IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 25, 2020, accepted December 18, 2020, date of publication December 24, 2020,
date of current version January 5, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3047341

Intrusion Detection Against MMS-Based Measurement Attacks at Digital Substations

RUOXI ZHU[1], (Graduate Student Member, IEEE), CHEN-CHING LIU[1], (Life Fellow, IEEE), JUNHO HONG[2], (Member, IEEE), AND JIANKANG WANG[3], (Member, IEEE)

[1]The Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, VA 24061, USA
[2]Department of Electrical and Computer Engineering, University of Michigan–Dearborn, Dearborn, MI 48128, USA
[3]Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210, USA

Corresponding author: Ruoxi Zhu (ruoxi@vt.edu)

This work was supported by the National Science Foundation at Virginia Tech, a Collaborative Project with The Ohio State University, under Grant ECCS-1824577.

ABSTRACT Information and Communications Technology (ICT) supports the development of novel control and communication functions for monitoring, operation, and control of power systems. However, the high-level deployment of ICT also increases the risk of cyber intrusions for Supervisory Control And Data Acquisition (SCADA) systems. Attackers can gain access to the protected infrastructures of the grid and launch attacks to manipulate measurements at the substations. The fabricated measurements can mislead the operators in the control center to take undesirable actions. The Intrusion Detection System (IDS) proposed in this paper is deployed in IEC 61850 based substations. The proposed IDS identifies falsified measurements in Manufacturing Messaging Specification (MMS) messages. By cross-checking the consistency of electric circuit relationships at the substation level in a distributed manner, the falsified measurements can be detected and discarded before the malicious packets are sent out of the substations through DNP3 communication. A cyber-physical system testbed is used to validate the performance of the proposed IDS. Using the IEEE 39-bus test system, simulation results demonstrate high accuracy of the proposed substation-based intrusion detection system.

INDEX TERMS Cyber security of substation, measurement-based attack, MMS, IEC 61850, intrusion detection, SCADA.

I. INTRODUCTION

As complex cyber-physical systems, modern power grids utilize layers of ICT to maintain system reliability and efficiency. The fast-increasing connectivity through industrial control systems is known to be a source of vulnerabilities that can be exploited for potential cyber intrusions [1]. Substations in a smart grid play an important role to integrate the functions of communication and power infrastructures. In December 2016, the new malware, "CRASHOVERRIGE," is deployed to compromise transmission level substations in Ukraine [2]. In comparison with the malware "BlackEnergy3," used in the cyberattack in Ukraine, December 2015, the new malware is capable of understanding and compromising industrial processes to disrupt the operations at substations.

Much of the literature on cyber security of power grids is concerned with the SCADA system in the transmission level. False data injection attacks (FDIAs) are well studied as a threat to cyber security of a smart grid [3]. Under the assumption that the adversary has the knowledge of system configuration, malicious measurements may be able to bypass bad data detection [4]. Research has been conducted on the attack model of FDIAs, impact of FDIAs, and vulnerability assessment for state estimation with respect to FDIAs [5]–[7]. Phasor Measurement Units (PMUs) are used as countermeasures to defend against FDIAs [8]–[10]. By analyzing the behavior of FDIAs, data driven and machine learning methods are exploited to detect attacks in real-time [11]–[13]. However, the previous work is mostly centralized, which is not designed to detect FDIAs before falsified measurements arrive at the control center level. To prevent the malicious measurements from intrusion into software applications at the control center, e.g., the Energy Management System (EMS), it is important to detect and stop the falsified measurements before they are sent out of the substations.

IEC 62351 standard is developed to handle the security of multi-protocol messaging [14]. However, currently no

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. Inácio.

industrialized solution is deployed in Substation Automation Systems (SASs). On the other hand, DNP3 Secure Authentication (DNP3-SA) [15] provides a security mechanism for communication between substations and the control center; however, it is not able to detect attacks in which falsified measurements are encapsulated in the payload of DNP3 packets before authentication and integrity checking. Hence, substations are vulnerable to such attacks on measurements.

Motivated by the critical need to detect measurement attacks at the substation level, this paper is concerned with the study of attack paths in SAS and defense actions. Various studies in the literature have explored the cyber defense of substation automation. The risk and vulnerability assessment is proposed for SCADA and IEC 61850 based substations [16], [17]. To counter the threats to an IEC 61850-based substation, a signature-based IDS is developed based on the data collected by simulating the attacks on IEDs [18]. In [19]–[22], a comprehensive IDS integrates protocol specification, and logical behaviors for detecting abnormal behaviors within the cyber-physical systems. Based on IEC 61850 standards, the collaborative intrusion detection system proposed in [23] monitors and detects cyberattacks by screening the characteristics of Generic Object Oriented Substation Events (GOOSE) and Sample Value (SV) packets at each IED. Game-theoretic techniques are used in [24] to optimize the security mechanism for a large number of substations against coordinated attacks. Since the ICT-based IDS has a limited impact on such intrusions that bypass the cyber defense, some studies propose defense strategies according to physical nature of the power system. To detect intrusions against the protection system, context information based defense is proposed [25], [26]. By learning the pattern of attack data, an IDS is proposed [27] for IEEE 1815.1-based network at substations.

Regarding the detection of measurement attacks, several issues are observed: 1) Existing methods identify false measurements based on state estimation and bad data detection in the control center level. In other words, the technology does not detect measurement-based attacks at the substations before malicious measurements arrive at the control centers. 2) The specification-based IDS at the substation level is not able to identify false measurements if the fabricated data is encapsulated with legitimate headers. 3) Cyberattacks targeting measurements at multiple substations cannot be detected by local substation IDSs without a system strategy. 4) Although IEC 62351-4 specifies the cyber security of MMS, it is not commonly applied.

The proposed IDS in this paper is able to identify falsified measurements in MMS messages. Based on the law of physics of the electrical network, a distributed IDS against measurement attacks in the substation is proposed. The contributions of this paper are:

1) Proposing a new method to identify contaminated measurements at the substation level. By doing so, falsified measurements will be intercepted before they are sent to the control center.
2) Developing a distributed IDS in the substation level, which accurately determines the attack targets especially the cyberattack against multiple substations. Test results show that proposed IDS is efficient and promising for the real-time environment.
3) Analyzing the potential attack path of measurement attacks in the substation network. Based on the attack path, the attack model is developed for the measurement attacks.

The remaining of this paper is organized as follows: Section II describes vulnerabilities at the substation level. In Section III, the technical approach is provided. Section IV establishes the feasibility of the proposed algorithm with respect to different attack scenarios. Section V discusses the software testbed for validation of the IDS. Section VI shows the simulation results and performance of the IDS. Finally, the conclusions and future work are given in Section VII.

II. PROBLEM FORMULATION

IEC 61850 based SAS enables different devices to cooperatively maintain system properties in a modernized substation. Specifically, based on functionalities, the physical devices are organized in three levels: the process, bay, and station levels. To support communication properties in SAS, IEC 61850 based protocols, e.g., GOOSE, SV and MMS, are used. SV messages are used for sharing measurements of Current Transformers (CTs)/Voltage Transformers (VTs) with protective IEDs. Since there is a built-in security mechanism in SV streams, e.g., Message Authentication Code (MAC) in IEC 62351-6, for ensuring integrity, the proposed method to detect and mitigate measurement-based attacks against MMS messages does not affect the substation protection scheme. As a new function for cyber security, the proposed IDS is focused on MMS messages to prevent falsified measurements from being sent out of the substations.

In digital substations, MMS communication uses a client/server model for reporting, monitoring, and control between IEDs and the SCADA system. As shown in Fig. 1, in order to transmit the measurement data to the SCADA system, the gateway as MMS client sends "read-request" to access the information contained in the IED objects. Then, the corresponding IED, as MMS server, sends the response back with the measurement data encapsulated in MMS messages. As a line of defense to detect the measurement attack at SAS, the proposed IDS is configured to detect/mitigate the falsified measurements within MMS messages before they are sent to the control center through DNP3 communication.

In the cyberattack against Ukrainian power grid [2], the adversary takes control of servers in the substations through unauthorized remote access. Once the station network is compromised, the attackers will be capable of eavesdropping MMS communication and injecting malicious packets. Without cyber security scanning at the substation level, fabricated measurements will be sequentially transmitted through DNP3 polling. The proposed

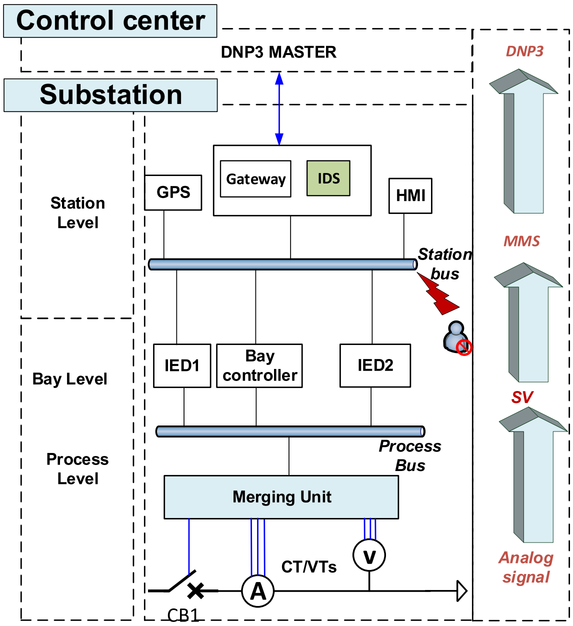


FIGURE 1. Attack path of measurement attacks.

defense action is a distributed IDS at the substation level. Falsified measurements are identified based on law of physics of the power network: Kirchhoff's Current Law (KCL), Kirchhoff's Voltage Law (KVL) and Ohm's law. The distributed nature of the proposed IDS enables each substation IDS to cross check the measurements with other substations.

III. TECHNICAL APPROACH AT SUBSTATION LEVEL

This section describes the potential measurement attack path on MMS messages and implementation of the proposed IDS at the substations.

A. MEASUREMENT ATTACK PATH IN SAS

Based on vulnerabilities with respect to measurement attacks, the attack path in the SAS is illustrated in Fig. 1.

1) BAY LEVEL AND STATION LEVEL

The substation network is accessed from the remote access point or internal network. Once adversaries compromise the targeted substation through unauthorized access, they will gain access to the bay level devices through the station network. Sequentially, the adversary executes the attacks against measured values through MMS communication between the IED and gateway.

As shown in Fig. 1, MMS messages are converted to DNP3 at the gateway according to IEEE Std 1815.1 [28], which defines the way data structures are mapped. The falsified measurements indicate a change in the system states, which creates the event data at the DNP3 outstation. Once an event polling is received, the DNP3 outstation at the substation will send the malicious data to the DNP3 master at the control center [15].

2) CONTROL CENTER LEVEL

Once the control center receives malicious DNP3 packets, system operators can be misled by fabricated measurements or triggered alarms and take undesirable actions. For example, multiple substations may send falsified high voltages at the substations. In response, operators may decide to switch off capacitor banks at these substations, leading to actual low voltage conditions in the power grid.

B. IMPLEMENTATION OF DISTRIBUTED IDS AT THE SUBSTATION

1) LAW OF PHYSICS

The proposed IDS applies the law of physics to detect anomalies in the measurements. The measurement system in IEC 61850 based substations includes sensing elements and IEDs. CT and VT (or Low-Power Voltage Transformers (LPVT) and Low–Power Current Transformers (LPCT)) are instrument transformers for current and voltage measurements. Note that CT/VT and the Merging Unit (MU) are subject to measurement errors, which may cause a violation of the detection rules, e.g., KCL, KVL or Ohm's Law. The accuracy of CT/VT and MUs under a normal condition is expressed by the accuracy class of the instrument [29]. To distinguish between measurement errors and cyberattacks, rules of the proposed IDS shown in Table 1 include the coefficient k_{ceri}/k_{veri}, given for each instrument i, $i = 1, 2, \ldots, n$. They specify the tolerance in measurement errors. Current and voltage measurements are assumed to be synchronized phasors with time stamps.

a) KCL: The current, i_{exit} (i_{enter}), denotes current phasors exiting (entering) the substation. When applying KCL to line currents at different voltage levels, the effect of a transformer must be considered. The compensation includes the magnitude and phase-shift determined by the transformation ratio and connection of the windings [30]. As shown in Table 1, when the difference between the summation of i_{exit} and that of i_{enter} is within the error tolerance, KCL is considered satisfied.

TABLE 1. IDS rules for measurement attacks.

Measurements	IDS rules
Current	Kirchhoff`s Current Law (KCL): $\left\vert\sum i_{exit} - \sum i_{enter}\right\vert \leq k_{cer1}\vert i_1\vert + \cdots + k_{cern}\vert i_n\vert$
Voltage	Kirchhoff`s Voltage Law (KVL): $\vert v_1 + \cdots + v_n\vert \leq k_{ver1}\vert v_1\vert + \cdots + k_{vern}\vert v_n\vert$
Voltage and Current	Ohm`s Law: $\left\vert v_j - v_k - i_{jk}Z_{line}\right\vert$ $\leq \text{MAX}\left\{k_{verj}\left\vert v_j\right\vert, k_{verk}\vert v_k\vert, k_{cerjk}\left\vert i_{jk}Z_{line}\right\vert\ \right\}$

b) KVL: For any loop in the circuit graph, KVL requires that the algebraic sum of voltage drops on all branches around the loop be zero. v_n denotes the voltage phasor at node n. Correspondingly, k_{vern} is the error coefficient of the voltage measurement. For each loop, one of the buses is assigned to be the responsible bus. Based on the inter-communication between substations, the responsible bus is tasked to verify KVL with measurements from other nodes in this loop. When the summation of branch voltages in the loop does not exceed the error tolerance, KVL holds.

c) Ohm‘s Law: In Table 1, current phasor i_{jk} denotes the line current between two substations j, k, and z_{line} denotes the line impedance. v_j, v_k are the voltage phasors from substation j and k *and* k_{verj}, $k_{verk}k_{cerjk}$ are the error coefficients of v_j, v_k and i_{jk}, respectively. Given the limit of the error tolerance, Ohm‘s Law between v_j and v_k is verified with local measurement i_{jk} and voltage measurement v_k from substation k.

2) DEPLOYMENT OF THE IDS IN SAS

Since MMS messages are the attack targets, the proposed IDS, as a novel security feature, is integrated with the gateway as shown in Fig. 1. Based on the proposed IDS, synchronized measurements are needed for verification by the three rules. Therefore, IEDs with IEC/TR 61850-90-5 capability are needed to provide synchronized data at the substation [31].

3) DISTRIBUTED ARCHITECTURE

To cross check measurements with other substations, the enabling technology of the proposed algorithm is the wide-area communication of synchronized measurements. IEC/TR 61850-90-5 is developed for exchanging synchrophasor data between different LANs through WANs based on IEC 61850 standard [31]. To secure the communication over public network, IEC 61850-90-5 provides message authentication and integrity mechanisms, including Group Domain of Interpretation (GDOI) key distribution model, Hash based Message Authentication Code (HMAC), and Transport Layer Security (TLS). The proposed distributed IDS shown in Fig. 2 uses IEC 61850-90-5 for secure transmission of the synchronized data.

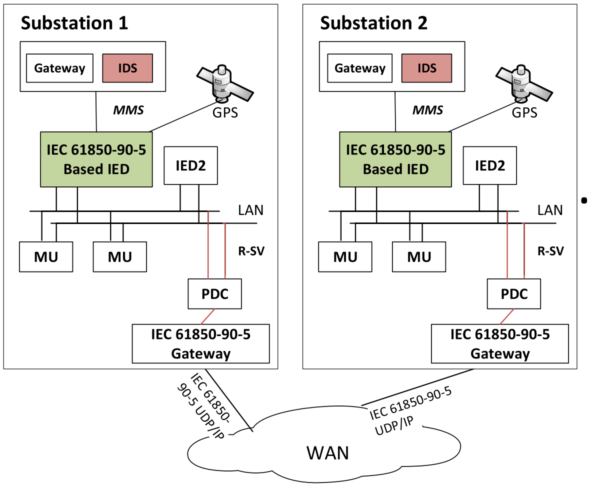


FIGURE 2. Communication mechanism between the substations.

As shown in Fig. 2, the synchronized data will be sent from the IED to the substation Phasor Data Concentrator (PDC). IEC 61850-90-5 will map the measurement data onto the UDP/IP protocol and then forward Routable-SV (R-SV) over WAN. Once the local PDC receives data from other substations, the real-time measurement will be transmitted to the proposed IDS, where the data stream is parsed with local measurements according to the proposed rules.

4) TIME SYNCHRONIZATION

To synchronize local measurements with the measurements from other substations, IED supporting IEC 61850-90-5 generates time stamps of the measurements to provide GPS synchronized time for the IDS. Once a substation PDC receives synchronized measurements from other substations, it will align the data according to the time stamps. Each substation, as a distributed node of the proposed IDS, analyzes the measurements based on time stamps of the packets. Therefore, the communication delay between substations does not impact the accuracy of the IDS.

C. SPECIFICATION OF IDS

Figure 3 describes functions of the proposed IDS. First, the module of packet filtering filters out irrelevant traffic. Only MMS messages responding to the data access request will proceed to the packet parsing module. Synchronized data from other substations are transmitted from the substation PDC to the IDS as an input. At the module of packet parsing, measurement messages with time stamps are generated based on local sample values. Using synchronized measurements from local and other buses, circuit laws in Table 1 are used to identify possible violations. After all rules are checked, the IDS triggers alarms if any violation is detected. For mitigation, the proposed IDS will discard malicious data once a violation is verified. Meanwhile, the IDS will transmit actual measurements with time stamps to the gateway. Hence, the control center is not impacted by measurement attacks that take place in the substations.

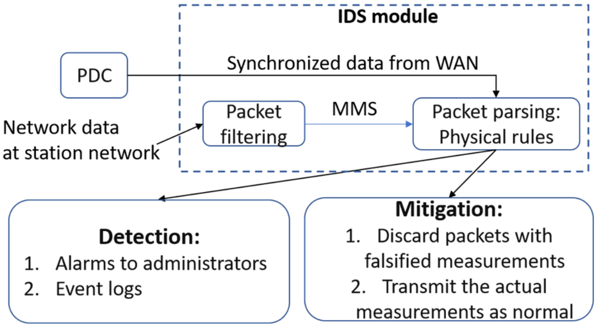

IDS module
PDC
Synchronized data from WAN
Network data at station network
Packet filtering
MMS
Packet parsing: Physical rules
Detection:
1. Alarms to administrators
2. Event logs
Mitigation:
1. Discard packets with falsified measurements
2. Transmit the actual measurements as normal

FIGURE 3. Specification of IDS.

IV. COMPUTATIONAL ALGORITHMS

This section shows that the law of physics used in the IDS can be used to detect false measurements under various attack scenarios. From the system topology, the adjacency matrix $\boldsymbol{A}$ of the graph-theoretic model of a power system is defined [32]. As shown in (1), the column with label *nd* and row with label *br* corresponds to each node and branch, respectively. Loads and generators are treated as branches connected to the ground node. Nonzero entries "1″ and "−1″ in each row represent the polarity of the connection.

$$\boldsymbol{A}=\begin{array}{c} \\ br_1 \\ br_2 \\ \vdots \\ br_m \end{array}\begin{array}{c} \begin{array}{cccc} nd_1 & nd_2 & \ldots & nd_n \end{array} \\ \left[\begin{array}{cccc} 1 & -1 & \ldots & 0 \\ 0 & 1 & -1 & \ldots \\ 0 & 1 & \ldots & -1 \\ -1 & \ldots & 0 & 1 \end{array}\right] \end{array} \tag{1}$$

The branch voltage vector is a linear combination of the corresponding nodal voltages, i.e.,

$$\boldsymbol{V_b}=\boldsymbol{AV_n} \tag{2}$$

where $\boldsymbol{V_b}, \boldsymbol{V_n}$ denotes the vector of branch voltages (voltage drops on branches) and nodal voltages, respectively.

According to KCL, the sum of all currents at each node equals 0, which is formulated by the matrix $\boldsymbol{A^T}$ in (3).

$$\boldsymbol{A^T I_b}=\boldsymbol{0} \tag{3}$$

where $\boldsymbol{I_b}$ is the vector of all branch currents.

A. MEASUREMENT ATTACKS AT A SINGLE SUBSTATION

Let $v'_{nj} = \epsilon v_{nj}$ represent the observed voltage measurement at bus j, where $\epsilon \neq 1$ means that the voltage measurement is falsified. Similarly, $i'_{jk} = \varepsilon_{jk} i_{jk}$, ε_{jk} denotes the attack model of current measurement. $\varepsilon_{jk} \neq 1$ means that the current measurement is falsified. Then $\left(\varepsilon_{jk}-1\right) i_{jk}$ represents the value added to the original measurement.

Scenario 1: multiple branch currents at bus j are falsified:

a) If $\sum\left(\varepsilon_{exit}-1\right) i_{exit} \neq \sum\left(\varepsilon_{enter}-1\right) i_{enter}$:

$$\begin{aligned}\sum i'_{exit} &= \sum i_{exit}+\sum\left(\varepsilon_{exit}-1\right) i_{exit} \\ &\neq \sum i_{enter}+\sum\left(\varepsilon_{enter}-1\right) i_{enter} \\ &= \sum i'_{enter},\end{aligned}$$

then KCL will be violated.

b) If $\sum\left(\varepsilon_{exit}-1\right) i_{exit} = \sum\left(\varepsilon_{enter}-1\right) i_{enter}$:

$$\sum i'_{exit}=\sum \varepsilon_{exit} i_{exit}=\sum \varepsilon_{enter} i_{enter}=\sum i'_{enter},$$

In this case, KCL will fail to detect the malicious current measurements. However, Ohm's law will be violated by i'_{jk}: $i'_{jk} z_{line}=(\varepsilon_{jk} i_{jk}) z_{line} \neq i_{jk} z_{line}=v_{nj}-v_{nk}$.

Scenario 2: voltage measurement at bus j is falsified:

For any branch current i_{jk}, $i_{jk} z_{line} \neq v'_{nj}-v_{nk}$. Thus, Ohm's law of the IDS will be violated at bus j.

Scenario 3: voltage and current measurements are attacked at bus j :

For any line at bus j, if $i'_{jk} z_{line} \neq v'_{nj}-v_{nk}$, the IDS will detect the attack by Ohm's law.

B. MEASUREMENT ATTACKS AT MULTIPLE SUBSTATIONS

Let $\boldsymbol{V'_n}=\boldsymbol{T_{vol} V_n}$ represent the vector of voltage measurements that may contain falsified data. $\boldsymbol{T_{vol}}$ defines the attack model, where $\boldsymbol{T_{vol}} = diag\left(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n\right).\varepsilon_i \neq 1$ means that the ith voltage measurement is falsified. Similarly, $\boldsymbol{I'_b}=\boldsymbol{T_{cur} I_b}$, $\boldsymbol{T_{cur}}=diag\left(\lambda_1, \lambda_2, \ldots, \lambda_m\right)$. $\lambda_i \neq 1$ means that the ith branch current is falsified. The adversary can choose any $\boldsymbol{T_{cur}}, \boldsymbol{T_{vol}}$ to construct the malicious measurements. Thus, there are two attack scenarios:

Scenario1: Suppose voltage and current measurements are attacked at multiple substations, and $\boldsymbol{T_{cur}}, \boldsymbol{T_{vol}}$ are matrices and not scalar.

According to (3), the falsified current measurements are verified as follows:

$$\boldsymbol{A^T I'_b}=\boldsymbol{A^T}\left(\boldsymbol{T_{cur} I_b}\right) \neq \boldsymbol{A^T I_b}=\boldsymbol{0} \tag{4}$$

Both voltage and current measurements are verified by Ohm's law:

$$\boldsymbol{T_{cur}} diag\left(\boldsymbol{Z_{line}}\right) \boldsymbol{I_b}=\boldsymbol{T_{cur} A V_n} \neq \boldsymbol{A T_{vol} V_n} \tag{5}$$

Inequalities (4) and (5) show that this proposed attack will be detected by KCL and Ohm's law.

Scenario 2: Suppose voltage and current measurements are attacked at multiple substations and $T_{vol}=\mu_1, T_{cur}=\mu_2$, where μ_1, μ_2 are scalar.

a) If $\mu_1 \neq \mu_2$,

$$\boldsymbol{A^T}\left(\boldsymbol{T_{cur} I_b}\right)=\mu_1 \boldsymbol{A^T I_b}=\boldsymbol{0} \tag{6}$$

Thus, KCL will fail to detect such attacks that all branch currents in the system are falsified by the factor μ_1. However, inequality (5) is satisfied, thus Ohm's law will detect such attacks.

b) If $T_{vol}=T_{cur}=\mu$, measurements at all buses are multiplied by the same factor μ as follows:

$$\boldsymbol{T_{cur} diag}\left(\boldsymbol{Z_{line}}\right) \boldsymbol{I_b}=\boldsymbol{T_{cur} A V_n}=\mu \boldsymbol{A V_n}=\boldsymbol{A T_{vol} V_n} \tag{7}$$

Equations (6), (7) show that the attack targeting *all* buses in the system by the same factor can avoid being detected by the proposed IDS. However, it is unlikely that all of the large number of buses will be attacked at the same time.

C. KVL DETECTION

Measurement attacks that cannot be detected by Ohm's law and KCL are analyzed based on the KVL detection. Under this specific scenario, the falsified voltage and current measurement v'_j, i'_{kj} satisfy KCL and Ohm's law at bus j:

$$v_k-v'_j=i'_{kj} z_{kj} \tag{8}$$

Normally, KVL is satisfied around each loop, i.e., $i_{12} z_{12}+\ldots+i_{n1} z_{n1}=0$. However, under the attack given by (8), KVL for the related loop is expressed as:

$$\begin{aligned} & v_1-v_2+\ldots+v_k-v'_j+v_j-v_{j+1}+\ldots+v_n-v_1 \\ & \quad = i_{12} z_{12}+\ldots+i'_{kj} z_{kj}+\ldots+i_{n1} z_{n1} \neq 0 \end{aligned} \tag{9}$$

Inequality (9) indicates that KVL is able to uncover such attacks that cannot be detected by KCL and Ohm's Law.

V. TESTBED SETUP

A cyber-physical system testbed is developed to simulate the measurement attacks and implement the proposed IDS at the substation level. Simulations are performed on an embedded computer. The IEEE 39-bus system is implemented in an industry level power system simulator. As the physical system layer in the co-simulation environment, the simulated voltage and current measurements are exported to a simulated substation automation system in real-time. A commercial grade IEC 61850 source code is embedded to implement the MMS communication. To detect measurement attacks, the proposed IDS will parse the data flow of local measurements and synchronized data from other substations. Fig. 4 illustrates the data flow of the proposed testbed.

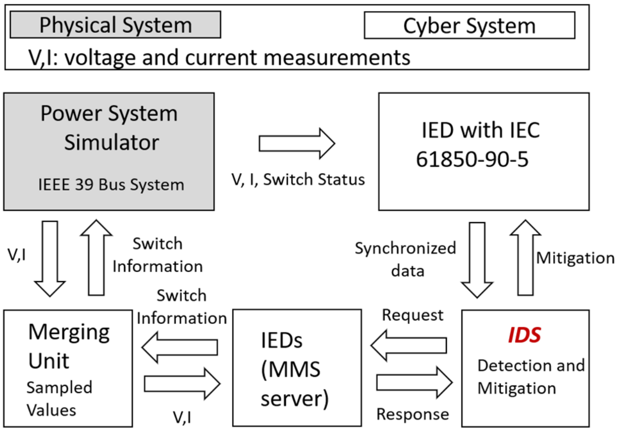


FIGURE 4. Data flow of cyber-physical system testbed.

Communication between the substations is needed to identify falsified measurements using KVL and Ohm's Law. Industrial communication protocols (e.g., IEC 61850 and IEC 61850-90-5) are used to establish the communication network among substations. Each of the 39 substations is assigned a unique address in LAN. Data packets with measurements are sent to the destination IP address of the corresponding substations. Since data streaming among substations is transmitted in a distributed manner [31], data exchange between substations is executed in parallel using multiprocessing on the proposed simulation environment.

For KCL validation, IDS in substation LAN will parse local current measurements. Moreover, using the proposed ICT network, every substation checks Ohm's Law with local voltage measurements as well as those transmitted from other substations. For KVL validation, the loops in the IEEE 39 bus system are detected by the circuit analysis tool in Python. As shown in Fig. 5, there are 21 independent loops in the graph. The dashed lines in the figure represent the loops including ground node, generator nodes, and load nodes. For instance, the yellow dashed line between node 15 and node 16 indicates that the loads which are connected to ground form a loop in the circuit with the transmission line between bus 15 and bus 16. The blue dashed line between node 31 and node 32 shows that the two generators which are connected to ground form a circuit loop with the transmission line between node 31 and node 32.

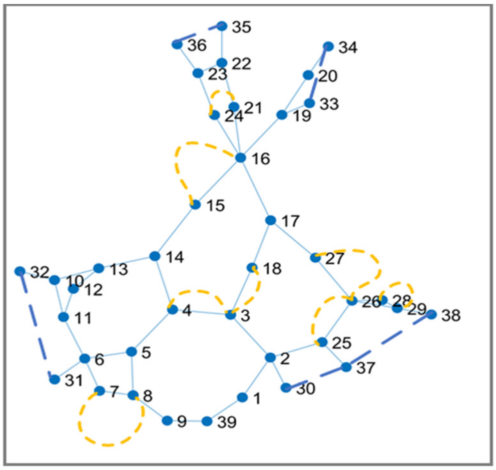


FIGURE 5. Independent circuit loops for IEEE 39 bus system.

For the IDS measurement checking, a responsible node (bus) is predefined for each loop. For instance, node 11, node 12 and node 13 in loop 1 send packets to the responsible node, node 10, such that the current measurements from each node in loop 1 are extracted from the payload of the packets for KVL validation.

VI. EXPERIMENTATION & EVALUATION

A. INTRUSION DETECTION RESULTS

Measurement attacks targeting single or multiple substations are simulated. A stealth false data injection attack is simulated for comparison between the proposed substation level IDS and a control center EMS based IDS. Representative attack scenarios are developed for simulation and validation of the proposed IDS.

Based on the concept of "undetectable" malicious measurements, e.g., [3]–[7], a general attack model can be constructed by $z_{bad} = z + a$, where z denotes the original measurements and a is the attack vector. To bypass the bad data detection in state estimation, if the attacker uses an attack vector $a = Hc$, where H is the measurement matrix used in state estimation, and c is an arbitrary nonzero vector, the threshold of bad data detection will not be violated. However, the proposed stealth attack will undermine the results of state estimation.

In this attack scenario, the original measurements are generated by combining the power flow results with measurement errors. The measurements of voltage magnitudes at bus 11 and bus 13 are falsified with a constructed vector c. The injected error shown in Fig. 6 represents the difference between the voltage magnitudes of power flow results and manipulated results of state estimation. It is noted that the differences at bus 11 and bus 13 are significant.

Table 2 shows the detection results of the stealth attack. By the IDS, the malicious voltage measurements violate Ohm's law at bus 11 and 13, which triggers the alerts at 0.078 and 0.095 seconds at each substation. However,

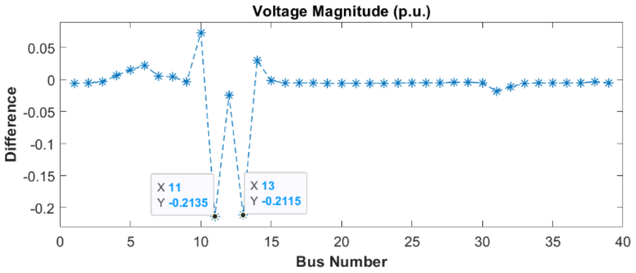


FIGURE 6. Difference between the original and estimated measurements after a stealth attack.

the norm of measurement residuals, $\|z_{bad} - X_{est}\|$, is less than the threshold, referred to the Chi-squares table. Thus, without the proposed substation IDS, this attack can successfully inject malicious errors and bypass bad data detection. Much research has been concerned with the detection of stealth attacks targeting state estimation. Usually it is assumed that attackers have full/partial knowledge of the current system configuration. However, the proposed substation IDS is able to detect and mitigate the falsified measurements before they are sent out of the substation, whether the attacks are independent or coordinated.

TABLE 2. IDS rules for stealth attack.

Stealth attack	Attack targets	IDS alerts	Bad data detection results
$\boldsymbol{z_{bad}} = \boldsymbol{z} + \boldsymbol{Hc}$	Bus 11, Bus 13	t = 0.078s, 0.095s: Ohm`s Law alert triggered at buses 11,13	$\|z_{bad} - X_{est}\| < \tau$

Table 3 shows the detection results for different attack scenarios. For scenarios 1, the attacker falsified the voltage measurements by increasing the magnitude of measurements to 1.3 times. As current measurements are not fabricated, KCL and KVL are not violated according to the detection algorithms. From the detection results in Table 3, Ohm‘s Law at bus 10 successfully detects the attack, IDS warning is triggered as a response.

For scenario 2, current measurements on the line between bus 10 and bus 13 are falsified at bus 10, causing a violation of KCL and Ohm‘s Law at bus 10. The IDS warning at bus 10 is triggered. Since the falsified current violates KVL of Loop 1 (including buses 10,11, 12, 13), KVL alert is also triggered.

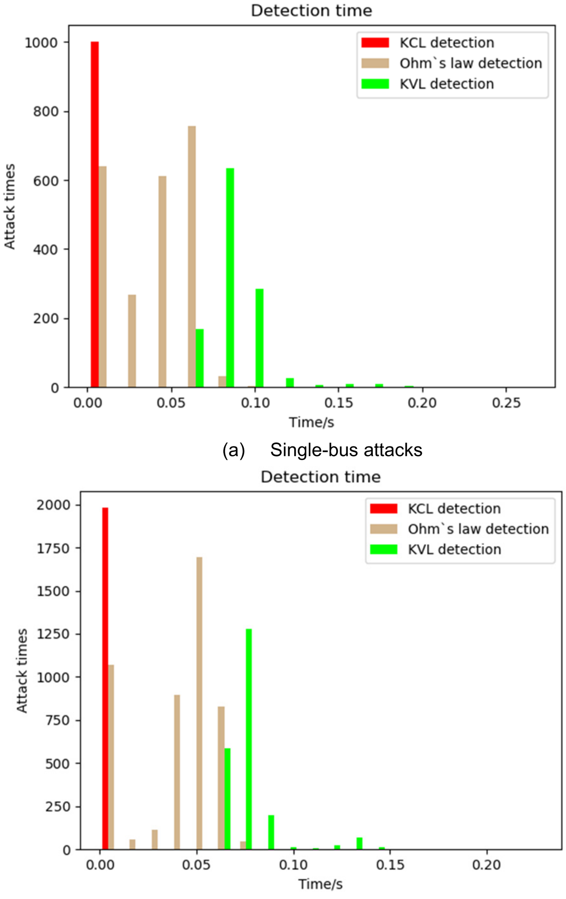
For scenario 3, all current measurements at bus 11 and bus 13 are falsified by increasing the line current to 3 times of the measurements. KCL fails to detect this attack. However, Ohm‘s Law successfully detects this measurement attack at buses 11 and 13. KVL alerts are triggered by Loop 1 and Loop 2. Thus, IDS warning at both buses is triggered.

Similarly, if both voltage and current measurements are falsified at scenarios 4 and 5, the proposed IDS is able to detect the measurement-based attack by checking IDS rules. As shown in Table 3, Detection Time (DT) is estimated by the time difference between the time stamp in the messages and the time when the scanned packet is detected by any rule. The detection of KVL usually takes more time to complete. Ohm‘s Law detection is relatively fast since the time delay is based solely on the transmission delay of other buses. For KCL, the detection is the fastest as there is no need for communication with other substations. Once an alert is triggered by a violation, the IDS warning is triggered. Therefore, DT of a particular measurement attack is determined by the fastest alert.

B. PERFORMANCE OF THE IDS

1) DETECTION TIME (DT)

Using Monte Carlo simulation, the measurement attacks targeting a random bus in IEEE 39 bus system are executed 1000 times on the proposed testbed. DT as a performance metric is measured for each attack.



(a) Single-bus attacks

(b) Two-bus attacks

FIGURE 7. Distribution of detection time of each rule in IDS.

Fig. 7 illustrates the distribution of DT under single-bus and two-bus attacks, respectively. From the distribution of the results, KVL detection requires more time to check the detection rule. As the responsible bus in the loop validates KVL by collecting the measurement packets from other buses in the loop, the latency is caused by the highest transmission delay over all buses in the loop. Specifically, the maximum DT observed from KVL detection reached 0.15 second, as this loop is the largest loop in the system with 8 substations.

TABLE 3. IDS performance for measurement attack scenarios.

Attack Scenario	Attack Target	IDS Alert with Detection Time (DT)
1. Increase voltage magnitude to 1.3 times of the measurement	Bus 10	t = 0.072s: Ohm`s Law alert triggered at bus 10
2. Increase line current between bus 10 and bus 13 to 3 times of the measurement	Bus 10	t = 0.003s: KCL alert triggered at bus 10 t = 0.065s: Ohm`s Law alert triggered at bus 10 t = 0.093s: KVL alert triggered at bus 10 (Loop 1)
3. Increase all the current magnitude to 3 times of the measurement	Bus 11 and 13	t = 0.055s: Ohm`s Law alert triggered at bus 11 t = 0.065s: Ohm`s Law alert triggered at bus 13 t = 0.092s: KVL alert triggered at bus 10 (Loop 1) t = 0.103s: KVL alert triggered at bus 13 (Loop 2)
4. Increase voltage to 1.3 times, current to 3 times of the measurement	Bus 10	t = 0.063s: Ohm`s Law alert triggered at bus 10 t = 0.085s: KVL alert triggered at bus 10 (Loop 1)
5. Increase voltage to 1.3 times, current to 3 times of measurement	Bus 11 and 13	t = 0.059s: Ohm`s Law alert triggered at bus 11 t = 0.062s: Ohm`s Law alert triggered at bus 13 t = 0.086s: KVL alert triggered at bus 10 (Loop 1) t = 0.097s: KVL alert triggered at bus 13 (Loop 2)

The communication between buses is efficient. Indeed, checking of the Ohm‘s Law is completed within 0.1 second. As validation of KCL is processed at the local substation without any confirmation information from outer network, DT for KCL is around 0.01 second. In Fig. 7, the maximum DT is lower than 0.2 second, which is smaller than the cyclical time of DNP3 polling. Hence, the proposed IDS is able to identify falsified measurements before the measurement messages are sent out by DNP3 outstation.

A histogram comparing the results is shown in Fig. 7(a) and (b). It is noted that the DT distribution of single-bus attacks is close to that of two-bus attacks as expected. The reason is that the proposed IDS checks the consistency of measurements in a distributed manner at the substation level.

The general DT distribution for various attack scenarios in 39-bus system is given in Fig. 8. In order to evaluate the performance of the proposed IDS under multiple cyberattacks, substations are randomly selected by the measurement attack. The Y axis in Fig. 8 represents the number of substations that are attacked simultaneously. For each attack scenario, the detection time of the attack is the time when the first alert is triggered by the IDS. In Fig. 8, the band represented by the box gives the maximum, minimum, and median of the detection time over 100 experiments, respectively. The outliers are defined as red points located outside the box. By comparing the respective median of each box, all medians are close to each other, and fall under 0.025s. The results show that, for a broad range of attacks, the distributed IDS responds within a short time.

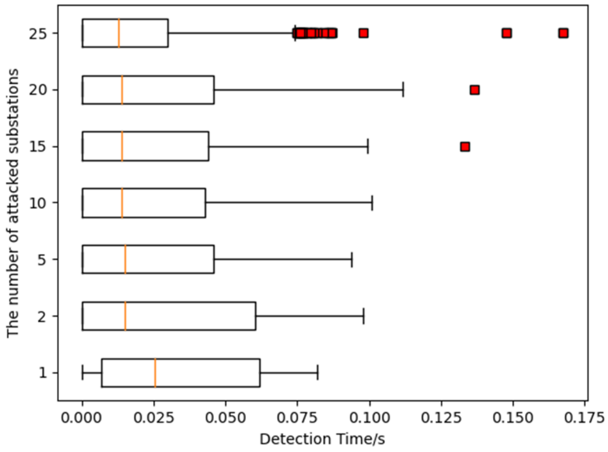


FIGURE 8. Distribution of detection time for attacks targeting multiple substations.

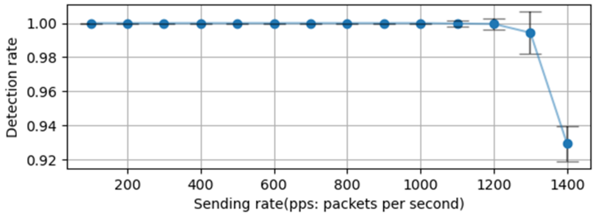


FIGURE 9. Detection rate with different traffic rates.

2) DETECTION RATE (DR)

The accuracy of the proposed IDS is measured by DR, which is the ratio of TP (number of attacked instances IDS correctly detects) and $FN+TP$ (overall number of the attack instances).

$$DR = \frac{TP}{FN + TP} \tag{10}$$

Measurement packets mixed with the falsified measurements are sent in different rates. For a given rate, the experiments are repeated 100 times. The error bar is calculated based on the standard deviation of the results. Fig. 9 shows the impact of traffic rate for DR. The results show that the IDS is able to detect the falsified data in the mixed data stream. In other words, if the attacker floods the system with duplicate packets at a rate of 1000 packets per second, the alarms are triggered once the first fabricated measurement is captured. Therefore, the mitigation strategy is able to prevent the substation from further flooding. However, it is observed that DR declines from 100% to 93%, when the sending rate exceeds 1000 packets per second. The error bar indicates the low performance of the IDS when the data traffic is too fast. Along with the increase of traffic speed, the delay time between any two packets becomes too small. The IDS is not fast enough to identify each packet within the mixed data stream at such a high speed, causing the falsified measurements in the missing packets to be misclassified.

VII. CONCLUSION

In this paper, the potential attack path of measurement attacks at the substation level is established. The performance of the proposed IDS has been validated by simulation with realistic measurement attacks. The proposed method achieves a high level of detection accuracy under high speed traffic of measurement messages. By the proposed IDS, measurement attacks are detected within the substations, thereby avoiding the impact of falsified measurements on system operation in the control center. For the future work, collaborative IDSs with communication among the substations should be studied so that the distributed IDSs will be able to work as a team to detect various attack types targeting the digital substations.

ACKNOWLEDGMENT

The authors would like to thank Mr. Randy Steele, American Electric Power, for his helpful discussions.

REFERENCES

[1] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 58–66, Jan. 2012, doi: 10.1109/MPE.2011.943114.

[2] D. I. J. Slowik. *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack*. Accessed: 2019. [Online]. Available: https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

[3] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017, doi: 10.1109/TII.2016.2614396.

[4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011, doi: 10.1145/1952982.1952995.

[5] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011, doi: 10.1109/TSG.2011.2163807.

[6] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012, doi: 10.1109/TSG.2012.2195338.

[7] B. Chen, H. Li, and B. Zhou, "Real-time identification of false data injection attacks: A novel dynamic-static parallel state estimation based mechanism," *IEEE Access*, vol. 7, pp. 95812–95824, 2019, doi: 10.1109/ACCESS.2019.2929785.

[8] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011, doi: 10.1109/TSG.2011.2119336.

[9] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1244–1253, Sep. 2013, doi: 10.1109/TSG.2013.2245155.

[10] J. Zhao, G. Zhang, and R. A. Jabr, "Robust detection of cyber attacks on state estimators using phasor measurements," *IEEE Trans. Power Syst.*, vol. 32, no. 3, pp. 2468–2470, May 2017, doi: 10.1109/TPWRS.2016.2603447.

[11] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017, doi: 10.1109/TSG.2017.2703842.

[12] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids," *IEEE Access*, vol. 5, pp. 26022–26033, 2017, doi: 10.1109/ACCESS.2017.2769099.

[13] Z. Wang, Y. Chen, F. Liu, Y. Xia, and X. Zhang, "Power system security under false data injection attacks with exploitation and exploration based on reinforcement learning," *IEEE Access*, vol. 6, pp. 48785–48796, 2018, doi: 10.1109/ACCESS.2018.2856520.

[14] *Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 6: Security for IEC 61850, 1.0*, Standard IEC 62351-6, IEC, 2007.

[15] *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*, IEEE Standard 1815-2012, Oct. 2012.

[16] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008, doi: 10.1109/tpwrs.2008.2002298.

[17] N. Liu, J. Zhang, and X. Wu, "Asset analysis of risk assessment for IEC 61850-based power control systems—Part I: Methodology," *IEEE Trans. Power Del.*, vol. 26, no. 2, pp. 869–875, Apr. 2011, doi: 10.1109/TPWRD.2010.2090950.

[18] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan, "An intrusion detection system for IEC61850 automated substations," *IEEE Trans. Power Del.*, vol. 25, no. 4, pp. 2376–2383, Oct. 2010, doi: 10.1109/TPWRD.2010.2050076.

[19] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, and S. Sezer, "Multidimensional intrusion detection system for IEC 61850-based SCADA networks," *IEEE Trans. Power Del.*, vol. 32, no. 2, pp. 1068–1078, Apr. 2017, doi: 10.1109/TPWRD.2016.2603339.

[20] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta, "A multidimensional critical state analysis for detecting intrusions in SCADA systems," *IEEE Trans. Ind. Informat.*, vol. 7, no. 2, pp. 179–186, May 2011, doi: 10.1109/TII.2010.2099234.

[21] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011, doi: 10.1109/TSG.2011.2159406.

[22] J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1643–1653, Jul. 2014, doi: 10.1109/tsg.2013.2294473.

[23] J. Hong and C.-C. Liu, "Intelligent electronic devices with collaborative intrusion detection systems," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 271–281, Jan. 2019, doi: 10.1109/tsg.2017.2737826.

[24] M. Touhiduzzaman, A. Hahn, and A. K. Srivastava, "A diversity-based substation cyber defense strategy utilizing coloring games," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5405–5415, Sep. 2019, doi: 10.1109/TSG.2018.2881672.

[25] R. Macwan, C. Drew, P. Panumpabi, A. Valdes, N. Vaidya, P. Sauer, and D. Ischchenko, "Collaborative defense against data injection attack in IEC61850 based smart substations," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5, doi: 10.1109/PESGM.2016.7741376.

[26] S. Sheng, W. L. Chan, K. K. Li, D. Xianzhong, and Z. Xiangjun, "Context information-based cyber security defense of protection system," *IEEE Trans. Power Del.*, vol. 22, no. 3, pp. 1477–1481, Jul. 2007, doi: 10.1109/TPWRD.2006.886775.

[27] S. Kwon, H. Yoo, and T. Shon, "IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system," *IEEE Access*, vol. 8, pp. 77572–77586, 2020, doi: 10.1109/ACCESS.2020.2989770.

[28] *IEEE Standard for Exchanging Information Between Networks Implementing IEC 61850 and IEEE Std 1815(TM) [Distributed Network Protocol (DNP3)]*, IEEE Standard 1815.1-2015, Dec. 2015.

[29] R. Minkner and E. O. Schweitzer, "Low power voltage and current transducers for protecting and measuring medium and high voltage systems," in *Proc. Western Protective Relay Conf.*, Spokane, WA, USA, 1999.

[30] L. Sevov, Z. Zhang, I. Voloh, and J. Cardenas, "Differential protection for power transformers with non-standard phase shifts," in *Proc. 64th Annu. Conf. Protective Relay Eng.*, Apr. 2011, pp. 301–309, doi: 10.1109/CPRE.2011.6035631.

[31] *Communication Networks and Systems for Power Utility Automation—Part 90-5: Use of IEC 61850 to Transmit Synchrophasor Information According to IEEE C37.118*, Standard IEC TR 61850-90-5:2012, 2012.

[32] F. H. Branin, "Computer methods of network analysis," *Proc. IEEE*, vol. 55, no. 11, pp. 1787–1801, Nov. 1967, doi: 10.1109/PROC.1967.6010.

RUOXI ZHU (Graduate Student Member, IEEE) received the M.S. degree in electrical engineering from Virginia Tech, in 2020, where she is currently pursuing the Ph.D. degree. Her research interests include cyber-physical security of power systems, and voltage stability monitoring and control.

CHEN-CHING LIU (Life Fellow, IEEE) is currently an American Electric Power Professor and the Director of the Power and Energy Center, Virginia Tech. He is also an Adjunct Full Professor with University College Dublin, Ireland. He is a member of the U.S. National Academy of Engineering.

JUNHO HONG (Member, IEEE) is currently an Assistant Professor of electrical and computer engineering with the University of Michigan–Dearborn. He has been working on cybersecurity of energy delivery systems with the Department of Energy sponsored projects in the areas of substation, microgrid, HVDC, FACTS, and high-power EV charger.

JIANKANG WANG (Member, IEEE) is currently an Assistant Professor of electrical and computer engineering with The Ohio State University, where she is also an Adjunct Professor with the Department of Integrated System Engineering. She was appointed as a Lead Technical Specialist with California ISO, in 2018. Her research interests include electricity markets, renewable energy, PEV integration, and power system cyber-security.