Ensuring a Secure and Resilient Smart Grid: Cyber-Attacks and Countermeasures

Charalambos Konstantinou
Electrical and Computer Engineering
NYU Polytechnic School of Engineering
E–mail: ckonstantinou@nyu.edu

***Abstract*—Over the past years, advanced Smart Grid technologies are deployed in order to enhance grid efficiency and resiliency. Their increased dependency on cyber-resources however, has an immediate impact to the exposure of grid devices to potential vulnerabilities. This paper surveys the latest on Smart Grid security. Specifically, it focuses on the deep understanding of the risk in terms of threats, vulnerabilities and consequences that arise from cyber-attacks. Further, it explores relevant published literature for defense and mitigation techniques against Smart Grid attacks.**

I. Introduction

The most critical infrastructure domain today is the electric power grid since its reliable operation is correlated with the proper functioning of all the other critical infrastructure sectors. During the last years, Information and Communication Technologies (ICT) modernize the current grid by establishing dynamic and interactive communication between the power equipment. However, the inadequate level of security measures prior the implementation of those technologies led to a greater threat landscape. It has shown [1] that non-compliance with the highest levels of security within the grid may result to a variety of severe effects that may have an impact on data integrity and even cause degradation of systems' availability.

The transition of power grid from a centralized, producer-controlled network to a decentralized, consumer-interactive network is already under-way. Power systems are becoming increasingly dependent on modern devices and computer communication. Hence, new security and privacy challenges arise since the potential risks are growing. Network connections increase potential cascade failure, the growing number of interconnections results in the creation of new paths to undermine systems, the large number of smart nodes multiply the entry points for Denial of Service (DoS) attacks and in general the complexity of the new formed system increases errors and potential attackers. For example, many communication protocols in Energy Management Systems (EMSs) and Supervisory Control And Data Acquisition (SCADA) systems were not designed for critical-security environments, thus several attacks are possible [2] [3]. Firewalls mainly do not detect intrusions through insider connections or trusted parties. Monitoring and communication devices usually use Ethernet and TCP/IP connections, for higher speeds and for minimizing the cost, although they are vulnerable to various attacks [4] [5] [6], e.g. TCP SYN and IP spoofing. Modern processor-based power grid devices may be infected with malware prior their placement and installation into the system. Therefore, research community should move towards to the development of new solutions based on the new developed Smart Grid architecture and considering the potential cyber-security threats.

The ultimate aim of Smart Grid is to enhance reliability, efficiency and security. The latter must be examined carefully since malicious threats and consequently cyber-attacks in electric power systems are increasing. Cyber-security efforts focus on attack prevention and defense strategies, while the first step to deploy protection mechanisms is the understanding and detection of security breaches within the network. The objective of this paper is to provide an overview of the threat surface of Smart Grid, examine cyber-security risks and attacks and finally review proposed security solutions to thwart those attacks.

The rest of the paper is organized as follows. Section II examines the network architecture of power grid and identifies the differences between the Industrial Control System's (ICS) security concerns and the Information Technology (IT) environment; this Section also provides information on attack methodologies against the energy sector based on real cyber-security incidents. Section III presents related work on existing proposed security solutions for the Smart Grid infrastructure and discuss some of the constraints that may exist for each methodology. Finally, Section IV concludes the paper and indicates guidelines for future work.

II. Threat Landscape of Smart Grid

A. Network Architecture of Smart Grid

The network structure of electric power grid indicates that it is a highly complex physical system. For instance, statistics [7] in 2010 showed that there are more than 130 million customers, over 2000 power distribution substations and about 5600 distributed energy centres and all over the US. The conceptual model of Smart Grid network, presented in Fig. 1, illustrates that Smart Grid consists of seven logical domains: Bulk Generation, Transmission,

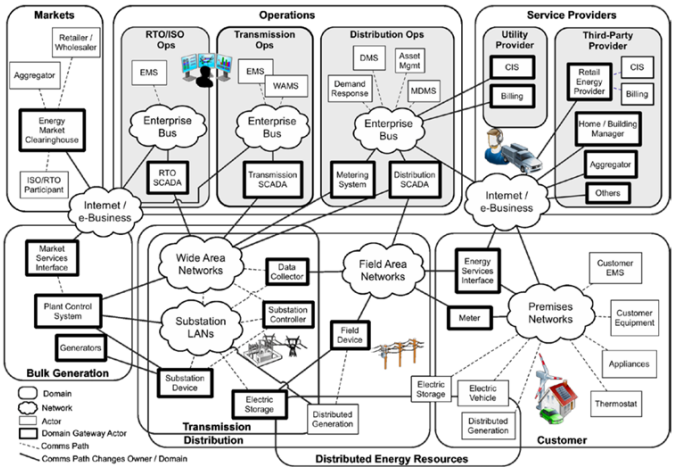

Fig. 1. Conceptual Reference Diagram for Smart Grid Information Networks [12].

Distribution, Customer, Markets, Service Provider and Operations. The first four domains can generate, store and deliver electricity in a two-way communication technology. The rest domains essentially manage the power flow and provide necessary information or services to power utilities.

A key component of Smart Grid's network is the SCADA system. SCADA technologies are responsible for monitoring and control the vital functions of generation, transmission and distribution domains. SCADA systems consist of four basic components [8]: field interface devices (e.g. Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs)), a communication system (e.g. radio, cable, satellite), a central Master Terminal Unit (MTU), and Human Machine Interface (HMI) systems or software.

Smart Grid is a combination of the power grid and communication networks, thus communication protocols and standards consist another primary part of the grid's architecture. The most common protocols for communication in the grid are IEC60870-5 and DNP3 [8]. The former one is mostly used in Europe for the communication between RTUs and MTU in SCADA systems [9] [10]. In Asia and North America the most prevalent used protocol is DNP3 which is currently being replacing by IEC 61850 since it supports more enhanced capabilities including a peer-to-peer communication mode for field devices [11].

The Smart Grid phenomenon is like an "Internet of watts" [13] because of the similarities between the Smart Grid network (as an ICS) and the Internet (as the main element of an IT environment) in terms of hierarchical structure and complexity. However, there are fundamental differences between these two systems in many features [14]. For example, performance and reliability requirements are different between them. Furthermore, different risks and priorities must be assigned in each system; the prioritization of security attributes in the ICS environment compared to IT systems is reversed. Availability and integrity are primary concerns, while confidentiality is pushed aside to ensure easy and fast dataflow between critical components in real time without security and reliability failures. Nevertheless, evidently Smart Grid devices being in use today such as relays and data concentrators are based on microprocessor architectures and therefore are perceptive to attacks whose roots arise from traditional attacks against the cyber-infrastructure.

B. Growing Threats

The development of Smart Grid in terms of better control and higher reliability requires the establishment of security mechanisms in order to support the new sophisticated features. In the past, several real world examples have shown that the power grid as an ICS is exposed to various threats that can lead to severe consequences.

In April 2001, hackers installed a rootkit into the network of California Independent System Operator (Cal-ISO). While the attacks were on going, rolling blackouts swept the state affecting over 400,000 utility customers [15]. In January 2003, Slammer worm exploiting a buffer overflow vulnerability on Microsoft's SQL Servers, overload networks and disabled data servers. Thereafter, the monitoring system of Ohio's Davis-Besse nuclear power plant was offline for five hours [16]. In January 2008, CIA claimed that a cyber-attack had caused a multi-city power outage at an unspecified location outside the U.S [17]. Operation Night Dragon, uncovered in 2010, was targeting oil, gas and energy companies using common hacking tools in order to find project details and financial information about oil-gas exploration and bids [18]. The Stuxnet incident (discovered in 2010) and its relatives Duqu, Flame and Gauss are some of the most talked-about cases of targeted attacks [19]. While the Duqu, Flame and Gauss focused on traditional espionage scopes, Stuxnet [20] presented a foundational shift in malware with its ability to usurp the operation of an ICS by manipulating PLCs using four zero-day vulnerabilities and spreading through injected portable media drives.

As cyber-security concerns have grown, the identification of vulnerabilities that exist within ICS architectures and more precisely within the platforms supporting the electric grid should be examined thoroughly. Analysis performed by the National Institute of Standards and Technology (NIST) [14] determined vulnerabilities that may be found in typical ICSs, and proposed guidelines for addressing these issues. Particularly, policy and procedure vulnerabilities must be examined thoroughly based on the established guidelines and management systems. Network and platform vulnerabilities can be mitigated through various security controls such as OS and application patching, security software, encrypted network communications etc. However, trying to enumerate all possible threats and vulnerabilities in the Smart Grid is not practical taking into account the system's complexity and the fact that new types of attacks are based on zero-day exploits. In addition, even vulnerabilities are well known, the problem is escalating.

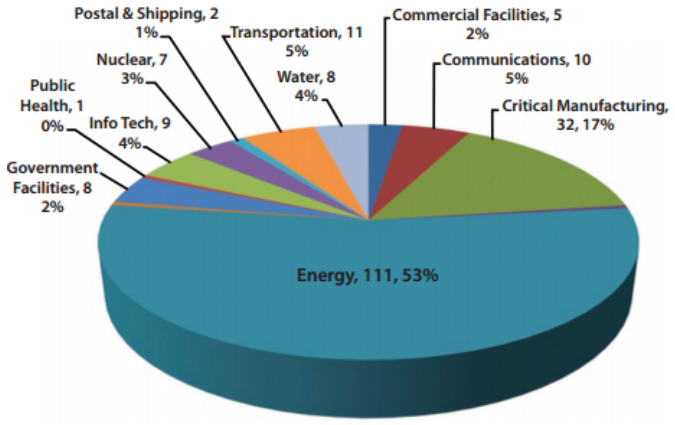

Fig. 2. Cyber-incidents reported to ICS-CERT from October 2012–May 2013 across all critical infrastructure sectors [21].

In the latest monitor report [21] of Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) the received notifications for incidents across all critical infrastructure sectors were more than 200. As shown in Fig. 2, 53% of the incidents hit the energy sector and the majority of them involved cyber-attacker techniques; in other words, attacks are determined as "*deliberate actions which alter, disrupt, degrade or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks*" [22].

C. Attacks Classification and Methodologies

This section makes an introduction to malicious attacks which could induce catastrophic damage to the Smart Grid. After reviewing NIST guidelines [1] and existing research on cyber-security, pertinent issues are categorized into two major groups, attacks that could compromise systems and devices and attacks that could impact the communication of the Smart Grid.

1) Systems and Devices:

Software Vulnerabilities: Buffer overflows, integer overflows, and Structured Query Language (SQL) injection can provide an attacker with the ability to disrupt the normal operation of devices such as PLCs, RTUs and IEDs [23] [24]. In addition, many control systems are running firmware and operating systems with published vulnerabilities making them open for attacks [25] [26].

Malware: An attacker can develop malicious software [27] and spread it on target systems. Specifically, malware can be used to replace or add any function to a device or system (e.g. smart meters [28], PLCs [20]). For example, it can inject malicious control communication programs [29], send sensitive information and manage the control operation of devices.

Authentication: NIST requirements [1] recommend that each device has a unique key and credentials so that, if one is attacked, others will not be affected. However, many devices lack of authentication support, hence unauthorized users could gain access and manipulate system settings and operations [30], [31].

Malicious Insider: An authorized employee or in general a legitimate user can access privileged system's resources to perform malicious actions. Insider's knowledge of the defense mechanisms allow him to easily circumvent protection settings and deploy a powerful attack [32].

Portable Media: Most devices used in Smart Grid infrastructure are not directly connected to untrusted networks (e.g. Internet). Nonetheless, media or devices can be infiltrated inside the trusted perimeter by personnel causing malware transferring into the system (e.g. Stuxnet [20]).

Supply Chain: Backdoors or malicious codes can be installed into devices prior the shipment to the target location. That may provide access to unauthorized users [33] without having physical system access.

2) Communications:

Vulnerabilities in Common Protocols: The existing protocols used in the Smart Grid inherit their vulnerabilities into the grid components. For example Modbus client-server protocol was designed for low-speed serial communication in process control networks. Therefore, it cannot address security issues and several attacks are possible: broadcast message spoofing attack, baseline response replay attack, response delay attack etc. [34]. Furthermore, widely adopted IP-based protocols (e.g. IEC 61850 [11] uses TCP/IP as a part of its protocol stacks) have vulnerabilities that may result in DoS attacks [4] [5] [6].

Firewalls: Firewalls consist an essential part of the network perimeter, hence their poor configuration settings can be detected and leveraged by attackers as entry points into the system; and therefore led them to inject large number of packets into the network that may cause congestion and limits to the network's availability [35].

False Data Injection: An adversary can attack the Smart Grid by attacking the EMS via faking meter data (replay attack) and misleading EMS by the state estimator to make bad decisions [36]. Also, if an attacker has already compromised one device he can take advantage of the configuration of a power system to launch attacks by injecting false data to the monitoring center [37] causing a huge financial impact on electricity markets [38].

Identity Spoofing: Identity spoofing attacks allow attackers to impersonate an authorized user [27] and hence spoofed messages into the network appear as they originate from a trusted system. For example, if the attacker can manipulate some network address (e.g. Address Resolution Protocol (ARP)) [39] or routing mechanisms Man in the Middle (MitM) attacks can be launched to the network. MitM attacks due to possible routing layer vulnerabilities such as weak authentication protocols or poor integrity checking [40] in firmware may eventually enable DoS attacks [1].

Virtual Private Network (VPN): VPNs create secure encrypted connections (tunnels) to make sure of secure and confidential data transmission between a client device and a server device. However, VPN only secures the tunnel and

TABLE I
TAXONOMY OF BASIC CYBER-ATTACKS IN SMART GRID

Device attack: Compromise the control of a grid device. Usually the first step of a sophisticated attack.
Data attack: Insert, modify or delete data in the network traffic in order to mislead Smart Grid's decision systems.
Privacy attack: Learn or infer users private information by analyzing electricity usage data.
Network availability attack: Delay or cause failure of communications due to alterations on computational and communication resources of Smart Grid.

not the client or the server. If the VPN is not integrated into a suitable firewall then an attacker could hijack the VPN connection [41].

Eavesdropping: Monitoring network traffic gives the opportunity to attackers to gather, examine and thus deduce information from communication patterns, compromising the confidentiality of communications in the Smart Grid. A typical example is to sniff IP packets on the Local Area Network (LAN) or intercepting wireless transmissions on the Home Area Network (HAN) [42].

Access through Database Links: Databases used in ICS are often connected to computers or databases with web-enabled applications located on the business network. Gaining access to the database on the business network allows attackers to exploit the communication channel between the two networks and hence bypass the security mechanisms used to protect the control systems environment [43].

The aforementioned cyber-attacks can be classified into four broad categories based on their security objectives and consequences at the time of their deployment, as presented in Table I [44].

III. SECURITY COUNTERMEASURES

To maintain the reliability and stability of the Smart Grid as a system, cyber-security protection technologies are necessary for defending against adversary actions. Since threats are constantly evolving, protection demands advanced cyber-security mechanisms. Thus, the development of a secure Smart Grid should encounter the following fundamental security techniques for defending the above mentioned cyber-attacks:

A. Devices

Malware Protection: In previous research [45] a method for firmware diversity is presented, capable of significantly slowing a large-scale compromise of smart meters. It proposes a form of return address encryption to protect addresses on the stack that can be implemented via binary rewriting.

Communication: Zhang *et al.* [31] proposed a 256-bit Advanced Encryption Standard (AES) as a security solution for the traffic between two Smart Grid devices in Ethernet networks. In their design, all data packets in Ethernet networks consist of four fields: one header and three data fields (16 bytes). The header contains the destination IP address and all other nodes except the recipient cannot read the data payload and will simply discard it. To indicate whether a message is encrypted or not, the header adds an extra AES status flag; thus this message may be transmitted through other networks. Experiment results indicate that the data transmission is secure assuming there are no eavesdroppers on the Ethernet network.

Specification-based Intrusion Detection System (IDS): Berthier *et al.* [46] after studying the threat models and constraints of Advanced Metering Infrastructure (AMI), they analyze the requirements for host intrusion detection design. Based on a literature survey they propose that the best IDS solution for AMI is a specification-based detection technique which identifies deviations from a correct behavior profile using logical specification. A machine learning algorithm is shown in [47] which classifies fixed-length patterns generated via sliding window techniques [48] to infer the classification of variable-length patterns from the aggregation of the machine learning based classification results.

IDS via Attestation: A propitious new approach to provide remote code verification is a technology called attestation. Code attestation enables an external entity to inquire the software that is executing on a system in a way that prevents malware from hiding. Since attestation reveals a signature of executing code, even unknown software will alter that signature and thus can be detected. LeMay *et al.* have studied hardware-based approaches for attestation [49] [50]. Software-based attestation is an approach that does not rely on specialized hardware, but makes some assumptions that the verifier can uniquely communicate with the device under verification [51]. Shah *et al.* demonstrate the feasibility of this concept on SCADA devices [52].

Authentication: Fouda *et al.* [53] propose a lightweight two-step mutual authentication protocol by combining the public key encryption scheme [54] and Diffie-Hellman key agreement scheme [55]. Based on the proposed protocol forward secrecy is guaranteed since each session requires random numbers which are deleted after the generation of the session key. Since field devices in the Smart Grid often have limited storage space, the authors in [56] addressed the authentication issue from a storage load minimization perspective. According to their findings, the proposed one-time signature scheme reduces the signature size by 40% and the storage load on receiver by a factor of 8. Both authentication schemes [53] [56] adopt public key cryptography without specifying how public keys are managed.

Smart Meter Data Privacy: Kalogridis and Efthymiou [57] [58] propose a method that transforms customer's electrical energy signature to hide behavioral patterns. In Smart Grid metering there are two types of data: low-frequency data (periodic power use summary–cannot cause

privacy leakage) and high frequency data (detailed power usage patterns related to users private lives). The idea is to assign each smart meter two IDentification signatures, one for Low-Frequency data transmission (LFID) and the other for High-Frequency data transmission (HFID). The authors focus on the initial device registration process when a smart meter joins the grid. Using two separate steps, the smart meter first informs the utility about its LFID and the LFID public key, which in turn passes them to the proper community gateway. At the second step, the smart meter sends its HFID and HFID public key to a trusted third party (escrow), and the escrow forwards them to the control center. Since the utility is not involved in the second step, the HFID remains unknown.

B. Network

Smart Meters Communication: Li *et al.* [59] propose a data aggregation protocol that can be used to aggregate Smart Meter communications to a gateway. The protocol uses a spanning tree rooted at the gateway device, and performs aggregation at each node by combining child node packets and sending the resulting packet to its parent. This protocol uses homomorphic encryption to protect the privacy of the data. Also, Bartoli *et al.* [60] analyze the trade-off between security and efficiency and design two algorithms for per-hop and end-to-end communication protocol respectively. An AES-Counter with Cipher Block Chaining-Message Authentication Code (AES-CCM) is used with 128 bit shared key to encrypt the line between the meter and the gateway and according to their experiment results ensures that their protocol is reliable and energy efficient.

Topology Design: A network topology represents the connectivity structure among nodes, which can have an impact on the robustness against attacks. Lee *et al.* [61] examine the resiliency of Internet topologies under attacking strategies, with various metrics including ”path-failure ratio” and ”attack power” (ratio of the failure to attack). The idea presented can be expanded to the Smart Grid network topology because of the routes' similarities which an attacker must follow to achieve his purpose. Experiments in the paper reveal that ”path-based” attacks can result in greater damage to the connectivity of a network than other types of attacks. Thus, connecting networking nodes to be highly resilient under attacks can be the basis to build a secure communication architecture in the Smart Grid.

Protocols: IEC 61850 communication standard defines data formats and interoperability technologies for communication in power systems [11]. IEC 61850 intends to replace DNP3 in substation communications and additionally it is believed that can be potentially used for outside substation communication in future power systems [62]. Zhang and Gunter [63] propose a prototype multicast system SecureSCL (Secure Substation Configuration Language) to handle publish-subscribe connections in IEC 61850 power substation networks. Using a cross-layer approach they aim to secure substation's inter-communications based on IPsec multicast. Algorithms were also developed to detect four classified multicast configuration anomalies.

Other protocols should also be taken into account for secure communications. IEC 62351 for example, is a support standard for IEC 61850 related to security and technical requirements of vendors. Fries *et al* [11] indicate that IEC 62351 should be updated due to issues related with demand response and customer participation in the grid.

Authentication requirements are also important for the design or the upgrade of communications protocols used in the power grid system. Wang *et al.* [64] propose an efficient multicast authentication scheme named ”TV-HORS” which combines one-way hash chains with ”TV-OTS”, a novel signature model – Time Valid One Time Signature – in order to avoid frequent public key distribution. The scheme according to their results minimizes the computational cost, it has low communication overhead, and it is robust to malicious attacks. Those requirements are also the base for the proposed authentication scheme ”DREAM” [65].

Communication Channel Capacity: Li *et al.* [66] work towards the determination of communication channel capacity that is needed to guarantee security. The used model which can be applied to a simplified dynamic Smart Grid model, considers a single receiver and sender, and it is assumed that there is an eavesdropper listening. The information from the calculation of the channel capacity could be eventually essential for the determination of a secure network topology for the Smart Grid.

IDS Modules: Zhang *et al.* [67] propose a hierarchical IDS framework, where an IDS module is installed distributedly along the network hierarchy. Particularly, on SCADA control centers in the top layer, on community gateways in the middle layer and on smart meters in the bottom layer. Each module has two components: a recorder (for logging and accuracy evaluation) and a classifier (for attack classification). According to the authors, the classifier must be trained before put in use (e.g. machine learning techniques such as Support Vector Machines (SVMs)) in order to invoke an alarm if an attack is detected.

Wired, Wireless and Sensor Networks: Networking security problems in the Smart Grid environment mostly focus on issues of the wired, wireless, and sensor networks. For wired networks, Sun *et al.* [68] propose that Ethernet Passive Optical Networks (EPON) would be a promising solution for the Smart Grid broadband access networks. For wireless networks, the NIST report [1] states that schemes like 802.11i would improve the deployment of secure Smart Grid wireless networks. Moreover, Metke and Ekl [69] argue that wireless Smart Grids could be further secured with existing standards like 802.16e (Mobile WiMax) and 3GPP LTE. For sensor networks, proposed solutions [1] [69] [70] include that wireless mesh networks should be

deployed in the AMI in order to overcome bad links by using redundant communication paths. However, wireless mesh technologies are vulnerable to several attacks such as message modification, route injection, cross-layer traffic injection, etc. [1]. Existing routing protocols lack techniques to secure the data and the paths due to their inherent distribution features [1]. Without routing security, traffic in the AMI is not reliable. Bennett and Wicker [70], however, among other recommendations, propose the solution of establishing a dedicated path between two communication nodes to address "black hole" attacks against the AODV (Ad Hoc On Demand Distance Vector) routing protocol.

Ethernet Switches, Firewalls and Gateway Controllers: The power grid has two major directional information flows: bottom-up and top-down. Therefore, Ethernet switches, firewalls and gateway controllers are valuable for cyber-security because they are the gatekeepers to substations. The above mentioned components can contribute to the necessary network separation such as Demilitarized Zones (DMZs) but most importantly, they could perform traffic control on information flows in Smart Grid to block undesired or even suspicious flows generated by malicious nodes [71].

C. Management

Cryptography: Cryptographic approaches are becoming primary countermeasures against malicious cyber-attacks. Additional to the encryption and authentication procedures [31] [60] [30] [31] [53] [56] [64] [65] key management processes are also part of cryptographic methods. Insufficient management of the key process may result in possible key disclosure to adversaries and eventually jeopardize the purpose of secure communications in the grid. Public key Infrastructure (PKI) is a classic public key management system which publishes the public key values used in public key cryptography. The necessity for PKI arises from the trust assumptions behind digital signature verification. When the scale is large (such as the power grid infrastructure) a PKI is needed using digital signatures to establish trust that a given public key is owned by a particular identity. PKI is not by itself an authentication, authorization, auditing, privacy or integrity mechanism; it is an infrastructure that supports these needs and operations. It does not infer trust by itself, but requires the establishment of a trust base, on which PKI can rely. That means that the basis of trust must be established on a particular lever, e.g. business level, before it can be accepted by the PKI. Thus, *PKI is a system that is used to create, storage and distribute digital signatures which verify that a particular key belongs to a certain entity.*

A good example to deploy PKI technology into the Smart Grid is proposed by Hayden *et al.* [72]. By using an identity-based cryptograph (IBC) method, the authors address the authenticity and confidentiality issues in an AMI communication network. According to the implementation results, their design does not require a complex setup procedure and is scalable in terms of small packet overhead (128 bytes). The proposed mechanism however, requires a central key-generating server to distribute a private key for a certain device or a user. In general, there are some constraints regarding cryptography and key management [73] related to communications (different channels have dissimilar bandwidths), devices power and storage (do not have enough processing power and storage to perform advanced encryption and authentication techniques), and connectivity (all devices, certificate authorities, and servers, must be connected at all times).

TABLE II
SECURITY TECHNIQUES FOR DEFENDING BASIC CYBER-ATTACKS

Devices: Malware Protection, Communication, Specification-based IDS, IDS via Attestation, Authentication, Smart Meter Data Privacy
Network: Smart Meters Communication, Topology Design, Protocols, Communication Channel Capacity, IDS Modules, Wired, Wireless and Sensor Networks, Ethernet Switches, Firewalls and Gateway Controllers
Manangement: Cryptography, Access Control

Access Control: In order to limit the access only to authorized personnel, Cheung *et al.* [74] propose a Smart Grid role-based access control (SRAC) strategy. Each regional network in this model, preserves the security policy for the inside community and residential networks and also operates as the communication interface with users from other regional networks according to the predefined role constraints. For instance, users may have multiple roles, but conflict of interest of those roles must be prevented. The authors suggest an XML-based security policy and based on case studies show that the proposed SRAC model is effective.

The above mentioned countermeasures against cyber-attacks are summarized in Table II.

IV. CONCLUSIONS

This paper presents an overview of security related issues on the Smart Grid environment. It examines the architecture of the current grid infrastructure and present threats and vulnerabilities that arise from the highly complexity of the grid as a system. Also, it enumerates possible cyber-attack techniques able to exploit the security breaches of the power grid infrastructure. Finally, related work on existing and future security solutions is presented. In the future, a platform profiling methodology will be developed, based on monitoring and controlling grid components internally (through hardware performance counters), externally (through network profiling) and in an intermediate stage (through the system board, JTAG, and external connections).

REFERENCES

[1] National Institute of Standards and Technology. (2010) Guidelines for smart grid cyber security, NIST IR-7628. http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

[2] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, "Attack taxonomies for the modbus protocols," *Critical Infrastructure Protection*, vol. 1, pp. 37–44, 2008.

[3] S. East, J. Butts, M. Papa, and S. Shenoi, "A taxonomy of attacks on the dnp3 protocol," *Critical Infrastructure Protection*, vol. 3, pp. 67–81, 2009.

[4] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on tcp," in *IEEE Symposium on Security and Privacy*, 1997.

[5] A. Yaar, A. Perrig, and D. Song, "Pi: A path identification mechanism to defend against ddos attacks," in *IEEE Symposium on Security and Privacy*, 2003.

[6] M. J. and R. P., "A taxonomy of ddos attack and ddos defense mechanisms," *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, 2004.

[7] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, "GridWorks: Overview of the Electric Grid," http://sites.energetics.com/gridworks/grid.html, 2010.

[8] National Communications System, Technical Report, "Supervisory Control and Data Acquisition (SCADA) systems," http://www.scadahacker.com/library, 2004.

[9] S. Ward and et al., "Cyber security issues for protective relays," *IEEE Power Enginnering Society General Meeting*, pp. 1–27, 2007.

[10] S. Hong and M. Lee, "Challenges and direction toward secure communication in the scada system," in *8th Annual Communication Networks and Services Research Conference*, 2010, pp. 381–386.

[11] S. Fries, H. Hof, and M. Seewald, "Enhancing iec 62351 to improve security for energy automation in smart grid environments," *The 5th International Conference on Internet and Web Applications and Services (ICIW 2010)*, pp. 135–142, 2010.

[12] National Institute of Standards and Technology, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, Special Publication 1108R2."

[13] Alstrom Grid and Intel and McAfee, "Smart Grid Cyber Security," http://www.mcafee.com/us/resources/white-papers/wp-smart-grid-cyber-security.pdf, 2013.

[14] National Institute of Standards and Technology, "NIST Guide to Industrial Control Systems (ICS) Security, Special Publication 800-82."

[15] SANS Institute, "Can Hackers Turn Your Lights Off? The Vulnerability of the US Power Grid to Electronic Attack," http://www.sans.org/reading-room/whitepapers/hackers/hackers-turn-lights-off-vulnerability-power-grid-electronic-attack-606.

[16] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," *IEEE Security and Privacy*, vol. 1, no. 4, pp. 33–39, 2003.

[17] A. Paller, "Cia confirms cyber attack caused multi-city power outage," *SANS Newsbites*, vol. 10, no. 5, 2008.

[18] McAfee Foundstone Professional Services and McAfee Labs, "Global Energy Cyberattacks: Night Dragon," http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

[19] B. Bencsth, G. Pk, L. Buttyn, and M. Flegyhzi, "The cousins of stuxnet: Duqu, flame, and gauss." *Future Internet*, vol. 4, no. 4, pp. 971–1003, 2012.

[20] T. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[21] "ICS-CERT," http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013.pdf.

[22] W. A. Owens, K. W. Dam, and H. S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. The National Academies Press, 2009.

[23] Idaho National Laboratory, "Vulnerability Analysis of Energy Delivery Control Systems," 2011.

[24] Davis, M., "SmartGrid Device Security Adventures in a new medium ," http://www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf, 2009.

[25] 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.

[26] R. Anderson and S. Fuloria, "Who controls the off switch?" in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 96–101.

[27] J. Wang, *Computer Network Security*. Beijing: Higher Education Press and New York: Springer Berlin Heidelberg, 2009.

[28] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 244–249.

[29] I. N. Fovino, A. Carcano, M. Masera, and A. Trombetta, "An experimental investigation of malware attacks on scada systems," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 4, pp. 139–145, 2009.

[30] Wightman, R., "Hacking and Exploiting PLCs," 2012.

[31] P. Zhang, O. Elkeelany, and L. McDaniel, "An implementation of secured smart grid ethernet communications using aes," in *IEEE SoutheastCon 2010 (SoutheastCon), Proceedings of the*, 2010, pp. 394–397.

[32] S. Spoonamore and R. L. Krutz, "Smart Grid and Cyber Challenges," http://www.whitehouse.gov/files/documents/cyber/.

[33] M. Rogers and C. D. Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," in *U.S. House of Representatives, 112th Congress*, 2012.

[34] Y. Mo, T.-H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[35] T. Nash, "Backdoors and holes in network perimeter," http://ics-cert.us-cert.gov/control_systems/, 2005.

[36] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 220–225.

[37] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 21–32.

[38] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 226–231.

[39] U. Premaratne, J. Samarabandu, T. Sidhu, R. Beresh, and J.-C. Tan, "An intrusion detection system for iec61850 automated substations," *Power Delivery, IEEE Transactions on*, vol. 25, no. 4, pp. 2376–2383, 2010.

[40] DHS, "Common cyber security vulnerabilities observed in dhs industrial control systems assessments," http://ics-cert.us-cert.gov/control_systems/, 2009.

[41] G. Dondossola, "Smart grid cyber security, the value of risk," http://www.ieee-isgt-2012.eu/wp-content/uploads/2012/08/Value-of-Risk_Dondossola_IEEE-PES-ISGT-Europe-2012.pdf, 2012.

[42] D. Dzung, M. Naedele, T. von Hoff, and M. Crevatin, "Security for industrial communication systems," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1152–1177, 2005.

[43] DHS, "Improving industrial control systems cybersecurity with defense-in-depth strategies," http://ics-cert.us-cert.gov/control_systems/, 2009.

[44] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing

smart grid: cyber attacks, countermeasures, and challenges," *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 38–45, 2012.

[45] S. McLaughlin, D. Podkuiko, A. Delozier, S. Miadzvezhanka, and P. McDaniel, "Embedded firmware diversity for smart electric meters," in *5th USENIX Workshop on Hot Topics in Security (HotSec 2010)*, 2010.

[46] R. Berthier, W. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 350–355.

[47] N. Stakhanova, S. Basu, and J. Wong, "On the symbiosis of specification-based and anomaly-based detection," *Computers and Security*, vol. 29, no. 2, pp. 253–268, 2010.

[48] K. Ku-Mahamud, N. Zakaria, N. Katuk, and M. Shbier, "Flood pattern detection using sliding window technique," in *Modelling Simulation, 2009. AMS '09. Third Asia International Conference on*, 2009, pp. 45–50.

[49] M. LeMay, G. Gross, C. A. Gunter, and S. Garg, "Unified architecture for large-scale attested metering," in *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, ser. HICSS '07. IEEE Computer Society, 2007.

[50] M. LeMay and C. Gunter, "Cumulative attestation kernels for embedded systems," *Smart Grid, IEEE Transactions on*, vol. 3, no. 2, pp. 744–760, 2012.

[51] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, "Swatt: software-based attestation for embedded devices," in *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*, 2004, pp. 272–282.

[52] A. Shah, A. Perrig, and B. Sinopoli, "Mechanisms to provide integrity in scada and pcs devices," 2008.

[53] M. Fouda, Z. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 675–685, 2011.

[54] S. Aboud, M. Al-Fayoumi, M. Al-Fayoumi, and H. Jabbar, "An efficient rsa public key encryption scheme," in *Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on*, 2008, pp. 127–130.

[55] J. Herzog, "The diffie-hellman key-agreement scheme in the strand-space model," in *Computer Security Foundations Workshop, 2003. Proceedings. 16th IEEE*, 2003, pp. 234–247.

[56] Q. Li and G. Cao, "Multicast authentication in the smart grid with one-time signature," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 686–696, 2011.

[57] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 232–237.

[58] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 238–243.

[59] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 327–332.

[60] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure lossless aggregation for smart grid m2m networks," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 333–338.

[61] H. Lee, J. Kim, and W. Lee, "Resiliency of network topologies under path-based attacks," in *IEICE Trans. Commun.*, vol. E89-B, 2006, p. 28782884.

[62] S. Mohagheghi, J. Stoupis, and Z. Wang, "Communication protocols and networks for power systems-current status and future trends," in *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, 2009, pp. 1–9.

[63] J. Zhang and C. Gunter, "Application-aware secure multicast for power grid communications," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 339–344.

[64] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, "Time valid one-time signature for time-critical multicast data authentication," in *INFOCOM 2009, IEEE*, 2009, pp. 1233–1241.

[65] Y. Huang, W. He, K. Nahrstedt, and W. Lee, "Dos-resistant broadcast authentication protocol with low end-to-end delay," in *INFOCOM Workshops 2008, IEEE*, 2008, pp. 1–6.

[66] H. Li, L. Lai, and R. Qiu, "Communication capacity requirement for reliable and secure state estimation in smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 191–196.

[67] Y. Zhang, L. Wang, W. Sun, R. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 796–808, 2011.

[68] S. Zhongwei, H. Sitian, M. Yaning, and S. Fengjie, "Security mechanism for smart distribution grid using ethernet passive optical network," in *Advanced Computer Control (ICACC), 2010 2nd International Conference on*, vol. 3, 2010, pp. 246–250.

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

[70] C. Bennett and S. Wicker, "Decreased time delay and security enhancement recommendations for ami smart meter networks," in *Innovative Smart Grid Technologies (ISGT), 2010*, Jan 2010, pp. 1–6.

[71] I. Barda, "Cyber security for advanced smart-grid applications," *ISGF conference*, 2013, http://indiasmartgrid.org/en/.

[72] H.-H. So, S. Kwok, E. Lam, and K.-S. Lui, "Zero-configuration identity-based signcryption scheme for smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 321–326.

[73] S. Iyer, *Cyber Security for Smart Grid, Cryptography, and Privacy*. International Journal of Digital Multimedia Broadcasting, 2011.

[74] H. Cheung, A. Hamlyn, T. Mander, C. Yang, and R. Cheung, "Role-based model security access control for smart power-grids computer networks," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, 2008, pp. 1–7.