Journal of Energy and Power Engineering 9 (2015) 632-647
doi: 10.17265/1934-8975/2015.07.005

# Smart Grid Cyber Security: An Overview of Threats and Countermeasures

Carlos Lopez[1, 2, 3], Arman Sargolzaei[1, 2], Hugo Santana[1] and Carlos Huerta[1]

*1. PLC (Power Line Carrier) International Inc., Smart Communication Systems, Miami, FL 33155, USA*

*2. Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174, USA*

*3. US Naval Research Laboratory Corrosion Science and Engineering, Washington DC 20375, USA*

Received: February 27, 2015 / Accepted: May 04, 2015 / Published: July 31, 2015.

**Abstract:** The smart grid is the next generation of power and distribution systems. The integration of advanced network, communications, and computing techniques allows for the enhancement of efficiency and reliability. The smart grid interconnects the flow of information via the power line, intelligent metering, renewable and distributed energy systems, and a monitoring and controlling infrastructure. For all the advantages that these components come with, they remain at risk to a spectrum of physical and digital attacks. This paper will focus on digital vulnerabilities within the smart grid and how they may be exploited to form full fledged attacks on the system. A number of countermeasures and solutions from the literature will also be reported, to give an overview of the options for dealing with such problems. This paper serves as a triggering point for future research into smart grid cyber security.

**Key words:** Smart grid, power line communications, smart metering, threats, vulnerabilities, countermeasures, solutions.

## 1. Introduction

The power grid is the infrastructure which transports electricity from where it is generated, coal plants, natural gas refineries, nuclear reactors and others. The traditional power grid involved large centralized electric power plants. These plants fed power over a one-way channel from the distributor to the user. It served its function over the last century, but it has recently been subject to deregulation and is burdened with several issues ranging from the technical to the economic [1]. The advent of newly improved telecommunications techniques for control and monitoring of energy flow made the creation of the smart grid possible [2].

The smart grid is the next generation power grid in which electricity is managed and distributed in advanced two-way communication systems. It delivers power from suppliers to consumers in a way that it controls intelligent appliances to save energy, reduce cost, increase reliability, as well as transparency [3]. Fig. 1 illustrates the smart grid architecture, where a central control can mitigate the generation of power via numerous sources such as coal, wind, solar, nuclear and others. This power is then transmitted to various distribution centers and organized via various concentrations pertaining to the spectrum of consumers, such as households, universities, businesses and others. There are five key factors to consider for the efficient operation of the smart grid: communications, smart metering, distributed energy resources, monitoring and controlling [3, 4].

Communication across the power line uses feeder section lines as a medium between consumers and utilities [3]. Communication also happens through microwave channels, fiber-optic links, wireless, Ethernet,

**Corresponding author:** Arman Sargolzaei, Ph.D. candidate, research fields: security of networked control systems, smart grid, control and power systems, nonlinear systems and telecommunication. E-mail: a.sargolzaei@gmail.com.

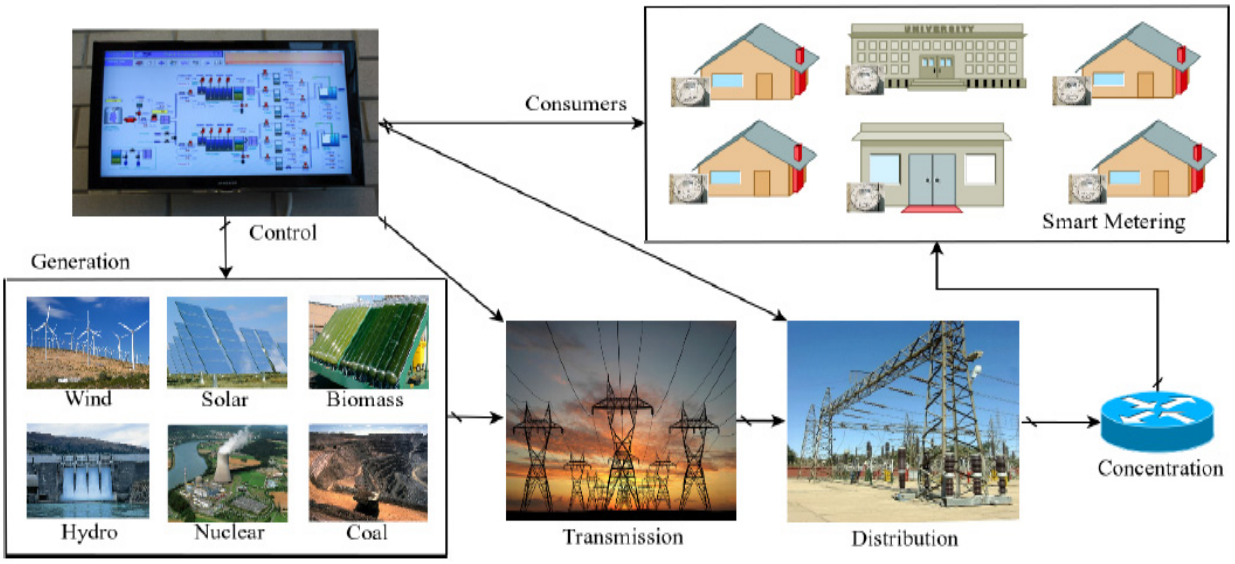


**Fig. 1 Smart grid layout.**

as well pilot wire cables, where a wide range of bandwidths are implemented [5]. Smart metering implements intelligent devices for real time monitoring of energy consumption [6]. The distribution of energy resources allows for the moving away from centralized power stations to more widely available options as well the inclusion of alternative energy supplies [7, 8]. SCADA (supervisory control and data acquisition), defines standards for the operation, monitoring and controlling of grid industrial processes [9, 10].

As mentioned previously, the smart grid allows for more efficient energy distribution than its predecessor, however, Refs. [1, 11-15] demonstrates that, the smart grid is vulnerable to security threats at both the physical and logical layer. Threats from the physical layer are theft, vandalism and sabotage, while protecting the logical layer means protecting the data. The smart energy sector has been subject to a wide spectrum of attacks over the last five years. Web-based applications and SCADA systems are vulnerable to entities coming between the data and the data-gathering system, such as the Stuxnet worm which hit Iranian power stations in 2010 [16]. It has been demonstrated in 2011 [17], that the load on devices can be increased overflowing levels over the internet. The metering network can be compromised and deny consumer services, according to the work of Berthier, et al. in 2012 [18].

Several solutions and countermeasures to these problems have been proposed in Refs. [2, 11, 14, 19-22]. At the metering level, they would involve more widely distributed intrusion detection techniques or minimizing the information load of metering devices. Further research on the encryption of the data is fundamentally important, according to the Government Accountability Office [23]. Another high priority R & D challenge, according to Ref. [20], is the manipulation of cryptographic public key infrastructure of the network to account for the increased complexity of the smart grid.

This paper provides the results of comprehensive literature review to identify useful techniques, algorithms, and other methods which can be applied to cyber security problems related to the smart grid. Following the introduction, the paper is organized as follows: Section 2 includes smart grid infrastructure, detailing key components; Section 3 will provide an overview of the wide spectrum of possible attacks that the smart grid is vulnerable to; Section 4 shows

possible countermeasures and solutions that will secure smart grid operations; the paper concludes in Section 5.

## 2. Smart Grid Overview

### *2.1 Smart Metering*

A smart meter is a device which identifies electricity consumption and other information to a corresponding utility for monitoring and billing purposes. The meters communicate with the line and utility systems via a centralized headend, called AMI (advanced metering infrastructure). The AMI connects to large numbers of smart meters in order to serve large districts [4]. Research bears out that the metering infrastructure of the grid can be broken down into a hierarchical structure [24]. Smart appliances: connected through a local HAN (home area network) to a smart meter through which energy consumption data is reported [25]. Smart meters: measures power consumption and sends data to a concentrator node through a NAN (neighborhood area network) [25]. Concentrator nodes: collects data from all nearest neighbor smart meters and has capability to process data from particular devices via a WAN (wide area network) [26]. Utility centers: stores and processes data for billing and monitoring grid status [4].

### *2.2 Power Line Communications*

In general, power lines are designed for the transmission of AC power at 50-60 Hz. Attaching a PLC (power line carrier) system to a communication system involves a transmitter and receiver between a feeder line two way connection with utilities [3]. Connecting PLC transceivers to the grid line requires coupling circuits to drive PLC signals into the power line and protect communication equipment from high current main signals [27]. PLC signals respect CENELEC (European Electrotechnical Standards Organization) and FCC (Federal Communications Commission) standards, where they can be subdivided according to low and high voltage and frequency ranges, respectively [28].

Narrowband channels operate at low and high voltages and support low to medium data rate (up to 100 Kb/s) applications, such as power consumption measurements [29]. Broadband channels operate at low to medium voltages and support high data rate (up to 100 Mb/s) applications, such as video phones, relaying applications, SCADA, voice and data. A widely used modern technique called OFDM (orthogonal frequency division multiplexing) was implemented in the early 2000's and continues to the present day. This is used to encode multiple carrier frequencies within a single line for use in distribution automation and advanced metering management within the smart gird [3, 30]. Other widely used forms of modulation include SSB (single side band) and QAM (quadrature amplitude) [31].

### *2.3 Distributed Energy Resources*

The old central power source and transmission framework is changing to the paradigm of a massively distributed spectrum of variable and small renewable energy sources [3]. These include wind [32], solar, and other alternatives which could act as stand alone supplies. Regardless of the sort of generation, the growth of these energy alternatives in the market must be respected due to several key factors [33]: Government regulations promote and in some cases mandate their use; tax breaks provide financial incentive; they reduce the load on transmission line systems; they lower the need for traditional large power plants; they help in peak shaving, adding temporary power to the grid when peak loading happens.

Every DER (distributed energy resource) includes an EPP (electronic power processor) to govern the exchange power between it and the grid, along with a SPI (switching power interface) to control drawn currents [3]. The research by Tenti and Mattavelli [34] details the importance of both EPP's and SPI's

working together to take full advantage of smart grid capability. When this occurs, the work of Castabeber [35] demonstrates that DERs become even more attractive in terms of management convenience. Individual DERs effectively act as micro grids and successful cross-communication with nearest neighbor EPP's allows for exploitation of such functionalities without a central supervisor.

Microgrids are small-scale power grids which can be made smart when controlled through two-level control: analog-centric for power stability and digital-centric for automation [36]. Military and academic institutions have taken to the use of microgrids in order to increase power availability in adverse conditions and reduce energy usage costs [37-39]. The ability to run microgrids in so-called island mode provides high local reliability, though this causes difficulty in correlating its supplies with those of the main grid. This has been addressed through the use of stochastic modeling techniques by Liang and Zhuang [40]. These techniques implemented state evolution modeling in order to capture the trajectory of the evolution of operational states of devices within the microgrid and its connection to the main grid. State estimation was used to estimate the states of the power system based on real time measurements, these being analog, logic, and pseudo measurements which amount to predictive information on power generation and loading. Reliability analysis was performed implementing Monte Carlo simulations, where scenarios (output states) are randomly generated based on a probablity density function and the outputs as organized as viable system operational states.

### *2.4 Monitoring and Control*

IEDs (intelligent electronic devices) are microprocessor based devices used for the protection, automation, control and monitoring of power system hardware. Upon acquiring power system data, IEDs perform calculations which create local databases about the specific asset they are monitoring, examples of which include system health or performance history on primary equipment such as transformers, capacitor banks and circuit breakers [41]. Synchronizing events in time at the substation level typically involves GPS (global positioning system) receivers, distributing clock signals through those generated by orbitting satellites. IED's utilize precise timing methods like the IRIG-B (inter range instrumentation group B) and SNTP (simple network time protocol) standard to provide better accuracy and precision [42].

IRIG-B signals are composed of 100 bits produced every second, 74 of which contain time-of-year and year information in BCD (binary coded decimal) format, with identifier bits referencing the start and end of a frame [43]. These signals can be transmitted by a range of media, such as shielded cables and optical fibers for unmodulated data and coaxial or shielded twisted-pair cable for modulated data [43]. SNTP is a version of the NTP (network timing protocol), which is a technique for transferring time data between computers over a data network [44]. SNTP is the simple version of NTP, meaning that it lacks state estimating capabilities. This makes it more ideal for sending substation timing information between a server (sourced by GPS signals for example) and a client (a specific IED).

SCADA protocols set the standard for data transmissions over communication channels and exist at the generation, transmission and distribution level [10]. It provides for the automation of monitoring and data acquisition of the grid, linking back to a control center via a gateway system. The DNP3 (distributed networking protocol 3.0), IEC (International Electrotechnical Commission) 61850, IEC 62351 and other protocols are implemented for the secure communication of power system data [2]. DNP3 was initially designed for the transmission of serial data, based on RS-232 (recommend standard number 232) standards and others, but has recently been ported to the TCP/IP (transmission control protocol/internet protocol) layer for use in two-way communications.

IEC 62351 is used to establish Ethernet-based communications for power substations. They specify protocols at the TCP/IP, UDP (user datagram protocol)/IP and MAC (message authentication code) layers and define the timing requirements for information exchange [2]. IEC 61850 uses the security specifications of IEC 62351 in order to provide for data modeling, reporting, transfer and storage of substation configuration data [12].

In response to the 2003 North American blackout, the FERC (Federal Energy Regulatory Commission) committed the NERC (North American Electric Reliability Corporation) to be the ERO (Electric Reliability Organization) for the United States. NERC enforces CIP (critical infrastructure protection) standards 002-009, which provide frameworks for identifying and protecting critical electronic assets which support reliable power grid operations [45]. NERC standards specify government mandated requirements for cyber asset identification, security controls, training, security parameters, physical security, systems security, incident reporting and recovery plants [46].

## 3. Threats, Vulnerabilities and Attacks

### *3.1 Metering Infrastructure Attacks*

#### 3.1.1 Compromising the Physical Meter

Meters can be hacked directly by accessing onboard memory, thereby reading diagnostic ports and other network interfaces. Some of the tools used by hackers are either hardware tools available for purchase or open source software tools. Prime examples of both, respectively, are the SecureState "Termineter" [47] and the InGuardian "OptiGuard" [12]. Both Termineter and Optiguard are sets of Python based libraries designed to provide functionality for the C12.18 and C12.19 ANSI (American National Standards Institute) communication protocols. The C12.18 protocol is a set of standards for two-way communication between meters and their optical (infrared) serial ports [48]. Communication is established via an ANSI type 2 optical probe. The intruder takes advantage of the C12.18 protocol to open the port, allowing C12.19 standardized data to pass through it. The C12.19 protocol allows for the viewing of meter table data, this includes meter identity, operating mode, configuration mode, status, measurements and more [49].

#### 3.1.2 NAN Sniffing and Eavesdropping

NAN sniffing is used to capture a smart meter's consumption data by breaking network encryption [24]. This allows attackers to learn the communication protocol used in a meter. This information would allow for the creation of false consumption reports and can set the stage for larger scale attacks. The eavesdropping attack undermines the confidentiality of the metering reports by an adversarial party. This third party does this by monitoring network traffic and can obtain data such as future price information, control structure, and power consumption [50].

In the laboratory, the work of Valli [51] saw the capturing of NAN packets from a meter by placing it inside of a Faraday cage and exposing their equipment to a range of frequencies. In this work, they were able to capture packets by letting their devices listen in on the radio emissions of a meter using the ZigBee standard [52]. They found that, packets were collected from the meter's HAN and were able to determine that the packets were encrypted.

#### 3.1.3 Jamming and Access Restriction

A jamming attack is used to prevent meters from connecting with the utility company through stuffing the wireless media with noise. This can be implemented in two fashions: continuous noise signal emission causing the channel to remain blocked; and noise signal emission only in response to the sensing of normal radio channel signals [53]. Smart meters are thusly affected in two corresponding ways: The channel will always be seen as busy by carriers; and data packets will be prevented from being received [53].

A restriction attack disrupts meter operations at the

MAC address layer. The attacking entity prevents the meter from initiating legitimate MAC address operations and can cause data packet collisions [53]. This attack is characterized by the fact that, it targets communications channels such that preference is given to the adversarial signal as opposed to those of legitimate meters [53].

The work of Lazos and Krunz detailed the channel selective jamming attack, which targets control channels in a wireless mesh network [54]. Their work analyzed the selective jamming on carrier signal sensing MAC protocols, which essentially checks a multiple node channel to see if traffic can flow through it. The studied channel used a split phase design, where time measuring signals are split into alternating control and data transmission phases.

Each node converges to a default channel for assignment negotiation during the control phase. Selective targeting of the default channel can lead to the signal jamming in the control phase. This forces the node to defer channel negotiation until the next default phase, forcing inactivity during the transmission phase, effectively stopping the channel. Wireless mesh networks have been shown to be important for the exchange of information in the smart grid [55]. Jamming of this kind can lead to catastrophic effects on the communications infrastructure of the grid's devices and components.

3.1.4 Bad Data Injection

The attacks mimic legitimate senders and receivers to acquire unauthorized access to the wireless network. Once access is granted, the victim's resources become overwhelmed through the processing of fictitious messages and measurements placed into the network by the attacker. The work of Kosut [56, 57] divides malicious data attacks into two regimes: strong and weak. The main difference between being the number of meters an adversary has managed to take control of.

The strong attack regime refers to the situation where the attacker has a sufficiently large number of meters to launch an undetected attack. Kosut's work is based on earlier works of Liu, et al. [58], where they implemented mathematical models of the DC and AC power flow out of a power system.

3.1.5 Spoofing

Spoofing a meter means to impersonate its identity on the network. The work of McLaughlin [13] demonstrated proof of this concept by having their fake meter implement the ANSI C12.21 protocol [59] to create a cryptographic nonce (a random number used for authentication) to send to a utility company. The utility will then compute a MAC by hashing together a password and the nonce. The MAC is then sent back to the meter, which calculates its own MAC, thereby, completing the authentication process. The issue with this system is that utility fails to verify the freshness of the meter's nonce, making it easy for impersonators to play themselves off as the real meter [13].

3.1.6 Man in the Middle Attacks

MITM (man in the middle) attacks are executed when the adversary inserts themselves in between communicating devices and examines the traffic between them [12]. They are like an amalgam of eavesdropping, injection and spoofing attacks mentioned earlier. The third party connects to two devices and directs communication between them while viewing the traffic. Sophisticated MITM attacks can mitigate encryption by passing a fake encryption key in place of legitimate ones [12].

3.1.7 Energy Theft Attack

The work of McLaughlin and Byres [13, 60] makes use of the attack tree concept in order to demonstrate a scenario where multiple versions of the abovementioned attacks might be brought together. There are three sections to the attack tree found in Fig. 2, which detail where in the process energy theft may take place: An attacker can interrupt a measurement before it takes place; one may tamper with the stored demand data either before or while the measurements are stored in the meter; the adversary may modify the network even before or while the meter takes its data and logs it.

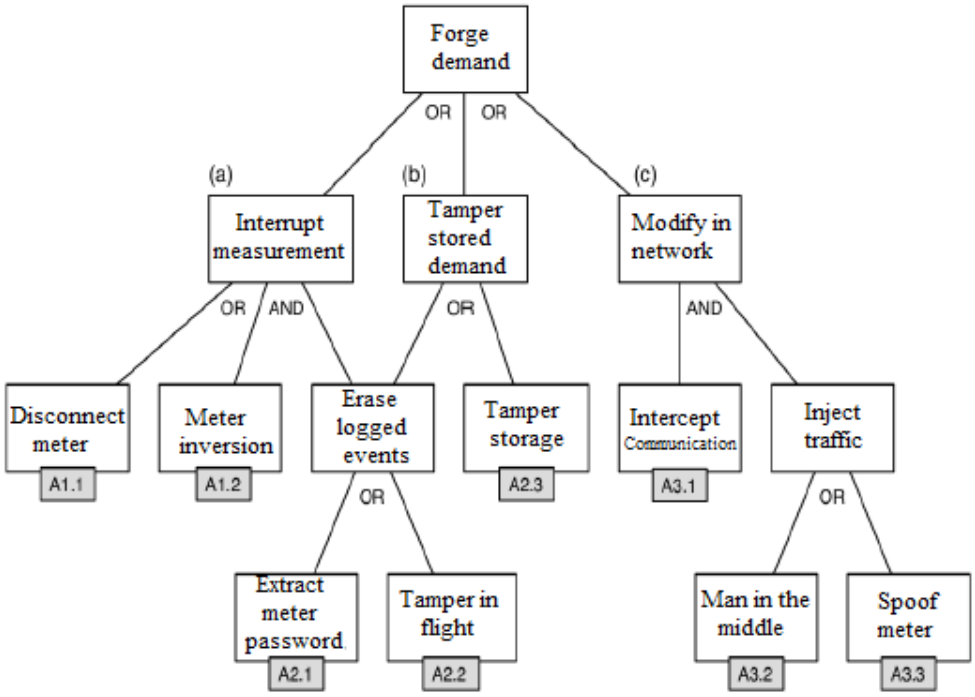


**Fig. 2 Attack scenarios.**

*3.2 Decryption Attacks*

This attack is used to discover the encryption key of a network in order to connect to it and steal its data. An attacker may do this by accessing the physical frames of the network, taking them, and storing enough of them so they can be decrypted using correct algorithms [61]. Another form of attack which yields success is called the side channel attack. This attack exploits some aspect of a physical system which is employing a data encryption algorithm [61, 62]. The following sections will delve into detail on different ways this attack may be expressed.

3.2.1 Electromagnetic Attacks

These attacks deal with discerning the encoded plaintext of a power line message through the leakage of electromagnetic radiation [63, 64]. These attacks use special probes placed at various locations along the unit or circuit in question. Where one places the probe depends on if one is aiming to detect direct or unintentional emissions. Direct emissions are intentional current flows through a line, where short current bursts with sharp rising edges can cause large bandwidths [63]. Unintentional emissions are those electromagnetic leakages which couple to those of other circuit components or cabling. These emissions are typically modulations of the carrier signals that are either present or have been introduced into the device. Under these definitions, direct emissions are the more difficult of the two to detect, requiring close proximity to the device in question. An attacker would likely prefer the unintentional emissions, as these provide a wide spectrum of signals to probe [65] and through which encryption keys in the data may be found [63, 66].

Many proofs of the concept have been demonstrated in the laboratory. The work of Enev and Gupta [67] experimented on the information leakage from eight televisions connected to the same power line. It was found that, the radiative interference patterns of TV power supplies yielded discernable information about the media being played. The work of Hayashi [68-70] has demonstrated the viability of obtaining secret keys from the radiation patterns of power and communication cables attached to FPGA (field programmable gate array) boards. His work has shown

that, cryptographic key information may leak from near field [68] and far field [69] radiation patterns.

3.2.2 Power Analysis Attacks

Power analysis attacks are characterized by analyzing the use of electrical power of a device while it performs an encryption algorithm [62]. They are divided into two classes, simple and differential. SPA (simple power analysis) attacks observe the data visually (oscilloscope, for example), and interpreting what cryptographic algorithm the signal has been encoded with. DPA (differential power analysis) applies statistical error-correcting algorithms to SPA by monitoring trends in the data. DPA attacks are especially dangerous, as they can be so precise that even the switching of a transistor can give away an encryption key. All cryptographic algorithms, and devices running them, have so far been shown to be vulnerable to DPA [62].

3.2.3 Fault Analysis Attack

This class of attack injects faults into a device performing some computation and checks the output signal to obtain patterns associated with encryption within the data. These faults can be anything from unusual environmental conditions (increased heat, for example), the injection of a laser beam at the appropriate frequency [64], or the injection of data packets that collide with legitimate packets [71]. The work of Yuan and Liu [72-74] has shown the load redistribution attack. This is a false data injection attack which modifies selected information in a SCADA power system. This is especially dangerous due to it being able to manipulate estimation of system power flow. Transmission line power flow exceeding transmission line capacity being a possible scenario [73]. Depending on if the attack is short term or long term, it can have damaging effects on the SCED (security-constrained economic dispatch) price estimation [73].

*3.3 Denial of Service Attacks*

This attack seeks to sabotage a power grid network by overwhelming its communication and computational resources in order to prevent it from working [21]. This denies customers of that grid utility their power service. This attack can be applied at multiple layers in the smart grid.

3.3.1 Physical Layer Attacks

One only needs to connect to the communication channel rather than the actual network to launch this attack [2]. Channel jamming attacks become one of the most efficient to use by attackers and one of the most dangerous for utilities and customers alike. Examples of such attacks include the continuous emission and injection of high power wave tones and FM (frequency modulation) modulated noise into the communication channel at a brute force level. A more sophisticated attack is detailed by the work of Proano and Lazos [75], wherein they exploit specific weaknesses in communications protocols (in their case TCP) to perform their attacks. Their selective jamming attacks see the adversary classifying packets in real time, decoding the control field at the MAC layer, and corrupting them before the end of their transmissions.

3.3.2 MAC Layer Attacks

The MAC (media access control) layer is responsible for two-way communication and is susceptible to attackers who wish to modify parameters, which gives the attacker better leeway in accessing the network at the cost of degrading network performance for legitimate customers on the same channel [2]. Examples include spoofing attacks which can target both network availability and integrity. One way this attack may be realized is through sending of fake ARP (address resolution protocol) messages and packets into the local area network. The attacker's MAC address becomes associated with the IP address of a legitimate host, this causes traffic meant for the host to go to the adversary [76].

3.3.3 Network/Transport Layer

TCP/IP protocols are said to be the two more

vulnerable standards in the network infrastructure, due to the use of email as the communication media [2, 12]. Traffic flooding and worm attacks through the internet have led to serious performance issues [2]. Buffer flooding attacks on through the DNP3 protocol have been examined in the literature [77, 78]. The work of East [79] saw the creation of a taxonomy of such attacks, which can range from sending fake DNP3 messages in order to reset, manipulate, or corrupt data from a substation.

3.3.4 Application Layer

Application layer attacks seek to exhaust the resources of a communication channel, focusing on transmission bandwidth in computers and routers [2]. These attacks seek to limit the bandwidths of CPU's and I/O's (input/output's) of connected devices. The work of Ranjan [80] saw the study and categorization of a number of such attacks. A flood attack sends requests at higher than normal frequencies, while asymmetrical attacks send high workload requests. One-shot attacks have the attacker spreading the workload over multiple sessions, using HTTP (hyper text transfer protocol) floods to stress the servers over time.

*3.4 Control and Monitoring Attacks*

Fieldbus is the family of industrial computer network protocols brought together under a standard known as IEC 61158. They include DNP3, Modbus, PROFIBUS (process field bus), CIP (modeling and data management). Each is designed so that they follow the master-slave model of device communication [12]. Many protocols lack authentication and are without encryption procedures, leaving a system using Fieldbus protocols susceptible to a range of attacks [4, 12]: the sending of illegitimate data packets causing protocol failure; protocol commands can force slave devices into inoperable states; protocol commands can force restarts, thus interrupting industrial processes; codes can erase data from diagnostics; other codes can retrieve user or business information; certain commands can broadcast to multiple devices at once, therefore stopping the flow of network traffic (denial of service); querying network devices via a forced configuration and function scans.

3.4.1 Generation Level Attacks

The control processes of generation SCADA, aka G-SCADA, controllers are susceptible to a range of vulnerabilities [4, 12]: Individual controllers can be manipulated, resulting in control codes being overwritten with harmful commands; programmable logic controllers, HMI and SCADA systems can be used to establish an external control channel to steal data; the HMI can be accessed and used to manually override portions of the control process; a man-in-the-middle attack inline on the Ethernet network can alter the flow of I/O traffic between the HMI (reading) and logic controllers (writing) [16].

3.4.2 Transmission Level Attacks

Transmission SCADA, aka T-SCADA, standards are responsible for the monitoring of inputs and outputs through the transmission system. Examples of inputs might include phasor measurements, line voltages, frequencies, transformer settings and load values. Examples of outputs might include capacitance, load adjustments and breaker controls [12]. These I/O values can be redefined upon an attacker compromising T-SCADA server, examples of which are the following [12]: the centralized SCADA console can receive misrepresented values; malicious data can be written to the main controller; the manipulation of secure channels leading to substation gateways use SSL (secure socket layer) and TLS (transport layer security) certificate-based protocols. Implanting an unauthorized device with the appropriate certificate can lead to the compromise of the wide area network.

3.4.3 Distribution Level Attacks

Compromising distribution SCADA, or D-SCADA, systems can lead to the access of power output management systems, AMI headend and generation

systems. At the device level, the compromising of field controllers and others can lead to an array of consequences, ranging from merely operational inefficiencies to outages that come from the reporting of false data [12]. An example would be an auto recloser, a type of RTU (remote terminal unit) which acts as a breaker to protect against power surges and leads to a recovery mode state once conditions return to normal. The right manipulation could lead to the recloser tripping at the inappropriate moment, which has a cascading effect throughout the distribution system. An attacker acquiring complete control over an RTU is in a position to insert malicious logic or code into the RTU controller. Malware within the RTU can cause random faults in the system, while at the same time, reporting nominal working conditions to the utility center. This disrupts power distribution in the targeted area, which resembles denial of service attacks stated earlier.

3.4.4 Time Delay Switch Attack

The work of Sargolzaei, et al. [81-83] has demonstrated what is called the TDS (time delay switch) attack. It introduces a range of time delays into the data stream during the various state measuring points of a power plant, where it was shown to be very effective when applied at the interplay between power station levels. Their work focused on the attack's ability to intrude communication channels for the sensing loop and automatic generation control signals of a power system. These signals exist between the IT layer and the control area of the power plant. It was demonstrated that TDS attacks can be used to sabotage an entire power system by forcing it into a state of destabilization.

## 4. Countermeasures and Solutions

*4.1 Infrastructure Countermeasures*

4.1.1 Injection/Spoofing Countermeasures

At the cyber defense level, BDI (bad data injection) puts prime importance on the transmission and authentic receiving of legitimate data. The most recent works in the literature have focused on strict authentication and key management [84]. Strict authentication techniques in the literature deal with using TLS and SSL protocols are used in conjunction with the SHA (secure hash algorithm) and HMAC (hash message authentication code) is also used to verify communication channel traffic [84]. Dynamic key management has been implemented in the literature as a means of throwing attackers off by constantly refreshing secret keys in the data stream [85].

4.1.2 Theft Detectors

The work by Mashima and Cardenas [19] correlates energy theft with the creation of a set of time series representing the customer's electricity consumption in watt-hours. The goal of the attackers is to use the time series to force the utility to lower the energy bill. A theft detector can be constructed by taking the average of the series over a number of measurements and check whether this is less than some threshold value. This threshold value being the minimum of daily averages taken over a pre-set number of days in the past [19].

4.1.3 Secure Key Management

It is crucial to design secure and scalable management schemes based upon the generation, distribution, and updating of shared cryptographic keys [20]. PKI (public key infrastructure) has been touted as a viable solution when implemented as a key management device. PKI being a standard for binding public cryptographic keys with user identities by means of central certificate authority [86]. An alternative that is useful for the distribution of public keys would be the dated but applicable technique created by Diffie and Hellman [20].

4.1.4 Privacy Preserving Metering

The information network in the smart grid will frequently transport confidential user information such as customer identity, location, associated electronic devices, power usage, etc. In order to protect this data from these above listed attacks, the following scheme has been proposed [87]: The meter will transmit

legitimate measurement data to the user through a secure channel; the user will calculate the final bill by combining the meter data with a certified tariff policy; the bill is then transmitted to the provider alongside a zero knowledge proof, which will validate the computation. It is the act of limiting the data exchange to purely billing information that the user's privacy is maintained [1].

4.1.5 Distributed Data Aggregation

Incremental data aggregation approaches have been proposed in the literature [88, 89]. The aggregator acts as the root of an aggregation network tree which connects all nearest neighbor smart meters. All meters would forward their collected data towards this centralized tree, where all data along the path would be encrypted via homomorphic encryption. Homomorphic encryption allows for computations to be enacted on the plaintext of an encrypted message through the ciphertext. This encryption process happens at each node of the tree before being forwarded to the next level, where the highest level is connected to the service provider. In this scheme, individual meters only see portions of the data, preserving user identity [1].

4.1.6 Memory Attestation

Attestation refers to validating the integrity of a device for computing. A number of attestation schemes have been proposed in the literature to deal with MITM or DOS (denial of service) attacks. The work of Song [90] saw the creation of a protocol which checks for the modification of memory in the channel and generates a checksum rule when this occurs. This checksum is only sent in one direction, thus negating the attacker's ability to take advantage of the grid's two-way communication scheme. The work of He [91] proposed a DRMA (delay resilient remote memory) technique, which can detect compromised devices based on their response time when compared to the delivery time of a healthy grid. Based on data coming from the real-time delay, compromised devices can be sorted out from healthy ones.

4.1.7 Anonymization

Anonymization has been proposed as a solution to the problem of meters being subjected to MITM, spoofing and other attacks [1]. Data are broken down into high and low frequency components, which encompass consumption and billing data, respectively. The work of Efthymiou and Kalogridis [92] keeping suggest doing the connection between high and low frequency data known only to a third party. The data can then be sampled at the appropriate frequency without compromising load balancing mechanisms.

4.1.8 State Estimation

The work of Giani [93, 94] shows a countermeasure against unobservable attacks based on state estimation and the use of PMU's (phase measurement units). Her team examined the compromising of a 19 bus portion of an IEEE 300 bus test case. Each attack is associated with what is called an island, modeled as a perturbation in the power flow [94]. The voltage phase angles evolve in time in unison in each island, and should ideally have only one way (state) in which they travel. If the number of travelling states becomes large, one would observe deviation in the power flow which is associated with a compromised device [93, 94].

*4.2 Decryption Countermeasures*

4.2.1 Electromagnetic and Power Analysis Countermeasures

The most generally implemented countermeasure against EM (electromagnetic) and DPA attacks is to decrease the relationship between the data and the power consumption of the device. Multiple options exist for this purpose of making attacks computationally expensive for the attacker. Reducing the signal to noise ratio via the addition of Gaussian noise into the data will hide interesting signals in the power trace [95]. DPA attacks usually assume the signal is sampled periodically, so an effective further countermeasure would be to randomize and shuffle data points in time [95]. It is possible to make the

vulnerable part of a signal disappear in the power trace by randomly applying cryptographic masks to it [95].

4.2.2 Fault Analysis Countermeasures

The literature describes general countermeasure against fault analysis attacks: sensor-based and error detection based [96]. Sensor-based techniques focus on finding environmental faults caused by such attacks. Error-detection based strategies involve the introduction of redundancies at the hardware, software and information levels in order to detect fault injection [96]. Temporal redundancy involves repeating the same process or following it up with the inverse process to check for faults. Information redundancy checks for separation between the output of codes predicting a certain output and the actual output of said code. These tests have been applied to AES (advanced encryption standard) hardware, which is slated to have future applications in the smart grid.

*4.3 SCADA Countermeasures*

4.3.1 Live Forensics

The work of Ahmed [97] demonstrated a need for forensically examining SCADA systems without turning them off. Ahmed put forward a technique called live forensics in order to detect and thus partially mitigate threats in real time. The work of Taveras capitalized on the work of Ahmed, where live data acquisition was used to take in both volatile and non-volatile information from various levels of the SCADA system [98]. This is done by setting up a watch dog by means of finite state estimation, constantly monitoring events. If the system were to go into a particular strange state that violates a predefined rule, the watchdog will switch to forensics mode in order to collect the data. Wu [99] implemented these techniques on a programmable logic controller, where they targeted the change of the memory addresses in the controller. Further research is needed to make these techniques viable for the large amounts of data found in actual SCADA systems.

4.3.2 Industrial Protocol Filters

The traffic associated with protocols like Modbus, DNP3, IEC 61850 and others can be filtered depending upon the needs of the SCADA distribution. The work of Kang [100] demonstrated a number of techniques for preventing infected traffic from attacking SCADA protocols. Dubbed the IndusCAP-Gate system, it automatically generates whitelists by analyzing traffic and performing multiple filtering based up said lists for blocking suspected traffic [100]. Multiple filters are a series of four filters for analyzing data packets, checking policy adherence in the packets and access control.

4.3.3 Intrusion Detection and Prevention Systems

DPI (deep packet inspection) can be performed on a network, with the traffic being checked against a set of vulnerability signatures [12]. A number of open source tools exist for this purpose. The de facto standard is snort, maintained by Sourcefire. It reads network packets, logs them and analyzes network traffic. Once traffic is received, snort will decode packets and turn them into data structures and identifies the protocols therein. It can then decode IP, TCP or UDP dependencies, raising an alarm if malformed headers or similar issues are detected [101]. Yasakethu and Jiang proposed an IDS (intrusion detection system) method based on machine learning so as to sequentially acquire knowledge about incoming data and make predictions about future events based on previous data [102]. The proposed machine-machine interface would involve rule based algorithms in order to identify causality between events and vector machines to classify said events [103]. ANN (artificial neural networks) and Hidden Markov Models would then be used for nonlinear data analysis when coping with data that is temporally dependent [102].

## 5. Conclusions

This paper was used to identify interesting projects and possible avenues of further research with which to take part in the smart grid security industry. Multiple issues of importance to smart grid cyber security were

studied and discussed. These include the smart metering infrastructure, power line communication, distributed energy resources and network systems. The available literature shows a spectrum of possible routes through which the smart grid may be made vulnerable to attack. An observed trend was that many of the attacks were almost identical in their function, but they are simply applied to the grid in different ways. The literature bears out a number of theoretical, computational and experimental algorithms to increase the safety of the smart grid.

## References


[1] Bari, A. 2014. "Challenges in the Smart Grid Applications: An Overview." *International Journal of Distributed Server Networks* 2014 (1): 1-11.

[2] Wange, W. 2011. "A Survey on the Communication Architectures in Smart Grid." *Computer Networks* 55 (15): 3604-29.

[3] Ye, Y., and Qian, Y. 2012. "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges." *IEEE Communications Surveys and Tutorials* 15 (1): 5-20.

[4] Knapp, E. D. 2011. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems.* New York: Elsevier Inc.

[5] Horowitz, S., and Phadke, A. 2008. *Power System Relaying.* New York: John Wiley & Sons, Ltd.

[6] Depuru, S. 2011. "Smart Meters for Power Grid: Challenges, Issues, Advantages and Status." *Renewable and Sustainable Energy Reviews* 15 (6): 2736-42.

[7] Richter, A. 2012. "Transitioning from the Traditional to the Smart Grid: Lessons Learned from Closed Loop Supply Chains." In *Proceedings of the 2012 International Conference on Smart Grid* Technology*, Economics and Policies,* 1-7.

[8] Pepermans, G. 2005. "Distributed Generation: Definition, Benefits and Issues." *Energy Policy* 33 (6): 787-98.

[9] Taylor, G. A. 2006. "Distributed Monitoring and Control of Future Power Systems via Grid Computing." In *Proceedings of the IEEE Power Engineering Society General Meeting,* 1-5.

[10] Galloway, B., and Hancke, G. 2012. "Introduction to Industrial Control Networks." *IEEE Communications Surveys and Tutorials* 15 (2): 860-80.

[11] Ericsson, G. 2010. "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure." *IEEE Transactions on Power Delivery* 25 (3): 1501-7.

[12] Knapp, E. D., and Samani, R. 2013. *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure.* New York: Elsevier Inc.

[13] McLaughlin, S. 2009. "Energy Theft in the Advanced Metering Infrastructure." *IEEE Journal on Selected Issues in Communications* 6027 (15): 176-87.

[14] Molazem, F. 2012. "Security and Privacy of Smart Meters: A Survey." In *Overview of Computer Security,* British Columbia: University of British Columbia.

[15] Cleveland, F. 2008. "Cyber Security Issues for Advanced Metering Infrastructure." In *Proceedings of the Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century,* 1-5.

[16] Langner, R. 2013. "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve." The Langner Group.

[17] Mohsenian-Rad, A. H. 2011. "Distributed Internet Based Load Altering Attacks against Smart Power Grids." *IEEE Transactions on Smart Grid* 2 (4): 667-74.

[18] Berthier, R. 2010. "Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions." In *Proceedings of the First IEEE International Conference on Smart Grid Communications (SmartGrid-Comm),* 350-5.

[19] Mashima, D., and Cardenas, A. 2012. "Evaluating Electricity Theft Detectors in Smart Grid Networks." In *Research in Attacks, Intrusions and Defenses,* Berlin: Springer-Verlag Berlin Heidelberg.

[20] Panel, S. G. I. 2010. "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security." The Smart Grid Interoperability Panel Cyber Security Working Group.

[21] Li, X. 2012. "Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges." *IEEE Transactions on the Smart Grid* 50 (8): 38-45.

[22] Tubert-Broham, I. 1999. *An Introduction to Cryptography.* Santa Clara, CA: Network Associates, Inc.

[23] U. S. G. A. (United States Government Accountability) Office. 2012. "Challenges in Securing the Electricity Grid." GAO-12-926T, Testimony before the Committee on Energy and Natural Resource, U.S. Senate.

[24] Skopik, F. 2012. "A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures." *International Journal of Smart Grid and Clean Energy* 1 (1): 22-8.

[25] Mohammadi, N. 2012. "A Framework for Intrusion Detection System in Advanced Metering Infrastructure." *Security Communication Networks* 7 (1): 195-205.

[26] Grochocki, D. 2012. "Ami Threats, Intrusion Detection Requirements and Deployment Recommendations." In

*Proceedings of the 3rd IEEE International Conference on Smart Grid Communications,* 395-400.

[27] Fezzani, K. 2006. "Analysis and Optimization of Power Line Coupling Circuits for CENELEC-PLC Modem." In *Proceedings of the IEEE International Conference on Electronics, Circuits, and Systems,* 676-9.

[28] Khan, F. 2012. "An Overview of OFDM Based Narrowband and Communication Standards for Smart Grid Applications." *World Applied Sciences Journal* 20 (9): 1236-42.

[29] Galli, S., Scaglione, A., and Wang, Z. 2011. "For the Grid and through the Grid: The Role of Power Line Communication in the Smart Grid." CoRR (Computing Research Repository).

[30] Langfeld, P., and Dostert, K. 2001. *OFDM System Synchronization for Powerline Communication.* Karlsruhe: Institute of Industrial Information Systems.

[31] Zuberi, K. H. 2003. *PLC (Powerline Carrier) Communication Systems.* Stockholm: Royal Institute of Technolog.

[32] E. E. R. E. (Energy Efficiency and Renewable Energy) U.S. Department of Energy. 2008. *Annual Report on U.S. Wind Power Installation, Cost, and Performance Trends 2007.* Report summary.

[33] Frederich, G., and Dove, P. 2010. "Integrating Distributed Energy Resources into the Smart Grid." Advantech Corportation Industrial Group.

[34] Tenti, P., and Mattavelli, P. 2010. "Improving Power Quality and Distribution Efficiency in Micro-grids by Cooperative Control of Switching Power Interfaces." In *Proceedings of the International Power Electronics Conference,* 472-9.

[35] Castabeber, A. 2010. "Surround Control of Distributed Resources in Micro-grids." In *Proceedings of the 2010 IEEE International Conference on Sustainable Energy Technologies,* 1-6.

[36] Sobe, A., and Elmenreich, W. 2013. "Smart Microgrids: Overview and Outlook." CoRR (Computing Research Repository).

[37] Ferdinando, L. 2013. "Fort Bliss Unveils Army's First Microgrid." United States Army. Accessed May 16, 2013. http://www.army.mil/article/103577/Fort Bliss Unveils Army s First Microgrid/.

[38] Buxbaum, P. 2014. "Microgrid and Power." KMI Media Group. Accessed February 12, 2014. http://www.kmimediagroup.com/military-logistics-forum/432-articles-mlf/microgrids-and-power/5463-microgrids-and-power.

[39] Barnes, N. 2011. "Smart Microgrids on Colleges and University Campuses." AASHE (Association for the Advancement of Sustainability in Higher Education). Accessed May 18, 2011. http://www.aashe.org/blog/smart-microgrids-collee-university-campuses.

[40] Liang H., and Zhuang, W. 2014. "Stochastic Modeling and Optimization in a Microgrid: A Survey." *Energies* 7 (4): 2027-50.

[41] Dolezilek, D., and Schweitzer, S. 2009. *Practical Applications of Smart Grid.* Pullman, WA: Schweitzer Engineering Laboratories, Inc.

[42] Ingram, D. 2012. "Evaluation of Precision Time Synchronization Methods for Substation Application." In *Proceedings of the International IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication,* 1-6.

[43] Sciences, C. 2014. "Overview of IRIG-B Time Code Standard." Precise Time and Frequency, Inc. Accessed January 15, 2014. http://www.cyber-sciences.com/documents/TN-102IRIG-B.pdf.

[44] Dickerson, B. 2014. "Precision Timing in the Power Industry: How and Why We Use It." Arbiter Systems, Inc. Accessed January 15, 2014. http://www.arbiter.com/news/technology.php?id=4.

[45] Zafirovic-Vukotic, M. 2008. "Securing SCADA Communications Following NERC CIP Requirements." RuggedCom Inc.

[46] N. A. E. R. C. (North American Electric Reliability Corporation) and C. I. P. (critical infrastructure protection) Committee. 2006. "NERC Standard CIP-002 through CIP-009." Cyber Security.

[47] SecureState. 2006. "Termineter: Smart Meter Testing Framework." SecureState. Accessed June 16, 2013. https://code.google.com/p/termineter/.

[48] ANSI (American National Standards Institute). "Protocol Specifications for ANSI Type 2 Optical Port." ANSI.

[49] ANSI. 2009. "American National Standard for Utility Industry End Device Data Tables." ANSI.

[50] Aloul, F. 2012. "Smart Grid Security: Threats, Vulnerabilities and Solutions." *International Journal of Smart Grid and Clean Energy* 1 (1): 1-6.

[51] Valli, C. 2012. "Eavesdropping on the Smart Grid." In *Proceedings of the Australian Digital Forensics Conference,* 54-60.

[52] Parikh, P. 2010. "Opportunities and Challenges of Wireless Communication Technologies for Smart Grid Applications." In *Proceedings of the IEEE Power and Energy Society General Meeting,* 1-7.

[53] Baig, Z., and Amoudi, A. R. 2013. "An Analysis of Smart Grid Attacks and Coutermeasures." *Journal of Communications* 8 (8): 473-9.

[54] Lazos, L., and Krunz, M. 2011. "Slective Jamming/Dropping Insider Attacks in Wireless Mesh Networks." *IEEE Network* 25 (1): 30-4.

[55] Xu, Y. 2013. "Wireless Mesh Network in Smart Grid:

Modeling and Analysis for Time Critical Communications." *IEEE Transactions on Wireless Communications* 12 (7): 3360-71.

[56] Kosut, O. 2010. "Malicious Data Attacks on the Smart Grid." *IEEE SmartGridComm* 2 (4): 645-58.

[57] Kosut, O. 2010. "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures." In *Proceedings of the 2010 First IEEE International Conference on SmartGridComm (Smart Grid Communications),* 220-5.

[58] Liu, Y., Ning, P., and Reiter, M. 2009. "False Data Injection Attacks Against State Estimation in Electric Power Grids." In *Proceedings of the ACM (Association for Computing Machinery) Conference on Computer and Communications Security,* 21-32.

[59] ANSI. 1999. "Protocol Specification for Telephone Modem Communication." Accredited Standard Committee on Electricity Metering.

[60] Byres, E. 2004. "The Use of Attack Trees in Assessing Vulnerabilities in Scada Systems." In *International Infrastructure Survivability Workshop,* Lisbon: Institute of Electrical and Electronics Engineers.

[61] Carcelle, X. 2006. *Power Line Communications in Practice.* Boston: Artech House.

[62] Standaert, F. X. 2010. *Introduction to Side-Channel Attacks.* Paris: Springer.

[63] Agrawal, D. 2003. *The EM Side-Channel(s): Attacks and Assessment Methodologies.* London: Springer.

[64] Di-Battista, J. 2010. "When Failure Analysis Meets Side-Channel Attacks." In *Springer Cryptographic Hardware and Embedded Systems: Lecture Notes in Computer Science,* Berlin: Springer Berlin Heidelberg.

[65] Debeer, F. 2011. "Practical Electro-Magnetic Analysis." In *Non-invasive Attack Testing Workshop NIAT,* Nara: Todai-ji Cultural Center (Technical Programs).

[66] Meynard, O. 2012. "Characterization of the Information Leakage of Cryptographic Devices by Using EM Analysis." In *Springer Information Security and Cryptology: Lecture Notes in Computer Science,* Berlin: Springer Berlin Heidelberg.

[67] Enev, M., and Gupta, S. 2011. "Televisions, Video Privacy, and Powerline Electromagnetic Interference." In *Proceedings of the 18th ACM Conference on Computer and Communications Security,* 537-50.

[68] Hayashi, Y. 2009. "An Analysis of Information Leakage from a Cryptographic Hardware via Common-Mode Current." In *Proceedings of the 2009 International Symposium on Electromagnetic Compatibility,* 17-20.

[69] Hayashi, Y. 2010. "Information Leakage from Cryptographic Hardware via Common-Mode Current." In *Proceedings of the IEEE International Symposium on EMC (Electromagnetic Compatibility),* 109-14.

[70] Hayashi, Y. 2012. "Evaluation of Information Leakage from Cryptographic Hardware via Common-Mode Current." *Institute of Electronics, Information and Communication Engineers Transactions on Electronics,* E95.C (6): 1089-97.

[71] Moradi, A. 2011. "On the Power of Fault-Sensitivity Analysis and Collision Side-Channel Attacks in a Combined Setting." In *Springer Cryptographic Hardware and Embedded Systems,* Berlin: Springer Berlin Heidelberg.

[72] Yuan, Y. 2011. "Modeling Load Redistribution Attacks in Power Systems." *IEEE Transactions on Smart Grid* 2 (2): 382-90.

[73] Yuan, Y. 2012. "Quantitative Analysis of Load Redistribution Attacks in Power Systems." *IEEE Transactions on Parallel and Distributed Systems* 23 (9): 1731-8.

[74] Liu, Y., Ning, P., and Reiter, M. 2011. "False Data Injection Attacks against State Estimation in Electric Power Grids." ACM Transactions on Information and System Security.

[75] Proano, A., and Lazos, L. 2010. "Selective Jamming Attacks in Wireless Networks." In *Proceedings of the IEEE ICC (International Conference on Communications),* 1-6.

[76] Premaratne, U. 2010. "An Intrusion Detection System for IEC 61850 Automated Substations." *IEEE Transactions on Power Delivery* 25 (4): 2376-83.

[77] Jin, D. 2011. "An Event Buffer Flooding Attack in DNP3 Controlled SCADA Systems." In *Proceedings of the 2011 Winter Simulation Conference,* 2614-26.

[78] Lee, D. 2014. "Simulated Attack on DNP3 Protocol in SCADA Systems." In *Proceedings of the 31st Symposium on Cryptography and Information Security,* 1-6.

[79] East, S. 2009. "A Taxonomy of Attacks on the DNP3 Protocol." In *IFIP Advances in Information and Communication Technology,* Berlin: Springer Berlin Heidelberg.

[80] Ranjan, S. 2009. "DDos-Shield: DDos-Resilient Scheduling to Counter Application Layer Attacks." *IEEE/ACM Transactions on Networking* 17 (1): 26-39.

[81] Sargolzaei, A., Kang, K. Y., and Abdelghani, M. N. 2013. "Time-Delay Switch Attack on Load Frequency Control in Smart Grid." *Advances in Communication Technology* 5 (December): 55-64.

[82] Sargolzaei, A., Kang, K. Y., and Abdelghani, M. N. 2014. "Control of Nonlinear Heartbeat Models under Time-Delay-Switched Feedback Using Emotional Learning Control." *Int. J. Recent Trends Engineering Technology* 10 (2): 85-91.

[83] Sargolzaei, A., Kyle, Y., and Abdelghani, M. 2014.

"Delayed Inputs Attack on Load Frequency Control in Smart Grid." In *Proceedings of the 2014 IEEE PES (Power and Energy Society) ISGT (Innovative Smart Grid Technologies Conference),* 1-5.

[84] Wang, D. 2013. "A Survey on Bad Data Injection Attack in Smart Grid." In *Proceedings of the 5th IEEE PES Asia-Pacific Power and Energy Engineering Conference,* 1-6.

[85] Sun, Y. 2012. "A Dynamic Secret-Based Encryption Method in Smart Grid Wireless Communication." In *Proceedings of the IEEE Innovative Smart Grid Technologies-Asia,* 1-5.

[86] Baumeister, T. 2011. "Adapting PKI for the Smart Grid." In *Proceedings of the IEEE International Conference on Smart Grid Communications,* 249-54.

[87] Rial, A., and Danezis, G. 2011. "Privacy-Preserving Smart Metering." In *Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society,* 49-60.

[88] Li, F. 2010. "Secure Information Aggregation for Smart Grids Using Homomorphic Encryption." In *Proceedings of the 1st IEEE Conference on Smart Grid Communications,* 327-32.

[89] Ruj, S. 2011. "A Security Architecture for Data Aggregation and Access Control in Smart Grids." CoRR (Computing Research Repository).

[90] Song, K. 2011. "OMAP: One-Way Memory Attestation Protocol for Smart Meters." In *Proceedings of the Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops,* 111-8.

[91] He, X. 2013. "A Novel Delay-Resilient Remote Memory Attestation for Smart Grid." In *Proceedings of the 8th International Conference on Springer Wireless Algorithms, Systems, and Applications,* 88-99.

[92] Efthymiou, C., and Kalogridis, G. 2010. "Smart Grid Privacy via Anonymization of Smart Metering Data." In *Proceedings of the First IEEE International Conference on Smart Grid Communications,* 238-43.

[93] Giani, A. 2011. "Smart Grid Data Integrity Attacks: Characterizations and Countermeasures." In *Proceedings of the Second International Conference on Smart Grid Communications,* 232-7.

[94] Giani, A. 2013. "Smart Grid Data Integrity Attacks." *IEEE Transactions on Smart Grid* 4 (3): 1244-53.

[95] Güneysu, T., and Moradi, A. 2011. "Generic Side-Channel Countermeasures for Configurable Devices." In *Proceedings of the 13th International Workshop on Spring Cryptographic Hardware and Embedded Systems,* 33-48.

[96] Bousselam, K. 2012. "On Countermeasures against Fault Attacks on the Advanced Encryption Standard." In *Fault Analysis in Cryptography,* Berlin: Springer Berlin Heidelberg.

[97] Ahmed, I. 2012. "SCADA Systems: Challenges for Forensic Investigators." *Computer* 45 (12): 44-51.

[98] Taveras, P. 2013. "SCADA Live Forensics: Real Time Data Acquisition Process to Detect, Prevent or Evaluate Critical Situations." *European Scientific Journal* 9 (21): 253-62.

[99] Wu, T. 2013. "Towards a SCADA Forensic Architecture." In *Proceedings of the 1st International Symposium for ICS (Industrial Control System) and SCADA Cyber Security Research,* 12-21.

[100] Kang, D. 2014. "Whitelists Based Multiple Filtering Techniques in SCADA Sensor Networks." *Journal of Applied Mathematics* 2014 (June): 597697: (1-7).

[101] Pathan, A. S. 2014. *The State of the Art in Intrusion Protection and Detection.* Boca Raton, FL: Auerbach Publications.

[102] Yasakethu, S., and Jiang, J. 2013. "Intrusion Detection via Machine Learning for SCADA System Protection." In *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research,* 101-5.

[103] Mitchell, R., and Chen, I. R. 2013. "Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications." *IEEE Transactions on Smart Grid* 4 (3): 1254-63.