Electrical Power and Energy Systems 99 (2018) 45–56

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Review

Cyber security of a power grid: State-of-the-art

Chih-Che Sun[a], Adam Hahn[a], Chen-Ching Liu[a,b,*]

[a] School of Electrical Engineering and Computer Science, Washington State University, Pullman WA, 99164, USA
[b] School of Mechanical and Materials Engineering, University College Dublin, Belfield, Dublin 4, Ireland

ARTICLE INFO

Keywords:
Cyber-physical system
Cyber security
Intrusion detection
CPS testbed
Smart grid

ABSTRACT

The integration of computing and communication capabilities with the power grid has led to numerous vulnerabilities in the cyber-physical system (CPS). This cyber security threat can significantly impact the physical infrastructure, economy, and society. In traditional IT environments, there are already abundant attack cases demonstrating that unauthorized users have the capability to access and manipulate sensitive data from a protected network domain. Electric power grids have also heavily adopted information technology (IT) to perform real-time control, monitoring, and maintenance tasks. In 2015, a sophisticated cyber attack targeted Ukrainian's power grid causing wide area power outages. It highlights the importance of investment on cyber security against intruders. This paper provides a state-of-the-art survey of the most relevant cyber security studies in power systems. It reviews research that demonstrates cyber security risks and constructs solutions to enhance the security of a power grid. To achieve this goal, this paper covers: (1) a survey of the state-of-the-art smart grid technologies, (2) power industry practices and standards, (3) solutions that address cyber security issues, (4) a review of existing CPS testbeds for cyber security research, and (5) unsolved cyber security problems. Power grid cyber security research has been conducted at Washington State University (WSU) with a hardware-in-a-loop CPS testbed. A demonstration is provided to show how the proposed defense systems can be deployed to protect a power grid against cyber intruders.

1. Introduction

To improve the efficiency and reliability, a significant investment has been made by industry and government to build a smarter and more automated/connected power system. With the support of information and communications technology (ICT), power system operators can perform operation and control tasks based on data acquired from remote facilities. For example, the advanced automation system isolates a faulted segment by opening switching devices (e.g., circuit breakers and automated reclosers), and sends the fault information back to the control center. Since power grids span a wide geographic area, public and private networks (e.g., fiber optics, RF/microwave, cellular) can provide a communication path between remote sites and a control center. These capabilities also open doors for attackers to access a power grid and cause disruptions to the normal operation of the grid. Cyber attackers also have the ability to access power system communication networks and connect to remote access points at a power system infrastructure. This can lead to serious and harmful

Abbreviations: ADS, Anomaly detection system; ADA, Advanced distribution automation; AMI, Advanced metering infrastructure; AMR, Automatic meter reading; ANSI, America National Standards Institute; CC, Control center; CCADS, Coordinated cyber attack detection system; CIP, Critical infrastructure protection; CPS, Cyber-physical system; CT, Current transformer; DA, Distribution automation; DER, Distributed energy resources; DMS, Distribution management system; DNP3, Distributed network protocol 3.0; DOE, Department of Energy; DoS, Denial of service; EMS, Energy management system; E-ISAC, Electricity Information Sharing and Analysis Center; ESCSWG, Energy Sector Control Systems Working Group; FCN, Field communication network; FDIR, Fault detection, isolation and recovery; FRTU, Feeder remote terminal unit; GOOSE, Generic object-oriented substation event; GPS, Global positioning system; HAN, Home area network; HMI, Human machine interface; HIDS, Host-based IDS; LAN, Local area network; MDMS, Meter data management system; MMS, Manufacturing message specification; MTTC, Mean-time-to-compromise; MU, Merging unit; NAN, Neighborhood area network; NERC, North American Electric Reliability Corporation; NIDS, Network-based IDS; NIST, National Institute for Standards and Technology; IADS, Integrated ADS; ICT, Information and communications technology; ICCP, Inter-control center communications protocol; IDPS, Intrusion detection and prevention system; IDS, Intrusion detection system; IEC, International Electrotechnical Commission; IED, Intelligent electronic device; IP, Internet Protocol; ISA, International Society for Automation; ISEAGE, Internet-scale event and attack generation environment; ISM, Industrial, scientific, and medical (radio bandwidth); IT, Information technology; OMS, Outage management system; OPC, Object linking and embedding for process control; PDC, Phasor data concentrator; PLC, Programmable logic controller; PMU, Phasor measurement unit; RTDS, Real-time digital simulator; RTU, Remote terminal unit; SAS, Substation automation system; SAIFI, System average interruption frequency index; SAIDI, System average interruption duration index; SCADA, Supervisory control and data acquisition; SCL, Substation configuration language; SCT, Smart City Testbed; SDO, Standard Development Organization; SMV, Sample measured value; TO, Transmission operator; VT, Voltage transformer; WAMS, Wide area monitoring system; WAN, Wide area network; WSU, Washington State University

* Corresponding author at: School of Electrical Engineering and Computer Science, Washington State University, Pullman WA, 99164, USA.
E-mail addresses: csun@eecs.wsu.edu (C.-C. Sun), ahahn@eecs.wsu.edu (A. Hahn), liu@wsu.edu (C.-C. Liu).

https://doi.org/10.1016/j.ijepes.2017.12.020
Received 9 November 2017; Accepted 18 December 2017

consequences. As a result, cyber security of smart grids has been recognized as a critical issue.

In December 2015, Ukraine's power system experienced a wide area power outage in a cyber attack incident. The outage affected approximately 225,000 customers. The power companies, SANS institute and Electricity Information Sharing and Analysis Center (E-ISAC), published reports [1] about the event. The attack started from malware installations by phishing mails several months prior to the attack. During the reconnaissance period, attackers monitored the operations of the targeted power grid for planning of the attack steps. On the attack day, human machine interface (HMI) was hijacked and used by the attackers to remotely open a number of circuit breakers which directly cut power to the customers. To further complicate the restoration process, the telephone system and communication network were compromised by a denial of service (DoS) attack so that the call-center could not accept incoming trouble calls from customers. Furthermore, the malware on the HMI was used to delete software on the system, which prevented the operators from determining the extent of the power outage and hampered restoration actions.

While numerous efforts have focused the development and deployment of technologies to protect computer systems and networks, these techniques do not provide perfect security. Hence, important issues of cyber security research include classification of the normal or abnormal system activities and identification of vulnerabilities. In order to discover weaknesses of the smart grid communication systems, different cyber assessment approaches are proposed to support different subsystems. The studies of attack/impact analysis provide the requirements to design cyber detection systems, e.g., intrusion detection systems (IDSs) and anomaly detection systems (ADSs).

In the remaining of this paper, Section 2 describes the state-of-the-art of smart grid technology. Section 3 presents the cyber security vulnerabilities in a smart grid. In Section 4, the solutions against cyber intrusions are provided. Section 5 describes the potential cyber threats yet to be solved. In Section 6, research on cyber security at WSU will be used to demonstrate the emerging solutions, including the cyber-physical testbed and anomaly detection systems. The conclusions are given in Section 7.

2. State-of-the-art

This section provides an overview of the emerging smart grid technology and their impact on grid operations. Due to differences of configurations and objectives between power transmission and distribution systems, they possess unique monitoring requirements, control systems, and embedded digital communication applications.

2.1. Digital communication systems

In a traditional substation, analog communication between each pair of devices requires an individual copper cable. Digital communication, on the other hand, enables interconnectivity among various devices. Engineering costs can be reduced and the communication configuration becomes easier by using Ethernet and/or Internet Protocol (IP). It also improves the efficiency of data exchange since the configuration of digital communication allows multiple signals to be transmitted concurrently on the same line. Fig. 1 shows the differences in configuration between traditional and digital substation communication networks. By connecting to the local area network (LAN), gateway devices (e.g., remote terminal units (RTUs) and routers) can aggregate the internal data in a substation and forward it to the destinations (e.g., control centers and data centers).

2.2. Communication architecture of smart grids

2.2.1. ICT of transmission system

The primary purpose of a transmission system is to deliver electric energy from generators to remote load centers. Dynamic interactions among the large number of geographically dispersed generators, transmission lines, and loads are key factors that affect the system stability (e.g., small disturbance, transient, and voltage stability issues). The ICT system supports on-line data acquisition for monitoring and control in a power system. Fig. 2 shows the communication structure in the transmission system operation level, such as operator level, control center level, and substation level.

Supervisory control and data acquisition (SCADA): For on-line operation and monitoring, SCADA systems have been installed in various industries (e.g., water, oil/gas, and power). In a power grid, the SCADA system is a common tool for collecting measurements and status data and sending control commands to switching devices (e.g., circuit breakers). Based on the collected data, an energy management system (EMS) provides analytical tools for operators to determine the system state and take appropriate actions.

Substation automation system (SAS): The concept of SASs has been the subject of Working Group (WG) 10 of International Electrotechnical Commission (IEC) Technical Committee (TC) 57. IEC 61850 standard specifies the design of SASs [2]. It provides some advantages: (1) Reducing the engineering cost by integrating Ethernet-based communication, (2) Enhancing interoperability of devices from different vendors, and (3) Minimizing the impact when the communication topology is changed [3]. Ethernet-based communication network supports multiple standards that encompass different media types, such as copper and fiber-optic. Due to the ubiquitous nature of Ethernet and large numbers of suppliers, the communication equipment cost is reduced. In addition, utilization of substation configuration language (SCL) improves the interoperability of IEC 61850 based devices. SCL uses a standard file format to exchange information between proprietary configuration tools for substation devices. It reduces the impact when a device is added/removed from the substation communication network. IEC 61850 provides high-speed communication protocols for substation automation facilities. Generic object oriented substation event (GOOSE) messages are used to send tripping signals from protective IEDs to circuit breakers. Measurement values (i.e., current and voltage) are sent from merging units (MUs) to IEDs by sampled measured value (SMV). In addition, the manufacturing message specification (MMS) is used for exchanging system data (e.g., measurement readings and devices' status) and control commands between a user interface and IEDs.

Phasor measurement unit (PMU): The synchrophasor system has been deployed in large scale over the last decade to enhance the power system observability. The digital sensor of a standard PMU is able to sample 60–120 data points per second. The collected data (e.g., voltage, current, frequency, and phase angle) can be synchronized by time stamps from the global positioning system (GPS). In 2017, over 2500 of PMUs are installed and networked in North America [4]. The collected measurements in each PMU are sent to a phasor data concentrator (PDC) in a control center using IEEE C37.118 protocol [5]. Various PMU applications (e.g., wide-area visualization, oscillation detection, and voltage stability) have been proposed to improve the reliability of a power grid.

2.2.2. Distribution system

The effort in distribution automation over the last decades helped to increase the reliability of the grid, but also increased the complexity of operation and control. These increasingly digital devices and systems include remote controlled switching devices, protection relays, voltage regulators, distributed energy resources, smart meters, and outage management systems. The equipped network interfaces enable remote monitoring and control from a distribution operating center. Fig. 3 illustrates an ICT model of a distribution system.

AMI: With the embedded digital sensors, a smart meter is able to record the power consumption profile at a time scale of seconds. Compared to the automatic meter reading (AMR) system, AMI has a

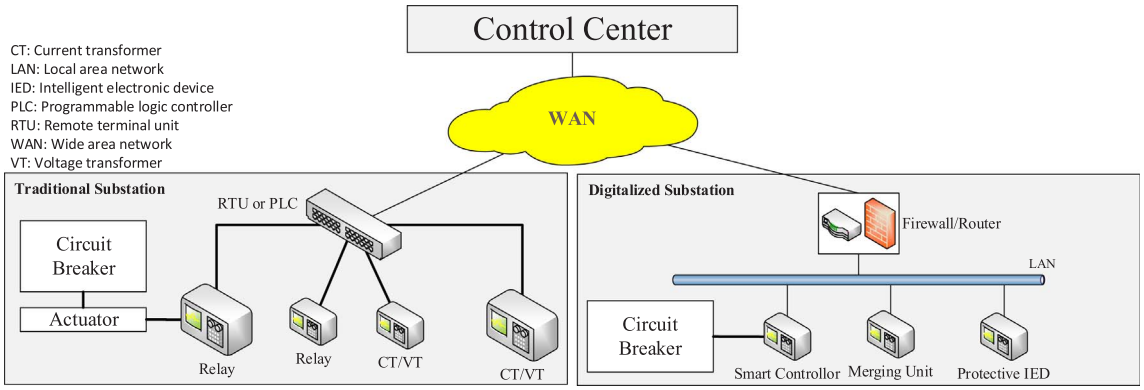

Fig. 1. Comparison of communication systems for traditional and digitalized substations.

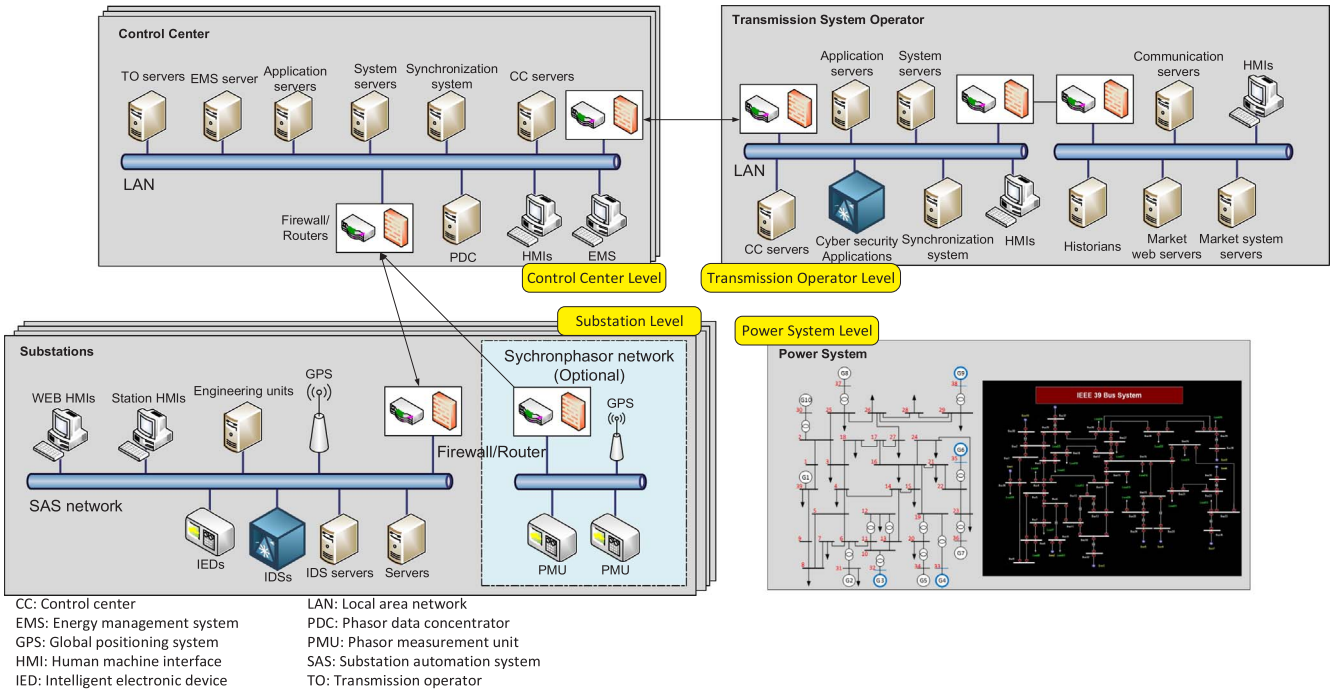

Fig. 2. ICT model in a transmission system.

higher data exchange rate and is equipped with a full duplexed communication module, sending and receiving meter readings and control commands [6]. Generally, meter readings are sent to a control center every 5–60 min, depending on the meter configuration and availability of a network [7]. The communication network of AMI is formed by smart meters, local data aggregators, and meter data management systems (MDMSs). With wireless communication protocols as defined in IEEE 802.15.4 standard [8], the communication distance between a local data aggregator and smart meters can be extended by the mesh and point-to-multipoint networking topologies [9]. The wireless signal strength of a local data aggregator is not necessary to cover all smart meters in a neighborhood. This feature allows AMI devices to consume less transmitting power (0 dBm) via low-gain antennas. Finally, the meter data is sent to MDMS in a distribution operation center for further analysis and planning purposes.

The real-time meter readings enable several on-line operations which can improve system reliability and energy efficiency. For example, demand response [10] has been developed for reshaping the power demand curve. The peak load can be reduced by shifting energy usage from the peak time to off-peak periods. It prevents overloading in the power network and reduces the cost of electricity for consumers. AMI also contributes to the outage management system (OMS) by reporting power outage events with the embedded storage [11]. Compared to trouble calls from customers, operators can respond to an outage event faster and reduce the outage duration.

DER: DERs (e.g., distributed generators, renewable energy devices, and energy storage) are usually deployed in a distribution system. These devices may be owned and controlled by consumers, third-parties, or utilities for local consumption and/or trading in the electricity market [12]. These devices are also increasingly dependent on digital control as many devices utilize smart inverters to provide improved control over how the device is integrated with the grid and supports advanced applications, such as fault ride-through and VAR support. However, because these devices are increasingly owned by consumers, they are often not configured as securely as smart meters and often connected to other consumer devices (e.g., home WiFi routers). For a utility scale DER system, facilities DER energy management systems are used to manage a group of DER systems via WAN/LAN at the facility [13].

Distribution Automation (DA): DA enables remote monitoring and control in a distribution system; such remote controlled devices include feeder switches, voltage regulators, and capacitor banks. It provides functions of fault detection, isolation and recovery (FDIR) and volt-var control that improves reliability indices, including system average

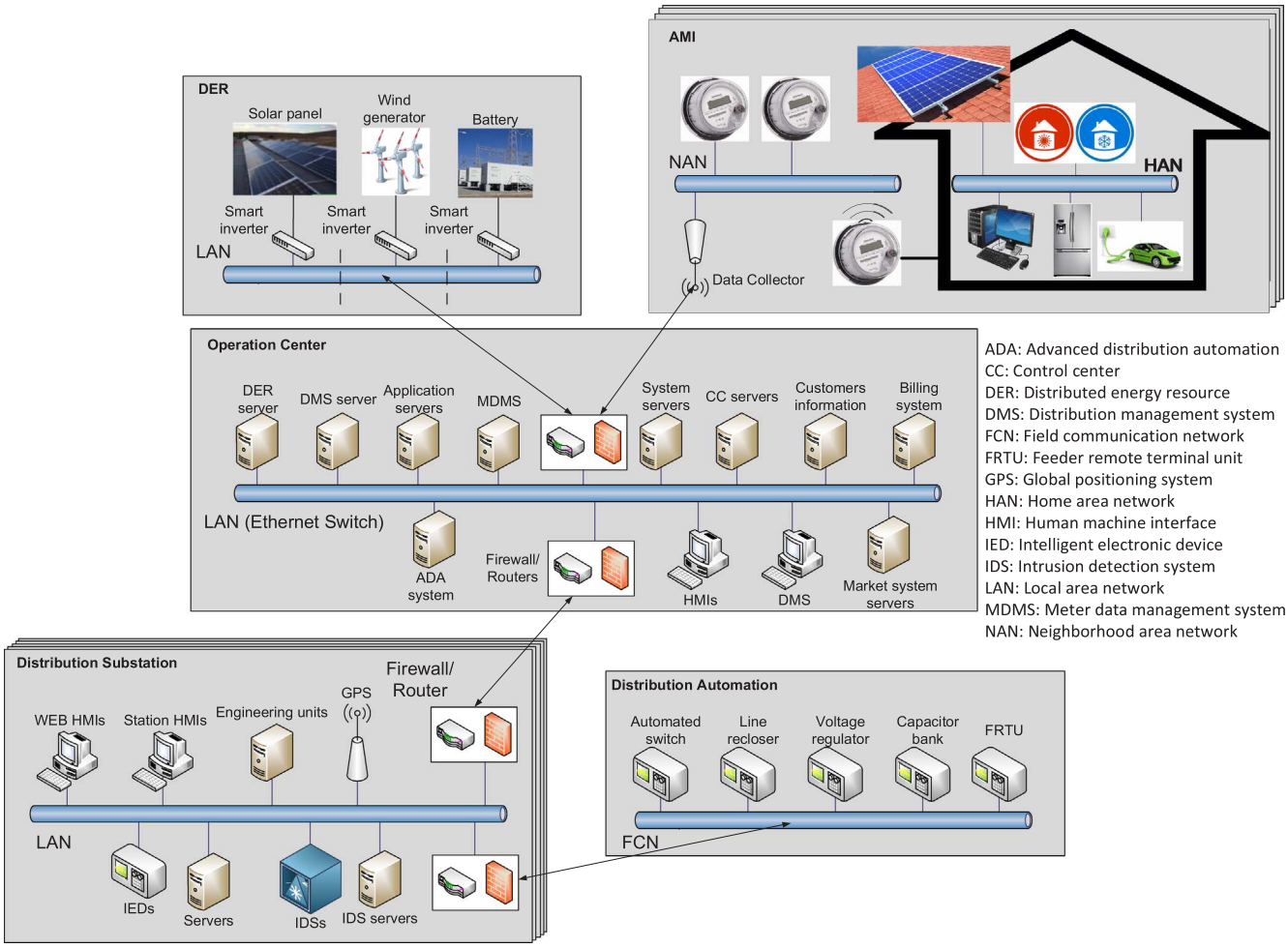

Fig. 3. ICT model in a distribution system.

interruption duration index (SAIDI) and system average interruption frequency index (SAIFI). While many DA devices are found within substations, which have some physical security and dedicated wired communication, many are physically exposed pole-top devices that depend on vulnerable wireless communication.

3. Cyber security

Many industry and government reports have identified that cyber intruders have become a serious threat to the secure operation of a smart grid. Forty-six cyber attack incidents have been reported in the energy sector in 2015 [14], most of which targeted the IT system of utilities and vendors. The U.S. Department of Energy (DOE) indicates that the actual number of cyber attacks is higher than reported [15]. To identify and eliminate cyber vulnerabilities in a smart grid, methods to detect cyber intrusions and mitigate their impact need to be developed.

3.1. Vulnerabilities in cyber infrastructures

To prevent unauthorized access to a private network, firewalls are installed behind an access point (e.g., router and gateway) in order to filter incoming network traffic as a front line defense. Using the properties of packets, such as time delay, source/destination IP address and port numbers, firewalls are capable of inspecting and discarding suspicious packets. However, the performance of firewalls relies on a predefined rule set. Since a commercial grade firewall has hundreds of configurable rules [16], which can often conflict in many cases [17]. Furthermore, developing accurate firewall rules requires that the utility have perfect knowledge of all cyber assets in their network and all authorized communications. However, this information is rarely available, while the grid's dependency on proprietary software platforms further complicates this process. In [18–20], identification approaches have been proposed to discover anomalies in firewall policies. In addition, America National Standards Institute (ANSI)/International Society for Automation (ISA) also propose best practices (i.e., ANSI/ISA 62443-1-1) for a high-level security policy to mitigate threats in control systems. Furthermore, firewalls have other limitations as they cannot protect against spoofed messages which may bypass their filter rules, and they may also contain software vulnerabilities that may allow an attacker to bypass their protection.

Network packets travelling in a WAN may not be protected by firewalls as there is often a concern that the devices may introduce excessive communication latency. To ensure confidentiality and integrity of the grid data, cryptographic protection mechanisms of communication protocols are critical. Many communication protocols and devices used by the power industry communications were developed before cyber security becomes a serious concern and do not implement strong cryptographic protection. For example, MODBUS and Distributed Network Protocol 3.0 (DNP3) are used in SCADA, SAS, PMU and DER systems [21,22]. However, they may not be well protected against cyber attacks [23]. Moreover, DNP3 is used in WAN communication that increases security risks as WAN is accessible to many users. To secure communication protocols, MODBUS authentication frameworks have been proposed [24,25]. A lightweight security authentication scheme [26,27] and a secured frame format are proposed for DNP3 [28].

3.2. Vulnerability assessment in a smart grid

It is necessary to study the interactions between the cyber system and physical system in a cyber attack event. As a core component in control systems, SCADA is a primary target for attackers. Ref. [29] indicates that information exchange among various power entities via WANs is a source of vulnerabilities. SCADA integrates smart grid subsystems (e.g., AMI, DER, and DA) in a distribution system. Cyber attacks become damaging once intruders gain access to the SCADA network. In 2010, Stuxnet, a computer worm, was deployed to infect programmable logic controllers (PLCs) in an industrial control system [30]. It reprogrammed the PLCs to act in a manner intended by the attacker and to hide the modifications from the operators. The affected systems include SCADA, PLCs, and nuclear facilities [31]. Ref. [32] provides an assessment framework to evaluate the vulnerabilities of SCADA systems. In [33], the mean-time-to-compromise (MTTC) is proposed as an index to quantify the vulnerability of a SCADA system. Specific vulnerabilities of SCADA and EMSs have been reported [34,35].

Power system operators rely on SCADA and SAS to perform operations via communications between a control center and remote sites. An IEC 61850 based substation automation system contains various IEDs. Ref. [36] indicates that multicast messages defined in IEC 61850 (e.g., GOOSE and SV) do not include cyber and information security features. They are vulnerable to spoofing, replay, and packet modification, injection and generation attacks. Although IEC 62351 proposes comprehensive security measures (e.g., authentication) to secure IEC 61850 based communication protocols, the weaknesses still exist by analyzing the specifications of both IEC standards [37]. An attack example is demonstrated in [38] in which attackers are able to modify the GOOSE packets to trip circuit breakers. In a massive attack event, attackers can trigger a sequence of cascading events by compromising critical substations, causing a catastrophic outage.

A high level penetration of smart meters brings advantages to distribution system operation. However, smart meters also bring cyber security concerns, e.g., privacy, smart meter data modification attacks, unauthorized remote load control, and interoperability problem. Note that intruder(s) may access the AMI network from various nodes in a public area, such as smart meters and local data collectors. These problems indicate that a single layer of cyber security protection cannot provide a higher level of cyber security. Several cyber attacks targeting the AMI have been identified, including energy theft, false data injection, and leakage of the customer information [39–42].

3.3. Smart grid standard and regulations

To ensure system reliability, [43] proposes baseline requirements and suggests implementation guidelines for data delivery systems in power grids. Critical infrastructure protection (CIP) standards CIP-002 through CIP-009 are established by North American Electric Reliability Corporation (NERC) [44]. The purpose is to “provide a cyber security framework for the identification and protection of critical cyber assets to support reliable operation of the bulk electric system.” A “Roadmap to Achieve Energy Delivery System Cyber Security” is published by the Energy Sector Control Systems Working Group (ESCSWG) for improving cyber security of energy delivery systems [45]. A smart grid cyber security guideline, NISTIR 7628, is published by National Institute of Standards and Technology (NIST) [46,47]. Standard Development Organizations (SDOs), such as IEC, ANSI, NIST, and IEEE, publish multiple standards to serve as a paradigm for each subsystem of a smart grid. Table 1 lists major standards for a smart grid.

4. Anomaly and intrusion detection systems

As previously mentioned, ADSs and IDSs are critical for detecting if an attacker has compromised grid systems and gained access to power grid networks. While these techniques have been heavily researched for IT systems, the unique communication protocols and operations requirements of the smart grid require the development of techniques that are tailored towards these environments. This section will explore the current types of IDSs and how they are integrated and validated on CPS testbeds.

4.1. Types of IDSs

The design of an IDS includes three parts: (1) Detection technique, (2) IDS type, and (3) Active/passive detection. IDSs can be categorized by different ways as shown in Table 2.

4.1.1. Detection techniques

Knowledge based (or signature based) IDSs possess a database of attack patterns or footprints. By comparing the signatures, intrusion events are identified as the network traffic matches the same pattern in a pre-defined database. Knowledge based IDSs have a low false positive rate for detecting known attacks, however, this depends on a strong set of rules that is tailored for the environment. While these are effective against known attack patterns, they are not able to detect attacks which do not have previously developed signatures and also require frequent database updates.

Unlike knowledge based IDSs, behavior based (or anomaly based) IDSs overcome the disadvantage by using profiles of network traffic rather than searching for specific signatures. A base-line profile of normal network traffic is constructed to serve as the standard of normal conditions. Once the deviation of an inspected network profile from the standard is significant, an anomaly alarm will be triggered. However, a major drawback of anomaly based detection is the difficulty in defining anomaly patterns of network traffic, along with the fact that many system anomalies may be benign, such as system maintenance session or upgrades. If the malicious behavior falls under the accepted areas, the attack is regarded as normal.

4.1.2. Anomaly data types

Detection approaches can be categorized based on the type of data they monitor. A network-based IDS (NIDS) monitors traffic in a network segment. With a physical network interface card connected to a LAN, a NIDS is able to access network flows in the same network segment. Some techniques only inspect the lower-level network data, such as network flows, which include the Ethernet and IP addresses, along with the source and destination ports. Other techniques inspect the header information and contents in higher layers of the communication structure, such as the SCADA protocol and payload. According to the unique defined format and structure of each communication protocol, a predefined rule set is used to inspect the incoming network traffic.

A host-based IDS (HIDS) is installed in each communication device individually. It monitors network activities and the device status in a single host system by analyzing log files, executables, system calls, process memory contents, and host network traffic. Since a HIDS does not utilize a LAN, the detection range is limited in the host devices.

4.1.3. Active and passive detection

A passive IDS only analyzes network flows and detects anomalies. When an anomaly is detected, a passive IDS triggers alarms. However, operators need to mitigate and clear the incident manually. In contrast, active IDSs are configured to disconnect suspicious connections automatically. Hence, an active IDS is also called intrusion detection and prevention system (IDPS).

4.2. Detection systems in smart grids

Research has been conducted to explore the development of IDS techniques applied to an array of smart grid environments and applications. Table 3 provides an overview of the proposed techniques including network-based, host-based, or integrated methods. However,

Table 1
Major standards for operating a smart grid.

Subsystem name	Standard name	Applied system
SCADA	IEC 60870-6	Monitoring and control over a WAN
PMU	IEEE C37.118	Phasor data exchange
Substation	IEEE 61850	Substation communication networks and systems
	IEEE C37.1	Definition, specification, and application for monitoring and control function
	IEEE 1379	Communication and interoperation of IEDs and RTUs.
	IEEE 1646	Communication delay time among internal or external devices
	IEEE C37.111	Define file format of measurement from IEDs
AMI	ANSI C12 series (i.e., C12.18 to C12.22)	Define communication protocol for metering applications

Table 2
Structure of cyber protection systems.

Detection technique	IDS type	Active/passive detection
Knowledge based	Network based	Passive (intrusion detection)
Behavior based	Host based	Active (intrusion prevention)

Table 3
Intrusion detection techniques in a smart grid.

Protection range	Category	Detection system
SCADA	Network-based	[48–50]
	Host-based	[51,52]
Substation	Network-based	[53]
	Host-based	[54]
	Integrated	[38,55,56]
Wide area monitoring system (WAMS)	Host-based	[57]
GPS (PMU)	Host-based	[58]
Distribution system	Host-based	[59]
AMI	Host-based	[60–63]

while many approaches have been proposed, most have not yet been integrated into industry due to insufficient verification and validation on realistic environments.

4.3. CPS testbed

Since a field test of cyber attacks may cause damages to the real world power grid, a real-time CPS testbed is an alternative for study of the interactions between cyber and physical systems. In general, a CPS testbed has three parts: (1) Power systems simulation tools (e.g., real time digital simulator (RTDS), DIgSILENT, PowerWrold, TSAT, and PSS/E), (2) Communication system simulation/emulation tools (e.g., network simulator3, Mininet, and OPNET), and (3) Connection between (1) and (2), e.g., object linking and embedding (OLE) for process control (OPC) communication. A hardware-in-the-loop testbed involves physical devices (e.g., smart meters, IEDs, PMUs and switching devices) for the study of specific cyber security areas, e.g., distribution system, transmission system, SCADA, AMI network, and DERs. Testbed-based research is essential for research concerning: (1) Vulnerability assessment, (2) Impact analysis, and (3) Attack-defense evaluation and validation. Table 4 lists a number of CPS testbeds in the U.S.

5. Potential threats

5.1. Overview

Existing security protection and mitigation mechanisms do not necessarily apply to the smart grid environment. Difficulties arise from the strict availability requirements of a power grid. For example, the GOOSE protocol used between protection IEDs and smart controllers (circuit breakers) in a SAS requires 4 ms latency, while many other grid applications require latencies of 30, 40 and 100 ms. The process time in most protection mechanisms cannot meet this requirement. Since analog communication systems have been deployed with various types of physical equipment in a power grid, it is necessary to upgrade them to be compatible with the smart grid technology.

5.2. Synchronization of smart grid data

GPS provides precise timing information to synchronize the large number of measurements. However, civilian GPS bands do not provide authentication and encryption mechanisms. GPS spoofing attacks can disrupt time synchronization of measurements in a WAMS, causing misoperations in a power system [70–72]. Although detection systems for time stamp attacks have been proposed, as shown in Table 3, there is not an effective method to restore correct time stamps for attacked data points. Thus, a mitigation method should remove the attack source quickly.

5.3. Vulnerability of wireless communication

Wireless technology enables communication among devices without being limited by physical cables and rugged terrain. In a smart grid, DA, AMI and PMU systems utilize wireless systems to transmit/receive data. Based on current regulations on the frequency spectrum, most wireless communications use industrial, scientific, and medical (ISM) radio band for communication channels [73,74]. Since ISM band is license-free, adversaries can legally access the bandwidth, causing an increase in cyber security risks. Under this circumstance, reliable encryption and authentication mechanisms are critical for protection of data confidentiality and integrity. As a matter of fact, latest cryptographic mechanisms already made eavesdropping difficult. However, data availability is not ensured in a wireless communication environment. A portable software defined radio transmitter is able to emit wireless signals at the designated frequency bandwidth in an open space [75]. If attackers launched a jamming attack near smart grid devices (e.g., smart meters, meter data collectors, DA remote control devices, and GPS antenna of PMUs), components can be disconnected in a certain area. The effective area depends on the emission power of a jamming device (i.e., signal transmitter).

5.4. Validation of ADS and IDS

Tests can be conducted to determine a system's vulnerabilities with respect to cyber attacks. However, most of the validation work involves either cyber or physical system simulators. It is not necessarily applicable to the real world environment. Taking the communication protocol as an example, a practical encryption mechanism can secure data against eavesdropping. Nonetheless, it requires extra time to encrypt and decrypt the data. To avoid the problem, a unified benchmark system is needed for the performance evaluation of an ADS/IDS. For example, [76] provides a framework to evaluate cyber protection systems in AMI.

Table 4
Some CPS testbeds in the U.S.

Testbed Name	Institute	Features
Smart City Testbed [64]	Washington State University	▪ Multiple industry standards based network simulation environment, covering transmission and distribution systems ▪ Power systems simulator ▪ Physical devices integration
National SCADA Test Bed [65]	U.S. National Labs (Argonne, Idaho, Oak Ridge, Pacific Northwest, and Sandia)	▪ Comprehensive components of cyber and physical systems, including full size physical substations
Virtual Power System Testbed [66]	University of Illinois at Urbana-Champaign	▪ Real-time immersive network simulation environment. ▪ Power system simulator
PowerCyber Security Testbed [67]	Iowa State University	▪ Accessible to remote users ▪ Wide-area network emulation (ISEAGE) ▪ Power system simulator
Distribution Cyber Security Testbed [68]	National Renewable Energy Laboratory	▪ Focus on cyber security of distribution systems ▪ Able to interact with field equipment
SCADA Security Testbed [69]	Mississippi State University	▪ Integration with PMUs and the communication system ▪ Power system simulation

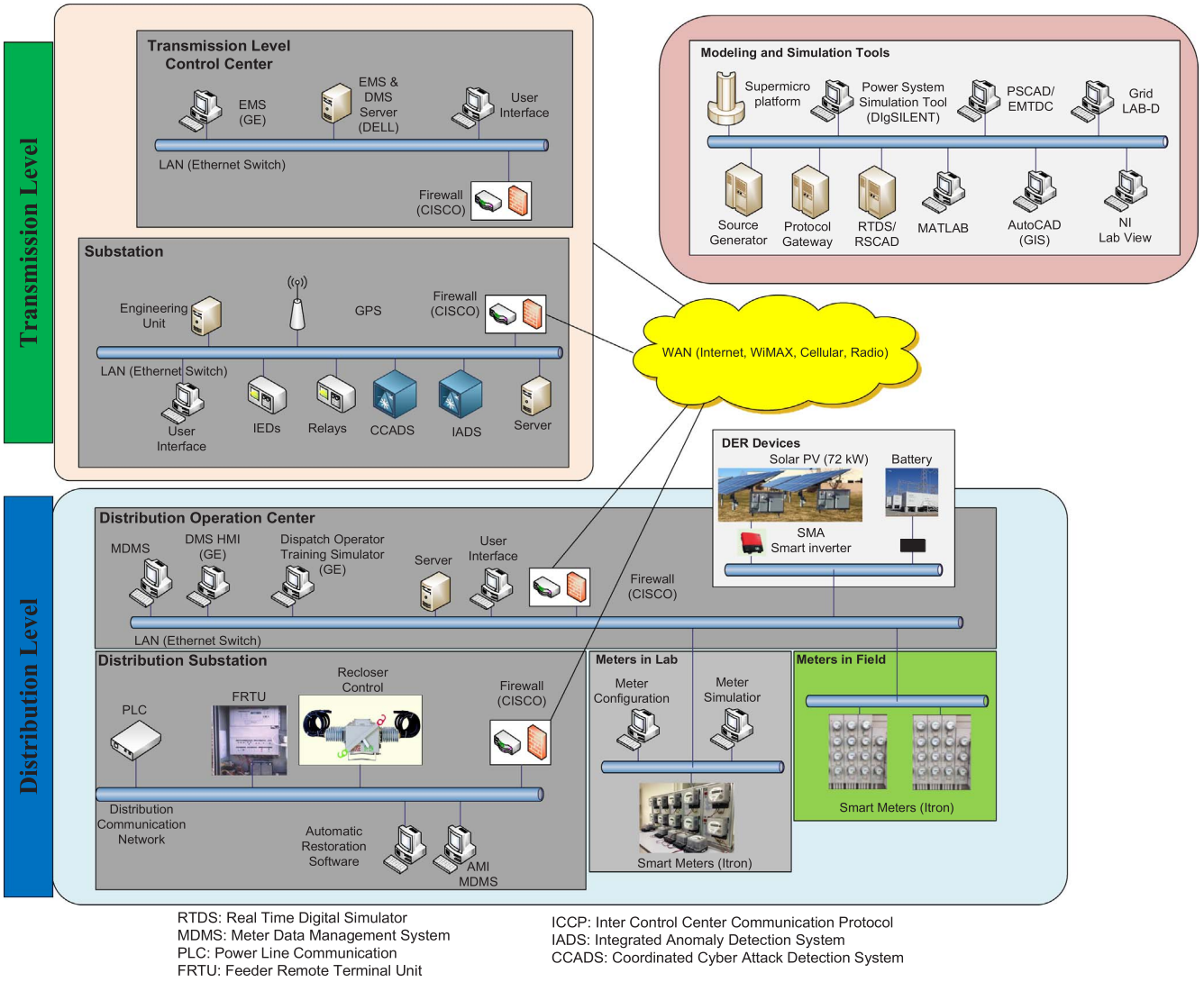

Fig. 4. SCT at WSU.

5.5. Coordinated attacks

Since power grids are designed to be robust, simple cyber attacks are unlikely to cause operational impacts to the grid. In recent attack events on Ukraine's power grids [1] and the physical attack on PG&E's transmission substation in San Jose, California [77], attackers have a well-organized plan including multiple attack steps within a time window. Unfortunately, most ADS/IDS cannot handle coordinated cyber attack events since they are designed to monitor a local area. In a coordinated cyber attack, decoys might deceive defenders to waste the protection resource on minor abnormality in a power system.

Table 5
Modules of SCT at WSU.

	Subsystem	Physical devices	Cyber components
Transmission	Control Center	HMI and data servers	EMS, firewalls, DNP 3.0
	SAS	Protective IEDs and data servers	HMI, firewalls, IEC 61,850 and DNP 3.0
Distribution	Operation Center	HMI and data servers	DMS, firewalls, DNP 3.0
	Distribution Automation	Feeder protection relays and automated switches	DNP 3.0
	AMI	Smart meters and data collector	IEEE 802.15.4 and ANSI C12.19
	DER	Solar panels (72 kW) and smart inverters	MODBUS and VOLTTRON [80]

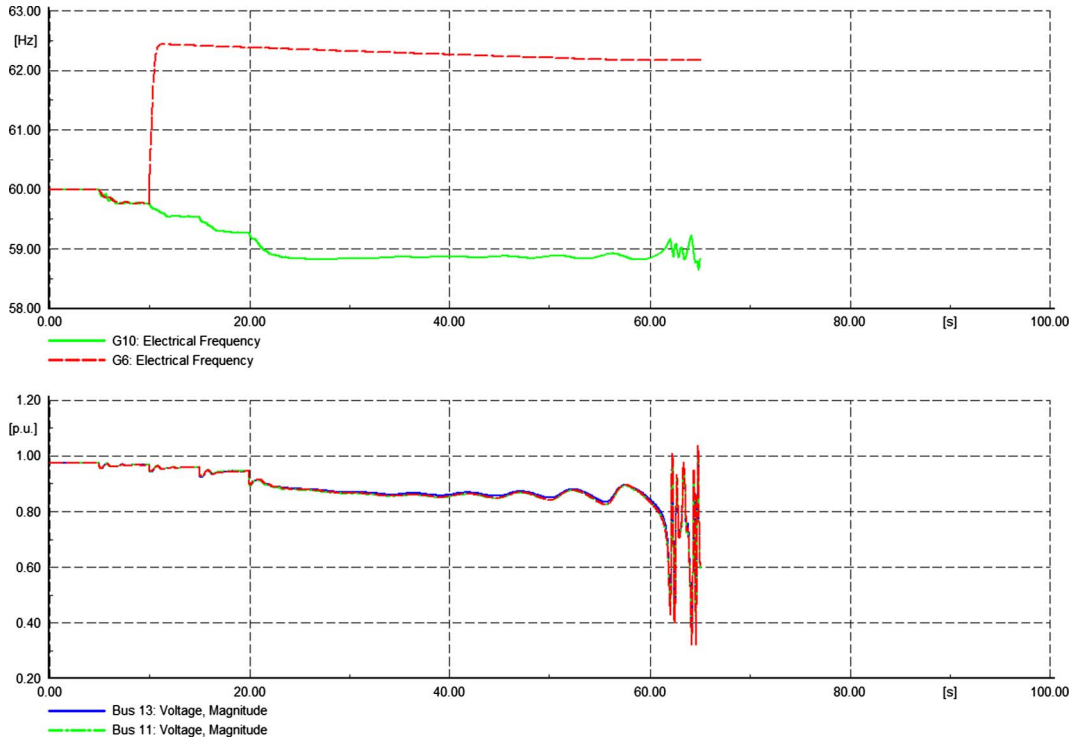

Fig. 5. Attacks trigger cascading events in IEEE 39-bus system.

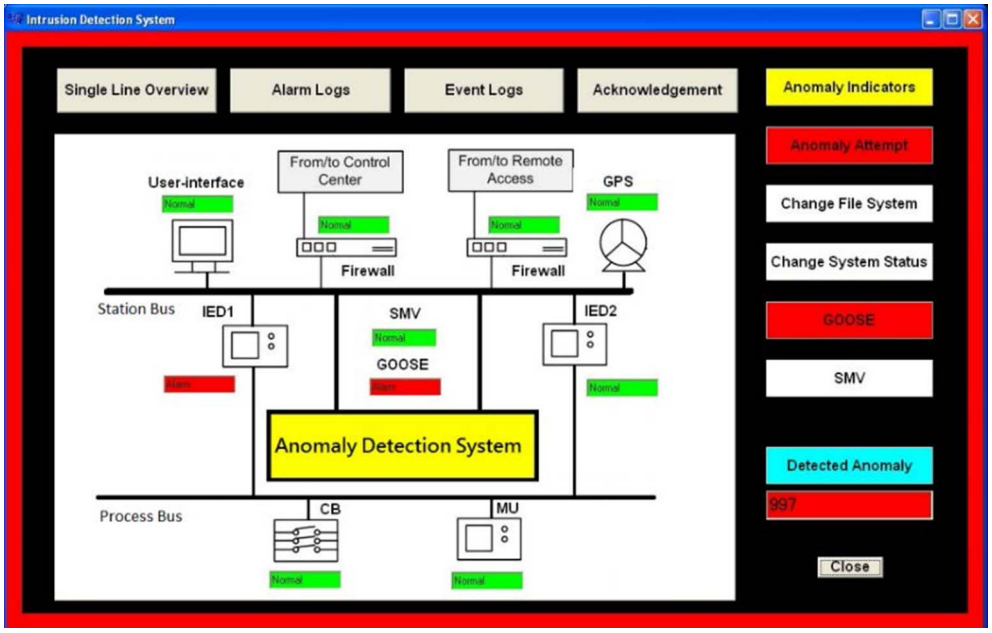

Fig. 6. HMI of the proposed IADS.

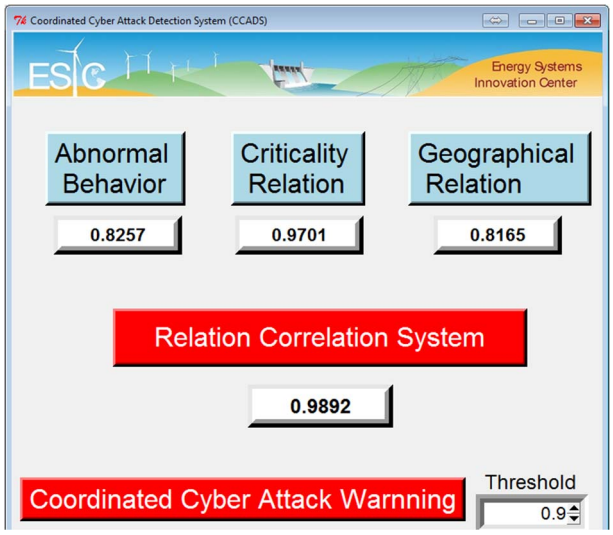

Fig. 7. The HMI of CCADS.

5.6. Modeling of human factor

In some cyber attack scenarios, intruders use incorrect system information to mislead operators. A power system can become unstable due to inappropriate operations. Under this circumstance, cyber protection systems cannot trigger warning signals since the abnormal actions are taken by operators. The other issue is the cyber attack from insiders. According to the statistical data in 2013 [78], 34% of reported cyber crimes in the U.S. are committed by insiders. Comparing with outside attackers, insiders have better knowledge of the vulnerabilities of a power grid. Unfortunately, insider attacks are difficult to prevent and detect [79].

6. Demonstration with WSU testbed

6.1. Smart City Testbed (SCT)

SCT is a hardware-in-a-loop CPS testbed at WSU [64]. Fig. 4 and Table 5 describe the architecture of SCT. In the cyber module, SCT includes EMS/DMS and SCADA system and uses multiple communication protocols, including DNP 3.0, IEC 61,850, IEEE 802.15.4, ANSI C12.19, and Modbus. The physical system module consists of feeder protection relays, protective IEDs, smart meters and meter data collector, and solar panels with smart inverters. DIgSILENT PowerFactory is used as a power system simulation tool. The simulation functions include time domain simulation, dynamic analysis, state estimation, and optimal power flow. It also supports transmission and distribution system modeling. With the OPC communication, PowerFactory can be connected with the cyber module to provide a simulation environment for cyber system events.

6.2. Cyber physical system security

Researchers are working to develop trustworthy defense against cyber attacks on a smart grid. In [38], an integrated ADS (IADS) is proposed for securing the substation communication system. The proposed IADS combines the capabilities of network- and host-based ADSs. To detect anomalies in a substation, a signature database is established for inspection of GOOSE and SV packets by NIDS. Violations of predefined rules trigger an intrusion alarm. HADS, on the other hand, applies a temporal anomaly detection method to generate an event log matrix by recording each type of anomalies in physical devices. The proposed IADS also validates its performance in a simulated substation attack using SCT. Ukrainian's power grid incident shows that the coordinated cyber attacks can make a significant impact. A coordinated cyber attack detection system (CCADS) [81] is proposed based on the work of IADS.

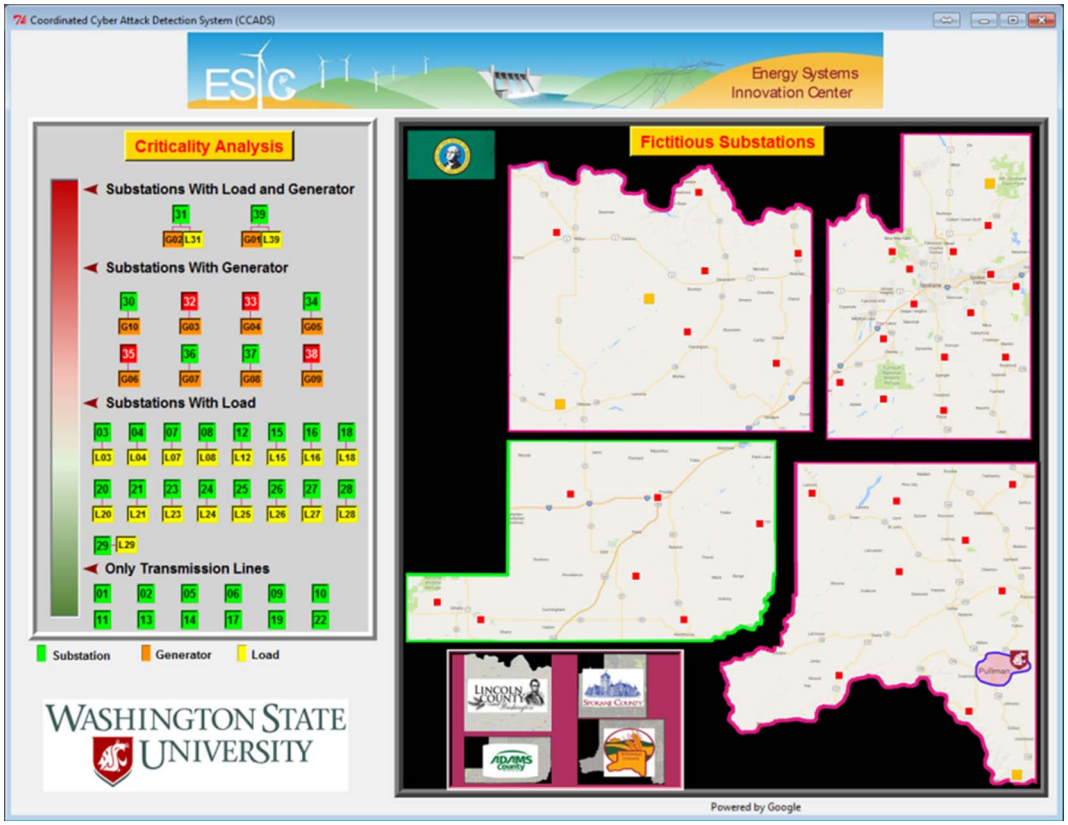

Fig. 8. HMI of CCADS presenting the criticality and geography relations of targeted substation.

A coordinated cyber attack has unique features: (1) A well-organized attack plan before the attack, and (2) Each attack step related to other step(s). Based on these observations, CCADS is designed to identify pre-defined relations among detected events captured by IADS. Three pre-defined relations are developed: anomalies, targeted substation locations, and criticality of substations. The proposed Relation Algorithm (RA) provides a reasoning process to quantify the likelihood of coordinated cyber attack events. The index ranges from 0 to 1, representing the strength of the relations. Finally, a relation correlation system combines the indices from all relations to calculate the similarity index. If the similarity index is greater than a user-defined threshold, the attack event is judged to be a coordinated cyber attack. The threshold represents the sensitivity of CCADS.

In this paper, a demonstration with two attack scenarios on the IEEE 39 bus system is provided to:

1. Demonstrate how the SCT supports cyber security research.
2. Demonstrate the collaboration between the proposed IADS and CCADS.
3. Demonstrate how the proposed ADSs protect a power grid against coordinated cyber attacks.

In this demonstration, attackers are assumed to have the knowledge to access multiple substation communication systems. By capturing and analyzing unencrypted GOOSE packets, attackers are able to modify and resend them to trip circuit breakers in targeted substations.

In the first attack scenario, attackers' targets are substations 38, 35, 33 and 32 since these substations connect to generation sources. The attack starts at t = 5 s, and the targets are compromised one by one every 5 s. Once the last targeted substation (i.e., substation 32) is compromised, this power system collapses due to insufficient power generation. Fig. 5 is a screenshot from PowerFactor with the measurements (i.e., voltage and frequency) during the cyber attack. After 4 generators are disconnected from the power grid, cascading events are triggered. Finally, a wide area power outage is caused by the coordinated cyber attacks.

In the second scenario, the same attack is simulated with the proposed ADSs. Fig. 6 shows the interface of IADS in one of targeted substations. It indicates the number of malicious GOOSE packets that have been detected. Once the CCADS receives the information from IADS, it performs the reasoning to calculate the index value for each pre-defined relation and the final result. Fig. 7 shows that the relation correlation system gives an index value of 0.9892 which is higher than the user-defined threshold, 0.9. Thus, the CCADS triggers the alarm to report a coordinated cyber attack. Fig. 8 shows the criticality and geographic relations of targeted substations by graphical interfaces. During the cyber attack, circuit breakers remain closed in targeted substations since the proposed IADS captures the malicious network packets. Thus, effectiveness of the proposed ADSs is validated by the SCT.

7. Conclusion

ICT systems have become a backbone of modern power grids. Cyber security is important for stability and reliability of the smart grid. This paper is a state-of-the-art survey of cyber security R&D for a smart grid. Vulnerabilities are increasingly present in the cyber-power system environment due to the growing dependency on computer systems and digital communication. Since there are limitations for firewalls to identify malicious packets, ADSs/IDSs are critical to detect anomalies inside a private network (e.g., LAN, HAN, and NAN). Furthermore, the performance of detection systems should meet the requirements for power systems, such as accuracy and communication delay. With a realistic CPS testbed, researchers can test their cyber protection systems to evaluate whether requirements are met.

Research results on cyber security of a smart grid are demonstrated on a cyber-power system testbed. Test cases of coordinated cyber attack show that attackers are able to impact a power system by compromising critical substations. Furthermore, the proposed IADS and CCADS are applied to validate the anomaly detection capabilities. Once the malicious network packets are detected by IADSs, CCADS analyzes the predefined relations by collecting attack information from each targeted substation. Based on the similarity index which is calculated by CCADS, the coordinated cyber attack alarm is triggered. Concurrently, IADSs execute the mitigation process, blocking the circuit breaker operations and sending a disconnect command to firewalls to block the intruders' connections.

In order to prevent unknown cyber attacks, Section 5 summarizes the potential cyber security vulnerabilities to indicate research needs for enhancing cyber security of a smart grid. Wireless communications are threatened by jamming attacks since the absence of mitigation approaches creates a weakness in connectivity of smart grid components. GPS signals are vulnerable to spoofing attacks that may impact the time-based synchronization requirements for PMU data. Then, there is no standard to assess the performance of ADSs/IDSs. Although several detection systems have been proposed and tested for different sectors of a smart grid, there is no guarantee for the detection rate in practice. Finally, further research on coordinated cyber attacks is much needed. The Ukrainian power grid attack has shown that coordinated cyber attacks increase the success rate of cyber intrusions. Also, the response of operators should be taken into account in the cyber security studies. In a cyber attack event, an operator could be deceived by falsified data.

Acknowledgments

This paper is based on work supported by the Department of Energy under Award Number DE-OE0000780. The views and opinions of the authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. The authors also thank DOE for their funding under project Grid Modernization Laboratory Call (GMLC) Project GM0100.

Conflict of Interest

None.

Appendix A. Supplementary material

Supplementary data associated with this article can be found, in the online version, at http://dx.doi.org/10.1016/j.ijepes.2017.12.020.

References

[1] SANS and Electricity Information Sharing and Analysis Center (E-ISAC). Analysis of the cyber attack on the Ukrainian power grid; Mar. 18, 2016. Available: < http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf > .
[2] Clavel F, Savary E, Angays P, Vieux-Melchior A. Integration of a new standard: a network simulator of IEC 61850 architectures for electrical substations. IEEE Ind Appl Mag 2015;21(1):41–8.
[3] Cheng X, Lee WJ, Pan X. Modernizing substation automation systems: adopting IEC Standard 61850 for modeling and communication. IEEE Ind Appl Mag 2017;23(1):42–9.
[4] North American SynchroPhasor Initiative. Sychrophasors & the grid; 2017. Available: < https://www.naspi.org/sites/default/files/reference_documents/naspi_naruc_silverstein_20170714.pdf > .
[5] IEEE Standard for Synchrophasor Data Transfer for Power Systems. IEEE Standard C37.118.2-2011 (Revision of IEEE Standard C37.118-2005); 2011.
[6] Fischer R, Schulz N, Anderson GH. Information management for an automated meter reading system. In: Proc of the 62nd American power conf; Apr. 2000.
[7] CENTRON Meter Technical Reference Guide. Liberty Lake, WA, USA: Itron Inc.; 2006. Available: < http://www.smartmetereducationnetwork.com/uploads/how-to-tell-if-I-have-a-ami-dte-smart-advanced-meter/Itron%20Centron%20Meter%20Technical%20Guide1482163-201106090057150.pdf > .
[8] IEEE Standard for Low-Rate Wireless Networks. IEEE Standard 802.15.4-2015 (Revision of IEEE Standard 802.15.4-2011); 2016.

[9] Leon G. Smart planning for smart grid AMI mesh networks. Technology white paper. EDX Wireless [Online]. Available: < http://www.edxwireless.biz/news/EDXWP_Smart_Grid_AMI_Mesh_ Networks_May_11.pdf > .

[10] The U.S. Pacific Northwest National Laboratory (PNNL). AMI communication requirements to implement demand-response: applicability of hybrid spread spectrum wireless [Online]. Available: < http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20806.pdf > .

[11] Jiang Y, Liu CC, Diedesch M, Lee E, Srivastava AK. Outage management of distribution systems incorporating information from smart meters. IEEE Trans Power Syst Sept. 2016;31(5):4144–54.

[12] Smart Grid Interoperability Panel (SGIP). Distributed Energy Resources (DER): hierarchical classification of use cases and the process for developing information exchange requirements and object models, white paper; 2014. Available: < http://www.sgip.org/wp-content/uploads/Distributed-Energy-Resources_DER-Hierarchical-Classification-of-Use-Cases-and-the-Process-for-Developing-Information-Exchange-Requirements-and-Object-Models-2014-07-18.pdf > .

[13] Qi J, Hahn A, Lu X, Wang J, Liu CC. Cybersecurity for distributed energy resources and smart inverters. IET Cyber-Phys Syst: Theor Appl 2016;1(1):28–39.

[14] NCCIC and ICS-CERT. NCCIC/ICS-CERT 2015 year in review; Apr. 19, 2016. Available: < https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf > .

[15] The U.S. Department of Energy. Cyber threat and vulnerability analysis of the U.S. electric sector; Aug. 2016. Available: < https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf > .

[16] Chapman D, Fox A, Stiffler R. Cisco secure PIX firewalls. Cisco Press; 2001.

[17] Hari A, Suri S, Parulkar G. Detecting and resolving packet filter conflicts. In: Proc of the IEEE INFOCOM 2000. Conf comput commun; 2000. p. 1203–12.

[18] Hamed H, Al-Shaer E, Marrero W. Modeling and verification of IPSec and VPN security policies. In 13TH IEEE intl conf network protocols (ICNP'05); 2005. p. 10.

[19] Al-Shaer ES, Hamed HH. Discovery of policy anomalies in distributed firewalls. In: IEEE INFOCOM 2004, vol. 4; 2004. p. 2605–16.

[20] Yuan L, Chen H, Mai J, Chuah CN, Su Z, Mohapatra P. FIREMAN: a toolkit for firewall modeling and analysis. In: 2006 IEEE symp. security and privacy (S&P'06), Berkeley/Oakland, CA; 2006.

[21] Modbus Application Protocol Specification, V1.1B Modbus Organization; 2006. Available: < http://www.modbus-IDA.org > .

[22] Padilla E, Agbossou K, Cardenas A. Towards smart integration of distributed energy resources using distributed network protocol over ethernet. IEEE Trans Smart Grid Jul. 2014;5(4):1686–95.

[23] Shahzad A, Musa S, Aborujilah A, Irfan M. Industrial Control Systems (ICSs) vulnerabilities analysis and SCADA security enhancement using testbed encryption. In: Proc of the ACM 8th intl conf ubiquitous inf. management and commun (ICUIMC '14). New York, NY; Jan. 2014. p. 7.

[24] Phan RCW. Authenticated modbus protocol for critical infrastructure protection. IEEE Trans Power Del July 2012;27(3):1687–9.

[25] Hayes G, El-Khatib K. Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol. In: 2013 Third intl conf commun and inf technol (ICCIT), Beirut; 2013. p. 179–84.

[26] Gilchrist G. Secure authentication for DNP3. In: Proc IEEE power energy soc gen meeting-convers del elect energy 21st century, Pittsburgh, PA, USA; 2008. p. 1–3.

[27] Amoah R, Camtepe S, Foo E. Securing DNP3 broadcast communications in SCADA systems. IEEE Trans Ind Informat Aug. 2016;12(4):1474–85.

[28] Song KY, Yu KS, Lim D. Secure frame format for avoiding replay attack in distributed network protocol (DNP3). In: 2015 Intl conf inf and comm technol convergence (ICTC), Jeju; 2015. p. 344–49.

[29] Ericsson G. Toward a framework for managing information security for an electric power utility—CIGRÉ experiences. IEEE Trans Power Del Jul. 2007;22(3):1461–9.

[30] Falliere N, Murchu LO, Chien E. W32.Stuxnet Dossier. Symantec security response, Version 1.4; Feb. 2011. Available: < https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf > .

[31] Kushner D. The real story of stuxnet. IEEE Spectr Mar. 2013;50(3):48–53.

[32] Ten CW, Liu CC, Manimaran G. Vulnerability assessment of cybersecurity for SCADA systems. IEEE Trans Power Syst Nov. 2008;23(4):1836–46.

[33] Zhang Y, Wang L, Xiang Y, Ten CW. Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation. IEEE Trans Power Syst Nov. 2016;31(6):4379–94.

[34] Amanullah MTO, Kalam A, Zayegh A. Network security vulnerabilities in SCADA and EMS. In: 2005 IEEE/PES transmission & distribution conference & exposition: Asia and Pacific, Dalian; 2005. p. 1–6.

[35] Li GW, Ju WY, Shi DY. Functional vulnerability assessment of SCADA network. In: 2012 Asia-Pacific power and energy eng conf, Shanghai; 2012. p. 1–4.

[36] Hong J, Liu CC, Govindarasu M. Detection of cyber intrusions using network-based multicast messages for substation automation. In: 2014 IEEE power & energy society innovative smart grid technol conf (ISGT), Washington, DC; 2014. p. 1–5.

[37] Strobel M, Wiedermann N, Eckert C. Novel weaknesses in IEC 62351 protected smart grid control systems. In: 2016 IEEE intl conf smart grid commun (SmartGridComm), Sydney, NSW; 2016. p. 266–70.

[38] Hong J, Liu CC, Govindarasu M. Integrated anomaly detection for cyber security of the substations. IEEE Trans Smart Grid Jul. 2014;5(4):1643–53.

[39] Namboodiri V, Aravinthan V, Mohapatra SN, Karimi B, Jewell W. Toward a secure wireless-based home area network for metering in smart grids. IEEE Syst J Jun. 2014;8(2):509–20.

[40] Liang X, Li X, Lu R, Lin X, Shen X. UDP: usage-based dynamic pricing with privacy preservation for smart grid. IEEE Trans Smart Grid Mar. 2013;4(1):141–50.

[41] Krebs B. FBI: Smart meter hacks likely to spread; 2012. Available: < http://krebsonsecurity.com/2012/04/fbi-smart-meterhacks-likely-to-spread/ > .

[42] Rosenbaum H. Danville utilities sees increase in meter tampering; 2012. Available: < http://www.wset.com/story/20442252/danville-utilities-sees-increase-in-meter-tampering > .

[43] Bakken DE, Bose A, Hauser CH, Whitehead DE, Zweigle GC. Smart generation and transmission with coherent, real-time data. Proc IEEE Jun. 2011;99(6):928–51.

[44] North American Electric Reliability Corporation (NERC). CIP standard. Available online: < ftp://www.nerc.com/pub/sys/all_updl/standards/sar/CIP-002-009-1_30-day_Pre-ballot_Comment.pdf > .

[45] The U.S. Department of Energy, Energy Sector Control Systems Working Group (ESCSWG). Roadmap to achieve energy delivery system cyber security. Available online: < http://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011 > .

[46] National Institute for Standards and Technology. Guidelines for smart grid cyber security, NISTIR 7628. [Online]. Available: < http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778 > .

[47] National Institute for Standards and Technology. The cyber security coordination task group: smart grid cyber security strategy and requirements. Available online: < http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf > .

[48] Yang Y, McLaughlin K, Sezer S, Littler T, Im EG, Pranggono B, et al. Multiattribute SCADA-specific intrusion detection system for power networks. IEEE Trans Power Del Jun. 2014;29(3):1092–102.

[49] Zhang Y, Wang L, Sun W, Green II RC, Alam M. Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Trans Smart Grid Dec. 2011;2(4):796–808.

[50] Yang Y, McLaughlin K, Littler T, Sezer S, Pranggono B, Wang HF. Intrusion detection system for IEC 60870-5-104 based SCADA Networks. In: 2013 IEEE power & energy society general meeting, Vancouver, BC; 2013. p. 1–5.

[51] Mo Y, Chabukswar R, Sinopoli B. Detecting integrity attacks on SCADA systems. IEEE Trans Control Syst Technol Jul. 2014;22(4):1396–407.

[52] Barbosa RRR, Sadre R, Pras A. Flow whitelisting in SCADA networks. Int J Crit Infrastruct Protect Aug. 2013;6:150–8.

[53] Hahn A, Govindarasu M. Model-based intrusion detection for the smart grid (MINDS). In: ACM proc of the eighth annual CSIIRW, New York, NY, USA; 2013.

[54] Ten CW, Hong J, Liu CC. Anomaly detection for cybersecurity of the substations. IEEE Trans Smart Grid Dec. 2011;2(4):865–73.

[55] Yang Y, Xu HQ, Gao L, Yuan YB, McLaughlin K, Sezer S. Multidimensional intrusion detection system for IEC 61850-based SCADA networks. IEEE Trans Power Del Apr. 2017;32(2):1068–78.

[56] Premaratne UK, Samarabandu J, Sidhu TS, Beresh R, Tan JC. An intrusion detection system for IEC61850 automated substations. IEEE Trans Power Del Oct. 2010;25(4):2376–83.

[57] Wu J, Xiong J, Shil P, Shi Y. Real time anomaly detection in wide area monitoring of smart grids. In: 2014 IEEE/ACM intl conf comput-aided design (ICCAD), San Jose, CA; 2014. p. 197–204.

[58] Fan Y, Zhang Z, Trinkle M, Dimitrovski AD, Song JB, Li H. A cross-layer defense mechanism against gps spoofing attacks on PMUs in smart grids. IEEE Trans Smart Grid Nov. 2015;6(6):2659–68.

[59] Mitchell R, Chen IR. Behavior-rule based intrusion detection systems for safety critical smart grid applications. IEEE Trans Smart Grid Sept. 2013;4(3):1254–63.

[60] McLaughlin S, Holbert B, Fawaz A, Berthier R, Zonouz S. A multi-sensor energy theft detection framework for advanced metering infrastructures. IEEE J Select Areas Commun Jul. 2013;31(7):1319–30.

[61] Liu Y, Hu S, Ho TY. Leveraging strategic detection techniques for smart home pricing cyberattacks. IEEE Trans Depend Secure Comput 2016;13(2):220–35.

[62] Liu X, Zhu P, Zhang Y, Chen K. A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. IEEE Trans Smart Grid Sept. 2015;6(5):2435–43.

[63] Berthier R, Sanders W. Specification-based intrusion detection for advanced metering infrastructures. In: Proc IEEE 17th Pacific rim int symp dependable computing; Dec. 2011. p. 184–93.

[64] Sun CC, Hong J, Liu CC. A co-simulation environment for integrated cyber and power systems. In: 2015 IEEE intl conf smart grid commun (SmartGridComm), Miami, FL; 2015. p. 133–38.

[65] Idaho National Laboratory. Fact sheet: national SCADA test bed; 2009. Available: < https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf > .

[66] Bergman DC, Jin D, Nicol DM, Yardley T. The virtual power system testbed and inter-testbed integration. In: 2nd Workshop cyber security experimentation and test; Aug. 2009.

[67] Ashok A, Krishnaswamy S, Govindarasu M. PowerCyber: a remotely accessible testbed for cyber physical security of the smart grid. In: 2016 IEEE power & energy society innovative smart grid technol conf (ISGT), Minneapolis, MN; 2016. p. 1–5.

[68] National Renewable Energy Laboratory (NREL). NREL's cybersecurity initiative aims to wall off the smart grid from hackers; 2016. Available: < http://www.nrel.gov/news/features/2016/21612 > .

[69] Reaves B, Morris T. An open virtual testbed for industrial control system security research. Int J Inf Security 2012;11(4):215–29.

[70] Bonebrake C, Ross O'Neil L. Attacks on GPS time reliability. IEEE Secur Priv 2014;12(3):82–4.

[71] Zhang Z, Gong S, Dimitrovski AD, Li H. Time synchronization attack in smart grid: impact and analysis. IEEE Trans Smart Grid Mar. 2013;4(1):87–98.

[72] Jiang X, Zhang J, Harding BJ, Makela JJ, Domínguez-García AD. Spoofing GPS receiver clock offset of phasor measurement units. IEEE Trans Power Syst 2013;28(3):3253–62.

[73] The U.S. Department of Commerce. United States frequency allocations. Available

online: < https://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf > .
[74] Loy M, Karingattil R, Williams L. ISM-band and short range device regulatory compliance overview. Texas instruments, SWRA048; May, 2005. Available: < http://www.ti.com/lit/an/swra048/swra048.pdf > .
[75] Alakoca H, Tugrel HB, Kurt GK, Ayyildiz C. CP and pilot jamming attacks on SC-FDMA: performance tests with software defined radios. In: 2016 10th Intel conf signal processing and commun syst (ICSPCS), Gold Coast, QLD; 2016. p. 1–6.
[76] Cárdenas AA, Berthier R, Bobba RB, Huh JH, Jetcheva JG, Grochocki D, et al. A framework for evaluating intrusion detection architectures in advanced metering infrastructures. IEEE Trans Smart Grid Mar. 2014;5(2):906–15.
[77] CNN. Sniper Attack on silicon valley power grid spurs security crusade by ex-regulator; Feb. 7, 2014. Available: < http://www.cnn.com/2014/02/07/us/california-sniper-attack-power-substation/index.html > .
[78] Kluitenberg H. Security risk management in it small and medium enterprises. In: Proc 20th twenty student conf IT, Enschede, The Netherlands; 2014.
[79] Bao H, Lu R, Li B, Deng R. BLITHE: behavior rule-based insider threat detection for smart grid. IEEE Internet Things J Apr. 2016;3(2):190–205.
[80] Pacific Northwest National Laboratory. VOLTTRON 3.0: user guide; Nov. 2015. Available: < http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24907.pdf > .
[81] Sun CC, Hong J, Liu CC. A coordinated cyber attack detection system (CCADS) for multiple substations. In: 2016 power syst computation conf (PSCC), Genoa, IT; 2016. p. 1–7.