Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 9594267, 16 pages
https://doi.org/10.1155/2022/9594267

Research Article

Detection Scheme for Tampering Behavior on Distributed Controller of Electric-Thermal Integrated Energy System Based on Relation Network

Chaoqun Zhu, Jie Li, Jie Shen, Lei Zhou, Xiaoming Zhang, Dan Zhu, and Yafei Li

Marketing Department of State Grid Suzhou Power Supply Company, Suzhou 215000, China

Correspondence should be addressed to Chaoqun Zhu; 2016124296@jou.edu.cn

Received 13 June 2022; Revised 26 July 2022; Accepted 2 August 2022; Published 27 August 2022

Academic Editor: Shahid Mumtaz

In recent years, with the development of smart grid, the power systems and other energy systems are gradually forming integrated energy systems. The electric-thermal integrated energy system is a mature integrated energy system at present. The electric-thermal integrated energy system uses modern communication technology to realize the comprehensive regulation of electric energy and thermal energy, which greatly improves the efficiency of energy use. However, this also greatly increases the risk of malicious tampering with the energy dispatch system. In this paper, we study the regulation of electric-thermal integrated energy systems considering false data injection attacks. First, we establish a compromised model of an electric-thermal integrated energy system considering false data injection attacks. Then, we designed vulnerable variable observers for different tampering scenarios to observe the tampered variables. Finally, considering the relationship between the observed data and the measured data, we design a tampering behavior detection method based on relation network. The simulation results verify the effectiveness of the detection method proposed in this paper.

1. Introduction

The electric-thermal integrated energy system (ETIES) is an important part of the integrated energy system. With the aid of the advanced network information technology and innovative operation and management models, ETIES integrates electrical and thermal energy in the region, realizes operation optimization and coordinated control among various heterogeneous energy sub-networks through energy coupling equipment, and effectively improves energy conversion efficiency and promotes sustainable energy while meeting the diverse energy needs of users [1–3]. However, ETIES based on distributed optimization architecture is a highly integrated information-physical energy system. The information system of ETIES is bound to endure a huge threat of cyber attacks while exchanging a large amount of information data [4, 5].

The spread of malicious attacks in the communication network will destroy the environment of network communication, make the economic operation of the system impossible, even destroy the stability of the system [6, 7]. In [8], the authors propose that the measurement equipment in the cyber physical system suffer from multiple types of cyber-attacks, and summarizes the current mainstream attack defense schemes based on learning-based methods. In [9], the authors propose that the energy-water nexus with multiple sensors may be vulnerable to cyber-attacks. To deal with the potential threats, an observer-based attack detection method is proposed. As a typical information-physical system, the monitoring and control of power system highly depends on the accuracy of measured data [10]. When the measurement data is compromised, the operation stability and security of the power system will be greatly reduced, thus threatening social security and social economy. To enhance the resilience of the sensors in power systems, the attack defense scheme based on the features of the measured data is proposed. This type of attack detection scheme enables cyber physical system to maintain good detection performance under cyber-attacks.

False data injection attack (FDI attack) is a new form of attack that has appeared in recent years to undermine the credibility of the operational data of integrated energy systems [11, 12]. When the attacker has the ability to inject data streams into the data transmission channel of the integrated energy system, attack vectors can be constructed targeting the vulnerabilities of the traditional bad data detection methods and identification methods of the integrated energy system, and arbitrarily manipulate the data of the attacked data channel of the integrated energy system. The flow changes the real data of the system into false data, which affects the real-time operation status of the power system, thus threatening the stable, safe and economic operation of the power system. Therefore, it is necessary to improve the attack defense capability of monitoring node sensors to resist the damage to the system caused by cyber-attacks [13, 14].

At present, there are two main perspectives in the research on considering the existence of FDI attacks in the system. On the one hand, from the perspective of FDI attackers, researchers design an optimal attack strategy that can improve the probability of successful attack and attack effect. Reference [15] studies the attack vector construction method from the attacker's point of view. Combining the l_0 norm and l_1 norm of the attack vector, an attack evaluation index to measure the attack effect and attack cost is proposed. References [16–18] considered the scenarios where the measurement data in the actual system has different security protection levels, and proposed a corresponding minimum attack vector construction method. In order to reduce the attack cost and improve the attack efficiency, the literature [19, 20] designed an attack vector construction method based on the minimum cut set with the goal of making the energy system lose its ability to observe the external environment. At the same time, other attack scenarios can also be considered when constructing false data injection attack vectors. The attacker in [21] used traditional attack methods such as worms to break through the firewall and obtained the control authority of the basic equipment, and then launched a false data injection attack to tamper with the state variables of the energy system, thereby causing cascading failures of associated equipment. Reference [22] proposed a form of attack based on false data injection attacks to attack the topology of power systems—Man-in-the-middle attacks (MITM attacks). In this form of attack, the attacker eavesdrops on the data transmission terminals of the power system, and spoofs the status of the power system equipment by injecting false data. At this time, the communication mode between data transmission terminals changes from direct communication in normal state to relay communication through third-party devices, and the reliability of the association state between devices will be destroyed. Reference [23] demonstrates the attack effect of a multi-level MITM attack with the help of a simulation platform. The simulation results show that this type of attack can mislead the control center to make a wrong assessment of the current energy system topology by controlling the switch state between the devices, and trigger misoperations to cause power system physical layer accidents. Reference [24] added a data frame attack to the man-in-the-middle attack based on the normalized residual search method. Different from traditional false data injection attacks, which aim to maintain the concealment of false data, the main purpose of this type of attack is to deliberately launch bad data detection (BDD) to make real data be regarded as false data, thereby disturbing state estimation of energy system.

On the other hand, researchers propose defense strategies against network attacks from the perspective of system defense. References [25, 26] use Petri nets to describe the information flow between data interaction terminals in a power cyber-physical system and propose a cooperative intrusion detection algorithm against false data injection attacks. The analysis model based on Petri net can clearly describe the transient and steady-state reliability of power system under multiple attack events. The detection of false data injection attacks based on machine learning algorithms is also a research direction that domestic and foreign researchers focus on. Reference [27] considered the behavior characteristics of false data injection attacks against load frequency control systems, and designed an intelligent attack detection algorithm based on multi-layer perceptrons to effectively identify false data injection attacks. Reference [28] considered the behavior characteristics of false data injection attack on power system transmission lines, using programmable logic controller as a detection method. The computing node of the algorithm is tested, and the classifier of machine learning is used to realize the identification of false data injection attacks. This distributed attack detection algorithm can effectively reduce decision-making delay and improve attack detection efficiency. Reference [29] proposed an unsupervised attack detection scheme based on the isolation forest algorithm, and used the principal component analysis method to extract the features of the power system variables, thereby reducing the dimensionality problem in the machine learning process. Reference [30] considered the problem of a small number of abnormal samples in the process of machine learning training, and proposed an intelligent attack detection algorithm using the support vector description domain to detect false data injection attacks in the load frequency control system. Reference [31] considered the false data injection attack form for load forecasting, proposed a machine learning-based load forecasting anomaly detection method, and estimated the false data injection attack type through naive Bayesian classification.

Similar to the original social power supply, heating and other systems, in the operation process of ETIES, one of the most concerned issues is how to realize the economic scheduling of the system, that is, how to comprehensively allocate the capacity distribution between multiple energy units on the premise of meeting the system security constraints, so as to minimize the economic cost of the system, and then realize the dual guarantee of system operation in terms of security and economy. The economic scheduling method of ETIES can be divided into centralized method and distributed method. Although the centralized method has high efficiency in information processing, it has some

problems, such as high communication cost and sensitivity to single point of failure. The distributed method can use the sparse communication network structure to realize the decentralized cooperation of various equipment components of the system, which has less communication burden, stronger robustness and privacy. Therefore, in recent years, experts and scholars at home and abroad have proposed many ETIES economic scheduling methods based on distributed optimization.

However, it is worth noting that although the above method can effectively solve the distributed economic scheduling problem of ETIES, its premise is that the system operates in an ideal network communication environment, that is, a large number of interactive measurement and control data can be reliably transmitted on the communication line. However, ETIES based on distributed optimization architecture is an energy system with high integration of information and physics. While the information system of ETIES interacts with a large amount of information and data, it is bound to suffer from a huge threat of network attack. The spread of malicious attacks in the communication network will destroy the bad environment of network communication, make the economic operation of the system impossible, and even destroy the stability of the system, resulting in the paralysis of the energy supply system.

ETIES is a large system with electrical-thermal coupling characteristics, and its structure and operation are much more complex than traditional power systems. Therefore, malicious attackers need to adopt more complex and targeted strategies according to system conditions when attacking ETIES. So far, most of the research on the impact of network attacks on system performance is carried out on a single power system, and there is no research on the impact of network attacks on the operational security of ETIES. The distributed scheduling of ETIES depends on the security and reliability of the communication network, and network attacks will inevitably affect the scheduling process of ETIES, thereby affecting the performance of the system.

Aiming at this research gap, the motivation of the paper is to enhance the safety and security of the electric-thermal integrated energy system by studying the ETIES model under FDI attacks and designing an attack detection method based on machine learning algorithm.

The main contributions of the paper are three fold:

(1) We establish attack templates in the electric-thermal integrated energy system and discuss the impact of false data injection attacks on the integrated energy system.

(2) In the electric-thermal integrated energy system under FDI attack, we propose an observer-based method for observing vulnerable variables of the system, so that the compromised variables can be effectively observed.

(3) Using the observation data obtained by the observer, we propose a relation network-based attack detection algorithm to detect FDI attacks in integrated energy systems.

The scope of the paper is shown as follows: first, the compromised model of the electric-thermal integrated energy system is discussed in this paper; Then, based on the variables in the system, a machine-learning-based attack detection method is studied to identify the FDI attacks on ETIES.

The remaining part of this paper is organized as follows: in Section 2, the model of the compromised electric-thermal integrated energy system under FDI attacks is established. In Section 3, the observer of the vulnerable variables is designed. In Section 4, the attack detection method based on relation network is designed. In Section 5, simulations are designed and the results are discussed. In Section 6, conclusions are stated.

1.1. Indices and Variables. x_p^P: Incremental cost of power only device.

x_p^C: incremental cost of combined heat and power device.

x_h^C: thermal incremental cost of combined heat and power device.

x_h^H: thermal incremental cost of heat only device.

u_p^P: electric power mismatch of power only device.

u_p^C: electric power mismatch of combined heat and power device.

u_h^C: thermal power mismatch of combined heat and power device.

u_h^H: thermal power mismatch of heat only device.

$m(k)$: attack vector.

y_p^P: electric output power of power only device.

y_p^C: electric output power of combined heat and power device.

y_h^C: thermal output power of combined heat and power device.

y_h^H: thermal output power of heat only device.

x: state vector of the system.

$\overline{x}$: augmented state vector of the system.

$\widehat{\overline{x}}$: observation of augmented state vector.

e: estimation error.

d_m: data vector in the measured data set.

d_o: data vector in the observed data set.

$\mathcal{F}(d_m)$: feature vectors of measured data.

$\mathcal{F}(d_o)$: feature vectors of observed data.

$\mathcal{P}_i^m$: prototype of the measured data feature vector in class i.

$\mathcal{P}_i^o$: prototype of the observed data feature vector in class i.

N_i^m: number of samples in class i of measured data feature vectors.

N_i^o: number of samples in class i of observed data feature vectors.

$\mathcal{C}$: concatenation module in relation network.

$\mathcal{R}$: relation module in relation network.

$\mathcal{S}$: similarity score in relation network.

L_m: objective function in relation network.

l_m: labels for measured data.

l_o: labels for observed data.

MA: evaluation index of accuracy.

MD: evaluation index of the probability of detecting correctly.

MS: evaluation index of success ratio.

MI: evaluation index of probability of identifying normal cases.

MF: trade off between *MD* and *MS*.

1.2. Abbreviations. ETIES: electric-thermal integrated energy system.

FDI: false data injection.

MITM: man-in-the-middle.

BDD: bad data detection.

DDCA: distributed energy double-consensus algorithm.

POD: power only device.

CHP: COMBINED heat and power.

RELU: rectified linear unit.

2. FDI Attacks against Compromised Electric-Thermal Integrated Energy System and Countermeasures

In this section, we propose the FDI attacks against electric-thermal integrated energy system and study the countermeasures by designing the attack detection scheme. First, we introduce the basics of the energy management control strategy of electric-thermal integrated energy system, and propose the compromised model as the first step to mitigate FDI attacks. Second, based on the compromised model, we design observers to detect the variables compromised by FDI attacks. Finally, based on the observed data obtained by the proposed observers and the measured data obtained by measurement in ETIES, we propose an attack detection method to identify the safety status of ETIES.

2.1. Basics of Compromised Electric-Thermal Integrated Energy System. The typical distributed energy management method of electric-thermal integrated energy system is to use distributed energy double-consensus algorithm (DDCA). DDCA employs two different consensus protocols. One of the consensus protocols is used to calculate the incremental cost corresponding to the optimal solution of the ETIES economic dispatch problem. Another consensus protocol aims to estimate the amount of electrical/thermal local power mismatch for coordinating device output. The two protocols of DDCA use different but strongly coupled consistency variables to calculate the electric/thermal incremental cost, electric/thermal output power and electric/thermal local power mismatch corresponding to the optimal solution of ETIES economic dispatching problem, so as to finally realize the distributed economic dispatching of ETIES. ETIES scheduling depends on the information exchange and local calculation between each unit and its neighbors. Each energy unit contains a distributed controller for operation.

The attacker can attack the incremental cost estimator and the output power decision of the energy unit in DDCA, thereby affecting the output power of the unit in the energy unit. Inspired by reference [32], the compromised incremental cost estimator and output power decision-maker studied in this paper can be written as

$$\begin{cases} x(k+1) = Ax(k) + Bu(k), \text{normal}, \\ x(k+1) = Ax(k) + Bu(k) + Mm(k), \text{compromised}, \end{cases} \tag{1}$$

where

$$\begin{aligned} x &= \left[x_p^P \;\; x_p^C \;\; x_h^C \;\; x_h^H \right]^T, \\ u &= \left[u_p^P \;\; u_p^C \;\; u_h^C \;\; u_h^H \right]^T, \end{aligned} \tag{2}$$

where A is the consistency algorithm update matrix in DDCA, which is determined by the adjacency relationship between the current energy unit and the surrounding energy unit; B is the algorithm convergence rate adjustment matrix in DDCA; M is the corresponding attack weight matrix.

The compromised output power decision-maker studied in this paper can be written as

$$\begin{cases} y(k) = Cx(k), \text{normal}, \\ y(k) = Cx(k) + Nm(k), \text{compromised}, \end{cases} \tag{3}$$

where

$$y = \left[y_p^P \;\; y_p^C \;\; y_h^C \;\; y_h^H \right]^T, \tag{4}$$

where C is the cost coefficient matrix; N is the corresponding attack weight matrix.

It can be learned that FDI attacks can change the power output of the energy unit by tampering with the state variables of different modules in the ETIES, which has an impact on the power balance of the integrated energy system. In the next section, observers for different attack intrusion locations are designed to observe the FDI attacks.

3. Design of Observers for Detecting Compromised Variables in ETIES

3.1. Observer Design of Incremental Cost Estimator under FDI Attacks. In this part, we focus on the observer for compromised incremental cost estimator. The compromised system $\sum_{ice}$ can be expressed as

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) + Mm(k), \\ y(k) = Cx(k). \end{cases} \tag{5}$$

Taking the attack vector $m(k-1)$ at $k-1$ time as an additional state, we can obtain the augmented state vector $\overline{x}(k) = [x(k)m(k-1)]^T$. The following augmented system can be established

$$\begin{cases} \overline{E}\overline{x}(k+1) = \overline{A}\overline{x}(k) + \overline{B}u(k), \\ y(k) = \overline{C}\overline{x}(k), \end{cases} \tag{6}$$

where

$$\begin{aligned}\overline{E} &= \begin{bmatrix} I_n & -M \\ 0 & 0 \end{bmatrix},\\ \overline{A} &= \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix},\\ \overline{B} &= \begin{bmatrix} B \\ 0 \end{bmatrix},\\ \overline{C} &= \begin{bmatrix} C \\ 0 \end{bmatrix}^T.\end{aligned} \tag{7}$$

The following observer of the augmented system is designed

$$\begin{cases} z(k+1) = R\overline{A}\hat{\overline{x}}(k) + R\overline{B}u(k) + L(y(k) - \overline{C}\hat{\overline{x}}(k)), \\ \hat{\overline{x}}(k) = z(k) + Ty(k), \end{cases} \tag{8}$$

where z represents the state vector of the dynamic system (4); R, L and T are the gain matrices with appropriate dimensions.

Theorem 1. *When the compromised system has a state observer in the form equation (5), it needs to meet the following requirements: (1) $R\overline{E} + T\overline{C} = I_{n+q}$; (2) There are symmetric positive definite matrices P and W satisfying*

$$\begin{bmatrix} -P & (R\overline{A})^T P - \overline{C}^T W^T \\ * & -P \end{bmatrix} < 0. \tag{9}$$

Proof. Proof. Consider nonsingular matrices $U \in \mathbb{R}^{(n+q)\times(n+q)}$ and $V \in \mathbb{R}^{(n+q)\times(n+q)}$ such that

$$U\overline{E}V = \begin{bmatrix} I_N & 0 \\ 0 & 0 \end{bmatrix}. \tag{10}$$

Based on Sylvester inequality, we can derive

$$\begin{aligned}&\operatorname{rank}\begin{bmatrix} I_n & 0 \\ 0 & 0 \\ C & 0 \end{bmatrix}\\ &= \operatorname{rank}\left\{ \begin{bmatrix} U & 0 \\ 0 & I_m \end{bmatrix} \begin{bmatrix} \overline{E} \\ \overline{C} \end{bmatrix} V \right\}\\ &= \operatorname{rank}\begin{bmatrix} \overline{E} \\ \overline{C} \end{bmatrix}\\ &= n+q.\end{aligned} \tag{11}$$

Therefore, we can derive

$$\begin{aligned}&\operatorname{rank}\begin{bmatrix} I_N & 0 \\ C & 0 \end{bmatrix}\\ &= \operatorname{rank}\begin{bmatrix} \overline{E} \\ \overline{C} \end{bmatrix}\\ &= n+q,\\ &\operatorname{rank}(U\overline{E}V + \overline{C}V) = \operatorname{rank}\begin{bmatrix} I_N & 0 \\ C & 0 \end{bmatrix} = n+q.\end{aligned} \tag{12}$$

When the matrix to be designed R is

$$R = V(U\overline{E}V + CV)^{-1}U. \tag{13}$$

Then the matrix R is a nonsingular matrix. Let the matrix T be

$$T = V(U\overline{E}V + CV)^{-1}. \tag{14}$$

There exists $R\overline{E} + T\overline{C} = I_{n+q}$. The relationship between matrix $[R, T]$ and matrix $[\overline{EC}]^T$ is satisfied

$$\begin{bmatrix} \overline{E} \\ \overline{C} \end{bmatrix} \begin{bmatrix} R & T \end{bmatrix} \begin{bmatrix} \overline{E} \\ \overline{C} \end{bmatrix} = \begin{bmatrix} \overline{E} \\ \overline{C} \end{bmatrix}. \tag{15}$$

Then according to Moore Penrose theorem, it can be seen that $[R, T]$ is a kind of generalized inverse matrix of $[\overline{EC}]^T$, and has

$$\begin{bmatrix} R & T \end{bmatrix} = \begin{bmatrix} \overline{E} \\ \overline{C} \end{bmatrix}^{\dagger} + \Theta\left(I_{n+q+m} - \begin{bmatrix} \overline{E} \\ \overline{C} \end{bmatrix} \begin{bmatrix} \overline{E} \\ \overline{C} \end{bmatrix}^{\dagger} \right). \tag{16}$$

Among them, $\Theta \in \mathbb{R}^{(n+q)\times(n+q+m)}$ is a freely selected matrix, and the main purpose of parameter selection is to make R a nonsingular matrix.

For the system estimation error, we can derive

$$e(k) = \overline{x}(k) - \hat{\overline{x}}(k). \tag{17}$$

Thus

$$\begin{aligned} e(k+1) &= (R\overline{E} + T\overline{C})x(k+1) - z(k+1) - Ty(k+1) \\ &= R\overline{E}x(k+1) - z(k+1) \\ &= (R\overline{A} - L\overline{C})e(k). \end{aligned} \tag{18}$$

Select the following Lyapunov function

$$V(k) = e^T(k)Pe(k), \quad P > 0. \tag{19}$$

We can derive

$$\begin{aligned} \Delta V(k) &= V(k+1) - V(k) \\ &= e^T(k)\left[(R\overline{A} - L\overline{C})^T P(R\overline{A} - L\overline{C}) - P\right]e(k). \end{aligned} \tag{20}$$

If there exists matrix P and matrix L satisfying

$$\begin{bmatrix} -P & (R\overline{A} - L\overline{C})^T P \\ P(R\overline{A} - L\overline{C}) & -P \end{bmatrix} < 0. \tag{21}$$

Then according to Schur complement theorem and Lyapunov stability theory, it can be obtained that $\Delta V(k) < 0$ and $e(k)$ is convergent. Let $W = PL$, then inequality equation (21) is equivalent to inequality equation (9).

The proof is completed. It can be learned that the defender can observe the system variables through the observer proposed in this paper when the incremental cost estimator is compromised. □

3.2. Observer Design of Output Power Decision-Maker under FDI Attacks. In this part, we focus on the observer for compromised output power decision-maker. The compromised system $\sum_{opd}$ can be expressed as

$$\begin{cases} x(k+1) = Ax(k) + Bu(k), \\ y(k) = Cx(k) + Nm(k). \end{cases} \tag{22}$$

Taking the attack vector $m(k)$ as an additional state, we can obtain the augmented state vector $\overline{x}(k) = [x(k)m(k)]^T$. The following augmented system can be established

$$\begin{cases} \overline{E}\overline{x}(k+1) = \overline{A}\overline{x}(k) + \overline{B}u(k), \\ y(k) = \overline{C}\overline{x}(k), \end{cases} \tag{23}$$

where

$$\begin{aligned} \overline{E} &= \begin{bmatrix} I_n & 0 \\ 0 & 0 \end{bmatrix}, \\ \overline{A} &= \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix}, \\ \overline{B} &= \begin{bmatrix} B \\ 0 \end{bmatrix}, \\ \overline{C} &= \begin{bmatrix} C \\ N \end{bmatrix}^T. \end{aligned} \tag{24}$$

Similarly, for this augmented system, we can also construct an observer in the form of formula (8). Conditions for the existence of observer are stated in Theorem 1. Due to space limitation, the proof of the existence of the observer is not repeated in this subsection. It can be learned that the observer design method based on augmented system can be effectively applied to the situations where incremental cost estimator or output power decision-maker is compromised.

3.3. Observer Design in Situations of Multiple Modules being Compromised considering Uncertainties. In this part, multipoint FDI attacks are considered: the attacker can launch FDI attacks on incremental cost estimator and output power decision-maker simultaneously. The compromised system $\sum_s$ can be expressed as

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) + Mm(k) + E_a\omega_a(k), \\ y(k) = Cx(k) + Nm(k) + E_s\omega_s(k), \end{cases} \tag{25}$$

where $\omega_a(k)$ and $\omega_s(k)$ are unknown input vectors caused by uncertainties of system; E_a and E_s are known constant coefficient matrices with appropriate dimensions. Taking the attack vector as an additional state, we can obtain the augmented state vector $\overline{x}(k) = [x(k)\ m(k)]^T$. The following augmented system can be established

$$\begin{cases} \overline{x}(k+1) = \overline{A}\overline{x}(k) + \overline{B}u(k) + \overline{E_a}\omega_a(k) + Gm^d(k), \\ y(k) = \overline{C}\overline{x}(k) + E_s\omega_s(k), \\ m^d(k) = m(k+1) - m(k), \end{cases} \tag{26}$$

where

$$\begin{aligned} \overline{A} &= \begin{bmatrix} A & M \\ 0 & I_q \end{bmatrix}, \\ \overline{B} &= \begin{bmatrix} B \\ 0 \end{bmatrix}, \\ \overline{C} &= \begin{bmatrix} C \\ N \end{bmatrix}^T, \\ \overline{E_a} &= \begin{bmatrix} E_a \\ 0 \end{bmatrix}^T, \\ G &= \begin{bmatrix} 0 \\ I_q \end{bmatrix}^T. \end{aligned} \tag{27}$$

The following augmented system can be established

$$\begin{cases} z(k+1) = Rz(k) + Su(k) + (L_1 + L_2)y(k), \\ \hat{\overline{x}}(k) = z(k) + Ty(k), \end{cases} \tag{28}$$

where z represents the state vector of the dynamic system equation (26); R, S, L_1, L_2 and T are the gain matrices with appropriate dimensions. The estimation error can be defined as $e(k) = \overline{x}(k) - \hat{\overline{x}}(k)$.

The derivative of the estimation error can be calculated as

$$\begin{aligned} e(k+1) &= (I - T\overline{C})\overline{x}(k+1) - z(k+1) - TE_s\omega_s(k) \\ &= \left[(I - T\overline{C})\overline{A} - L_1\overline{C}\right]e(k) \\ &\quad + \left[(I - T\overline{C})\overline{A} - L_1\overline{C} - R\right]z(k) \\ &\quad + [(I - T\overline{C})\overline{B} - S]u_k \\ &\quad + \left[((I - T\overline{C})\overline{A} - L_1\overline{C})T - L_2\right]y(k) \\ &\quad + (I - T\overline{C})\overline{E_a}\omega_a(k) + (I - T\overline{C})Gm^d(k) \\ &\quad - L_1E_s\omega_s(k) - TE_s\omega_s(k+1). \end{aligned} \tag{29}$$

If the following relationships can be held:

$$\begin{aligned} (I - T\overline{C})\overline{E_a} &= 0, \\ (I - T\overline{C})\overline{A} - L_1\overline{C} &= R, \\ (I - T\overline{C})\overline{B} &= S, \\ RT &= L_2. \end{aligned} \tag{30}$$

The derivative of the estimation error can be expressed as

$$\begin{aligned} e(k+1) &= \mathrm{Re}(k) + (I - T\overline{C})Gm^d(k) \\ &\quad - L_1E_s\omega_s(k) - TE_s\omega_s(k+1). \end{aligned} \tag{31}$$

The proof of the necessary conditions for the existence of the observer for the augmented system (26) can be found in [33] and omitted in here.

Theorem 2. *For the augmented system 23, there exists a robust observer in the form of equation (24) such that* $\|e(k)\|_{l_2} \le \sqrt{2}r\|\gamma(k)\|_{l_2}$ *where* $\gamma(k) = \left[\, m^d(k) \;\; \omega_s(k) \,\right]^T$, *if there exists a positive definite matrix P and matrix Q, such that*

$$\begin{bmatrix} -P + I_{\overline{n}} & * & * & * \\ 0_{l_\gamma \times \overline{n}} & -r^2 I_{l_\gamma} & * & * \\ 0_{l_\gamma \times \overline{n}} & 0_{l_\gamma \times l_\gamma} & -r^2 I_{l_\gamma} & * \\ PA_1 - Q\overline{C} & PV_1 - QV_2 & P\overline{V}_2 & -P \end{bmatrix} < 0, \tag{32}$$

where $A_1 = (I - T\overline{C})\overline{A}$, $Q = PL_1$, $V_1 = [(I - T\overline{C})G0_{\overline{n}\times l_n}]$, $V_2 = [0_{p\times q}E_s]$, *and* $\overline{V}_2 = -TV_2$.

Proof. Proof. Take the following Lyapunov function candidate for system (30)

$$V(k) = e^T(k)Pe(k), \tag{33}$$

one has

$$\begin{aligned} \Delta V(k) &= V(k+1) - V(k) \\ &= \begin{bmatrix} e(k) \\ \gamma(k) \\ \gamma(k+1) \end{bmatrix}^T \left(\begin{bmatrix} R \\ V_1 - L_1V_2 \\ \overline{V}_2 \end{bmatrix} P \begin{bmatrix} R \\ V_1 - L_1V_2 \\ \overline{V}_2 \end{bmatrix}^T + \begin{bmatrix} -P & 0 \\ 0 & 0 \end{bmatrix} \right) \begin{bmatrix} e(k) \\ \gamma(k) \\ \gamma(k+1) \end{bmatrix}. \end{aligned} \tag{34}$$

If $\gamma(k) = 0$, from equations (32) and (34) one has $\Delta V(k) < 0$. The error dynamic is asymptotically stable.

Let

$$\begin{aligned} \Gamma = \sum_{k=0}^{\infty} \big(&\Delta V(k) + e^T(k)e(k) - r^2\gamma^T(k)\gamma(k) \\ &- r^2\gamma^T(k+1)\gamma(k+1) \big). \end{aligned} \tag{35}$$

We can derive

$$\begin{aligned} \Gamma = \sum_{k=0}^{\infty} &\begin{bmatrix} e(k) \\ \gamma(k) \\ \gamma(k+1) \end{bmatrix}^T \left[\left(\left(\begin{bmatrix} R \\ V_1 - L_1V_2 \\ \overline{V}_2 \end{bmatrix} P \right) P^{-1} \right. \right. \\ &\left. \left. \left(P \begin{bmatrix} R \\ V_1 - L_1V_2 \\ \overline{V}_2 \end{bmatrix} \right) \right) + \begin{bmatrix} -P + I & 0 \\ 0 & -r^2 I \end{bmatrix} \right] \begin{bmatrix} e(k) \\ \gamma(k) \\ \gamma(k+1) \end{bmatrix}. \end{aligned} \tag{36}$$

Based on equations (32) and (36), we can derive

$$\begin{aligned} &\sum_{k=0}^{\infty} \left(e^T(k)e(k) - r^2\gamma^T(k)\gamma(k) - r^2\gamma^T(k+1)\gamma(k+1) \right) \\ &+ V(\infty) - V(0) < 0. \end{aligned} \tag{37}$$

In view of the fact that $V(\infty) \ge 0$ and $V(0) = 0$, we can derive

$$\sum_{k=0}^{\infty} e^T(k)e(k) - 2r^2\gamma^T(k)\gamma(k) < 0, \tag{38}$$

which is equivalent to $\|e(k)\|_{l_2} \le \sqrt{2}r\|\gamma(k)\|_{l_2}$. The proof is completed.

Based on the proposed observer, we can derive the observed data of the variables and the measured data of those in DDCA. For the defender, it is necessary to identify the similarities between the measured data and the observed data under normal situations and distinguish the differences under the compromised situations. □

4. Detection Scheme against FDI Attack considering Dual Source Data

In this section, we study the attack detection scheme against FDI attacks based on the observed data of the variables and

the measured data of those in DDCA. A relation-based detection network is proposed to extract the similarity of the dual source data. We design the machine-learning-based detection scheme based on the following considerations:

(i) The method of calculating dual source data vector similarity based on traditional Euclidean distance requires too much prior knowledge level of defenders. In this paper, we use an embedding module and a relation module to extract the similarity of the dual source data automatically.

(ii) Traditional machine learning methods need the distance of data vector in feature space to identify, which means that large scale of training data set is needed. In this paper, we skip the learning of feature distance and directly learn the relationship between dual source data, so as to effectively reduce the demand for the size of data set.

As is shown in Figure 1, the detection network contains measured data set, observed data set, Embedding module, and relation module. The data in the observed data set can reflect the current real operating state of the DDCA system, and the data in the measured data set may be tampered with. As to the attack detection network, we identify the attack by comparing the observed data with measured data. The measured data set consists of the compromised data set and the normal data set. When the data for comparison comes from the compromised data set, the relationship between dual source data is strong similarity. When the data for comparison comes from the normal data set, the relationship between two dual data is weak similarity.

As to the datasets, the data vectors in each dataset consists of the time series data of target variables in DDCA, including the data of incremental cost and those of output power. The data vector in the measured data set is written as d_m. The data vector in the observed data set is written as d_o. The embedding module, which consists of full connect layers and rectified linear units (ReLUs), is used to extract the features of samples with a nonlinear function $\mathscr{E}$. Compared with the traditional manual feature extraction method, the feature extraction by full connect layers can reduce the prior knowledge requirements of attack detection network for attack features. Rectified linear units are used to improve the generalization ability of the embedding module. The feature vectors of measured data and observed data generated by the embedding module can be expressed as $\mathscr{F}(d_m)$ and $\mathscr{F}(d_o)$. To alleviate the over fitting problem of the embedding module, class prototype of each feature vector class is adopted. The prototype $\mathscr{P}_i^m$ of the measured data feature vectors and the prototype $\mathscr{P}_i^o$ of the observed data feature vectors can be expressed as

$$\mathscr{P}_i^m = \frac{1}{N_i^m}\sum_{j=1}^{N_i^m}\mathscr{F}(d_m),$$
$$\mathscr{P}_i^o = \frac{1}{N_i^o}\sum_{j=1}^{N_i^o}\mathscr{F}(d_o). \tag{39}$$

We can derive the class feature vector $\mathscr{C}(\mathscr{P}_i^m, \mathscr{P}_i^o)$ by concatenating the prototypes in depth dimension. The relation module is used to extract the similarity between the concatenations with a nonlinear relation function $\mathscr{R}$. The similarity $\mathscr{S}$ can be written as

$$\mathscr{S} = \mathscr{R}\left(\mathscr{C}\left(\mathscr{P}_i^m, \mathscr{P}_i^o\right)\right). \tag{40}$$

To train the attack detection model, mean square error (MSE) is used as the objective function L_m.

$$L_m = \begin{cases} \sum\sum(\mathscr{S}-1)^2, l_m = l_o, \\ \sum\sum(\mathscr{S}-0)^2, l_m \neq l_o. \end{cases} \tag{41}$$

If the measured data is compromised, then $l_m \neq l_o$ and $\mathscr{S}$ is closed to 0. If the measured data is normal, then $l_m = l_o$ and $\mathscr{S}$ is closed to 1.

Pseudocode for the proposed detection scheme is provided in Figure 2. First, input samples of variables of interest in DDCA as measured data set. Label the compromised data and the normal data. Then, use the proposed observer to observe the variables and form the observed data set. Then, obtain the feature vectors and prototype vectors in order with the help of the proposed module. Based on the relation feature vector concatenated by prototype vectors, calculate the similarity score using relation module. Based on the proposed objective function, optimize the model parameters with the stochastic gradient descent optimizer. After training the model, sample the incoming data, calculate the similarity and output the type of the test data.

5. Case Study

In this section, simulations are carried out to illustrate the effectiveness of the proposed observer and attack detection network of the variables in DDCA. The Barry Island electricity and heating networks is used as the tested system. The structure and parameters of the system can be found in [34].

5.1. Performance of the Observer for the Compromised System. In the DDCA system, the coefficient matrices are

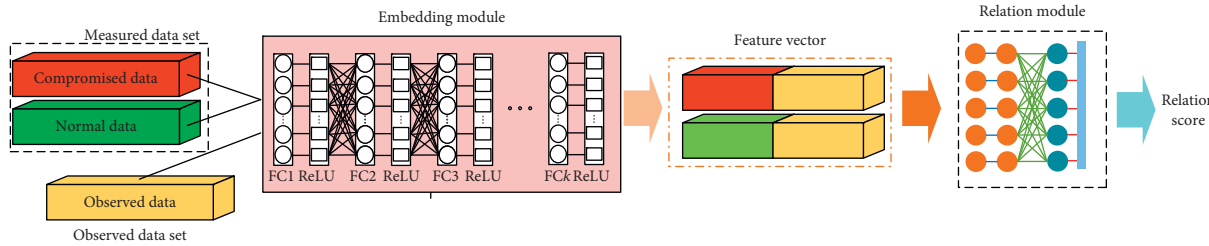

Figure 1: The relation network for FDI attack detection.

1: Input the measured data vector d_m containing x_p^P, x_p^C, x_h^C, x_h^H, $\tilde{x}_p^P$, $\tilde{x}_p^C$, $\tilde{x}_h^C$ and $\tilde{x}_h^H$ to form measured dataset.

2: Input the observed data vector d_o containing $\hat{x}_p^P$, $\hat{x}_p^C$, $\hat{x}_h^C$, and $\hat{x}_h^H$ obtained by the proposed observer to from observed dataset.

3: Obtain feature vectors $F(d_o)$ and $F(d_m)$ using embedding module.

4: Obtain prototype vectors P_i^o and P_i^m of each class using prototype equation.

5: Concatenate P_i^o and P_i^m as relation feature vector $C(P_i^m, P_i^o)$.

6: Calculate similarity score S using relation module.

7: Calculate L_m

8: Optimize (Stochastic Gradient Descent)

9: End While

10: Input test data vector.

11. Calculate relation score.

12. Output the type of the test data.

Figure 2: Pseudocode for the proposed detection scheme.

$$A = \begin{bmatrix} 0.9988 & 0.0007 & 0.0006 & -0.0037 \\ 0.0014 & 0.98 & -0.0012 & -0.0206 \\ 0.001 & 0.0037 & 1.0467 & 9.5584 \\ 0 & 0 & 0.0101 & 1.0234 \end{bmatrix},$$

$$B = \begin{bmatrix} 0.0052 & 0.0012 \\ 0.0315 & -0.0755 \\ -0.0582 & 0.0454 \\ -0.0003 & 0.0002 \end{bmatrix}, \quad (42)$$

$$C = \begin{bmatrix} 0.45 & 0.32 & 0.12 & 0.11 \\ 0.38 & 0.42 & 0.13 & 0.07 \\ 0.27 & 0.31 & 0.33 & 0.09 \\ 0.07 & 0.13 & 0.43 & 0.37 \end{bmatrix}.$$

The attack vector is $m(k) = [m_1(k) \ m_2(k)]^T$, where

$$m_1(k) = \begin{cases} 0, & k < 60, \\ 0.05(k-60), & 60 \le k < 100, \\ 2, & k \ge 100, \end{cases} \quad (43)$$

$$m_2(k) = \begin{cases} 0, & k < 60, \\ 1, & k \ge 60. \end{cases}$$

First, we illustrate the performance of observer against false data injection attacks on incremental cost estimator. The attack target variable is x_p^P. Based on the method proposed in Section 1, the observed data of the variable x_p^P can be obtained. The simulation result of the dual source data is shown in Figure 3. The observation error is shown in Figure 4. It can be learned that when the attack volume is a static value, the observed data can effectively track the measured data. When the attack volume changes, there is a certain observation error between the observed data and the measured data, because the changed attack volume is equivalent to the changing disturbance volume. The difference between the observed data and the measured data will be an important basis for the attack detection network to identify whether the system is compromised.

Then, the performance of observer against false data injection attacks on output power decision-maker is studied. The attack target variable is y_p^C. Based on the method proposed in Section 2, the observed data of the state variable x_p^C in DDCA can be obtained. The simulation results are shown in Figures 5 and 6.

It can be learned that the FDI attacks on electric output power y_p^C in the output power decision-maker makes the measured incremental cost data x_p^P different from the observed ones. Compared with the FDI attacks on incremental cost estimator, the impact of FDI attacks on output power decision-maker can be reflected by the variables in incremental cost estimator.

To illustrate the performance of the proposed observer in situations of multiple modules being compromised, we analysis the simulation results considering the situation that x_h^C and y_h^C are compromised simultaneously. Based on the method proposed in Section 3, the observed data of the variable x_h^C can be obtained. The simulation results are shown in Figures 7 and8. It can be learned that there are obvious differences between the measured data and the observed data. The difference of dual source data is affected by the attack volume, as well as the system noise, disturbance and delay. Therefore, it is necessary to identify whether the system is compromised based on the attack detection scheme.

5.2. Performance of the Observer for the Relation-Based Attack Detection Scheme. In this subsection, we evaluate the performance of the proposed attack detection scheme. In the embedding module, there are three full connect layers and rectified linear units. The batch size of the relation network is chosen as 20. In the measured data set, there are 500 normal

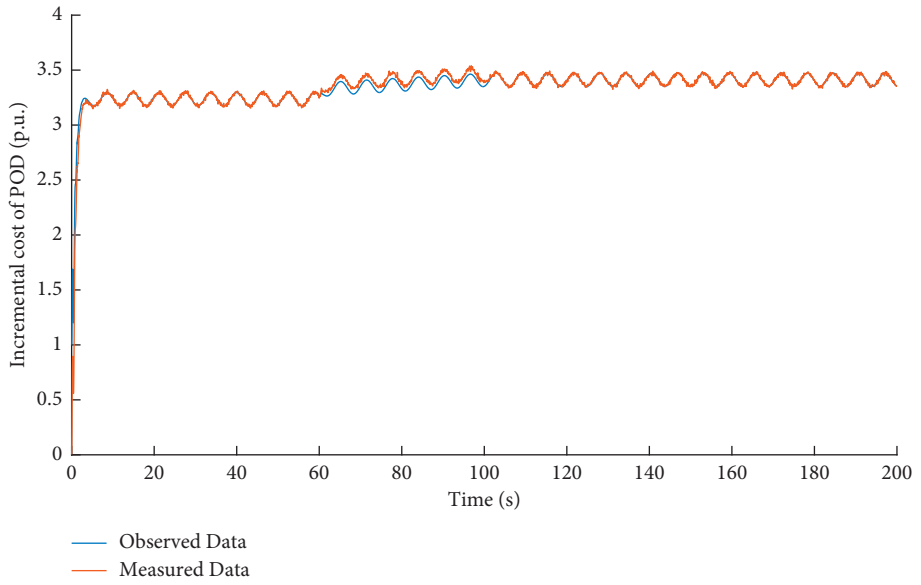

Figure 3: Dual source data of variable x_p^P under FDI attacks on incremental cost estimator.

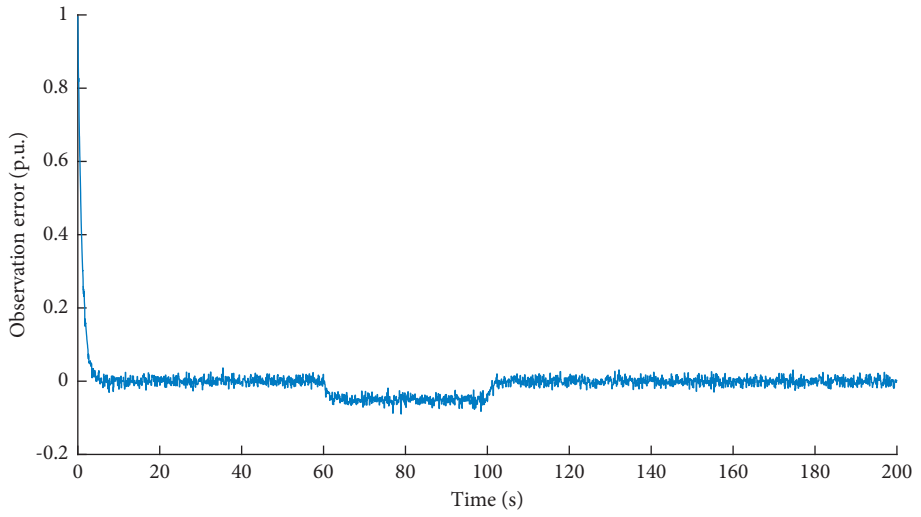

Figure 4: Observation error of variable x_p^P under FDI attacks on incremental cost estimator.

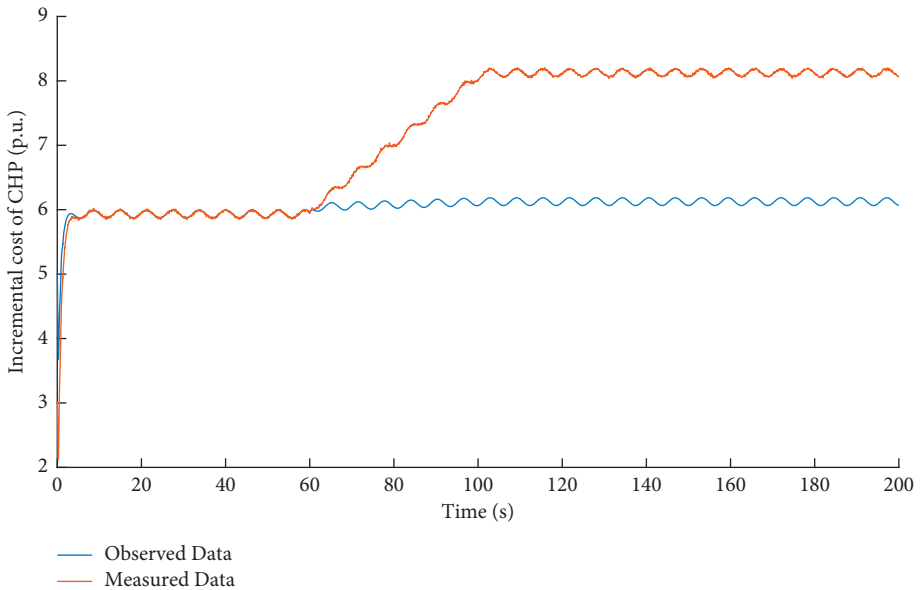

Figure 5: Dual source data of variable x_p^C under FDI attacks on output power decision-maker.

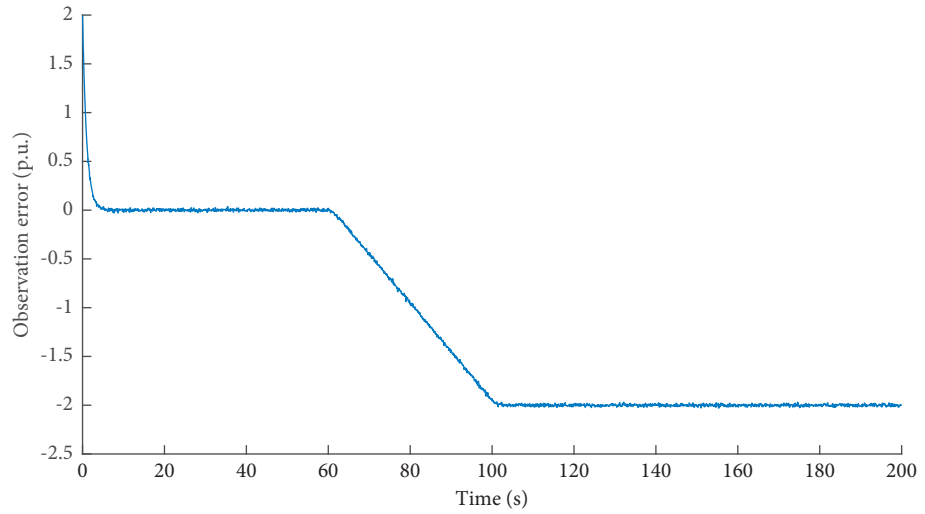

Figure 6: Observation error of variable x_p^C under FDI attacks on output power decision-maker.

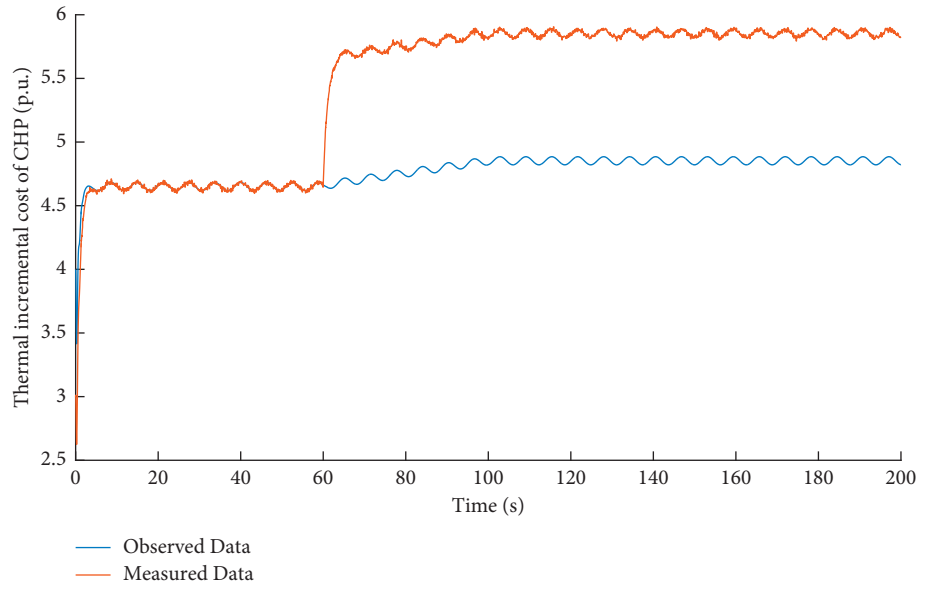

Figure 7: Dual source data of variable x_h^C under FDI attacks on multiple modules.

sample data and 500 compromised data from the historical database. In the observed data set, 1000 observed data are generated based on the proposed method studied in Section B. The simulations are carried out on a personal computer with Intel processor core i7, cache 3.4 GHz, NVIDIA GTX 2060, and random-access memory (RAM) 32 GB.

To evaluate the performance of the relation-based attack detection scheme, the following metrics are used:

(1) Accuracy:

$$MA = \frac{TP + TN}{TP + TN + FP + FN}, \tag{44}$$

where TP represents the number of true positive detection results; TN represents the number of true negative detection results; FP represents the number of false positive detection results; FN represents the number of false negative detection results.

(2) The probability of detecting correctly:

$$MD = \frac{TP}{TP + FN}. \tag{45}$$

(3) Success ratio:

$$MS = \frac{TP}{TP + FP}. \tag{46}$$

(4) Probability of identifying normal cases:

$$MI = \frac{TN}{TN + FP}. \tag{47}$$

(5) Trade off between M_{dc} and M_s:

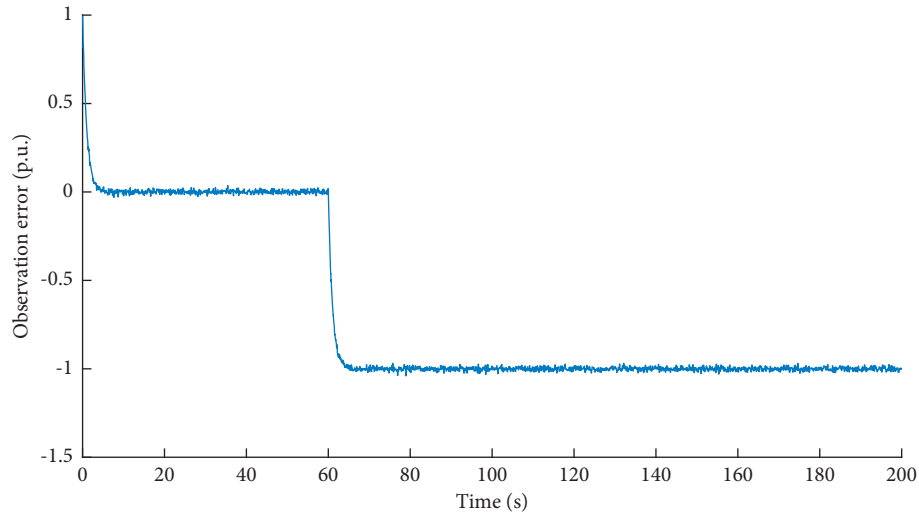

Figure 8: Observation error of variable x_h^C under FDI attacks on multiple modules.

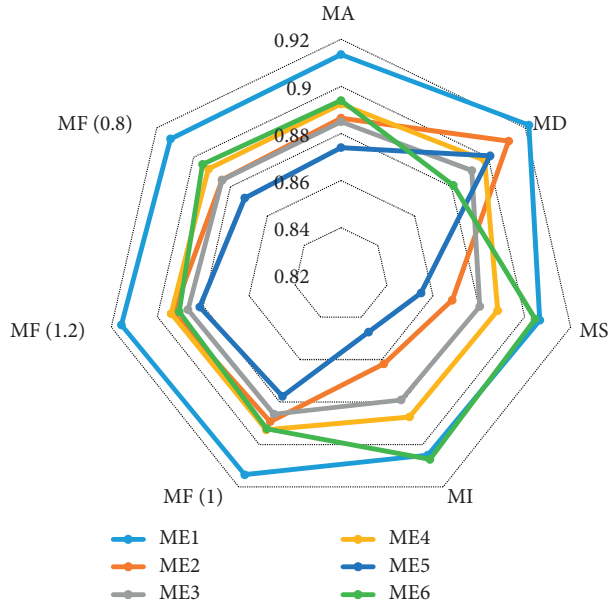

Figure 9: Performance of different attack detection method.

$$MF(\mathcal{T}) = \frac{\left(1+\mathcal{T}^2\right)\cdot M_{dc}\cdot M_s}{\mathcal{T}^2\cdot M_{dc}+M_s}, \tag{48}$$

where $\mathcal{T}$ is the trade-off coefficient. Details about the performance metrics can be found in [31].

To illustrate the effectiveness of the proposed detection scheme, six methods are adopted for comparison: (1) The proposed relation-based attack detection scheme (ME1); (2) Attack detection scheme using relation network without prototype module (ME2); (3) Attack detection scheme using multi-layer perception (ME3); (4) Attack detection scheme using signal forecasting method (ME4); (5) Attack detection scheme using support vector machine (ME5); (6) Attack detection scheme using clustering artificial bee colony algorithm (ME6).

The simulation results are shown in Figure 9. Compared with other attack detection scheme, the attack detection scheme (ME1) proposed in this paper has better performance in each algorithm evaluation index, that is, the proposed detection scheme can effectively detect false data injection attacks on variables in DDCA. The better performance of the proposed attack detection scheme mainly comes from the fact that the relation-based attack detection network focuses on exploiting the differences between normal data and compromised data, while the other attack detection schemes focus on exploiting the features. If the common features of normal data and compromised data are

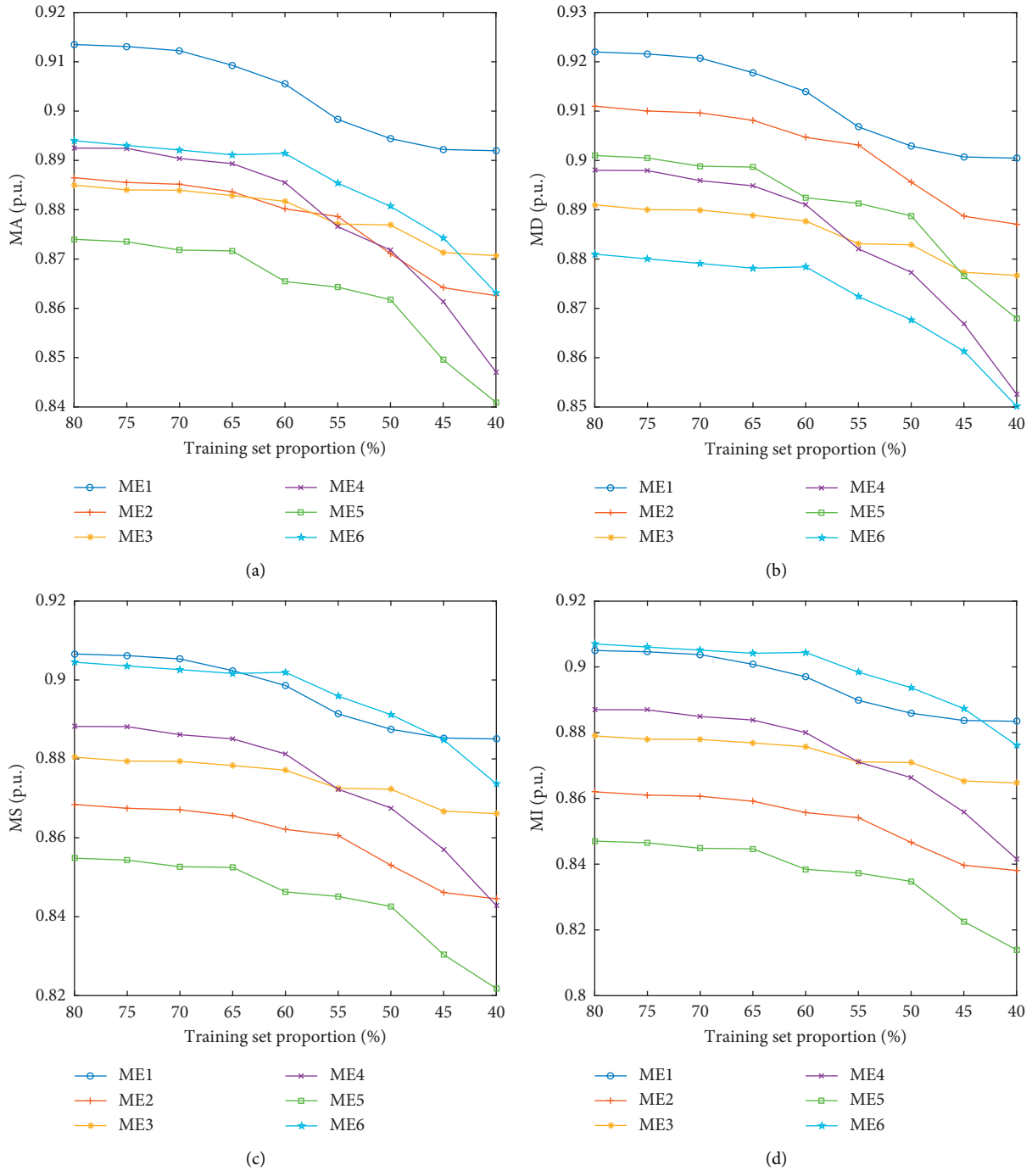

Figure 10: Performance of detection schemes considering different training set proportion. (a) MA. (b) MD. (c). MS. (d) MI.

learned by the other attack detection schemes, it will have a negative impact on the performance of the attack detection schemes.

5.3. Stability and Reliability of the Relation-Based Attack Detection Scheme. In order to further investigate the stability of the detection performance of the proposed attack detection scheme, the performance of the attack detection scheme with different proportion of training sets is studied: at an interval of 5%, samples with a proportion from 40% to 80% are selected as the training sets. The simulation results are shown in Figure 10. It can be seen that although the performance of the proposed attack detection scheme will decline with the sample size, and the performance of some training sample sizes is inferior to other schemes, its overall attack detection performance is basically in the first echelon, which verifies that the attack detection scheme still has excellent detection effect under the sample size discussed in this section.

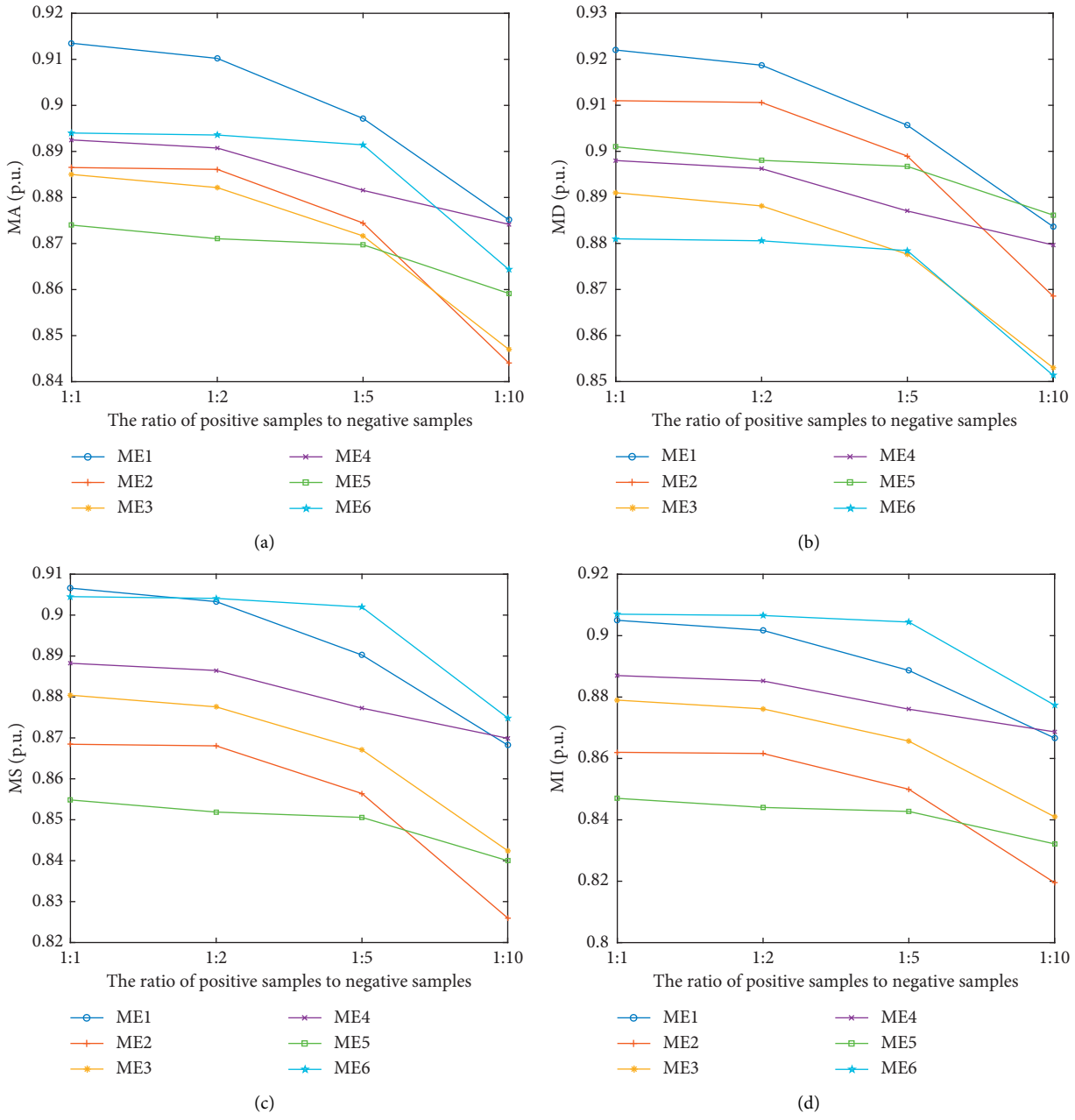

Figure 11: Performance of detection schemes considering different ratio of positive samples to negative samples. (a) MA. (b) MS. (c) MS. (d) MI.

Considering the insufficient samples of compromised data in practice, we further discuss the reliability and stability under different positive and negative sample ratios. In this section, the ratio of positive samples to negative samples is 1 : 1, 1 : 2, 1 : 5 and 1 : 10 respectively. The specific performance verification effect is shown in Figure 11. It can be learned that when the number of positive samples is smaller than the number of negative samples, the performance of the proposed attack detection scheme will decline to a certain extent, but the overall performance still has certain advantages over other detection schemes. The decline of detection performance is mainly due to the fact that the attack detection network can not fully learn the difference between positive and negative samples.

Considering that the detection scheme proposed in this paper depends on the real-time data of the sensors, we further study the impact of measurement noise and measurement delay on the attack detection performance in the process of collecting sensor data. We design two metrics, security noise and security delay, to evaluate the detection performance of the proposed attack detection method. Safe noise (delay) refers to the maximum noise (delay) that can be tolerated when the detection accuracy (MA) reaches a specified threshold.

Table 1: Safe noise and delay considering different threshold of detection accuracy.

Threshold of MA	75%	80%	85%	90%
Safe noise	15.2 dB	11.3 dB	9.8 dB	4.4 dB
Safe delay	7.2 s	5.7 s	2.9 s	2.1 s

Safe noise and safe delay considering different threshold of MA are in Table 1. It can be learned that the safe noise (delay) decreases with the increase of the threshold. It can be seen that when there are high requirements for the accuracy of the detection scheme, the data required by the detection scheme is also more ideal. Noise and delay have a significant impact on the detection effect. Correspondingly, if the requirements for detection performance are appropriately reduced, the proposed detection scheme has a certain tolerance to noise and delay. As a remedy, the defender should also consider using a variety of detection schemes to cross check the attack behavior, so as to improve the overall accuracy.

6. Conclusions and Discussions

6.1. Conclusions. In this article, false data injection attacks on distributed controller of electric-thermal integrated energy system and countermeasures are studied. Observers of variables in DDCA are designed to track the compromised data. The proposed observer can achieve the observation considering different attack targets in DDCA. Based on the observed data and the measured data, we proposed a relation-based attack detection scheme to identify the false data injection attacks.

The simulation results show that the attack detection scheme has better performance than the current mainstream scheme under multiple evaluation indexes. The better detection performance of the proposed scheme is attributed to its direct judgment of the difference between normal data pairs and compromised data pairs, which reduces the learning of other unnecessary or incorrect features. For the stability of the proposed scheme, compared with other schemes, the proposed scheme can maintain better detection performance with less proportion of training sets.

Therefore, we believe that the proposed attack detection scheme can achieve good performance against FDI attacks on ETIES.

6.2. Discussions. It can be seen that the limitation of the proposed method used in this paper is that it requires real-time data of the system, which makes the defender have a certain dependence on the real-time sensor communication network. As to practical implementation, the challenge is how to deal with the large-scale destruction of more sensors by attackers. In such a scenario, the trusted data available in this paper will be reduced, and the ability to identify attacks will be reduced.

A possible mitigation approach is to stop using the real-time data obtained by the sensors of the system. As an alternative, the defender can use the system model and historical data to generate prediction data for real-time data, and use the predicted data combined with the algorithm proposed in this paper to identify cyber attacks. It can be seen that this research idea further reduces the dependence on real-time sensors, thereby reducing the uncertainty under large-scale attacks.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work is supported by the National Grid Corporation of China project "All-electric Campus."

References

[1] A. Qian and H. Ran, "Key technologies and challenges for multi-energy complementarity and optimization of integrated energy system," *Automation of Electric Power Systems*, vol. 42, no. 4, pp. 2–10, 2018.

[2] J. Li, J. Fang, Q. Zeng, and Z. Chen, "Optimal operation of the integrated electrical and heating systems to accommodate the intermittent renewable sources," *Applied Energy*, vol. 167, pp. 244–254, 2016.

[3] J. Li, M. Zhu, and Y. Huang, "Classification and location scheme selection of coupling components in integrated electrical and heating systems with renewable energy," *CSEE Journal of Power and Energy Systems*, vol. 6, no. 3, pp. 619–629, 2019.

[4] Y. Ding, Y. Jiang, and Y. Song, "Review of risk assessment for energy internet, part i: physical level," *Proceedings of the CSEE*, vol. 36, no. 14, pp. 3806–3817, 2016.

[5] J. Yibao, S. Yonghua, D. Yi, G. Chuangxin, and J. Wende, "Review of risk assessment for energy internet part t ii: information and market level," *Proceedings of the CSEE*, vol. 36, pp. 4023–4025, 2016.

[6] M. S. Mahmoud, H. M. Khalid, and M. M. Hamdan, *Cyberphysical Infrastructures in Power Systems: Architectures and Vulnerabilities*, Academic Press, Massachusetts, MA, USA, 2021.

[7] W. He, W. Xu, X. Ge, Q.-L. Han, W. Du, and F. Qian, "Secure control of multi-agent systems against malicious attacks: a brief survey," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 3595–3608, 2022.

[8] Y. Miao, C. Chen, L. Pan, Q.-L. Han, J. Zhang, and Y. Xiang, "Machine learning–based cyber attacks targeting on controlled information: a survey," *ACM Computing Surveys*, vol. 54, no. 7, pp. 1–36, 2022.

[9] H. M. Khalid, S. M. Muyeen, and J. C.-H. Peng, "Cyber-attacks in a looped energy-water nexus: an inoculated sub-observer-based approach," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2054–2065, 2020.

[10] C. Chen, Y. Wang, M. Cui et al., "Data-driven detection of stealthy false data injection attack against power system state estimation," *IEEE Transactions on Industrial Informatics*, p. 1, 2022.

[11] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–33, 2011.

[12] M. Molnár and I. Vokony, "Impact analysis of false data injection attacks on distribution system state estimation," in *Proceedings of the IEEE International Conference on Environment and Electrical Engineering and 2021 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*, pp. 1–6, IEEE, Bari, Italy, September 2021.

[13] H. M. Khalid and J. C.-H. Peng, "A bayesian algorithm to enhance the resilience of wams applications against cyber attacks," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2026–2037, 2016.

[14] H. M. Khalid and C. H. Peng, "Immunity toward data-injection attacks using multisensor track fusion-based model prediction," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 697–707, 2017.

[15] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proceedings of the Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, Stockholm, Sweden, January 2011.

[16] K. C. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *Proceedings of the 50th IEEE Conference on Decision and Control and European Control Conference*, pp. 4054–4059, IEEE, Orlando, FL, USA, December 2011.

[17] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proceedings of the first IEEE international conference on smart grid communications*, pp. 214–219, IEEE, Gaithersburg, MD, USA, October 2010.

[18] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[19] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: attack strategies and countermeasures," in *Proceedings of the first IEEE international conference on smart grid communications*, pp. 220–225, IEEE, Gaithersburg, MD, USA, October 2010.

[20] K. C. Sou, H. Sandberg, and K. H. Johansson, "Computing critical k -tuples in power networks," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1511–1520, 2012.

[21] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-security in smart grid: survey and challenges," *Computers & Electrical Engineering*, vol. 67, no. 11, pp. 469–482, 2018.

[22] J. Kim and L. Tong, "On topology attack of a smart grid: undetectable attacks and countermeasures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1294–1305, 2013.

[23] D. Deb, S. R. Chakraborty, M. Lagineni, and K. Singh, "Security analysis of MITM attack on SCADA network," *Machine Learning, Image Processing, Network Security and Data Sciences*, Springer, Berlin, Germany, 2020.

[24] J. Kim, L. Tong, and R. J. Thomas, "Data framing attack on state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1460–1470, 2014.

[25] X. Liu, P. Zhu, Y. Zhang, and K. Chen, "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2435–2443, 2015.

[26] B. Li, R. Lu, K.-K. R. Choo, W. Wang, and S. Luo, "On reliability analysis of smart grids under topology attacks: a stochastic petri net approach," *ACM Transactions on Cyber-Physical Systems*, vol. 3, no. 1, pp. 1–25, 2019.

[27] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 1932–1941, 2018.

[28] P. Xun, P. Zhu, Z. Zhang, P. Cui, and Y. Xiong, "Detectors on edge nodes against false data injection on transmission lines of smart grid," *Electronics*, vol. 7, no. 6, pp. 89–103, 2018.

[29] S. Ahmed, Y. Lee, S.-H. Hyun, and I. Koo, "Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2765–2777, 2019.

[30] W. Bi, K. Zhang, Y. Li, K. Yuan, and Y. Wang, "Detection scheme against cyber-physical attacks on load frequency control based on dynamic characteristics analysis," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2859–2868, 2019.

[31] M. Cui, J. Wang, and M. Yue, "Machine learning-based anomaly detection for load forecasting under cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5724–5734, 2019.

[32] Q. Sun, R. Fan, Y. Li, B. Huang, and D. Ma, "A distributed double-consensus algorithm for residential we-energy," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 8, pp. 1–4842, 2019.

[33] Z. Gao, X. Liu, and M. Z. Chen, "Unknown input observer-based robust fault estimation for systems corrupted by partially decoupled disturbances," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 4, pp. 1–2547, 2015.

[34] X. Liu, J. Wu, N. Jenkins, and A. Bagdanavicius, "Combined analysis of electricity and heat networks," *Applied Energy*, vol. 162, pp. 1238–1250, 2016.