A Review on Cyber Security Issues and Mitigation Methods in Smart Grid Systems

Maneli Malek Pour, Arash Anzalchi, and Arif Sarwat
Department of Electrical and Computer Engineering
Florida International University
asarwat@fiu.edu

***Abstract*—The future power system will be an innovative administration of existing power grids, which is called smart grid. Above all, the application of advanced communication and computing tools is going to significantly improve the productivity and consistency of smart grid systems with renewable energy resources. Together with the topographies of the smart grid, cyber security appears as a serious concern since a huge number of automatic devices are linked through communication networks. Cyber-attacks on these devices has a direct influence on the reliability of extensive infrastructure of the power system. In this survey, several published works related to smart grid system vulnerabilities, potential intentional attacks, and suggested countermeasures for these threats have been investigated.**

I. Introduction

THE influence of cyber-attacks on the renovated structure of power system has been one of the burning issues in the recent years. As a result of its extremely integrated architecture, the smart grid (SG) is further exposed to virtual threats and attacks [1]. The SG is a power delivery infrastructure includes various energy measures, resources, and technologies such as smart meters, virtual power plants (VPPs), microgrids, renewable energy resources, and communication technologies [2]–[4]. It provides the two-way flow of power and information, controls, and optimizes the production and distribution of electricity through high-voltage network from the power generator to energy storage systems and end user consumers [5]–[8].

The implementation of the SG requires utilization of multiple communication mechanisms, power electronic devices, electric vehicle charging stations, etc. which are considered as the heart of SGs [9]–[11]. Because of extensive integrated topology of the SGs and their communication systems, they are more weak in the occurrence of cyber threats. In this survey, general vulnerabilities for the SG system has been introduced firstly (Section II). These weaknesses cause various cyber-physical attacks on the SG. Common attacks and the cyber-physical impact of them are covered in Section III. Then, in Section IV some countermeasures and solutions for the attacks have been presented, and at the end, the paper is concluded in section V.

This work was supported by the National Science Foundation under grants CPS-1446570 and CAREER-1553494. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

978-1-5386-1539-3/17/$31.00 ©2017 IEEE

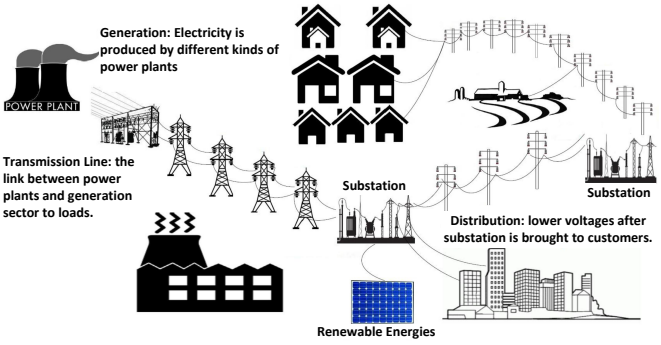

Fig. 1. a schematic structure for the SG system describing its major technologies

Figure 1 below shows a schematic structure for the SG system describing its major technologies.

There are three key security concepts that should be met in every cyber system: confidentiality, integrity, and availability. In the SGs, confidentiality refers to putting authorized limitations on information in the personal privacy of consumers using the SG technologies and the SG normal operations. Integrity refers to protecting against incorrect information alteration and destruction, in order to prevent corruption of important data exchange, and guarantee the authenticity and validity of stored data. This data can be related to customers (e.g., account balance of customer and information on pricing) or network operations (e.g., running status of devices, voltage readings). Lastly, availability refers to ensuring that a reliable and timely access is provided for authorized users, and denying their access is not possible for an unauthorized user or system [12], [13].

II. Cyber System Vulnerabilities of Smart Grid

Consumers' Lack of Awareness: a comprehensive and strong security architecture for the SGs, including all important features required to analyze and detect the attacks, needs a huge investigation that might not be affordable for utilities alone. Therefore, the customers need to learn adequately about the risks, costs, and advantages of the SG systems, because of the demand for a higher level of security, and support the utilities, both for themselves and the society.

Young and Unknown Technologies: many new technologies are adding to the SG which could be eye-catching to hackers and opponents for the reason that their point of weaknesses and security regulations has not been recognized

yet. Therefore, finding a gap to exploit the vulnerabilities would be simple.

Scalability: is defined as a system ability to update its scale based on the growth in the size of demand. The SG technologies are considered as potential solutions for controlling the complex electrical power systems, which are widely growing in population and technology. It is obvious that the growth in the quantity of circulating data and energy flows, the SG protocols, and the size of network structure directly affect the size and complexity of the SGs. This volume of information and complexity might cause data accumulation, and control efficiency destruction, if not handled and accommodated properly in the SG. Therefore, efficient data flow construction solutions are required to prevent these problems in the system [14].

The Weaknesses Received from Joined Communication Technologies: applying existing ICTs in the structure of the SGs can lead to inheriting almost all the susceptibilities and unresolved problems (e.g., routing problems, IP spoofing, Denial of Service attacks, etc.) from these technologies to the SG system.

Lack of Standards and Regulations: interoperability of a SG refers to the ability of various systems to work cooperatively, interchange equipment or data from each other, and use the harmonious parts to perform a task. To achieve interoperability, standards and regulations must include each part of the SG. It is also worthy to mention that novel protocols publishing continuously, sometimes cause security missing in the SGd (e.g., Distributed Network Protocol)

III. Cyber-physical Attacks in Smart Grid

Man-in-the-Middle Attack: the Man-in-the-Middle (MITM) attack is a type of eavesdropping, wherein the adversary tries to make separated connections with a risky communication at both endpoints and transmits information in between. Moreover, the authorized users at the endpoints think they are talking directly to each other using their personal connection. Some utilities still apply normal User Datagram Protocol (UDP), in order to transmit the data measured by Phasor Measurement Unit (PMU), without other cyber protections, such as SSL. This can increase the chance of exploitation for MITM attacks. In addition, for the network from substation to control center, which called Wide Area Network (WAN), some of the utility companies use the public communication line, which is vulnerable to network attacks, and some other utility companies use private communication line, in which the attacker can use the hardware access to enter. The MITM attacks are generally applied to corrupt information including control commands, values of measurements, pricing signals, etc., in the transferred packets, and also exploit important parts of the system for coming attacks, by accessing the observations of control center operators [12].

Distributed Denial of Service Attack (DDoS): in the WAN, there are some vulnerabilities to access PMU communication network. The malwares can be installed on the router located at the substation, or communication network can be accessed by guessing the default password considered for the devices. A DoS attack tries to make an important resource inaccessible to its authorized users in a suitable volume when needed. In the power system, all communication channels must be available as much as possible, specifically when the power system is closing to an instability point where an important control action required. If the DoS attack is successful in such a situation, the reliability needed for the modern power grids will be at risk [12].

The DDoS attack is a type of DoS attack, which is used by infected (often by Trojan program) multiple risky systems to target a single system. It is a potential cyber threat in Advanced Metering Infrastructure (AMI), which often includes two phases: (1) agents recruitment phase, and (2) actual attack phase [15].

1) *Agents Recruitment Phase:* to initiate a DDoS in AMI network, an attacker first needs to recognize the weak meters which are considered as the agents. A large number of homogeneous devices in AMI network makes it possible that a security error in a single meter exists in many other meters. Then the attacker communicates with many IP-based smart meters that have already been infected with malicious code. Instead of entering a large number of agents, the attacker can implant the malicious program or change the firmware in the middle of the communication session by exploiting hardware and software weaknesses. A suitable propagation model to distribute attack malware should be chosen. The attacker can put the malicious program in a file source, and each agent copies the code from it(repository model), can make the risky agent download the malware from the attacking host(Back-chaining Model), or can infect and exploit the agents without agents necessity to download the malware from an allocated source(The Autonomous model). IP spoofing can be applied to hide the infected agents, which makes the process of finding the source of attack among a huge number of meters harder [15].
2) *Actual Attack Phase:* three categories of possible attack mechanism to launch a DDOS attack on AMI infrastructure are [15]:
    - Attacks on protocol: the attacker could exploit the vulnerabilities of the protocol to consume users resources. For instance, a TCP SYN flooding attack can be used to deactivate the service on data collecting unit or head-end of AMI environment which is using Transportation Control Protocol (TCP).
    - Attacks on infrastructure: The attacker may deliberately interrupt the routing tables to worsen the action efficiency of packet distribution in AMI packet-exchange network.
    - Attacks on bandwidth: many agents can be manipulated to send an exceeding volume of communication packets to the system user. Therefore, the flooding traffic will make the authorized user drop some of the legitimate packets (the drop ratio can be considerable).

False data injection attack [16]: as a well-crafted type of integrity attack, false data injection attack is able to have

an impact on the operation and control of SGs by passing the bad data detection systems through state estimation, and the compromised sensors are made to mimic the events that do not occur actually. The attacker could inject the malicious data to a randomly chosen vector, or a specific meter to disturb the state variables. The latter is more serious attack since the attacker knows adequately about the network topology, and cause preset changes in the state variables. The detection of malicious data attacks is more complicated if critical meters have been compromised. Some conventional techniques, which protect specific critical sensors in the power system, can relieve the false data injection attacks.

These attacks can have various types regarding the type of the attacked meters (e.g. in load alteration attacks and load relocation attacks, load meter quantity is altered to initiate a cyber attack on the SG.

Jamming attack [17]: is a type of Denial of Service (DoS) attack, which can be applied to affect the communications in real-time. The state estimation and online checking can be unsuccessful to show the real operating status of the system as a result of jamming, and the related electricity price will be computed in error. The main motivation for initiating the attack is manipulating the prices in power market. The pricing mechanism depends on the state estimation from the sensors which would be unavailable to the control center, when the jamming occurs.

One of the methods of Jamming attack is discrete time method which consists of time intervals. Only a limited number of sensors out of the whole wireless sensor networks (WSNs) can be attacked in SG, basically because an exceeding jamming attack may cause wide area power failure which results an error in price manipulation. Moreover, a wide-area jamming attack can enhance the detection probability.

The procedure of jamming attack is as follows:

1) When a time interval starts, particular channels in the network are jammed to make measurements unavailable and leave real-time prices at related buses undetermined.
2) The control center replaces the unavailable measurements by default values in the DC optimal power flow model.
3) During a time interval, the adversary observes the power market and jams the doubtful measurements.
4) After stopping the jamming, the adversary can anticipate real-time prices having the access to real-time measurements.
5) 5. The adversary can buy power at lower price and sell it in higher value by comparing the real-time in the middle of jamming and after that, in order to take advantage from the difference between these two prices

IV. Countermeasures and Protective Actions Against Cyber Attacks

A. IP Fast Hopping mechanism

Many methods are introduced based on the point of time the guarding against DDoS attacks occurs. Two categories are defined for these approaches: a) Attack prevention methods, which include refining protocol and overall system security level, resource allotment & accounting, firewalls, etc., and b) Attack detection methods, which include attack source recognition and appropriate reaction [15].

As an instance of the prevention mechanisms, IP Fast Hopping, is proposed which to refine even huge malicious streams. It is a new method that can be applied to hide details and endpoints of users communication period to counteract exhausting of servers resources initiated by DDoS attacks. It covers the actual IP address of the server between large numbers of imaginary IP addresses. The transferring of the real IP address on one of the imaginary addresses is unique for each communication period, and the imaginary IP address is changing in real-time based on a specific schedule. Only the legitimate user is able to have access to the information of schedule changing to send a request to a real IP address, limiting the ability of an attacker to produce high load on the server. This approach is distributed as it distributes the authorized users traffic in some sub-streams and causes load reduction on network system during attack [18].

B. Encryption Mechanisms [19]

Many standard encryption algorithms and authentication structures are employed to improve the confidentiality and integrity (which are two of main security concepts) of the data and protect against potential threats in the SG. As it was declared in previous studies, the device cost and power consumption should be taken into account in cryptography design.

There are several categories of encryption mechanisms. One of them is Symmetric encryption algorithms, which include some well-known models such as DES (Data Encryption Standard), Triple DES, and AES (Advanced Encryption Standard). For instance, ZigBee uses 128-bit AES encryption. Another category is asymmetric encryption algorithms, and as it said in previous works Asymmetric encryption algorithms are generally more costly than Symmetric ones in computational-based point of view.

Symmetric code effectively manages the huge volume of data, while usually has a shorter lifetime in compare with the asymmetric cipher. Changing the symmetric cipher with a specific manner is recommended and becomes an important issue in SG, in which there are a huge number of widely distributed objects.

The encryption key management is a controversial and essential concern in applying cryptographic algorithms for the SG. Public key infrastructure (PKI) is the base for a most efficient key management system in the SG. All of the suggested methods employ an external team or system for authentication recognition or key generation, which can lead to extra cost for tools and increase in communication traffic. Some novel methods which are recently proposed a focus on the privacy aspect of smart metering data, protecting home area network (HAN), improving the efficiency and security of advanced metering infrastructure (AMI), and securing the information aggregation in SG.

C. IDS-based Technologies

Supervisory Control And Data Acquisition (SCADA) systems in the application of the SG will unavoidably contain legacy systems that cannot be updated, protected, or repaired by conventional Information Technology security methods, due to the lack of built-in security for SCADA systems, and inadequate computation resources for legacy devices. Hence, Intrusion Detection System (IDS) technologies in the IT domain are required to control the operation of such systems and to detect threats, coming from mistakes of authorized users or deliberate attacks. Many intrusion detection approaches addressed the SCADA systems, have been proposed, such as Statistics- based intrusion detection methods, and SCADA-specific intrusion detection approaches, which has recently started to develop.

IDSs uses statistical methods to categorize network traffic as usual or unusual in SCADA systems. In order to build the statistical models, various modeling methods like regression models, neural networks, and Bayesian networks can be applied. Nevertheless, most statistical intrusion methods produce false positives resulting in false alerts, and false negatives resulting in problems for identifying actual attacks [20].

A typical IDS consist of agents, management or database servers, and user interface. There are three categories for the IDS methods: centralized, embedded and dedicated. The IDS can infer potential detrimental or suspicious activities by checking corresponding physical or cyber events, e.g., doubtful power failure notifications from a certain client, unusual log information, unusual traffic for communication, and several lacks of communication cases. Three possible detection mechanisms are stateful specification-based monitoring, a stateless specification based monitoring, and anomaly-based monitoring. In addition to detection mechanism, the whole system security level must be maintained by the protector, doing activities such as deleting software bugs, updating firmware and protocols, repair software timely, etc [15].

SCADA-specific IDSs employ critical state, model, and rule-based approaches for SCADA systems. However, there is not enough information regarding the variety of SCADA protocols and applications. Several types of research have been presented in this regard such as critical state-based IDS for SCADA on the basis of Modbus protocol in a power station, model-based controlling methods to discover unknown attacks in SCADA systems, A rule-based IDS for an intelligent electronic device (IED) based on IEC 61850, etc [20].

V. Conclusion

Cyber security in the SG is a fresh research topic that has been the center of attention in the industry section, government, and universities. In this study, vulnerabilities of the SG, different kinds of attacks in the system and some countermeasures to increase the security of the future power systems have been discussed.

As it is reviewed, cyber security is still progressing in the SG, and because of structures of the SG communication network, it is almost unrealistic to uniformly organize robust security methods all over the SG.

References

[1] A. Anzalchi and A. Sarwat, "A survey on security assessment of metering infrastructure in smart grid systems," in *SoutheastCon 2015*, April 2015, pp. 1–4.

[2] M. A. Salmani, A. Anzalchi, and S. Salmani, "Virtual power plant: New solution for managing distributed generations in decentralized power systems," in *2010 International Conference on Management and Service Science*, Aug 2010, pp. 1–6.

[3] A. Anzalchi and A. Sarwat, "Analysis of carbon tax as an incentive toward building sustainable grid with renewable energy utilization," in *2015 Seventh Annual IEEE Green Technologies Conference*, April 2015, pp. 103–109.

[4] A. Anzalchi and B. Mozafari, "Wind-pv-grid connected hybrid renewable system in kish island," in *International Review on Modelling and Simulations (I.RE.MO.S.)*, vol. 4, no. 6, April 2011, pp. 3376–3382.

[5] A. Anzalchi, M. Moghaddami, A. Moghaddasi, M. M. Pour, and A. Sarwat, "A modified higher order power filter for grid-connected renewable energy systems," in *2016 IEEE/IAS 52nd Industrial and Commercial Power Systems Technical Conference (I CPS)*, May 2016, pp. 1–9.

[6] A. Anzalchi, M. M. Pour, and A. Sarwat, "A combinatorial approach for addressing intermittency and providing inertial response in a grid-connected photovoltaic system," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, July 2016, pp. 1–5.

[7] A. Anzalchi, M. Moghaddami, A. Moghaddasi, A. I. Sarwat, and A. K. Rathore, "A new topology of higher order power filter for single-phase grid-tied voltage-source inverters," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 12, pp. 7511–7522, Dec 2016.

[8] A. Anzalchi and A. Sarwat, "Artificial neural network based duty cycle estimation for maximum power point tracking in photovoltaic systems," in *SoutheastCon 2015*, April 2015, pp. 1–5.

[9] A. Moghadasi, M. Moghaddami, A. Anzalchi, A. Sarwat, and O. A. Mohammed, "Prioritized coordinated reactive power control of wind turbin involving statcom using multi-objective optimization," in *2016 IEEE/IAS 52nd Industrial and Commercial Power Systems Technical Conference (I CPS)*, May 2016, pp. 1–9.

[10] M. Moghaddami, A. Anzalchi, A. Moghadasi, and A. Sarwat, "Pareto optimization of circular power pads for contactless electric vehicle battery charger," in *2016 IEEE Industry Applications Society Annual Meeting*, Oct 2016, pp. 1–6.

[11] M. Moghaddami, A. Anzalchi, and A. I. Sarwat, "Finite element based design optimization of magnetic structures for roadway inductive power transfer systems," in *2016 IEEE Transportation Electrification Conference and Expo (ITEC)*, June 2016, pp. 1–6.

[12] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sept 2015.

[13] W. Stallings and L. Brown, *Computer Security: Principles and Practice*, 3rd ed. Upper Saddle River, NJ, USA: Prentice Hall Press, 2015.

[14] C. D. Cameron, P. Taylor, and C. Patsios, "Scalability in smart grid data flow architectures," in *2014 49th International Universities Power Engineering Conference (UPEC)*, Sept 2014, pp. 1–6.

[15] Y. Guo, C. W. Ten, S. Hu, and W. W. Weaver, "Modeling distributed denial of service attack in advanced metering infrastructure," in *2015 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Feb 2015, pp. 1–5.

[16] K. Khanna, B. K. Panigrahi, and A. Joshi, "Feasibility and mitigation of false data injection attacks in smart grid," in *2016 IEEE 6th International Conference on Power Systems (ICPS)*, March 2016, pp. 1–6.

[17] J. Ma, Y. Liu, L. Song, and Z. Han, "Multiact dynamic game strategy for jamming attack in electricity market," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2273–2282, Sept 2015.

[18] V. Krylov, K. Kravtsov, E. Sokolova, and D. Lyakhmanov, "Sdi defense against ddos attacks based on ip fast hopping method," in *2014 International Science and Technology Conference (Modern Networking Technologies) (MoNeTeC)*, Oct 2014, pp. 1–5.

[19] T. Liu, Y. Liu, Y. Mao, Y. Sun, X. Guan, W. Gong, and S. Xiao, "A dynamic secret-based encryption scheme for smart grid wireless communication," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1175–1182, May 2014.

[20] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, and H. F. Wang, "Multiattribute scada-specific intrusion detection system for power networks," *IEEE Transactions on Power Delivery*, vol. 29, no. 3, pp. 1092–1102, June 2014.