

# Information and Communication Infrastructures in Modern Wide-Area Systems



Weikang Wang, Kaiqi Sun, Chujie Zeng, Chang Chen, Wei Qiu, Shutang You, and Yilu Liu

**Abstract** Information and communication infrastructures (ICIs) in modern wide-area systems handle the transmitting, receiving, and storing of high-speed, large-volume synchrophasor data. Such infrastructures are important components in modern wide-area systems. Although power systems are becoming rather complex, with the introduction of synchrophasor technology, the highly accurate, high-speed, widely deployed, and time-synchronized phasor measurement units (PMUs) are providing operators and auditors an unprecedented way to understand the complex power systems. Consequently, these advanced PMUs challenge the current information and communication infrastructures. This chapter reviews the basics, challenges, and visions of the ICIs in wide-area monitoring systems (WAMS). We will first overview some important wide-area ICI topics and share our experience in building an efficient, reliable, and secure distribution-level WAMS, FNET/GridEye. We will introduce some key technologies that ensure the efficiency and reliability of such a WAMS. Finally, some outstanding challenges and future directions of the contemporary ICIs are discussed and envisioned.

**Keywords** ICI · Phasor measurement units · WAMs · Wide-area systems · infrastructures · Wide-area power systems · Measurement systems

---

W. Wang · K. Sun · C. Zeng · C. Chen (✉) · W. Qiu · S. You · Y. Liu  
The University of Tennessee, Knoxville, TN, USA  
e-mail: [cchen75@utk.edu](mailto:cchen75@utk.edu)

Y. Liu  
Oak Ridge National Laboratory, Oak Ridge, TN, USA

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2021

H. Haes Alhelou et al. (eds.), *Wide Area Power Systems Stability, Protection, and Security*, Power Systems, [https://doi.org/10.1007/978-3-030-54275-7\\_3](https://doi.org/10.1007/978-3-030-54275-7_3)

# 1 Communication Infrastructures in Modern Wide-Area System

## 1.1 Introduction

Wide-area communication infrastructures (WACIs) are a series of cyber-physical components which act as the backbone of data transmission. In the WACIs, there are three fundamental elements, which are protocol, method, and scheme. A communication method defines the physical medium on which the data is transmitted. A protocol defines the way in which the data is formatted. Finally, a scheme specifies the overall architecture of a communication system and the directions of data streams in between. These components are integral to a WACI and they work together to ensure efficient and reliable transmission of wide-area measuring data. In the following sections, these components will be illustrated in detail.

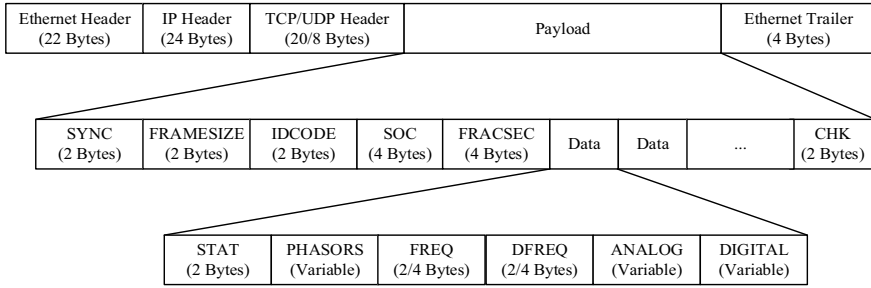
## 1.2 Communication Protocols

Communications protocols in wide-area systems define the formats in which the data are transmitted between a PMU and a phasor data concentrator (PDC). In the modern wide-area systems, several protocols including IEEE C37.118, IEC-61850-90-5, and Streaming Telemetry Transport Protocol (STTP) have been proposed and adopted in real operations. Communication protocols vary on their reliability, efficiency, security, etc. and are subject to specific use cases. This section will focus on three widely accepted communication protocols and give a comparison to demonstrate their pros and cons.

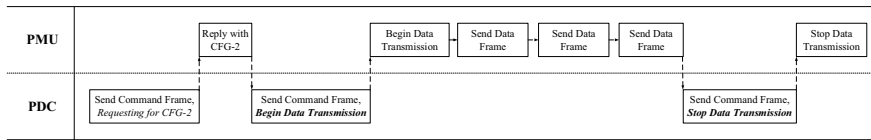
### 1.2.1 IEEE C37.118

The synchrophasor data exchange protocol IEEE C37.118 was published in 2005 [1]. Later in 2011, the standard was divided into two parts where IEEE C37.118.1 [2] defines the requirement for synchrophasor measurement and IEEE C37.118.2 [3] defines the synchrophasor data transmission format. In 2014, the IEEE C37.118.1a amendment [4] was published, which updated some performance requirements.

A PMU communicates with a PDC via binary frames. The IEEE C37.118.2 standard defines four frame types: configuration frame, header frame, command frame, and data frame. A configuration frame defines the format of the synchrophasor data stream. Hence, it must be received before data parsing. There are three types of configuration frames: CFG-1, CFG-2 and CFG-3. The first two are identical in structure but are used in different contexts. CFG-1 provides information about the device's reporting capability, indicating all the data that the device reports. CFG-2 indicates synchrophasor measurements that are currently being transmitted. CFG-3 is optional



**Fig. 1** Data frame structure of IEEE C37.118.2 protocol



**Fig. 2** Message exchange flow of IEEE C37.118.2 protocol

and indicates PMU characteristics and quantities being sent. Then, a header frame is supposed to transmit human-readable ancillary information, such as data sources, scaling, algorithms used and other related information. A command frame is used to control the behavior of an established connection. Possible commands include turn off transmission of data frames, turn on the transmission of data frames, send the header frame, send CFG-1 frame, etc. Finally, a data frame is used to transmit measurement data and a set of status bits. A data frame can be properly parsed only when an active configuration frame is present. A sample structure of the message in the IEEE C37.118.2 protocol is demonstrated in Fig. 1.

A typical IEEE C37.118.2 message exchange flow between a PMU and a PDC is shown in Fig. 2. First, the PDC sends a command message requesting the configuration frame. Then, the PMU replies with the requested configuration frame. Afterward, the PDC sends out the command frame asking for data transmission. The PMU responds by flushing data frames to the PDC continuously until it receives the turn-off command from the PDC.

**1.2.2 IEC 61850-90-5**

IEC 61850 standard [5] is the de-facto standard for substation automation. In 2012, IEC 61850-90-5 standard [6] was introduced as the synchrophasor data transmission protocol within IEC 61850 stack. IEC 61850-90-5 standard is usually preferred when IEC 61850 is already adopted. It employs existing elements of IEC 61850 and adopts IEEE C37.118.1, which defines the measurement requirements.

In IEC 61850, sample values (SV) and generic object-oriented substation events (GOOSE) are two types of real-time communication services. SV is used to exchange streaming data like phasor measurements while GOOSE is used to transmit status and control commands. SV and the GOOSE can only be used within a local area network (LAN) as they are Ethernet layer messages [7]. However, a WAMS requires communication over wide-area network (WAN). The routable SV and GOOSE then are introduced and termed as R-SV and R-GOOSE respectively. User Datagram Protocol (UDP) is usually used due to the need for multicasting. Control blocks are used to control the message flow. The control blocks for R-SV and R-GOOSE are termed as Routed Multicast Sampled Value Control Block (R-MSVCB) and Routed GOOSE Control Block (R-GoCB) respectively.

The structure of R-SV message is shown in Fig. 3, where the Sample Value Application Protocol Data Unit (SV APDU) and Application Service Data Units (ASDU) are expanded. A typical communication procedure is demonstrated in Fig. 4. First, the PDC sends a Manufacturing Message Specification (MMS) request message asking for PMU information. After the PDC receives the response, it sends out an R-MSVCB to start the data transmission process. After receiving this message, the PMU continuously sends R-SV messages to the PDC until it receives another R-MSVCB requesting the end of data transmission.

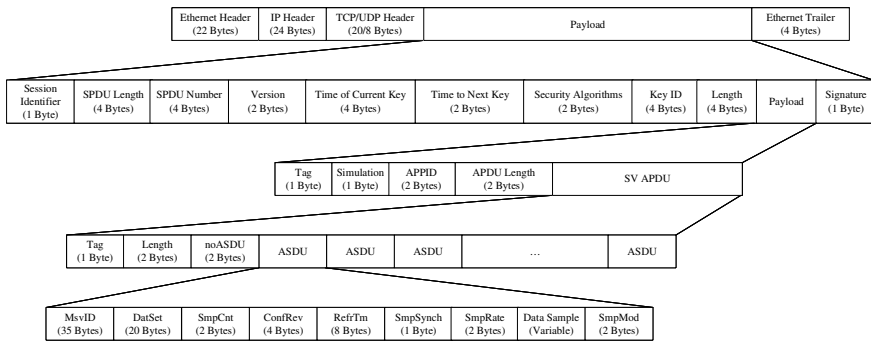


Fig. 3 R-SV frame structure of IEC 61850-90-5 protocol

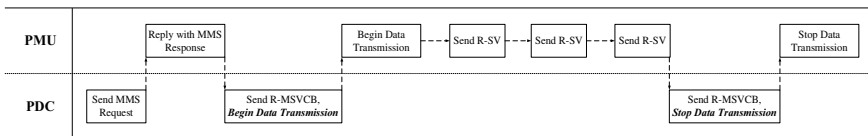


Fig. 4 Message exchange flow of IEC 61850-90-5 protocol

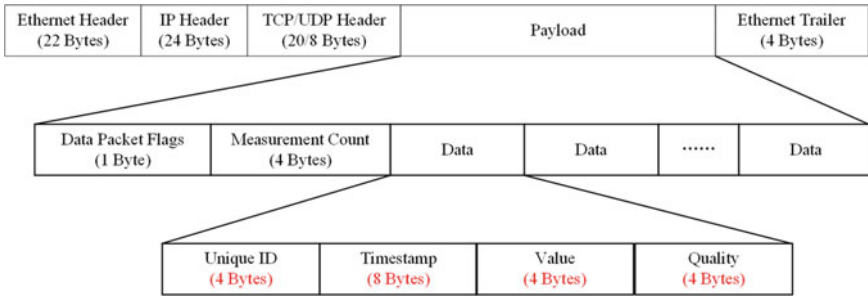


Fig. 5 STTP data frame structure

### 1.2.3 Streaming Telemetry Transport Protocol

The data losses and delivery latencies of IEEE C37.118 and IEC TR 61850 will greatly increase when the frame size approaches 32 K byte [8]. To address this issue, a signal-based protocol—the Streaming Telemetry Transport Protocol (STTP) is designed, which can send the compressed data instead of the raw data in binary. Figure 5 shows the latest version of data frame of STTP, where the length of each element before compression is colored in red. In this version, more than 65 K measurement values can be transmitted in one frame. In the payload of the frame, the data packet flag is the indicator representing the data payload format, which is omitted when UDP encryption is enabled with the UPDATE CIPHER KEYS command. The number of measurements is recorded in the measurement count field. The data block consists of four parts- a Unique ID that indicates a measurement, a timestamp, a measurement value, and a quality flag.

STTP uses lossless algorithms to compress the raw data. When it is used over UDP, the Gzip algorithm is used to compress the payload. For STTP TCP compression, a time-series special compression (TSSC) is implemented to compress the data [9]. The TSSC can compress streaming time-series data quickly. It works by first find the different bits between two values with XOR calculation. Then, Only the bits that have changed since the last measurement and the code word that represent the length of the calculated bits are stored. This method performs well when the data has a certain trend, for example, when the sampling rate is very high so the difference between every two values is small.

### 1.2.4 Comparison of Communication Protocols

In terms of structure, both IEEE C37.118.2 and IEC 61850-90-5 are frame-based and must transmit the configuration prior to the data transmission. However, STTP is measurement-based and its configuration differ from one data packet to another. Since variable configuration introduces extra overhead, STTP consumes higher bandwidth than the other two. However, STTP supports compression. The experiment shows

**Table 1** Comparison of wide-area communication protocols

Feature	IEEE C37.118.2	IEC 61850-90-5	STTP
Structure	Frame-based	Frame-based	Dynamic
Efficiency	Good	Fair	Good with TCP Fair with UDP
Scalability	Limited	Limited	Good
Compression	Yes/No	No	Yes/No
Encryption	No	Yes	Yes
Multicast supported	Yes	Yes	Limited

that when using TCP and stateful compression, STTP consumes bandwidth at least 30% less than IEEE C37.118 [9]. Both IEEE C37.118.2 and IEC 61850-90-5 have a 65 K bytes frame size limitation, as a result, no more than 6700 uniquely identifiable measurements can be transmitted in one connection [9]. On the contrary, STTP does not have such a limitation, making it more scalable. In terms of security, IEEE C37.118.2 only utilizes a cyclic redundancy check (CRC) codes to ensure data integrity, which can be easily modified by the intruder [10]. IEC 61850-90-5 ensures integrity with asymmetric cryptography and ensures confidentiality with symmetric encryption [6, 10]. STTP uses Transport Layer Security (TLS) to provide security. Table 1 summarizes the differences of three protocols.

### 1.3 Communication Methods

For now, the communication methods that could be used in synchrophasor data transfer could be basically classified into two categories: wired communication and wireless communication.







The wired communication is the most common communication technology used in the world. The main media in use for wired communication are power supply cable and optical fiber [11]. The wired communication relies on the physical circuit to exchange data, thus it could offer high reliability, huge bandwidth and high protection capacity against interference [12]. However, the wired communication also has some disadvantages due to its physical constraint. With the development of communication technology, wireless communication witnesses a continuous increasing share in the communication mix. The most popular media for wireless communication are cellular, microwave, and satellite. Table 2 shows the feature comparison between the wired communication and wireless communication on mobility, cost, expansion, and remote-access capability.

According to the different media adopting, the communication methods for synchrophasor data transfer could be summarized in Table 3.

**Table 2** The feature comparison between the wired communication and wireless communication

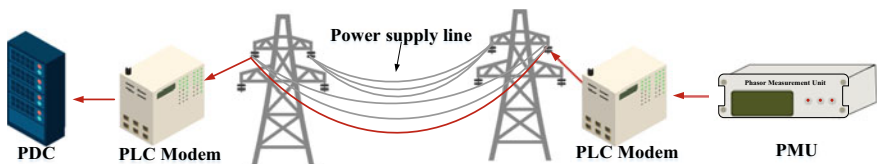
	Mobility	Cost	Expansion	Remote access capacity
Wired communication	Limited by cable	High cost (physical media depending & installation cost)	Hard	weak
Wireless communication	Not limited to the physical location	Low cost (easy deployment & maintenance-free)	Easy	Strong (could be deployed in forest or hilly terrains)

**Table 3** The communication method for synchrophasor applications

Synchrophasor communication method	Wired communication	Power line communication	 or 
		Optical fiber communication	
	Wireless communication	Cellular communication	
		Microwave-based Communication	
		Satellite communication	

### 1.3.1 Power Line Communication (PLC) for Synchrophasor Data Transfer

The PLC technology uses standard power supply cables to realize Synchrophasor data transfer between two PMUs. The structure of the WAMS using PLC technology to achieve synchrophasor data transfer could be depicted as Fig. 6.



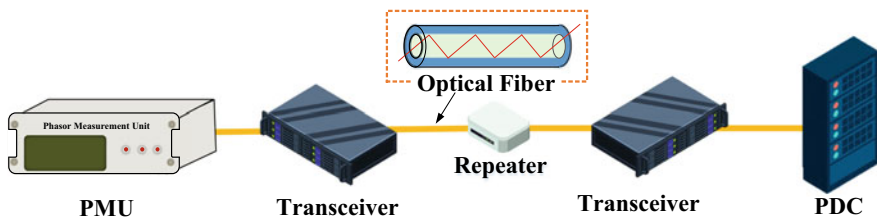
**Fig. 6** The PLC for synchrophasor application

PLC technology avoids additional network cables installation, it provides the easiest and economical means for the installation and deployment of the construction system. There are two types of PLC technologies: narrowband PLC (NB-PLC) and broadband PLC (BB-PLC). The NB-PLC, which is also named low-speed PLC (LS-PLC), could offer a nominal speed of few kilobytes per second and normally could be connected to cost-effective electronic equipment in a simple way. The BB-PLC, which is also named high-speed PLC (HS-PLC), could offer a nominal speed from Mb to hundreds of Mb per second. In most of the synchrophasor applications, the BB-PLC is adopted as its communication method for data rates requirements. However, PLC technology also has some disadvantages. The noisy background is serious in the power supply cables. Thus, the communication channel of the PLC is difficult to be modeled. In addition, the fading and interference of the PLC are severe in practice so that it is not suitable for higher bandwidth synchrophasor applications. For now, the PLC methods are usually working with other wireless communication methods such as cellular communication or microwave communication to provide a hybrid communication solution for synchrophasor applications.

### 1.3.2 Optical Fiber-Based Communication (OFC) for Synchrophasor Data Transfer

The OFC has been widely used in telephone signals transmitting, cable television signals transmitting, and internet communication. The OFC uses the optical fiber to send the pulses of infrared light to realize the data transfer from PMUs to PDC. The typical structure of the WAMS using OFC technology to achieve synchrophasor data transfer could be depicted as Fig. 7.

Compared to the PLC method, the OFC has higher data rates, lower attenuation, higher reliability, and negligible interference. In spite of having several advantages, due to its physical constraints, the OFC technology still suffers from many disadvantages, such as high installation and maintenance costs, potential risk of stolen or damaged, and expansion issues.

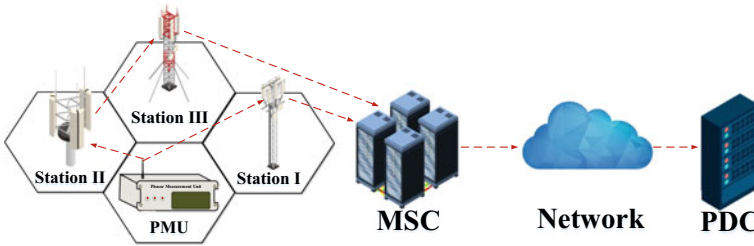


**Fig. 7** The OFC for synchrophasor application



**Table 4** Data rates of different cellular technologies for synchrophasor applications

Cellular technology	Data rates
General Packet Radio Service (GPRS)	$\leq 114$ Kbps
Enhanced Data rates for GSM Evolution (EDGE)	$\leq 384$ Kbps
Universal Mobile Telecommunications (UMTS)	$\leq 2$ Mbps
High-Speed Packet Access (HSPA)	Up to 384 Kbps
Long Term Evolution-Advanced (LTE-A)	Up to 384 Kbps



**Fig. 8** The cellular communication for synchrophasor application

### 1.3.3 Cellular Communication for Synchrophasor Data Transfer

The cellular communication method is the most common wireless communication method in the world. The data cellular communication network has been deployed over most of the inhabited land area of Earth. Due to the high proliferation of the cellular communication infrastructure, it has been regarded as an economic alternative for synchrophasor applications. The data rates of different cellular technologies for synchrophasor applications are shown in Table 4 [13].

The typical structure of the WAMS using cellular communication technology to achieve synchrophasor data transfer could be depicted as Fig. 8.

As shown in Fig. 8, the cellular communication system is comprised of cellular stations, mobile switching centers (MSC) and cellular networks. The shared nature of the cellular communication system is an advantage. However, it is unacceptable for the synchrophasor applications due to security considerations. In addition, the uninterrupted communication of cellular communication is difficult to be guaranteed, but it is a forced requirement for mission-critical applications.

### 1.3.4 Microwave-Based Communication for Synchrophasor Data Transfer

The microwave-based communication system could realize the several Gbps data rates, which could cater to the demands of the synchrophasor data transfer. The

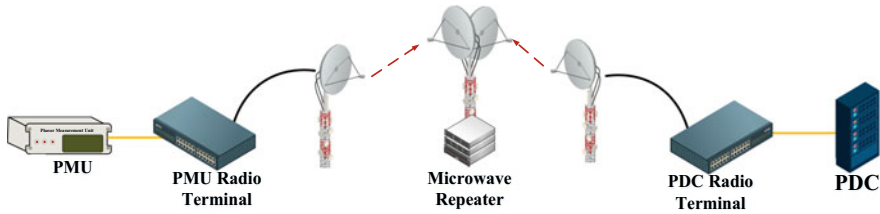


Fig. 9 The microwave-based communication for synchrophasor application

typical structure of WAMS using microwave-based communication technology to achieve synchrophasor data transfer could be depicted as Fig. 9.

The process of microwave-based communication is similar to the OFC except it is wireless communication. Microwave-based communication has a very large information-carrying capacity due to its high-frequency characteristic. In addition, the interference of microwave-based communication is also negligible. However, the main disadvantage of microwave-based communication is that the signal propagates in space is susceptible to cyber-physical attacks, which significantly affects its reliability and security.

### 1.3.5 Satellite Communication for Synchrophasor Data Transfer

Satellite communication is a prospective solution for synchrophasor data transfer. Compared to other communication methods, satellite communication could provide uninterrupted communication for unaffected by natural disasters due to its communication equipment is in space. The typical structure of the WAMS using satellite technology to achieve synchrophasor data transfer could be depicted as Fig. 10.

The communicating process of the satellite communication system is similar to microwave-based communication. The PMUs collect the phasor measurements data from the power system and compress the data as packages. The main disadvantage of the satellite communication system is its communication delay, besides, the antenna for satellite signal receiving is quite expensive, which limits the large-scale promotion of the satellite communication methods in the synchrophasor applications.

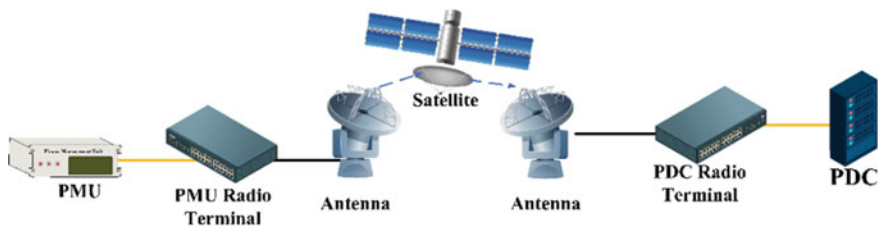


Fig. 10 The satellite communication for synchrophasor application

## 1.4 Communication Requirement

The synchrophasor applications require high reliability of the communication channel, to provide uninterrupted synchrophasor data measurement for the system operators to help with monitoring the status of the modern power grid in real-time. The primary requirements of communication methods choosing for synchrophasor data transfer in WAMS are throughput, bandwidth, time delay, and reliability.

- Throughput

The throughput is a bottleneck for the synchrophasor data transfer in the WAMS. The throughput represents the average data delivered per second, which is determined by measuring the data transfer speed at a specific time. The throughput must be considered as primary factors in the WAMS communication system design to build a reliable communication channel while controlling the cost in a reasonable scope.

- Bandwidth

The higher bandwidth of communication methods adopted for synchrophasor applications is required to guarantee the large volume synchrophasor data transfer in the WAMS. The bandwidth is defined as how much data can be sent over a specific network connection per give unit time [14]. The bandwidth design in the WAMS should keep enough redundancy for future synchrophasor applications development.

- Time delay

Time delay, i.e. latency, is one of the most stringent requirements for the communication system in the WAMS. Time delays are caused by communication disturbances or data alignment. The time delay could be classified as, according to the root cause, transducer delays, the propagation delay, processing delay, communication link transmission delay and data alignment delay. In general, the permissible time from PMUs to PDC is 20 ms, If the PDCs also need to transfer data to Central PDCs, an extra 40 ms is permitted from PMUs to the central PDCs. The WAMS requires a short time delay to support the local area and wide area real-time response control and protection [15]. However, the time delay requirements are subject to the actual application types. Table 5 lists the communication time delay requirement of some typical synchrophasor applications [17].

**Table 5** Communication time delay requirement for synchrophasor applications

Synchrophasor application	Communication delay (ms)
State estimation	100
Generator synchronization	50
Intelligent scheduling	50
Oscillation control	200
Islanding	50

**Table 6** Reliability comparison between different communication methods

Communication method	Throughput	Time delay (ms)	Bit error rate
Power line communication	256 kbps ~ 2.7 Mbps	150–350	$<10^{-2}$
Optical Fiber communication	10 Gbps	100–150	$10^{-15}$
Wireless communication	75 mbps	100–150	$10^{-7}$ – $10^{-12}$
Satellite communication	256 kbps–1 Mbps	1000–1400	$10^{-7}$

- Reliability

The reliability of communication is the backbone of the WAMS for providing uninterrupted, real-time monitoring, protection, and control of the power system. The throughput, time delay and bandwidth rate support the WAMS operating at a prescribed level of reliability. The bit error rate is usually to measure WAMS reliability. Table 6 indicates the throughput, time delay, and bit error rate of various communication methods in the WAMS to show their reliability comparison.

## 1.5 *Advanced Topic for Communication Infrastructure: Cybersecurity*

### 1.5.1 Challenges of Cyber Attacks

Nowadays, with an increasing number of PMUs, PDC and other types of power electronic devices in the power system, the communication infrastructure of WAMS is confronted more challenges including safe operation, cybersecurity, and data quality. For example, it is reported that more than 360 cyber-physical attacks happened during 2011 and 2014 according to the Energy Department in the USA [18]. Additionally, the safe operation of the power system is threatened by multiple aspects. At the physical level, the GPS signal can be spoofed thereby increasing the error of synchronous measurement. At the communication level, the denial of service and man-in-the-middle attacks cause erroneous failures by leveraging the knowledge of grid structure.

The synchrophasors support a two-way communication channel. Synchrophasor data measurement values flow from the power devices to the control center and server. Then the control signals flow in the other direction. The protocol used by the device helps the transmission and integration of data. However, the vulnerability of the protocol puts the data security in the public eye. In the IEEE C37.118, the packet and the CRC code can be modified and transmitted to the receiver. Thereafter, the availability and confidentiality of the data will be changed. In the communication system, some primary attacks include

- Denial of service (DoS)

The power system network resources, such as the IP address and bandwidth, are controlled by the DoS attackers. Legitimate users will be denied access to the server. The DoS attacks control multiple devices and machines, making the network channel blocked or dropped.

- Man-in-the-middle (MITM)

The attackers impersonate the other end of a legitimate protocol session between the server and a legitimate client. In the WAMS, the MITM would happen between PDC and PMUs. The destinations and the packet of the PMU can be modified by the MITM attacker. Meanwhile, the PDC can be deceived using fake certificates. In this case, the entire PMU data system will be chaotic.

- Delay

When there is a lot of information redundancy in the network, the useful bandwidth and throughput of the routers will be limited. In this case, the measurement synchrophasor data need to wait longer to transfer to the target device, resulting in the data loss and real-time control of the grid.

### 1.5.2 Remedies to Cyber Attacks

To address the challenge of cybersecurity, different strategies are proposed to decline the potential damage. Specifically, the solutions can be summarized as follows:

- DoS attack Countermeasures

To detect the DoS attack, the “air-gapped” network may provide a solution because it is completely isolated from the local machine. However, the construction of such a separate network requires separate infrastructure, thereby increasing costs. Some other methods, such as anomaly detection method using wavelet analysis and cumulative sum [16], is used to detect anomalous traffic.

- Man-in-the-middle (MITM)

The primary means to prevent this MITM attack is to check and authenticate the client and the server. One of the commonly used certificates is X.509, the devices and system can communication only after passing authentication. The public key cryptography is used to prevent MITM attack [19].

- Delay

To address the delay attack, it is reasonable to use the new IP Multicast protocols. This IP multicast can minimize packet replication, which can provide higher bandwidth.

Here, a tree construction model is used to minimize the invalid synchrophasor data, this tree structure is sensitive to the delay [20].

## ***1.6 Advanced Topic for Communication Infrastructure: Data Compression***

### **1.6.1 Challenges of Communication Efficiency from Advanced PMUs**

The performance of communication systems has significant effects on the WAMS. To build an efficient and secure PMUs communication, some factors that challenge PMU communication should be addressed. These factors include

- The high-density deployment of PMUs

The number of PMUs has been growing rapidly with the development of WAMS [21]. The traffic of data stream increases with the increasing deployment of the PMUs, which challenges the network bandwidth limit of WAMSs.

- High reporting rate

The reporting rate of PMUs can reach up to 1440 Hz, depending on the phasor calculating algorithms. In an extreme case, several terabytes of data may be generated per day, causing an unprecedented burden for servers to digest it [22].

- Data communication delay

Since most of the devices accommodated in the WAMS are executed in real-time, communication delay occurs in PMU measurement. The large volume of data puts pressure on bandwidth, which greatly increases the delay [23]. Large communication delays will deteriorate the reliability and accuracy of data [24].

- Data loss

Data losses are becoming serious due to the old PMUs and the incapable of the network to accommodate high sampling rate PMUs [25]. This can lead to harmful consequences such as affecting the performance of PMU-based control and closed-loop control [25].

### **1.6.2 Data Compression for Efficient Communication**

Data compression is the process of efficiently encoding data to reduce the number of bits required to transmit or store data. An intelligent data compression algorithm requires a prior understanding of the characteristics of the original data, in which

some patterns, e.g. repeated data, can be reduced [26]. The compression ratio (CR) is the primary indicator to represent the efficiency of data compression, which can be calculated by (1).

$$CR = \frac{\textit{Original Data}}{\textit{Compressed Data}} \quad (1)$$

Data compression methods can generally be divided into lossy and lossless data compression. The lossy data compression may incur an irreversible loss of data information, but it may achieve a much higher CR. Therefore, lossy compression methods are most used to compress multimedia data, where some loss of data quality is tolerable. Lossless data compression methods allow data to be reconstructed without any loss, although the CR may be sacrificed. These methods are adopted when a high data accuracy is required. Since the WAMS ICIs have stringent requirements for data accuracy, here, we only discuss some lossless methods.

- Entropy coding

Entropy coding, such as Huffman coding and arithmetic coding, is independent of the specific characteristics of the data. It replaces each symbol with a sequence whose length depends on how frequently the symbol appears in the original data set [27]. Huffman coding is the mostly used entropy coding method. However, entropy coding does not work well with streaming data since it needs to get the whole data and construct the coding tree [28]. Additionally, errors in the coded sequence of bits will tend to propagate when decoding.

- Bit-wise difference coding

As STTP provides a bit-wise coding method, which compares each value with previous values by bit., it performs well with streaming data. However, since the values are dependent on each other, the error propagation will be even serious compared with entropy coding as all the values followed by the wrong bits will be damaged.

To gain higher CR, a preprocessing is usually necessary for raw data before compression [29]. This step is known as “data prediction”, which can reduce the variance of data by the prior knowledge of the system [30, 31]. By doing this, a to-compress value is compared with a predicted value instead of the original value that is supposed to be compared. If the predictor is good enough, the errors will fall within a tight range near zero, yielding a highly repetitive pattern so that is can be reduced. The prediction step can be roughly divided into linear prediction and non-linear prediction. The linear prediction is used when a linear relationship exists between consecutive data points, e.g. phase angle. As opposed to it, non-linear predictions may fit other signals, e.g. point-of-wave, considering time and other parameters [30, 32].

### 1.6.3 Open Topics for Data Compression

Although many efforts have been done for PMU data compression, there are still some open issues such as real-time compression and the trade-off between CR and data accuracy. First, offline compression could result in severe congestion in the communication system due to the huge data volume. However, the real-time data compression methods generally have large sampling window and inaccurate measurement during disturbances. This can lead to long delays or packet loss [33]. How to implement and optimize real-time compression should be deeply investigated. Lossless data compression algorithms are preferred in the PMU level to maintain data reliability [30]. However, the Lossy algorithms can have much higher CRs. How to maintain data accuracy without sacrificing CR for high-resolution data still needs to be studied.

## 2 Information Infrastructures in Modern Wide-Area Systems

### 2.1 Introduction

Wide-area information infrastructures (WAI) provide critical functionalities to collect, process, store, and distribute information. In this verse, the data center architecture, data management, and data center security are discussed. A data center architecture specifies a structure of the information infrastructures from a high-level and defines the data streams from the PMUs to control centers. Data management includes the storage and distribution of measurement data and analytical results. Finally, the data center security covers basic topics including firewalls, access control, etc.

### 2.2 Information Infrastructure Architecture

Information architectures mainly fall into two categories, centralized and decentralized [13]. In a centralized architecture, all PMUs reports to one central control station. The advantages of a centralized communication architecture are simple topology and low cost. However, the reliability of centralized communication architecture is worse than the decentralized architecture since the failure of the single control station can be unaffordable. In decentralized communication architecture, there is more than one control stations. Compared to the centralized communication architecture, decentralized communication architecture is more robust, but the installation and maintenance cost may be much higher due to the complexity of the communication architecture. Generally, the choice of communication architecture should consider requirements such as efficiency, reliability, security, etc. Figures 11 and



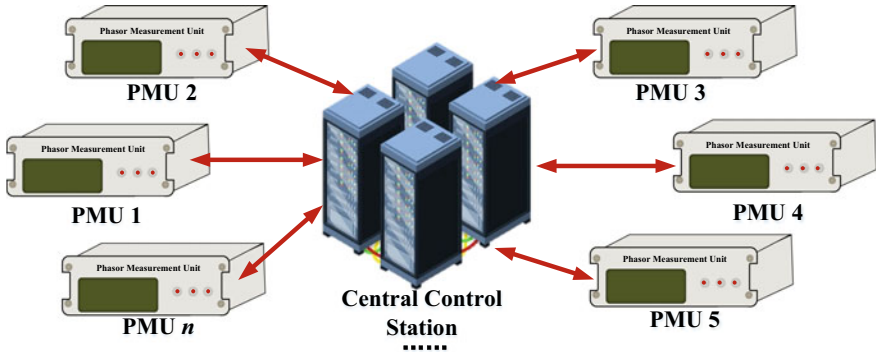


Fig. 11 Centralized information infrastructure

12 demonstrate the centralized and the decentralized communication architectures, respectively.

A generic information infrastructure architecture is demonstrated in Fig. 13. In Fig. 13 a decentralized architecture is employed, where each local control station operates independently and streams data to others as a client. Heterogeneous methods are adopted for the PMU to control center communication. Within the control center, multiple PDCs that communicate directly with the data server, and a load balancer may increase the capability of digesting large amounts of data in a distributed manner. For security, PDCs only push data into a short-term data storage server, then such a server periodically flushes data into another server for long-term data archive. Moreover, a caching server acts as a high-performance interface for data access. For performance, PDCs also push the same data into the data cache server while they write into the short-term data server.

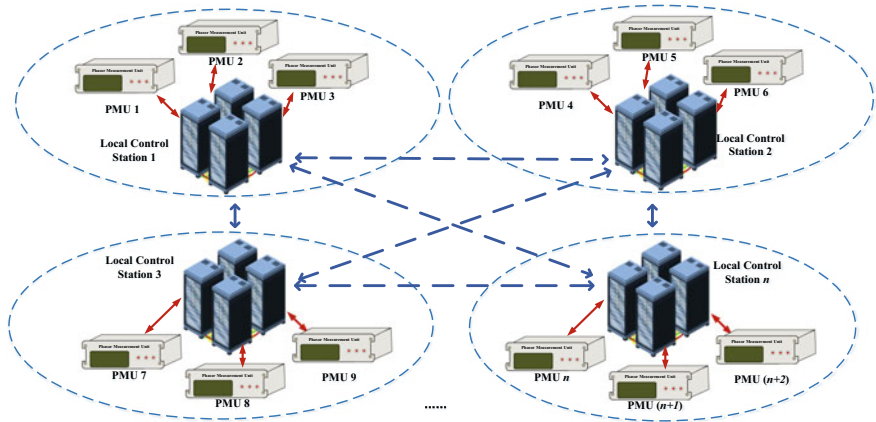


Fig. 12 Decentralized information infrastructure

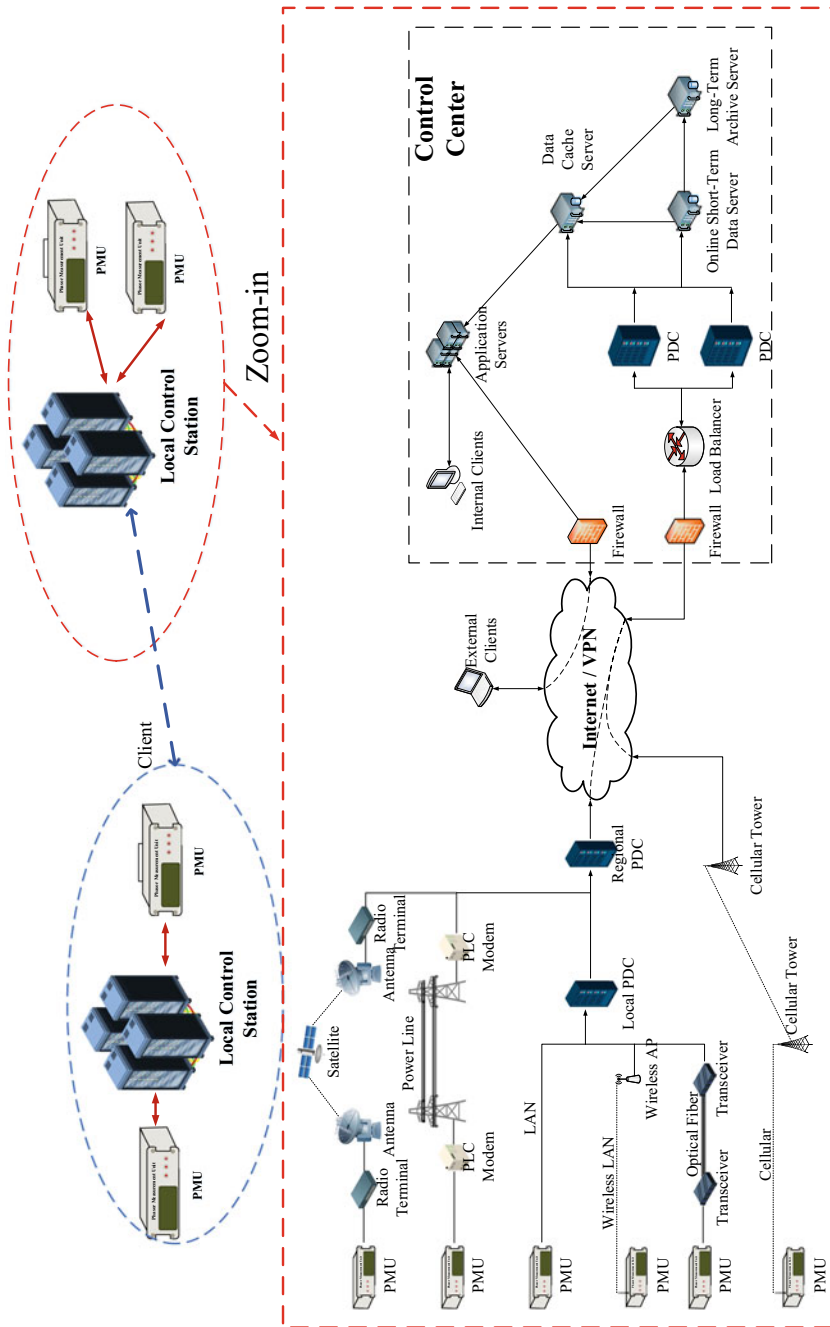


Fig. 13 A generic architecture of a wide-area information infrastructure

## 2.3 Data Center Management

The main purpose of the contemporary WAMSs is to provide accurate and large-volume measurements of electrical quantities to demonstrate the power system dynamics. With the fast development of synchrophasor technology, to properly manage the synchrophasor data becomes a rather important issue for control centers nowadays. From the functionality standpoint, data center management consists of data storage, data warehousing, and data center security.

### 2.3.1 Data Storage

#### Storage Method

Storage method defines the binary representation of the data in a computer system. In general, data storage can be implemented in three methods, relational database, non-relational database, and formatted files. The relational database is a mature technology, which is primarily used to permanently store structured data. Relational databases have advantages including well-defined structure, efficient data manipulation (small volume), etc. Relational databases can provide reliable storage, but its data is not directly readable by human-being. A database management system (DBMS) may be required to manage such a database and its data. A known issue of relational databases is the deterioration of insertion efficiency under large-volume data due to the reading of a whole large page [34], which makes it difficult to storage large-volume PMU data in WAMSs. However, formatted files can provide straightforward views of the collected data and are directly readable by human-being. Another advantage of this method is it provides better extensibility. For example, once defined, a relational database may be difficult to change due to its defined relational structure, which, in return, makes adding new measurement types difficult. However, new measurements can be easily added into the formatted files by creating new columns without altering the relational structure. The disadvantages of the formatted files are also obvious. Since they usually store data in plain, formatted files, the sacrifice of storage efficiency is usually inevitable. Moreover, the plain text format usually takes up larger space due to a lack of encoding. It is worth to note, in recent years, non-relation databases have been proposed and developed to combine the advantages of the relational databases and formatted files. Non-relational database exploits advanced data structures to efficiently store the time-series data but also keep acceptable extensibility. The insertion efficiency in non-relational databases is ultra-high because it does not require the reading of a whole large page, but a small immutable batch [34]. To sum up, relational databases provide good features to handle the storage of structured and small-in-size data, which is an ideal storage method for the analytical results [35]. As opposed to it, non-relational databases provide ultra-high

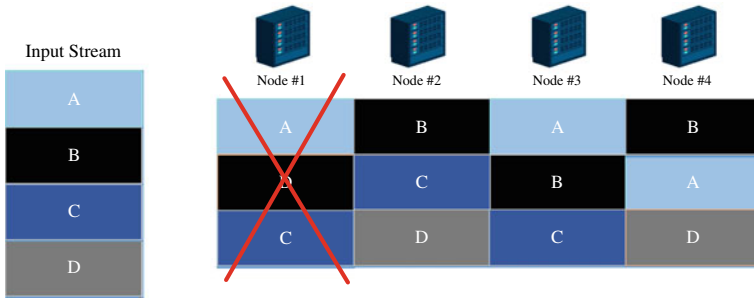
**Table 7** Performance comparison of storage methods

	Relational database	Non-relational database	Formatted files
Reliability	High	High	High
Efficiency	Medium	High	Medium
Extensibility	Low	Medium	High
Space	Low	Low	Medium
Scenario	Analytical results	Timeseries measurements	Timeseries measurements

data manipulation efficiency and they are widely adopted to store real-time, large-in-size PMU data [46]. Table 7 compares formatted files and databases on various matrices.

### Storage Scheme

The storage scheme defines how the data is stored across the information system. Typically, there are mainly 3 storage schemes in contemporary WAMS. First, a single machine scheme can provide the easiest and most direct way to store the data. This scheme is usually adopted in a simple client–server paradigm. Its advantage is simplicity since the administrator maintains only one machine. However, its disadvantage it cannot reliably store the data and the failure of the machine can be immediately unaffordable to power companies. Second, a multi-machine scheme provides better reliability by storing the data in a simultaneous, fully redundant manner. However, the scheme brings some other issues. First, the cost to set up a multiple-machine data storage system can be big. Since each machine stores a complete copy of data, it is expected to have advanced configurations to properly handle the data. When the number of machines increases, the cost could be unaffordable for users. Secondly, the fully redundant strategy may be unnecessary and could be a waste of storage resources. Finally, a cluster scheme can more efficiently utilize the storage resources. It utilizes a series of conventional computers, employing a partial overlapping strategy to store massive-volume data. A single machine is referred to as a node in the cluster and it only stores a small chunk of data. Furthermore, a chunk of data is replicated by  $n$  times and sent to  $n$  node when it is received from the PMU. Figure 14 demonstrates the effectiveness of the cluster scheme. In Fig. 14, the input stream is segmented as 4 data chunks (A, B, C, D) and each data chunk is replicated by 3 times. As is seen, although Node #1 goes offline due to a hardware failure, other nodes can still ensure the integrity of the input stream. The cluster scheme resolves the issues brought by the naïve multi-machine scheme and it is widely adopted in many industries nowadays [36].



**Fig. 14** The cluster data storage scheme

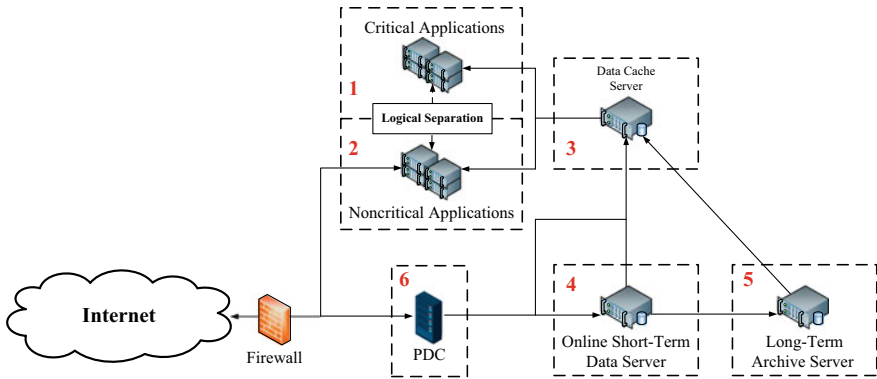
### 2.3.2 Data Warehousing

A data warehouse is a system that provides functionalities including data reporting, data analysis, and business intelligence. Data warehousing is an integral part of the modern WAMS, and it serves as a fundamental component for monitoring, operation, analysis, and compliance for various entities.

#### Data Reporting

A data reporting system receives a query request from a user and prepares the requested data. A data reporting system is an important component in a WAI since many operations in the control room are data-driven. In general, data reporting in modern WAMSs can be categorized as online reporting and offline reporting. Online reporting can support various real-time WAMS applications including monitoring, control, analytics, alarms, etc. To support such real-time WAMS applications, an online reporting system is required to have low latency, high availability, and high resiliency, although its throughput can be small. Offline reporting supports other analytical applications including post-event analysis, compliance determination, transmission planning, etc. As opposed to an online reporting system, an offline reporting system is required to have a large throughput to efficiently query large-volume data. However, there are usually low requirements for latency, availability or resiliency.

In modern WAMS, data reporting systems are implemented via various schemes to meet business requirements. An online data query usually requests a small amount of data but the tolerance for latency is low. To meet this requirement, an online data reporting system may utilize a random-access memory (RAM) to enable low-latency data reporting. In this scenario, when the PDC receives the data, it writes the data into a RAM-based cache instead of a read-only member (ROM). When an application files a data query request for real-time measurement data, the data reporting system fetches the requested data from the RAM and sends it out. On the other hand, an offline data query usually involves large-volume, historical measuring data and there



**Fig. 15** Control station subnets separation

is usually a loose requirement for latency. In this scenario, the data reporting system directs a data query request to the ROM, where the historical data archives reside. Moreover, solid-state drives (SSD) can be used to replace the conventional hard disk drive (HDD) to improve the query speed, although their cost for large-volume, high-accuracy PMU data can be big [37].

### 2.3.3 Wide-Area Data Center Security

#### Network Access Control

Network access control plays an important role in securing information systems, including WAMS. In WAMS, PMUs and some clients must communicate with the control center through the public Internet, which raises the concern regarding security and therefore shall be restricted. Least functionality, the separation of duties and role-based access control (RBAC) [38, 39] shall be considered. For example, PMUs shall have only access to PDC. And the IEEE 1686 standard [40] suggests that the intelligent electronic devices shall be protected with ID/password pairs and have the ability to provide RBAC. The control center LAN can be divided into 6 subnets according to different duties they serve.

- Critical applications subnet
- Noncritical applications subnet
- Data cache subnet
- Real-time data subnet
- Archive data subnet
- Data concentration subnet

Figure 15 shows the connection between subnets. Because subnet 1 usually consists of real-time control and protection applications, it shall be isolated from the Internet and should be logically isolated from subnet 2: communication between

subnet 1 and 2 should be blocked with few necessary exceptions. Subnet 1 and 2 can only access data via subnet 3, which improves both security and performance. PMUs on the Internet only push data to subnet 6, then subnet 6 will forward data into subnet 3 and 4 for short-term storage. For long-term storage, subnet 4 will forward data to subnet 5.

For individual components in WAMS, the IEEE 1686 standard [40] suggests that the intelligent electronic devices shall be protected with ID/password pairs and have the ability to provide RBAC.

## ***2.4 Advanced Topic for Information Infrastructure: False Data Injection Attack***

In the smart grid, the False Data Injection Attack (FDIA) is applicable to various layers and structures. Generally, these FDIA occur at the physical layer, network layer, and data center [41]. Particularly, the FDIA can manipulate the measurement value without the need to modify the code program. By exploiting communication protocol vulnerabilities or attacking server permissions, false data can directly replace and disturb measurement value stored in the data center.

The FDIA has a wide range of impacts in the following two parts. The first is economic impacts, such as energy theft, resulting in the electrical bill drop. The FDIA attack could impact the topology of the smart grid. Under normal operating conditions, the FDIA can cause erroneous control, leading to a significant loss. The second is stability impacts. By injecting fake measurements, the power grid will produce false responses, causing unstable conditions.

FDIA mainly implements attacks by tampering with data, so it is difficult to rule out the attack using the device operating conditions or data delay. In addition, there are many FDIA attack methods, including ramp attack, scale attack, noise attack, and replacement attack, etc. To remedy this, two types of methods are used including model-based and data-driven detection. In the model-based method, the real-time measurements of the data center are used to model the static and dynamic system parameters and configuration. For example, the Weighted Least Squares (WLS) is utilized to find the system estimated states. However, the WLS is built based on the assumption of stable power system state modeling. Thereafter, some dynamic estimation methods such as distributed and extended Kalman filter, are used to simulate a non-linear system model, which can eventually estimate and detect FDIA at a more accurate level. Some other estimation-free model-based methods have also developed to detect the FDIA. The cooperative vulnerability factor and matrix separation are introduced according to the normal and anomalies power grid under FDIA. Different from the model-based method, the data-driven method does not depend on the model of the power system. Using the characteristics of measurement data, these methods are mainly divided into machine learning and data mining algorithms. Machine learning methods learn the characteristics of the data to determine whether

the data has been attacked. For example, the Support Vector Machine (SVM) is one of the most common FDIA detection methods. The normal and attacked data belong to different hyperplanes in SVM so that FDIA can be distinguished. Not only that, the artificial neural networks, K-nearest neighbor, decision tree and random forests can also be used to detect abnormal behavior. However, these machine learning methods have insufficient learning ability on the one hand, and limited ability to process huge data on the other. To eliminate this defect, the deep learning methods such as the Recurrent Neural Networks (RNN), Deep Belief Network (DBN) and Convolutional Neural Network (CNN) provide new workarounds for FDIA detection [42]. Typically, they have better recognition ability and accuracy when facing different FDIA attacks.

The prerequisite for using machine learning is that the difference in attack data is known, namely, which type of FDIA attack method is already clear. The data mining method provides another perspective to deal with the hidden patterns or attributes of false data. Since it's a kind of unsupervised method, it is not necessary to know the label of the data in advance. For example, the Principal Component Analysis (PCA) is used to detect the FDIA using the covariance of the different measurement data. The rest methods include Hoeffding adaptive trees, non-nested generalized exemplars, and common path mining. The data mining method has low computational complexity, so they are especially suitable for big data detection in the data center of WAMS.

### **3 Development of a Distribution-Level Wide-Area Monitoring System-FNET/GridEye: Infrastructures and Applications**

#### ***3.1 Introduction***

As an advanced technology, a WAMS measures critical electrical quantities, providing the system operators an unprecedented way to monitor and control the electric power systems to meet the challenge brought by low inertia power systems. The PMU is the most important component in WAMS. The PMUs provide high-resolution, high-accuracy, and time-synchronized phasor measurements, which are generally known as synchrophasors. Based on the extraordinary ability of synchrophasor technology, FNET/GridEye, the first distribution-level wide-area phasor measurement system, is developed in 2003. FNET/GridEye is a frequency monitoring network. The FNET/GridEye mainly adopts two types of low-cost and high-accuracy PMU variants, frequency disturbance recorders (FDRs) and universal grid analyzers (UGAs), which are referred as synchronized measurement devices (SMDs), to collect power grid quantities including but not limited to frequency, voltage magnitude, voltage phase angle, harmonics. During the past 17 years,



FNET/GridEye has been helping utilities, balancing authorities (BAs), regional coordinators (RCs), electric reliability organizations (EROs), and the U.S. federal government on many critical aspects including situation awareness, operations, post-event analysis, compliance, etc., and is widely acknowledged by the power industry.

### 3.2 FNET/GridEye Communication and Information Infrastructures

FNET/GridEye is developed as a pilot wide-area phasor measurement system that can cover the national or continental level power grid at a much lower cost before the universal PMU installations can be achieved [43]. The SMDs transmit the collected phasor measurements to two data centers located at the University of Tennessee, Knoxville (UTK), and the Oak Ridge National Lab (ORNL). The FNET/GridEye data center employs a multi-layer architecture, it is designed to receive, process, utilize, and archive a large volume of phasor measurements in real-time [44]. The structure of the FNET/GridEye data center is shown in Fig. 16. As shown in Fig. 16, the FNET/GridEye data center consists of four fundamental layers: data collection layer, real-time analysis layer, data storage layer, and non-real-time analysis layer. In the data collection layer, the FDRs and UGAs collect the phasor measurements data from the power system and compress the data as packages. Then, the FDRs and UGAs send connecting signals to two PDCs through Ethernet via TCP/IP protocol. Once connected, the compressed data package will be as data frames and send to PDCs via standard PMU communication protocols (such as IEEE C37.118.2-2011). For protecting the information security, the Firewall is also configured on the PDCs' server. When the PDCs receive the data frames, the main PDCs will de-compress the data and send it to the real-time analysis layer and data storage layer, where a data cluster is deployed. The real-time analysis layer hosts various FNET/GridEye applications that utilize the field-collected synchrophasor measurement data to monitor the

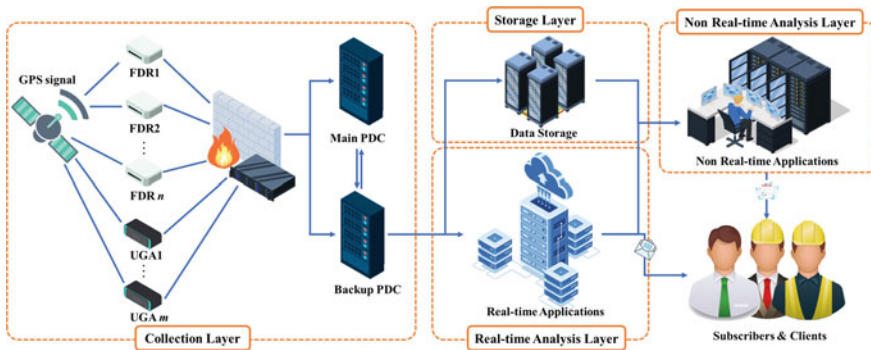


Fig. 16 The structure of the FNET/GridEye data center

operational status of worldwide power grids. Frequency disturbance events including inter-area oscillation, generator trip, and load disconnection, etc. will be detected by the developed real-time application modules. Then the modules send disturbance alerts to the subscribers and clients of FNET/GridEye for warning. On the other hand, the data storage layer archives phasor measurement data streams from the main PDC for offline applications in the non-real-time analysis layer. The non-real-time analysis layer runs an offline application to further investigate the archived data from the real-time analysis layer and the data storage layer. With the increasing deployment of SMDs, FNET/GridEye has evolved its data center towards reliability, availability, and security. The multi-layer structure of the FNET/GridEye data center facilitates the concentrating, processing, and archiving of a large volume of phasor measurements to successfully meet the timeliness requirements of various applications.

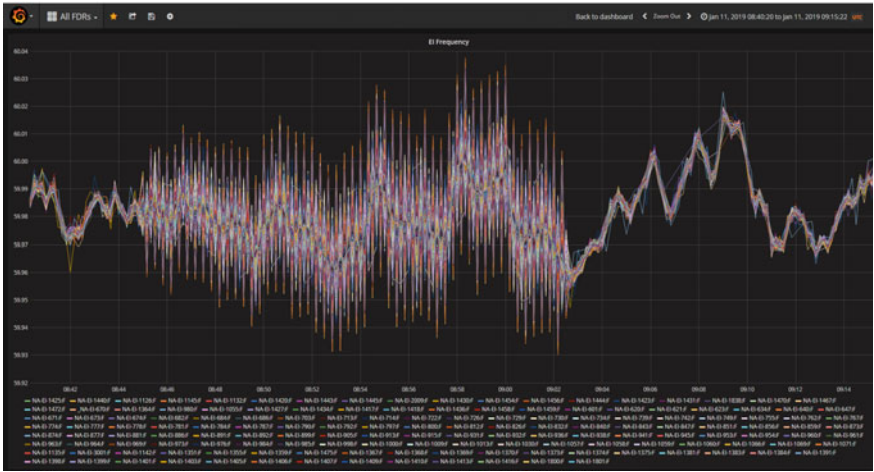
### 3.3 *FNET/GridEye Advanced Applications*

#### 3.3.1 **Real-Time Visualizations for Situation Awareness**

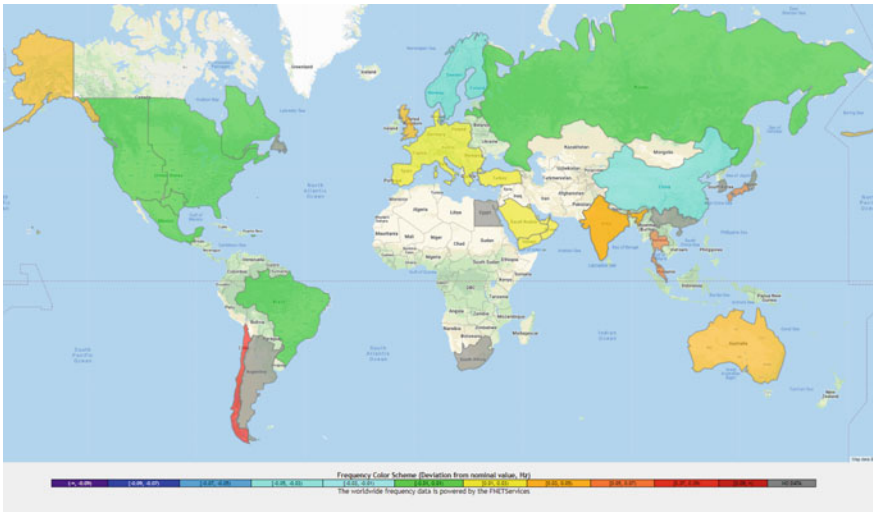
The purpose of the FNET/GridEye real-time visualizations is to provide control-room situation awareness tools for industry consortium and cooperative partners. The real-time visualizations query the real-time frequency and phase angle, which are collected from high-resolution SMDs located across the North American continent and the world [45]. Afterward, both data are processed by dedicated algorithms to generate insightful visualizations. Figure 17a, b demonstrate some examples of the real-time visualizations. In general, the FNET/GridEye real-time visualizations use the FNETVision [46], world-wide frequency table display, world-wide frequency map, and U.S. relative angle contour map. In addition, some sample events are also provided to all interested researchers for advancing studies.

#### 3.3.2 **Frequency Disturbance Detection**

The FNET/GridEye system exploits the real-time frequency and phase angle measurements to detect frequency disturbances [47, 48] and determine their location [49] and magnitude [50]. To locate the source of a frequency disturbance, FNET/GridEye exploits the time delay of arrival (TDOA) characteristics of phase angle data, using a triangulation algorithm to estimate the source of a generation event from the first several PMUs. Furthermore, the estimated event source is further aligned with the location of power plants and pump storage units to help improve the accuracy of disturbance source estimation. Apart from the source location, FNET/GridEye also employs a disturbance magnitude estimation algorithm to determine the size of a generation event. When an event happens, the primary frequency response will be activated to stabilize the frequency and, where the frequency change is proportional to the disturbance magnitude. Accordingly,



(a) Frequency visualization of a forced oscillation event



(b) Geological frequency map for world major power grids

Fig. 17 FNET/GridEye real-time visualizations

the magnitude can be calculated with FNET/GridEye frequency measurements. Figure 18 shows an example of a generator trip event captured by the FNET/GridEye system.



# FNET Event Report

## Basic Event Information

Event Date	Event Time	Event Type	Estimated Amount
2020-03-07	15:20:10 UTC	Generation Trip	670 MW
Point A	Point B	Point C Prime	
60.0033 Hz	59.9693 Hz	59.9739 Hz	N/A Hz
MOD-027-1 Event	Inter Connection	Estimated Reliability Coordinator	ROCOF
NO	EI	MRO	N/A
Estimated Event Location (44.8606, -89.6553)		Additional Location Information near Weston power plant (MRO) in (Rothschild, WI, 54474).	

\*Due to limited knowledge on WECC and ERCOT, the magnitude estimation may not be accurate. Please verify it before use.

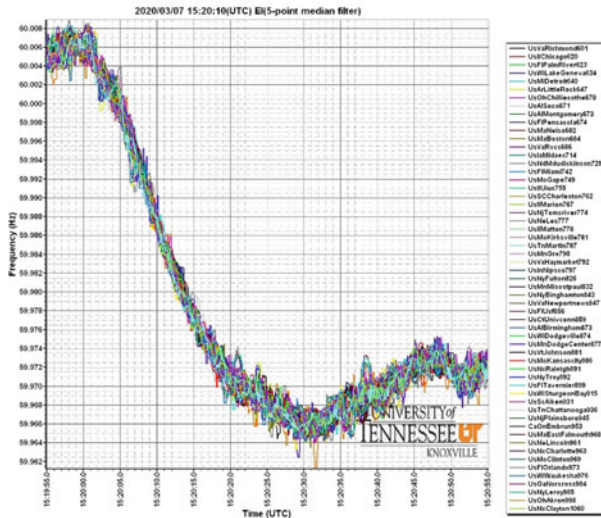
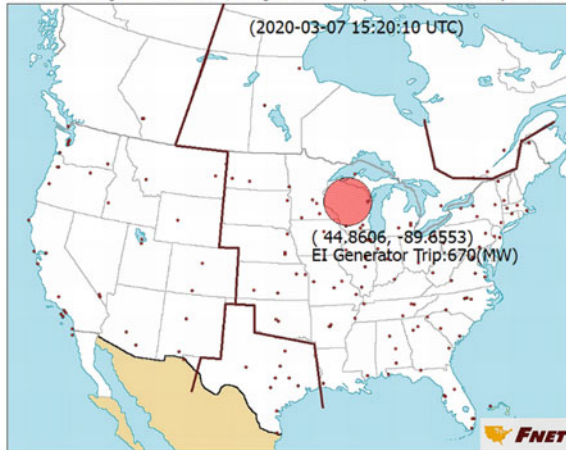


Fig. 18 FNET/GridEye generation event reports

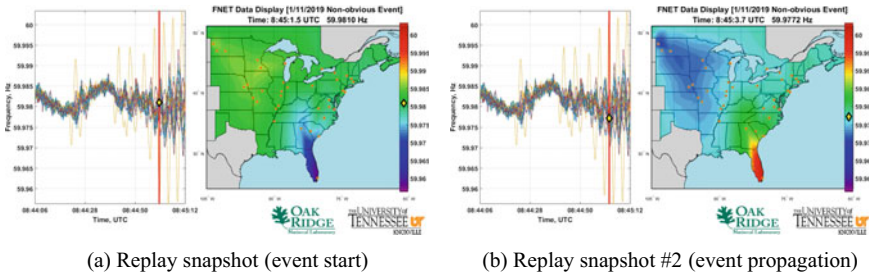


Fig. 19 Event replay for forced oscillation 01/11/2019

### 3.3.3 Dynamic Event Replay

An important offline application of FNET/GridEye is to replay power system disturbance events. Taking the forced oscillation event on January 11, 2019 as an example. An oscillation with 0.25 Hz dominant frequency happened in Tampa, Florida area due to a steam turbine control failure, which lasted for 18 min and caused a unit being removed from service by the plant operator. After such an event, FNET/GridEye utilized high-resolution frequency data to generate a video replay to help operators and regulators to investigate the causes and effects of the event, then take actions to avoid similar events thereafter. Figure 19 demonstrates the propagation of the electromechanical wave at the start of the event. As seen, the oscillatory energy evolves from FRCC, then travels to the test of the grid. The event replay function of the FNET/GridEye was also used for the post-event analysis of many other similar events with their replay videos posted on the project website [51] and the YouTube channel [52].

### 3.3.4 Model-Less Forced Oscillation Source Location

Low frequency forced oscillation is one of the major threats to the security and stability of power systems. Major state-of-the-art forced oscillation source location methods require a known model to locate the source of the forced oscillation [53, 54]. With highly accurate synchrophasor collected from the field, FNET/GridEye employs a data-driven approach to achieve model-less source location for forced oscillation events [55]. Figure 20 demonstrates the observation-time maps of two forced oscillation events. In Fig. 20, regions that are colored with shorter-wavelength colors (purple, blue, etc.) are closer to the oscillatory source, while other regions that are colored with longer-wavelength colors (red, orange, etc.) are farther from the oscillatory source. Finally, an FFT-based algorithm utilizes two-cycle measurements to locate the oscillatory source, which makes it robust to the change of dominant frequency. As Fig. 20 indicates, the FFT-based algorithm successfully locates the oscillatory sources for two events.

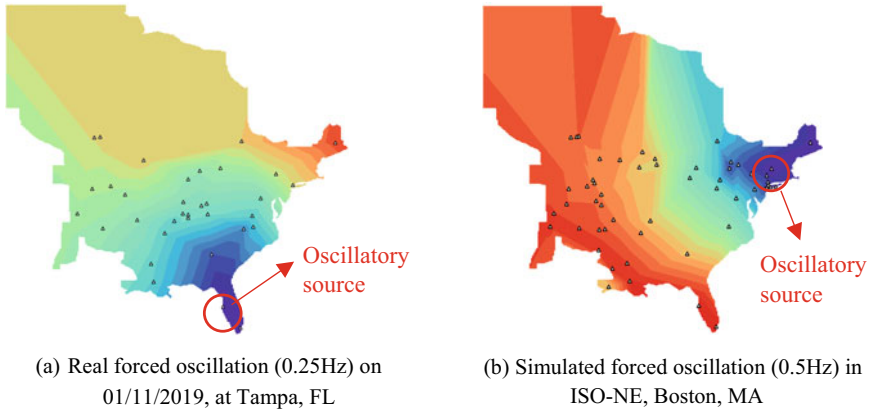


Fig. 20 Model-less ultra-wide-area forced oscillation source location

### 3.3.5 Load Control

Since PMUs can provide accurate frequency measurement in real-time and communicate with the control center, they can be used to help use distribution-level resources to improve system reliability. Figure 21a shows the framework of using local frequency measurement to control loads at the distribution level for frequency regulation. A mobile-device-PMU (MDPMU) is connected to the Energy Management Circuit Breaker (EMCB) to selectively trip load when the system frequency is low [56]. The location and amount of load to be tripped is determined in a centralized manner based on the offered price of load response and current generation-load imbalance calculated using the ROCOF value. Figure 21b shows the simulation result of the frequency control performance using FNET/GridEye sensors for distribution load response in a fictitious ERCOT system. It is seen the frequency crosses the under-frequency load shedding (UFLS) at 59.3 Hz when no load control is involved. Other frequency curves are the system frequencies with distribution-level load response using MDPMUs with different data reporting rates.

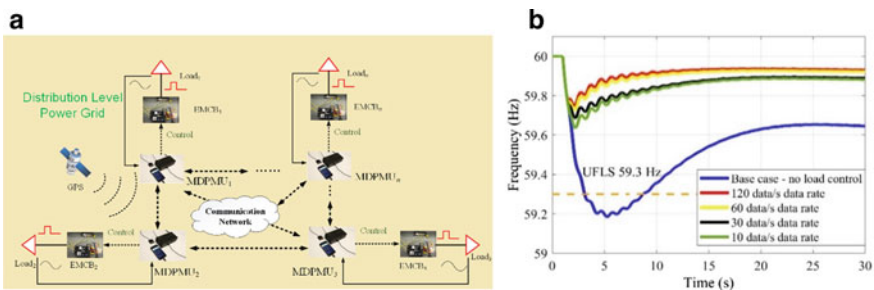


Fig. 21 (a) Distribution load response using (b) Frequency responses of ERCOT



### 3.4 Summary

This chapter first goes through a section of wide-area communication topics including communication protocol, method, schemes/architecture. For the wide-area communication, major wide-area communication protocols including IEEE C37.118, IEC61850-90-5, and STTP are explained and compared. Then, communication methods including power line, optical fiber, cellular, microwave, etc. are introduced and compared. Last but not the least, two types of communication schemes are demonstrated. Advanced topics including data compression and cybersecurity are also introduced and some potential applications are envisioned. Then, this chapter introduces some basics on the information infrastructure topics including data center paradigm, data center management, and data center security. This section first illustrates different data center paradigms and how various paradigms work together. Then, it introduces important data center management topics including data storage and warehousing. Different data storage schemes and data reporting schemes are explained and compared. Finally, security issues including the implementation of firewall and subdomains, and how they ensure the security of a WAMS data center are introduced. An advanced topic on false data injection attack (FDIA) is introduced and some effective methods to address FDIA are discussed. Lastly, the authors share their experience on the communication and information infrastructures using the distribution-level wide-area monitoring system, FNET/GridEye as an example. It introduces some key technologies that ensure the efficiency and reliability of such a WAMS. Various applications are demonstrated to illustrate the effectiveness of the FNET/GridEye system.

In modern WAMS, the actual communication and information infrastructures can be heterogeneous and rather complex due to the increasing integration of distributed energy resources [57, 58], the adoption of microgrid [59], etc. In fact, blended wide-area systems bring many new challenges in terms of compatibility, transparency, efficiency, security, etc. Some efforts have been made to establish ultra-wide-area communication and information infrastructures to promote interconnection-wise efficient, secure data communications [60, 61]. WAMS has several vital applications in smart grids to improve its operation, control, stability, and security [62–67]. However, the ever-growing WAMS demand continuous innovation in the communication and information infrastructures to support the need for the next five or ten years.

### References

1. IEEE, IEEE Std C37.118-2005. IEEE standard for synchrophasors for power systems (2005)
2. IEEE, IEEE Std C37.118.1-2011. IEEE standard for synchrophasor measurements for power systems (2011)
3. IEEE, IEEE Std C37.118.2-2011. IEEE standard for synchrophasor data transfer for power systems (2011)
4. IEEE, IEEE Std C37.118.1a-2014. IEEE standard for synchrophasor measurements for power systems—Amendment 1: modification of selected performance requirements (2014)

5. IEC, IEC 61850 Communication networks and systems for power utility automation (2013)
6. IEC, IEC 61850-90-5: 2012. Communication networks and systems for power utility automation—Part 90-5: use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118 (2012)
7. IEEE, IEEE Std 802.3-2018. IEEE Standard for Ethernet, pp. 1–5600 (2018)
8. R. Robertson, *Advanced Synchrophasor Protocol (ASP) Development and Demonstration Project* (Department of Energy, United States, 2020), pp. 1–105
9. R. Carroll, F. Robertson, *A Comparison of Phasor Communications Protocols* (No. PNNL-28499), (Pacific Northwest National Lab, Richland, WA, United States, 2019), pp. 1–86
10. I. Ali, M.A. Aftab, S. S. Hussain, Performance comparison of IEC 61850-90-5 and IEEE C37.118.2 based wide area PMU communication networks. *J. Modern Power Syst. Clean Energy* **4**(3), 487–495 (2016)
11. I. Edward, Chapter 4—Network Physical Layer Technologies, TCP/IP embedded internet applications (Newnes, Boston, MA, 2003), pp. 69–107
12. R. Zurawski, From wireline to wireless networks and technologies. *IEEE Trans. Ind. Informat.* **3**(2), 93–94 (2007)
13. B. Appasani, D.K. Mohanta, A review on synchrophasor communication system: communication technologies, standards and applications. *Protect. Contr. Modern Power Syst.* **3**(2), 37 (2018)
14. S. Kumar, M.K. Soni, D.K. Jain, Requirements and challenges of PMUs communication in WAMS environment. *Far East J. Electron. Commun.* **13**(2), 121–135 (2014)
15. K. Zhu, J. Song, M. Chenine, L. Nordström, Analysis of phasor data latency in wide area monitoring and control systems, in *Proceedings of 2010 IEEE International Conference on Communications Workshops*, Capetown (2010)
16. C. Callegari, S. Giordano, M. Pagano, T. Pepe, WAVE-CUSUM: Improving CUSUM performance in network anomaly detection by means of wavelet analysis. *Comput. Secur.* **31**(5), 727–735 (2012)
17. A.G. Phadke, J.S. Thorp, Communication needs for wide area measurement applications, in *Proceedings of 2010 5th International Conference on Critical Infrastructure*, Beijing (2010)
18. A.S. Musleh, G. Chen, Z.Y. Dong, A survey on the detection algorithms for false data injection attacks in smart grids, *IEEE Trans. Smart Grid* (2019)
19. C.T. Beasley, Electric power synchrophasor network cyber security vulnerabilities. Dissertation. Clemson University, (2014)
20. R. Kateb, P. Akaber, M.H.K. Tushar, A. Albarakati, M. Debbabi, C. Assi, Enhancing WAMS communication network against delay attacks. *IEEE Trans. Smart Grid* **10**(3), 2738–2751 (2019)
21. R. Klump, P. Agarwal, J. E. Tate, H. Khurana, Lossless compression of synchronized phasor measurements, in *Proceedings of 2010 IEEE PESGM* (2010), pp. 1–7
22. P.H. Gadde, M. Biswal, S. Brahma, H. Cao, Efficient compression of PMU Data in WAMS. *IEEE Trans. Smart Grid* **7**(5), 2406–2413 (2016)
23. Z. Hu, Y. Li, J. Wu, J. Guo, H. Gu, Research of PMU data transmission mechanism in smart grid based on NDN, in *Proceedings of 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)* (Beijing, 2017), pp. 1–6
24. M. Asprou, E. Kyriakides, The effect of time-delayed measurements on a PMU-based state estimator, in *Proceedings of 2015 IEEE Eindhoven (PowerTech, Eindhoven, 2015)*, pp. 1–6
25. M. Wang, Data quality management of synchrophasor data in power systems by exploiting low-dimensional models, in *Proceedings of 2017 51st Annual Conference on Information Sciences and Systems (CISS)* (Baltimore, MD, 2017), pp. 1–2
26. B. Calabrese, *Data Reduction, Encyclopedia of Bioinformatics and Computational Biology*, (Academic Press, 2019), pp. 480–485
27. Z.M. Lu, S.Z. Guo, Chapter 1—Introduction, *Lossless Information Hiding in Images* (Syngress, 2017), pp. 1–68
28. S.B. Choi, M.H. Lee, High speed pattern matching for a fast Huffman decoder. *IEEE Trans. Consum. Electron.* **41**(1), 97–103 (1995)



29. A. Balaji, G. Sharma, M. Shaw, R. Guay, Preprocessing methods for improved lossless compression of color look-up tables. *J. Imag. Sci. Technol.* **52**(4) (2008)
30. J.E. Tate, Preprocessing and Golomb-Rice encoding for lossless compression of phasor angle data. *IEEE Trans. Smart Grid* **7**(2), 718–729 (2016)
31. T.J. Richardson, R.L. Urbanke, Efficient encoding of low-density parity-check codes. *IEEE Trans. Inf. Theory* **47**(2), 638–656 (2001)
32. T. Izumi, Y. Iiguni, Data compression of nonlinear time series using a hybrid linear/nonlinear predictor. *Signal Process.* **86**(9), 2439–2446 (2006)
33. W. Ren, T. Yardley, K. Nahrstedt, ISAAC: intelligent synchrophasor data real-time compression framework for WAMS, in *Proceedings of 2017 IEEE International Conference on Smart Grid Communications* (Dresden, 2017), pp. 430–436
34. Timescale, Time-series data: Why (and how) to use a relational database instead of NoSQL (2020). <https://blog.timescale.com/blog/time-series-data-why-and-how-to-use-a-relational-database-instead-of-nosql-d0cd6975e87c/>. Accessed 13 Mar 2020
35. A. Armenia, J.H. Chow, A flexible phasor data concentrator design leveraging existing software technologies. *IEEE Trans. Smart Grid* **1**(1), 73–81 (2010)
36. S. Ghemawat, H. Gombioff, S. Leung, The Google file system, in *Proceedings of the 19th ACM Symposium on Operating Systems Principles* (ACM, Bolto cn Landing, NY, 2003), pp. 20–43
37. I. Kosen, C. Huang, Z. Chen, X. Zhang, L. Min, D. Zhou, L. Zhu, Y. Liu, UPS: Unified PMU-Data storage system to enhance T+D PMU Data usability. *IEEE Trans. Smart Grid* **11**(1), 739–748 (2020)
38. J.T. Force, T. Initiative, Security and privacy controls for federal information systems and organizations. *NIST Spec. Publ.* **800**(53), 8–13 (2013)
39. D.F. Ferraiolo, R. Sandhu, S. Gavrilu, D.R. Kuhn, R. Chandramouli, Proposed NIST standard for role-based access control. *ACM Trans. Inf. Syst. Secur.* **4**(3), 224–274 (2001)
40. IEEE, IEEE Std 1686-2013 IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities (2014), pp. 1–29
41. G. Liang, J. Zhao, F. Luo, S.R. Weller, Z.Y. Dong, A review of false data injection attacks against modern power systems. *IEEE Trans. Smart Grid* **8**(4), 1630–1638 (2017)
42. W. Qiu, Q. Tang, Y. Wang, L. Zhan, Y. Liu, W. Yao, Multi-view convolutional neural network for data spoofing cyber-attack detection in distribution synchrophasors, *IEEE Trans. Smart Grid* (2020)
43. Y. Liu, S. You, W. Yao, Y. Cui, L. Wu, D. Zhou, J. Zhao, H. Liu, Y. Liu, A distribution level wide area monitoring system for the electric power grid—FNET/GridEye. *IEEE Access* **5**, 2329–2338 (2017)
44. D. Zhou, J. Guo, Y. Zhang, J. Chai, H. Liu, Y. Liu, C. Huang, X. Gui, Y. Liu, Distributed data analytics platform for wide-area Synchrophasor measurement systems. *IEEE Trans. Smart Grid* **7**(5), 2397–2405 (2016)
45. X. Deng, H. Li, W. Yu, W. Wang, Y. Liu, Frequency observations and statistic analysis of worldwide main power grids using FNET/GridEye, in *Proceedings of 2019 IEEE PESGM* (IEEE, Atlanta, GA, 2019), pp. 1–5
46. W. Wang, J. Zhao, W. Yu, Y. Liu, FNETVision: A WAMS big data knowledge discovery system, in *Proceedings of 2018 IEEE PESGM* (IEEE, Portland, OR, 2018), pp. 1–5
47. W. Wang, H. Yin, C. Chen, A. Till, W. Yao, X. Deng, Y. Liu, Frequency disturbance event detection based on synchrophasors and deep learning. *IEEE Trans. Smart Grid* (2020)
48. W. Wang, W. Yao, C. Chen, X. Deng, Y. Liu, Fast and accurate frequency response estimation for large power system disturbances using second derivative of frequency data. *IEEE Trans. Power Syst.* (2020)
49. R. Gardner, J. Bank, J. Wang, A. Arana, Y. Liu, Power system event location analysis using wide-area measurements, in *Proceedings of 2006 IEEE PESGM* (IEEE, Montreal, QB, 2006), pp. 1–7
50. Y. Zhang, X. Deng, S. You, J. Dong, W. Yu, Y. Liu, Measurement-driven disturbance magnitude estimations for bulk power systems, in *Proceedings of 2019 IEEE PES GTD Grand International Conference and Exposition Asia* (2019)

51. PowerIT Group, FNET/GridEye Web Display (Sample Events) (2020). [https://fnetpublic.utk.edu/sample\\_events.html](https://fnetpublic.utk.edu/sample_events.html). Accessed 11 Mar 2020
52. YouTube, FNET/GridEye UTK ORNL (2020). [https://www.youtube.com/channel/UC40n2KTjwRhC9\\_CvtIasaWA](https://www.youtube.com/channel/UC40n2KTjwRhC9_CvtIasaWA), Accessed 11 Mar 2020
53. R. Jha, N. Senroy, Forced oscillation source location in power systems using system dissipating energy. *IET Smart Grid* **2**(4), 514–521 (2019)
54. S. Feng, B. Zheng, P. Jiang, J. Lei, A Two-level forced oscillations source location method based on phasor and energy analysis. *IEEE Access* **6**, 44318–44327
55. W. Wang, C. Chen, L. Zhu, W. Qiu, K. Sun, Y. Liu, Model-less source location for forced oscillation based on synchrophasor and moving fast fourier transformation, in *Proceedings of 2020 IEEE PES ISGT-Europe* (IEEE, Hague, The Netherlands, 2020)
56. W. Yao, S. You, W. Wang, X. Deng, Y. Li, L. Zhan, Y. Liu, A fast load control system based on mobile distribution-level phasor measurement unit. *IEEE Trans. Smart Grid* **11**(1), 895–904 (2020)
57. T. Li, Y. Li, M. Liao, W. Wang, C. Zeng, A new wind power forecasting approach based on conjugated gradient neural network. *Math. Probl. Eng.* **2016**, 1–8 (2016)
58. W. Wang, K. Sun, C. Chen, W. Qiu, H. Yin, S. You, W. Yao, J. Dong, C. Zeng, X. Deng, Y. Liu, Advanced synchrophasor-based application for potential distributed energy resources management: key technology, challenge and vision, in *Proceedings of 2020 IAS I&CPS Asia* (IEEE, Weihai, China, 2020)
59. S. Parhizi, H. Lotfi, A. Khodaei, S. Bahramirad, State of the art in research on microgrids: a review. *IEEE Access* **3**, 890–925 (2015)
60. EIDSN, Our Mission (2020). <https://eidsn.org>. Accessed 11 Mar 2020
61. WECC Data Exchange Work Group, Guideline for WECC operations network node responsibilities and procedures, WECC (2012)
62. H.H. Alhelou, M.H. Golshan, J. Askari-Marnani, Robust sensor fault detection and isolation scheme for interconnected smart power systems in presence of RER and EVs using unknown input observer. *Int. J. Electr. Power Energy Syst.* **99**, 682–694 (2018)
63. H.H. Alhelou, M.E. Hamedani-Golshan, R. Zamani, E. Heydarian-Forushani, P. Siano, Challenges and opportunities of load frequency control in conventional, modern and future smart power systems: a comprehensive review. *Energies* **11**(10), 2497 (2018)
64. H. Haes Alhelou, M.E. Hamedani Golshan, M. Hajiakbari Fini, Wind driven optimization algorithm application to load frequency control in interconnected power systems considering GRC and GDB nonlinearities. *Electric Power Compon. Syst.* **46**(11–12), 1223–1238 (2018)
65. H. Haes Alhelou, M.E. Hamedani-Golshan, T.C. Njenda, P. Siano, A survey on power system blackout and cascading events: research motivations and challenges. *Energies* **12**(4), 682 (2019)
66. H.H. Alhelou, M.E.H. Golshan, N.D. Hatziargyriou, A decentralized functional observer based optimal LFC considering unknown inputs, uncertainties, and cyber-attacks. *IEEE Trans. Power Syst.* **34**(6), 4408–4417 (2019)
67. H.H. Alhelou, M.E.H. Golshan, N.D. Hatziargyriou, Deterministic dynamic state estimation-based optimal lfc for interconnected power systems using unknown input observer. *IEEE Trans. Smart Grid* (2019)
68. H.H. Alhelou, S.J. Mirjalili, R. Zamani, P. Siano, Assessing the optimal generation technology mix determination considering demand response and EVs. *Int. J. Electr. Power Energy Syst.* **119**, 105871 (2020)