Chapter 1
Security Challenges in Smart Grid Implementation

Sanjay Goel and Yuan Hong

Abstract The smart grid architecture amalgamates the physical power grid and a communication grid into a single monolithic network. It poses several security threats that are well known (Li et al. in IEEE Trans Smart Grid 3:1540–1551, 2012 [1], McDaniel and McLaughlin in IEEE Secur Priv 7:75, 77, 2009 [2], Bisoi and Dash 2011 [3]). However, it faces unknown threats from the cyber-physical interfaces whereby either cyber-threats can lead to actuation of physical devices or vice versa if physical devices could be manipulated to disrupt the communication infrastructure. The most prevalent threats to the operation and safety of the smart grid come from physical destruction of infrastructure, data poisoning, denial of services, malware, and intrusion. The most prevalent threat to the consumer is breach of privacy of the data and malicious control of personal devices and appliances. This chapter articulates the smart grid architecture and the cyber-physical threats to which the smart grid is vulnerable.

1.1 Smart Grid Architecture

1.1.1 Introduction

The smart grid is a traditional power grid with a communication network overlaid on top of the traditional power grid. The communication and power grid are interrelated such that the communication network depends on the power grid for data and the power grid depends on the communication for operational activities. The role of the grid is to provide ubiquitous communication capability for collecting data from sensors and meters, process it in situ, and provide pertinent information to support multiple activities such as ensuring grid stability, detecting and resolving anomalies, forecasting load, and facilitating demand response. All this needs to be done while protecting the privacy of the consumers, protecting critical operational data that from national adversaries, and ensuring the integrity of the data for both business and operational needs. This is not a trivial challenge for several reasons, including need

S. Goel et al., *Smart Grid Security*, SpringerBriefs in Cybersecurity,
DOI 10.1007/978-1-4471-6663-4_1

to integrate disparate communication media into a single monolithic network, need to provide guaranteed latency and bandwidth for several applications, and need to ensure privacy and security of the data as necessary.

The power grid is typically segregated into transmission, distribution, and the last mile. Transmission carries high-voltage current over long distances to substations. Distribution carries lower-voltage data from substations to local transformers. The last mile connects the local transformers to consumers, and it is where utilities and consumers interact to support real-time management of energy generation, distribution, usage, and efficiency. With the integration of the smart grid technologies, the traditional network is now entering households and businesses. Parallel to the power grid, the communication grid can be segregated into wide area network (WAN), metropolitan area network (MAN), field area network (FAN), and home area network (HAN) as shown in Fig. 1.1.

The primary goal associated with the transmission network is to provide situational awareness where technologies for monitoring and control of the grid across a large geographical network are necessary. This will include incorporation of synchrophasors for monitoring the state of the grid to ensure its synchronization as well as supporting SCADA systems. Any failure at this level will have far-reaching consequences on the stability of the entire grid including large-scale blackouts. Consequently, WAN will need to provide high bandwidth (600–1500 kbps), low latency (20–200 ms), and high reliability (over 99.999 %). This kind of reliability will probably not be met by wireless technologies and will rely primarily on fibre optic or other wired technology. At the distribution level, the goal is to be able to monitor the distribution network for faults and other anomalies as well as to be able to integrate microgeneration sources. This will have a variable requirement for bandwidth (10–100 kbps) and latency (from 10 ms to 15 s) with a reliability greater than 99 %.

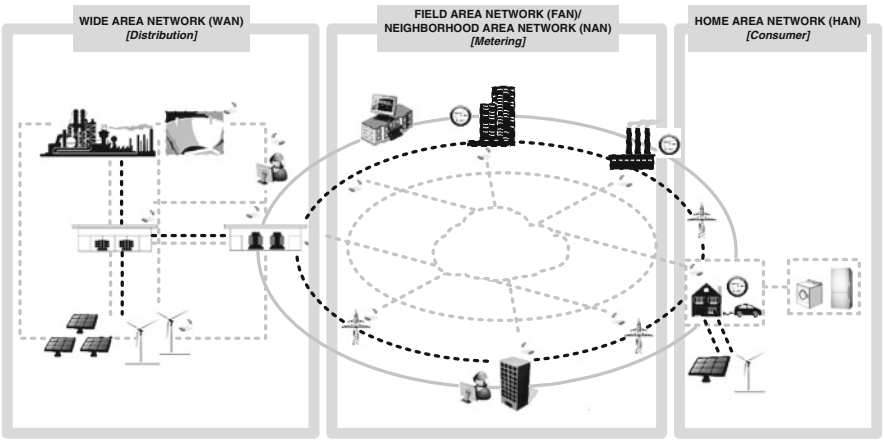

Fig. 1.1 The evolution towards the smart grid

A key requirement would be to handle peak data from multiple sources during power outages. These networks are typically dense and entrenched throughout the city requiring a combination of different technologies including wireless, PLC, and AMI. The last mile would be responsible for metering from the customer as well as providing demand response capability. This would require vendor interoperability to be able to support different types of devices in customer homes. Redundancy, fault tolerance, and security are all critical for this network. HAN would require a short range with the ability to penetrate through walls with very high data rate from multiple appliances. The communication channel should be able to handle a barrage of interference from multiple devices and be able to operate reliably. For aesthetics and convenience, the HAN network will most likely be wireless.

1.1.2 Communication Technologies

Currently, most power system infrastructure uses a combination of multiple technologies including dedicated cable, microwave, power line communication, and fibre optic technology. Replacing all existing infrastructure with dedicated fibre optic communication would be cost prohibitive. The infrastructure consequently would be a combination of wireless, fibre optic, power line carrier (PLC), and traditional cable or Ethernet.

One of the most seductive technologies to implement would be the PLC given that the power infrastructure already connects together the entire grid across all levels of the grid. The technology has been developed since 1920, initially for voice and data communication over high-voltage lines between remote stations and most recently for load control and automatic meter reading. The earlier technology was very narrow band operating below 3 kHz frequency resulting in low data rate of 60 bps which could be transmitted over large distances. The CENELEC standard in 1992 regulates the use of spectrum in four bands: 3–95 kHz for power utilities; 95–125 kHz for general applications, 125–140 kHz for home networks, and 140–148.5 for security applications. An innovation that is propagating at the WAN level is the use of optical fibres encased in the ground wire that runs on top of all the transmission towers to take a preferential lightning hit. Most electrical power grid systems in the world use the ground wire with an optical fibre encased in it. These communication channels operate efficiently over large distances with minimal losses and high reliability. These optical fibres in the newer installation of transmission lines facilitate the deployment of smart grid without any need for additional communication capacity. While such an infrastructure supports the requirements of the smart grid, the TCP/IP protocol that drive communication today would not provide the requisite security required for communication among power plants (including nuclear), control equipment, substations, and eventually distribution grids.

Wireless media will be a critical part of the smart grid communication infrastructure primarily due to convenience and accessibility especially in the area of metering and home area networking. Communication is possible by transmitting

from hop to hop (electrical poles) across large distances. There are several different technologies that can be used including Microwave, WIMAX, MESH, LTE, Cellular, WLAN, and Zigbee. Microwave is a high-capacity point-to-point wireless transport for providing a backbone to telecommunication services including radio access network and WAN. It can be used for applications such as SCADA, AMI, and Demand Response. WiMAX is a cost-effective channel broadband connectivity across large areas as an alternative to GSM and CDMA. It can be used for AMI, SCADA, demand response, mobile workforce, and video surveillance. Mesh network is created by using a network of radio nodes arranged in a mesh topology and is commonly used for providing the last mile of connectivity for broadband access. It can overlay or replace copper DSL or provide a redundant channel of communication. It can be used for remote monitoring, demand response, AMI, and distribution automation. The problem is delay caused due to hops from router to router; however, it is easily expandable by adding additional nodes and permits building redundancy in the network. LTE is the next-generation network for mobile communication that provides high spectral efficiency and low latency. It can be used for all applications in which mesh network are used; however, it is not readily available and cost of installation is high. Cellular networks are typically used for most consumer applications including mobile phones, Internet connectivity, voice and video chat, and text messaging. It can be used in the smart grid for workforce coordination, AMI, etc. The main advantage is that it is already widely deployed requiring minimal capital costs for operationalizing smart grid initiatives. Wireless LAN (WLAN) is already used extensively for indoor connectivity and could be leveraged easily for home area networking and connecting smart meters with internal visualization devices. Zigbee is a standard developed specifically for the smart grid targeted at networking in-home applications including smart meters, smart lighting, and appliances.

1.1.3 Sensors and Devices

While the communication infrastructure is the enabler for the smart grid, the real benefit will come from the sensors and devices on the network. A smart meter will be installed on each node of the network that will facilitate a two-way exchange of power through metering in both directions and allow fine-grained control of electricity usage of customer appliances to the utility company. The meters will also allow remote access to appliances in the households to customers and provide them with detailed usage statistics. In addition, it will provide commercial entity access to devices for monitoring, diagnostics, and repair. The smart grid will also minimize the manual data collection from the grid.

Until recently, utility company employees have manually gathered operational data including electricity metering, identifying broken equipment, and faults. The smart grid infrastructure will allow remote control and automation of several

operational activities including monitoring of the distributed infrastructure comprised of wires, substations, transformers, switches, etc. Each device on the network will contain sensors to gather data (voltage, phase, temperature, etc.). That data will be relayed to the control centre through the two-way communication system of the grid. One of the key needs of the grid is improved stability that will require synchronized phasor (synchrophasor) devices installed throughout the network for data collection. Synchrophasors will provide real-time measures of electrical quantities from the entire power grid for several critical applications including estimation of dynamic state response, grid synchronization, and fault identification. These devices consist of GPS satellite-synchronized clocks, phasor measurement units (PMUs), phasor data concentrator, and analysis software.

Another key element of the smart grid is the self-healing of the grid that can correct flaws automatically or isolate the faults to minimize the outages for consumers. To develop self-healing abilities in the grid, a processer will be required in each switch, and circuit breaker and electromechanical switches will need to be replaced with solid-state electronic circuits. Automated reclosers will be added on to the grid to allow temporary instantaneous faults caused by events such as falling tree limbs and heavy winds to be self-corrected. To manage and analyse the data, distributed analytic processing capability as well as storage in the grid will need to be incorporated. Finally, the grid will need to be secured both through perimeter defence and improved visibility into the network for intrusions and attacks as we will discuss that further.

Summary

Smart grid requires a massive communication infrastructure with complete connectivity across the entire country. Based on geographically dispersed infrastructure elements, communication will need to be a hybrid with a variety of communication media. Initially, communication will be shared by other services at least in the distribution network; however, over time, communication networks are likely to become more dedicated as communication infrastructure is laid out exclusively for the smart grid. The grid infrastructure also requires sensors for monitoring and diagnostics throughout the grid as well as upgrading the existing electromechanical switches to electronic switches for imbuing self-correction ability in the grid. A key imperative to the success of the smart grid would be a robust security mechanism that not only prevents intrusion but also ensures privacy of customers and integrity of the data.

1.2 Smart Grid Security Concerns and Threats

The smart grid is poised to fundamentally change the electrical grid from the centralized utility-centric grid to a distributed consumer-centric grid where the consumers are well informed and active participants in energy consumption and

generation. The smart grid also brings improved visibility into the grid that will help in better monitoring and control of the grid to ensure stability and reduce chances of large-scale blackouts. A ubiquitous communication network that connects all the users, utilities, and producers into a monolithic network enables this functionality. However, all this comes at a cost, which is increased risk of cyber-attacks. There are threats from several actors including terrorists, nation states, criminals, and disgruntled employees. In addition, there is need to protect customer privacy which can be revealed through the fine-grained transmission of usage data. If security is in adequate, the communication network in the grid can become a liability rather than an asset. There have been numerous attacks on the smart grid, and there are several security threats, some of which we discuss in this chapter.

1.2.1 Reported Attacks on Electric Grids

There have been several documented impact on the electric grid attributed to targeted cyber-attacks or as unintended consequences of network anomalies that led to SCADA system failures [4] described ahead. In January 2003, the Slammer worm infected a computer network at the Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system and the plants process computer for several hours. In August 2003, a failure of the alarm processor of FirstEnergy prevented monitoring of the grid and as several transmission lines tripped for various reasons, a cascading failure resulted in disabling power plants through north-east and leading to an extended blackout. In August 2006, circulation pumps at the Brown Ferry nuclear plant in Alabama failed due to excessive traffic on the control system network. Investigation of a 2009 incident revealed that hackers were able to steal power by hacking into smart meters and changing the power consumption reading. Phishing incidents were also detected at an electric bulk provider and malware samples were detected that indicated a targeted and sophisticated intrusion.

Most of the above attacks raised concern, and there has been innuendo regarding the participation of nation states in these attacks. There were also attacks that were in the category of information warfare and propaganda such as the attack on Estonia and Georgia during conflicts with Russia. The first major cyber-warfare attack that attacked the critical infrastructure of a country was the Stuxnet attack that was targeted at degrading the Iranian nuclear enrichment facilities. Stuxnet is a worm that exploits multiple zero-day vulnerabilities that make use of stolen digital certificates to control WinCC SCADA application on Siemens S7 PLC Microcontroller [5]. The payload for Stuxnet was delivered using infected USB drives of nuclear inspectors. The malware was not only able to increase the RPM of the centrifuges used for enriching uranium, but it also made it appear that the centrifuges were operating normally. This was the first major strategic attack on critical infrastructure of another country and had propelled countries into an arms race to develop such weapons as strategic options both for deterrence and counter-attacks.

There have been several data for reconnaissance and probing the critical infrastructure [5]. Night Dragon was an intrusion ostensibly originating in China [6] and aimed at probing industrial control systems of energy companies (oil, gas, and petrochemical) in the United States. The attacks used a combination of social engineering and vulnerabilities in remote administration tools on Windows platforms to break into critical computers on the network to gather proprietary information including documents related to oil and gas field exploration and business negotiations as well as details of SCADA systems. Researchers in Budapest discovered another computer malware named Duqu which is a collection of tools and services including keystroke loggers, kernel drivers, and injection tools. It was found on computers in companies manufacturing industrial control systems. There is speculation that the malware was used by Stuxnet writers to collect information that went into development of the Stuxnet. An even more sophisticated malware targeted at control systems was the Flame toolkit which includes a backdoor, Trojan, as well as replicator and propagation mechanism that allows it to propagate on the network and removable media. Flame is an intelligence-gathering malware that can sniff traffic, take screenshots, record audio conversations, capture keystrokes, and transmit files through a command and control server.

Attacks on the smart grid can occur at multiple levels including, transmission, distribution, and home networks. The attacks can include protocol-based attacks, routing attacks, intrusions, malware, and denial-of-service attacks. The attack vectors are varied including social engineering, random network scans, insider malicious activities, and physical destruction of the communication infrastructure.

1.2.2 Security Concerns

Smart grids consist of a network of sensors, monitors, devices, as well as computers for data collection and analysis. All of these are susceptible to cyber-attacks. Analysts have identified five major challenges faced by computerized security systems related to smart grids [7] including high volume of sensitive customer information, distributed control devices, lack of physical protection, weak industry standards, and a large number of stakeholders dependent on the grid. The concerns of smart grid security as with other typical systems are confidentiality, integrity, and availability. Confidentiality entails protecting both consumer and operations data; integrity is also required both at the consumer level for metering and billing and at the operational level to ensure stability of the grid; availability means that the power continues to be transmitted and received by customers, regardless of the status of the system.

Smart grid faces the same security challenges as any complex computer network and needs both perimeter defence and visibility into the network. The fundamental issue is that given massive size and interconnectivity in the entire network, worms and viruses can spread quickly. Also, given the distributed nature of the network,

there are an enormous number of vulnerable targets. Additionally, SCADA systems are designed with inadequate security; for instance, Siemens still uses a hard-coded password for allowing access to control systems [8], which once compromised can lead to massive security breaches. Administrative passwords are often precoded and never changed from the original settings. There are several entry points into the networks, including infiltration through infected devices, network-based intrusion, compromised supply chain, and malicious insider.

There are several threats that the smart grid faces apart from dedicated attacks and intrusion by third parties [9–14], including privacy breach through data theft, electricity theft, disruption of services, physical damage to devices, denial of service, and market fraud. Hacking into smart meters, tapping wireless communication, or stealing the data from servers of the utility can provide fine-grained metering information of the users' consumption [9]. This information is necessary for the utility for billing, demand response, and load forecasting. The same information, however, can reveal the lifestyle of an individual. Each appliance has a unique electricity usage signature which can be extracted from the overall usage pattern indicating what the user is engaged in, i.e. working on a computer, watching television, taking shower, and cooking. Employers, marketers, insurance companies, as well as criminals can exploit this information for different purposes. Marketing companies could use this information for targeted marketing or introducing non-competitive pricing. Criminals can use this information to determine the daily routine or a family, i.e. when there is no one in the house or when someone is alone in the house for committing burglary or other crimes. Electricity theft can occur by altering the meter reading either by tampering with the meter or changing the information after breaking the encryption key [9].

1.2.3 Impact of Threats on Smart Grid

A small disruption (about 5 %) in communication can cause major latency issues leading to significant operational performance degradation [15]. Several metrics have been defined for communications in the smart grid including packet delivery ratio (# delivered/# expected), average end-to-end delay, and average packet hop (# of intermediate nodes), successful DR request ratio (# D-R requests delivered/# D-R requests issued) [15]. Limiting values of these metrics need to be defined and then guaranteed to ensure seamless performance of the grid. A key concern beyond communication latency issues is that data collected from sensors could be corrupted. There are mechanisms in place that can detect corruption of data based on other sensor values. An attacker can, however, manipulate data from enough sensors as to make data corruption unobservable [16]. Such attacks are not random but rather coordinated and not likely to be in sequence to avoid detection. For such attacks to succeed, the hacker would need knowledge of measurement detection and analysis techniques used at the control centre.

Smart grid relies extensively on wide area monitoring systems (WAMs), and the values from distributed sensors in the network are spatially analysed based on the GPS locations of the sensors [17]. GPS could be spoofed in measurement devices leading to wrong control decisions based on spoofed data, the outcome of which can be mild to severe based on the breadth of the attack. GPS can be spoofed by causing interference such that GPS receiver loses signal and then creating a false signal with a higher correlation peak that provides false information. False data can prevent fault signal from reaching the controller or provide a false location of the fault resulting in delay in power line repair and restoration. Voltage spikes can be camouflaged, and false voltage spikes can be generated leading to wrong corrective action by the controller causing instability in the grid. Coordinates of the disturbance can be falsified preventing triangulation and delaying the identification of fault location. Since message timing is crucial in smart grids, an attacker can use legitimate means to delay messages and cause denial of service or trigger faults. Attacker can flood the data stream with false data and severely degrade performance [18].

Summary

Ubiquitous communication is a necessary element of the smart grid, but it also provides hacker access to the grid components through the same network. There are security threats to the physical communication infrastructure as well as to the logical operation of the network based on conventional threats such as intrusion, denial of service, malware, and social engineering. Additionally, there are threats due to inadvertent errors, equipment failures, and natural disasters. There are several actors that pose a threat, including disgruntled employees, competitors, terrorists, nation states, and criminals. The entire smart grid is data driven where data is used for critical operations including, resource management, load forecasting, error correction, and fault isolation. Confidentiality, integrity, and availability are all very important in smart grid data security. There are numerous data-poisoning attacks that can destabilize the grid through unwarranted corrective actions or lack of necessary corrective actions, both of which can result in cascading failures. Lack of availability will result in a loss of visibility into the network that again is dangerous for the grid. In short, ensuring the security of the grid is critical to the success of the grid.

1.3 Ensuring Security in Smart Grids

The power grid is a very complex system that is geographically and logically distributed. The smart grid provides the communication infrastructure to connect the dispersed components and manage the grid by extensive data collection and analysis to get real-time operational intelligence. Such operational intelligence provides several benefits to the grid including improved load forecasts, peak load reduction through demand response, better utilization of renewable microenergy

sources, and automated fault detection and isolation as well as correction in some cases. On the flip side, the communication infrastructure that permeates throughout the grid provides attackers access to the entire power grid. Consequently, it is imperative to have strong security in the smart grid.

The smart grid connects users, power plants, utilities, substations, and oversight bodies into the network with components, including protection relays and circuit breakers, SCADA systems, and household appliances. The smart power grid is distributed into three distinct segments, i.e. transmission, distribution, and HANs. In the traditional grid, the primary use of communication infrastructure in the distribution network was for monitoring substations. However, the communication network extends all the way to households and individual appliances with the smart grid. This also means that there is a much larger network to secure. Traditionally, the bulk distribution system has been the primary focus of cyber-security where the impact is the greatest. Failure on the distribution network has the possibility of triggering large-scale cascading failures. However, with the smart grid, attacks at the smart meter level can also have a large impact as attacks can spread through the network quickly leading to large catastrophic failures. There are several points of vulnerabilities in the grid [19] including the architecture, interoperability, communication protocols, interfaces, HANs, customer portals, and hardware.

A part of the problem today is the massive volumes of data being collected and analysed in distributed locations in the grid providing many targets for hackers for data manipulation attacks. A large part of the data volume comes from synchrophasors that provide the state information from the grid including voltages and currents required for ensuring grid stability. The data and software components of the infrastructure form a large chunk of the vulnerabilities that need to be addressed. Some of the conventional vulnerabilities come from validation checks in software including cross-site scripting, command injection, and buffer overflow [20]. Other vulnerabilities include poor management of access control, privileges, and permissions; lack of proper authentication; management of access credentials; and missing integrity checks. Other problems include poor configuration of systems, delayed patch management, lack of security audits, insufficient monitoring of logs, improper configuration of hardware and network devices, and finally lack of training of administrators in security practices.

There are a lot of legacy devices that were manufactured decades ago and do not have built-in cyber-security. During the transition period, when the devices are being gradually replaced, however, they form a large vulnerability. The past security paradigm in grid infrastructure was “security through obscurity”, i.e. if the existence of a vulnerability is unknown, it will stay protected. We all know this is not true in the case of the Internet where networks are constantly being scanned for points of vulnerabilities. Also, as the software on SCADA systems get increasingly standardized, there is a chance of large-scale attacks through the network that can lead to large-scale failures and disruptions. Migration plan, thorough testing, and agile monitoring of the grid is necessary for ensuring that the legacy systems do not become a cyber-security liability for the smart grid.

1.3.1 Standards and Architectures

Standards are still evolving for smart grid appliances; consequently, security controls are being created differently for different devices preventing standardization in testing and evaluation. Several groups are actively working on creating standards, including Smart Grid Interoperability Panel (SGiP), Cyber Security Working Group (previously NIST Cyber Security Coordination task group—CSCTG), and GridWise Architectural Council (GWAC). There are several requirements for security for smart grid that can be grouped into data security (access control, data authentication, storage, backup and recovery, and cryptographic protocols), security management (risk analysis, security policies, and training), and infrastructure security (system and device configuration, perimeter security, and personal key exchange) [21]. In addition, processes need to be developed to gain visibility into the network for extensive data logging and analysis. There is security need to be implemented through the communication infrastructure and systems, including SCADA (DNP3, GOOSE, IEC 61850, IEC 60870-5), WANs, land mobile radio (LMR), WLAN, and WiMax.

Most of the communication on the smart grid network would be encrypted with a need to use a public key infrastructure [22] in the grid. In addition, the communications infrastructure needs to be imbued with security incorporating, appropriate network topology design, secure routing protocols, secure message forwarding, end-to-end encryption, security broadcasting, and defence against denial of service (e.g. excess capacity, quick detection, and countermeasures). There also needs to be data packet authentication and bad data detection.

Numerous architectures have been provided for the smart grid communication networks. Reference [23] provides a 3-tiered architecture for the network including, HANs, neighbourhood area networks (NANs), and WANs and suggest use of a mesh area network that provides multiple redundant paths. Their architecture is primarily focused on preventing denial-of-service attacks and signal interruption. This architecture is agnostic to false-data injection attacks. Reference [19] suggests a layered approach to security for the smart grid that goes from technical execution at the lowest level to strategic direction at the top level, i.e. physical, network, host, data, application, business process, and enterprise organization.

1.3.2 Sensors and Devices

Individual smart meters need to be protected from tampering, data leakage, and intrusion. The hacker can gain access at the customer endpoint, crack wireless communications between the AMI meter and endpoint equipment, or crack wireless communications from the AMI meter to the local concentrator. Intrusion can allow access to the communication network of the utility through the endpoint. There have been several suggestions for their protection. One is to restrict transmission to only

changes in power consumption; however, hackers can reconstruct the energy usage profiles from the power usage changes that are transmitted. There have been suggestions to include artificial spoofed packets into the data stream such that the energy usage looks normal rather than when an owner is not present. Spoofed packets can be randomly generated using Poisson distribution of power consumption or history templates [1]. At the transmission level, intrusion and buffer overflow type of attacks need to be detected. Most communication networks leave open a connection awaiting response to a SYN/ACK signal, sometimes as long as 75 s. An attacker can flood buffer with spoofed SYN requests creating congestion on the network. Bayesian statistical analysis can be used on the packet information to detect attack [24]. A fusion centre that uses transmitted data and library of previous data can also be used to determine whether malicious data are passed [25]. Each node will need to be analysed independently to protect against distributed attacks.

Most security models evaluate whether the current state of the system is valid by comparing it with a set of known security states. An exposure analysis graph can be used to identify users and data flows. Here, each node on graph has the following vertices: security mechanism, system privileges, information objects, and untrusted users; edges are directed paths to other nodes. This can be used to check for spoofing, tampering, repudiation, information disclosure or leakage, denial of service, and escalation of privileges [26]. Hierarchical Petri nets have been used to model multiple attacks [27]. Attack trees cannot track coordinated attacks, and multi-step Petri nets are limited to tracking three attackers. Hierarchical Petri nets are not limited to the number of attacks and can be used for multiple attacks including eavesdropping, interference or interruption of communication, unauthorized data access, service theft, and denial of service. The hierarchical model is built in teams such that local experts map the threat paths and outcomes in their areas, regional experts take local, mapping Petri net to network and create hierarchical structure and regional hierarchies combined into single overall Super Petri net using corresponding points.

Security of the physical state estimation is essential for the stability of the grid. Data collected from synchrophasors and other state estimation devices need to be analysed for corruption on malicious alteration. Security-oriented physical state estimation system [28] attempts to do that by exploiting the interrelation among the cyber- and physical components of the power grid. It utilizes information provided by alerts from bot host and network-based intrusion detection systems in its analysis. It uses file and memory check information from host-based IDS and permission issues, invalid signatures, and data packet inconsistency information from network-based intrusion detection systems to detect intrusion. It creates an attack graph template showing potential attack paths possible to be traversed by intruder and potential vulnerabilities. It works off base-case power flow solution, which defines how measurements should be correlated and checks for attacks using the template, and computes the probability that system has been compromised. Potentially compromised domains are noted and suspicious measurements identified. It then proceeds to suspicious measurements, attempts to estimate state while ignoring suspicious measurements, and if that is not possible waits for next interval to compute the state estimate. Reference [29] suggests different levels of protection

of data based on criticality and providing the maximum security to a strategic subset of sensor measurements that influence the most system variables. Reference [2] suggests a comprehensive and integrated agent-based security platform with three layers of security, i.e. power, automation and control (monitors and control power grid processes), and cyber-security (handles access and data checking). Security agents located in meters, substations, and relay station command centers to handle protocol translation, security patch updates, pattern recognition, process flow, intrusion detection, data encryption, and access control. They propose using an anomaly-based detection system such that alarms are issued for activities outside of normal behaviour.

1.3.3 Network Security Threats

Several researchers have identified the various types of cyber-attacks that could threaten smart grid operations. The most exhaustive list was provided by [30], which includes eavesdropping, traffic analysis, interception of signals (electromagnetic and radio frequency), media scavenging, data interception and alteration, identity spoofing, bypassing controls, authorization violation, physical intrusion, man-in-the-middle, replay, malware, Trojans, trap doors, service spoofing, and resource exhaustion. A key threat to the grid is the potential for hackers to leverage the AMU for access to the bulk electric grid.

The main four that seem to be the focus of most research are eavesdropping, injecting false data via intercept/alter, service spoofing, and resource exhaustion. Some smart grid administrators do not even concern themselves with the spread of malware (like from viruses or Trojan horses) or the risk of a remote attacker assuming control of the system, believing that the firewall and other network protection on their computer system will be sufficient. However, many of these systems use HTTP and TCP/IP protocols, two systems that have documented vulnerabilities [31].

Eavesdropping is the situation where an outsider intruder listens or gathers data intended for the smart grid system. In this attack, the attacker, or eavesdropper, taps into the transmission signal between the data source (a home sensor, for instance) and the smart grid control centre. Eavesdropper can intercede between the time the data are encoded and the time it is decoded. That may slow down an eavesdropper, but some malicious attackers could have access to the common decoding algorithms, and with enough trial and error determine how to read the data.

Such successful decoding could then lead to the next type of attack: injecting false data. In this attack, the malicious intruder intercepts valid data and transmits false data to the control centre. Most control systems are decided to question or ignore data whose mean square difference from the normal or expected is too high [32]. Knowing this, though, an attacker can analyse data for a period of time, determine an acceptable range of values, and inject data that will be accepted by the control system [33]. The attacker can also serve as a “man-in-the-middle” and send fraudulent

messages to either the customer or the system. Surprisingly, such an attack does not require much effort to cause an undetectable change in the system's operations. Experiments have shown that on an IEEE 300-bus system, it only took injecting bad data from ten different meters to cause an undetectable error that negatively affected most of the system control variables [32]. On most IEEE n-bus systems, it took as few as four strategically selected meters to cause such an error [32].

What is worse is that such attacks can be conducted from a variety of sources. An individual meter can be attacked, causing it to transmit corrupted data or causing it to stop transmitting entirely. A substation, which collects data and monitors distribution for a particular region could also be subject to attack. A substation attack can involve blocking data from certain sources, injecting false command codes, or misrepresenting the power flow into or out of that substation [2]. Even the control centre itself is not immune. If an intruder can gain access, the SCADA could be flooded with bad data, a communication link with a substation (or series of substations) can be broken, command codes could be altered, and consumer price rates can be changed [2].

Response and recovery engine [34] employs 2-player adversarial Stackelberg stochastic game theory along with attack–response trees that create Markov decision trees for intrusion prevention, detection, and response. There are three main types of intrusion response systems, i.e. lookup tables with predefined mappings, which are neither scalable nor flexible, and heuristic based, which could become predictable to the intruder and selection models. They suggest an engine with a state space large enough for decision analyst to be able to create attack–response trees that uses a multi-step process for the response, i.e. determine what areas have been attacked, identify appropriate attack–response trees for the attacked areas, create responses by collapsing response sequences into Markov decision processes (resolve uncertainties using Bayes binary classification), and determine best action to take based on chosen responses and system criteria. The process can be repeated for each new attack.

Several security systems detect an error or attack and trigger an alarm, but are not designed to adaptively fix and prevent future attacks. Reference [35] focuses on preventing future attacks and suggest an anomaly security system that uses past normal data as well as data with intrusion to update anomaly classification information. It also suggests using instruction set randomization to prevent code-Injection attacks and a transformational key such that injected code does not mesh with the rest of the code. This can also prevent man-in-the-middle and denial-of-service attacks. Anomaly classifications help identify bad data injection which is not perfect and will lead to false positives. They suggest using false-positive correction as bad data for an attack. Their model suggests a 3-step process, i.e. filtering to trap any suspicious activity, classification to evaluate malicious behaviour and supervision to provide feedback to proxy/agent, and remediation to prevent future attacks.

Summary

Cyber-security in the smart grid is required at the perimeter as well as internal to the network. The standard perimeter defence would include firewalls, intrusion

detection systems, and secure architecture, while the internal defence would include integrity checks, network monitoring, and log analysis. In addition, it is necessary to institute a key exchange mechanism along with protocols for end-to-end encryption of data. It is also necessary to institute robustness to false-data injection (FDI) and denial-of-service attacks by creating redundant channels and fall-back positions for state estimation and load forecasting.

1.4 Mitigating Cyber-Physical Threats

One of the key security unknowns is how vulnerabilities can be exploited in the cyber-physical domain, i.e. can a cyber-vulnerability lead to an attack on the physical infrastructure or vice versa can a physical vulnerability expose an attack on the cyber-infrastructure. It is anticipated that the SCADA systems be targets of multifarious attacks from several actors including foreign governments, terrorists, and competitors. SCADA systems are typically engaged in data collection, analysis, control, and visualization. Such systems would be used not only for the traditional operation of the power grid but also for smart grid-specific applications including enabling microgeneration, automated recovery from faults, enabling electricity market functions (price signalling, energy trading), and demand response (DR). Its enhanced capability would also make them ripe targets for cyber-attacks. The typical modus operandi of a cyber-attack would involve the following: (1) gaining access to the SCADA network either through a corporate network, VPN connection, or a remote site connection, (2) probing the SCADA network to discover the appliances, data storage, and vulnerabilities and deduce the SCADA processes, (3) attacking and controlling the SCADA system by gaining root privileges, getting access to the data, and launching control commands.

A typical cyber-physical system attack would involve four steps: (1) identifying weaknesses in the cyber-infrastructure; (2) intruding into the system and gaining privileges; (3) understand and gaining control of the control system; and (4) using the control system to launch physical attacks. One of the key concerns is data manipulation at destabilization of the grid as well as denial of service. For instance, in case synchrophaser data are manipulated through FDI, the grid could be made to oscillate and eventually go down. The demand can also be manipulated forcing a demand–response from the utility company effectively denying the availability of power for some consumers [36].

There are several potential attacks that can be launched against SCADA systems including false-data injection, replay attack (forging time stamps), denial of service, and sensor spoofing. For instance, the smart grid will have automatic detection of anomalies—if a false anomaly is injected into the grid, it could lead to dispatch of crews in unneeded areas. Most importantly, attacks in a substation can include missing or corrupted sensor data as well as false-command injection and delay in data transmission. Such attacks can cause circuit breakers to open at the wrong times, system run exceeding limits, system outage, false alarms, damage to

equipment, and injuries/deaths or operators and end-users [36]. There can also be attacks that corrupt data going from transducers in the field causing circuit breakers to trip and leading to outage. Attacks could also include tampering metering data that can lead to false implication of users resulting in penalties including fines and termination of connection. Often, substations are controlled from control centres, and any falsification of communication data between the two can lead to system outages, false alarms, incorrect procedures, system outages, and physical injuries.

Many of the software for SCADA systems were developed decades ago without security considerations, making SCADA systems highly vulnerable to software exploits. A lot of software does not have adequate authentication and access control mechanisms, making access to hackers easier. Due to the large number of vendors and devices, it is difficult to test all the devices and software ahead of time. Over the last two decades, we are seeing more homogeneity in SCADA system software that allows for better testing and validation of software for security compliance. This homogeneity, however, is a mixed blessing—having obscure operating systems and devices makes generic attacks harder; however, it makes targeted attacks by dedicated adversaries easier [37]. Since late nineties, there has been a strong focus on standardization of SCADA systems leading to greater homogeneity which makes them targets for mass non-specific attacks and probes. Coordinated large-scale attacks will be facilitated by the homogeneity in the network that can overcome the resilience of the network and cause large-scale failures in the grid.

1.4.1 Risks at Cyber-Physical Interface

The risks at the cyber-physical interface follow the logical divisions of the smart grid infrastructure, i.e. generation, transmission, and distribution [38]. At the generation level, the risks occur at the level of automatic voltage regulation, governor control, and automatic generation control.

1.4.1.1 Generation

Power carried in alternating current networks is typically comprised of real power and reactive power. The real power is used for doing work, while reactive power is used for maintaining voltage stability. By controlling the production, absorption, and flow of reactive power, voltage can be maintained within acceptable limits, while transmission losses are minimized. Generator exciter control is used to control the amount of reactive power being absorbed or injected into the systems. The control module communicates with the plant via Ethernet, and by comparing the generator voltage output and voltage set points, it alters the current flow through the exciter to maintain stable voltage. Similarly, governor control is used to control the frequency of the rotor by altering the power output from the generator. Again an Ethernet connection is used to measure the rotor speed and provide feedback to the

governor control for altering the power output. Both of these control systems are local without requiring remote telemetry; however, there are vulnerabilities associated with malware that can be inserted locally through USB or by compromising the local area network. Altering the set points or injecting false data on the output readings can lead to instability of the generator.

Another area of concern is the automatic generator control wherein output from multiple generators is adjusted for changes in the load. The output from the generators must match the anticipated load on the grid very closely or else consumers would experience voltage sags and spikes which are both bad for operation of electric and electronic equipment. The balance can be estimated by measuring system frequency. Increasing frequency means more power is being generated than used, and vice versa decreasing frequency means more load on the system than the generators are producing. Automatic generator control increases or decreases load across multiple generators based on prior protocols. An attack on the automatic generator control can result in significant operational damage through instability in the grid. Since multiple generators are involved, there is obvious need for remote telemetry to gather load data and provide feedback to the generators. This increases the vulnerabilities in the network that can include disruption of telemetry, false-data injection, intrusion, and denial of service.

1.4.1.2 Transmission

At the transmission level, there are two applications that are critical, i.e. VAR compensation and state estimation. VAR compensation is done using fast-acting devices for providing reactive power on high-voltage transmission lines for impedance matching. If the grid's reactive load is leading, VARs are consumed to lower the voltage, and if the reactive load is lagging, the capacitor banks are switched on to increase the voltage. The modern VAR compensation devices are thyristor controlled that can operate autonomously. There is a network of such devices that need to communicate with each other to determine the operating point. A denial-of-service attack on the network could result in an inability to communicate impacting the dynamic control capabilities causing degradation of power quality or disruption of power due to voltage sags and surges triggering shutdown of critical devices. There could also be timing-based attacks that disrupt the synchronization of the devices, which is critical for operation of the network. Finally, there could be data injection attacks that send incorrect operational data that may result in incorrect VAR compensation impacting the synchronization.

To improve the situational awareness of the electric grid and to maintain the stability of the grid, the state of the grid needs to be monitored. The new smart grid will also be retrofitted with synchrophasors. These devices measure the characteristics of the electrical current travelling at different points on the grid at short time intervals (typically 30 measurements per second). They typically use a common time source typically based on GPS to allow for time synchronization across the entire grid. This data will facilitate a number of applications while enhancing

others, such as real-time monitoring of the system, state estimation, disturbance monitoring, instability prediction, and wide area protection and control. The characteristics of the data generated by synchrophasors make them particularly vulnerable to cyber-attacks. They play a critical role in maintenance and control and power generation and distribution, making them attractive targets for malicious actors for disrupting the power grid. Synchrophasor data are collected at geographically diverse locations and are usually routed to data concentrators in central locations using public Internet, making it susceptible to several attacks including FDI, disruption of communication, and corrupting the analysis. One of the attacks is based on data analysis where a hacker has access to partial data which can be analysed by a hacker to predict behaviour of the grid and then use the information to attack the grid. There are obvious ways in which the data can be protected including data obfuscation, anonymization, and encryption.

1.4.1.3 Distribution

The distribution system carries lower-voltage power across distribution lines to the customers. This system will have several applications that will have intelligence built into it. The most visible applications are the Advanced Metering Infrastructure (AMI) and DR. The AMI will allow for increased reliability, incorporating renewable integration from microenergy sources, and provide visibility into the usage at the customer end down to the appliance level. Smart meters will provide utilities with load control switching (LCS) ability to turn off appliances during peak hours to better balance the load. The smart meters pose strong vulnerability at individual consumer level whereby services could be disabled or enabled by hackers at will if they were to breach the security of the smart meter. The second major application is billing application for which the smart meters will read usage data, validate it, and create electricity bills. In addition, the meters will be used to establish and terminate services as well as restrict services for non-payment of dues.

A second key application at the distribution level is the self-healing elements of the grid where automatic reclosers are used to clear momentary faults. Faults that cannot be autocorrected can be detected through sensors placed in the distribution network. Data injection attacks can be used to show spurious attacks that will lead to unproductive dispatch of resources. At the same time, a denial of service on the network can prevent crews from reaching a site of an actual disruption.

1.4.2 Mitigating Cyber-Physical Threats

The fundamental problem with the smart grid is its geographic expanse across a vast area with several soft targets that are vulnerable to attacks. Physically defending the entire grid is a daunting task; consequently, building resilience in the infrastructure is a critical mitigation strategy, including self-recovery, redundancy

in power distribution and communication, excess capacity in communication, power conduits, and physical power hardware. The second critical issue is to ensure that the critical control systems have a system of alerts that quickly provides alerts when the device is operating at a dangerous level. Thirdly, we need to deploy manipulation detection algorithms on a case-by-case basis of different algorithms to minimize the impact of data poisoning. Perfect security is unachievable; however, the goal is to minimize the risks such that malicious activity can be detected quickly, catastrophic situations can be avoided, and recovery from attacks and anomalies can be swift. We recommend a risk analysis approach to understand the high-level exposure to the smart grid and mitigate the threats that it faces. Cyber-physical threats require creation of detailed attack trees to understand the cyber-physical interactions in the grid.

Summary

There is considerable danger to the smart grids associated with the cyber-physical threats. We have risks at each level of the grid, including generation, transmission, distribution, and home networks. The scope of damage varies from catastrophic to minor based on the attack vector and where it is launched. The increasing homogeneity and connectedness in the grid provides a fertile ground for launching large-scale attacks that can have serious repercussions on the operations of the grid including large-scale blackouts. Our policy has to be quick detection and containment for defending against zero-day attack vectors, and for the run of the mill cyber-attacks, we need to develop redundancy and resilience into the grid to prevent catastrophic failures.

1.5 Mitigating Smart Meter Threats

1.5.1 Threats and Vulnerabilities in Meter Infrastructure

As the key components in smart grid infrastructure, smart meters accommodate the most valuable data (e.g. meter readings) for improving the performance of power grid and changing the lives of electricity consumers. For instance, meter readings are required to support many smart grid applications and services, including automatic meter reading, billing, dynamic pricing, and detection of impending blackouts and energy thefts, which can bring great convenience to both utilities and energy consumers. However, the massive amount of data collected from smart meters should be carefully protected against misuse. It is desirable to incorporate security mechanisms into the design and implementation of smart meter infrastructure so as to increase robustness and resilience for the system and gain energy consumers' trust.

Skopik et al. [39] analysed the security threats and vulnerabilities in smart meter infrastructure detailed in three tiers: smart meters, utility, and Web application. The first-tier smart meter vulnerabilities are categorized as the attacks to the smart

meters (devices) itself, such as manipulating the hardware and the firmware, and exploiting limitation design and implementation. The corresponding countermeasures and defence mechanisms for such attack include authentication and strong encryption of communication, secure key management, securing the firmware, and secure source code development. The second-tier vulnerabilities occur at the utility, which suffers the potential attacks such as near-me area network (NAN) sniffing, own or foreign meter emulation, large-scale meter takeover, and concentrator nodes (s) attacking. Secure system design, secure operation, and secure service evolution can be utilized to tackle such security concerns at the utility [3]. The last tier, Web application vulnerabilities can be exploited by attackers by compromising the security in smart metering data management and value-added services, such as automatic billing, as well as the privacy in smart grid [40].

In smart grid, the AMI accommodates two-way communication between the smart meters and utility and enables remote control and monitoring for both energy service providers and consumers. Rahman et al. [41] investigated the non-invasive threats and the vulnerabilities in such infrastructure, such as lack of authentication, slave meter data tampering, slave meter unauthorized disconnection, insecure protocol implementation, and firmware upgrade vulnerabilities. More specifically, the non-malicious threats involve reachability and integrity threats, and availability threats (e.g. improper scheduling of data delivery between meters and collectors leads to buffer overflow and data loss in the collector side). The malicious threats could be typical cyber-threats on AMI such as DoS, link flooding, and wireless link jamming. For instance, a large number of compromised collectors can launch a distributed DoS attack to a headend. In this scenario, it is infeasible to resolve the cyber-threats from the compromised collectors. Indeed, the heterogeneity of interdependent hardware configurations (each operating with various security parameters) would lead to both malicious and non-malicious attacks [41]. Rahman et al. have proposed the detection methods in an automated security analysis tool for AMI—SmartAnalyzer. It provides the following functionalities [41]:

- Extensible global model abstraction capable of representing millions of AMI device configurations.
- Formal modelling and encoding of various invariant and user-driven constraints into SMT logics.
- Verifying the satisfaction of the constraints with AMI configuration using an SMT solver [26, 30].
- Identifying potential security threats from the constraint violations and providing remediation plans for security hardening by analysing the verification results.

With AMI, meters are not read manually anymore, but digitally instead. The digital usage rates transmitted from site to site would leave loopholes and security vulnerabilities for malicious attackers and energy theft. Xiao et al. [42] have also identified three classes of attacks based on when and where the data for the amount of service are manipulated: (1) while the data are recoded, (2) while the data are at rest in the meter, and (3) as the data are in flight across the network. They discussed

the possible way to resolve these types of attacks by installing a redundant meter at the energy provider end. However, the above solution is impractical because of the huge number of "inspector" meters required for all the end-users (each user needs one). Alternatively, Xiao et al. [42] proposed a model, in which N number of end-users' meters are monitored by a "head inspector". The head inspector utilizes a series of algorithms to collect heuristic usage information based on an adaptive-tree-based inspection scheme. The inspection strategy in response to anomalous readings can be adjusted to pinpoint the meters where fault or security compromise occurs. This strategy is effective to address the aforementioned classes while maintaining a low cost compared to monitoring each meter directly.

1.5.2 Security Breach on Smart Meter

Similar to other contexts of security, Gering [43] discussed the confidentiality, integrity, and availability of smart meters. Specifically, "confidentiality" ensures that sensitive data are not exposed to the unauthorized person or system and the information disclosure should be limited. "Integrity" ensures that actions can be traced to initiators, which helps to protect against deception. "Availability" ensures that data, commands, and communications are accessible and usable when desired. To guarantee each of them, for instance, Gering [43] stated that encryption techniques can be used to ensure confidentiality using techniques such as triple data encryption algorithms, advanced encryption standards, elliptical curve cryptography, and RSA public key cryptography.

Some examples of breaching different aspects of security are given below:

- To hack into a smart meter, David Baker (the director of service at IOActive, a Seattle-based research company) described a possible way to pass through the smart meter's wireless networking device. A software radio, which can be programmed to emulate a variety of communications devices, can be used to listen wireless communications with the network and deduce how to communicate with the meters over time. Besides this, he also discussed another method —attacking the hardware. An attacker could steal a meter from the side of a house and reverse-engineer it. However, this method requires a good knowledge of integrated circuits for reengineering the meter, which is inexpensive [8].
- An independent security researcher specialized in wireless sensor networks, Goodspeed (an independent security researcher) told another story about smart meter hacking [8]. If the meter has not been built with rigorous security features at the physical level, a hacker can insert a needle into each side of the device's memory chip. It is indeed a probe to intercept the electrical signals in the memory chip. Then, the hacker can readily obtain more information from the device by analysing such signals. Even if some security features have been integrated into the meter, it may be possible to extract the information using some customized tools.

- Besides the inevitable smart meter hacking activities, a massive network virus or worm can also attack utilities. In this case, utilities can implement granular security architectures to protect their smart grid system [44]. The unique standard-based hardware and software security should be embedded into the network node and device. Such security modules could help prevent device penetration attacks (in the form of worms or viruses) from spreading throughout the network. The embedded device-level security ensures that a hacked or compromised device can be quickly identified and isolated before spreading or causing greater damage. Including the above case, utilities leverage the best efforts they made and millions of dollars of investments on smart grid/meter security to the latest security technologies in other contexts.

1.6 Mitigating Data Manipulation Threats

1.6.1 Introduction

Cyber-security in critical infrastructure and particularly the smart grid has received significant research interest [45–47, 30, 43, 48, 48]. In modern smart grid, Supervisory Control and Data Acquisition (SCADA) software and hardware component is generally implemented to supervise, control, optimize, and manage power generation and transmission. The SCADA system integrates new components (e.g. smart meters), networks, sensors (e.g. phasor measurement units or PMUs), and control devices. More intelligently, the future smart grid infrastructure will accommodate renewable energy resources, electric vehicles loads, and storage, among others [50] by making the components intensively interconnected. However, new vulnerabilities may arise along with the convenience brought by new features in smart grid. So far, hackers begin to penetrate the control network and administrative devices in the US electric grids via Internet [51]. In August 2010, a computer worm targeted the SCADA system, infected thousands of computers, and tried to compromise the critical infrastructure [52].

As a centralized control centre which conducts controlling and monitoring activities for the power grid, SCADA system receives and stores various real-time meter measurements, including bus voltage, bus real and reactive power injections, and branch reactive power flows in every subsystem of a power grid. State estimation plays a key role in controlling- and monitoring-based energy management in SCADA system [14, 53], which optimally estimates the state of the grid by analysing data such as system parameters, power meters, and voltage sensors. More specifically, such function estimates unknown system variables using the meter measurements data in the electric grid. Results of the state estimation will be generated to maintain system in normal state, to optimize the power flow such as increasing the yield of an electric generator, to balance supply and demand load, and/or to ensure reliable operations such as detecting faults in the system [54].

A malicious adversary may aim at altering the data (e.g. meter readings) transmitted to the control centre. Thus, such violation of data integrity will result in great threat to the entire smart grid system since the decisions of energy management created in system estimation might be significantly deflected by this kind of malicious behaviour, namely FDI attack. Essentially, FDI attacks maliciously modify the data generated in smart grid (transmitted to and stored in SCADA system) and may potentially trigger two negative impacts [36]:

- If the data are modified in a way that is not detectable as false by state estimation, the observable state of the system will be wrong and may lead to actions by the grid operator where security concern may arise in the system.
- The malicious intent may not be able to hide the attack. Even though the attack is detected, part of the system may become unobservable, which means that the state estimator cannot estimate state values such as voltage magnitudes and voltage, and the transmission grid would be vulnerable to a local physical attack. By the time the consequences of the physical attack have propagated into the rest of the system where the state is observable, it may already be too late to avoid an outage of a larger part of the system.
- Data manipulation threats and FDI attacks would explicitly or implicitly lead to significant errors by compromising the meter readings in state estimation (optimal estimation of the power system state using data from power meter voltage sensors and system parameters [50]) or other smart grid components. Roughly speaking, FDI attacks can be categorized into the following two types [54].
- Observable/non-stealth attack: naive false-data integrity detection algorithms can easily detect such attacks since only meter measurement data have been changed. Difference between the compromised data and the physical information could be used to detect and report such kind of attack by the control centre.
- Unobservable/stealth attack (the compromised meter readings are consistent with the physical power flow constraints) will bypass many false-data integrity detection algorithms.

In this chapter, we summarize the potential data manipulation threats of FDI attacks in smart grid (particularly the unobservable attacks). The state-of-the-art defence mechanism or countermeasures are proposed to detect and tackle the threats as well as system vulnerabilities.

1.6.2 Resolving Data Integrity Violation in State Estimation

Compromising meters at the control centre and introducing malicious measurement has been discovered as an attacking technique for adversaries recently [55]. For instance, an online video tutorial shows people how to manipulate electric meters to cut the electricity bills (https://www.youtube.com/watch?v=wa13_l-qjBE). Following the same instructions, it is possible that the attackers target the meters at the

smart grid control centre and inject bad measurements. If the outcome of state estimation is altered by the adversaries with such injected bad measurement, severe incidents such as power outage of large geographic areas may occur.

Some researchers have developed techniques to identify and tackle the observable malicious measurement injection [56, 57], where most of the techniques were targeted at arbitrary, interacting/correlated malicious measurements. More recently, more practical and advanced problems on attacking smart grid state estimation are investigated. For example, Liu et al. [32, 55] discovered that if prior knowledge such as the configuration of the power system is known to the adversaries, malicious measurement could bypass the regular detection and identification techniques proposed for observable attacks. Observable malicious measurement attacks could be easily detected because "the difference between the observable measurement and the estimated measurement becomes significant" [56]. Liu et al. [32, 55] studied a new class of threats to state estimation, namely FDI, assuming that the adversary can take advantage of the power grid configuration from the perspective of the attackers. They showed that the attacker can inject malicious measurements that can bypass the bad measurement detection on observable attacks and focused on two realistic attacking scenarios:

1. The attacker has limited access to some specific meters
2. The attacker is limited in the resources required for compromising meters. Specifically, two attacking goals are considered in [32, 55], which are random FDI attacks (injecting a random error to the result of state estimation) and targeted FDI attacks (injecting an arbitrary error to the result of state estimation).

Note that in the above work, the attacker is assumed to know the target power grid configuration and the meters are manipulated before they are used for state estimation, possibly as an insider or ex-insider. Although strong requirements are posed in the scenarios, the electrical engineers and security personnel should be aware of the threat which would lead to catastrophic impacts as well.

Rather than assuming that an adversary possesses complete knowledge on the power grid topology and transmission line admittances [32, 55], Rahman and Mohsenian-Rad [58] investigated a more practical scenario in which the attack has limited information with respect to the power network topology or admittance for some transmission lines. They disclosed that it is possible to compromise state estimation with only incomplete information against smart power grids. A more realistic FDI attack was introduced in [58], where various grid parameters and attributes such as the position of circuit breaker switches and transformer tap changers are unknown to the potential adversaries, and the adversaries also have limited access to most of the grid facilities. Covertly compromising the readings of multiple power grid sensors and PMUs in order to mislead the operation and control centres was identified as the major threat against smart power grids in [58], though adversaries only have incomplete information. Moreover, two types of FDI attack were introduced in [58], which are perfect attacks (the attacker has complete knowledge of the admittance for all lines on at least one cut on the grid topology) and imperfect attacks (the above information is not available). Rahman and

Mohsenian-Rad also showed that it is possible to construct a probability distribution function for unknown admittance to design an imperfect attack and simulated the result with a novel vulnerability measure.

For "unobservable attack", Kosut et al. [16, 59] distinguished two primary regimes in which malicious unobservable data attacks occur, by whether the attackers have controlled sufficient meters to commit the unobservable attack. They discovered that two regimes have completely different behaviour to corrupt state estimation [16].

1. Strong attack regime: adversaries are able to access a sufficient number of meters to commit an unobservable attack. Attacks cannot be detected by the control centre, even if there is no measurement error.
2. Weak attack regime: adversaries do not have access to a sufficient number of meters; the attacks can be detected, though imperfectly due to measurement errors.

Kosut et al. studied the behaviour and presented the results of both regimes in [16, 59]. Also, from the perspective of the attacker, Kosut et al. [59] investigated that how vulnerable a power system is to the unobservable attack. More specifically, they explored the smallest number of compromised meters required to perform the unobservable attack and presented an efficient algorithm to find the small sets of meters required for triggering such attacks based on the purely topological conditions for observability (graph-theoretic approach). They also examined the worst malicious data attacks in the regime that the adversary cannot perform an unobservable attack. In [16], another relevant problem from the perspective of attackers was studied is examining the trade-off between maximizing the estimation error at the control centre and minimizing the detection probability. Besides the graph-theoretic approach presented in [59], detection mechanisms and countermeasures are proposed for the weak attack regime in [16]. Specifically, since the adversary can choose where to attack the network and design arbitrary injected data, hypothesis test cannot be used for formulating the malicious data detection problem. Instead, a detector based on the generalized likelihood ratio test was proposed, which is known to perform well in practice. If the detector has sufficient data samples, the performance is close to optimal. However, solving a combinatorial optimization problem is desirable for the detector; thus, if the number of corrupted meters is large, it is difficult to implement the detector due to efficiency. To tackle this issue, another detector is studied—using a convex regularization of the convexity of the optimization problem based on L1 norm minimization.

Giani et al. [50] tackled another specific unobservable attack problem for smart grid state estimation—unobservable low-sparsity cyber-attacks, which require coordination of a small number of ($\leq$5) meters. Since cyber-attacks of large number of meters in control centre tends to be improbable (for the reason that high degree of temporal coordination across geographically separated attack points is required for unobservable attack), they proposed an efficient algorithm to find all unobservable attacks involving the compromise of exactly two power injection meters and an

arbitrary number of power meters on lines. The algorithm requires O(n2m) flops for a power system with n buses and m line meters. If all lines are metered, there exist canonical forms that characterize all 3, 4, and 5 sparse unobservable attacks. These can be quickly detected with O(n2) flops using standard graph algorithms. Known-secure phase measurement units (PMUs) can be used as countermeasures against an arbitrary collection of cyber-attacks.

In some occasions, simultaneous attacks may occur on multiple meters of electric grids to manipulate state estimation. To formally formulate this type of data injection attacking problem, Kim and Poor [60] presented a unified formulation for the problem of constructing attacking vectors under an optimization framework by considering constraints on the measurements and limited resources of the attacker. Linearized measurement models were given against the attacks of manipulating system state estimators. They also showed that the proposed approach significantly outperforms the prior work.

1.6.3 Resolving Other Data Manipulation Threats

1.6.3.1 Topology

As an important input to smart grid operations, topology of smart grid includes state estimation, real-time pricing, and real-time dispatch [33]. Adversaries could partially manipulate the grid operations by perturbing the topology information of smart grid. Although topology information involves the data for power grid state estimation, topology attack may have different behaviour and targets from the FDI attack committed for state estimation. For example, an adversary may mask a connected line as disconnected or vice versa so that the control centre makes improper decisions in contingency analysis, optimal dispatch, or load shedding [33]. Moreover, since topology information can be used for computing real-time locational marginal price, adversaries may modify the topology estimate to maximize the adversaries' gain. Thus, besides state estimation, topology of smart grid is vulnerable to malicious data injection attacks.

Kim and Long [33] focused on the man-in-the-middle attacks applied to topology of smart grid, where the adversary intercepts network data (e.g. breaker and switch states) and meter data from remote terminal units, partially modifies them, and forwards the maliciously modified data to the control centre. Similar to "observable attack", if not both network data and meter data are altered in the attack, modern power systems equipped with bad data test could discover such inconsistency. Therefore, the adversary is assumed to successfully bypass the bad data test by modifying both network and meter data (consistent with the "target" topology) with known global information about system state. Similar to the state estimation attack, the feasibility condition for undetectable attacks was given along with the low detection probabilities in [33].

1.6.3.2 Load

Adversaries may commit cyber-attacks to electricity generation, distribution/control, and consumption in smart power grids. Compromising state estimation (as summarized above) indeed attacks the electricity distribution/control. Mohsenian-Rad and Leon-Garcia [9] investigated a typical data manipulation threat in the consumption sector—the load might be modified by adversaries. More specifically, with the development of demand-side management and the growth of Information Technology integrated into consumption, altering the load at specific grid locations through the Internet and by distributed software intruding agents has been identified as a new class of cyber-intrusions. Such data manipulation threat may involve abruptly increasing the load at the most crucial locations in the grid and then cause circuit overflow, or other malfunctioning that can immediately bring down the grid, or significant damage to the power transmission and user equipment.

Specifically, such attack called "Internet-based load-altering attack" is defined in [61] as follows. An Internet-based load-altering attack is an attempt to control and change (usually increase) certain load types that are accessible through the Internet in order to damage the grid through circuit overflow or disturbing the balance between power supply and demand. Notice that three types of loads are accessible through the Internet and can be the target of load-altering attacks [61]:

1. Data centres and computation load: a data centre's power load is highly elastic and relies on the data centre's computation load. The energy consumption of data centre can be doubled when computer servers are busy, compared to when the computer servers are idle. Thus, data centre can be the appropriate target of Internet-based load-altering attack.
2. Direct load control: with Internet-based load-altering attack, the adversaries may compromise the command signals to seize the operation of the residential and industrial load which are supposed to be controlled by direct load control programs (one of the most common demand-side management programs used for minimizing peak demand, improving system operation, or maximizing quality of service).
3. Indirect load control: in smart grid, indirect load control allows customers to control their loads independently in terms of the price signals sent by utilities, e.g. through the Internet. Given the price information and based on the energy consumption for each household appliance, the decisions can be made by minimizing the cost of energy, minimizing the finishing time for the operation of appliances, or achieving a desired trade-off between cost and timing. Since the price information is obtained through the Internet, load-altering attacks can inject false-price data into the automated residential load control. Major changes of the load profile can be caused by modifying the energy consumption program in thousands of households.

Essentially, Mohsenian-Rad and Leon-Garcia [61] overviewed a collection of defence mechanisms which can facilitate blocking the Internet-based load-altering attacks or mitigating the damage caused by such attacks. The defence mechanisms

range from protecting the command and price signals in direct and indirect load control to load shedding, attack detection, protecting smart meters, and load relocating. To reduce cost for applying defence mechanisms, the authors proposed a cost-efficient load-protecting strategy to minimize the cost of load protection while preventing from overloading the grid.

Summary

In summary, data manipulation threats may exist in most data-intensive components in smart grid infrastructure. How to detect the FDI attacks (both observable and unobservable), and eliminate or mitigate the vulnerabilities in smart grid have attracted considerable interest in smart grid research. As a primary data manipulation threat to smart grid infrastructure, the FDI attackers intend to mislead the decision-making of smart grid by hacking the readings of multiple sensors and PMUs. FDI can be executed to the smart grid components and devices in which data are generated, transmitted, received, and stored. For instance, state estimation requires data analysis received from meters; thus, data collected from the meters will be the target of potential FDI attacks, vulnerable to data manipulation threats.

In this chapter, we illustrated the behaviour and characteristics of the data manipulation threats and attacks according to their targets such as state estimation [16, 59], topology information [33], and load at the energy consumption side [61] and briefly introduce the defence mechanisms and countermeasures proposed in the literature.

1.7 Mitigating Privacy Threats

1.7.1 Introduction

Today, enormous amount of data/information are ubiquitously collected by commercial companies, organizations, or governments for analysis, which facilitates the development of services and applications in many industries. In practice, it is often necessary for the data owners to share their data to other parties for functioning the corresponding services and applications, or deriving more comprehensive and precise knowledge. However, explicitly sharing data would incur significant privacy risks to the individuals or organizations. Some serious privacy-leaking incidents happened recently; for example, AOL Inc. published their customers' 3-month Web search history in 2006 for research purpose. Although the IDs have been removed before data publication, many AOL users were still identified from their search information by the adversaries, and then, much of their private information and personal behaviour were exposed to the public. Also in 2006, Netflix Inc. published their customers' movie rating information to accommodate an open competition for the best collaborative filtering algorithm of predicting users' movie

ratings. In 2007, two researchers from the University of Texas identified individual users from the Netflix movie rating data by linking the datasets to some other sources such as Internet Movie Database.

Such incidents exist almost everywhere, such as healthcare systems, location-based services, and DNA applications. Smart grid has a similar story as above on privacy threats. More specifically, implementing "smart" in modern grid systems requires information disclosure across different parties, many of which are untrusted in general. For example, utilities need to monitor electricity usage and load and determine bills; electricity usage advisory companies need to access the metering information to promote energy conservation and awareness; marketers access the profile of the customers for targeted advertisements; law enforcement officers access smart grid data for criminal investigation [37]. All of these data access may comprise consumers' privacy in smart grid system. Precisely speaking, utility usually collects the fine-grained energy usage (perhaps at the appliance level) from their customers, where the households' personal behaviour could be learnt from the status of appliances [41, 23].

On the one hand, consumers wish to save energy and their money with smart grid applications. However, on the other hand, they worry about the private information leakage since an intelligent monitoring device transmits their live usage to utility every 15 min with smart metering service [37]. Besides the personal behaviour patterns learnt by strangers, metering information disclosure may also make them vulnerable to annoying advertisements, thieves, or even robbers (e.g. criminals can identify the best times for a burglary or to identify high-priced appliances to steal [37]). A report released in 2010 by the consulting company Accenture states that one-third out of more than 9000 consumers from 17 different countries are not comfortable to use energy management programs provided by smart grid (e.g. smart metering) if their personal consumption information could be easily accessed by utilities [37]. Therefore, it is desirable to design smart grid services and applications without compromising individual customers' privacy and organizations' proprietary information. In this chapter, we investigate the privacy issues in smart grid infrastructure by illustrating the privacy threats, privacy laws, and state-of-the-art schemes related to smart grid.

1.7.2 Privacy Threats in Smart Grid Infrastructure

Personally identifiable information (PII) is the information that can be used on its own or with other information to identify or locate an individual person. PII can be one's name, contact and biographical information, individual preferences, transactional history, activities, or any information derived from the above [62]. In the context of smart grid [47, 62], at the customers' end, the linkage of any PII and the energy consumption could be utilized to identify individuals. Many customers' activities and end-user components may disclose their personal information to

utilities or other untrusted parties, such as smart meters, smart appliances, dynamic pricing, load management, and consumer access to energy-related information [62]. For example, smart appliances communicate frequently with the grid to share the real-time energy usage information as well as the status of the appliance; dynamic pricing provides the current or future pricing information to customers and enable them to modify their demand at different time (e.g. time-of-use pricing, critical peak pricing, real-time pricing)—the preferences and response could indicate the personal behaviour and help identify customers.

A senior consultant with Cutter Consortium's Business Technologies Strategies practice and privacy professor, Rebecca Herold identified and discussed the data privacy concerns in the smart grid in the NIST SmartGrid privacy group report [63]. The privacy concerns w.r.t. PII are summarized as below:

- Identity Theft: the combination of PII may be misused to impersonate a utility or consumers, resulting in potentially severe threats. Attackers can masquerade them to forge negative credit reports, behave fraudulent utility use, and other damaging consumer actions.
- Determine Personal Behaviour Patterns: energy consumption profiles/patterns in the fine-grained metering data directly or indirectly reveal specific times and locations of electricity use in different locations. Also, the types of activities and appliances can be inferred from such data.
- Determine Specific Appliances Used: the appliances used at specific times can be easily inferred by adversaries if they can access the fine-grained consumption data [40].
- Perform Real-time Surveillance: the utilities collect the fine-grained metering data for energy management and value-added services development. If the time interval becomes shorter, the data collection can be considered as the real-time surveillance by potential adversaries.
- Reveal Activities through Residual Data: the power status of different appliances can reveal such information.
- Target Home Invasions: the living habits of the household can be indicated from the fine-grained metering data. The attackers can easily target a house and learn when the house owners do not stay at home, and then possibly breaks into the house.
- Provide Accidental Invasions: similar to home invasions, criminals may break into houses without target, but learn the living habits of various households.
- Activity Censorship: residential activities could be revealed by the fine-grained metering data. Such information might be shared with local government, law enforcement, or public media. Then, the residents may be under risk of harassment, embarrassment, etc.
- Decisions and Actions based upon Inaccurate Data: PII might be inappropriately modified since metering data are stored, collected, and analysed at different locations.
- Reveal Activities When Used with Data from Other Utilities.

1.7.3 Privacy Laws w.r.t. Smart Grid

In many jurisdictions, privacy laws, which deal with the regulation of personal information of individuals, are considered in the context of individuals' privacy rights and reasonable expectation of privacy. For instance, the United States established Health Insurance Portability and Accountability Act (HIPAA), Financial Service Modernization Act (GLB), Family Educational Rights and Privacy Act (FERPA), etc. The offenders might be prosecuted in a case where individuals' privacy has been compromised. After the Netflix privacy-leaking incident, four customers filed a class action lawsuit against Netflix, alleging that Netflix had violated US fair trade laws and the Video Privacy Protection Act by releasing the datasets (for research and competition purpose). In this section, we introduce some current federal privacy laws w.r.t. smart grid.

1.7.3.1 Smart Meters and the Fourth Amendment [64, 65]

In reality, law enforcements may need to investigate crimes in the houses. They can track residents' daily behaviour and routines using the smart meter data; then, there is no restriction on such data access for law enforcement. By establishing protection of personal privacy rights in investigations, the Fourth Amendment was enacted to restrict access to smart meter data or creating rules to obtain such information. It guarantees that the "right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated" [64]. Under the modern conception of the Fourth Amendment, law enforcement officers may not be able to break into system for obtaining the smart metering data when a person has a reasonable expectation of privacy. However, since smart meters are an emerging technology not yet judicially tested, it is difficult to claim the certainty for handling it under the Fourth Amendment [64].

1.7.3.2 Electronic Communications Privacy Act (ECPA) [64]

The ECPA was enacted in 1986 to address the interception of wire, oral, and electronic communications [64]. ECPA prohibits the interception of electronic communications in general, but allows government to conduct surveillance with a specific mechanism (if a party has consented to such interception). In smart grid, the transmission of customers' fine-grained energy consumption via smart grid network falls into the electronic communications under ECPA. Utility would communicate with all the customers and continuously receive information from them via the network (assuming consents from customers have already been established). If the utility consents to interception of the electronic communication by the law enforcement, the surveillance would not violate ECPA. Note that in some types of criminal cases, court orders could authorize electronic surveillance in smart grid without the consent.

1.7.3.3 The Stored Communications Act (SCA)

The SCA (Title II of the ECPA) was enacted in 1986 to address access to stored wire and electronic communications and transactional records [64]. It prohibits unauthorized persons from accessing a facility which provides electronic communication service (ECS). It also limits the ECS providers to disclose information carried or maintained by them. Law enforcement could compel the disclosure of stored communications with a specific mechanism provided by SCA. The protection and disclosure restrictions apply to smart grid (i.e. metering data) since smart meter network might be deployed with the establishment of an ECS.

1.7.3.4 The Federal Privacy Act of 1974 (FPA) [64]

Energy consumption under smart meter is subject to the protections contained in the Federal Privacy Act (FPA). In other words, the FPA protects the smart meter data, and indicates that such time series information is personally identifiable: as a grouping of information of an individual, the smart meter data are typically stored and linked to a consumer's account (may include name, social security number, credit card information, or other PII) [64].

1.7.4 Embedding Privacy Protection into the Design and Implementation of "Smart Grid"

Generating "intelligence" in power grid system, for example, implementing efficient energy distribution, flexible load management, and dynamic pricing model, requires the collection and analysis of huge amount of data in smart grid. Thus, PII might be leaked to untrusted or semi-trusted parties in smart grid. So far, the primary privacy-leaking threats are caused by the fine-grained readings of smart meters in the infrastructure, which are required to monitor the grid status for utilities, consumers, and some other entities. After realizing privacy issues in smart grid infrastructure, contemporary smart grid services start integrating privacy-preserving schemes into their design and implementation [66]. In this section, we outline the privacy-preserving solutions proposed for the design and implementation of smart grid.

1.7.4.1 Metering Data Protection

Smart grid customers concern that their personal information (e.g. their living habits) might be exposed to other parties from the frequently collected metering data. The research question regarding metering data protection is that how to technically anonymise the fine-grained meter readings yet without negatively

affecting the network operations, billing applications, and other services. Increasing time intervals of meter readings could clearly remove the attribution of the metering data to specific consumptions; however, many smart grid services might be unavailable for such limited data disclosure. Instead, the following techniques have been proven to be effective for smart metering data protection [66]:

- Anonymization of Metering Data: Separating the technical data (e.g., meter readings) from customer IDs. Thus, the overall meter readings or even the detailed energy consumption cannot be linked to individuals. For this purpose, a third-party ID escrow company should be involved [67].
  Specifically, the utility collects smart meter readings linked to unique IDs instead of customers. In [67], readings are distinguished into two types: (1) low-frequency readings for billing purposes (one reading per week or month, which do not compromise privacy) and (2) high-frequency readings (below a minute). Note that high-frequency readings are required for the maintenance of infrastructure and system, and do not necessarily be linked to the real-world consumers. Low-frequency readings can be sent to the utility and billing company, and high-frequency readings should be processed at the next substation (e.g. for load management), but not stored at the utility end. Such work presented a framework that separates two kinds of readings, such that basic billing services are not affected and anonymized metering information can still be used for technical maintenance without compromising the privacy [66].
- Metering Data Obfuscation: Masking the own energy consumption profile with local buffers such as batteries. For instance, with an electric vehicle, the energy consumption of the individual appliances at different times cannot be inferred from the obfuscated data, while the overall consumption remains intact.
- The basic idea of obfuscating the metering data is to locally install intelligent power routers with rechargeable batteries. Then, the usage of individual appliances could be obfuscated. The household load peaks could be smoothened and obscure [68]. The intelligent power management algorithms are used to obfuscate the actual electricity consumption of a household. Varodayan and Khisti [69] presented a preliminary proof that integrating a rechargeable battery and loading/discharging it in non-periodic intervals could greatly reduce the information leakage on the status of the appliances of a household. Note that utilizing a rechargeable battery does not mean that the load peak or energy consumption profile could be completely hidden, but the inference from the metering data could be significantly limited.
  Similarly, Wang et al. [6] proposed a protocol to enable individual meters to report the true energy consumption readings with a predetermined probability. The randomized response model also obfuscated the metering data so as to prevent the inference of individual households' electricity consumption patterns.
- Privacy-Preserving Metering Data Aggregation: Online aggregation of data from geographically colocated consumers. For instance, the utilities can get the aggregated metering information rather than a single household.

- Smart meter data aggregation [70] was originally developed for reducing substantial amount of information and providing aggregated (metering) information for specific purposes. Indeed, metering data aggregation can also reduce the risks of leaking information from the household energy consumption. Two types of aggregation have been realized:

  (1) Spatial aggregation: the metering information is aggregated by geographical locations, where the sum of meter readings of a larger grid segment is transmitted to the data recipients such as the smart grid control centre, instead of the meter readings of single household.
  (2) Temporal aggregation: the aggregation of single readings from a particular meter over a longer interval, which is collected from a single smart meter (e.g. a household). As discussed earlier, the utility of temporally aggregated metering data is limited (e.g. only available for billing purpose).

Aggregation effectively protects privacy but has some new concerns on utility. Skopik raised some possible problems on privacy-preserving metering data aggregation. For instance, for both spatially and temporally aggregated data, it is difficult to run some smart grid services which rely on high-frequency metering information (e.g. dynamic load management, load forecasting, and energy feedback [66]). Also, without the detailed energy consumption information, it is difficult to detect wrong readings or energy theft. Finally, since data should be encrypted before sending out from households for preventing eavesdropping, decryption might be necessary at the other end which performs aggregation operations (e.g. substations). This requires great efforts to implement smart metering/grid services or applications with limited information disclosure.

Note that trade-off between privacy and utility exists in any privacy-preserving technique, including smart grid/metering [40]. Sankar et al. [40] presented a privacy-utility trade-off to quantify privacy and utility requirements of smart meter data. They tried to decouple the revealed meter data from the consumers' personal identifiable information as much as possible with their approach, which distorts the data to minimize the presence of intermittent activity in the data. The trade-off between privacy and utility is quantified based on the rate distortion theory. With an interference-aware reverse waterfilling solution, the privacy–utility tradeoffs on the total load can be achieved, considering the presence of high-power but less private appliance spectra as implicit noise, and filtering out lower-power appliances with a distortion threshold.

1.7.4.2 Privacy-Preserving Applications

Besides the above technical solutions with limited disclosure, cryptographic primitives have been widely utilized to build effective privacy-preserving protocols for many applications in smart grid [46, 71], where efficiency could be relatively ensured. In the following, we introduce some typical examples for this category of privacy-preserving applications in smart grid.

Lin and Fang [72] observed that the aggregated statistics of energy usage could bring intelligence to smart metering-assisted sustainable energy system (e.g. home electricity, water, gas, smart vehicles) and proposed two privacy-preserving schemes to securely collect aggregated statistics while preserving consumers' privacy. The proposed two privacy-preserving schemes are dynamic profiling applications based on the aggregated statistical information of the metering readings: (1) the scheme can extract aggregated statistical information. For example, the scheme enables an aggregator to extract the summation information from the submitted individual responses and can privately answer the statistical question like "What is the total energy consumption when the home temperature is 25 °C?" [72], and (2) extracting correlation information among various factors for the smart system design. For example, the scheme can efficiently answer the query as a conjunction "How many more percent of users consume how much energy on average when annual income is larger than $100K AND the room temperature is 25°C?". Such scheme can also be used as an underlying tool for baseline inference and association rule mining. The system also provides a mechanism to verify the correctness of users' responses which can be deduced from the metering information. The protocols are developed based on the secret key distribution protocol (Diffie–Hellman key-exchange-based protocol).

With the rapid development of smart grid services, vehicle to grid (V2G) becomes an essential component integrated in smart grid network, where the charging status of a battery vehicle should be periodically collected or continuously monitored to perform efficient power scheduling [73, 74]. A battery vehicle is normally associated with a default interest group which is a power grid operator or an organization. In the V2G networks, privacy concerns may arise while providing service in the smart grid system. Yang et al. [74] studied the potential privacy leakage of battery vehicle owners' identity and location and presented a privacy-preserving communication and precise reward architecture, which protects privacy in the process of battery vehicles' monitoring and rewarding. A secure communication architecture based on cryptographic primitives was given to accommodate mutual authentication, confidentiality, data integrity, and privacy protection/anonymity.

Also in the context of V2G network in smart grid, Liu et al. [73] studied the privacy-preserving authentication problem for V2G networks in the smart grid in which every aggregator charges battery vehicles with two modes: home mode and visiting mode. Specifically, battery vehicle may move around in different areas belonging to different groups and thus have requirements on security, privacy, and authentication. The proposed scheme effectively protects the individual privacy while periodically collecting power status data, which refers to a battery vehicle's energy-related status information (e.g. charging efficiency, and battery saturation status). The authors provided a sound security proof for the proposed scheme, including data confidentiality, integrity, availability, mutual authentication, forward/backward security, and privacy preservation.

Summary

In summary, privacy protection is increasingly integrated into the design and implementation of smart grid services, for preventing privacy breach at the individual smart grid component level (end-user, electricity distribution, electricity generation). For the above three components, Wolf [62] illustrated the technologies and applications with privacy issues, e.g. smart meters (remote connect/disconnect of meter, meter detects meter bypass, data collection, communication and storage, in-home appliances that communicate with the utility operator, in-home devices that communicate usage information to the customer, consumer access to energy-related information, and automated feeder equipment), fault detection, load management, and plug-in hybrid electric vehicles. The privacy issues in many of the above applications and technologies have been resolved. However, the privacy-preserving schemes are still worth exploring for the remaining problems by tackling the privacy challenges [2] in the future.

References

1. Li H, Gong S, Lai L, Han Z (2012) Efficient and secure wireless communications for advanced metering infrastructure in smart grids. IEEE Trans Smart Grid 3(3):1540–1551
2. McDaniel P, McLaughlin S (2009) Security and privacy challenges in the smart grid. IEEE Secur Priv 7(3):75–77
3. Bisoi S, Dash AK (2011) The role of utilities in securing a smart grid: electric light and power. Available via http://www.elp.com/articles/print/volume-89/issue-6/sections/the-role-of-utilities-in-securing-a-smart-grid.html. Accessed 6 Jul 2014
4. Wilshusen G (2012) CyberSecurity—challenges in securing the electricity grid. GAO-12926T—Testimony before the Committee on Energy and Natural Resources, US Senate, 17 July 2012
5. ENISA, Smart grid security—annex II. Security aspects of the smart grid. 2012-04-25. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf
6. Wang S, Cui L, Que J, Choi D, Jiang X, Cheng S, Xie L (2012) A randomized response model for privacy preserving smart metering. IEEE Trans Smart Grid 3(3):1317–1324
7. Pearson I (2011) Smart grid cyber security for Europe. Energy Policy 39:5211–5218
8. Naone E (2009) Meters for the smart grid: MIT Technology review. September/October 2009:110–111
9. NRG Expert (2011) Chapter 13—Security. Global smart grid report, pp 172–179
10. Steven J, Peterson G, Frinckle D (2010) Smart-grid security issues. IEEE Secur Priv 8(1):81–85
11. Shapiro J (2011) Cyber security and smart grid. In: Presentation at the clean air through energy efficiency (CAFEE) conference, Dallas, 8–11 Nov 2011
12. Aloul F, Al-Ali AR, Al-Dalky R, Al-Mardini M, El-Hajj W (2012) Smart grid security: threats, vulnerabilities, and solutions. Int J Smart Grid Clean Energy 1(1):1–6
13. Echelon (2012) Protect your grid: Echelon's answer for a safe, secure grid. White paper
14. Monticelli A (1999) State estimation in electric power systems: a generalized approach. Springer, Berlin

15. AlMajali A, Viswanathan A, Neuman C (2012) Analyzing resiliency of the smart grid communication architectures under cyber attack. In: Proceedings of the 5th workshop on cyber security experimentation and test, Bellevue, 6 Aug 2012
16. Kosut O, Jia L, Thomas RJ, Tong L (2011) Malicious data attacks on the smart grid. IEEE Trans Smart Grid 2(4):645–658
17. Zhang Z, Gong S, Dimitrovski A, Li H (2013) Time synchronization attack in smart grid: impact and analysis. IEEE Trans Smart Grid 4(1):87–98
18. Lu Z, Lu X, Wang W, Wang C (2010) Review and evaluation of security threats on the communication networks in the smart grid. In: Proceedings of military communications conference, San Jose, 31 Oct–3 Nov 2010
19. Lafferty S, Ghazi T (2011) The increasing importance of security for the smart grid. POWERGrid Int 16(4):60–63
20. Ernst & Young (2011) Attacking the smart grid. Insights on governance, risk and compliance, Dec 2011
21. Ai Ling AP, Masao M (2011) Smart grid information security (IS) functional requirement. Int J Emerg Sci 1(3):371–386
22. Mo Y, Hyun-Jin T, Brancik KK, Dickinson D, Lee H, Perric A, Sinopoli B (2011) Cyber-physical security of a smart grid infrastructure. Proc IEEE 100(1):195–209
23. Zhang Y, Wang L, Sun W, Green RC, Alam M (2011) Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Trans Smart Grid 2(4):796–808
24. Choi K, Chen X, Li S, Kim M, Chae K, Na J (2012) Intrusion detection of MSM based DoS attacks using data mining in smart grid. Energies 5:4091–4109
25. Chen P, Cheng S, Chen K (2012) Smart attacks in smart grid communication networks. IEEE Commun Mag 50(80):24–29
26. Hahn A, Govindarasu M (2011) Cyber attack exposure evaluation framework for the smart grid. IEEE Trans Smart Grid 2(4):835–843
27. Chen T, Sanchez-Aarnoutse JC, Buford J (2011) Petri net modeling of cyber-physical attacks on smart grid. IEEE Trans Smart Grid 2(4):741–749
28. Zonouz S, Rogers K, Berthier R, Bobba R, Sanders W, Overbye T (2012) SCPSE: security-oriented cyber-physical state estimation for power grid critical infrastructures. IEEE Trans Smart Grid 3(4):1790–1799
29. Bobba R, Rogers K, Wang Q, Khurana H, Nahrstedt K, Oberbye T (2010) Detecting false data injection attacks on DC state estimation. In: Proceedings of 1st workshop on secure control systems, Stockholm, Apr 2010
30. Ghansah I (2012) Smart grid cyber security potential threats, vulnerabilities and risks. Public interest energy research (PIER) program interim report, May 2012
31. Li H, Lai L, Zhang W (2011) Communication requirement for reliable and secure state estimation and control in smart grid. IEEE Trans Smart Grid 2(3):476–486
32. Liu Y, Ning P, Reiter M (2011) False data injection attacks against state estimation in electric power grids. ACM Trans Inf Syst Secur 14:13:1–13:33
33. Kim J, Tong L (2013) On topology attacks of a smart grid. IEEE J Sel Areas Commun 31 (7):1294–1305
34. Zonouz S, Khurana H, Sanders W, Yardley T (2009) RRE: a game-theoretic intrusion response and recovery engine. IEEE Trans Parallel Distrib Syst 25(2):395–406
35. Locasto M, Wang K, Keromytis A, Stolfo S (2005) FLIPS: Hybrid adaptive intrusion prevention. In: Proceedings symposium on recent advances in intrusion detection, Seattle, pp 82–101, 7–9 Sept 2005
36. Hug G, Giampapa JA (2012) Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans Smart Grid 3(3):1362, 1370
37. Shaw WT (2004) SCADA system vulnerabilities to cyber attack. Electric energy Online 8(6). Retrieved from http://www.electricenergyonline.com/show_article.php?mag=&article=181
38. Kim T (2011) Securing Communication of SCADA Components in Smart Grid Environment. Int J Syst Appl, Eng Dev 5 (2):135–142

39. Skopik F, Ma Z, Bleier T, Gruneis H (2012) A survey on threats and vulnerabilities in smart metering infrastructures. Int J Smart Grid Clean Energy 1(1):22–28
40. Sankar L, Rajagopalan SR, Mohajer S, Poor HV (2012) Smart meter privacy: a theoretical framework. IEEE Trans Smart Grid. doi:10.1109/TSG.2012.2211046
41. Rahman MA, Al-Shaer E, Bera P (2012) A noninvasive threat analyzer for advanced metering infrastructure in smart grid. IEEE Trans Smart Grid. doi:10.1109/TSG.2012.2228283
42. Xiao Z, Xiao Y, Du D (2012) Exploring malicious meter inspection in neighborhood area smart grids. IEEE Trans Smart Grid. doi:10.1109/TSG.2012.2229397
43. Gering K (2010) A meter perspective on cyber security: electronic perspectives. May/June 2010:102–105
44. Bell R (2010) In smart grid security, the details matter: power Grid Internation. Available via: http://www.elp.com/articles/powergrid_international/print/volume-15/issue-4/Features/in-smart-grid-security-the-details-matter.html. Accessed 6 Jul 2014
45. Falk R, Fries S (2011) Smart grid cyber security—an overview of selected scenarios and their security implications. PIK-Praxis der Informationsverarbeitung und Kommunikation 34 (4):168–175
46. Iyer S (2011) Cyber security for smart grid, cryptography, and privacy. Int J Digital Multimedia Broadcast 2011
47. Liu J, Xiao Y, Li S, Liang W, Chen C, Philip L Cyber security and privacy issues in smart grids. IEEE Commun Surv Tutor 14(4):981, 997 (Fourth Quarter)
48. Boyer WF, McBride SA (2009) Study of security attributes of smart grid systems–current cyber security issues. Idaho National Laboratory, USDOE, Under Contract DE-AC07-05ID14517
49. Baumeister T (2010) Literature review on smart grid cyber security. University of Hawaii at Manoa, technical report, 2010
50. Giani A, Bitar E, Garcia M, McQueen M, Khargonekar P, Poolla K (2013) Smart grid data integrity attacks. IEEE Trans Smart Grid 4(3):1244, 1253
51. Gorman S (2009) Electricity grid in U.S. penetrated by spies. Wall St J 8:A1
52. Baldor LC (2010) New threat: hackers look to take over power plants. Associated Press, New York
53. Abur A, Exposito AG (2004) Power system state estimation: theory and implementation. CRC Press, Boca Raton
54. Huang Y, Esmalifalak M, Nguyen H, Zheng R, Han Z, Li H, Song L (2013) Bad data injection in smart grid: attack and defense mechanisms. IEEE Commun Mag 51(1):27–33
55. Liu Y, Reiter MK, Ning P (2009) False data injection attacks against state estimation in electric power grids. In: ACM conference on computer and communications security, pp 21–32
56. Jeu-Min L, Heng-Yau P (2007) A static state estimation approach including bad data detection and identification in power systems. In: IEEE power engineering society general meeting, p 17, June 2007
57. Milli L, Cutsem TV, Pavella MR (1985) Bad data identification methods in power system state estimation, a comparative study. IEEE Trans Power Appar Syst 103(11):3037–3049
58. Rahman MA, Mohsenian-Rad H (2012) False data injection attacks with incomplete information against smart power grids. In: Global communications conference (GLOBECOM), 2012 IEEE, pp 3153–3158
59. Kosut O, Jia L, Thomas RJ, Tong L (2010) Malicious data attacks on smart grid state estimation: attack strategies and countermeasures. In: 1st IEEE international conference on smart grid communications (SmartGridComm), 2010, pp 220, 225, 4–6 Oct 2010
60. Kim TT, Poor HV (2011) Strategic protection against data injection attacks on power grids. IEEE Trans Smart Grid 2(2):326, 333
61. Mohsenian-Rad A-H, Leon-Garcia A (2011) Distributed internet-based load altering attacks against smart power grids. IEEE Trans Smart Grid 2(4):667, 674
62. Cavoukian A, Polonetsky J, Wolf C (2010) Smart privacy for the smart grid: embedding privacy into the design of electricity conservation. Identity Inf Soc 3(2):275–294
63. Rebecca H (2009) SmartGrid privacy concerns. NIST SmartGrid privacy group report, 2009

64. Murrill B, Liu E (2012) Thompson RII Smart meter data: privacy and cybersecurity. CRS Report for Congress, 7-5700, 3 Feb 2012
65. McNeil S (2011) Privacy and the Modern Grid. Harv J Law Technol 25(1)
66. Skopik F (2012) Security is not enough! on privacy challenges in smart grids. Int J Smart Grid Clean Energy 1(1):7–14
67. Efthymiou C, Kalogridis G (2010) Smart grid privacy via anonymization of smart metering data. In: 1st IEEE international conference on smart grid communications (SmartGridComm), pp 238–243. doi:10.1109/SMARTGRID.2010.5622050
68. Kalogridis G, Efthymiou C, Denic SZ, Lewis TA, Cepeda R (2010) Privacy for smart meters: towards undetectable appliance load signatures. In Proceedings of SmartGridComm 2010, pp 232–237
69. David P (2011) Varodayan and Ashish Khisti, "Smart meter privacy using a rechargeable battery: minimizing the rate of information leakage", In Proceedings of ICASSP 2011, pp 1932–1935
70. Kursawe K, Danezis G, Kohlweiss M (2011) Privacy-friendly aggregation for the smart-grid. In Proceedings of international conference on privacy enhancing technologies, pp 175–191
71. Go W, Kwak J (2012) Privacy-enhanced secure data transaction system for smart grid. Int J Secur Appl 6(3):37–44
72. Lin H, Fang Y (2013) Privacy-aware profiling and statistical data extraction for smart sustainable energy systems. IEEE Trans Smart Grid 4(1):332, 340
73. Liu H, Ning H, Zhang Y, Yang LT (2012) Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid. IEEE Trans Smart Grid 3(4):1722, 1733
74. Yang Z, Yu S, Lou W, Liu C (2011) Privacy-preserving communication and precise reward architecture for V2G networks in smart grid. IEEE Trans Smart Grid 2(4):697, 706