J. Mod. Power Syst. Clean Energy (2019) 7(3):449–467
https://doi.org/10.1007/s40565-018-0473-6

# Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies

**Aditya SUNDARARAJAN[1], Tanwir KHAN[1], Amir MOGHADASI[1], Arif I. SARWAT[1]**

**Abstract** Synchrophasor devices guarantee situation awareness for real-time monitoring and operational visibility of smart grid. With their widespread implementation, significant challenges have emerged, especially in communication, data quality and cybersecurity. The existing literature treats these challenges as separate problems, when in reality, they have a complex interplay. This paper conducts a comprehensive review of quality and cybersecurity challenges for synchrophasors, and identifies the interdependencies between them. It also summarizes different methods used to evaluate the dependency and surveys how quality checking methods can be used to detect potential cyberattacks. This paper serves as a starting point for researchers entering the fields of synchrophasor data analytics and security.

**Keywords** Synchrophasors, Data quality, Cybersecurity, Methodologies

CrossCheck date: 24 August 2018

Received: 11 November 2017 / Accepted: 24 August 2018 / Published online: 31 December 2018


✉ Arif I. SARWAT
asarwat@fiu.edu

Aditya SUNDARARAJAN
asund005@fiu.edu

Tanwir KHAN
tkhan016@fiu.edu

Amir MOGHADASI
amogh004@fiu.edu

[1] Florida International University, 10555 W Flagler St., Miami, FL 33174, USA

## 1 Introduction

Smart grid has complex dependencies between physical and cyber realms [1–4]. This has been demonstrated by recent attacks on smart grid which is summarized in Table 1 [5–10]. These attacks exploited a limited visibility of the system and inadequate support from reliability coordinators [11–22]. Wide-area measurement systems (WAMS) increase the situation awareness (SA) for operators [23–25]. WAMS devices that are part of the wide area monitoring, protection, automation and control include phasor measurement units (PMUs) at transmission, frequency disturbance recorders (FDRs) at low-voltage distribution and micro-PMUs ($\mu$−PMUs) for distributed renewables, called synchrophasors [26–35].

Significant challenges to the implementation of synchrophasors have emerged in communication, data quality and cybersecurity. The existing communication infrastructure is slow, expensive and inflexible. To leverage SA and support timeliness, adequate quality checking methods must be in-place at the phasor data concentrators (PDCs) which aggregate and process raw data and flag corrupt data. Due to their ubiquity, synchrophasors have an increased attack surface. The applications and challenges of synchrophasors are wellresearched [36–41]. However, the challenges of data quality and cybersecurity are considered one independent of the other, when in reality, they are interdependent [42–69]. Further, the literature does not leverage the knowledge of one challenge to address the other. For example, studying the changes to data quality can be key to potentially identify an underlying attack vector or an unexploited vulnerability.

The main contributions of this paper are: ① maps the dependencies between data quality and cybersecurity challenges of synchrophasors; ② reviews the methods to evaluate

**Table 1** Summary of the recent cyberattacks on smart grid impacting data quality

| Source of attack (Year) | Target of attack | Data quality characteristic impacted | Cybersecurity characteristic impacted | Attack specifics |
|---|---|---|---|---|
| Vulnerability in network firewall (2001) | California ISO (CAISO) web servers | Consistency, accuracy | Integrity | Poor security configuration during planned maintenance |
| Stuxnet worm (2010) | Programmable logic controllers (PLCs) at SCADA | Accuracy, consistency, plausibility | Integrity, availability | Exploits zero-day vulnerabilities of PLCs |
| BlackEnergy (2011) | Human-machine interface of utility grid control systems | Plausibility, origin, accuracy, consistency | Confidentiality, integrity, availability | General electric's human machine interface (HMI) targeted |
| Remote access Trojan; watering-hole attack (2014) | Industrial control system (ICS)/SCADA | Plausibility, origin, accuracy, consistency | Confidentiality, integrity, availability | Conducted by dragonfly, energetic bear |
| Trojan.Laziok reconnaissance malware (2015) | Energy companies | Origin, plausibility | Confidentiality | Gathered information from compromised devices |
| BlackEnergy3 (2015) | Ukrainian grid control center | Plausibility, origin, accuracy, consistency | Confidentiality, integrity, availability | Lack of SA left 220000+ customers without power |
| WannaCry ransomware cryptoworm (2017) | Computers running microsoft Windows operating system | Availability, origin | Availability | Used EternalBlue, a vulnerability in older Windows systems |

the challenges; and ③ surveys how data quality checking methods can leverage their observations to detect issues related to security. The paper also provides a high-level overview of synchrophasors, their standards, key applications, and challenges [70–73]. It is key to know that poor quality can be due to device errors or communication challenges like congestion and packet collision. Similarly, all cyber-attacks do not impact the data, although reduction in quality is one of the biggest observable consequences of a successful attack. A layout of WAMS comprising synchrophasors is shown in Fig. 1. This paper explores the challenges for PMUs at transmission and FDRs at distribution level.

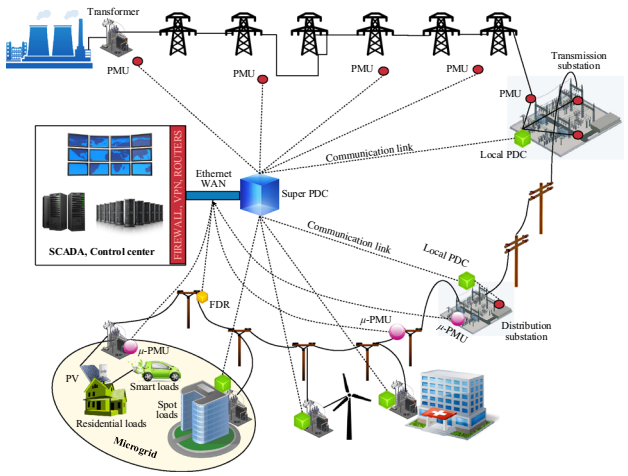


**Fig. 1** Layout of smart grid WAMS comprising PMUs, $\mu$-PMUs, FDRs and PDCs

This survey paper considers data quality and cybersecurity as *challenges*, where each has different *issues*. Issues are the ways in which the particular challenge manifests when observed. Figure 2 maps the challenges to their corresponding issues. The challenge of quality manifests in three ways: noise, outliers and missingness. Noise can be due to logical inconsistencies in data values or attributes while outliers result from poor integrity and origination. Missing data is a direct consequence of poor completeness and availability. Accuracy is impacted by noise, outliers as well as missingness while plausibility is a characteristic impacted by noise and outliers. These characteristics are discussed in Section 3.1. Cybersecurity manifests as delay/

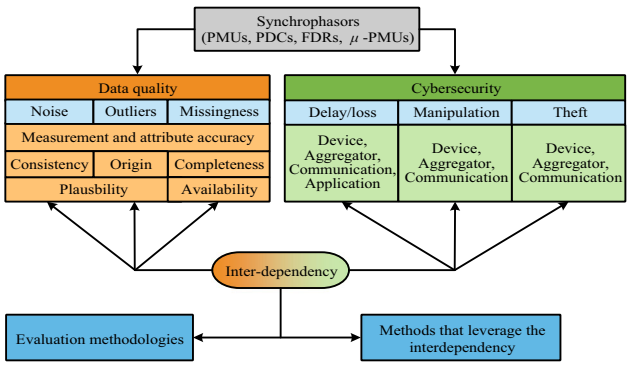


**Fig. 2** Proposed structure

loss, manipulation or theft. While a delay/loss corresponds to a packet delay or drop due to congestion, timeout, buffer fullness or an intentional attack that affects availability, manipulation deals with attacks that alter the information, thereby impacting integrity. Theft captures attacks which compromise the confidentiality of data such as snooping, spoofing or espionage. These attacks occur at different levels of the synchrophasor hierarchy: *Device* corresponds to the edge devices like PMUs, FDRs, or $\mu-$PMUs, while *Aggregator* implies Local PDCs or SuperPDCs. *Communication* refers to the synchrophasor network while *Application* contains the different power system applications that use synchrophasor data.

The rest of the paper is organized as follows. Section 2 summarizes the architecture, major applications and key challenges of synchrophasors. The characteristics are described in Section 3, and their interdependencies mapped in Section 4. While evaluation methods for data quality and cybersecurity are discussed in Section 4.1, Section 4.2 surveys methods which use data quality characteristics to detect potential cyber-attacks. Section 5 highlights future directions of research in synchrophasor data analytics and cybersecurity.

## 2 Architecture, applications, challenges

Synchrophasors can be standalone devices with dedicated purposes, or be a part of a larger system like the substations, depending on various functional and operational requirements. With increased penetration of renewables and smart loads, synchrophasors are used at distribution transformers and points of common coupling to study frequency disturbances and harmonics. The architecture of synchrophasor devices are summarized at the device and network levels below.

1) PMU device: It comprises current transformers (CTs) and potential transformers (PTs) that measure current and voltage magnitudes which are then converted to digital data, a microprocessor module that compiles these values, computes phasors, and synchronizes them with the coordinated universal time (UTC) standard reference used by global positioning system (GPS) receivers that acquire a time-lag based on the atomic clock of GPS satellites [23, 74–77]. They measure local frequency and its rate of change, and can record individual phase voltage and current along with harmonics, negative and zero sequence values [78]. The information paints a dynamic picture of the grid at a given time. PMUs and PDCs transmit measured data as frames [79]. A 16-bit cyclic redundancy check ensures data integrity. PDCs equipped with logging functionality use comma separated values or transient data exchange for data logs, and common format for event data exchange for event logs [80, 81]. The data transfer rate of PMUs, which determine the message processing delays and network latencies, depend greatly on the timing requirements of applications.
2) PMU network: If there are multiple PMUs in a substation, Local PDCs aggregate site-level data and then transmit to a SuperPDC. PDCs conduct various data quality checks and set flags according to the issues encountered, log performance, validate, transform, scale and normalize data, and convert between protocols [82]. There is typically a direct interface between PDC and the utility's SCADA or energy management system. PDCs can be deployed as standalone devices or integrated with other systems in the grid.
3) FDR device: The Oak Ridge National Laboratory and the University of Tennessee Knoxville have been leading the FNET/GridEye project since 2004. FDRs have been installed and managed to capture dynamic behaviors of the grid. Although FDRs are essentially PMUs, they are connected at 120 V, and hence incur lower installation costs than traditional PMUs do [83]. FDRs are largely deployed at renewable integration zones of the grid, and measure nearly 1440 samples per second with a hardware accuracy of $\pm 0.5$ mHz while PMUs measure between 10 and 240 samples per second and use GPS receivers that have 1μs accuracy for synchronization [84–87]. Given the availability of an extensive discussion of the architecture by the author of [88, 89], it is beyond the scope of this paper.
4) FDR network: FDRs use the internet to send data directly to the central servers for analytics and can provide information on transients, load shedding, breaker reclosing and the switching operations of capacitor banks and load tap changers [87]. Unlike PMUs, FDRs can be installed at buildings and offices.
5) Synchrophasor standards: Multiple standards exist for PMU data measurement, transfer and communication, proposed by IEEE, the National Institute of Standards & Technology (NIST), the North American Electric Reliability Commission (NERC) and the International Electrotechnical Commission (IEC) [90–97]. Due to multiple specifications and guidelines, there are possible contradictions in recommendations [70–73, 98]. A North American SynchroPhasor Initiative (NASPI) report in early 2016 identified the need for standardizing definitions related to synchrophasor data quality and availability by establishing the PMU applications requirements task force (PARTF) [99]. IEEE standard C37.X deals with WAMS, specifically PMUs [82, 100, 101]. These standards are summarized in Table 2 with their core contributions highlighted. A

**Table 2** Various standards and guidelines for synchrophasors

| Body | Standard | Core contribution |
|---|---|---|
| IEEE | 1344-1995 | Original parameter definitions for synchrophasors |
| | C37.118-2005 | Improved message formats, inclusion of time quality, total vector error (TVE) |
| | C37.239-2010 | PMU/PDC event logging |
| | 1711-2010 | Serial SCADA protection protocol for substation serial link cybersecurity |
| | C37.118.1-2011 | PMU measurement provisions, performance requirements |
| | C37.118.2-2011 | Synchrophasor data transfer requirements |
| | C37.238-2011 | Common profile for applying precision time protocol (PTP) using Ethernet |
| | C37.242-2013 | Synchronization, calibration, testing and installation of PMUs for PC |
| | C37.244-2013 | PDC functions and requirements for PC and monitoring |
| | C37.111-2013 | PMU/PDC data logging using COMFEDE |
| | 1686-2013 | Procuring, installing and commissioning IED cybersecurity |
| | C37.240-2014 | Sound engineering practices for high cybersecurity of substation APC |
| IEC | 61850 | Interoperable and adaptable architectures to substation automation |
| | 61850-90-5 | Requirements for data exchange between PMUs, PDCs, PCs and control center |
| | 62351-1,2 | Security threats and vulnerabilities in smart grid devices |
| | 62351-6 | Prescribes digital signature using asymmetric cryptography for sending PMU data |
| NERC | CIP 002-009 | Series of standards to ensure enterprise, field and personnel security |
| NIST | NISTIR 7628 | Provides guidelines for smart grid cybersecurity (including WAMS) |

more comprehensive review of the synchrophasor standards is documented in [102].

6) Applications: Synchrophasors streamline security, reliability and stability of power systems. They have online and offline applications [103]. Online applications of PMUs include enhancing real-time SA, analyzing faults and disturbances, detecting and appraising oscillations and harmonics that impact power quality, and improving accuracy and reducing computational time of state estimation. Offline applications include congestion management, providing effective protection schemes, benchmarking, system restoration, overload monitoring and dynamic rating, validating the network model of SCADA, and improving overall power quality [25, 104, 105]. Real-time (online) applications of FDRs include frequency monitoring interface integrated with command and control centers in the future for power system health diagnosis to prevent cascading failures, and event trigger module that detects and notifies the mismatch between generation and load caused by frequency variations. Offline applications include event visualization that renders the data read from the even data files [106].
7) Challenges: One of the major drawbacks of synchrophasors is the lack of transmission protocol, which makes them vulnerable to spoofing attacks [26]. The existing architecture is not scalable since it entails an initially high investment. NASPI's research initiative task force (RITT) emphasizes optimal placement as a significant challenge but also one dependent on the nature of applications the utility intends to use them for [18]. The literature has multiple models including but not limited to genetic algorithm, simulated annealing, Tabu search, Madtharads method, particle swarm optimization, artificial neural networks, binary search and binary integer programming to address this challenge [27, 28, 31–34, 107, 108]. More recently, managing and analyzing large volumes of synchrophasor data has become increasingly challenging. Lack of standardized data management solutions for smart grid has only made this problem more challenging. The ubiquitous presence of these devices has expanded their attack surface, making them vulnerable to different types of attacks. These two challenges are elaborated in the following section since they percolate to applications that directly operate upon the streaming data subject to minimal processing owing to timeliness requirements.

## 3 Data quality and cybersecurity challenges in synchrophasors

Due to their wide-ranging communication and automation capabilities, the challenges of synchrophasor data quality and cybersecurity have gained prominence.

### 3.1 Data quality challenges

NERC's real-time tools best practices task force (RTBPTF) and NASPI's PARTF impose requirements to ensure synchrophasor data quality [42, 109]. Data quality can be contextualized in different ways, depending on the needs of the concerned domain. For instance, data quality requirements of a smart meter recording energy consumption might differ from those of a net meter at a solar photovoltaic (PV) power plant. NASPI contextualizes synchrophasor data quality to determine "fitness of use" in terms of accuracy and lineage for static data points; lineage, completeness and logical consistency for static datasets; and availability, timeliness and origination for streams of data points [42].

There could be different causes for poor data quality as follow.

1) Device: poor calibration of device, biases due to CT, PT; erroneous filter design, poor synchronization of timing measurements, and issues due to measurement channel;
2) Communication: latency exceeding stipulated limits, network congestion, signal interferences and failure of communication nodes;
3) Aggregator: data transformation resulting in errors, delayed arrival of packets dropped due to time-limit exceeding, and unwanted duplication or corruption of data during computations;
4) Application: storage and maintenance issues, insufficient training size, erroneous manipulations to the data and poor association of context.

Although data quality requirements vary with applications, they have been extensively documented [42, 52, 102, 109]. The existing literature on synchrophasor data quality is summarized in Table 3.

1) Completeness: focuses on the gaps between different values, accounts for missing values [42]. The attributes of completeness defined at device and aggregator-levels are: *gap rate*—number of gaps in data per unit time; *mean gap size*—mean of the length of known gaps; and *largest known gap*—length of the largest known gap among the different gaps. While completeness is impacted by device malfunction, packet drops and communication link failure, the literature does not recognize the possibility of an attack behind such causes.
2) Accuracy: can be of the value or attribute, primarily measured in total vector error (TVE), which according to IEEE standard C37.118, is the vector difference between the measured and expected phasor value (magnitude, angle and frequency). Accuracy is categorized into that of: *data values*—impacted by factors like the difference between expected and observed signals or the introduction of noise to the data within the synchrophasor; and *data attributes*—affected by factors like accuracy of the measured timestamp, agreement between encoded and actual location coordinates of the device, and alignment of the location recorded in the power system topology with its actual location [46].
3) Plausibility and Availability: Measurement specifiers are the attributes of data which describe whether the process of measuring some phenomenon of the power system (observed value) and calculating its value (expected value) are documented effectively in terms of standard units to a given precision and are within a stated confidence interval [46, 48]. These specifiers have decisive sub-attributes influencing the qualitative value of data: data representing the measurement of quality or condition of the grid, and data represented in the form of SI units up to 3 decimal places with a confidence interval included.

   Network availability plays an important role in streaming data [49], and in-turn affects data availability. In case of high network latency, the incoming data streams from different synchrophasors get delayed or lost, causing applications to perceive them as missing or incomplete. Hence, network availability can be considered an indirect attribute affecting quality. This can be mitigated if the overlying applications are programmed to account for the delays, or if a more lenient waiting time limit is set. However, the second solution is dependent on the kind of applications the synchrophasors cater to. The latency requirements for synchrophasors recommended by the standards are very stringent.
4) Origination: is the source from which the data is measured. Its trustworthiness is associated with the background and source. Its attributes are as follow. ① *Point of origin*: the class of device from where the data originated (measurement (M) or performance (P) for PMUs), the standard followed by the device, and any data manipulation or standardization techniques through which the data passes [42, 118]; ② *Coverage*: physical location of the device based on its geospatial or electrical topology location [44, 45]; ③ *Transformation* applied to the data at the device, aggregator or application level.
5) Consistency: determines how agreeable the data is with the overall structure of its type. Incompatibility of attributes in terms of measurement rates or header labeling between datasets results in outliers, leading to an inconsistent result from an application. The attributes of consistency are as follow. ① *Header frame consistency*: consistency of the header frame of

**Table 3** Summary of existing research in synchrophasor data quality challenges and solutions

| Attribute | Challenges | Solutions |
|---|---|---|
| Completeness (Device, Aggregator) [42, 50, 110] | PMU/PDC device damage<br>Faulty PMU-PDC communication<br>Network error<br>Database storage error<br>Data missing for failing to comply with latency and QoS requirements | Acquiring better management techniques<br>Use of TCP protocol to re-transmit the lost data packets at the cost of timeliness<br>Adjusting the synchrophasor frame rate by increasing the wait time at PDC |
| Measurement accuracy (Device) [42, 43, 110–113] | Expected signal differs from measured signal due to harmonic interference<br>Introduction of noise to data | Improving phase error using filtering techniques<br>NIST calibration per Standard C37.118-2005<br>Omnidirectional antennas<br>Context-based reconstruction of missing data<br>Network time protocol (NTP), e-Loran and<br>chip scale atomic clock (CSAC) |
| Attribute accuracy (Device, Aggregator, Communication) [42, 44] | Measured vs actual timestamp discrepancy due to satellite timing error; disagreement between encoded and actual location of PMU | Development of linear state estimation tools Avoiding timestamp discrepancy by modifying<br>real-time clock element<br>Using OMP-based identification, BB algorithm to solve PMU location discrepancies |
| Plausibility and availability (Communication, Application) [47–49, 51, 114, 115] | Impact of measurement system on individual data points<br>Data inaccessibility due to high network<br>latency or device failure<br>Delayed data arrival due to increased<br>routing traffic | Use of electrical data recorder (EDR) tools for capturing high-rate time series data, data storage and analysis<br>A more lenient time limit could be set for noncritical application usage<br>Latency-aware application design |
| Origination (Device, Aggregator, Communication, Application) [42, 53, 116, 117] | Poor standard interpretation, implementation<br>Misalignment, erroneous compression<br>Latency, loss of communication nodes<br>Data corruption due to delivery time of<br>PDC exceeding permissible slot<br>Network unavailability to process incoming data streams | Redundancy in communication by using wireless and wired connections<br>Lagrange interpolating polynomial method<br>Data substitution, imputation, interpolation and extrapolation<br>Stochastic forecasting with prediction error<br>minimization (PEM) |
| Logical consistency (Aggregator, Communication) [42] | Data transmitted contains no headers<br>Sampling rate of data changed at PMU without being adjusted at PDC<br>Data duplication while processing<br>Data from different PMUs with incorrect timestamps | Logical consistency can be ensured by maintaining the PMU registries and data protocols |

the device. This could be categorized into: persistence of PMU header that states whether the PMU header structure is consistent over time, and persistence of PDC header that states whether the PDC header structure is consistent over time. ② *Data frame consistency*: consistency of data frames of the device. This could be categorized into: persistence of PMU data frame that states whether the PMU data frame structure is consistent over time, and persistence of the PDC data frame that states whether the PDC data frame structure is consistent over time. ③ *Order consistency of data frames*: whether the order in which the data frames are recorded is consistent in the device. ④ *Consistency in compliance to standards* recommended for PMU and all the devices associated with it. ⑤ *Consistency of reporting rate*: whether data reporting rate is consistent across all devices.

Emerging research in this area has lately focused on determining solutions for ensuring data quality. These solutions include using omnidirectional antennas to

**Table 4** Summary of existing research in synchrophasor cybersecurity challenges and solutions

| Level | Challenges | Solutions |
|---|---|---|
| Device, Aggregator [54, 55, 97, 102, 110, 121] | Device damage<br>Device calibration tampering<br>Forging PMU data<br>GPS spoofing | Multi-alteration technique to trace adversary in event of GPS spoofing<br>Visible GPS satellite prediction<br>Anomaly between expected and measured GPS signals<br>Using SSL/TLS or IPSec to encrypt data before transmission<br>Using state estimation technique to mitigate device calibration and tampering<br>Rigorous penetration testing prior to installation |
| Communication [57, 61, 62, 66, 112–115, 122] | Denial of service<br>Man-in-the-middle<br>False data injection<br>Snooping attack<br>Delay attack | Airgapping PMU network<br>Filtering routers, disabling IP broadcasts, applying security patches, disabling unused ports<br>Server authentication by clients before establishing connection<br>Use of time-series state estimation<br>Cryptographic methods like AES, DES<br>Mutual authentication<br>Cyber trust model with blockchains<br>NASPInet hub-spoke model<br>Optimal key generation and distribution |
| Application [63–65, 116, 117] | Phishing and social engineering<br>APT and insider threats<br>Replay attacks | Authentication, authorization and accounting (AAA)<br>Use of secure data transfer protocol to prevent replay attack |

improve GPS availability, context-aware determination of missing data streams using accurate timing information, network time protocol (NTP) and associated chip scale atomic clocks (CSACs) as backups for synchronization when GPS fails, imputation, interpolation and extrapolation, stochastic forecasting with prediction error minimization (PEM) and data substitution [52].

6) Evaluation of quality: Methods to evaluate quality is discussed in Section 4.1. The approach for performance evaluation is to first study the impacts of device calibration and network conditions on quality, then examine how poor quality reduces the application performance [42]. Two effective methods are proposed to evaluate the impact of quality on performance: ① *Benchmarking* that tests an application multiple times with numerous erroneous datasets in contrast to those with no known errors, and ② *Standardization* that documents, for each application, the level of tolerable errors.

### 3.2 Cybersecurity challenges

Synchrophasors cater to applications like state estimation, contingency analysis and optimal power flow that need real-time high-resolution data measurement, communication and analytics [119]. Therefore, a successful attack on these devices might cause erroneous SA or cascading failures [56, 120]. Yet, many industrial organizations do not consider synchrophasors as critical cyber assets. Recent cyberattacks on the smart grid in Table 1 mostly used powerful malware like worms, viruses or Trojan horse, but a few attacks like the one on the Pacific Gas & Electric transmission substation relied on physical means. These attacks jeopardized not just the availability of power but also that of control data (information). In Table 4, cybersecurity of synchrophasors are categorized into: ① Device, Aggregator; ② Communication; and ③ Control center application.

1) Device, Aggregator: NASPI network (NASPInet) is logically capable of integrating WAMS across multiple geographically distant organizations using phasor gateways (PGWs). The attacks at this level compromise data integrity, targeting devices from individual PMUs to PDCs, SuperPDCs or even PGWs. Some attacks include: ① tampering the signal measurement units of devices through interference; ② illicitly changing the calibration of devices to report erroneous readings; ③ forging data to reflect wrong measurements; and ④ GPS spoofing by broadcasting fabricated

signals to the receiver to yield erroneous synchronization of phasors computed, modifying satellite position, or replaying legitimate GPS signals at later timestamps [54].

GPS spoofing can be mitigated by enabling the receiver to predict visible GPS satellites at a given position and time instant and use the coarse/acquisition (C/A) code from those satellites. Another strategy compares the measured GPS signal to the estimated signal and computes the anomaly error which must have an accuracy of $\leq$ 40 ns for nearly 95% of the values according to IEEE C37.118 [44]. Synchrophasors must be subject to rigorous testing before installation. Some methods include port scans, device security feature robustness, network congestion testing, denial of service testing, network traffic sniffing and disclosure testing [55]. These tests should be periodically conducted by certified white hat penetration testers after installation. Regular patches and configuration updates must be made down to the end-device level.

2) Communication: Synchrophasors support bidirectional communication channels, where data measurements flow from devices to the control center while control signals flow the other way. The vulnerabilities of the protocols used by the devices also contribute to the overall security. Attacks on communication channels compromise integrity, availability and confidentiality. Some attacks include: ① *Denial of service* (*DoS*) by overwhelming PMUs, PDCs or other aggregation devices higher in the hierarchy with bogus frames so that legitimate frames are lost, delayed, denied or dropped; ② *Man-in-the-middle (MITM)* attacks by a malicious entity posing itself as PDC (to PMU) or PGW (to PDC) and sending malicious commands that causes PMUs/PDCs to behave in an abnormal manner that triggers failures; ③ *False data injection (FDI)* by intercepting frames over the channel, altering or replacing them with malicious information that then gets propagated to higher levels of the WAMS; ④ *Snooping* by the attacker eavesdropping on the channel for incoming or outgoing frames, typically not modifying or stealing but just capturing a copy of that information for packet replay or espionage; and ⑤ *Delay* caused by compromising communication routers that deliberately induce latencies in propagation to critically affect the grid's SA.

Many authentication and authorization algorithms are proposed to secure synchrophasor data over communication channels [57]. These methods range from conventional encryption methods to cyber trust. Due to the ubiquity and widespread range of these devices, key distribution and management becomes a problem. Mutual authentication is also proposed to account for trust [61]. Decentralized, blockchain-based trust acquisition is being considered too. The publish-subscribe hub-spoke architecture proposed by NASPInet supports dynamic sharing of device data to alleviate shortcomings of the communication medium like delays and latencies. Standards like IEC 61850-90-5 recommend trusted key distribution center to generate and distribute keys that meet system requirements [63–66].

3) Application: Despite being protected by enterprise security tools for intrusion detection and prevention, virtualization, segmentation, authentication, authorization and access control, cyberattacks still proliferate [67, 68]. It is understood that any successful attack at the other two levels perpetrated in a manner undetectable by the enterprise security systems can pose a significant threat. The attacks at this level are the most dangerous, since crucial power system applications use data from WAMS to conduct analysis to address reliability, power quality, network topology, and faults. An adverse impact on these calculations could compromise the "self-healing" nature of the grid. More recent solutions include game theory, machine learning, proactive data visualization, and defense-in-depth [12, 123].

#### 3.2.1 *Evaluation of security*

Works have tested the resilience of PMUs and PDCs against different attacks. The authors in [124] conducted penetration testing of a synchrophasor network in IEEE 68-bus system to map vulnerabilities against the common vulnerabilities exposure (CVE) database. Potential corrective measures to ensure the security of PMUs and PDCs is proposed [125]. Considering the security at substation and information levels, the authors provide a wide range of tools to mitigate breaches at both fronts. A multilayered architecture at the substation is proposed where different levels of data abstraction is provided between PMUs and external environment, supplemented by firewalls, user datagram protocol (UDP) secure for communication over untrusted networks, and remote access using secure shell (SSH).

## 4 Data quality-cybersecurity dependency

The severity of an attack can be understood from the extent of its impacts on the targeted system. With the smart grid encouraging interoperability between devices, information, applications, and protocols, a transparent and direct

**Table 5** Summary of the interdependency between quality and cybersecurity challenges

| Level | Quality attribute | Quality issue | Cyber-attack observed | Security attribute impacted |
|---|---|---|---|---|
| Device | Completeness, accuracy, plausibility | Synchronization signal loss, measurement signal loss, missing data | GPS spoofing, replay, device tamper, changing device calibration, FDI | Integrity |
| Aggregator | Origin, consistency, plausibility | Corrupted data, anomalies, outliers | FDI, tampering, buffer overflow, MITM | Confidentiality, integrity |
| Communication | Availability, origin, consistency | Anomalies, outliers, inconsistent, out-of-order data | DoS, MITM, FDI, snooping, replay, delay | Confidentiality, integrity, availability |
| Application | Origin, availability, consistency, completeness, accuracy | DoS, delay, APT, FDI, theft/fraud, insider attack | Corrupted data, missingness, anomalies, outliers | Confidentiality, integrity, availability |

information exchange is now feasible. This also means that if information in one of the interconnected systems is infected, it is bound to propagate to other systems upon exchange, affecting the whole network. Synchrophasor devices harbor such vulnerabilities, as summarized in Section 3.2. However, to mitigate cyberattacks on interconnected systems, the relationship between devices and data must be known.

Table 5 summarizes key interdependencies between the two challenges. There is a tight coupling between data quality and cyber-attacks, implying it is wise to study synchrophasor cybersecurity by accounting for the impacts on quality. In most attacks, plausibility, completeness, accuracy and consistency are primarily impacted [126, 127]. In Section 4.1, specific evaluation methods for quantifying this relationship are reviewed. Section 4.2 looks at how data quality characteristics can be used as markers to detect potential cyber-attacks within the context of synchrophasors. Results from these subsections are summarized in Tables 6 and 7, respectively.

### 4.1 Interdependency evaluation methods

Next to communications, cybersecurity was found to impact the design and installation costs for synchrophasors [141]. This is because they are critical to the missionsupport systems of the grid. Different practical ways for utilities to mitigate quality issues like accuracy, timeliness and consistency are also identified. Some methods include employing dedicated communication channels between PMUs and PDCs, encrypting PMU data before communication, and enhancing communication endpoints using firewalls and routers. The report, however, does not delve into the details of how such methods could impact latency (and hence, timeliness) and availability of the data.

Given different manufacturers of devices, there will be differences in measurement and calibration quality despite adhering to the standards. The varying application requirements cause differences in application-level PMU performance, of which data quality is a major one. The static and dynamic PMU testing efforts of the Performance and Standards Task Team (PSTT) of NASPI and the PMU performance characterization are briefly summarized in [142]. In it, the different steady-state tests performed on magnitude, phase and frequency evaluate their conformance to accuracy requirements, which is an important attribute of data quality and is a direct target of many cyberattacks. Given the impact of instrumentation channels on the quality, they have been well-characterized and evaluated for impacts on accuracy in the literature. The errors induced by them could be rectified through model-based correction algorithms and state estimation based error filtering. Some other avenues where data quality could be evaluated include the cable configurations, testing and validating the devices to ensure accurate, consistent performance and interoperability at all levels [143, 144]. Although not explicit, these works hint at the improvement in the resilience of synchrophasor devices against potentially malicious activities by accounting for proper testing methods to characterize and evaluate the different sources of errors prior to deployment that might contribute to poor quality.

Final conclusions can be gathered from [145]. The report by the Pacific Northwest National Laboratory (PNNL) analyzes existing synchrophasor networks in terms of their communication and information-level interoperability, security and performance. It concluded that latency is a key issue for the future synchrophasor designs which is expected to compound latency due to PDC functionality. It also emphasized that substations generally did not employ

**Table 6** Summary of evaluation methods for quality (DQ) and cybersecurity (CS) issues

| Issue | Challenge | Evaluation methods |
|---|---|---|
| Noise (DQ) | Consistency, accuracy | Cable configuration, testing, validation<br>Specifying confidence interval, precision, TVE, ROCOF for measurements<br>Evaluating instrumentation channels<br>Model-based correction<br>State estimation-based error filtering<br>Presistence in Data/Header frames<br>Standards compliance |
| Outlier (DQ) | Consistency, origin, accuracy | Standardization, benchmarking<br>Enhancing endpoints with switches, routers<br>Specifying device model, coverage and content |
| Missingness (DQ) | Completeness, availability, accuracy | Dedicated communication channels<br>Enhancing endpoints with switches, routers |
| Delay/loss (CS) | All levels | Regular penetration testing of all levels<br>Link-level encryption, selective encryption<br>Dedicated communication channels<br>Data redundancy for fault tolerance |
| Manipulation (CS) | Device, Aggregator, Communication | Regular penetration testing of all levels<br>Link-level encryption, selective encryption<br>Data abstraction, multi-layered architecture<br>Data redundancy for fault tolerance<br>Augmenting ID/IPS, firewalls, ACLs, VPNs |
| Theft (CS) | Device, Aggregator, Communication | Regular penetration testing of all levels<br>Data abstraction, multi-layered architecture<br>Data redundancy for fault tolerance<br>Augmenting firewalls, ACLs, VPNs |

redundancy; there is little consistency in adoption of security methods for synchrophasor networks. Some tools include link-level encryption, virtual private networks (VPNs), ID/IPS, firewalls and access control lists (ACLs). Further, existing data quality checking methods locate a compromise in integrity by identifying faulted data values (due to measurement errors, communication delays or external events) but not due to result of device tampering, MITM, spoofing or FDI. Since both faults and attacks have the same impact on quality, it is important to differentiate the two causes while checking for the attributes such as accuracy, consistency and timeliness.

To summarize, the following measures can be used as metrics to quantify data quality: TVE, errors in magnitude, phase, frequency and ROCOF, harmonics and noise for measurement accuracy; comparison between measured and expected results, confidence interval and precision for measurement specifiers; temporal, geospatial and topological accuracy for attribute accuracy; device model specifications, geospatial and topological coordinates, coverage and content for origination; persistence in Header and Data frames, standards compliance, reporting rate and order for logical consistency; and gap rate, gap size and largest known gap for completeness. Benchmarking and standardization are two methods that can be used to evaluate data quality. Similarly, cybersecurity can be quantified by conducting extensive penetration testing of the synchrophasor networks integrated into benchmarked IEEE bus systems for different types of attacks (DoS, MITM, FDI, spoofing, probing, cache poisoning) and discovering potential vulnerabilities that could be exploited. While doing so, it would be important to also repeat the evaluation of the quality attributes using the above metrics and explore how they are impacted due to the specific attacks, and whether they violate the industry standards requirements specified for different applications.

**Table 7** Summary showing how quality can help identify cybersecurity issues

| Cyber-attack | Quality affected | Quality check looks for | Mitigation methods using quality |
|---|---|---|---|
| Device tampering (delay/loss, theft) [128, 129] | Completeness, plausibility, accuracy, consistency, origination | Large gap sizes, inaccurate readings, ping fail | Statistical substitution: regression, imputation, interpolation<br>Intelligent substitution: neural networks, logistic regression, optimization<br>Securing the physical devices |
| Spoofing PMU data (manipulation) [130–132] | Consistency, accuracy, plausibility | Unexpected values, errors, mismatch with SCADA values, redundant timestamp, out-of-order packet arrival | Monitoring line impedances for anomalies<br>Divergence and miscorrelation between SCADA and PMU data |
| GPS spoofing (manipulation, delay/loss) [54, 133–135] | Consistency, origination, plausibility | Inaccurate timing value, TVE $> 1\%$, packets arrive out-of-order | Using multiple synchronization sources or telecommunications<br>Anti-spoofing checking methods at receivers<br>Internal holdover oscillators as backups for providing accurate timing signals<br>Spoofing match algorithm with Golden Search for lighter computation |
| Denial of service (delay/loss) [129] | Completeness, accuracy, consistency | Congestion at PDCs/network, delayed arrival of packets, dropped packets, inability to reach suspected device | Augmenting PDCs with inline blocking tools<br>Employ port hardening and disable IP broadcasts<br>Use high bandwidth communications (expensive) |
| Man-in-the-middle (delay/loss, manipulation, theft) [129] | Origination, accuracy, availability, consistency | Mismatch between obtained and expected value, abnormal delay in packet arrival | Mutual authentication, message authentication codes<br>Digital certificates with active management of CRLs |
| False data injection (manipulation, theft) [136–140] | Plausibility, consistency, accuracy, origination | Mismatch with SCADA values, unexpected values, spatio-temporal outliers | Spatio-temporal correlations, density based local outlier factoring<br>Monitor line impedance for anomalies<br>Random time-hopping of packets<br>Divergence and miscorrelation between SCADA and PMU data |
| Snooping, sniffing (theft) [59, 129] | Plausibility, origin | No observable changesadditional analysis needed | Using secure gateway/VPN communication<br>Employing TLS/SSL, SSH, lightweight selective encryption |
| Delay (delay/loss) [59, 129] | Completeness, consistency, availability, accuracy | Observable patterns in gaps, slow arrival of packets | Statistical and intelligent substitutions<br>Redundant measurement devices on the same line |
| APT, insider threat (delay/loss, theft, manipulation) [123] | Accuracy, consistency, origin, plausibility | No observable changesadditional analysis needed | Defense-in-depth<br>Machine learning, advanced data analytics |

### 4.2 Addressing cyber-attacks using quality issues

It can be seen from Table 7 that successful cyberattacks compromise synchrophasor data quality since the security requirements are violated [146]. Given synchrophasors use TCP/UDP on the transport layer for their communications, attacks typically possible on TCP/IP stack like DoS, MITM, packet replay or spoofing are possible in synchrophasor domains as well.

Physical attacks like device tampering causes loss or incurs theft of critical information, easily observed through large gaps sizes, poor accuracy in obtained values and unreliable origin. The lost data is typically handled through substitution, either statistical or intelligent [128, 129]. The best way to prevent physical attacks like cable disconnects, direct damage to device, etc. is by ensuring the devices are isolated from external weather and human elements.

Spoofing synchrophasor data is achievable through polynomial fitting or data mirroring techniques. Such attacks impact quality that manifests as outliers or noise. Several methods have been proposed to counter these attacks: intra-PMU and inter-PMU correlations to determine the relationship between PMU parameters and across PMUs in a locality, respectively; machine learning techniques like support vector machines (SVMs) and more [130–132].

GPS spoofing exploits publicly available civilian GPS signals using air or cable to produce signals that initially align with the original, but slowly start increasing the power to drown the authentic signal and thereby compromising the receiver [54, 133]. By introducing measurement errors in the time synchronization, the attacks induce changes in data consistency and plausibility which can be used as markers to identify the likelihood of the attack [134, 135, 147].

In a successful DoS where multiple synchrophasor devices get compromised, packet delay or loss is observed. This impact in quality can serve a clue to the onset of DoS-style attacks. Typical solutions involve augmenting inline blocking tools, high bandwidth connections, disabling IP broadcasts and port hardening.

MITM is possible in synchrophasors where the attacker acts as a legitimate PDC to the PMUs and viceversa, thereby intercepting and/or modifying all messages exchanged. This is noticed by quality checking methods in the form of poor accuracy and consistency in values between what was sent by PMU and what was received by PDC. It can be avoided by having the devices employ mutual authentication and a digital certificate mechanism with an actively managed certificate evocation lists (CRLs) and certificate authorities [59, 129].

FDI impacts the consistency, accuracy and plausibility of the data. The effects are typically observed as spatio-temporal outliers in the data. Quality checking methods check for this anomaly and may employ correlation across different timestamps to identify the corruption of data. FDI is one of the widely explored attacks on synchrophasor domain, with solutions like determining the mismatch between the values obtained from PMUs and that observed in SCADA, monitoring the line impedances which get affected when data is manipulated, and using density-based local outlier filter (LOF) analysis [136–140].

Sometimes, attackers simply capture the packets flowing in a channel with an intent to listen. Such sniffing/snooping attacks have been conducted using WireShark to realize messages are exchanged in plaintext. This attack is difficult to detect using data quality checking methods since most often, no quality characteristic is impacted as the attackers do not affect the data actively. However, technologies like VPN, encryption of selective messages (to reduce the overall process overhead), or transport layer security (TLS)/secure ocket layer (SSL), secure shell (SSH) can be used to mitigate them. While TLS has been shown to be susceptible to poisoning attacks and VPN to side channel attacks, careful network design can account for them [129, 148].

With the increased frequency of campaign efforts and nation-sponsored attacks against the grid, synchrophasors could be lucrative targets for sophisticated attacks like advanced persistent threats (APTs), social engineering, watering-hole attacks and malware-based intrusions [149–153]. While these attacks scale beyond specific devices in the synchrophasor hierarchy, the quality checking methods alone would not be sufficient [123]. The use of defense-in-depth model augmented with stakeholder interactions, awareness and training, and intelligent solutions like machine learning for attack data classification and/or event prediction, root-cause analysis of observed events, developing evolving defense topographies using moving target defense, and advanced visualization techniques for efficient cognition of events would play a critical role.

The key takeaway from this section is that impacts on data quality can provide strong markers for an underlying cyber-attack. Noise, outliers and missing values are all commonly observed issues which quality checking methods may be programmed to detect, analyze and base decisions on. Certain sophisticated attacks like APTs, insider threats, sniffing, and social engineering have indirect impacts on quality which a checking method may not be able to detect with enough confidence or precision. Additional solutions are required to mitigate such attacks in the synchrophasor domain. These solutions include statistical methods like divergence, correlation, regression and substitution; intelligent methods like neural networks and evolutionary algorithms for event classification and

prediction, logistic regression for substitution; technologies like VPNs, firewalls, ID/IPS, anomaly detectors, selective encryption, port hardening, network isolation and use of TLS/SSL, SSH; and human-in-the-loop solutions like advanced visualization techniques, awareness and training, and stakeholder engagements. While the impacts on quality can also be due to underlying device or measurement errors, most of the works in the literature assume the data has been subject to delay/loss, manipulation or theft intentionally. This paves way for the recommendation that the upcoming research in this area must look at ways to differentiate the impacts on data quality due to attacks from errors.

## 5 Future directions of research and conclusion

The future directions of research in the areas of synchrophasor data quality, cybersecurity and communications are multi-faceted. Addressing data quality challenges must begin with a strong push to the adoption of industry-wide, vendor-agnostic data management, processing and storage standards for smart grid. Most recent cyber-attacks were successful due to the difference in speed of cognition of the information generated by automated vulnerability detection tools and the speed with which the machine data is created (called cognitive gap) [123]. The design of synchrophasor devices are also expected to improve in the future [103]. Keeping in mind the quality challenges, an improvement to PDC design called flexible integrated synchrophasor system (FIPS) was proposed to minimize issues in quality and communication, and tackles specific tasks of PDC such as data alignment, employs cryptographic methods to ensure confidential exchange of data without jeopardizing integrity, and establishes relevance to the NASPInet [121]. To ensure device and applicationlevel interoperability, development of technical standards and conformance testing rules is expected. Further, the emergence of distribution-level $\mu-$PMUs will evoke the need for developing measurement, communication, quality and security standards. Further, with the deployment of distributed renewable sources, electric and autonomous vehicles, energy storage and transactive energy, there is a strong impetus for enhancing technologies behind monitoring and control, of which synchrophasors will play a major role [141].

To conclude, while existing research has focused on the synchrophasor challenges of quality and cybersecurity individually, their interdependency has largely been ignored. This paper makes one of the first attempts at highlighting the impacts of cyber-attacks on various quality attributes, thereby recommending that the future research on the design and development of security solutions should account for their impacts on quality as well, and that different quality characteristics can be used by quality checking methods to flag for potential cyber-attacks. Plausibility, completeness, accuracy and consistency are some of the attributes that are most adversely impacted by a majority of the attacks on synchrophasors. At the same time, not all cases of poor data quality imply a successful cyber-attack as the reason. Different metrics that could be used to quantify quality attributes were summarized, and the methods that help evaluate the impacts of quality and security on performance were also briefly highlighted. This paper serves as a starting point for researchers entering these areas as it summarizes and determines their interdependency and relevance to smart grid security.

**Acknowledgements** This work was supported by the National Science Foundation Grant (No. CNS-1553494) and the Department of Energy Grant (No. 800006104). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF and DOE.



## References

[1] Ozgur U, Nair HT, Sundararajan A et al (2017) An efficient MQTT framework for control and protection of networked cyber-physical systems. In: Proceedings of IEEE conference on communications and network security, Las Vegas, USA, 9–11 October 2017, pp 421–426

[2] Sanjab A, Saad W, Guvenc I et al (2016) Smart grid security: threats, challenges, and solutions. arXiv:1606.06992 [cs.IT]

[3] Sundararajan A, Pons A, Sarwat AI (2015) A generic framework for EEG-based biometric authentication. In: Proceedings of the 12th international conference on information technology new generations, Las Vegas, USA, 13–15 April 2015, pp 139–144

[4] Anzalchi A, Sarwat A (2015) A survey on security assessment of metering infrastructure in smart grid systems. In: Proceedings of IEEE SoutheastCon, Fort Lauderdale, USA, 9–12 April 2015, pp 1–4

[5] Dagle JE (2004) Data management issues associated with the August 14th, 2003 blackout investigation. In: Proceedings of IEEE power engineering society general meeting, Denver, USA, 6–10 June 2004, pp 1680–1684

[6] Larsson S, Ek E (2004) The blackout in southern Sweden and eastern Denmark, September 23, 2003. In: Proceedings of IEEE power engineering society general meeting, Denver, USA, 6–10 June 2004, pp 1668–1672

[7] Corsi S, Sabelli C (2004) General blackout in Italy Sunday September 28th, 2003, h 03:28:00. In: Proceedings of IEEE power engineering society general meeting, Denver, USA, 6–10 June 2004, pp 1691–1702

[8] Berizzi A (2004) The Italian 2003 blackout. In: Proceedings of IEEE power engineering society general meeting, Denver, USA, 6-10 June 2004, pp 1673–1679
[9] Gomes P (2004) New strategies to improve bulk power systems security: lessons learned from large blackouts. In: Proceedings of IEEE power engineering society general meeting, Denver, USA, 6–10 June 2004, pp 1703–1708
[10] Imai S (2004) TEPCO observations on August 14 blackout and recommendations to prevent future blackouts based on TEPCOs experience. In: Proceedings of IEEE power engineering society general meeting, Denver, USA, 6–10 June 2004, pp 1–27
[11] Jamei M, Sarwat AI, Iyengar SS et al (2015) Security breach possibility with RSS-based localization of smart meters incorporating maximum likelihood estimator. In: Selvaraj H, Zydek D, Chmaj G (eds) Progress in systems engineering. Advances in intelligent systems and computing, vol 366. Springer, Cham. https://doi.org/10.1007/978-3-31908422-0-20
[12] Wei L, Sarwat AI, Saad W (2016) Risk assessment of coordinated cyber-physical attacks against power grids: a stochastic game approach. In: Proceedings of IEEE industry applications society annual meeting, Portland, USA, 2–6 October 2016, pp 1–7
[13] Hauer JF, Bhatt NB, Shah K et al (2004) Performance of "WAMS East" in providing dynamic information for the North East blackout of August 14, 2003. In: Proceedings of IEEE power and energy society general meeting, Denver, USA, 6–10 June 2004, pp 1685–1690
[14] U.S.-Canada Power System Outage Task Force (2004) Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations. North American Electric Reliability Commission (NERC) Report. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Outage_Task_Force_DRAFT_Report_on_Implementation.pdf. Accessed October 2017
[15] Zima M, Larsson M, Korba P et al (2005) Design aspects for wide-area monitoring and control system. Proceedings of the IEEE 93(5):980–996
[16] Wei L, Sarwat A, Saad W et al (2018) Stochastic games for power grid protection against coordinated cyber-physical attacks. IEEE Trans Smart Grid 9(2):684–694
[17] Ashton PM, Taylor GA, Irving MR et al (2012) Prospective wide area monitoring of the Great Britain transmission system using phasor measurement units. In: Proceedings of IEEE power engineering society general meeting, San Diego, USA, 22–16 July 2012, pp 1–8
[18] Chow JH, Beard L, Patel M et al (2015) Guidelines for siting phasor measurement units. North American SynchroPhasor Initiative Research Initiative Task team (NASPI-RITT) Report. https://www.researchgate.net/publication/279658581_Guidelines_for_Siting_Phasor_Measurement_Units__Version_8_June_15_2011_North_American_SynchroPhasor_Initiative_(NASPI)_Research_Initiative_Task_Team_(RITT)_Report. Accessed 15 June 2011
[19] Gomes P, Martins N, de Mello P et al (1998) Assuring system reliability in a competitive environment. In: Proceedings of CIGRE meeting, Paris, France, 30 August–5 September 1998, pp 38–104
[20] de Azevedo R, Allen D, Perpuly Y et al (2015) PMU placement considering data uncertainty and redundancy. In: Proceedings of IEEE SoutheastCon, Fort Lauderdale, USA, 9–12 April 2015, pp 1–6
[21] Parvez I, Islam A, Kaleem F (2014) A key management-based two-level encryption method for AMI. In: Proceedings of IEEE power engineering society general meeting-conference & exposition, National Harbor, USA, 27–31 July 2014, pp 1–5
[22] Wang Y, Saad W, Sarwat AI et al (2018) Reactive power compensation game under prospect-theoretic framing effects. IEEE Trans Smart Grid 9(5):4181–4193
[23] Ma J, Zhang P, Fu HJ et al (2010) Application of phasor measurement unit on locating disturbance source for low-frequency oscillation. IEEE Trans Smart Grid 1(3):340–346
[24] Narendra K (2007) Role of phasor measurement unit (PMU) in wide area monitoring and control. ERL phase power technologies report, pp 1–45. http://www.erlphase.com/downloads/application_notes/Roles_of_PMUs_in_Wide_Area_Monitoring_and_Control.pdf. Accessed 17 July 2017
[25] Novosel D, Vu K (2006) Benefits of PMU technology for various applications. In: Proceedings of international council on large electric systems- CIGRE croatian national committee, 7th symposium on power system management, Paris, France, 5–8 November 2006, pp 1–13
[26] Ferrari L, Gentz R, Scaglione A et al (2014) The pulse coupled phasor measurement units. In: Proceedings of IEEE international conference on smart grid communications (SmartGridComm), Venice, Italy, 3–6 November 2014, pp 320–325
[27] Sreenivasareddy PS, Chowdhury SP, Chowdhury S (2010) PMU placement-a comparative survey and review. In: Proceedings of IET international conference on developments in power system protection, Manchester, UK, 29 March–1 April 2010, pp 1–4
[28] Aamre K, Centeno VA, Pal A (2015) Unified PMU placement algorithm for power systems. In: Proceedings of North American power symposium (NAPS), Charlotte, USA, 4–6 October 2015, pp 1–6
[29] Parvez I, Sarwat AI, Wei L et al (2016) Securing metering infrastructure of smart grid: a machine learning and localization based key management approach. MDPI J Energies 9(9):691–708
[30] Parvez I, Jamei M, Sundararajan A et al (2014) RSS based loop-free compass routing protocol for data communication in advanced metering infrastructure (AMI) of smart grid. In: Proceedings of 2014 IEEE symposium on computational intelligence applications in smart grid (CIASG), Orlando, USA, 9–12 December 2014, pp 1–6
[31] Negash K, Khan B, Yohannes E (2016) Artificial intelligence versus conventional mathematical techniques: a review for optimal placement for phasor measurement units. Technol Econ Smart Grids Sustain Energy. https://doi.org/10.1007/s40866-016-0009-y
[32] Rahman NHA, Zobaa AF (2016) Optimal PMU placement using topology transformation method in power systems. J Adv Res 7(5):625–634
[33] Nazari-Heris M, Mohammed-Ivatloo B (2015) Application of heuristic algorithms to optimal PMU placement in electric power systems: an updated review. Renew Sustain Energy Rev 50:214–228
[34] Chouhan D, Jaiswal V (2016) A literature review on optimal placement of PMU and voltage stability. Indian J Sci Technol 9(47):1–7
[35] Meier A, Stewart E, McEachern A et al (2017) Precision micro-synchrophasors for distribution systems: a summary of applications. IEEE Trans Smart Grid 8(6):2926–2936
[36] Sexauer J, Javanbakht P, Mohaghehi S (2013) Phasor measurement units for the distribution grid: necessity and benefits. In: Proceedings of IEEE PES innovative smart grid technologies, Washington DC, USA, 24–27 February 2013, pp 1–7
[37] Singh B, Sharma NK, Tiwari AN et al (2011) Applications of phasor measurement units (PMUs) in electric power system networks incorporated with FACTS controllers. Int J Eng Sci Technol 3(3):64–82

[38] Sanchez-Ayala G, Aguerc JR, Elizondo D et al (2013) Current trends on applications of PMUs in distribution systems. In: Proceedings of IEEE PES innovative smart grid technologies conference (ISGT), Washington DC, USA, 24–27 February 2013, pp 1–6
[39] Lee H, Tushar Cui B et al (2017) A review of synchrophasor applications in smart grid. WIREs Energy Environ 6(3):1–31
[40] Lauby M (2010) Real-time application of PMUs to improve reliability task force (RAPIR TF). NERC technical presentation. https://www.nerc.com/comm/oc/related%20files%20dl/rapir_oc_slides.pdf. Accessed 1 August 2017
[41] Mohanta DK, Murthy C, Roy DS (2016) A brief review of phasor measurement units as sensors for smart grid. Electric Power Compon Syst 44(4):411–425
[42] NASPI PMU Applications Requirements Task Force White Paper (2017) PMU data quality: a framework for the attributes of PMU data quality and a methodology for examining data quality impacts to synchrophasor applications. NASPI technical report. https://www.naspi.org/sites/default/files/reference_documents/PARTF_WhitePaper_20170314_Final_PNNL.pdf. Accessed 1 August 2017
[43] Christoforidis GP, Meliopoulos APS (1990) Effects of modeling on the accuracy of harmonic analysis. IEEE Trans Power Deliv 5(3):1598–1607
[44] Zhu F, Youssef A, Hamouda W (2016) Detection techniques for data-level spoofing in GPS-based phasor measurement units. In: Proceedings of international conference on selected topics in mobile & wireless networking (MoWNeT), Cairo, Egypt, 11–13 April 2016, pp 1–8
[45] Yang B, Yamazaki J, Saito N, et al (2015) Big data analytic empowered grid applications—is PMU a big data issue? In: Proceedings of 12th international conference on the European energy market (EEM), Lisbon, Portugal, 19–22 May 2015, pp 1–4
[46] Rahman NHA, Zobaa AF (2016) Optimal PMU placement using topology transformation method in power systems. J Adv Res 7(5):625–634
[47] Veda S, Chaudhuri NR, Baone CA, et al (2014) Assessment of impact of data quality on PMU-based applications. In: Proceedings of CIGRE US national committee grid of the future symposium, http://cigre-usnc.tamu.edu/wpcontent/uploads/2015/06/Assessment-of-Impact-of-DataQuality-on-PMU-Based-Applications.pdf. Accessed 1 August 2017
[48] Zhu K (1988) A method for plausibility checks and data validation in power systems. IEEE Trans Power Syst 3(1):267–271
[49] Danielson CFM, Vanfretti L, Almas MS et al (2013) Analysis of communication network challenges for synchrophasor-based widearea applications. In: Proceedings of IREP symposium on bulk power system dynamics and control - IX optimization, security and control of the emerging power grid (IREP), Rethymno, Greece, 25–30 August 2013, pp 1–13
[50] Hu Y, Novosel D (2006) Challenges in implementing a large-scale PMU system. In: Proceedings of 2006 international conference on power system technology, Chongqing, China, 22–26 October 2006, pp 1–7
[51] Jones KD, Pal A, Thorp JS (2015) Methodology for performing synchrophasor data conditioning and validation. IEEE Trans Power Syst 30(3):1121–1130
[52] Huang C, Li F, Zhan L et al (2016) Data quality issues for synchrophasor applications part II: problem formulation and potential solutions. J Mod Power Syst Clean Energy 4(3):353–361
[53] Huang C, Li F, Zhan L et al (2016) Data quality issues for synchrophasor applications part I: a review. J Mod Power Syst Clean Energy 4(3):342–352
[54] Shepard DP, Humphreys TE, Fansler AA (2012) Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. Int J Crit Infrastruct Prot 5(3–4):146–153
[55] Morris T, Pan S, Lewis J et al (2011) Cybersecurity testing of substation phasor measurement units and phasor data concentrators. In: Proceedings of the seventh annual workshop on cyber security and information intelligence research, Oak Ridge, USA, 12–14 October 2011, pp 1–4
[56] Hao Y, Wang M, Chow J (2015) Likelihood of cyber data injection attacks to power systems. In: Proceedings of IEEE global conference on signal and information processing (GlobalSIP), Orlando, USA, 14–16 December 2015, pp 657–661
[57] Kumar S, Soni MK, Jain DK (2015) Cyber security threats in synchrophasor system in wide area monitoring system. Int J Comput Appl 115(8):17–22
[58] Lin H, Deng Y, Shukla S et al (2012) Cyber security impacts on all-PMU state estimator-a case study on cosimulation platform GECO. In: Proceedings of IEEE third international conference on smart grid communications (SmartGridComm), Tainan, China, 5–8 November 2012, pp 587–592
[59] Beasley CT (2014) Electric power synchrophasor network cyber security vulnerabilities. Dissertation. Clemson University
[60] Rizzetti TA, Canha LN, Milbradt R et al (2015) Security aspects on PMU data communication based on IP networks in smart grids. In: Proceedings of 23rd international conference on electricity distribution, Lyon, France, June 15–18, 2015, pp 1477–1481
[61] Saxena N, Choi BJ (2015) State of the art authentication, access control, and secure integration in smart grid. MDPI J Energies 8(10):11883–11915
[62] Deng Y, Shukla S (2012) Vulnerabilities and countermeasures a survey on the cyber security issues in the transmission subsystem of a smart grid. Journal of Cyber Security and Mobility, https://www.semanticscholar.org/paper/Vulnerabilitiesand-Countermeasures-%E2%80%93-A-Survey-on-a-Deng-Shukla/6c4b97cc4f70fb34cad8c2b03f7fb5dfb8a5e84d. Accessed 30 June 2017
[63] Pan S (2014) Cybersecurity testing and intrusion detection for cyber-physical power systems. Dissertation. Mississippi State University
[64] Ashok A, Hahn A, Govindarasu M (2014) Cyberphysical security of wide-area monitoring, protection and control in a smart grid environment. J Adv Res 5(4):481–489
[65] Adhikari U, Morris T, Pan S (2016) WAMS cyber physical test bed for power system, cybersecurity study, and data mining. IEEE Trans Smart Grid 8(6):2744–2753
[66] Paudel S, Smith P, Zseby T (2016) Data integrity attacks in smart grid wide area monitoring. In: Proceedings of the 4th international symposium for ICS & SCADA cyber security research, Belfast, UK, 23-25 August 2016, pp 1-10
[67] Akyol BA (2012) Cyber security challenges in using cloud computing in the electric utility industry. DOE technical report by Pacific Northwest National Laboratory (PNNL). https://www.pnnl.gov/main/publications/external/technicalreports/PNNL-21724.pdf. Accessed 1 September 2012
[68] Weekes MA, Hydro M, Hydro KWM (2007) PMU challenges and performance issues. In: Proceedings of the IEEE power engineering society general meeting, Tampa, USA, 24–28 June 2007, pp 1–4
[69] Song H, Wu J, Wu K (2014) A wide-area measurement systems-based adaptive strategy for controlled islanding in bulk power systems. MDPI J Energies 7(4):2631–2657
[70] Johnson A (2017) Standards associated with synchrophasors. In: Proceedings of IEEE PES general meeting presentation. https://www.naspi.org/sites/default/files/201703/01_scejohnson_

Standards_Associated_with_Synchrophasor_s20161019. Accessed 12 August 2018
[71] Martin K (2015) Synchrophasor measurements under the IEEE standard C37.118.1-2011 with amendment C37.118.1a. IEEE Trans Power Deliv 30(3):1514–1522
[72] Ali I, Aftab MA, Hussain SMS (2016) Performance comparison of IEC 61850-90-5 and IEEE C37.118.2 based wide area PMU communication networks. J Mod Power Syst Clean Energy 4(3):487–495
[73] Retty HA (2013) Evaluation and standardizing of phasor data concentrators. Dissertation. Virginia Polytechnic Institute and State University
[74] Premerlani WJ, Kasztenny BZ, Adamiak MG (2006) System and method for synchronized phasor measurement. United States Patent Application Publication, US 2006/0247874 A1. https://patents.google.com/patent/US7444248. Accessed 30 June 2017
[75] IEEE power and energy society standard (2011) IEEE standard for synchrophasor data transfer for power systems. https://doi.org/10.1109/ieeestd.2011.6111222. Accessed 28 December 2011
[76] Phadke AG, Thorp JS (2017) Synchronized phasor measurements and their applications. Springer Science+Business Media, 2nd edn. https://www.springer.com/us/book/9783319505824. Accessed 30 June 2017
[77] Rihan M, Ahmed M, Beg MS (2011) Phasor measurement units in the Indian smart grid. In: Proceedings of IEEE conference on innovative smart grid technologies India (ISGT India), Kollam, India, 1–3 December 2011, pp 261–267
[78] NASPI Time Synchronization Task Force (2017) Time synchronization in the electric power system. NASPI Technical Report. https://www.naspi.org/sites/default/files/referencedocuments/tstf_electric_power_system_report_pnnl_2633_1march_20170.pdf. Accessed 3 August 2017
[79] C37.118-2005-IEEE standard for synchrophasors for power systems (2006) IEEE power and energy society standard. https://ieeexplore.ieee.org/document/1611105/, https://doi.org/10.1109/ieeestd.2006.99376. Accessed 3 August 2017
[80] Kezunovic M, Dutta P (2011) The role of data exchange standards in developing automated fault disturbance monitoring. In: Proceedings of 6th international workshop on deregulated electricity market issues in South-Eastern Europe (DEMSEE). https://pdfs.semanticscholar.org/f8c3/8c8d8aac32b6cbfa1d84948db977fc8d6a8e.pdf. Accessed 3 August 2017
[81] IEEE Power and Energy Society Standard (2011) IEEE standard for synchrophasor measurements for power systems. https://ieeexplore.ieee.org/document/6111219/, https://doi.org/10.1109/ieeestd.2011.6111219. Accessed 3 August 2017
[82] IEEE Power and Energy Society Standard (2014) IEEE guide for phasor data concentrator requirements for power system protection, control, and monitoring. https://ieeexplore.ieee.org/document/6514039/, https://doi.org/10.1109/ieeestd.2013.6514039. Accessed 3 August 2017
[83] Chai J, Liu Y, Guo J et al (2016) Wide-area measurement data analytics using FNET/GridEye: a review. In: Proceedings of power systems computation conference, Genoa, Italy, 20–24 June 2016, pp 1–6
[84] Eissa MM, El-Mesalawy MM, Liu Y et al (2012) Wide area synchronized frequency measurement system architecture with secure communication for 500kV/220kV Egyptian grid. In: Proceedings of IEEE international conference on smart grid engineering (SGE'12), Oshawa, Canada, 27–29 August 2012, p 1
[85] Liu Y (2014) FNET/GridEye. Technical document of Oak Ridge National Laboratory. https://web.ornl.gov/sci/renewables/docs/factsheets/FNET-GridEye-Factsheet.pdf. Accessed September 2014
[86] Stenbakken G, Zhou M (2007) Dynamic phasor measurement unit test system. In: Proceedings of IEEE power engineering society general meeting, Tampa, USA, 24–28 June 2007, pp 1–8
[87] Wang L, Burgett J, Zuo J et al (2007) Frequency disturbance recorder design and developments. In: Proceedings of IEEE power engineering society general meeting, Tampa, USA, 24–28 June 2007, pp 1–7
[88] Wang L (2010) Next generation frequency disturbance recorder design and timing analysis. Dissertation. Virginia Polytechnic Institute and State University
[89] Culliss JA (2015) A 3rd generation frequency disturbance recorder: a secure, low cost synchrophasor measurement device. Dissertation. University of Tennessee
[90] IEEE Power and Energy Society (2013) IEEE standard for intelligent electronic devices cyber security capabilities. IEEE power and energy society standard, https://doi.org/10.1109/ieeestd.2014.6704702. Accessed 28 May 2017
[91] IEEE Power and Energy Society (2014) IEEE standard cyber-security requirements for substation automation, protection, and control systems. IEEE power and energy society standard. https://doi.org/10.1109/ieeestd.2015.7024885. Accessed 29 May 2017
[92] IEEE Power and Energy Society (2011) IEEE trial-use standard for a cryptographic protocol for cyber security for substation serial links. IEEE power and energy society standard, https://doi.org/10.1109/ieeestd.2011.5715000. Accessed 29 May 2017
[93] Firouzi SR, Hooshyar H, Mahmood F et al (2016) An IEC 61850-90-5 gateway for IEEE C37.118.2 synchrophasor data transfer. In: Proceedings of 6th NASPI-ISGAN international synchrophasor symposium, Boston, USA, 17–21 July 2016, pp 1–5. Accessed 29 May 2017
[94] Mackiewicz R (2006) Overview of IEC 61850 and benefits. In: Proceedings of IEEE PES power systems conference and exposition, Atlanta, GA, 29 October–1 November 2006, pp 623–630
[95] International Electrotechnical Commission (2013) Common format for transient data exchange (COMTRADE) for power systems. IEC 60255-24 Part 24, https://doi.org/10.1109/ieeestd.2013.6512503. Accessed 2 March 2017
[96] SGIP (2010) Introduction to NISTIR 7628 guidelines for smart grid cyber security. The smart grid interoperability panel cyber security working group report. https://www.smartgrid.gov/files/nistir7628.pdf. Accessed 29 May 2017
[97] Sun CC, Liu CC, Xie J (2016) Cyber-physical system security of a power grid: state-of-the-art. MDPI J Electron 5(3):40
[98] Kezunovic M, Sprintson A, Guan Y et al (2012) Verifying interoperability and application performanceof PMUs and PMU-enabled IEDs at the device and system level. Power Systems Engineering ResearchCenter Final Project Report, 2018. https://pserc.wisc.edu/documents/publications/reports/2012_reports/T-43_Final-Report_Aug-2012.pdf. Accessed 14 November 2018
[99] Pacific Northwest National Laboratory, National Institute of Standards & Technology Team (2017) Synchrophasor data quality attributes and a methodology for examining data quality impacts upon synchrophasor applications—overview. NASPI technical report. https://www.nist.gov/publications/synchrophasordata-quality-attributes-and-methodology-examining-dataquality-impacts. Accessed 17 July 2017
[100] IEEE Power and Energy Society Standard (2013) IEEE guide for synchronization, calibration, testing, and installation of phasor measurement units (PMUs) for power system protection

and control. https://doi.org/10.1109/ieeestd.2013.6475134. Accessed 23 July 2018
[101] IEEE Power and Energy Society Standard (2010) IEEE standard for common format for event data exchange (COMFEDE) for power systems. https://doi.org/10.1109/ieeestd.2010.5638582. Accessed 23 July 2018
[102] Huang C, Li F, Zhou D et al (2016) Data quality issues for synchrophasor applications part I: a review. J Mod Power Syst Clean Energy 4(3):342–352
[103] Sarwat AI, Sundararajan A, Parvez I et al (2018) Toward a smart city of interdependent critical infrastructure networks. Sustain Interdepend Netw Chapter 3:21–45
[104] Sarwat AI, Sundararajan A, Parvez I (2017) Trends and future directions of research for smart grid IoT sensor networks. In: Proceedings of international symposium on sensor networks, systems and security, chapter 3, Lakeland, FL, USA, pp 45–61. https://doi.org/10.1007/978-3-319-75683-7
[105] Aminifar F, Fotuhi-Firuzabad M, Safdarian A et al (2014) Synchrophasor measurement technology in power systems: panorama and state-of-the-art. IEEE Access 2:1607–1628
[106] Zhang Y, Markham P, Xia T et al (2010) Wide-area frequency monitoring network (FNET) architecture and applications. IEEE Transa Smart Grid 1(2):159–167
[107] Yuill W, Edwards A, Chowdhury S et al (2011) Optimal PMU placement: a comprehensive literature review. In: Proceedings of IEEE power and energy society general meeting, Detroit, USA, 24–29 July 2011, pp 1-8
[108] Manousakis NM, Korres GN, Georgilakis PS (2011) Optimal placement of phasor measurement units: a literature review. In: Proceedings of international conference on intelligent system applications to power systems, Hersonissos, Greece, 25–28 September 2011, pp 1–6
[109] NERC (2010) Real-time application of synchrophasors for improving reliability. NERC technical report, pp 1–77. https://www.smartgrid.gov/document/real_time_application_synchrophasors_improving_reliability. Accessed 17 July 2017
[110] Wu H, Giri J (2006) PMU impact on state estimation reliability for improved grid security. In: Proceedings of 2005/2006 IEEE/PES transmission and distribution conference and exhibition, Dallas, USA, 21–24 May 2006, pp 1349–1351
[111] Terzija V, Valverde G, Cai D et al (2010) Wide area monitoring, protection, and control of future electric power networks. Proc IEEE 99(1):80–93
[112] Cokkinides GJ, Miliopoulos APS, Stefopoulos G et al (2007) Visualization and characterization of stability swings via GPS-synchronized data. In: Proceedings of 40th annual Hawaii international conference on system sciences, Waikoloa, USA, 3–7 January 2007, 120 pp
[113] Stenbakken G, Nelson T (2007) Static calibration and dynamic characterization of PMUs at NIST. In: Proceedings of IEEE power engineering society general meeting, Tampa, USA, 24–28 June 2007, pp 1–4
[114] Maaß H, Cakmak HK, Bach F et al (2015) Data processing of high-rate low-voltage distribution grid recordings for smart grid monitoring and analysis. EURASIP J Adv Signal Process. https://doi.org/10.1186/s13634015-0203-4
[115] Maass H, Cakmak HK, Suess W et al (2013) First evaluation results using the new electrical data recorder for power grid analysis. IEEE Trans Instrum Meas 62(9):2384–2390
[116] Castello P, Ferrari P, Flammini A et al (2015) A distributed PMU for electrical substations with wireless redundant process bus. IEEE Trans Instrum Meas 64(5):1149–1157
[117] Dua D, Dambhare S, Gajbhiye RK et al (2008) Optimal multistage scheduling of PMU placement: an ILP approach. IEEE Trans Power Deliv 23(4):1812–1820
[118] NASPI PRSVTT, NASPI DNMTT working group (2016) Categorizing phasor measurement units by application data requirements. Draft report. https://www.naspi.org/sites/default/files/201609/naspi_prsvtt_report_20141023.pdf. Accessed 17 July 2017
[119] Idaho National Laboratory (INL) (2016) Cyber threat and vulnerability analysis of the U.S. electric sector. Mission support center analysis report. https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf. Accessed 23 June 2018
[120] Reinhard K, Pinte B, Kirihara K et al (2015) Synchrophasor data quality activity research update. Trustworthy cyber infrastructure for the smart grid. https://tcipg.org/sites/default/files/rgroup/tcipgreading-group-spring_2015_02-27_0. Accessed 23 June 2018
[121] Armenia A, Chow JH (2010) A flexible phasor data concentrator design leveraging existing software technologies. IEEE Trans Smart Grid 1(1):73–81
[122] Zhu H, Shi Y (2014) Phasor measurement unit placement for identifying power line outages in wide-area transmission system monitoring. In: Proceedings of 47th Hawaii international conference on system sciences, Waikoloa, USA, 6–9 January 2014, pp 2483–2492
[123] Sundararajan A, Khan T, Aburub H et al (2018) A tri-modular human-on-the-loop framework for intelligent smart grid cyber-attack visualization. In: Proceedings of IEEE southeast conference, Tampa, USA, 18–22 April 2018, pp 1–8
[124] Beasley C, Venayagamoorthy GK, Brooks R (2014) Cyber security evaluation of synchrophasors in a power system. In: Proceedings of Clemson University power systems conference, Clemson, USA, 11–14 March 2014, pp 1–5
[125] Stewart J, Maufer T, Smith R et al (2011) Synchrophasor security practices. In: Proceedings of 14th annual Georgia Tech fault and disturbance analysis conference, Atlanta, USA, 9–10 May 2011, pp 1–11. https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6449_SynchrophasorSecurity_EE_20100913_Web.pdf?v=20150812-082045. Accessed 23 June 2018
[126] Srivastava AK (2015) Meeting PMU data quality requirements for mission critical applications. PSERC Webinar. https://pserc.wisc.edu/documents/general_information/presentations/pserc_seminars/announcements/2015_webinars/Srivastava_PSERC_Webinar_Nov_2015Announcement.pdf. Accessed 23 June 2018
[127] Zhu K (2013) Data quality in wide-area monitoring and control systems, PMU data latency, completeness, and design of wide-area damping systems. Dissertation. KTH Royal Institute of Technology
[128] Oleka EU, Khanal A, Osareh AR et al (2015) Exploring the challenging issues with synchrophasor technology deployments in electric power grids. Int J Energy Power Eng 9(9):1085–1088
[129] Esfahani MS (2014) Security analysis of phasor measurement units in smart grid communication infrastructures. Dissertation. University of Nebraska-Lincoln
[130] Landford J, Meier R, Barella R et al (2016) Fast sequence component analysis for attack detection in smart grid. In: Proceedings of 5th international conference on smart cities and green ICT systems (SMART-GREENS), Rome, Italy, 23–25 April 2016, pp 225–232. https://ieeexplore.ieee.org/document/7951353/
[131] Pal S, Sikdar B, Chow J (2016) Detecting data integrity attacks on SCADA systems using limited PMUs. In: Proceedings of IEEE international conference on smart grid communications

(SmartGridComm), Sydney, Australia, 6–9 November 2016, pp 545–550
[132] Pal S, Sikdar B (2014) A mechanism for detecting data manipulation attacks on PMU data. In: Proceedings of IEEE international conference on communication systems, Macau, China, 19–21 November 2014, pp 253–257
[133] University of Tennessee Knoxville (2012) Frequency disturbance recorder (FDR) installation guide. UT Knoxville User Guide Report. https://powerit.utk.edu/fdr/FDRInstallAndConfigGuide.pdf. Accessed 1 August 2017
[134] Fan X, Du L, Duan D (2017) Synchrophasor data correction under GPS spoofing attack: a state estimation based approach. IEEE Trans Smart Grid 9(5):4538–4546
[135] Almas MS, Vanfretti L, Singh RS (2017) Vulnerability of synchrophasor-based WAMPAC applications' to time synchronization spoofing. IEEE Trans Smart Grid 9(5):4601–4612
[136] Aman MN, Sikdar B (2016) Detecting data tampering attacks in synchrophasor networks using time hopping. In: Proceedings of IEEE PES innovative smart grid technologies conference Europe (ISGT-Europe), Ljubljana, Slovenia, 9–12 October 2016, pp 1–6
[137] Wu M, Xie L (2017) Online detection of false data injection attacks to synchrophasor measurements: a data-driven approach. In: Proceedings of the 50th Hawaii international conference on system sciences, pp 1–10. http://hdl.handle.net/10125/41544. Accessed 4 January 2017
[138] Pal S, Sikdar B, Chow J (2017) Classification and detection of PMU data manipulation attacks using transmission line parameters. IEEE Trans Smart Grid 9(5):5057–5066
[139] Mao Z, Xu T, Overbye TJ (2017) Real-time detection of malicious PMU data. In: Proceedings of 19th international conference on intelligent system application to power systems (ISAP), San Antonio, USA, 17–20 September 2017, pp 1–6
[140] Zhang J, Chu Z, Sankar L, et al (2017) False data injection attacks on phasor measurements that bypass low-rank decomposition. In: Proceedings of IEEE international conference on smart grid communications (SmartGridComm), Dresden, Germany, 23–27 October 2017, pp 96–101
[141] US Department of Energy (DOE) (2016) Advancement of synchrophasor technology in projects funded by the American recovery and reinvestment act of 2009. Office of electricity delivery and energy reliability report. https://www.energy.gov/oe/downloads/advancementsynchrophasor-technology-projects-funded-americanrecovery-and-reinvestment. Accessed 1 August 2017
[142] Huang Z, Kasztenny B, Madani V et al (2008) Performance evaluation of phasor measurement systems. In: Proceedings of IEEE power engineering society general meeting, Pittsburgh, USA, 20–24 July 2008, pp 1–8
[143] Stenbakken G, Huang H, Martin K et al (2007) PMU system testing and calibration guide. Technical report for the North American synchrophasor initiative, performance and standard task team. https://www.naspi.org/sites/default/files/reference_documents/pmu_system_test_guide_20071230.pdf. Accessed 1 August 2017
[144] Meliopoulos S (2007) Synchrophasor measurement accuracy characterization. Technical report for the North American synchrophasor initiative, performance and standard task team. https://www.naspi.org/node/657. Accessed 26 August 2007
[145] Taft J (2018) Assessment of existing synchrophasor networks. Pacific northwest national laboratory (PNNL) technical report. https://gridarchitecture.pnnl.gov/media/whitepapers/Synchrophasor_net_assessment_final.pdf. Accessed April 2018
[146] Kumar S, Soni MK, Jain DK (2015) Cyber security threats in synchrophasor system in WAMS. Int J Comput Appl 115(8):17–22
[147] Yu DY, Ranganathan A, Locher T et al (2014) Short paper: detection of GPS spoofing attacks in power grids. In: Proceedings of the 2014 ACM conference on security and privacy in wireless & mobile networks, Oxford, UK, 23–25 July 2014, pp 99–104
[148] Khan R, Albalushi A, McLaughlin K et al (2017) Model based intrusion detection system for synchrophasor applications in smart grid. In: Proceedings of IEEE power & energy society general meeting, Chicago, USA, 16–20 July 2017, pp 1–5
[149] Tong Y (2015) Data security and privacy in smart grid. Dissertation. University of Tennessee
[150] Lau F, Rubin SH, Smith MH et al (2000) Distributed denial of service attacks. In: Proceedings of IEEE international conference on systems, man, and cybernetics, Nashville, USA, 8–11 October 2000, pp 2275–2280
[151] Liu L, Esmalifalak M, Ding Q et al (2014) Detecting false data injection attacks on power grid by sparse optimization. IEEE Trans Smart Grid 5(2):612–621
[152] Zhang J, Domnguez-Garca AD (2014) On the failure of power system automatic generation control due to measurement noise. In: Proceedings of 2014 IEEE PES general meeting & conference exposition, National Harbor, USA, 27–31 July 2014, pp 1–5
[153] Hastings J, Laverty DM, Morrow DJ (2014) Securing the smart grid. In: Proceedings of 49th international universities power engineering conference (UPEC), Cluj-Napoca, Romania, 2–5 September 2014, pp 1–6

**Aditya SUNDARARAJAN** is a graduate research assistant pursuing his Ph.D. in electrical and computer engineering. He is working on the visualization of threats, vulnerabilities, and attacks on the distribution grid. He is also working on analyzing, modeling, and visualizing high-dimensional heterogeneous power and weather systems data under high penetration photovoltaic (PV) scenarios of smart grid at the distribution level, in a real-time manner, to provide dynamic and situation-aware decision-making support at sub-second speeds - for the human operators at the utility command and control centers. He is also conducting preliminary research on biometric threats and vulnerabilities, and associated cyber-security challenges. His bachelors was in computer science and engineering. His areas of interest include big data analysis, human-on-the-loop cybersecurity, smart grid cyber physical system (CPS), security concerns of biometric and wearable devices, and computer programming.

**Tanwir KHAN** was a graduate research assistant pursuing his master's in computer science. His specialization is computer engineering and data science, and has been involved in multiple projects on data analytics, programming and application developing in the areas of smart grid cybersecurity, reliability and renewable integration. He is currently working as a software developer for INFOTECH Soft INC which deals with genomic data. His role as a software engineer involves the data profiling and processing of the human genomic data using Apache Accumulo and Apache spark.

**Amir MOGHADASI** received the B.Sc. degree in electrical engineering from Shaded University, Tehran, Iran, in 2007, the M.Sc. degree in electrical engineering from Iran University of Science and Technology (IUST), Tehran, in 2009, and the Ph.D. degree in electrical engineering from Florida International University (FIU), Miami, USA, in 2016. Dr. Moghadasi worked as a postdoctoral research associate at Florida International University. He was the lead researcher at FPL-FIU Solar Research Center to lead a research study on analysis of the effects of real-time operating the 1.4 MW PV systems installed at the FIU on the Florida, Power and Light (FPL)

distribution circuit. His research interests are power electronics, design and control of power converters, high-penetration renewable systems, power quality, and application of computational intelligence techniques in power systems. Dr. Moghadasi is currently working as a lead traction power engineer at WSP USA.

**Arif I. SARWAT** (M'08, SM16) received his masters from University of Florida in 2005 and Ph.D. degree from the University of South Florida in 2010. Currently, he is an associate professor and director of FPL-FIU Solar Research Facility in the department of electrical and computer engineering at the Florida International University (FIU), where he leads the Energy Power and Sustainability (EPS) group. His research interests include smart grids, plug-in hybrid and electric vehicle (PHEV and EV systems), high penetration renewable systems, grid resiliency, large scale data analysis, advance metering infrastructure, smart city infrastructure and cyber security. Dr. Sarwat is the recipient of the NSF CAREER award in 2016, and recipient of multiple federal and industry research awards. He was the author/co-author of conference best paper awards at the resilience week in 2017 and a journal Best Paper Award in 2016 from Journal of Modern Power Systems and Clean Energy. Dr. Sarwat received Faculty Award for Excellence in Research and Creative Activities in 2016, College of Engineering and Computing Worlds Ahead Performance in 2016 and FIU TOP Scholar Award in 2015. Dr. Sarwat worked at Siemens for more than nine years, winning three recognition awards. He is chair of IEEE Miami Section VT and Communication since 2012.