Cyber Security Threats - Smart Grid Infrastructure

Rajendra Kumar Pandey, *Senior Member IEEE*
Department of Electrical Engineering,
Indian Institute of Technology (BHU)
Varanasi, India
rkpandey.eee@iitbhu.ac.in

Mohit Misra
Department of Electrical Engineering,
Indian Institute of Technology (BHU)
Varanasi, India
mohit.misra@hotmail.com

***Abstract*— Smart grid is an evolving new power system framework with ICT driven power equipment massively layered structure. The new generation sensors, smart meters and electronic devices are integral components of smart grid. However, the upcoming deployment of smart devices at different layers followed by their integration with communication networks may introduce cyber threats. The interdependencies of various subsystems functioning in the smart grid, if affected by cyber-attack, may be vulnerable and greatly reduce efficiency and reliability due to any one of the device not responding in real time frame. The cyber security vulnerabilities become even more evident due to the existing superannuated cyber infrastructure. This paper presents a critical review on expected cyber security threats in complex environment and addresses the grave concern of a secure cyber infrastructure and related developments. An extensive review on the cyber security objectives and requirements along with the risk evaluation process has been undertaken. The paper analyses confidentiality and privacy issues of entire components of smart power system. A critical evaluation on upcoming challenges with innovative research concerns is highlighted to achieve a roadmap of an immune smart grid infrastructure. This will further facilitate R&D and associated developments.**

Keywords—cyber infrastructure, prosumer, Peak Load Management (PLM), Demand Response (DR), ICT, WANs, SCADA, denial-of-service (DoS), cyber security, cyber-attack.

I. INTRODUCTION

Smart grid can be regarded as "system of systems" that will expand its current capabilities of generation, transmission and distribution to distributed generation, renewable energy sources and electric vehicles. Smart grid delivers electricity between suppliers and prosumers using two way information and communication technology (ICT) and exchanging near real time information about the grid states to enable control and automation of intelligent devices. This allows the prosumer to save energy and reduce electricity bills while increasing reliability, efficiency, robustness and transparency of the system. It is enabled by numerous technological advances in sensing, measurement and control devices. Fig. 1 shows the reference NIST model for the smart grid [19]. Unlike the legacy power systems, the smart grid provides better situational awareness regarding the state of the system [4]. Consequently, peak load management (PLM) and demand response (DR) can be implemented in order to flatten the peak demand. The smart grid also performs predictive analysis in order to keep the power balanced. Likewise, the fusion of new storage technologies will supplement in intelligent demand prediction.

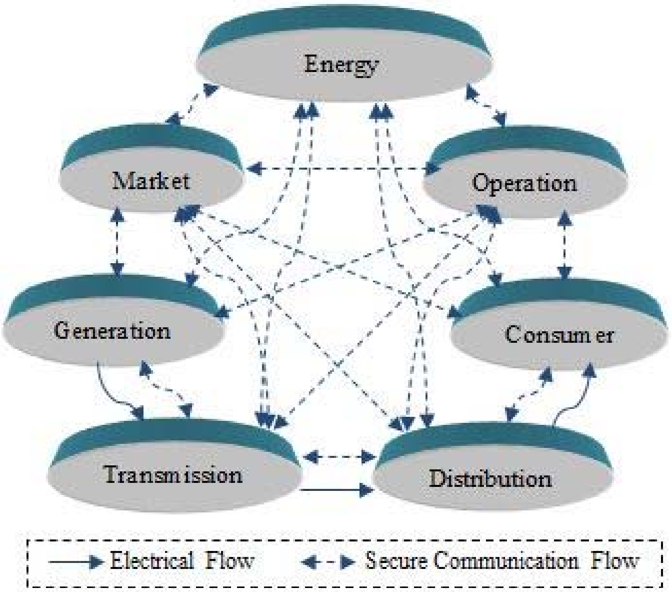

Fig. 1. NIST reference model for the smart grid

The smart grid is visualized to homogenize high speed and two way communication technology with various power and control equipment. However, such a substantial dependence on information and communication networking increases the risk of potential vulnerabilities in the smart grid. This greatly reduces the efficiency and reliability of the power system, which, nonetheless, is the ultimate goal. Metke *et al.* [25] have shown that network infiltration by adversaries may lead to serious consequences in the smart grid. According to the Electric Power Research Institute (EPRI) report, one of the upcoming challenges that the existing smart grid will face is the increasing possibility of cyber-attacks and incidents as increasing number of devices are getting interconnected [5]. Cyber security gets even more challenging when the scale and complexity of the smart grid increases. Various researchers and standard bodies have developed comprehensive frameworks to tackle cyber threats and provide architectural and analytical countermeasures to prevent such attacks [16,

978-1-4799-5141-3/14/$31.00 ©2016 IEEE

25]. Vulnerability assessment of electric power utilities also aids in finding the desired solution [26]. It is however, necessary to analyze and quantify the gravity of impacts of cyber-attacks before any evaluation. This requires identifying weak links within the cyber infrastructure. The grounds for cyber-attack on smart grid may range from economic reasons, pranks, disgruntled employees, industrial espionage, and all the way to terrorism. A feeble cyber infrastructure allows an adversary to infiltrate security through the weak links and then gain access to control software, and alter billing information and load conditions to destabilize the system causing a major economic disturbance. Furthermore, an adversary may invade consumers' privacy by collecting personal information. The wide scale of smart grid makes it nearly impossible to provide immunity to each and every component of such a complex network. To make the situation even worse, sophisticated control architecture, state estimation and algorithms manifolds the risk of attacks. Control system malware like Stuxnet, targeting vulnerable SCADA systems forced the utilities to rethink about their existing power grid security [2]. The utilities, therefore must take decisions on the choice of technical solutions when commissioning a new SCADA system or protecting an existing one. Cyber security must also address unintentional compromises of the information infrastructure due to user errors, equipment failures, and natural disasters [16]. The contemporary IT security techniques such as virtual private networks (VPNs), public key infrastructure (PKIs), intrusion detection systems (IDSs), firewall, anti-virus, etc. may be transplanted into the smart grid, but due to their inherent differences they still cannot be made effective without any enhancements [10]. The primary difference is the time criticalness of the network traffic in smart grid. The research on smart grid cyber security is in infancy, this motivates us to thoroughly examine the system components and identify all possible security threats and existing vulnerabilities in the smart grid cyber infrastructure. This paper focuses on risk inspection process where cyber security assets are identified, checked for any vulnerability in the system and later analyzed for the impact of the respective cyber threats in the system operation. This will assist the smart grid cyber security researchers in designing the appropriate cyber security architecture and network systems to deploy appropriate countermeasures in order to prevent, detect and mitigate cyber-attacks in the smart grid. Section II, introduces cyber security objectives and requirements in the smart grid. In Section III, risk assessment process along with analysis of various security threats in the smart grid cyber infrastructure and its associated impact in system operation has been presented, the need for data privacy and consumer protection has been highlighted in Section IV. Sections V concludes with future directions.

II. CYBER SECURITY OBJECTIVES AND REQUIREMENTS

This section deals with cyber security objectives and requirements in a smart grid cyber infrastructure. There are various organizations that have done extensive research on the developments in cyber security objectives and requirements including Electric Power Research Institute (EPRI), National Institute of Standards and Technology (NIST), Smart Grid Interoperability Panel (SGiP) and IEEE. The NIST report explains three high-level cyber security objectives namely: availability, integrity and confidentiality. Apart from such high-level security objectives for the smart grid, the NIST report also addresses specific security requirements like identification, authentication, authorization, trust, access control and privacy [16]. The frameworks and guidelines issued by such bodies needs to continuously evolve in order to ensure a safe, scalable and reliable operation of the smart grid. The high-level security objectives for protecting the smart grid cyber infrastructure are described below.

- Confidentiality: Preventing unauthorized access by an adversary of highly secured information such as power usage, price information and control commands that intrudes the privacy of customers and reveals the proprietary information of utilities is called confidentiality. However, according to Kerckhoff's principle [3], confidentiality of software should not be treated as important; rather focus should be given on the secrecy of keys.

- Integrity: Preventing modification of critical information of sensory devices, electronic equipment (e.g., smart meters), software and control command which might disrupt the decision making capability and corrupt the data exchange of the smart grid is called integrity. Yi *et al.* [6] have shown that bad data injection against the state estimation can compromise the integrity of the smart grid causing power mismanagement. Unlike in case of confidentiality, integrity of software should be kept critical because an adversary might control any device or electrical equipment through compromised software.

- Availability: Preventing an adversary from not granting access or control of the system to authorized personnel is called availability. Denial-of-service (DoS) attacks and distributed DoS (DDoS) attacks can delay, block or corrupt information causing unavailability of power or information exchange in the smart grid. In this case, availability of control command and price information is critical as it can cause revenue loss.

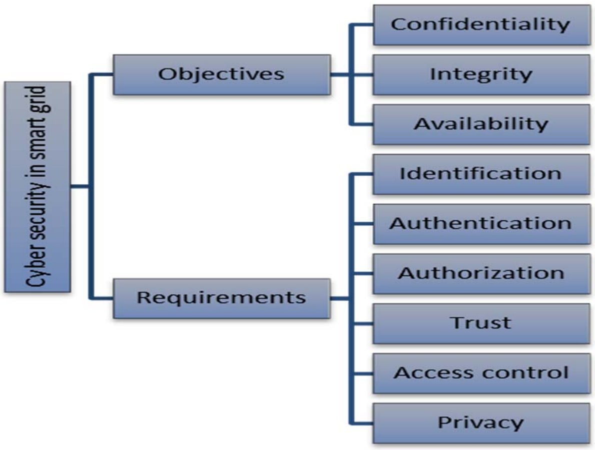

Fig. 2. High-level cyber security objectives and specific security requirements

Fig. 2 shows the high-level cyber security objectives and specific security requirements. The specific security requirements are essential for protection of cyber infrastructure in order to reduce liability and increase competency in the electric market place. A comprehensive analysis of the specific security requirements have been undertaken in Section III & IV.

III. CYBER SECURITY THREATS IN SMART GRID

It is exceedingly crucial to comprehend the prospective vulnerability threats in the smart grid. In this section, the risk assessment methodology that provides a basis for exploiting the possible entry points which are susceptible to malicious attacks have been outlined. How these attacks allow an adversary to take unwanted actions and consequently affect the entire smart grid infrastructure has also been highlighted.

A. Risk Inspection and Attenuation

Risk is the potential for an unwanted outcome resulting from internal or external factors, as determined from the likelihood of occurrence and the associated consequences [19]. Simply risk may be defined as the union of likelihood of an attack, possible actions that an adversary may pursue and its consequent outcomes.

$$\textit{Risk} = \textit{Likelihood of Attack} \times \textit{Possible Actions} \times \textit{Consequent Outcomes} \quad (1)$$

The first step in risk inspection is identifying the cyber security assets such as hardware devices, network parameters, software schemes and communication protocols. Then multiple testing schemes should be incorporated to check any vulnerability in the existing power system. After the cyber vulnerabilities have been identified, a comprehensive analysis to determine the impact of an attack in both the application and physical layer of the smart grid infrastructure needs to be carried out. This analysis can be done be performed by simulating a real time model and intentionally creating a pseudo cyber-attack to observe the repercussions. Various researches have been done under this domain to assist in analyzing the possible threats and its impact to the supporting infrastructure. Conte *et al.* [21] have studied vulnerabilities in the smart grid using graph-theoretic approach while Kundur *et al*. [22] have modeled the impact of cyber-attacks through graph based dynamical systems. Giani *at el*. [20] have analyzed vulnerabilities and its impact to the legacy SCADA systems by developing SCADA test bed architecture. The analysis of probable threats and its impact to the system environment have been identified; the next step is to find ways to alleviate the probable attacks. Desired security measures and attack resistant smart grid infrastructure needs to be developed and tested in real time environment. The results of the test should be properly examined so as to reduce the possibility of any further vulnerability and propose valid methods and protocols to mitigate such attacks. Also, guidance from security advisories and vendors; and knowledge from already deployed security measures need to be utilized in order to frame a resistant cyber infrastructure. An overview of risk evaluation process is shown in Fig. 3.

B. Probable Attack Points and Adversary Action

A smart grid cyber infrastructure is required to be modeled in such a manner that it is impervious to any invasion in the cyber workspace. This can be achieved only if the probable entry points which allow an adversary to invade the system is assessed. Legacy system which lack built-in security modules in many devices and applications make the system vulnerable. Moreover, for a system with such large number of electrical and electronic connections along with mighty communication channels, it is very difficult to make the entire smart grid cyber-attack resistant. But analyzing the different attack points could help us plan and develop system architectures and protocols which can make the smart grid attack resistant.

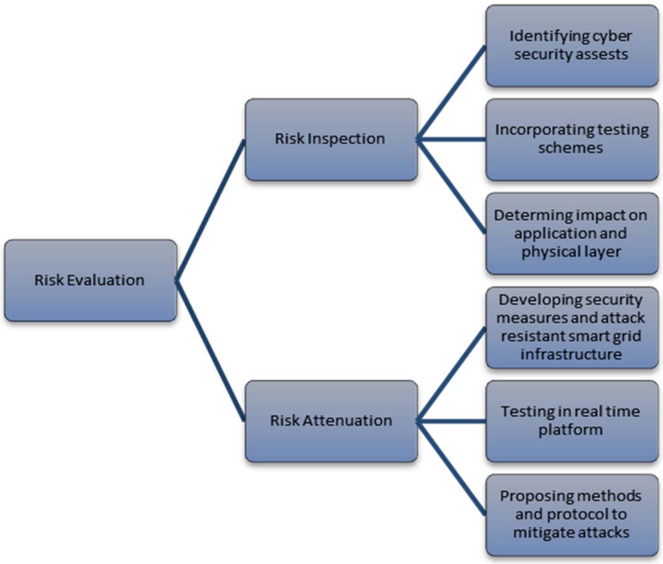
Risk Evaluation
Risk Inspection
Risk Attenuation
Identifying cyber security assests
Incorporating testing schemes
Determing impact on application and physical layer
Developing security measures and attack resistant smart grid infrastructure
Testing in real time platform
Proposing methods and protocol to mitigate attacks

Fig. 3. Risk evaluation process

The various attack points in power industry chain are listed below:

1) Generation System:

- The numerical relays in the generation plants adopt Ethernet based IEC 61850 for information exchange. An adversary may launch a DoS attack causing the relay to mal operate during the fault conditions or may even alter the relay settings causing inadvertent tripping of relays. For example, if an attacker successfully delays the transmission of message in case of trip protection in generating stations then it can cause serious damage to the power equipment.
- Various local control loops including that of speed control, valve control and AVR are linked with plant control center through Ethernet. If an adversary manages to find *security holes* then it can easily gain access inside the local area network (LAN) and plant a Trojan or get a backdoor entry hence enabling the adversary to compromise the digital control modules by disrupting the control logic. This could be the highest level of security threat.

- The generation plants are monitored and controlled by the SCADA system. Legacy SCADA still uses hardcoded passwords, ladder logic and lack authentication. An adversary may easily invade the SCADA system to change frequency measurements provided to the automatic governor control (AGC). Such an attack can directly affect the stability of the system. Mohajerin *et al.* [8] proposed a technique using reachability analysis to measure the effect of an intrusion attack on the AGC loop.

- RTUs and PLCs in power plants generally use MODBUS or DNP3 protocols for communication purpose. The MODBUS protocol does not provide security against unauthorized entry. So an adversary with IP connectivity can corrupt RTUs or PLCs leading to undesired system operation. Similarly, DNP3 protocol also does not employ encryption, authentication and authorization. So an attacker with network access can easily fabricate the messages. Jin *et al.* [23] have shown that "buffer flooding" attack can be easily done on a DNP3 based SCADA network. It is also possible to create "man-in-the-middle" attack [24] between the SCADA and the slave devices (RTUs or PLCs) to get information regarding the network topology and device functionality.

2) Transmission System:

- SCADA is the heart of transmission system at load dispatch centers. It is now applied to larger and wide area networks (WANs) due to advancement in information technology. Although load dispatch centers have independent control, but they are also connected to other centers through a common communication infrastructure. Today many major transmission companies have integrated internet into the communication network for better efficiency and reliability. But this puts the entire system at major risk because if an adversary manages to infiltrate any one of the SCADA networks then it can cause havoc to the entire system operation.

- RTUs and PLCs also have the same vulnerabilities in the transmission system as was in case of generation system. An adversary can specially craft an URL that can be sent to anyone at the control center. As the URL is opened from the HMI connected to the network, a malicious JavaScript snippet is executed in the web browser [18]. This then automatically detects the PLCs connected to that network and invades the system. Such attacks are categorized as Cross-Site Request Forgery (CSRF) attacks.

- State estimation, optimal power flow computation, economic dispatch and unit commitment studies are done by algorithms embedded in software specifically designed to perform computations using thousands of measurements. If an adversary manages to penetrate inside the network and falsely inject "bad data" or "redistribute load" then the system will immediately shift towards unstable operating conditions and impact the smart grid economically as well. Liu *et al.* [9] have created *false data injection* attacks which manage to pass through the security due to bad identification algorithms, provided they had the knowledge of the system configuration. But Yi *et al.* [6] manages to go a step forward and inject *stealth bad data* into the system with linear independent component analysis (ICA) technique even without the knowledge of the network topology.

- HVDC power lines are becoming paramount mode for bulk energy transfer. The present cyber security infrastructure at HVDC links are substandard with no authorization and access control features put into their SCADA network. An adversary can send control signals to change the commutation angle or may even block the power flow causing severe loss of power at the targeted area.

- Modern FACTS devices uses high speed communication link to exchange information with each other during operation–hence increasing the vulnerabilities in the system. An attacker can send incorrect operational data to the FACTS device resulting into unnecessary VAR compensation causing instability.

- Integration of renewable energy forecasts with real time system operations require advanced information technology. Manipulation of wind and solar forecast data sent to the control center can make the power system run haywire affecting system operations such as generation scheduling, dispatch, real time balancing and reserve requirements. Hackers might even go a step forward and reconfigure the entire energy gain and program the wind turbine to reverse its direction. Doing so, would not just harm the system operation, but also damage the wind farms.

3) Distribution System:

- A conventional meter can be modified by reversing the internal usage counter or can be manipulated to control the calculation of electric flow [12]. Intelligent Electronic Devices (IED) like smart meters can be controlled to deploy various functionalities from remote location. This enables an adversary to remotely connect or disconnect the devices or tamper with data sent to the system operator or sneak into confidential data of the consumers. Also, if an adversary manages to send false data packets to inject negative pricing in the system then it will result in power shortages at the targeted area causing loss of revenue to the utility company. Given that there are millions of conventional/smart meters connected to the system, it is difficult to secure every node–increasing the vulnerabilities of the system to manifold times. Anderson and Fuloria [11] have shown that an attacker could switch-off millions of smart meters simultaneously through a remote location. Smart meters also fail to comply to the Open Web Application Security Project (OWASP) standards such as injection, authentication, cross site scripting (XSS), insecure direct object references, security misconfiguration, sensitive data exposure and missing function level access control [17].

- Networking and communication within the AMI infrastructure will rely on technologies like WLAN, ZigBee, RF mesh, WiMax, WiFi and PLC. Wireless Local Area Networks (WLANs) follow IEEE 802.11 standards which by default do not provide authorization mechanisms. This protocol is also vulnerable to traffic analysis [7], eavesdropping and session hijacking attacks. ZigBee is based on IEEE 802.15.4 standards which are vulnerable to jamming attacks. Bennet and Wicker [13] have argued that the conventional ZigBee would suffer from delays due to multi-tier feature of the cluster-tree based routing strategy. Mobile communications are generally unprotected mediums and could reveal energy consumption data and prove susceptible to privacy invasion. Worldwide Interoperability for Microwave Access (WiMax) follows IEEE 802.16 standard which are vulnerable to scrambling and replay attacks [7]. Power Line Communication (PLC) can be susceptible to threats by hostile users on the network using access control to misguide services. Nowadays Ethernet Passive Optical Networks (EPON) is also getting popular for electric power system distribution automation systems in smart grid [14]. But EPON too is vulnerable to attacks such as DoS, eavesdropping and spoofing.

- An adversary can hijack the Virtual Private Network (VPN) of distribution utilities. The effects of slammer worms migrating through a VPN connection to SCADA network are reported in [27]. The worm manages to infect the control center LAN and blocked the SCADA traffic. Such intrusions are particularly dangerous as they can be controlled and monitored remotely.

- Due to lack of authentication and encryption at the Head End System (HES), an attacker can directly tamper the Meter Data Management System (MDMS) and send unauthorized trip signals to the smart meters. Also, an adversary can masquerade smart meters connected at consumers' end and send fake energy usage signals to the control center. Since the software installed at HES cannot spot the ambiguity, it executes the required control and sends command to turn off the smart meter. Such attacks can be very difficult to trace as the attacker impersonates a smart meter. Kosut *et al.* [15] have shown that an adversary can attack the Energy Management System (EMS) by faking meter data. The firmware installed at the HES can be also manipulated by changing the algorithms due to lack of proper access control.

- Consumers having net metering scheme installed at their premises can also fiddle with the net energy usage data sent to the utility's control center by hacking into the communication network of the AMI. The attacker can reduce the electricity bill or may earn credits into their account even if the consumer might not be selling electricity to the grid. This directly does not affect the system operation but increases the losses of distribution companies.

4) *Telemetry Infrastructure:*

Telemetry systems are often neglected during security planning, testing and evaluation process. They connect with control systems and SCADA architecture of various components in smart grid - generation systems, transmission systems, distribution systems and micro grids. Power system telemetry uses standard communication protocols like Modbus, IEC 870-5-10x, DNP3 and Profibus/Profinet. Irrespective of the type of protocol used, most ICS (Industrial Control System) protocols work on "master/slave" model having little or no security features and thus are susceptible to malicious network attacks. If an adversary gains access inside the "master" then the "slave devices" can then be forced to spuriously operate or even erase critical data. The above mentioned points highlight the type of attacks that can be made into the system without any physical presence of an adversary. However, there are certain ways in which system can be infiltrated by physical means.

- A disgruntled employee who has privilege to access the system components might alter the algorithms of software or may even change the settings of devices causing spurious operation. Also corporate data can be stolen from the database for internal rivalry between the competing service providers. Attacker can use key logger software to gain access to system usernames and passwords. Such actions might not only be difficult to detect but also to prevent.

- Devices such as laptops and USB memory sticks that are used both inside and outside the trusted perimeter can get infected with malware outside, and then invade the system when used inside [4].

- Devices can also be compromised before deploying them to the site by changing the source code of software or tampering with the control settings of hardware. Such attacks are supply chain attacks [4].

IV. Data Privacy and Consumer Protection

Data privacy and consumer protection remains top concern for the distribution utilities as well as consumers. Consumers need to gain confidence to share their personal data to the third party service providers or the utilities in order to improve the operational efficiency of the smart grid. In this section, a brief overview of the threats regarding privacy of the consumers has been given. Smart meters installed at the consumers' end exchange information with the home area network (HAN) or building area network (BAN) regarding the data usage of the consumers as well as send control signals to the smart appliances installed at the consumers' premises. These networks however, may be vulnerable to data leakage or eavesdropping that could reveal activities of the consumers and sensitive information like account numbers. For domestic consumers, such data leakage could also reveal information regarding the smart appliances, plug-in electric vehicles

(PEVs) and social networking activity which in turn exhibits consumers' personal behavior [1]. Also real time information of energy usage may disclose whether a residence or facility is occupied, where people are in the structure, what are they doing, and so on [16]. For industrial and commercial consumers, such data leakages can reveal highly sensitive information for example the technologies used, manufacturing output, sale events, etc. This raises the prospect of industrial espionage amongst various competitors. On the other hand, utilities and third party service provider aggregate energy usage data of different consumers for better demand forecast and peak load management. However, it is of growing concern that such personal information can be comfortably accessed by any authorized personnel at the control center– making data privacy and consumer protection a strenuous job for cyber security researchers and developers.

V. Conclusions

Cyber security in smart grid is still under critical stage of development. This paper presents smart gird cyber infrastructure framework with in-depth research directions. It is required to enhance the confidentiality, integrity and availability of the system by building a robust and efficient smart grid cyber infrastructure. Attack detection, mitigation, authentication and key management still remain challenging issues. The countermeasure schemes with protocols for vulnerabilities need to be developed, tested and deployed. It is recommended to have secure protocol by regulatory framework.

References

[1] E. L. Quinn, "Smart metering and privacy: Existing laws and competing policies," *SSRN eLibrary*, 2009.

[2] J. Vijayan, "Stuxnet renews power grid security concerns," *Computerworld*, Jul. 26, 2010.

[3] A. Kerckhoffs, "La cryptographie militairie," *J. Sciences Militaires*, Vol. IX, pp. 5–38, 1883.

[4] Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proc. of the IEEE*, Vol. 100, No.1, Jan. 2012, pp. 195-209.

[5] Electric Power Research Institute, "Report to nist on smart grid interoperability standards roadmap," 2009.

[6] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li and L. Song, "Bad data injection in smart grid: attack and defense mechanisms," *IEEE Communications Magazine*, Jan. 2013, pp. 27-33.

[7] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Communications Magazine*, Jan. 2013, pp. 42-49.

[8] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," *Proc. Amer. Control Conf.*, Jul. 2010, pp. 962–967.

[9] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *Proc. 16th ACM Conf. Comput. Commun. Security*, New York: ACM, 2009, pp. 21–32.

[10] J. Liu, Y. Xiao, S. Li, W. Lian and C. L. Philip Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications Surveys & Tutorials*, Vol. 14, No.4, pp. 981-997, Fourth Quarter 2012.

[11] R. Anderson and S. Fuloria, "Who controls the off switch?" *Proc. 1st IEEE SmartGridComm 2010*, Gaithersburg, MD, Oct. 2010, pp. 96-101.

[12] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security and Privacy*, Vol. 7, No. 3, May/Jun. 2009, pp. 75-77.

[13] C. Bennett and S.B. Wicker, "Decreased time delay and security enhancement recommendations for AMI smart meter networks," *Innovative Smart Grid Technologies (ISGT 2010)*, Gaithersburg, MD, Jan. 2010, pp. 1-6.

[14] Z. Sun, S. Huo, Y. Ma, and F. Sun, "Security mechanism for smart distribution grid using ethernet passive optical network," *2nd International Conference on Advanced Computer Control* (ICACC 2010), Vol. 3, Shenyang, China, Mar. 2010, pp. 246-250.

[15] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: attack strategies and countermeasures," *Proc. 1st IEEE SmartGridComm 2010*, Gaithersburg, MD, Oct. 2010, pp. 220-225.

[16] U.S. NIST, "Guidelines for smart grid cyber security (Vol. 1 to 3)," NIST IR-7628, Aug. 2010,

[17] Open Web Application Security Project, "Top 10 OWASP, 2013," Aug. 21, 2015

[18] Eduard Kovacs, "Flaws in rockwell PLCs expose operational networks," *Security Week*, Oct. 28, 2015.

[19] U.S. NIST, "NIST framework and roadmap for smart grid interoperability standards, release 1.0," *NIST Special Publication 1108*, Jan. 2010.

[20] A. Giani, G. Karsai, T. Roosta, A. Shah, B. Sinopoli and J. Wiley, "A testbed for secure and robust SCADA systems," in: *SIGBED Review*, Vol. 5, No. 2, Article No. 4, 2008

[21] D. Conte de Leon, J. Alves-Foss, A. Krings and P. Oman, "Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack," *Proc. First Workshop on Scientific Aspects of Cyber Terrorism*, Washington DC, 2002.

[22] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," *Proc. IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 244–249.

[23] D. Jin, D.M.Nicol, G. Yan, "An event buffer flooding attack in DNP3 controlled SCADA systems," *Proceedings of the 2011 Winter Simulation Conference*, 2011.

[24] I. Fovino, A. Carcano, M. Masera, and A. Trombetta, "Design and implementation of a secure Modbus protocol," *Critical Infrastructure Protection III*, Vol. 311, C. Palmer and S. Shenoi, Eds. Boston, MA: Springer-Verlag, 2009, pp. 83–96.

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

[26] J. Yu, A. Mao, Z. Guo, "Vulnerability assessment of cyber security in power industry," *Proc. of IEEE Power and Energy Society General Meeting* (PES '06), 2006, pp. 2200–2205.

[27] North American Electric Reliability Council, "SQL slammer worm lessons leanred for consideration by the electricity sector," Jun. 2013.