Vulnerabilities and Countermeasures – A Survey on the Cyber Security Issues in the Transmission Subsystem of a Smart Grid

Yi Deng and Sandeep Shukla

Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA 24060, USA; e-mail: {yideng56, shukla}@vt.edu

Abstract

With the increased investment and deployment of embedded computing and communication technologies in the power system – the smart grid vision is shaping up into a reality. The future power grid is a large cyber physical system (CPS) which is vulnerable to cyber security threats. Among the three major subsystems of a power grid – generation, transmission and distribution – this survey focuses on the transmission subsystem because most of the cyberization of the grid has been happening in this subsystem. This is due to the need for distributed measurement, monitoring and control to retain the stability, security, and reliability of power transmission system. Given the geographically dispersed generation facilities, substations, control centers, data concentrators etc., efficient data communication is required, and therefore large scale networking – either proprietary or leased – is happening. The goal of this paper is not to be comprehensive to include all efforts of securing the transmission system from cyber borne threats, but to provide a survey of various vulnerabilities, and countermeasures proposed by various research efforts. One of the focus area in this survey is the Phasor Measurement Units (PMUs) and Wide Area Measurement System (WAMS) technology – mostly due to our familiarity with the issues for this specific technology deployment – rather than any attempt to indicate that this is the most vulnerable technology in the transmission subsystem. Our hope is that this survey will familiarize any uninitiated reader with the issues and provide incentive to un-

Journal of Cyber Security and Mobility, Vol. 1, 251–276.

dertake systematic research programs to thwart cyber attacks on our national power delivery infrastructure.

Keywords: smart grid cyber security, cyber attacks, synchrophasor technology, phasor measurement unit (PMU), wide area measurement system (WAMS), power system monitoring, power system protection, power system control.

1 Introduction

The impact of the national power grid infrastructure is so deeply rooted in the modern society that we often forget about its importance as we do for the air we breathe. However, the present large and complex power system infrastructure is not built under any top-down planning but rather has evolved from the small system that was built in the late 19th Century. The entire system is continuously upgraded upon the development of advanced technologies through each decade [1]. With the advent of the information age in the late 1970s, people increasingly rely on all kinds of electrical equipments, and on ever-increasing demand for more energy, the power systems' capacity had to be revised dramatically over the years. During the recent three to four decades, the only effective way to achieve the goal of satisfying the growth on demand is either by increasing the power generation capacity, the number of power plants, the transmission line capacity or by limiting electricity usage. Apparently, these kinds of solutions are not satisfactory. To move forward, we need a new power system that is capable of allocating our current power resources intelligently and satisfying the growing complexity and demands of electricity in the 21st Century [2, 3].

The concept of a smart grid emerged around 2003 but currently the development and deployment of smart grid projects are in progress world-wide [4]. As shown in Figure 1, the smart grid still retains the legacy of traditional power grid infrastructure such as power generator (circle 1), transmission lines (circle 2), substations, distribution lines (circle 3), transformers, and user terminal equipments (circle 4). In addition, the system integrates renewable green energies, such as solar energy, wind energy, biofuel, wave energy, geothermal energy, and hydro energy to substitute the non-renewable resources. The ultimate purpose of smart grid is to bring economy, security, sustainability, and convenience to both utilities and customers.

Expected to be the next generation of power grid, the objectives of building a smart grid is to maintain an efficient, reliable and secure electricity

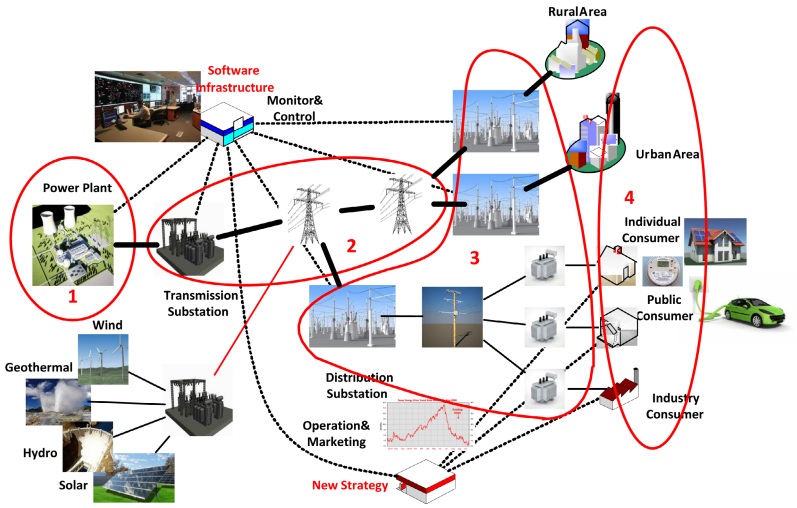

Figure 1 A hierarchical system infrastructure of the smart grid [5].

infrastructure to meet the increasing demand of electricity. The characteristics of a smart grid are defined as follows [6]:

- Utilizing digital, computational, communication and control technologies to create better monitoring, protection and control.
- Integrating the existing hardware and newly developed software to make the system optimal.
- Deployment and integration of distributed renewable resources to reduce the greenhouse gas emissions.
- Employing demand response strategy that makes the electric power dispatching more reasonable.
- Development and deployment of end-user intelligent devices e.g. smart meters to realize the interactive between utilities and consumer devices.
- Integration plug-in hybrid electric vehicles or pure electric vehicles to achieve electricity storage and peak shaving.

Traditionally, the power grid used limited one-way communication so the utility was inefficient to respond to an ever-changing electricity demands. The smart grid is using two-way interaction, where the system information exchanges timely between the power grid operators and the customers [7]. With the help of communication networks, a smart grid control center can monitor and control the real-time parameters of distributed power sources. If upgrading from Supervisory Control and Data Acquisition (SCADA) to

Wide Area Measurement System (WAMS), the smart grid control center is able to acquire the dynamic characteristics of transmission line parameters [8]. Consisting of smart meters, the Advanced Metering Infrastructure (AMI) engages the end users to the smart grid distribution mechanism [9].

However, when the smart grid gets great benefits from computational resources and communication networks, the system will face the risk of cyber attacks and challenges associated with the cyber infrastructure. As many popular website servers may be vulnerable to various types of cyber attacks (such as denial of service attacks), the system control center in a smart grid may become the main object of cyber attacks. Any adversary can attack the system control center by compromising certain numbers of remote sensors that are connected through the same network [10].

Among cyber security issues in the Internet space, one important property is – *information confidentiality*. All the safety measures should be taken to prevent the disclosure of information to unauthorized individuals or systems. Another important requirement – *data integrity* – makes sure that the transmitted data cannot be modified undetectably. A further requirement – *availability* of information ensures that the system must keep the information available when needed. However, in smart gird, the priority of Confidentiality, Integrity, and Availability (CIA) may be considered to be in the reverse order [11]. Among all the key features of a smart grid, the ability to provide a high quality, reliable and sustainable power is the fundamental requirement. The availability of power supply is the most critical quality metric when implementing a smart grid. In a smart grid, the definition of integrity means that the system control center can collect the measurement data accurately, timely, and effectively. Ideally, there should be no transmission error, no false data, and tampered data sent to a system control center. Lastly, the confidentiality in a smart grid determines the privacy issues caused by variety of intelligent devices installed in homes or in substations. The utilities are obliged to protect consumers' personal information, such as telephone numbers, social security numbers, etc., and even prevent from divulging users' personal habits.

At this point it is important to clarify that for the three major subsystems of a power system infrastructure – generation, transmission, and distribution – the cyber security challenges are different. A Generator can be attacked by a breach in the local control room, but can also be destabilized by other means germane to the transmission system vulnerabilities. A distribution substation can also be breached because modern substations are connected to a wide area network to communicate to the control center, and have internal local area

network for communication between intelligent electronic devices (IEDs). The Advanced Metering infrastructure (AMI) also communicates through wireless networks to the substations and control stations. The field technicians may also be equipped with network-enabled devices to communicate information on the location of equipments on a distribution network. Thus, various cyber threat models have been identified at the distribution level [12] – but this survey is not intended to cover the distribution system. Our focus is on the transmission system and its security in a smart grid.

A number of threat models have been identified for the transmission subsystem. The malicious data injection attack against the power system state estimation, is well studied in the literature [13]. In this attack, the adversary may execute a joint attack vector on partial meters so that all the bad data detection techniques we are using today will fail to detect the bad data. In [14], the authors defined a special linear injection attack model that mixed with meter measurements, and the bad data detector cannot perceive the false measurement data. By adjusting the attack model, the results of state estimation can be falsified to a certain extent. Meanwhile, there are other kinds of cyber attacks such as denials of service (DoS) attacks, traffic analysis attacks, high-level application attacks, etc., that may affect the security of the power system.

Synchronized phasor measurement technology provides the power system a more precise and real-time measurements for estimating the system state. Global Positioning System (GPS), with the capability of supplying high precision reference clock for other systems, synchronizes the wide area distributed Phasor Measurement Units (PMUs) measurement data. Having the GPS time reference, each PMU can measure the positive sequence phasors of voltages and currents accurately. Even more, PMUs provide the measurements of state vector directly, rather than estimating it from SCADA measurements. By using the PMUs in the smart grid, the operational process for a system control center will change. It increases the accuracy of state estimation and improves the observability of power network. Eventually it can prevent many common cyber attacks. In the next sections we will go into the details of some of these.

This paper is organized as follows. Section 2 discusses the existing cyber attacks against the operation of transmission subsystem of a smart grid. Section 3 introduces the principle of synchrophasor technology and the composition of wide area measurement system, and explores the phasor measurement applications in state estimation, power network observability, and cyber attacks prevention. Section 4 discusses the future directions of

using phasor measurement units in the smart grid security research. Section 5 provides concluding remarks.

2 Vulnerabilities in Smart Grid

Through the integration of advanced digital, computational and communication technologies, the centralized power system control center has more ways of managing the entire system. For example, the control center is capable of gathering information from wider geographical area, supporting greater data storage, calculating faster, and sending commands in real-time. Nevertheless, an indisputable fact is that whichever component is critical for system operation, it is weak and easy to become an attacking target. The two-way communication infrastructure provides the adversary with the possibility of attacks.

In the traditional power system, the attackers are difficult to compromise those measurement devices unless they implement a physical damage attack. However, in a smart grid system, the distributed and networked devices provide the interfaces for attacks to access. Wide area communication networks provide a possibility that the attackers can hack into the intra-network by breaking through the intermediate firewalls. Wireless communication networks between smart meters and meter data management center are direct exposure to the attackers. If the attackers can compromise a certain number of remote devices, they can even attack the system control center.

In literature, researchers have found some cyber attacks against power system. There are denial of service attack, malicious data injection attack, traffic analysis attack, and high-level applications attack.

2.1 Denial of Service Attack

The denial of service (DoS) attack is a common attack method in computer-based networks. The DoS attack attempts to prevent the provider from supplying resources and functions available to its users. In communication network areas, the main objects of DoS attack are popular website servers,data centers, wireless communication base stations, etc. The consequences of DoS attack include:

- The computational or communicational recourses of the attack objects are exhausted, and no additional performance to supply the normal services.

- The system configuration information such as package routing information are disrupted, and the information cannot reach to the destinations properly.
- The package state information is tampered, and the system executes a wrong operation.
- Physical damages are applied to the service provider and communication media, so that there are no connections available between the users and provider.

There are dozens of DoS attack methods found in cyber network. Among them, the flooding DoS attack is one of the most common type. The flooding DoS attack blocks the whole network channel by repeatedly sending high-priority data packets to the server, so that the server has no time to respond other requests, such as Internet control message protocol (ICMP) flood and synchronize message (SYN) flood. Furthermore, the properties of the communication infrastructure of a smart gird is real-time, and time-delay sensitive. For some applications, such as adaptive out-of-step,the requirements of end-to-end delays should be less than 50 ms [23]. Therefore, these kinds of applications are more vulnerable to DoS attack.

Take the application of backup relay protection scheme as an example. When a short circuit happens, the protective relays will trip the circuit breaker in order to prevent enlarge the impact. In the current power system, all the relays' trip decisions are determined by their local information separately. In the smart gird, the relays cannot make such hasty decision. A new protection strategy called agent-based backup relay protection scheme shown in Figure 2 improves the relay's reliability. For each relay R_i, it has three protection zones. For instance relay R_1 has zone1 (areas between R_1 and Bus_2), zone2 (areas between R_1 and R_2), and zone3 (areas between R_4 and R_5) respectively. If the errors happen between R_4 and R_5, the executive relays should be R_4 and R_5. In the new scheme, the measurement information from R_1 will also send to the executive relays for helping to reduce false trips by R_4 or R_5. In this case, the DoS attack will affect the agent-based protection scheme seriously. Once the system is paralyzed by a DoS attack, the agent network traffic will be saturated, and it cannot gather enough information from nearby relays. When the command message delay expires, the zone1 relays can only execute the default decisions which are not appropriate in some circumstances.

Defending methods against DoS attacks usually involves using firewalls to detect the attacks, or configuring routers to classify the network channels

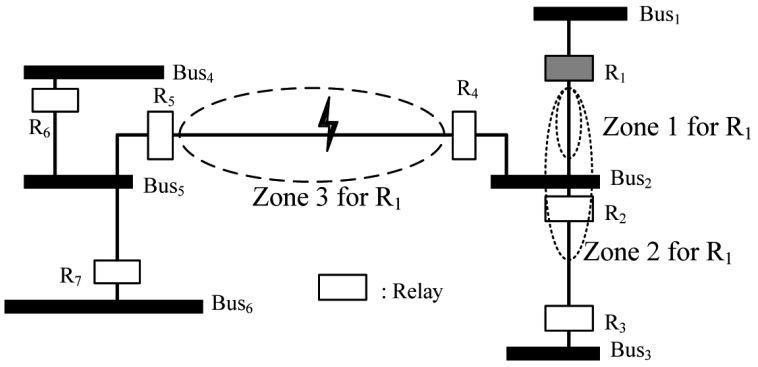

Figure 2 Agent-based supervision of backup relay protection architecture

and block the illegitimate traffic flows. The researchers in [24] did experiments to evaluate the impacts of DoS attack against the transmission delay of communication network in a smart gird.

2.2 Malicious Data Injection Attack

The problem of implementing a malicious data injection attack on power system state estimation was first proposed in [14]. By exploiting the configuration of a power system, an attacker could construct an algebraic attack vector mixed with the compromised meter measurements to introduce state estimation errors arbitrarily without been detected by current bad data detectors.

2.2.1 Power System State Estimation

For a power control center, it is important to monitor the state parameters of the system. The SCADA system in a power grid updates the measurements every 3 to 4 seconds, and yet the system states have actually changed during this period. Therefore, in most cases, the state estimator assumes that the system was in a 'static' state. It uses the active and reactive power flows, bus injections, and voltage magnitudes to calculate the state of a power system. When doing state estimation, the control center assumes that the bad data detector has screened out all the unexpected bad data. Hence the state variables are related to the measurements by the following nonlinear functions:

$$z = h(x) + e, \quad e \sim N(0, W) \tag{1}$$

where $z = (z_1, z_2, \ldots, z_m)^T \in R^m$ denotes the measurement vector acquired from m remote power meters. The z_i are bus voltages, bus real (active) and reactive power injections, and branch real (active) and reactive power flows. $x = (x_1, x_2, \ldots, x_n)^T \in R^n$ denotes the estimated n state vectors. The x_i are bus voltage phase angles and magnitudes. $e = (e_1, e_2, \ldots, e_m)^T$ denotes the measurement error vector introduced by m measurement instruments. The e_i is assumed to be an independent Gaussian distribution with zero mean and a diagonal covariance matrix W. $h(x)$ is a nonlinear function of the state vector x. This nonlinear function is determined by the system parameters and topology of power grid.

In this section, we mainly focus on the DC power flow model, so that the nonlinear state estimation Eq. (1) can be simplified by a linear model:

$$z = Hx + e \tag{2}$$

where $H = (h_{i,j})_{(m \times n)}$ denotes the measurement Jacobian matrix of size $m \times n$. The Weighted Least Square (WLS) method can solve this DC state estimation problem, which is defined as finding optimal estimate values of $\widehat{x}$ to minimize the target function:

$$J(x) = (z - H\widehat{x})^T W^{-1}(z - H\widehat{x}) \tag{3}$$

The estimated state vector $\widehat{x}$ is obtained by the matrix solution:

$$\widehat{x} = (H^T W^{-1} H)^{-1} H^T W^{-1} z = Mz \tag{4}$$

This state estimator is linear, so there will be no iterations. As soon as the measurements are transmitted to the estimator, the estimated state vector can be obtained by matrix multiplication. The Eq.(4) shows that the matrix M is a constant, as long as the system parameters and topologies do not change.

2.2.2 Bad Data Detection

When doing state estimation, the state estimator assumes that all the data candidates are accurate without bad data. Here, the bad data represents the measurements that have problems or errors coming from the measurement units or during the communication process. There are many possibilities to generate bad data. An uncalibrated measuring instrument may cause modest random errors, or a communication error might cause an immense error [15]. Based on the assumption that there is not much connection among these measurement data, that means the measurement data are mutually independent, it is possible to eliminate measurement errors by computing the measurement residuals, which are denoted by $z - H\widehat{x}$.

A common method [16] for detecting bad data is by checking the L_2-norm of measurement residuals:

$$\|z - H\widehat{x}\|_2 = \sqrt{\sum_{i=1}^{m} |z_i - H\widehat{x}_i|^2} \tag{5}$$

or the Largest Normalized Residual (LNR):

$$z_{(i)nor} = [z_i - H\widehat{x}_i]/\sigma_i \tag{6}$$

where σ_i is the measurement variances.

If the received measurements contain bad data, the $L_2 - norm$ or normalized residual of measurements will be abnormal, which is greater than a predefined threshold τ. As usual, the $L_2 - norm$ or normalized residual of measurement residuals follows a chi-squared distribution with $v = m - n$ degrees of freedom [17]. The threshold τ is determined by a hypothesis test with a significance level α. After eliminating the measurement with residuals above the threshold, the estimator will repeat the estimation process without the designated measurements. Then the estimator will do the detection process again, until no bad data was detected.

However, if there are interactions among bad data, the detection performance will dramatically decrease. The bad data can reinforce itself and make the detection procedure to eliminate good data [18].

2.2.3 Malicious Data Injection Attack

Malicious data injection attack was first proposed in [14]. It showed that by compromising enough power meters in a power system, the adversary can manipulate the meter measurements and change the state estimation values arbitrarily without being detected by bad data detection algorithms.

The basic idea of implementing malicious data injection attack is to inject an attack vector $a = (a_1, \ldots, a_m)^T$ into the original measurement vector $z = (z_1, \ldots, z_m)^T$. Let $z_a = z + a$ represents the real measurement data gathered from remote meters. If the state estimator uses the polluted data z_a as the input for state estimation, the estimated state vector should be denoted by $\widehat{x}_{bad}$, otherwise the normal measurement data z should be derived from the normal state vector $\widehat{x}$. The $\widehat{x}_{bad}$ can be represented as $\widehat{x}_{bad} = \widehat{x} + c$, where c denotes the estimation error vector introduced by the malicious data.

With the full knowledge of system parameters H, the adversary can carefully choose the attack vector a. Moreover, if the adversary formalizes the

attack model as $a = Hc$, the manipulated measurement data z_a can pass the bad data detection process. Take the L_2-norm detector as an example:

$$\begin{aligned} \|z_a - H\widehat{x}_{bad}\| &= \|z + a - H(\widehat{x} + c)\| \\ &= \|z - H\widehat{x} + (a - Hc)\| \\ &= \|z - H\widehat{x}\| \leq \tau \\ &\textit{when } a = Hc \end{aligned} \tag{7}$$

Based on this fact, other researchers did further studies on state estimation related attacks and defenses. In order to find out the minimum number of attackable power meters to make the entire system unobservable, Sandberg et al. [19] defined a security index to characterize the threshold between observable attack and unobservable attack. Regarding the cyber attack problems from the operator's perspective, Bobba et al. [20] found the minimum size set of measurements. If these set of measurements can be well protected, the entire system will prevent from unobservable attacks. In [13] two regimes of attack scenario are considered. One is called – *the strong attack regime* – where the adversary compromises a sufficient number of meters to make system unobservable to the system operator. The other is called – *the weak attack regime* – where the adversary can only control a small number of meters so that the system operator will enlarge its detection capability by using generalized likelihood ratio test (GLRT). On the other hand, the adversary have to trade-off between applying the maximum damages and increasing the probability of being detected by the system operator.In addition, to find the smallest subset of measurements that are well protected to attacks is a high-complexity combinatorial problem and NP-hard, Kim and Poor [21] tried to solve this problem by using a fast greedy algorithm. Giani et al. [22] showed that $p + 1$ secure measurements can neutralize p coordinated attacks.

2.3 Traffic Analysis Attack

In a smart gird system, the information transmitted over communication network should be encrypted. It is difficult for adversary to acquire the contents directly from the raw data. However, the traffic analysis attack is executed by monitoring and intercepting the frequency and timing of transmission messages to deduce the information of the victim networks. By implementation of traffic analysis attack, the adversary can gain the anonymity of some special data packages no matter the packages are encrypted or not. The underlying principle behind the traffic analysis attack is that the analyzed metadata con-

tain the information of sender, receiver, the time, and the length of messages [25]. When the attackers gain the basic network information, they can deduce information about passwords from the interactive between control center and users.

In the application of power system, many system parameters, such as bus voltages magnitude and phasors, active and reactive power are critical for system operation. The distributed monitors will send these system status messages periodically to the system control center. In most of the power systems, the SCADA information will mix with other management data flows into a shared network. By launching traffic analysis attack, the adversary may easily distinguish and isolate these information from other data flows. Then, the adversary may monitor and intercept these critical data, and infer the topology of power grid architecture. In combination with some basic knowledge, such as the serial and shunt admittance of transmission line, the attacker could infer the weakest areas or components in the system, and launch other special attacks to these fatal parts.

For preventing the traffic analysis attack that may analyze the timing and data volume information, a defense mechanism that is based on designing a concatenation of different packets, and implementing random packet drops was proposed [26].

2.4 High-level Application Attacks

The high-level application attacks aim to disrupt not only the basic functions of a power system, such as power flow measurement, state estimation, etc., but also the high-level applications that will execute in Energy Management System (EMS), such as power consumption auto-monitoring, economic dispatch, optimal power flow, adaptive protection, relay protection schemes, electricity real-time pricing, etc. For both consumers and utilities, the economy reason is an important intention of establishing a smart gird. If the smart gird electricity market is under attack, the impacts will destroy the faith of using smart gird.

Take the cyber attack on electricity pricing market as an example. The pricing mechanism in America's electricity market is Locational Marginal Price (LMP) that is usually determining the day-ahead price and the real-time price. In the day-ahead pricing market, the decision principle is matching the supplies and demands, and the LMP is calculated based on the Optimal Power Flow (OPF) results [27]. In the real-time pricing market, the LMP is calculated based on an ex-post formulation [28]. Usually, there are two

ways for the adversary to attack the electricity pricing. One direct method is to physically attack or manipulate the electric meter reading to change the quantity of electricity usage. Another indirect way is to compromise the meters in order to affect the LMP calculation. The later attack has broader and more serious consequences.

Researchers have investigated cyber attack issues on power system pricing market. In [29], the malicious data attacks to the real-time electricity market was studied. By attacking the state estimator that can determine the real-time prices, the adversary can influence the revenues of a real-time market. By analyzing an undetectable data injection attack that will manipulate the nodal price of ex-post real-time market, it is shown in [30] that the adversary could gain significant financial profit when the attack is conjunction with virtual biding. As the smart gird is a typical cyber physical system (CPS) with critical infrastructure. The high-level applications attack against any component or application in the system will cause unexpected physical damages.

3 Countermeasures in Start Grid

When facing large number of security issues in smart gird, one possible solution is to learn from the experiences of existing systems that have ever faced the cyber security problems, such as Internet security, IT network security, mobile communication network security, wireless communication security, etc. Most popular network protection technologies, such as firewalls, antivirus, cyber forensics, network identity and authentication, intrusion detection, situational awareness, virtual private network, etc. can be applied in smart gird security design. Moreover, another promising way is to introduce newly developed devices and applications, and construct well defined systems in smart gird to increase the reliability, accuracy, and security of power grid. PMU is such an innovated instrument dedicated for measuring the wide area synchronized phasor to tackle many challenge problems in power system. PMUs based WAMS is regarded as the next generation of wide area monitoring and control system established in smart gird.

3.1 Phasor Measurement Units (PMUs)

3.1.1 Synchrophasor Measurement Principles [15, 31]

In power system operation, the coordination of different parts of a power grid is critical. If one of the parts is seriously out of synch or a group of generators

going out of step with the rest of power system, the whole system will become unstable and even collapse. Therefore, the power engineers are always eager to monitor the phases of all the bus voltages and line currents in real-time.

In the past, the phasor measurement can only be applied independently. When measuring the phasor of input signal, the phasor measurement unit will sample the analog signal over a finite data window, which is usual one period of the fundamental frequency of the input signal. After digitization, the device applies the Discrete Fourier Transform (DFT) or Fast Fourier Transform (FFT) in practice to calculate the phasor. According to Nyquist criterion, which the sampling frequency should be greater than or equal to twice the maximum signal frequency, there is an antialiasing filter before the data acquisition. The function of antialiasing filter is used to limit the signal bandwidth less than half of sampling frequency.

Since there are N samples of input signal that are taken over one period of the power frequency denoted by $x_k\{k = 0, 1, \ldots, N-1\}$, the phasor representation is given by

$$X = \frac{\sqrt{2}}{N} \sum_{k=0}^{N-1} x_k \varepsilon^{-jk\frac{2\pi}{N}} \tag{8}$$

Usually, the SCADA system can accomplish the measurement of power flows, but the lack of wide area synchronization mechanism and high-speed communication network make the wide area synchrophasor observation impossible.

The successful use of GPS signal makes the possibility that distributed power system phasor information measures with the same reference time becomes true. As can be seen from Figure 3, the synchronized phasor measurement technology relies on the GPS time signal for supplying synchronous sampling time t' and sequential time stamps.

GPS receivers installed in PMUs provide a precise timing pulse, which keeps the accuracy better than 250 ns and allows the synchronization precisions of local sampling pulse better than one microsecond. Converting to the angle error in a 60 Hz power grid system, the measured phasor errors should be less than 0.02 degrees.

3.1.2 PMU Architecture

A brief block diagram of a generic PMU is shown in Figure 4. The analog inputs are voltages and currents obtained from the secondary windings of the current and voltage transformers. The antialiasing filters block is cooperate

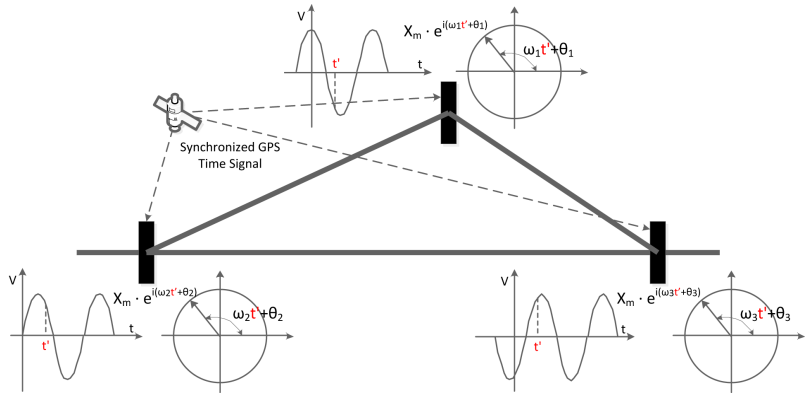

Figure 3 Wide area power parameters sampling with synchronized GPS time signal.

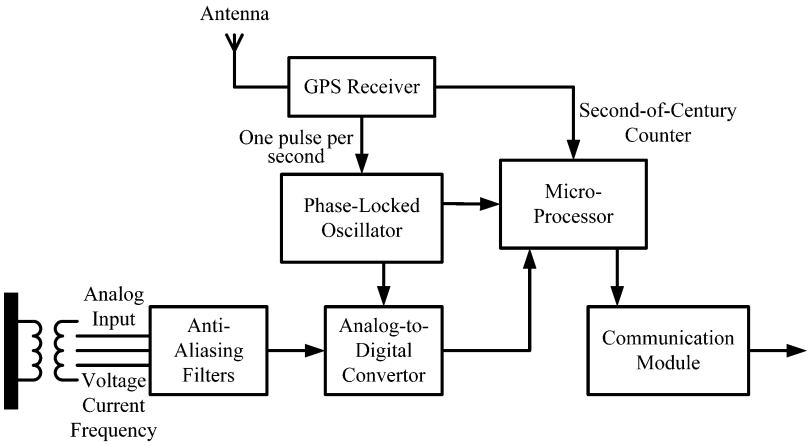

Figure 4 Phasor measurement unit block diagram.

with analog to digital converter (ADC) block to satisfy the Nyquist criterion. In practice, some types of PMUs implement the antialiasing function by using digital antialiasing filter. That means the ADCs first oversample the signal with high sampling frequency and then decimate the signal to a normal rate.

The sampling clock generated from the phase-locked oscillator can be stable. The phasor locked oscillator sync with one pulse per second signal extracted from GPS receiver. Within the modern PMUs, the sampling frequency is 96 or 128 samples per cycle. With the help of digital sampling technology and the higher demand of phasor measurement accuracy, the sampling frequency used in PMUs could be even higher.

After the voltage and current analog signals are digitized, the sampling data will be send to the centralized microprocessor to do the pre-processing. In some cases, the PMU has the ability to store the raw data from ADC to carry out digital fault recorder.

The microprocessor block will first calculate the positive-sequence estimates of all the current and voltage signals. Then assemble the original data with time-stamp. The time-stamp identifies the identity of the universal time coordinated (UTC) clock time, which is used by system control center for sequencing the distributed measurement data. The microprocessor can also process other information such as the local frequency and rate of change of frequency to help local decisions.

Finally, the communication network node is in charge of transfer the time-stamped measurement data compatible with defined IEEE standard for synchrophasors for power system [32].

3.2 Wide-Area Measurement System (WAMS)

The next generation of power system monitoring, protection and control system is wide area measurement system. WAMS is established based on PMUs and other latest communication technologies. Figure 5 shows general hardware architecture of WAMS. The WAMS is composed of five main components: substations with PMUs, substations with PDC, centralized SPDC, relay office, and high-performance regional or wide area networks [33].

Located at the lowest layer of the WAMS hierarchy, PMU installed substations consist of ordinary basic measuring devices including PMUs, digital relays, and intelligent electronic devices (IEDs). Since the volume of transmission data among all the connected equipment is modest, all these devices within substation are connected by the shared media access Ethernet.

In a PDC substation node, there usually is a PDC installed on the substation Ethernet. The first responsibility of a PDC is to gather all the PMU measurement data within the scope of its region. It may send the time-aligned data to the higher level PDC such as a Super PDC, over the network. It may also have the functionality to make certain regional control decisions.

The Super PDC node, which has the capability of storing, analyzing, and illustrating measurement data stays at the top level of the overall architecture. It may be housed in a data center, a phasor data processing center, or a system control center. Most of the monitoring functions, parts of the global protection schemes, and all of the controlling strategies are executed through SPDC.

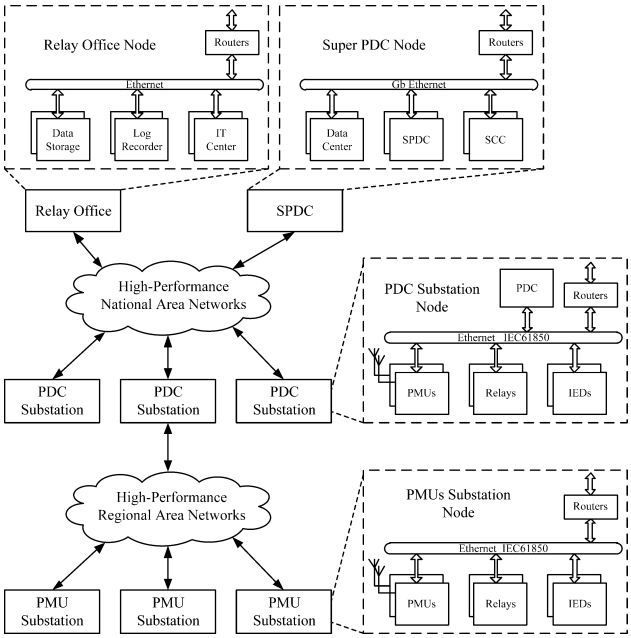

Figure 5 WAMS system architecture.

The communication infrastructure of WAMS can be classified into three types: intra substation local area networks (LAN), high-performance regional networks, and wide area fiber optic networks. The communication standard IEC 61850 defines the mapping of data models to a series of protocols such as manufacturing message specification (MMS), generic object oriented substation events (GOOSE), and sampled measured values (SMV). The high-performance regional networks interconnect several distributed PMUs and one PDC. The highest level of communication network is the most congested network. All the phasor information gathered by PMUs should upload to the centralized system-monitoring center.

3.3 State Estimation with Phasor Measurement

In theory, a PMU installed on one system bus can directly measure the bus voltage phasors and branch line current phasors incident to that bus as shown in Figure 6. Ideally, the wide area measurement system of smart gird is accomplished by deploying PMUs at all system buses. The measured state vector on each bus represents the state of power system at each given in-

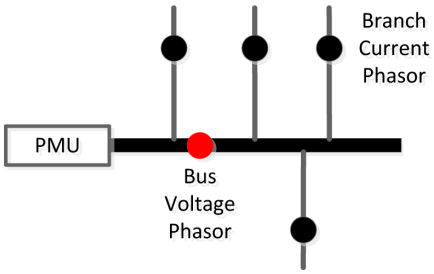

Figure 6 PMU measurements on system bus.

stant. Due to the high updating frequency of measurement data, the dynamic behavior of the power system can be observed directly [34].

The measurement vector consists of synchronized positive sequence voltage and current measurements with zero mean, normally distributed noise component.

$$z_p = \begin{bmatrix} V_p \\ I_p \end{bmatrix} + \begin{bmatrix} e_p \\ e_p \end{bmatrix} \tag{9}$$

The covariance matrix of measurement errors are denoted as W_p

$$W_p = \begin{bmatrix} W_V & 0 \\ 0 & I_p \end{bmatrix} \tag{10}$$

Consider the relationship between voltage measurements V_p and current measurements I_p, the state estimation solution could be solved using weighted least squares method:

$$G \cdot V_p = B^* \cdot W_p + z_p \tag{11}$$

where the G is the gain matrix that is a constant value as long as the system topology is constant. This all-PMU state estimation solution is direct and non-iterative.

In reality, the system does not install enough PMU, the synchrophasor need to mixed with traditional measurements $z_{mix} = [z, z_p]^T$. The hybrid measurement state estimator is presented in [35]. Nevertheless, due to the different nature of complex phasor measurements, the direct inclusion of phasor measurements in state estimators requires significant modifications to the existing EMS software. Zhou et al. [35] used a post-processing algorithm to achieve the estimated states from traditional estimator and then incorporate the phasor measurements.

By integrating phasor measurement data into the process of state estimation, the extra phasor measurement data can improve the network observability so that to prevent from the unobservable malicious data injection attack. Another benefit of using phasor measurement in state estimation is that it improves the bad data detection performance [36]. If the cyber attack is a weak regime attack, the performance of dad data detection scheme determines the attack detection probability. The performance of bad data detection is related to the measurement redundancy, by installing partial PMUs in critical system locations, the bad data detection and identification capability can be improved. So that by utilizing the PMUs especially the secured PMU measurement data can against the dedicated cyber attack on state estimation.

3.4 System Observability with Phasor Measurement

The system observability of a power system means that by installing a certain numbers of PMUs in the power system, all the bus states and branch states can be fully calculated. Baldwin et al. [37] used simulated annealing and graph theory to show that in order to keep the system completely observe, the system have to install PMUs in at least 1/5 to 1/4 of system buses. In an actual large system, the number of PMUs for maintaining the system complete observed is still large. Nuqui and Phadke [38] provided a PMU placement technology, which uses tree search algorithm to optimize the number of PMUs in Depth-of-n incomplete observability occasion.

Using PMU based measurement system provides the possibility of using limited number of secured PMUs to establish a complete observable power network or optimal placing the added PMUs into traditional power infrastructure to make the system from incomplete observability to complete observable.

4 PMU Based Security Issues

4.1 Dynamic State Estimator

Traditionally, the static state estimation is given based on an assumption that the whole system did not change its state during the data scanning interval. Therefore, the static state estimator uses the steady state system model and the SCADA measurements. However, the real practice is that the data scanning takes long enough that the system was actually different. Therefore, when using static state estimation, the system will lose power system details, and

have many blind spots when doing false detection. The adversary can attack the system during the scanning interval.

PMU measurements provide a possibility that the system control center is able to tracking the state of system continuously. So that the system control center can monitor and control the electric power system based on the real-time dynamic state. By analyzing the time correlation of measurement data, the dynamic state estimator improves the security performance of anomaly detection.

Dynamic state estimator combines the present or previous state of the power system along with the knowledge of the system's physical model, to predict the state vector for the next time instant [39].When the measurement data acquiring from next instant time arrives, the estimation of system state will be updated to more accurate values. The prediction provides advantages in system operation, power control, decision-making, and attack warning. It sets aside enough time for system control center to take reactions in emergency, and increases the safety sensitivity for any anomaly, such as data injection attack, etc.

The basic dynamic state estimation model is given by [15]:

$$x(k+1) = x(x) + (\Delta t)r \tag{12}$$

$$z(k) = Hx(k) + v(k) \tag{13}$$

where $x(k)$ is the state at the $k\ th$ time step; Δt is the time step; r is a maximum rate of change vector, $z(k)$ is the measurement; $v(k)$ is the measurement error. One of methods to solve this problem is using Kalman filtering with the assumption that Δt and $v(k)$ are modeled as zero mean, independent, Gaussian processes.

From another point of view, the dynamic state estimator essentially improves the system's timeframe resolution that prevents the adversary from manipulating the measurement vectors without be observed. There are few researchers exploit the dynamic model of the power network to improve the attack detectability. Pasqualetti et al. [40] showed that for the standard IEEE 14 bus system, it is known that an attack against the measurement data may be undetected by a static state estimator if the attacker compromises as few as four measurements. However, this kind of malicious data injection attack is always detectable by dynamic detection procedure that at least one phasor measurement is measured accurately.

4.2 PMU Data Authentication and Authorization

PMU data authentication and authorization are critical security services for a wide area measurement system, since it enables that the distributed PMUs transfer authenticated measurement data with system control center. Nowadays, the PMUs measurement data is transmitted over the public network, so it is easy for an adversary to manipulate the measurement data without device authentication. An authentication system is a system mechanism where the host service providers may identify their partners in a correct and secure way.

With the assumption that there is no physical layer authentication policy in the system, many cyber attacks that we mentioned above could be successful. If the adversary tampers the measurements with false data, the only method to detect the attack for a system control center is to utilize application layer detection scheme, such as bad data detection. Therefore, establish an authentication scheme is more efficient than post-detection scheme. There are some techniques that could be employed in the data authentication, such as secret password and cryptographic technology, symmetric key based scheme, tokens, etc.

Implementing authorization in PMUs based power system, the system control center prioritizes the distributed PMUs in different levels. The PMUs which are installed in critical places should have higher priority and security than others. They are authorized as first class measurement recourses. In such an authenticated and authorized system, the secured PMUs introduce redundant and trustworthy measurements for defending cyber attacks.

4.3 Spoofing GPS

As we can see from Figure 4 that the PMU GPS receiver provides the one pulse per second for synchronizing the sampling clock, and second of century counter for packaging actual time values into the sampling data. Only through analyzing the data bits of second of century (SOC) and fraction of second (FRACSEC) shown in Eq. (14) [32], the system control center can align all the distributed measurement data. Consequently, the precision of GPS clock time determines the accuracy of PMU measurement results.

$$Time = SOC + Fraction\ of\ Second/TIME\_BASE \tag{14}$$

It is difficult to acquire and track military GPS signal without encrypted military code (M code) [41], but for the civilian GPS signal, it is vulnerable by inducing a forged GPS signal [42]. For the PMU like civilian GPS receiver,

it is hard to detect a spoofing GPS signal because the attacker only needs to tamper the timing information slightly to affect the time accuracy.

The timing information from GPS signals is calculated from two parameters. One is the receiver clock time denoted by T_R that is demodulated from navigation messages with the precision of one second; the other is propagation time denoted by T_P that is acquired from the record of GPS signal propagation with the precision of a millisecond. So that the UTC can be calculated by

$$T_U TC = T_R - T_P - T_C \tag{15}$$

where T_C represents the corrections coming from the GPS receiver.

However, to get the receiver clock time from navigation message, the receiver should first acquire and track the GPS signal by using civilian Coarse Acquisition (C/A) code. To implement acquisition successfully, the receiver needs to search for the code phase of the received C/A code and the Doppler frequency shift [43]. In normal cases, the GPS receiver can acquire the signal by searching the highest correlation peak in the code phase-carrier frequency two-dimensional space [44]. For a GPS spoofer, its task is to mislead the GPS receiver into acquiring a fake signal. If the spoofer generates a new signal that has higher signal to noise ratio (SNR) with higher correlation peak, the GPS receiver will track the fake signal once it lose track caused by intentional signal interference. After that, the timing information calculated from the victim receiver has been manipulated by the spoofer.

Some researchers started to concern themselves with this problems. Gong et al. [44] carried out simulation experiments to assess the impact of time stamp attack to power system transmission line fault detection and location, voltage stability monitoring and location. Humphreys et al. [42] demonstrated a spoofing attack against a GPS time reference receiver installed in a PMU.

Another problem for using PMUs to realize the wide area synchronization is that the GPS signal receiver is the only source for supplying precise time. GPS signal may become unreliable due to weather changes, solar activities, intentional or unintentional jamming, or even worse that the Department of Defense (DoD) changes the GPS accuracy or turns off the civilian signal in some emergency cases. If that happens, the entire power grid system will be be paralyzed, and the security of power operation will be precarious. Therefore, alternative wide area synchronization mechanism should be in consideration.

5 Conclusion

The deployment process of smart gird will enter an explosive growth period during the next decade. From the experience of contemporary Internet, the cyber security issues should be a great deal of attention. In this paper, we introduced the system architecture and characteristics of smart gird. We also discussed the vulnerabilities in smart gird such as malicious data injection attack, denial of service attack, traffic analysis attack, and other high-level application attacks in detail. We introduced the basic concept of synchronized phasor measurement technology and its implementation, reviewed the recent research results that can be used to prevent cyber attacks. Finally, we pointed out the promising research areas based on PMU platform, and discussed potential security issues when establishing WAMS infrastructure. From our observation, we believe that the PMUs based WAMS system applications will play an leading role in the smart gird development, and PMUs based security applications development will become a focal point for smart gird security research.

References

[1] J.D. Glover, M.S. Sarma, and T.J. Overbye. Power System Analysis and Design, fourth edition. Cengage Learning, 2008.
[2] Department of Energy, Office of Electric Transmission and Distribution. “Grid 2030” A national vision of electricity’s second 100 years. Meeting Report, 2003.
[3] Department of Energy. The smart grid: An introduction. Report, 2009.
[4] International Energy Agency. Technology roadmap smart grids. Report for International Energy Agency’s Energy Technology Policy Division, 2011.
[5] G. Locke and P.D. Gallagher. NIST framework and roadmap for smart grid interoperability standards, Release 1.0. NIST Special Publication 1108, 2010.
[6] United States Congress (H.R. 6, 110th). Energy independence and security act of 2007. [Public Law No: 110-140] Title XIII, Sec. 1301.
[7] Department of Energy. Communication requirements of smart grid technologies. Report, 2010.
[8] A.G. Phadke. The wide world of wide-area measurement. IEEE Power & Energy Magazine, 2008.
[9] D.G. Hart. Using AMI to realize the smart grid. In Proceedings of IEEE Power and Energy Society General Meeting, pp. 1-2, 2008.
[10] S.M. Amin. Securing the electricity grid. The Bridge. Linking Engineering and Society, The Electricity Grid, 40(1):13–20, Spring 2010.
[11] P.D. Ray, R. Harnoor, and M. Hentea. Smart power gird security: A unified risk management approach. In Proceedings of 2010 IEEE International Carnahan Conference on Security Technology (ICCST), pp. 276–285, 2010.

[12] A.A. Cardenas, T. Roosta, and S. Sastry. Rethinking security properties, threat models and the design space in sensor networks: A case study in SCADA systems. Ad Hoc Networks, 7:1434–1447, 2009.
[13] O. Kosut, L. Jia, R.J. Thomas, and L. Tong. Malicious data attacks on the smart grid. IEEE Transactions on Smart Grid, 2(4):645–658, 2011.
[14] Y. Liu, P. Ning, and M.K. Reiter. False data injection attacks against state estimation in electric power grids. In Proceedings of ACM Conference on Computer and Communications Security, pp. 21–32, 2009.
[15] A.G. Phadke and J.S. Thorp. Synchronized Phasor Measurements and Their Applications. Springer, 2008.
[16] A. Monticelli. State Estimation in Electric Power System: A Generalized Approach. Kluwer Academic Publishers, 1999.
[17] A. Wood and B. Wollenberg. Power Generation, Operation, and Control, 2nd ed. John Wiley and Sons, 1996.
[18] A. Monticelli, F.F. Wu, and M. Yen. Multiple bad data identification for state estimation using combinatorial optimization. IEEE PAS-90, 1971.
[19] H. Sandberg, A. Teixeira, and K.H. Johansson. On security indices for state estimators in power networks. In Proceedings of 1st Workshop Secure Control Systems (CPSWEEK), Stockholm, Sweden, 2010.
[20] R.B. Bobba, K.M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T.J. Overbye. Detecting false data injection attacks on dc state estimation. In Proceedings of 1st Workshop Secure Control Systems (CPSWEEK), Stockholm, Sweden, 2010.
[21] T.T. Kim and H.V. Poor. Strategic protection against data injection attacks on power grids. IEEE Transactions on Smart Grid, 2(2):326–333, 2011.
[22] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla. Smart grid data integrity attacks: Characterizations and countermeasures. In Proceedings of 2011 IEEE International Conference on Smart Grid Communication (SmartGridComm), 2011.
[23] Y. Deng, H. Lin, A.G. Phadke, S. Shukla, and J.S. Thorp. Communication network modeling and simulation for wide area measurement applications. In Proceedings of 2012 IEEE PES Conference on Innovative Smart Grid Technologies (ISGT 2012), 2012.
[24] Z. Lu, X. Lu, W. Wang, and C. Wang. Review and evaluation of security threats on the communication networks in the smart grid. In Proceedings of the 2010 Military Communications Conference, 2010.
[25] G. Danezis and R. Clayton. Introducing traffic analysis. In Digital Privacy: Theory, Technologies, and Practices, Chapter 5. Auerbach Publications, 2008.
[26] B. Sikar and J.H. Chow. Defending synchrophasor data networks against traffic analysis attacks. IEEE Transactions on Smart Grid, 2(4):819–826, 2011.
[27] E. Litvinov, T. Zheng, G. Rosenwald, and P. Shamsollahi. Marginal loss modeling in LMP calculation. IEEE Transactions on Power Systems, 19(2):880–888, 2004.
[28] T. Zheng and E. Livino. Ex post pricing in the co-optimized energy and reserve market. IEEE Transaction on Power System, 21(4):1528–1538, 2006.
[29] L. Jia, R.J. Thomas, and L. Tong Malicious data attack on real-time electricity market. In Proceedings of 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 5952–5955, 2011.

[30] L. Xie, Y. Mo, and B. Sinopoli. Integrity data attacks in power market operations. IEEE Transactions on Smart Grid, 2(4):659–666, 2011.
[31] J. DeLaRee, V. Centeno, J.S. Thorp, and A.G. Phadke. Synchronized phasor measurement applications in power systems. IEEE Transactions on Smart Grid, 1(1):20–27, 2010.
[32] IEEE Power Engineering Society. IEEE standard for synchrophasors for power systems, IEEE Std C37.118TM-2005. 2006.
[33] Y. Deng, H. Lin, A.G. Phadke, S. Shukla, and J.S. Thorp. Networking technologies for wide-area measurement applications. In Smart Grid Communications and Networking, 2012 (to be published).
[34] A.G. Phadke, J.S. Thorp, R.F. Nuqui, and M. Zhou. Recent developments in state estimation with phasor measurements In Proceedings of Power Systems Conference and Exposition, PSCE '09. IEEE/PES, 2009.
[35] M. Zhou, V.A. Centeno, J.S. Thorp, and A.G. Phadke. An alternative for including phasor measurements in state estimators. IEEE Transactions on Power Systems, 21, 2006.
[36] J. Chen and A. Abur. Improved bad data processing via strategic placement of PMUs. In Proceedings of IEEE Power Engineering Society General Meeting, 2005.
[37] T.L. Baldwin, L. Mili, M.B. Boisen, and R. Adapa. Power system observability with minimal phasor measurement placement. IEEE Transactions on Power Systems, 8(2), 1993.
[38] R.F. Nuqui and A.G. Phadke. Phasor measurement unit placement techniques for complete and incomplete observability. IEEE Transactions on Power Delivery, 20(4):2381–2388, 2005.
[39] A. Jain and N.R. Shivakumar. Phasor measurements in dynamic state estimation of power systems. Proceedings of TENCON 2008 IEEE Region 10 Conference, pp. 1–6, 2008.
[40] F. Pasqualetti, F. Dorfler, and F. Bullo. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In Proceedings of IEEE Conference on Decision and Control, Orlando, 2011.
[41] B.C. Barker, J.W. Betz, J.E. Clark, J.T. Correia, J.T. Gillis, S. Lazar, K.A. Rehborn, and J.R. Straton. Overview of the GPS M code signal. In Proceedings of the 2000 National Technical Meeting of The Institute of Navigation, Anaheim, CA, 2000.
[42] T.E. Humphreys, B.M. Ledvina, M.L. Psiaki, B. W. O'Hanlon, and P.M. Kintner, Jr. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In Proceedings of ION GNSS 2008, 2008.
[43] K. Borre, D.M. Akos, N. Bertelsen, P. Rinder, and S.H. Jensen. A Software-Defined GPS and Galileo Receiver. Birkhauser, Boston, 2007.
[44] S. Gong, Z. Zhang, H. Li, and A.D. Dimitrovski. Time stamp attack in smart grid: Physical mechanism and damage analysis. In CoRR, 2012.

Biography

Yi Deng (M'12) received the B.Eng. and Ph.D. degrees in electrical engineering from Beijing Institute of Technology, Beijing, China, in 2005 and 2010 respectively. He is currently a postdoctoral associate with the

Department of Electrical and Computer Engineering at Virginia Polytechnic and State University in Blacksburg (Virginia Tech). His research interests include synchrophasor measurement technology, power system monitoring protection and control, communication in smart gird, and smart gird cyber security. Dr. Deng's research also covers signal processing, high-performance embedded computing (HPEC), hardware software co-design.

Sandeep K. Shukla (M'99, SM'02) received the bachelor's degree in 1991 from Jadavpur University, Calcutta, and the master's and PhD degrees in computer science in 1995 and 1997, respectively, from the State University of New York at Albany. He is an associate professor of computer engineering at Virginia Polytechnic and State University in Blacksburg (Virginia Tech), where he has been a faculty member since 2002. He is also a founder and director of the Center for Embedded Systems for Critical Applications (CESCA) and director of the FERMAT research lab. He has published more than 150 articles in journals, books, and conference proceedings, and has published eight books. He was awarded the PECASE (Presidential Early Career Award for Scientists and Engineers) award for his research in design automation for embedded systems design, which in particular focuses on system level design languages, formal methods, formal specification languages, probabilistic modeling and model checking, dynamic power management, application of stochastic models and model analysis tools for fault-tolerant nano-scale system design, reliability measurement of fault-tolerant nano-systems, and embedded software engineering. Professor Shukla was elected a College of Engineering Faculty fellow at Virginia Tech in 2004. He is a distinguished visitor of the IEEE Computer Society, a distinguished speaker of the ACM, and a senior member of the IEEE and ACM. He worked at GTE labs and Intel Corporation between 1997 and 2001. He was a researcher at the Center for Embedded Computer Systems at the University of California at Irvine. In 2007, Professor Shukla received a Distinguished Alumni award from the State University of New York at Albany for Excellence in Science and Technology. In 2008, he received the Friedrich Wilhelm Bessel Research Award from the Humboldt Foundation in Germany.