are widely distributed and physically insecure, so that both C_M and P_M are exposed to remote/local adversaries. Therefore, they often become the primary entry point of attacks against the grid.

Smart Grid Communication Infrastructure: The communication infrastructure facilitates the flow of information between the control system, the meters, and the sensors in the smart grid. This system is primarily considered as a *cyber aspect* (C_I in Figure 1), which interacts with the cyber (communication) modules of other components. We also consider the physical layer of the network and the network devices as the *physical aspect* of this component (P_I in Figure 1), which is used to support the cyber component—the actual communication.

Smart Grid Control System: The control systems take (often aggregated) inputs from the meters and other sensors, coordinate with power generators, and control the important functions of the power grid. We consider the communication channel (C_C) as the *cyber aspect* of control systems, and the power grid control module (P_C) as their *physical aspect*. Smart grid control systems are unlikely to be directly exposed to remote attackers, except for a number of high-profile attacks; rather, they are often intermediate targets for adversaries.

Power Grid: The power grid represents the conventional electrical grid that distributes power to the users. Its *physical aspect* (P_G) consists of the grid infrastructure managed by the grid control system through actuators, and the distributed sensors that monitor the grid status. Its *cyber aspect* connects to the communication infrastructure to report sensor readings (C_G in Fig. 1). Although technically the control system could use the communication infrastructure to control the actuators, we consider this control channel as part of the control system P_C. The power grid is often the target of security attacks, while the sensors may become adversaries' entry points.

IoT Devices and Home Hubs: IoT devices and the smart grid are envisioned to benefit each other under the concept of smart cities [2]. We consider the energy consumption modules as the *physical aspect* of the IoT devices (P_T). IoT devices communicate with the users or service providers through cloud platforms or home WiFi: C_T in Fig. 1. Although the IoT devices were envisioned to exchange information with the smart metering infrastructure, e.g., to receive real-time electricity prices, the adoption of such functionality is still limited. Meanwhile, standalone home hubs have become popular in the market, such as Samsung SmartThings Hub, Amazon Echo, Google Home, etc. Home hubs communicate with IoT devices in the household through different types of connectivity, such as Wi-Fi or Zigbee (their *cyber aspect*, C_H).

B. Smart Grid CPS Component Interactions

We group the interactions between smart grid components into two categories, and briefly discuss each interaction.

- Information flow, denoted by the numbers **1** to **7** in Figure 1 (thin dashed lines)
- Electricity/control flow, denoted by the letters **A** to **C** in the figure (thick dashed lines)

1: Smart Meter to Communication Infrastructure: Smart meters report power consumption details and operation status to the control center, possibly through local collectors and regional aggregators. The smart meters also receive information, such as electricity prices, from the communication network.

2: Communication Infrastructure to Control Center: Smart grid data centers receive smart metering data from the Advanced Metering Infrastructure (AMI) and grid status from sensors via the communication infrastructure.

3: Power Grid to Communication System: Sensors are widely distributed in the grid to monitor the real-time grid status. Sensor data is transmitted to the control system through a communication infrastructure. In the conventional power grid, this component is implemented by a SCADA network.

4: Smart Meter to IoT Devices: While the smart meters were envisioned to directly connect to household IoT devices, such proposals were never widely accepted in practice. We still include the link between smart meters to IoT devices since: (i) such functionality is supported in a small range of devices; and (ii) this link may be exploited by adversaries to reach smart meters from compromised IoT devices.

5: Home Hub to IoT Devices: Home hubs connect to IoT devices using open or proprietary application-layer protocols typically via wireless connectivity. Through this connection, device status and operation information is transmitted to the hub, and control commands are sent to the devices.

6: Direct connection to IoT Devices: One mechanism for commercial IoT devices to connect with users is via a direct connection through the home Wi-Fi. In this case, a service

runs on the device that expects incoming connections, and the client (smartphone app or web browser) directly connects with those devices, without going through an external server.

7: Cloud connection to IoT Devices: Another mechanism to connect to IoT devices is to employ a cloud server as an intermediary. In this case, IoT devices maintain continuous connections with the cloud, while users connect to the cloud platform to check device status and send control commands.

A: Control System to Power Grid: The control system manages the operations of the grid. Many smart grid functions, e.g., load balancing, are implemented through this channel.

B: Power Distribution to Households: This is the conventional power grid that is used to distribute electricity to the households. With the new development of Net Energy Metering (NEM), households may also sell energy to the grid.

C: Electricity Consumption by IoT Devices: IoT devices consume electricity off the grid. While each device has a very limited impact on the grid, the impact could be amplified if a large number of devices is compromised.

III. Attack Modeling from a CPS Perspective

A. Attack Objectives, Attack Surfaces and Attack Paths

Intuitively, all smart grid components that are physically insecure or revealed to the external network are possible attack surfaces. The power grid is a critical infrastructure component that is the primary target of high-profile state-sponsored or terrorist cyber-attacks. However, smart meters, household IoT devices, and other components may still become attack targets.

Every interaction among smart grid components (**1** to **7** and **A** to **C** in Figure 1) could be a potential attack path. While each attack path only links a cyber aspect with another cyber aspect, or a physical aspect with another physical aspect, attacks could *cross* between the cyber and physical aspects at any component. For example, if the control system is attacked at C_C, it possible for the attack to cross the C-P boundary and impact the physical aspect of the grid controller, P_C.

Formally, the attack path of a generic attack is denoted as:

$$(S : C_0) \rightarrow C_1 \rightarrow C_2 \twoheadrightarrow P_1 \rightarrow (O : P_0)$$

In this representation, $(S :)$ is the attack surface, which usually starts in the cyber world. C_i denotes a cyber component on the attack path, and $\twoheadrightarrow$ indicates the Cyber-Physical crossing. The attack path then reaches to the physical components P_j and finally arrive at the attack objective $(O :)$. With this abstract model, we have a clear view on the essential components on the attack path, which also give us hints to identify key points in breaking the path and blocking the attack.

IoT Devices and the Home Hubs. IoT devices and home hubs are among the primary entry points of remote adversaries, e.g., [3]–[5]. They are often accessible from the Internet and poorly managed, thus posing significant security risks [1], [6]. In practice, adversaries could reach IoT devices through compromised home hubs, the cloud (e.g., compromised accounts), or the Internet, i.e., the attack paths **5**, **6** and **7** in Figure 1. Although there is a potential attack path from C_T to C_M, this connection is rarely adopted in the industry. Meanwhile, a significant amount of compromised IoT devices could collude to attack the physical power grid from P_T to P_G via P_M, through the attack paths **C** and **B** in the figure [3], [4]. Last, compromised IoT devices (C_T) may be employed to attack external networks [7]. This family of attacks never impacted the smart grid, since they never crossed from C_T to P_T.

Smart Meters. Smart meters are considered viable attack surfaces because they are technically vulnerable and physically insecure [8]–[10]. They could be utilized for local attacks, such as usage fraud [11], or for large-scale attacks, such as false data injection against state estimation [12]–[14]. Attacks from compromised meters may propagate either through their cyber or physical aspects. In particular, false data injection attacks use the attack path **1**. Smart meters may interrupt the operations of IoT devices via attack path **C**, and/or manipulate the power demand in the power grid (similar to [3], [4]) via attack path **B**. Since smart meters include both physical and cyber aspects, attack paths could cross the C-P boundary from C_M to P_M, e.g., meters compromised from the cyber world could be utilized to attack the physical world. Lastly, as reported in [11], [15], malware may spread across smart meters; these are considered to be attacks from C_M to C_M.

Communication Infrastructure. The communication infrastructure C_I is a primary attack target [16], [17]. However, the ultimate goals of such attacks are the physical grid, while C_I is just a stepping stone on the attack path. As shown in Figure 1, attacks reach C_I from compromised terminal nodes through attack paths **1** and **3**. They further propagate to the grid control center C_C through path **2**. Meanwhile, attacks on the physical aspect of the infrastructure P_I will directly impact C_I.

Smart Grid Control System. The control centers are obvious targets of attacks against the smart grid. They are unlikely to be entry points of adversaries since they are usually well protected. Instead, they are often attacked remotely. Attacks from the communication infrastructure C_I reach the control system C_C through the attack path **2** in Figure 1. At the control center, they cross the C-P boundary from C_C to P_C, and further impact the physical power grid through the attack path **A**. Physical attacks to the power grid (e.g., MadIoT attacks [3]) may affect the control system through attack path **A**.

Power Grid. The physical aspect of the power grid P_G is usually the ultimate goal of attacks. Some grid components, such as the distributed sensors and state meters, may also become entry points of attacks [12], since they are widely distributed and not always physically secure. If the power grid P_G is attacked, possibly from P_C through attack path **A**, this is highly likely to further impact the regular electricity consumption of end users, P_M, via attack path **B**. Attacks on sensors and meters may be initiated from the cyber or physical world and propagate through the cyber world from C_G to the communication infrastructure C_I via attack path **3**.

B. Case Study: Data Injection Attack against State Estimation

In data injection attacks, adversaries attempt to interfere with meter or sensor data that is uploaded to the control center, so as to prevent the control center from accurately

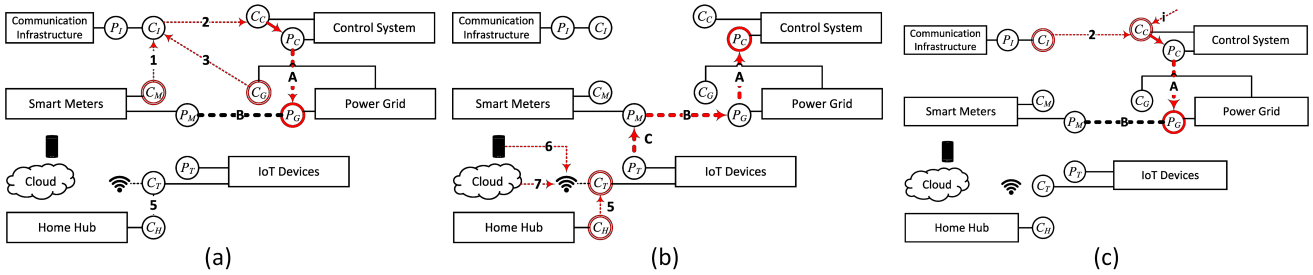

Fig. 2. Case studies: attack paths for (a) the data injection attack, (b) the MadIoT attack, and (c) the SCADA attacks.

measuring or estimating the state of the grid [12], [13], [18]. When the attack is successful, the controller would operate the grid based on wrong state information, which might ultimately cause large-scale grid failures. Figure 2 (a) demonstrates how this family of attacks is captured by our proposed model.

Attack Surface: As discussed in the literature, adversaries exploit the measurement devices that are distributed and physically insecure, including smart meters and sensors. False data is injected via compromised meters or through man-in-the-middle attacks. All the attacks in this class that were proposed in the literature come from the cyber (data) channel, therefore, both C_M and C_G in Figure 2 (a) become attack surfaces.

Attack Objective: The goal of such false data injection attacks is to interfere with the normal operation of the power grid, to disturb the optimization and reliability functions, and/or to cause physical damage to the grid. While P_G is the primary target of the attacks, P_M will be affected as well.

Attack Path: False data injected from C_M and C_G is transmitted to the communication infrastructure C_I via paths **1** and **3** in Figure 2 (a). The false data is then passed to the control center C_C through path **2**. These segments of the attack path employ the data communication channel. At the control center, the attack path crosses to the physical side, namely to P_C, and then to P_G via **A**, thus reaching the power grid.

Formally, the full attack path is then denoted as:

$$(S : C_M|C_G) \rightarrow C_I \rightarrow C_C \twoheadrightarrow P_C \rightarrow (O : P_G) \rightarrow P_M$$

in which $(S : C_M|C_G)$ denotes the two potential attack surfaces, $\twoheadrightarrow$ indicates the Cyber-Physical crossing, and $(O : P_G)$ denotes the attack objective.

This family of attacks is initiated from the cyber aspects of two components in the model, C_M and C_G, but it targets the physical aspect of the grid, P_G. Hence, there needs to be a point in the attack path to cross from the cyber to the physical aspect. We can see in Figure 2 (a) that the attack path crosses the C-P boundary at the control center, where grid status data from the cyber aspect is used to control the physical grid operations. Consequently, we claim that carefully designed defense mechanisms at this point would be very effective in countering the damaging effects of such attacks.

C. Case Study: MadIoT Attacks

The manipulation of demand via IoT attacks (MadIoT [3], [4]) employs a botnet of high-wattage IoT devices to interfere with the power demand in the grid. Figure 2 (b) demonstrates how this attack is captured by our proposed model.

Attack Surface: In the MadIoT attack [3], adversaries have control of a botnet of IoT devices. While it was not explicitly discussed how the devices were recruited, it is reasonable to assume that the attack originated from their cyber channels (C_T or C_H). For instance, the adversary could take control of the devices through compromised cloud or local accounts, insecure network connections, or device/app vulnerabilities.

Attack Objective: The objective of the MadIoT family of attacks is to interfere with the grid control functions in order to directly compromise P_G and P_C. A successful attack may cause regional power outages and even large-scale blackouts.

Attack Path: The MadIoT attacks are unique that they instantly cross the cyber-physical boundary at the compromised devices (from C_T to P_T) to directly attack the physical aspect of the power grid, as shown in Figure 2 (b). The attacks do not involve the cyber aspect of the grid (C_M, C_I, C_C or C_G); hence, the conventional non-smart power grid is also vulnerable to the MadIoT attacks, as long as a large number of remotely-exploitable devices are connected to the grid [19].

The full attack path of the MadIoT attacks is denoted as:

$$(S : C_T|C_H) \twoheadrightarrow P_T \rightarrow P_M \rightarrow (O : P_G \rightarrow P_C)$$

This attack could be hard to defend since it originates from a broad area, akin to DDoS attacks. We argue that a potential solution against MadIoT could be to effectively monitor and prevent the attack along the attack path in Figure 2 (b). For instance, situational awareness could be introduced at the AMI infrastructure to enable the detection of distributed attacks, and to prevent them from crossing the C-P boundary. One may also add defense capacity to the grid controller, as suggested in [3], to directly deploy protection on the physical aspect of the grid.

D. Case Study: SCADA Attacks

The core of the grid control subsystem is essentially an instance of the Supervisory Control and Data Acquisition (SCADA) system. Therefore, it is subject to various SCADA attacks [20]. In this case study, we examine the cyber-induced attacks against the SCADA systems in the power grid.

Attack Surface: As illustrated in Figure 2 (c), attackers may exploit Internet-facing interfaces of the power grid SCADA as the initial entry point. For instance, the cyber-induced SCADA attacks exploit software or network vulnerabilities to penetrate

into terminals that are connected to the Internet or private networks [21]–[23]. In our model, they are all abstracted as the cyber aspects of the communication infrastructure or the control system (C_I or C_C). Although the Stuxnet worm was initiated from removable drives connected to a terminal, we still consider it as an attack from the cyber aspect, since it exploits the computing/communication components instead of the electrical grid (power line) ones.

Attack Objective: The SCADA attacks usually attempt to bring serious physical damage to high-profile systems, such as (nuclear) power plants and/or control centers (e.g., the Stuxnet attack [23]). Although the attack path appears to be similar to the final stages of the false data injection attacks, SCADA attacks have the potential to cause significant damage. Since they directly compromise the control system, the SCADA attacks are capable of breaching all operation logic, safety protections, and fail-over mechanisms.

Attack Path: The attack path of the SCADA attacks is very similar to the later steps of the data injection attacks. As shown in Figure 2 (c), attacks reach the cyber aspect of the control system C_C from the smart grid communication system C_I (path 2) or a direct internet connection (path i). They can cross the C-P boundary from C_C to P_C, then reach the power grid P_G through path A. Attacks may also further affect the physical power consumption of households (P_M).

The full attack path of the SCADA attacks is denoted as:

$$(S : C_I | C_C) \twoheadrightarrow P_C \rightarrow (O : P_G) \rightarrow P_M$$

The above analysis also hints at potential protection strategies against SCADA attacks. First, the attack surfaces C_I and C_C, including the two channels, path 2 and path i, should be hardened to prevent unauthorized access. Meanwhile, protection mechanisms could be introduced at path A in Figure 2 (c) to prevent the attack from causing serious physical damage to the grid. More importantly, such protection mechanisms should be independent from cyber-channel protection ones (i.e., independent from SCADA's control and safety protection), so that they do not share the same attack surfaces.

IV. Analysis and Discussions

The objective of the proposed model is to enable researchers and practitioners to examine smart grid attacks and design defense mechanisms from a new angle–the CPS perspective. The abstract model will allow us to focus on the essence of the problems, the common properties of groups of attacks, and the critical points where defensive mechanisms should be deployed. For instance, as shown in the case studies, an effective defense is expected to eliminate the attack surface or block the attack path. The proposed CPS model abstracts the attack paths so that the crucial points become more identifiable, while the interactions are also highlighted.

In the design of defense mechanisms, the following aspects need to be considered, and the corresponding protection should be deployed: (i) system security at the attack surface; (ii) network security along the cyber aspects of the attack path; (iii) the critical point of the C-P boundary crossing, and (iv) power line and device security along the physical aspects of the attack path. In particular, we would argue that the Cyber-Physical separation plays an important role in smart grid security. All the attacks against the physical power grid need to cross the Cyber-Physical boundary at a certain point on the attack path. This point may become critical in defense due to its unique position and properties. By adopting the concept of *layered defense*, multiple controls that are complementary in functionalities may be deployed at different components, especially the attack surfaces and targets, or to monitor/eliminate different segments on the attack paths.

V. Related Work

Smart grid security has been studied since 2009 [11], [24], [25]. Existing research could be very roughly categorized into: (i) data security [26]–[29]; (ii) communication system security [25], [30]; (iii) control system/SCADA/CPS security [31], [32]; (iv) end point security and user privacy [33], [34]. Comprehensive surveys could be found at [35]–[38].

Security modeling in the smart grid, especially attack modeling, is the most relevant topic to this paper. Earlier works mostly focus one of the two subsystems of the smart grids: the Supervisory Control and Data Acquisition (SCADA) system [39], [40] or the Advanced Metering Infrastructure (AMI) [41], [42]. The former roughly corresponds to the control system and part of the communication infrastructure in our model, while the latter corresponds to the smart meters and part of the communication infrastructure in our model. Attack trees are frequently adopted in attack modeling in smart grids. However, attack trees could be very specific and complex for a particular attack, which makes it difficult for generalization and adaptation. There are also smart grid security models that focus on one aspect of the smart grid or one specific type of attacks, e.g., on the vulnerabilities [43], on the threats and risks (including attack surfaces) [44], [45], on malware attacks [46], on cyber-physical switching attacks [47], etc.

Our model is different from existing smart grid security models. First of all, our model is more abstract than the attack-specific models, which aims to capture the complete life-cycle of each single attack. Our model captures the essence of groups of attacks so that it could be used to guide the design of generalized defense mechanisms. Our model concentrates on the conceptual-level attack behaviors and interactions between smart grid components, so that it could be integrated with existing attack models (e.g., attack trees) that captures the details of specific attacks. Moreover, we highlight the cyber-physical interactions of the smart grid, which is one of the key features that distinguish smart grid attacks from conventional network or hardware/infrastructure attacks and controls.

VI. Conclusion

In this paper we have introduced a comprehensive model that captures both the cyber and physical aspects of the core components of the smart grid, and also includes household IoT devices—an intrinsic part of the smart grid concept. Our model further details the interactions between these

components, grouped into two classes: information flow and energy/control flow. We analyzed the cybersecurity issues of smart grid systems via the means provided by the model. The applicability of the model was illustrated through an analysis of three practical case studies for attacks on the smart grid that have already been discussed in the literature, the data injection attack against state estimation, MadIoT attacks, and SCADA attacks. Thus, our model enabled us to quickly identify the key elements of each attack (attack surface, attack path and objective), and can be leveraged to support designing effective defense mechanisms against such attacks. As future work, we are considering to use the proposed model as a guideline in creating the training content for the smart grid cybersecurity training system that we are currently developing. We believe that the model will allow us to create effective training content that provides a clear learning structure and is readily applicable to practical situations.

ACKNOWLEDGMENT

This work was mainly conducted while Bo Luo was a visiting professor at Japan Advanced Institute of Science and Technology (JAIST) in Ishikawa, Japan.

REFERENCES

[1] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security – a survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, 2017.

[2] S. Talari, M. Shafie-Khah, P. Siano, V. Loia, A. Tommasetti, and J. P. Catalão, "A review of smart cities based on the internet of things concept," *Energies*, vol. 10, no. 4, p. 421, 2017.

[3] S. Soltan, P. Mittal, and H. V. Poor, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," in *USENIX Security)*, 2018.

[4] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: power grid protections against iot demand attacks," in *USENIX Security*, 2019, pp. 1115–1132.

[5] L. Yang, C. Seasholtz, B. Luo, and F. Li, "Hide your hackable smart home from remote attacks: The multipath onion iot gateways," in *ESORICS*, 2018.

[6] K. Zhao and L. Ge, "A survey on the internet of things security," in *IEEE CIS*, 2013, pp. 663–667.

[7] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[8] N. Lewson, "Smart meter crypto flaw worse than thought," *Retrieved July*, vol. 31, p. 2017, 2010.

[9] R. Anderson and S. Fuloria, "Smart meter security: a survey," *University of Cambridge Computer Laboratory, United Kingdom*, 2011.

[10] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, 2019.

[11] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75–77, 2009.

[12] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[13] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE TPDS*, vol. 25, no. 3, 2013.

[14] L. Yang and F. Li, "Detecting false data injection in smart grid in-network aggregation," in *IEEE SmartGridComm*, 2013.

[15] K. Fehrenbacher, "Smart meter worm could spread like a virus," 2009.

[16] S. McLaughlin, D. Podkuiko, S. Miadzvezhanka, A. Delozier, and P. McDaniel, "Multi-vendor penetration testing in the advanced metering infrastructure," in *ACSAC*, 2010, pp. 107–116.

[17] R. Hewett, S. Rudrapattana, and P. Kijsanayothin, "Cyber-security analysis of smart grid scada systems with game models," in *CISR*, 2014.

[18] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, 2011.

[19] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well," in *ACSAC*, 2017.

[20] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on scada systems," in *2011 International conference on internet of things and 4th international conference on cyber, physical and social computing*, 2011.

[21] E. Byres, J. Carter, A. Elramly, and D. Hoffman, "Worlds in collision-ethernet and the factory floor," in *ISA Emerging Tech. Conf.*, 2002.

[22] Byres Research, "OPC security white paper #2 – OPC exposed," 2007.

[23] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, p. 29, 2011.

[24] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[25] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. on Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010.

[26] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *IEEE SmartGridComm*, 2010.

[27] W.-L. Chin, W. Li, and H.-H. Chen, "Energy big data security threats in iot-based smart grid communications," *IEEE Communications Magazine*, vol. 55, no. 10, pp. 70–75, 2017.

[28] F. Li, B. Luo, and P. Liu, "Secure and privacy-preserving information aggregation for smart grids," *International Journal of Security and Networks*, vol. 6, no. 1, pp. 28–39, 2011.

[29] F. Li and B. Luo, "Preserving data integrity for smart grid data aggregation," in *IEEE SmartGridComm*, 2012.

[30] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012.

[31] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2011.

[32] R. Tawde, A. Nivangune, and M. Sankhe, "Cyber security in smart grid scada automation systems," in *IEEE ICIIECS*, 2015.

[33] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2820–2835, 2017.

[34] L. Yang, H. Xue, and F. Li, "Privacy-preserving data sharing in smart grid systems," in *IEEE SmartGridComm*, 2014.

[35] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[36] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, 2014.

[37] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397–422, 2017.

[38] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[39] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE TSMC-Part A: Systems and Humans*, vol. 40, no. 4, 2010.

[40] C.-W. Ten, C.-C. Liu, and M. Govindarasu, "Vulnerability assessment of cybersecurity for scada systems using attack trees," in *2007 IEEE Power Engineering Society General Meeting*, 2007, pp. 1–8.

[41] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," in *International Workshop on Critical Information Infrastructures Security*. Springer, 2009, pp. 176–187.

[42] I. A. Tøndel, M. G. Jaatun, and M. B. Line, "Threat modeling of ami," in *Critical Information Infrastructures Security*. Springer, 2013.

[43] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Trans. Smart Grid*, vol. 4, no. 1, 2013.

[44] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, 2011.

[45] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Transactions on smart grid*, vol. 2, no. 4, pp. 741–749, 2011.

[46] P. Eder-Neuhauser, T. Zseby, J. Fabini, and G. Vormayr, "Cyber attack models for smart grid environments," *Sustainable Energy, Grids and Networks*, vol. 12, pp. 10–29, 2017.

[47] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. on Emerging Topics in Computing*, vol. 1, no. 2, 2013.