Evaluation of cybersecurity threats on Smart Metering System

[1]Samuel Tweneboah-Koduah; [2]Anthony K. Tsetse; [3]Julius Azasoo; [4]Barbara Endicott-Popovsky

1 School of Engineering and Science, Aalborg University, Denmark
2 Dept. of Computer Science, Northern Kentucky University, Griffin Hall 463, Highland Heights, KY 41099

3 Department of Computer & Immersive Technologies, University of Northampton, UK
Julius.Azasoo@northampton.ac.uk; School of Technology (SOT), GIMPA, Ghana jazasoo@gimpa.edu.gh

4 Center for Information Assurance and Cybersecurity in Education
Box 358523, Husky Hall 10909 NE 185th Street, Room HH 1439, Bothell, WA 98011-8246

Abstract

Smart metering has emerged as the next-generation of energy distribution, consumption, and monitoring systems via the convergence of power engineering and information and communication technology (ICT) integration otherwise known as smart grid systems. While the innovation is advancing the future power generation, distribution, energy consumption information delivery, the success of the platform is positively correlated to the successful integration and stability of technologies upon which the system is built. Nonetheless, the rising trend of cybersecurity attacks on cyber infrastructure and its dependent systems coupled with the systems inherent vulnerabilities present a source of concern not only to the vendors but also the consumers. These security concerns need to be addressed in order to increase consumer confidence so as to ensure greatest adoption and success of smart metering. In this paper, we present a functional communication architecture of the smart metering system. Following that, we demonstrate and discuss the taxonomy of smart metering common vulnerabilities exposure, upon which sophisticated threats can capitalize. We then introduce countermeasure techniques, whose integration is considered pivotal for achieving security protection against existing and future sophisticated attacks on smart metering systems.

Keywords

Smart metering infrastructure, smart grid, cybersecurity threats, energy management, ICT integration

1.0 Introduction

The modernization of the modern power grid systems otherwise known as the smart grid has been developed for the purpose of enabling bidirectional flows of metering information in order to provide consumers with diverse choices for how, when, and how much electricity they use. Integrated within the smart grid infrastructure setup is smart metering which core objective is to automate the monitoring of consumers' power consumption, as well as the billing and accounting. Smart metering infrastructure also known as Advanced Metering Infrastructure (AMI), is the core component in smart grid infrastructure systems. The functional architecture represents an automated two-way communication between a smart utility meter and a utility producer [1]. The metering system monitors consumers' power consumption by collecting information on such consumption and communicating such information back to the utility company for load monitoring and billing [1].

Additionally, smart metering infrastructure aims at providing better monitoring of power consumption, and an efficient and more transparent billing system. Thus, the utility providers are able to apply different prices for power consumption based on the time of day and season [2]. By design, smart metering enables consumers to access their own real-time use of power consumption information through a web interface and mobile app service. These goals could not have been achieved and realized without the integration of communication technology infrastructure required to gather, assemble, and synthesize data provided by smart meters and other interconnected components.

Smart Metering (SM) has gradually become an interest to both research and industrial communities most importantly to utility companies, energy regulators, energy distribution vendors as well as energy conservation societies [3]. The adoption and use of smart metering is advancing in recent times due to the ability to integrate information and communication technologies with the development of energy infrastructure systems. Notwithstanding, the recent upsurge in cyber attacks against critical infrastructure systems threaten the smooth functioning of a smart metering infrastructure development and the electric grid as a whole. In this paper, we assess cybersecurity issues in smart metering infrastructure. Our goal is to provide an initial step to classify the system's inherent vulnerabilities and the potential security threats capable of exploiting these vulnerabilities. We evaluate this by demonstrating the feasibility and impact of various

threat vectors upon a smart metering communication infrastructure network.

This paper is organized as follows. Beginning with this introduction, the next section reviews the state of the art of smart metering system. In Section III, smart metering functional architecture is presented. Section IV explores the evaluation of cyber cybersecurity challenges on smart metering. We discuss the study findings in section V and then conclude the paper in Section VI.

2.0 Related studies

As indicated earlier, the concept of smart metering has advanced in recent times due to the integration of information and communication technologies into energy development. Rinaldi classified such integration as cyber interdependency [4]. In a related study, Rinaldi, et al. argued that interdependencies in critical infrastructure systems give rise to functional and non-functional challenges which do not exist in single infrastructural system [5]. Accordingly, Li et al, posit that smart metering is part of the smart grid infrastructure system and for that matter, security attacks may take place both in the physical space, as in the conventional power grid, as well as cyberspace as in any modern communication infrastructure network [2].

Moreover, smart metering infrastructure system is often microprocessor-based, and usually, supports wireless connection for easy control and monitoring. Li et al. argue that smart meters are massively deployed as access points and in most cases connected to the Internet in order to engage customers in utility management. These access points, conversely, have become ideal portals for intrusions and malicious attacks [2]. Conversely, Li et al, maintain that the openness in the smart metering systems (to the public network) increases vulnerabilities in the grid thereby escalating sophisticated threat attacks on the system. In a related study, Flick and Morehouse claim that cybersecurity of critical infrastructure in general, and the electricity grid, in particular, has become the subject of increasing research interest both in academia and industry [6]. Contributing to this, Giani, et al., argue, the potential consequences of successful cyber attacks on the electric grid is staggering [7]. They stated, smart metering which is part of a Smart Grid infrastructure system incorporates sensing, communication, and distributed control to accommodate renewable generation, electronic vehicle (EV) loads, storage, and many other technologies. These activities substantially increase actionable data transfers making the system more vulnerable to cyber attacks, thus, increasing the urgency of cybersecurity research for electric grids [7].

Many recent papers have explored various aspects of cyber attacks on smart grid and smart metering systems. For instance, Yan et al, summarize possible vulnerabilities and cybersecurity requirements in smart grid communication systems and surveyed solutions capable of counteracting related cybersecurity threats [8]. Furthermore, a study by Wei et al. proposed a framework for protecting power grid automation systems against cyber attacks [9]. Their paper considered, among other things, integration with the existing legacy systems, desirable performance in terms of modularity, scalability, extendibility, and manageability, alignment to the "Roadmap to Secure Control Systems in the Energy Sector" and future intelligent power delivery systems [9]. Cleveland in [3] argued that while various AMI vendors and customers consider encryption as a security proof solution to the threats of cyber adversaries on AMIs, there are other potential cybersecurity challenges facing AMI systems. The challenges Cleveland identified include confidentiality, integrity, data availability and non-repudiation. The issues of privacy, confidentiality, and data availability as cybersecurity threats against smart grid systems have also been discussed in the following studies [2], [10]- [14].

3.0 Smart Metering Functional Architecture

The future power grid has a tiered architecture to supply energy to consumers [15]. This modern energy infrastructure system starts from power generation which flows through transmission systems to distribution and eventually to the final consumer. A smart grid system strives to use and coordinate various generations, and production as well as the distribution mechanisms of the grid [15]. Smart metering infrastructure is the core component in a smart grid infrastructure system. Its functional architecture represents an automated two-way communication between a smart utility meter and a utility producer [1]. Smart meters identify power consumption by collecting information on such consumption and communicate the information back to the utility company for load monitoring and billing for accounting purposes [1]. By generalizing the structures in [15], [2] and [1], we present functional smart metering architecture as illustrated in figure 1. The architecture consists of a micro-load management unit and its hardware subsystem which houses the various hardware components of the system. Each of the structures has its core components and functions explained below.

i. **Smart Meter:** This is the core of a smart metering infrastructure setup. It acts as the main source of energy-related information or other metrological data and provides interval data for customer energy loads.
ii. **Smart Metering Communications Network:** Like a traditional communication network, the

smart metering network provides a path for information flow within the grid.

iii. **Customer Gateway:** This acts as the conduit between a smart metering network and the other smart devices in the grid or within the customer facilities, such as a Home Area Network (HAN) or the Neighborhood Area Network (NAN)

Other components within the metering system include:

iv. The **Wide Area Network (WAN) Interface:** It collects metering and control information from the Server systems and relays the readings and status of the meter to the server.

v. The **Home Area Network (HAN)**: This serves as the communication medium for device interface sensors, actuator/network relays, the In-Home Display (IHD) units, etc. This communication medium can be a single unidirectional or bidirectional or a combination of multiple technologies such as power line carrier (PLC), Ethernet, or wireless communication technologies (e.g. Z-Wave, Bluetooth, ZigBee, WiFi, RF mesh, and WLAN (802.11)).

vi. The **WAN gateway:** This acts as the link between the metering Unit and the Micro-load metering information system to provide near real-time monitoring and control functions of the metering system and other auxiliary services, by providing access to the electrical utility companies and their consumers.

The utility company gains access to the metering system through a computer interface directly connected to the server. Utility consumers are usually provided access to the metering system through the web and/or mobile application interface, giving consumers the ability to monitor real-time information about energy consumption and billing, as well as performing home automation activities using integrated mobile devices.

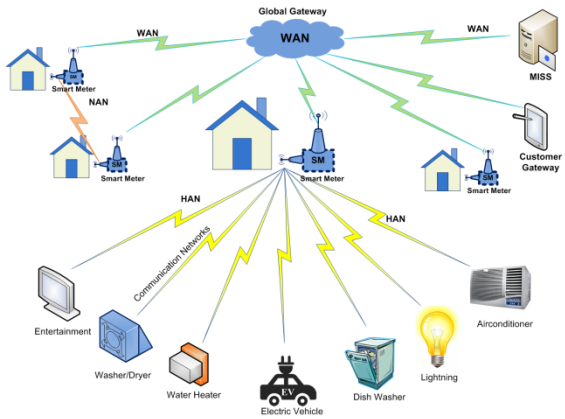

Figure 1: Smart Metering Communication Architecture

vii. The **Home Area Network (HAN) Gateway**: It provides a communication channel between the main metering unit and the micro-load controllers. As a result, the micro controllers and load management can be extended to an off-the-shelf micro-load meter for the use of Electric Vehicle (EV) charging systems and other energy consuming loads.

viii. The **Neighboring Area Network (NAN) Gateway:** Acts as the intermediary tier connecting multiple HANs collectively in the smart grid for the purpose of accumulating energy consumption information from households (the HANs), in a neighborhood and relay the data to the utility company [15] for billing and monitoring.

The Metering Unit **(MU)** is the main control center for the smart metering functional architecture. In the absence of the HAN, the MU is able to monitor the amount of energy being consumed, as well as the ability to curtail electric energy to all energy consuming devices and appliances. Furthermore, the Micro-Load Metering Unit monitors and reads the consumptions of all the devices and appliances attached to the main meter (including Electric Vehicle Charging Terminals (EVCT) by providing granular consumption data for consumption analysis and predicting future energy consumption. The micro-load controller functions to cut-off or connects micro-loads to the main source of electricity via the metering unit. This functionality is directly linked to the direct load control (DLC) which enables consumers to respond to pricing signals or time-of-use through an application program interface (API) such as Web or Mobil App.

4.0 Cybersecurity Challenges in Smart Metering

The conventional metering system is embedded with dedicated power devices, which are mostly integrated with control, monitoring and communication functionalities, using closed networks composed of predictable serial communication links. In contrast, smart metering decouples communication and control functionalities from power devices, and is modularized for the purposes of scalability and maintenance [2]. Moreover, smart metering core components are usually commercial off-the-shelf (COTS) products from diverse vendors having unknown incompatibilities.

Cybersecurity challenges of a smart metering system lie in the system's inherent vulnerabilities which expose the infrastructure setup to various attacks. The sources of vulnerabilities may include the firmware, hardware architecture, system applications, as well as the network interface. Besides, the bi-directional communication link between the metering unit and the main gateway

leave the system open for network-related attacks and protocol failure. Other communication attacks include wireless scrambling, eavesdropping, man-in-the-middle attacks, message modification and injection attacks. For example, IP-based devices are susceptible to IP misconfiguration and do exhibit nondeterministic behavior in terms of attack. IP misconfiguration inevitably decreases system operation and reliability. Besides, smart meters are deployed in smart grid as access points for each customer (in the NAN and HAN), in order to manage utility consumption. These devices are usually connected to the Internet through the metering gateway. In addition to IP spoofing, the gateway (both local and global), can become perfect points for intrusions, DoS attacks, and other Internet-based attacks.

Furthermore, per their design, utility consumers usually interact with the metering system through the web and/or mobile application interfaces. Most of these applications are either web-based or stand-alone. Web-based applications are integrated with the metering system application using application programming interface (API). An unpatched API may be susceptible to various attacks exposing the entire metering system to malicious attacks. Moreover, a poorly configured interface design may expose the smart metering system to injection and code execution attacks. In the Home Area Network (HAN), such attacks on a metering device could destabilize the communication system leading to a denial of essential services to interdependent devices. In the Neighborhood Area Network (NAN), such an attack could lead to distributed denial of service attacks due to inter-meter communications.

Many of these systems are designed with security in mind, however, security misconfiguration can occur at any level and in any part of the application. This could make the system vulnerable to software misconfiguration attack. At the firmware level, smart metering components usually have internal memory used for temporary storage and information processing. Like a conventional metering system, power fluctuations in the grid occasionally cause devices to lose memory leading to data loss. Furthermore, intermittent power fluctuations in semiconductor devices may lead to signal loss and potential system malfunction. Other security challenges in the smart metering infrastructure include component incompatibility, as well as device-based (physical) attacks, such as natural disasters, illegitimate use of the device (e.g. pilferage), and masquerading. To overcome these challenges will require innovative research and comprehensive system solutions which focus on the architectural redesign, firmware and hardware reconfiguration, network hardening and dynamic system application design.

4.1 Smart Metering Cyber attack

From the above challenges, we present a taxonomy of cybersecurity attacks in a smart metering communication system by analyzing system's vulnerabilities vis-à-vis potential threat actors. In this taxonomy, six types of vulnerabilities are discussed. These are IP misconfiguration, injection, DoS, Code execution, Memory corruption, and XSS & CSRF. Corresponding threat vectors include physical (device) attack, application (software) attack, network attack, web interface attack, and data attack (see table 1 and figure 2). Table 1 shows our proposed vulnerability threat matrix. In columns III and IV, threat vectors are matched with their corresponding vulnerabilities.

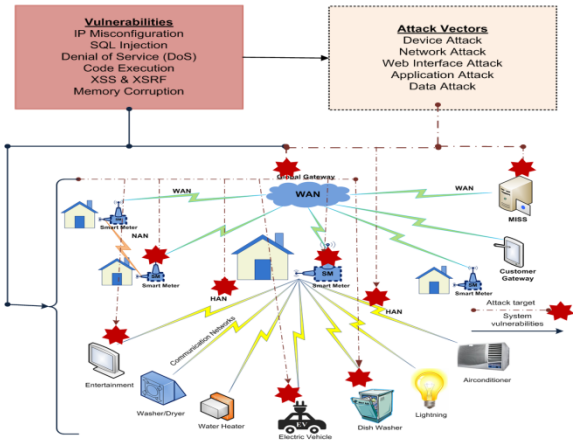

Figure 2: Smart metering and corresponding threat attack

Table 1: Vulnerability-Threat Matrix

Vulnerabilities (V)	**Cyber-attack vectors (AV)**	**Vulnerability-Threat Matrix**	
		Attack Vectors	**Vulnerabilities**
IP Misconfiguration **(IM)**	Device Attack **(DA)**	DA	IP, MC, CE, D
SQL Injection **(SI)**	Application Attack **(AA)**	AA	SI, D, CE
DoS **(D)**	Network Attack **(NA)**	NA	SI, D, CE
Code Execution **(DE)**	Web Interface Attack **(WiA)**	WiA	SI, D, XC, IP
XSS & CSRF **(XC)**	Data Integrity Attack **(DA)**	DA	SI, CE
Memory Corruption **(MC)**			

4.2 Attack Vectors

4.2.1 Device Attack

This is an attack type capable of compromising smart metering devices. It is the first point of call to compromise the functionality of the entire architecture

(depending on the devices involved). In a HAN, this type of attack could bring entire network down (especially when the metering unit is the point of attack). Similarly, in a NAN, a device attack may affect the resistance of the network which in the extreme case may lead to distributed denial of service attacks on the entire grid. Device attacks may be caused by IP misconfiguration, memory corruption, and wrongly executed code in the device operating system at the middleware layer.

4.2.2 Application Service Attack

This is a type of attack that compromises system applications (Web, Mobile, System, etc) which are run on various components of the system. Smart metering systems run multiple applications both at the local and the server levels. In most cases, these applications are owned by application service providers (ASPs) which are third party vendors. Cyber attacks on these applications will surely compromise the metering system. Common vulnerabilities in this type of attack include SQL injection, code execution, and DoS.

4.2.3 Network Attack

This is an attack which aims at compromising intercommunication among devices by either delaying message forwarding or completely failing to deliver. Network attacks may also destruct computational processes within the smart metering system. In a HAN, this type of attack aims at destructing the functionalities of the metering system. Similarly, in a NAN, a network attack may isolate or deny NAN devices from accessing vital information from the neighborhood or addressing messaging request from neighboring devices. Causes of network availability attacks include SQL injection, DoS and code execution in the network infrastructure system.

4.2.4 Web Interface Attack

This type of attack presents itself as a result of account enumeration, lack of account lockout or weak account credentials. In this case, an attacker may use weak account credentials (either capture plain-text credentials or enumerate accounts) to access the web interface. Web interface attacks may be caused by cross-site scripting (XSS), cross-site reference forgery (CSRF), IP misconfiguration and SQL injection. Other sources include insecure web interface design and weak account credentials. The attack compromises device integrity and could lead to denial of services.

4.2.5 Data Integrity Attack

This is an attack whereby the threat agent attempts to compromise system data by inserting, altering or completely deleting data (either stored or in transmission) so as to deceive smart metering to make wrong decisions or compromise its integrity. Data attacks may be caused by SQL injection and code execution which may be executed by a remote attacker.

4.3 Experimental Evaluation of Cyberattacks against Smart Metering (SQLi and DoS Attack)

In this section, we demonstrate how SQL injection and DoS attacks could be executed against a smart metering system. These demonstrations were performed on a live server with positive results. In each case, the results show that cyberattack on smart metering systems was successful.

SQL injection attack – Algorithm

Print header information
for URL in target URLs
for payload in get request payloads
response = send get request probe to server
if response.status code == 500
print payload and exist for manual attack
for paylaod in post request payloads
response = send post request probe to server

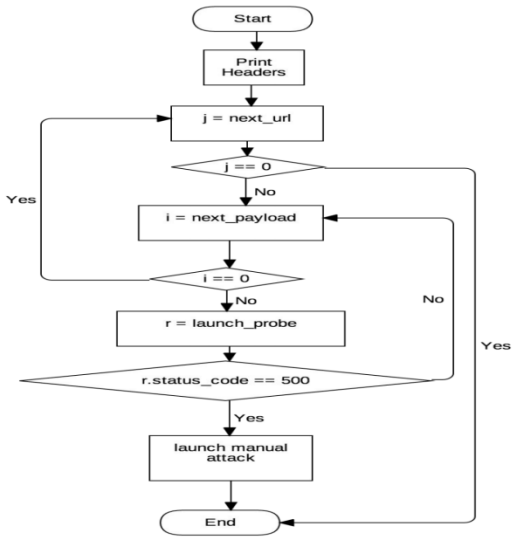

Figure 3: SQL injection attack – Flowchart

SQL injection attack – Python script

This function delivers a payload to the server using the http '*get'* method. To do this, the payload is added to the url. The url sends the request to @params payload {string}. *The request parameters for example requests.get('http://www.test.com/', params=payload) will map to http://www.test.com/?key=value*

###
def http_get(url, payload):
r = requests.get(url, params=payload)
return process_responds(r)
###

This function processes the request to determine if the probe is positive or negative

Probing Get (*assuming query is contracted: where id = <defined_param>*
('Params ', {'make': """})
('Url: ',
'http://metering.grid.com/metering/meter/topup_history'
)

data been sanitised
data been sanitised
data been sanitised
data been sanitised

Probbing Post

data been sanitised
data been sanitised
data been sanitised
data been sanitised

Vulnerability: *Weakness found (SQL injection)*
Threat*: data sanitised*
Effect*: sensitive information could be disclosed by injection attack*
Impact*: Data confidentiality and integrity could be compromised*

Denial of Service Attack

DoS attack on the Application layer
Attack url:
http://metering.smartmeter.com/metering/server/dashboard
Tool: loadtest
(https://www.npmjs.com/package/loadtest) requires nodejs to be installed
Test parameter: $ loadtest
http://metering.aborsour.com/metering/server/dashboard -t 50 -c 10 --rps 1000.

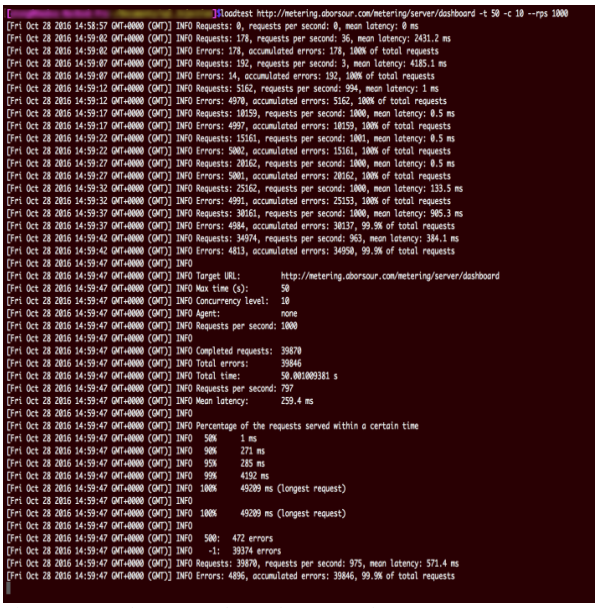

Figure 4: Results (screenshot) of DoS attack

5.0 Discussion

The idea of running both SQLi and DoS attacks on a smart metering system highlights their significant impact on distributed network system, such as smart metering (see table 1). In the case of the former, a payload request was sent to the server to probe the server for vulnerabilities. The server responded with an ACKnowledgement a message header which encourages an attack on the system. This means, SQL injection vulnerability in a smart metering system could allow remote authenticated users to execute arbitrary SQL commands via crafted serialized data both on the metering information system server (MISS in figure 2). For example, SQL injection vulnerability in the login page in the user interface device would allow remote attackers to execute arbitrary SQL commands via a crafted URL.

Per the CVE[1] database, DoS vulnerability remains the most common vulnerability type and can be exploited by various threat vectors. In the above test, we executed multiple (abnormal) remote requests (1000) to the server from concurrent connections in 50 seconds. The result (figure 4) shows the server failing or executing arbitrary code (crushing). For example, a buffer overflow in the Point-to-Point Protocol over the Ethernet (PPPoE) module in the customer gateway when CHAP authentication is configured on the server, could allow remote attackers to cause a denial of service or execute arbitrary code via crafted packets sent during authentication. For

[1] Common Vulnerability Exposure

instance, in CVE-2016-8666, an IP stack in the Linux kernel (before 4.6) allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have an unspecified impact by triggering use of the GRO functions (gro-receive and gro-complete) path for packets with tunnel stacking.

6.0 Conclusion

The core objective of smart grid is to improve efficiency and availability of power by adding more monitoring and control capabilities [16]. This objective is made plausible by the successful integration of a smart metering system for which which core value is to automate monitoring of consumer power consumption, efficient energy distribution, billing and accounting. In this paper, an attempt has been made to evaluate the taxonomy of the system inherent vulnerabilities which expose smart metering to various cyber threat vectors, and make case for research effort in this emerging technology. The discussion involved the identification of various vulnerabilities inherent within smart metering components matched with the potential threat vectors capable of exploiting these vulnerabilities. We executed two different attack scenarios (tests) as a proof of concept. Tests results show that vulnerable smart metering system could be abused by various threat actors via crafted vectors.

Finally, it is critical to continue the discussion while at the same time challenging device manufacturers and components' vendors to design, and implement solutions for such mechanisms so as to counteract threats from cyber adversaries of electrical grid so as to guarantee consumer utmost trust in a smart metering innovation and transformation.

Reference

[1] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements, and challenges," *Commun. Surv. Tutor. IEEE*, vol. 15, no. 1, pp. 5–20, 2013.

[2] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 38–45, 2012.

[3] F. M. Cleveland, "Cyber security issues for advanced metering infrasttructure (ami)," in *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, 2008, pp. 1–5.

[4] S. M. Rinaldi, "Modeling and simulating critical infrastructures and their interdependencies," in *System sciences, 2004. Proceedings of the 37th annual Hawaii international conference on*, 2004, p. 8–pp.

[5] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *Control Syst. IEEE*, vol. 21, no. 6, pp. 11–25, 2001.

[6] T. Flick and J. Morehouse, *Securing the smart grid: next generation power grid security*. Elsevier, 2010.

[7] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures π," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, 2011, pp. 232–237.

[8] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surv. Tutor.*, vol. 14, no. 4, pp. 998–1010, 2012.

[9] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in *Innovative Smart Grid Technologies (ISGT), 2010*, 2010, pp. 1–7.

[10] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. Chen, "Cyber security and privacy issues in smart grids," *Commun. Surv. Tutor. IEEE*, vol. 14, no. 4, pp. 981–997, 2012.

[11] G. N. Ericsson, "Cyber security and power system communication—essential parts of a smart grid infrastructure," *IEEE Trans. Power Deliv.*, vol. 25, no. 3, pp. 1501–1507, 2010.

[12] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 847–855, 2013.

[13] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *Military Communications Conference, 2010-MILCOM 2010*, 2010, pp. 1830–1835.

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

[15] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 42–49, 2013.

[16] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *IEEE PES General Meeting*, 2010, pp. 1–5.