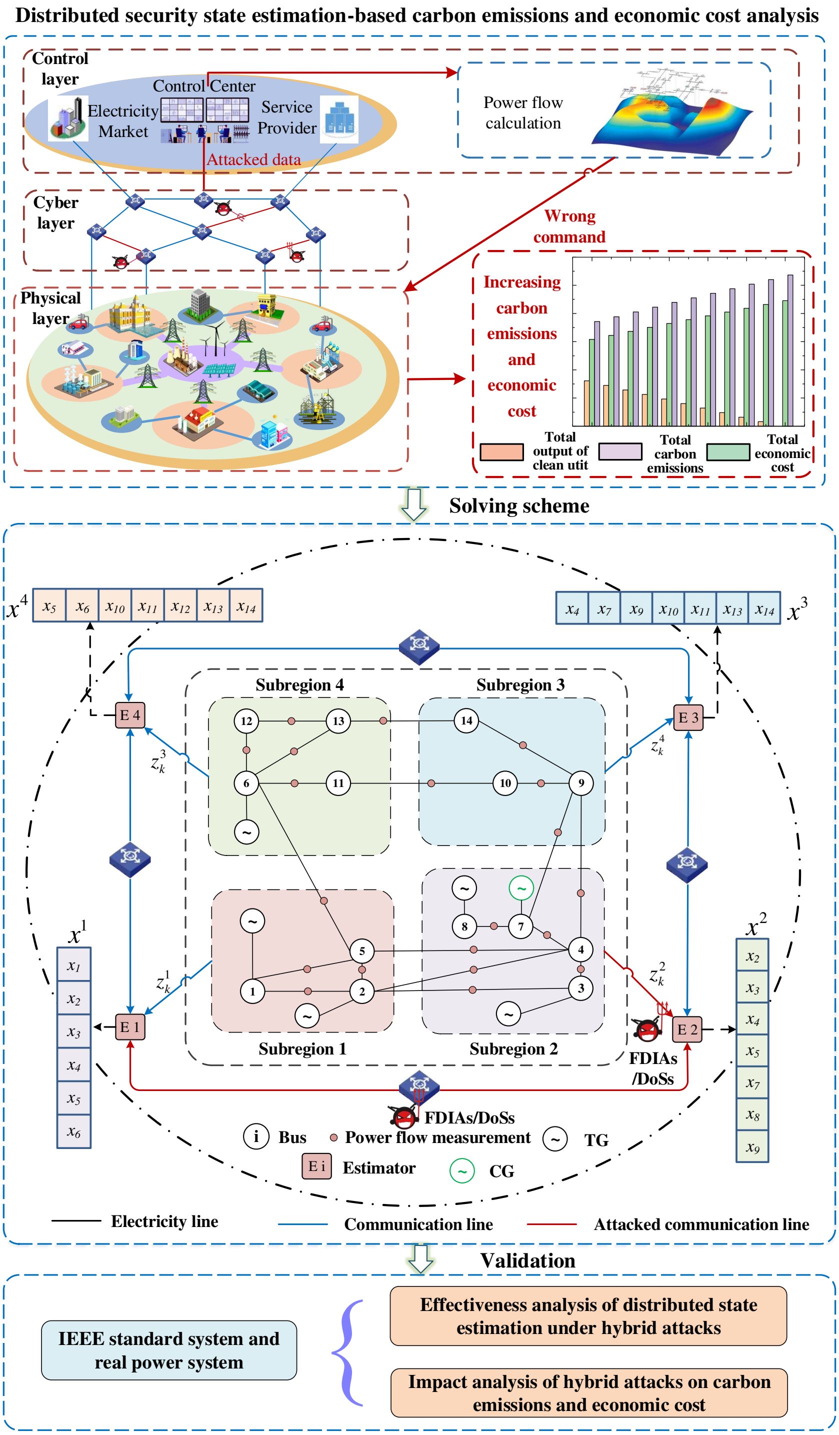
Graphical Abstract

Distributed security state estimation-based carbon emissions and economic cost analysis for cyber-physical power systems under hybrid attacks

Dajun Du,Minggao Zhu,Dakui Wu,Xue Li,Minrui Fei,Yukun Hu,Kang Li


Distributed security state estimation-based carbon emissions and economic cost analysis
Control layer
Control Center
Electricity Market
Service Provider
Attacked data
Power flow calculation
Cyber layer
Wrong command
Physical layer
Increasing carbon emissions and economic cost
Total output of clean utit
Total carbon emissions
Total economic cost
Solving scheme
x^4
x_5 x_6 x_{10} x_{11} x_{12} x_{13} x_{14}
x^3
x_4 x_7 x_9 x_{10} x_{11} x_{13} x_{14}
Subregion 4
Subregion 3
Subregion 1
Subregion 2
E 1
E 2
E 3
E 4
z_k^1
z_k^2
z_k^3
z_k^4
x^1
x_1 x_2 x_3 x_4 x_5 x_6
x^2
x_2 x_3 x_4 x_5 x_7 x_8 x_9
1 2 3 4 5 6 7 8 9 10 11 12 13 14
FDIAs /DoSs
FDIAs/DoSs
i Bus
Power flow measurement
TG
E i Estimator
CG
Electricity line
Communication line
Attacked communication line
Validation
IEEE standard system and real power system
Effectiveness analysis of distributed state estimation under hybrid attacks
Impact analysis of hybrid attacks on carbon emissions and economic cost

Highlights

Distributed security state estimation-based carbon emissions and economic cost analysis for cyber-physical power systems under hybrid attacks

Dajun Du,Minggao Zhu,Dakui Wu,Xue Li,Minrui Fei,Yukun Hu,Kang Li

- The incomplete and non-authenticity characters of the data caused by hybrid attacks are described.
- A novel residual-based attack detection method is proposed to determine secure and non-secure sets.
- A distributed security state estimation method with compensation mechanism is proposed.
- Carbon emissions and economic cost can be reduced by relieving attack impact on state estimation.

Distributed security state estimation-based carbon emissions and economic cost analysis for cyber-physical power systems under hybrid attacks

Dajun Du[a], Minggao Zhu[a,*], Dakui Wu[a], Xue Li[a], Minrui Fei[a], Yukun Hu[b] and Kang Li[c]

[a] *Shanghai Key Laboratory of Power Station Automation Technology, School of Mechatronics Engineering and Automation, Shanghai University, Shanghai, 200072, China*

[b] *Department of Civil, Environment & Geomatic Engineering, University College London, London, WC1E 6BT, United Kingdom*

[c] *School of Electronic and Electrical Engineering, University of Leeds, Leeds, LS2 9JT, United Kingdom*

ARTICLE INFO

Keywords:
Cyber-physical power system
Hybrid attacks
Attack detection
Distributed security state estimation
Convergence analysis
Carbon emissions

ABSTRACT

Sustainable cyber-physical power systems (CPPSs) are of great significance to reduce carbon emissions in response to the global climate change. However, when the data exchange in CPPSs suffers from hybrid attacks, the distributed state estimation and optimal power flow (OPF) analysis will be inevitably compromised, leading to inadequate even faulty scheduling of clean energy and thermal power generations and further affecting the total carbon emissions and economic cost. To address these problems, this paper proposes a novel consensus-based distributed security state estimation (DSSE) method for CPPSs, which is used to analyze the impact of hybrid attacks on carbon emissions and economic cost. First, the incomplete and non-authentic features of the data caused by hybrid attacks are described, and their influence on distributed state estimation model is analyzed. A new residual-based attack detection method is then constructed in each subregion, where secure and non-secure sets are employed to describe whether the subregion is attacked and the compensation mechanism is designed for non-secure set. Second, considering data compensation, distributed state estimation model is reconstructed, and a distributed security state estimation method under hybrid attacks is proposed while its convergence condition is derived. Third, the impacts of hybrid attacks on carbon emissions and economic cost are analyzed based on the proposed DSSE method. Finally, experimental results also validate the analysis.

1. Introduction

Due to high reliance on fossil fuels, the power generation sector still accounts for more than 35% of carbon emissions in China [1]. To achieve carbon neutrality goals in compliance with the Paris Agreement [2], traditional power systems are shifting to low-carbon and sustainable cyber-physical power systems (CPPSs) [3, 4, 5], which are usually achieved by integrating clean energy such as solar power, wind power, nuclear power and hydro, etc [6, 7, 8]. By the end of the first quarter of 2022, the installed capacity of China's solar power generation equipment reached 320 million kW (including 317.98 million kW of photovoltaic power generation and 0.57 million kW of solar thermal power generation), and the installed capacity of wind power generation equipment reached 340 million kW (including 309.87 million kW of onshore wind power and 26.65 million kW of offshore wind power) [9]. To support safe and reliable operation and control of CPPSs, a large number of measurement and control data from power grid are transmitted through communication networks [10], and these data will further be used for scheduling, control, protection and so on [11, 12].

However, due to the openness of communication network [13, 14, 15], CPPSs will inevitably become a target of attacks by the hacker [16, 17]. For example, the hacker compromised power system in Ukraine, causing widespread power outages in 2015 [18]. The hacker invaded several regional power companies in 2016, which brought 200 MW power generation units out of operation [19]. More recently, trunk line 765 of Venezuela's national grid was attacked in 2020, causing a total blackout in 11 states [20].

State estimation is a key building block of modern energy management in CPPSs. However, when the measurement data compromised by cyber attacks, the accuracy and convergence of state estimation will be affected. To address

[*] Corresponding author

ddj@i.shu.edu.cn (D. Du); minggaozhu@shu.edu.cn (M. Zhu); dkwu306@shu.edu.cn (D. Wu); lixue@shu.edu.cn (X. Li); mrfei@staff.shu.edu.cn (M. Fei); yukun.hu@ucl.ac.uk (Y. Hu); k.li1@leeds.ac.uk (K. Li)

ORCID(s): 0000-0003-2979-1507 (D. Du)

Nomenclature

Abbreviations

CPPSs cyber-physical power systems

OPF optimal power flow

DSSE distributed security state estimation

FDIAs false data injection attacks

ADMM alternating direction method of multipliers

AGC automatic generation control

IES integrated energy system

DoSs denial of service attacks

CGs clean energy generators

TGs thermal power generators

Variables

x global system state

x^i system state of subregion i

z measurement

z^i measurement of subregion i

ω process noises

Q process noises covariance

υ measurement noises

R measurement noises covariance

A state transition matrix

A^i state transition matrix of subregion i

H Jacobian matrix

H^i Jacobian matrix of subregion i

G system topology

L Laplacian matrix associated with system topology G

V the set of subregions

E the set of communication lines among subregions

Ω_i the set of neighboring subregions of subregion i

$\bar{P}^{tot}$ integrated energy system

$\hat{x}^i$ estimated state of the subregion i

$\tilde{x}^i$ local predicted state of the subregion i

$\tilde{z}^i$ local predicted measurement of the subregion i

$\hat{z}^i$ local estimated measurement of the subregion i

K^i Kalman gain

ε consensus gain

N^T the set of attack-free neighbor regions

N^F the set of neighbor regions under hybrid attacks

T diagonal matrix

φ status to describe whether FDIAs are successfully launched or not

μ status to describe whether DoSs are successfully launched or not

$\bar{P}^{tot}$ total power output of power grid

$\bar{P}^{TG}$ power output of thermal power unit

$\bar{P}^{CG}$ power output of clean power unit

S^T the set of generator working hours

S^{TG} the ste of thermal power unit

S^{CG} the ste of clean power unit

$\bar{E}$ carbon emissions

$\hat{e}$ estimation error

$\tilde{e}$ prediction error

$\check{P}$ error covariance

f_k attack detection function

τ detection threshold

η_k status to describe whether hybrid attacks are successfully detected or not

V_m node voltage amplitude

P_m node active injection power

Q_m node reactive injection power

P_{mn} branch active power flow

Q_{mn} branch reactive power flow

these problems, several research works have been reported. For example, a consensus nonconvex optimization protocol based on distributed state estimation was proposed to guarantee the consensus of estimated states under s-sparse attack [21]. When the measurement data is tampered by false data injection attacks (FDIAs), a mean square error based on distributed dynamic state estimation was employed to detect FDIAs to improve the security of state estimation [22]. An interactive Kalman filter to control data interaction between the nodes was proposed to improve the effectiveness of distributed state estimation under FDIAs [23]. A robust distributed state estimation based on iterative weighted least squares and improved alternating direction method of multipliers (ADMM) was proposed to handle the influence of FDIAs [24]. A blockchain based on distributed dynamic state estimation was proposed to improve the security under FDIAs [25]. A distributed estimation method based on ADMM was proposed to improve the effectiveness of state estimation under FDIAs [26]. Furthermore, some attack detection and defense methods based on state estimation have been summarized in [27]. However, the aforementioned studies primarily focus on the effectiveness and security of

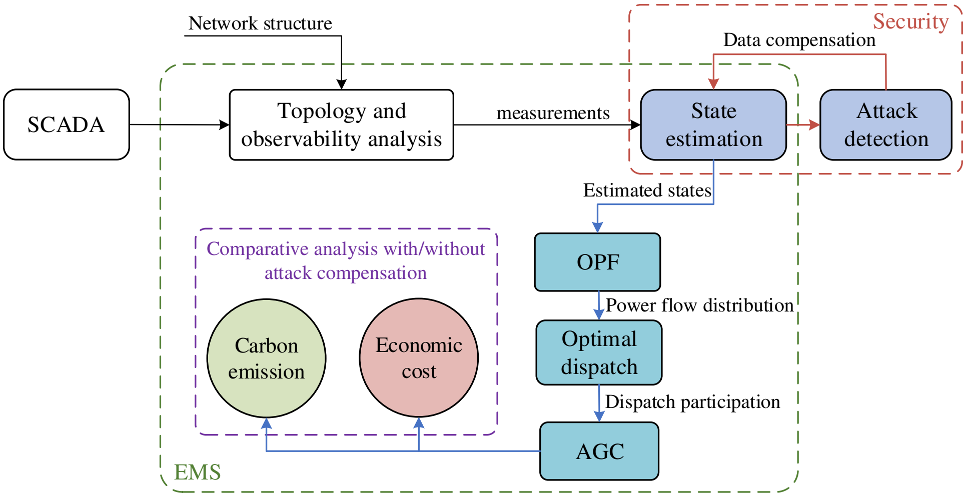


Figure 1: Overall functional structure diagram of CPPSs.

distributed state estimation under single type of attacks, and the impact of attack on carbon emissions and economic cost based on state estimation is not investigated deeply.

Generally, carbon emissions depend on the results of state estimation and optimal dispatch strategy, which is shown in Fig.1. First, the collected measurements from supervisory control and data acquisition system are transmitted to energy management system (EMS) through communication network. Second, these measurements are used for state estimation to obtain accurate state data, which are further used for power flow calculation to obtain optimal dispatch strategy for automatic generation control (AGC). Finally, the output of thermal power units is scheduled by AGC, which affects carbon emissions. Therefore, it is clear that distributed security state estimation is the cornerstone (i.e., there exist the close connection between distributed security state estimation and power system dispatch), and its corrupted results caused by cyber attacks will further affect the security and economy of CPPSs. At present, several research works have focused on the impact of cyber attacks on the security and economy of CPPSs. For security analysis, due to high coupling between cyber layer and physical layer in CPPSs, a failure caused by cyber attacks may cascade down to a dependent node [28], eventually leading to the collapse of the entire system [29]. The attacker performs unnecessary generation operations and load dumping by injecting false data [30] to make the control response of CPPSs improperly, resulting in unsafe situations. The false measurements injected by the attacker may mislead the secondary voltage controller into setting incorrect values, thereby damaging the stability and security of the entire system [31]. The impact of cyber attacks on frequency control of CPPSs has been analyzed, and it has also been revealed how frequency-based attacks can lead to widespread power outages [32]. For economy analysis, economic benefits are main target of the attacker. The attacker can modify price data in CPPSs, or directly modify their own smart meter readings to complete energy theft, and ultimately obtain illegal gains [33, 34]. Moreover, cyber attacks may change grid topology and even generation plans, which eventually have a significant impact on grid operational cost. For example, a load redistribution attack has been utilized to trip off a critical lines or breakers by misleading the control centre, which brings huge economic losses [35]. However, cyber attacks can lead to the incorrect state estimation results, which are used for power flow calculation and produce subsequent optimization dispatch strategy to affect carbon emissions and economic cost. Therefore, the impact of cyber attacks on carbon emissions and economic cost needs to be further investigated.

With respect to carbon emission analysis, a number of studies are reported in the literature. For example, the causal effect of coal substitution policy on air pollution emissions was analyzed [36]. A production model was developed to quantify carbon reduction potential of renewable energy substitutes for fossil energy [37]. An integrated energy system (IES) model was proposed [38], and carbon emissions from different IES energy chains were analyzed by life cycle assessment. Furthermore, the relationship between carbon emissions and energy demand was evaluated from life cycle perspective [39]. However, no researches have been reported in the literature on the impact of cyber-attacks on carbon emissions.

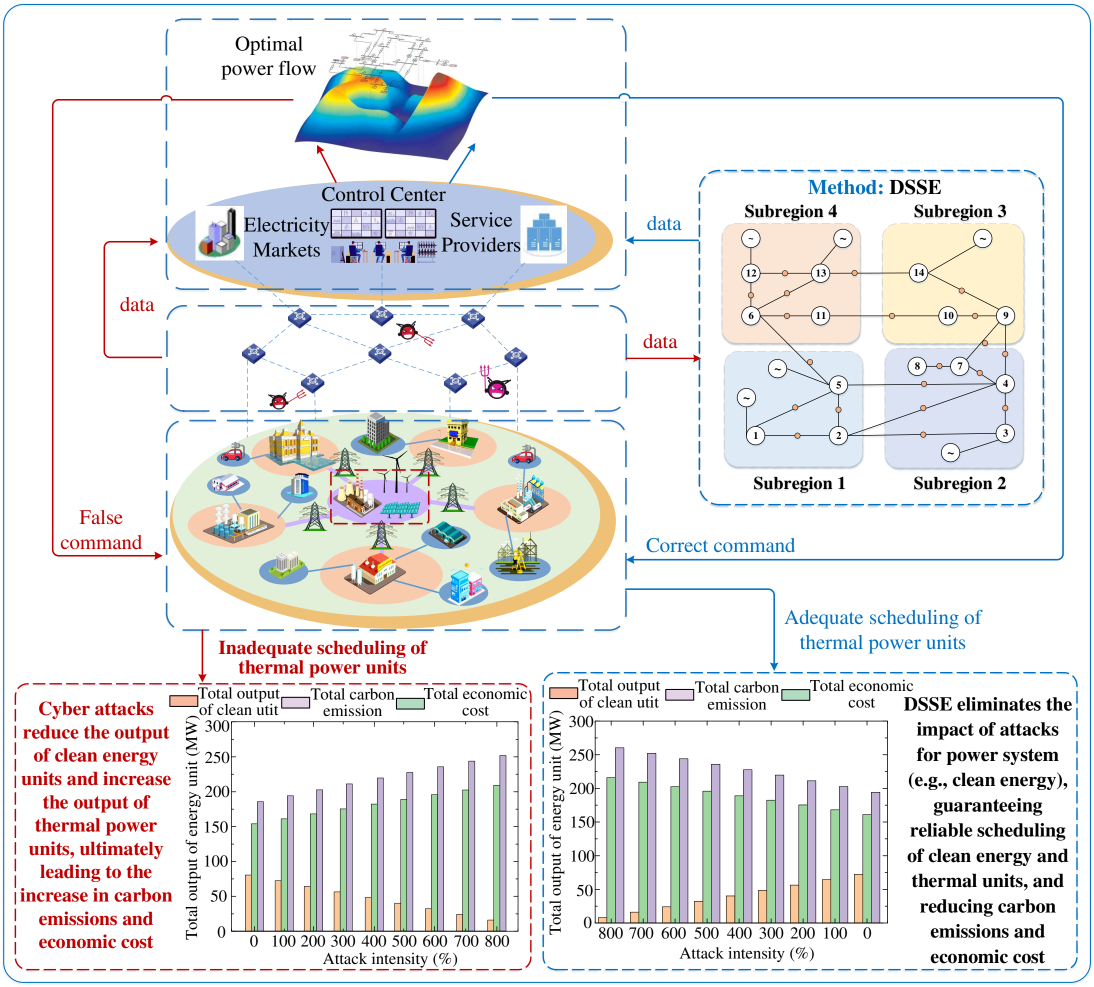

Optimal power flow
Control Center
Electricity Markets
Service Providers
data
data
data
False command
Correct command
Method: DSSE
Subregion 4
Subregion 3
Subregion 1
Subregion 2
12
13
14
6
11
10
9
8
7
5
4
1
2
3
Inadequate scheduling of thermal power units
Adequate scheduling of thermal power units
Cyber attacks reduce the output of clean energy units and increase the output of thermal power units, ultimately leading to the increase in carbon emissions and economic cost
Total output of clean utit
Total carbon emission
Total economic cost
Total output of energy unit (MW)
300
250
200
150
100
50
0
0 100 200 300 400 500 600 700 800
Attack intensity (%)
Total output of clean utit
Total carbon emission
Total economic cost
Total output of energy unit (MW)
300
250
200
150
100
50
0
800 700 600 500 400 300 200 100 0
Attack intensity (%)
DSSE eliminates the impact of attacks for power system (e.g., clean energy), guaranteeing reliable scheduling of clean energy and thermal units, and reducing carbon emissions and economic cost

Figure 2: Overall schematic of carbon emissions analysis of CPPSs under hybrid attacks assisted with distributed security state estimation.

Motivated by the above observations, as shown in Fig.2, this paper investigates carbon emissions and economic cost analysis of CPPSs under hybrid attacks based on distributed security state estimation. Specifically, the following questions and challenges are addressed

- How to describe the data incompleteness and non-authenticity caused by hybrid attacks and analyse the impact of hybrid attacks on state estimation? How to develop the corresponding attack detection and compensation mechanism?
- How to design distributed security state estimation method based on the reconstructed distributed estimation model to ensure the data security of CPPSs? How to analyze the convergence of the proposed method?
- How to analyze the connection between distributed security state estimation and the power system dispatch? How to assess the impact of hybrid attacks on carbon emissions and economic cost based on the proposed distributed security state estimation?

To answer these questions, this paper proposes a novel consensus-based DSSE method and further analyzes how hybrid attacks affect carbon emissions and economic cost by using the proposed method. The main contributions of this paper are summarized as follows:

- The data incompleteness and non-authenticity casued by hybrid attacks are described firstly, and their influence on the consensus based on distributed state estimator is analyzed. Considering the measurement and neighborhood data exchange, a new residual-based attack detection method is constructed for each subregion, where secure and non-secure sets are defined to describe whether a subregion is attacked. Furthermore, a Kalman prediction-based compensation mechanism is designed for non-secure set.

- According to the principle of minimum error covariance, a distributed security state estimation method is proposed to guarantee the security operation of CPPSs and provide data support for power flow calculation, and sufficient condition of its convergence is derived, requiring that the difference between the maximum eigenvalues of the matrix M (i.e., which is composed of Laplace matrix of secure and non-secure set topologies and system matrix) and the matrix N (i.e., which is composed of gain matrix, Jacobian matrix and system matrix) is less than 1, i.e., $\rho(\Gamma_{k|k}) < 1$.

- The results of distributed security state estimation are used for power flow calculation and produce subsequent optimization dispatch strategy to affect carbon emissions and economic cost, which reveals that there exist the close connection between distributed security state estimation and power system dispatch. On this basis, the impact of hybrid attacks on carbon emissions and economic cost are analyzed, and it is revealed that the total carbon emission and economic cost can be optimally controlled by relieving the impact of cyber attacks on state estimation. Finally, the impact of different attack intensities on the carbon emissions and economic cost are also analyzed.

The rest of this paper is organized as follows. Section II describes the problems of security, the exchanged state data description under hybrid attacks and carbon emissions in CPPSs. Section III analyses the impact of hybrid attacks on the distributed state estimation and designs an attack detection and attack compensation mechanism. Section IV presents a consensus-based distributed security state estimation method under hybrid attacks and their impact on carbon emissions and economic cost is analyzed. Experimental results are discussed in Section V, followed by the conclusion in Section VI.

2. Problem statement

2.1. *Problem of security in CPPSs*

CPPSs are usually composed of several interconnected subsystems located in different subregions, where state estimation is conducted for each subregion, forming distributed state estimation. For example, Fig.3 shows IEEE-14 bus system, which is divided into 4 different subregions. The measurement data of each subregion is transmitted to the corresponding local state estimator through a communication network. Each state estimator is connected with its neighbor state estimators, and sends the state estimation results to the neighboring state estimators to achieve distributed state estimation.

However, when the data is transmitted via communication network, it may be subject to cyber attacks such as FDIAs and DoSs. As shown in Fig.3, according to the specific attack location, it can be divided into the following two types: 1) attacking the communication between the subregion j and the corresponding local state estimator j (called attack Type 1), and 2) attacking the communication between state estimator j and state estimator i (called attack Type 2).

Generally, the attacker can launch not only single attack Type 1 or Type 2 but also attack Types 1 and 2 simultaneously. Thus, there are five attack statuses for FDIAs and DoSs as follows: 1) the attacker only launches FDIAs, 2) the attacker only launches DoSs, 3) the attacker launches DoSs firstly and then FDIAs, 4) the attacker launches FDIAs firstly and then DoSs, 5) the attacker launches FDIAs and DoSs simultaneously. This leads to 25 attack scenarios.

For the above 25 scenarios, it is analyzed by the following two steps from the communication prospective:

1) *Step 1*: When attack Type 1 occurs, there are five attack statuses. First, the attacker only launches a single type of attack. When attack Status 1 occurs (i.e., only FDIAs), the data from subregion j to the corresponding local state estimator j is tampered, i.e., the state estimator j receives false data. When attack Status 2 occurs (i.e., only DoSs), the data from subregion j to the corresponding local state estimator j is blocked, i.e., the state estimator j does not receive the data. Second, the attacker launches FDIAs and DoSs in chronological order. When attack Status 3 occurs, the previous DoSs cause data losses of the attacked node, while subsequent FDIAs

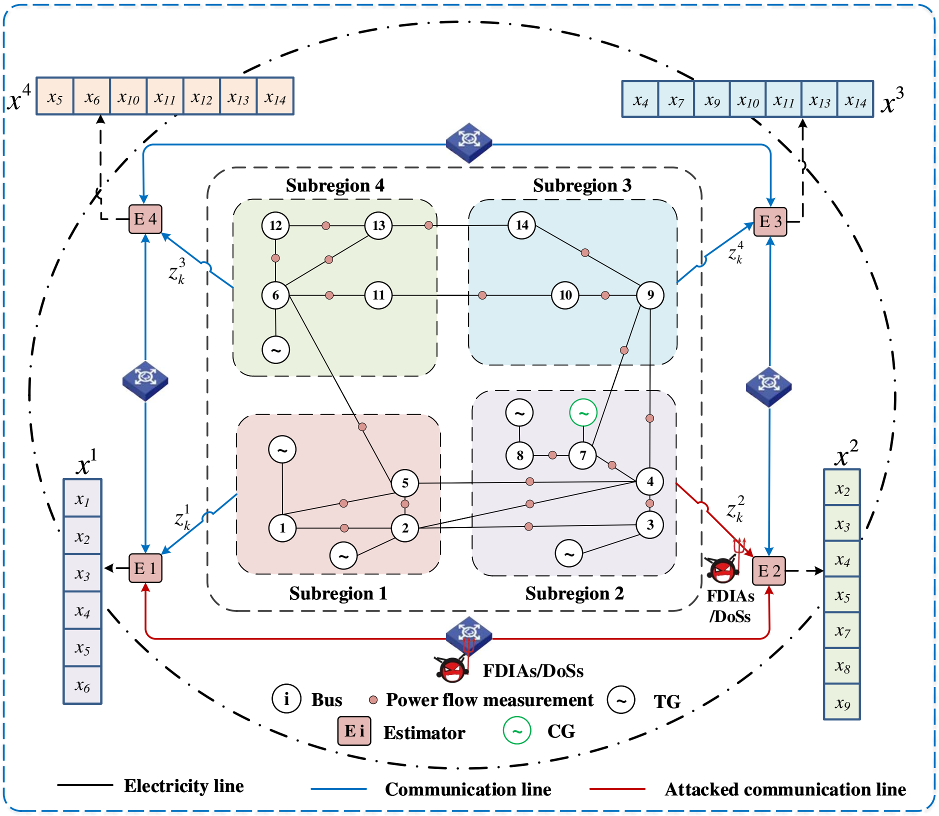

x^4
x_5 x_6 x_{10} x_{11} x_{12} x_{13} x_{14}
x_4 x_7 x_9 x_{10} x_{11} x_{13} x_{14}
x^3
Subregion 4
Subregion 3
Subregion 1
Subregion 2
E 4
E 3
E 1
E 2
z_k^3
z_k^4
z_k^1
z_k^2
x^1
x_1 x_2 x_3 x_4 x_5 x_6
x^2
x_2 x_3 x_4 x_5 x_7 x_8 x_9
FDIAs /DoSs
FDIAs/DoSs
i Bus
Power flow measurement
~ TG
Ei Estimator
~ CG
Electricity line
Communication line
Attacked communication line

Figure 3: Decomposition of IEEE 14-bus system and data interaction process of each subregion under hybrid attacks.

may tamper with the data of the normal node or fill the lost data of the attacked node with the tampered data, i.e., the state estimator j receives false data, so attack Status 3 is equivalent to attack Status 1. When attack Status 4 occurs, the previous FDIAs tamper with the data of the attacked node, while subsequent DoSs may block data transmission of the normal node, or it may block data transmission of the attacked node, i.e., the state estimator j does not receive the data, so attack Status 4 is equivalent to attack Status 2. Third, the attacker launches FDIAs and DoSs simultaneously, i.e., attack Status 5 occurs. However, for the same communication line, it is infeasible that FDIAs and DoSs are launched simultaneously. Thus, attack Status 5 is invalid. Finally, as shown in Fig.4, the above five attack statuses can be further summarized into two statuses (i.e., attack Status 1 and attack Status 2), and it leads to two consequences, i.e., false data (called Case 1) or data losses (called Case 2) for subregion j.

2) *Step 2*: Since attack Type 1 produces two consequences after the nodes being attacked (i.e., Case 1 and Case 2), attack Type 2 needs to analyze the above two consequences separately. First, according to Case 1 (i.e., subregion j with false data), when attack Type 2 occurs, attack Status 1 continues, e.g., the data from state estimator j to state estimator i is tampered, i.e., the state estimator i receives false data. Attack Status 2 blocks the false data from state estimator j to state estimator i, i.e., the state estimator i does not receive the data, which indicates that when attack Status 2 occurs in Type 2, the attack impacts in Type 1 do not need to be considered. Second, according to Case 2 (i.e., subregion j with data losses), the false data caused by attack Status 1 may be just added to the node with data losses in subregion j, or the data of other normal nodes in subregion j may be tampered. The data losses caused by attack Status 2 may be the same as the node whose data is lost in subregion j, or the data of other normal nodes in subregion j may be lost. Finally, as shown in Fig.4, the above two cases also lead to two consequences, i.e., false data (called Case 3) or data losses (called Case 4) for subregion i (An example is given to better illustrate the whole attack process in the Appendix A).

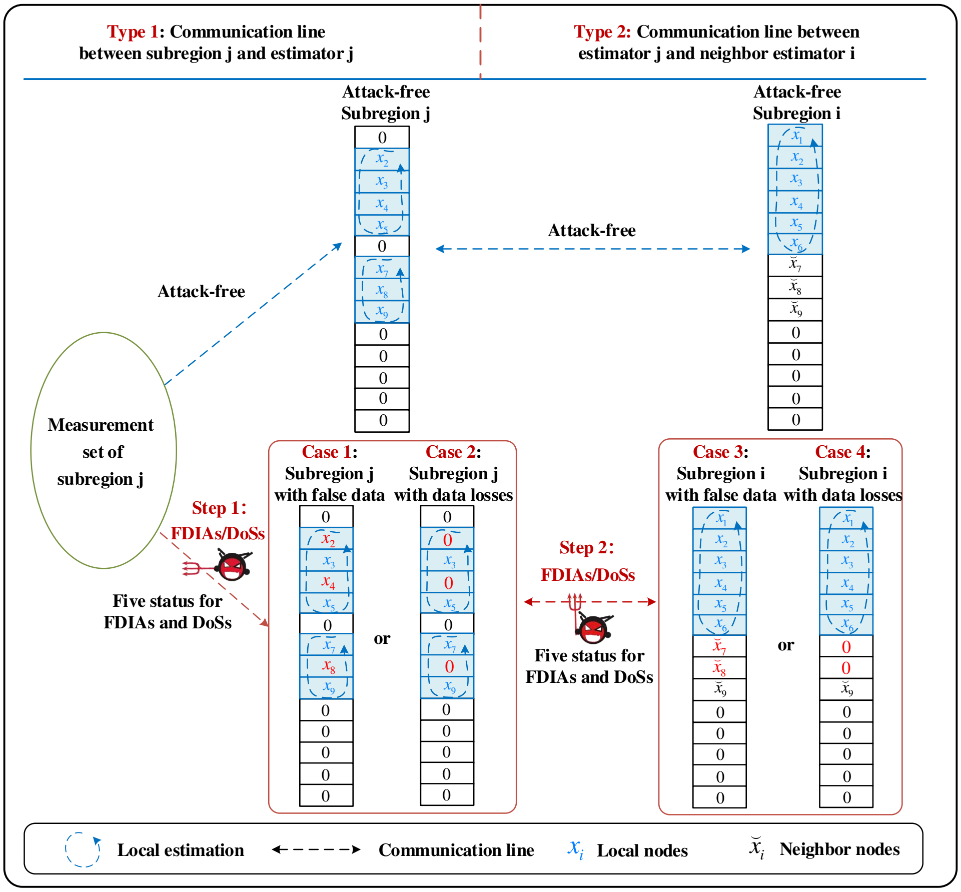

Type 1: Communication line between subregion j and estimator j
Type 2: Communication line between estimator j and neighbor estimator i
Attack-free Subregion j
Attack-free Subregion i
Attack-free
Attack-free
Measurement set of subregion j
Step 1: FDIAs/DoSs
Five status for FDIAs and DoSs
Case 1: Subregion j with false data
Case 2: Subregion j with data losses
or
Step 2: FDIAs/DoSs
Five status for FDIAs and DoSs
Case 3: Subregion i with false data
Case 4: Subregion i with data losses
or
Local estimation
Communication line
Local nodes
Neighbor nodes

Figure 4: Analysis of five attack statuses of hybrid attacks on two communication lines. Five attack statuses of hybrid attacks include: 1) The attacker only launches FDIAs; 2) The attacker only launches DoSs; 3) The attacker launches DoSs firstly and then FDIAs; 4) The attacker launches FDIAs firstly and then DoSs, 5) The attacker launches FDIAs and DoSs simultaneously.

Remark 1: It can be concluded from Steps 1 and 2 that when attack Type 2 is caused by attack Status 2, the attack impacts of attack Type 1 do not need to be considered, i.e., subregion i cannot receive any data from subregion j. When Type 2 is caused by Status 1, the attack impacts on Type 1 cannot be ignored, i.e., subregion i receives false data from subregion j.

2.2. *The exchanged state data description under hybrid attacks*

The above focuses on the analysis of hybrid attacks on the distributed state estimation process of multi-region CPPSs. In the following, the CPPSs model and the distributed state estimator model without hybrid attacks are presented, and then the exchanged state data description under hybrid attacks is provided to describe the above attack process. Consider the following model of CPPSs [40]

$$\begin{aligned} x_{k+1} &= Ax_k + \omega_k \\ z_k &= Hx_k + \upsilon_k \end{aligned} \tag{1}$$

where x_k and z_k are system state and measurement at the sampling instant k, A is state transition matrix and H is Jacobian matrix, ω_k and υ_k represent two independent process and measurement white noises respectively, and $E[\omega_k \omega_k^T] = Q$, $E[\upsilon_k \upsilon_k^T] = R$.

Since CPPSs are comprised of different subregions, distributed state estimation for each region can be employed to improve system resilience [41]. As shown in Fig.3, i.e., IEEE-14 bus system is divided into 4 different subregions, where communication line is used to indicate whether these subsystems can exchange the data. According to subregion structure, an undirected graph $G = (V, E)$ is applied to describe system topology [42], where $V = \{1, 2, \dots, M\}$ and $E = \{1, 2, \dots, M\}$ represent the set of subregions and communication lines among different subregions, respectively. If subregion j can transmit the data to subregion i, then the corresponding edge can be denoted by $(i, j) \in E$. Therefore, the set of neighboring regions of i is defined as $\Omega_i = \{j \in V | (i, j) \in E\}$, and its dimension is defined as $d = |\Omega_i|$. Furthermore, each subregion contains multiple nodes, these nodes may be power generation units, loads, etc. It should be noted that the lines between the nodes are power transmission lines, which is different from communication lines in different subregions. Finally, to represent the topological relationship between the subregions, the Laplacian matrix associated with the graph G is denoted as $L = (l_{ij})$, i.e.,

$$l_{ij} = \begin{cases} -1, & if\ (i,j) \in E\ \&\ i \neq j \\ -\sum_{j \in \Omega_i} l_{ij}, & if\ i = j \\ 0, & otherwise \end{cases} \tag{2}$$

According to CPPSs partition, system state and measurement of the whole system in (1) can be divided into subsystem state and measurement of multiple subregions, i.e., subsystem state and measurement of subregion are a subset of the whole system state and measurement. Thus, subsystem state and measurement of subregion i can be described as

$$\begin{aligned} x^i_{k+1} &= A^i x^i_k + \omega^i_k \\ z^i_k &= H^i x^i_k + v^i_k \end{aligned} \tag{3}$$

where x^i_k and z^i_k are subsystem state and measurement of subrigion i at the sampling instant k, respectively, A^i is state transition matrix of subregion i, H^i is the Jacobian matrix of subregion i.

According to the above distributed model in (3), distributed local state estimator is developed for each subregion. Using measurement z^i_k to run local estimation, state estimators in different subregions can achieve the data exchange through the consensus. The corresponding local state estimator i [43, 44] of subregion i is expressed as

$$\hat{x}^i_{k+1|k+1} = \tilde{x}^i_{k+1|k} + K^i_{k+1}[z^i_{k+1} - \tilde{z}^i_{k+1|k}] - \varepsilon A \sum_{j \in N_i} [\hat{x}^i_{k|k} - \hat{x}^j_{k|k}] \tag{4}$$

where $\hat{x}^i_{k+1|k+1}$ is the estimated state of subregion i, $\tilde{x}^i_{k+1|k}$ and $\tilde{z}^i_{k+1|k}$ are local predicted state and output of subregion i, and K^i_{k+1} is Kalman gain of the estimator. ε is consensus gain of the estimator i, and the range of ε is $(0.1/\Delta)$ with $\Delta = \max_i d_i$.

For distributed state estimator i in (4), it can be seen that $\hat{x}^j_{k|k}$ is the state data from the neighboring subregion j, and hybrid attacks make the state data transmitted incomplete and/or authentic. Therefore, according to the state data $\hat{x}^j_{k|k}$ of neighboring subregion j and two steps of attack process, the exchanged state data under hybrid attacks is described as (The specific exchanged state data description under hybrid attacks is given in the Appendix B)

$$\hat{x}^{j,*}_{t2,k|k} = (1 - \mu^2_k) T^2_k \{(1 - \mu^1_k)[\varphi_k (T^1_k \hat{x}^j_{k|k}) + (1 - \varphi_k) \hat{x}^j_{k|k}]\} \tag{5}$$

where $t2$ represents attack Type 2, $T^1_k = T^2_k = diag(\gamma_1, \gamma_2, \cdots, \gamma_n)$, $\gamma_i = d$ represents the i^{th} attacked communication channel, $d \in \mathbf{R}$ represents attack intensity, φ_k is a random variable with value of 0 or 1 (i.e., $\varphi_k = 1$ represents that FDIAs are successfully launched, $\varphi_k = 0$ otherwise). μ^1_k is a random variable with value of 0 or 1 (i.e., $\mu^1_k = 1$ represents that DoSs are successfully launched, $\mu^1_k = 0$ otherwise), and μ^2_k is same as μ^1_k.

Remark 2: The cunning attacker can launch many types of cyber attacks (e.g., FDIAs, DoSs etc.), but the mechanisms of these cyber attacks are different and difficult to be described by a universal formula. This paper focuses on two popular cyber attacks (i.e., FDIAs and DoSs) for CPPSs [45], because they destroy data integrity and authenticity. These two types of cyber attacks are described by a uniform formula (i.e., Eq.(5)).

Remark 3: The Eq.(5) aims to prevent secure subregion i from receiving the data of non-secure subregion j (i.e., due to the data incompleteness or the data non-authenticity). Note that the incomplete and non-authentic state $\hat{x}^{j,*}_{t2,k|k}$

of the attacked subregion j may be propagated to its neighboring subregions through the consensus term in (4), thus producing faulty distributed state estimation.

According to the above model of CPPSs under hybrid attacks, how to reveal the influence of hybrid attacks on distributed state estimation from the perspective of defender is a key issue to be addressed. To solve this problem, the influence of hybrid attacks on the consensus term in the state estimator model (3) will be analyzed in subsection 3.1, which reveals the process of hybrid attacks corrupting distributed state estimation. Moreover, when the incorrect state estimation results caused by hybrid attacks are used for OPF [46, 47], the wrong optimal dispatch strategy is obtained for AGC to schedule the output of thermal power units, which ultimately affects carbon emissions. To achieve low-carbon emissions in CPPSs, clean energy generators (CGs) should be fully used, while the output of thermal power generators (TGs) should be reduced [48, 49].

2.3. *Problem of carbon emissions in CPPSs*

For the distributed state estimator i in (4), false data or data loss will affect the results of state estimation. If these results are used in OPF analysis, it will inevitably lead to inadequate scheduling of the generation outputs from clean energy units and thermal power units and eventually affect carbon emissions of power system. To quantitatively analyze the impact of hybrid attacks on carbon emissions, the total power output of power grid at the sampling instant k without attacks is defined as $\bar{P}_k^{tot}$. It is composed of TGs and CGs, i.e.,

$$\bar{P}_k^{tot} = \bar{P}_{m,k}^{TG} + \bar{P}_{n,k}^{CG} \tag{6}$$

where $\bar{P}_{m,k}^{TG}$ represents power generation of thermal power unit m at the sampling instant k, $\bar{P}_{n,k}^{CG}$ represents power generation of clean power unit n at the sampling instant k. Further, the following conditions need to be met, i.e.,

$$\bar{P}_{m,k}^{TG,\min} \leq \bar{P}_{m,k}^{TG} \leq \bar{P}_{m,k}^{TG,\max}, k \in S^T, m \in S^{TG}$$

$$\bar{P}_{n,k}^{CG,\min} \leq \bar{P}_{n,k}^{CG} \leq \bar{P}_{n,k}^{CG,\max}, k \in S^T, n \in S^{CG}$$

where S^T represents the set of generator working hours k, S^{TG} represents the set of thermal power units, and S^{CG} represents the set of clean energy units.

Since carbon emissions of clean energy is negligible, carbon emissions mainly come from TGs. Carbon emission generated by TG m can be calculated by [50]

$$\bar{E}_m(\bar{P}_{m,k}^{TG}) = CF_m(a_m + b_m\bar{P}_{m,k}^{TG} + c_m(\bar{P}_{m,k}^{TG})^2) \tag{7}$$

Then, the total carbon emissions are

$$\bar{E} = \sum_{m\in S^{TG}} \sum_{k\in S^T} E_m\{\bar{P}_{m,k}^{TG}\} \tag{8}$$

To achieve the minimum carbon emission, i.e., it can be transformed into the following optimization problem

$$\min \bar{E} = \sum_{m\in S^{TG}} \sum_{k\in S^T} \bar{E}_m\{\bar{P}_{m,k}^{TG}\}$$

$s.t.$

$$\bar{P}_k = \bar{P}_{m,k}^{TG} + \bar{P}_{n,k}^{CG}$$

$$\bar{P}_{m,k}^{TG,\min} \leq \bar{P}_{m,k}^{TG} \leq \bar{P}_{m,k}^{TG,\max}, k \in S^T, m \in S^{TG}$$

$$\bar{P}_{n,k}^{CG,\min} \leq \bar{P}_{n,k}^{CG} \leq \bar{P}_{n,k}^{CG,\max}, k \in S^T, m \in S^{TG}$$

Remark 4: It is evident from the above analysis that carbon emissions of CPPSs are affected by the output of thermal power units, and the output of thermal power units is affected by the total load, and the outputs of both clean energy units and thermal power units. Hybrid attacks can tamper with the measurement in any node of any subregion, and then affect OPF analysis which is reliant on reliable measurements of power system states, and eventually affect carbon emissions. Therefore, it is necessary to quantitatively investigate how hybrid attacks affect state estimation and thus carbon emissions of thermal power units.

3. Analysis of distributed state estimation and detection mechanism under hybrid attacks

Aiming at addressing the problem raised in the previous section, this section first analyzes how hybrid attacks affect distributed state estimation and then proposes an attack detection method, and finally data compensation mechanism is designed to reconstruct the state estimation model.

3.1. *Distributed state estimation under hybrid attacks*

Since OPF will use state estimation results, it is necessary to analyze the impact of hybrid attacks on distributed state estimation. State prediction $\tilde{x}^i_{k+1|k}$ and measurement prediction $\tilde{z}^i_{k+1|k}$ are defined as

$$\tilde{x}^i_{k+1|k} = A\hat{x}^i_{k|k} \tag{9}$$

$$\tilde{z}^i_{k+1|k} = H^i\tilde{x}^i_{k+1|k} \tag{10}$$

Then, prediction error $\tilde{e}^i_{k+1|k} = x_{k+1} - \tilde{x}^i_{k+1|k}$ and its covariance $\breve{P}^i_{k+1|k}$ are expressed as

$$\tilde{e}^i_{k+1|k} = A\hat{e}^i_{k|k} + \omega_k \tag{11}$$

$$\breve{P}^i_{k+1|k} = E[\tilde{e}^i_{k+1|k}\tilde{e}^{iT}_{k+1|k}] = A\breve{P}^i_{k|k}A^T + Q \tag{12}$$

Furthermore, the attack-free estimation error $\hat{e}^i_{k+1|k+1} = x_{k+1} - \hat{x}^i_{k+1|k+1}$ can be obtained by

$$\hat{e}^i_{k+1|k+1} = F^i_{k+1}A\hat{e}^i_{k|k} + F^i_{k+1}\omega_k - K^i_{k+1}v^i_{k+1} - \varepsilon A\sum_{j\in N_i}[\hat{e}^i_{k|k} - \hat{e}^j_{k|k}] \tag{13}$$

where $F^i_{k+1} = I - K^i_{k+1}H^i$.

According to hybrid attacks analysis in Remark 1, attack Status 1 or 2 on attack Type 2 determine the state data received by subregion i from subregion j.

When attack Type 2 caused by attack Status 2, i.e., $\mu^2_k = 1$, then subregion i does not receive any data form subregion j at this sampling instant k. Thus, substituting (5) into (4), it follows that

$$\hat{x}^i_{k+1|k+1} = \tilde{x}^i_{k+1|k} + K^i_{k+1}[z^i_{k+1} - \tilde{z}^i_{k+1|k}] - \varepsilon A\sum_{j\in N^T_i}[\hat{x}^i_{k|k} - \hat{x}^j_{k|k}] - \varepsilon A\sum_{j\in N^F_i}[\hat{x}^i_{k|k}] \tag{14}$$

where N^T_i represents the set of attack-free neighbor subregions (called secure set), N^F_i represents the set of neighbor subregions under hybrid attacks (called non-secure set).

Remark 5: When different subregions in CPPSs are exposed to hybrid attacks, secure and non-secure sets can describe whether different subregions are attacked or not. It is obvious from last term of (14) that due to the loss of data in non-secure set caused by Status 2 (i.e., DoSs), subregion i cannot receive the data of subregion j in a consensus way, which indicates that the consensus term in (4) is violated.

When Type 2 caused by Status 1, i.e., $\mu^2_k = 0$. At this time, if Type 1 caused by Status 1, i.e., $\mu^1_k = 0$ and $\varphi_k = 1$. Then subregion i will receive false data form subregion j. Thus, substituting (5) into (4), it follows that

$$\hat{x}^i_{k+1|k+1} = \tilde{x}^i_{k+1|k} + K^i_{k+1}[z^i_{k+1} - \tilde{z}^i_{k+1|k}] - \varepsilon A\sum_{j\in N^T_i}[\hat{x}^i_{k|k} - \hat{x}^j_{k|k}] - \varepsilon A\sum_{j\in N^F_i}[\hat{x}^i_{k|k} - T_k\hat{x}^j_{k|k}] \tag{15}$$

where $T_k = T^2_kT^1_k$.

If Type 1 caused by Status 2, i.e., $\mu^1_k = 1$ and $\varphi_k = 0$. Then subregion i will receive false data form subregion j. Thus, substituting (5) into (4), it follows that

$$\hat{x}^i_{k+1|k+1} = \tilde{x}^i_{k+1|k} + K^i_{k+1}[z^i_{k+1} - \tilde{z}^i_{k+1|k}] - \varepsilon A\sum_{j\in N^T_i}[\hat{x}^i_{k|k} - \hat{x}^j_{k|k}] - \varepsilon A\sum_{j\in N^F_i}[\hat{x}^i_{k|k} - T^2_k\hat{x}^j_{k|k}]$$

Then, the estimation error of the above two cases can be obtained

$$\hat{e}^i_{k+1|k+1} = F^i_{k+1} A \hat{e}^i_{k|k} + F^i_{k+1} \omega_k - K^i_{k+1} \upsilon^i_{k+1} - \varepsilon A \sum_{j \in N_i^T} [\hat{e}^i_{k|k} - \hat{e}^j_{k|k}] - \varepsilon A \sum_{j \in N_i^F} [\hat{e}^i_{k|k} - T_k \hat{e}^j_{k|k}] \tag{16}$$

$$\hat{e}^i_{k+1|k+1} = F^i_{k+1} A \hat{e}^i_{k|k} + F^i_{k+1} \omega_k - K^i_{k+1} \upsilon^i_{k+1} - \varepsilon A \sum_{j \in N_i^T} [\hat{e}^i_{k|k} - \hat{e}^j_{k|k}] - \varepsilon A \sum_{j \in N_i^F} [\hat{e}^i_{k|k} - T_k^2 \hat{e}^j_{k|k}] \tag{17}$$

Remark 6: Comparing (16), (17) and (13), it is evident that the extra term $\varepsilon A \sum_{j \in N_i^F} [\hat{e}^i_{k|k} - T_k \hat{e}^j_{k|k}]$ and $\varepsilon A \sum_{j \in N_i^F} [\hat{e}^i_{k|k} - T_k^2 \hat{e}^j_{k|k}]$ in (16) and (17) reflect the impacts affected by attacks, which increases with each iteration because of the presence of T_k and T_k^2. It indicates that the difference always exists among the exchanged data and the consensus process cannot converge, which leads to the failure of the distributed state estimation.

3.2. *Attack detection mechanism*

After analyzing the impact of hybrid attacks on distributed state estimation, distributed attack detection method is designed to detect hybrid attacks for each subregion while performing state estimation.

Using statistical information received, some attack detection methods have been proposed [51, 52, 53]. However, the received data of subregion i is state estimation $\hat{x}^j_{k|k}$ of its neighbors j in CPPSs, so, subregion i needs to detect whether subregion j is safe during their data exchange, i.e., whether the received data from subregion j can be directly used for the consensus. Therefore, inspired by the work in [54], the detection function is formulated as

$$f^i_k = (z^i_k - H^i \hat{x}^{j*}_{k|k}) R^{-1} (z^i_k - H^i \hat{x}^{j*}_{k|k})^T \tag{18}$$

where f^i_k is the detection function of subregion i, $\hat{x}^{j*}_{k|k}$ is the data transmitted from subregion j to i. Then, the attack is detected by judging f^i_k and the threshold τ^i, and the detection mechanism is expressed as

$$\eta^i_k = \begin{cases} 0, & if\ f^i_k > \tau^i \\ 1, & \text{otherwise} \end{cases} \tag{19}$$

where $\eta^i_k = 0$ means that an alarm is triggered, and the choice of the threshold τ^i depends on 3σ criterion in engineering applications [55]. However, note that the proposed detection method is not always effective for other cyber attack detection, because their mechanisms are different.

Remark 7: FDIAs destroy data authenticity by injecting false data, which have various types (e.g., scaling attacks, stealth FDIAs, etc.) [56]. Stealth FDIAs are usually well-designed to bypass traditional residual testing (i.e., BDD detection) [57], but some detection methods (e.g., a detection method based on interval observer and logic localization judgment matrix [58]) have been proposed. This paper considers another form of FDIAs (i.e., scaling attack), and the corresponding distributed attack detection method (i.e., Eqs. (18) and (19)) is designed based on interaction data during the process of distributed state estimation. Therefore, for practical application, these attack detection methods can be combined into an integrated attack detector to improve the detection effectiveness for FDIAs.

When above attack detection mechanism is applied to each subregion, it is possible to determine whether a subregion belongs to secure set or non-secure set. For non-secure sets, it is necessary to design attack compensation mechanism to relieve the impact of hybrid attacks.

3.3. *Reconstruction of attack compensation-based distributed estimation model*

According to the above analysis of hybrid attacks on state estimation and attack detection method, when hybrid attacks are launched, then (4) can be further re-written as

$$\hat{x}^i_{k+1|k+1} = \tilde{x}^i_{k+1|k} + K^i_{k+1} [z^i_{k+1} - \tilde{z}^i_{k+1|k}] - \varepsilon A \sum_{j \in N_i^T} (1 - \eta^i_k) [\hat{x}^i_{k|k} - \hat{x}^j_{k|k}] - \varepsilon A \sum_{j \in N_i^F} \eta^i_k [\hat{x}^i_{k|k} - \hat{x}^{j,*}_{t2,k|k}] \tag{20}$$

When attack detection mechanism of the corresponding subregion in subsection 3.2 is triggered, the subregion is determined as non-secure. To reduce the impact of hybrid attacks on the state estimation of non-secure set, Kalman prediction-based attack compensation mechanism is employed, i.e., the attacked state is replaced by the predicted value of the latest received state, then (20) can be re-written as

$$\hat{x}^i_{k+1|k+1} = \tilde{x}^i_{k+1|k} + K^i_{k+1}[z^i_{k+1} - \tilde{z}^i_{k+1|k}] - \varepsilon A \sum_{j\in N_i^T} [\hat{x}^i_{k|k} - \hat{x}^j_{k|k}] - \varepsilon A \sum_{j\in N_i^F} [\hat{x}^i_{k|k} - \tilde{x}^j_{k|k-1}] \tag{21}$$

where $\tilde{x}^j_{k|k-1}$ is Kalman prediction value at sampling instant k using the measurements up to $k-1$. Thus, Eq. (26) is the reconstructed distributed estimation model based on attack compensation mechanism.

4. Consensus-based distributed security state estimation under hybrid attacks and carbon emissions analysis

In section 3, the impact of hybrid attacks on distributed state estimation is analyzed, and then attack detection mechanism is designed and distributed state estimation model is reconstructed. According to the reconstructed distributed state estimation mode, this section designs an appropriate DSSE method and provides sufficient condition for its convergence. Finally, the designed DSSE method is proposed to address the problem raised in subsection 2.3, i.e., how the impact of hybrid attacks on state estimation further affects the output and carbon emissions of thermal power units.

4.1. *Consensus-based distributed state estimation with attack compensation*

According to the reconstructed distributed estimation model in (21), the estimation error is expressed as

$$\hat{e}^i_{k+1|k+1} = F^i_{k+1}A\hat{e}^i_{k|k} + F^i_{k+1}\omega_k - K^i_{k+1}v^i_{k+1} - \varepsilon A \sum_{j\in N_i^T}[\hat{e}^i_{k|k} - \hat{e}^j_{k|k}] + \varepsilon A \sum_{j\in N_i^F} \omega_{k-1} - \varepsilon A \sum_{j\in N_i^F}[\hat{e}^i_{k|k} - A\hat{e}^j_{k-1|k-1}] \tag{22}$$

To make (22) clearer, r represents the neighbor region of subregion i, it follows that

$$\hat{e}^i_{k+1|k+1} = F^i_{k+1}A\hat{e}^i_{k|k} + F^i_{k+1}\omega_k - K^i_{k+1}v^i_{k+1} - \varepsilon A \sum_{r\in N_i^T}[\hat{e}^i_{k|k} - \hat{e}^r_{k|k}] + \varepsilon A \sum_{r\in N_i^F} [\omega_{k-1}] - \varepsilon A \sum_{r\in N_i^F}[\hat{e}^i_{k|k} - A\hat{e}^r_{k-1|k-1}] \tag{23}$$

If CPPSs are not attacked, state variation is stable and slow [59], i.e., x_k and $\hat{x}_{k|k}$ approach to x_{k-1} and $\hat{x}_{k-1|k-1}$, respectively. Therefore, $\hat{e}_{k-1|k-1}$ approaches to $\hat{e}_{k|k}$, (23) can be re-written as

$$\hat{e}^i_{k+1|k+1} = F^i_{k+1}A\hat{e}^i_{k|k} + F^i_{k+1}\omega_k - K^i_{k+1}v^i_{k+1} - \varepsilon A \sum_{r\in N_i^T}[\hat{e}^i_{k|k} - \hat{e}^r_{k|k}] + \varepsilon A \sum_{r\in N_i^F} [\omega_{k-1}] - \varepsilon A \sum_{j\in N_i^F}[\hat{e}^i_{k|k} - A\hat{e}^r_{k|k} - \Delta_k] \tag{24}$$

where Δ_k represents the subtle difference between $\hat{e}^i_{k|k}$ and $\hat{e}^i_{k-1|k-1}$.

Then, the estimation error covariance $\breve{P}^i_{k+1|k+1}$ is expressed as

$$\breve{P}^i_{k+1|k+1} = E[\hat{e}^i_{k+1|k+1}\hat{e}^{iT}_{k+1|k+1}] \tag{25}$$

Taking the partial derivative of the trace of (25), it follows that

$$\begin{aligned}\frac{\partial tr(\breve{P}^i_{k+1|k+1})}{\partial K^i_{k+1}} = & -2A\breve{P}^i_{k|k}A^T H^{iT} + 2K^i_{k+1}H^i A\breve{P}^i_{k|k}A^T H^{iT} - 2QH^{iT} + 2K^i_{k+1}H^i Q H^{iT} + 2K^i_{k+1}R^i_{k+1} \\ & -2\varepsilon A \sum_{r\in N_i^F} QH^{iT} - 2\varepsilon A \sum_{r\in N_i^T} (\breve{P}^i_{k|k} - \breve{P}^{r,i}_{k|k})A^T H^{iT} - 2\varepsilon A \sum_{r\in N_i^F} (\breve{P}^i_{k|k} - A\breve{P}^{r,i}_{k|k})A^T H^{iT}\end{aligned} \tag{26}$$

Making $\frac{\partial tr(\breve{P}^i_{k+1|k+1})}{\partial K^i_{k+1}} = 0$, the optimal gain K^i_{k+1} can be given by

$$\begin{aligned} K^i_{k+1} &= [A\breve{P}^i_{k|k}A^T H^{iT} + QH^{iT} + \varepsilon A \sum_{r\in N_i^F} QH^{iT} - \varepsilon A \sum_{r\in N_i^T} (\breve{P}^i_{k|k} - \breve{P}^{r,i}_{k|k})A^T H^{iT} - \varepsilon A \sum_{r\in N_i^F} (\breve{P}^i_{k|k} - A\breve{P}^{r,i}_{k|k})A^T H^{iT}] \\ &\quad (H^i A\breve{P}^i_{k|k}A^T H^{iT} + H^i Q H^{iT} + R^i_{k+1})^{-1} \end{aligned} \tag{27}$$

Finally, the above distributed state estimation algorithms can be summarized by Algorithm 1.

Algorithm 1 Distributed security state estimation algorithm under hybrid attacks

```
Require: the initial values $\tau^i$, $H^i$, $R$, $Q$, $\varepsilon$, $\hat{x}^i_{0|0}$, $\tilde{x}^i_{1|0}$, $\hat{x}^j_{0|0}$, $\breve{P}^i_{0|0}$, $\breve{P}^i_{1|0}$, $K^i_0$.
Ensure: estimation state $\hat{x}^i_{k+1|k+1}$.
for $k = 1$ to $T$ do
    Obtain values of $\tilde{x}^i_{k+1|k}$, $\tilde{z}^i_{k+1|k}$ by using Eqs. (9) and (10).
    Obtain value of $\tilde{e}^i_{k+1|k}$, $\breve{P}^i_{k+1|k}$ by using Eqs. (11) and (12).
    for $k = 1$ to $T$ do
        Construct detection function $f^i_k$ by using Eq. (18)
        if $f^i_k > \tau^i$ then
            Set $\eta^i_k = 0$
        end if
        Obtain $\hat{x}^i_{k+1|k+1}$ by using Eq. (21).
        Obtain $\hat{e}^i_{k+1|k+1}$ by using Eq. (24).
        Update $K^i_{k+1}$ by using Eq. (27).
    end for
end for
```

4.2. *Convergence analysis*

To analyze the convergence of the proposed distributed state estimation method, several variables are first defined i.e., $\hat{e}_{k|k} = (\hat{e}^1_{k|k}, \hat{e}^2_{k|k}, \cdots, \hat{e}^n_{k|k})^T$, $v_k = (v^1_k, v^2_k, \cdots, v^n_k)^T$, $\omega_k = (\omega^1_k, \omega^2_k, \cdots, \omega^n_k)^T$, then the global estimation error $\hat{e}_{k+1|k+1}$ at the samping instant $k+1$ can be given by

$$\begin{aligned} \hat{e}_{k+1|k+1} &= [(I_n - \varepsilon L_T - \varepsilon A L_T) \otimes A - diag(K^i_{k+1}H^i A)]\hat{e}_{k|k} \\ &\quad - diag(K^i_{k+1})v_{k+1} + (1_n \otimes \omega_k) - diag(K^i_{k+1}H^i)(1_n \otimes \omega_k) + \varepsilon(L_F \otimes A)\omega_{k-1} \end{aligned} \tag{28}$$

where L_T and L_F represent the global Laplacian submatrix of data received by the subregion i from secure subregion N_i^T and non-secure subregion N_i^F.

Furthermore, (28) can be re-written as

$$\hat{e}_{k+1|k+1} = \Gamma_{k|k}\hat{e}_{k|k} + W_{k|k} \tag{29}$$

where $\Gamma_{k|k} = [(I_n - \varepsilon L_T - \varepsilon A L_T) \otimes A - diag(K^i_{k+1}H^i A)]$, $W_{k|k} = diag(K^i_{k+1})v_{k+1} - (1_n \otimes \omega_k) + diag(K^i_{k+1}H^i)(1_n \otimes \omega_k) - \varepsilon(L_F \otimes A)\omega_{k-1}$.

For (29), if $\rho(\Gamma_{k|k}) < 1$, then estimation error $\hat{e}_{k+1|k+1}$ converges to $\bar{e}$. Next, taking the expectation of $W_{k|k}$ in (29), it follows that

$$\begin{aligned} E(W_{k|k}W^T_{k|k}) &= diag(K^i)\begin{pmatrix} R^1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & R^n \end{pmatrix} diag(K^i)^T + diag(K^i H^i)\begin{pmatrix} Q & \cdots & Q \\ \vdots & \ddots & \vdots \\ Q & \cdots & Q \end{pmatrix} diag(K^i H^i)^T \\ &\quad + \varepsilon^2(L_F \otimes A)\begin{pmatrix} Q & \cdots & Q \\ \vdots & \ddots & \vdots \\ Q & \cdots & Q \end{pmatrix}(L_F \otimes A)^T - \begin{pmatrix} Q & \cdots & Q \\ \vdots & \ddots & \vdots \\ Q & \cdots & Q \end{pmatrix} \end{aligned}$$

Obviously, there is no variable in the above expectation, so the expectation $E(W_{k|k}W_{k|k}^T)$ converges to $\tilde{Q}$. Then, the $\rho(\Gamma_{k|k}) < 1$ in (29) should be satisfied to ensure the convergence of global estimation error.

For the convenience of the following proof, first define $M = \frac{1}{2}[(I_n - \varepsilon L_T - \varepsilon AL_T) \otimes A + (I_n - \varepsilon L_T - \varepsilon AL_T)^T \otimes A^T]$, $N = \frac{1}{2}[diag(K_{k+1}^i H^i A) + diag(K_{k+1}^i H^i A)^T]$, then a sufficient condition is given to ensure that $\rho(\Gamma_{k|k}) < 1$.

Theorem 1: If $\max\left|\lambda_i(M) - \lambda_j(N)\right| < 1, (i,j) \in \{(1,1),(1,2),...,(m,n)\}$, then $\rho(\Gamma_{k|k}) < 1$.

Proof: According to [60], $x^T Z x = x^T(\frac{Z+Z^T}{2})x, \forall Z \in M_n$. Then, substitute $(I_n - \varepsilon L_T - \varepsilon AL_T) \otimes A$ and $diag(K_{k+1}^i H^i A)$ into Z, it follows that

$$y^T((I_n - \varepsilon L_T - \varepsilon AL_T) \otimes A)y = y^T M y, \tag{30}$$

$$y^T diag(K_{k+1}^i H^i A)y = y^T N y \tag{31}$$

For any non-zero $y \in R^{mn}$, the eigenvalues of the matrices M and N can be sorted as $\lambda_1(M) \leq \cdots \leq \lambda_m(M)$, $\lambda_1(N) \leq \cdots \leq \lambda_n(N)$.

According to $x^T A x = x^T m x$, m is the eigenvalue of the matrix A. Then, both sides of (30) and (31) are simultaneously left multiplied by $(y^T)^{-1}$ and right multiplied by $(y)^{-1}$, it follows that

$$\lambda_1(M) \leq \frac{y^T((I_n - \varepsilon L_T - \varepsilon AL_T) \otimes A)y}{y^T y} \leq \lambda_m(M) \tag{32}$$

$$\lambda_1(N) \leq \frac{y^T diag(K_{k+1}^i H^i A)y}{y^T y} \leq \lambda_n(N) \tag{33}$$

From the definition of $\Gamma_{k|k} = [(I_n - \varepsilon L_T - \varepsilon AL_T) \otimes A - diag(K_{k+1}^i H^i A)]$, subtract (33) from (32), it follows that

$$\left|\lambda_i(\Gamma_{k|k})\right| \leq \max_{y \neq 0}\left|\frac{y^T \Gamma_{k|k} y}{y^T y}\right| \leq \max_{i,j}\left|\lambda_i(M) - \lambda_j(N)\right|$$

It completes the proof.

Remark 8: The security scope of CPPSs is very broad, and this paper specifically focuses on the security of distributed security state estimation. This is because the distributed security state estimation results will be used for power flow calculation and produce subsequent optimization dispatch strategy to affect carbon emissions and economic cost. This paper proposes a novel consensus-based DSSE method to relieve the impact of hybrid attacks on carbon emissions and economic cost. First, a novel residual-based attack detection method is constructed in each subregion, where secure and non-secure sets are employed to describe whether the subregion is attacked and compensation mechanism is designed for non-secure set. Second, a distributed state estimation model is reconstructed by using data compensation mechanism, and then a distributed secure state estimation method is proposed. Finally, sufficient condition of its convergence is derived, requiring that the difference between the maximum eigenvalues of the matrix M (i.e., which is composed of Laplace matrix of secure and non-secure set topologies and system matrix) and the matrix N (i.e., which is composed of gain matrix, Jacobian matrix and system matrix) is less than 1, i.e., $\rho(\Gamma_{k|k}) < 1$, guaranteeing the security of distributed security state estimation results under hybrid attacks.

4.3. *Distributed security state estimation-based carbon emissions analysis*

Given the above design of DSSE method, the impact of hybrid attacks on carbon emissions can be analyzed. According to the collected measurements (e.g., V_m, P_m, Q_m, P_{mn}, Q_{mn}, etc.), the estimated voltage amplitude and phase angle $\hat{V}_m$ and $\hat{\theta}_m$ of each node can be obtained by the above distributed security state estimation method. Furthermore, the influence of state estimation results on carbon emissions with and without compensation mechanism is analyzed.

4.3.1. Carbon emissions analysis without compensation mechanism

Subsection 3.1 shows that hybrid attacks will destroy the process of distributed state estimation. If these results are directly used in OPF, it will inevitably affect the outputs of both clean energy units and thermal power units , and eventually the total carbon emission of power system.

Given the hybrid attacks analysis in Subsection 2.1, for attack Type 1 and attack Type 2, there will be also two processes:

1) Attack Type 1 occurs: When attack Type 1 is caused by attack Status 1 or attack Status 2, the data from subregion j to the corresponding local state estimator j is tampered or blocked, so that the state $x^{j,s1}_{t1,k+1|k+1}$ contains false data or suffers from data losses. For example, if the hacker attacks any node connected to thermal power units, clean energy units and load, it will cause the change of the corresponding variables such as active power injection P_m. Assume that the hacker attacks active injection power P^j_m of node m in subregion j at the samping instant $k+1$, the original injection power $P^j_{m,k+1}$ of the attacked node m in subregion j is affected by hybrid attacks and becomes $P^{j,a}_{m,k+1}$, so the local estimation of the corresponding subregion j is affected and can be re-written as

$$\hat{x}^{j,a}_{t1,k+1|k+1} = \tilde{x}^{j}_{k+1|k} + K^{j}_{k+1}[z^{j,a}_{k+1} - \tilde{z}^{j}_{k+1|k}] \tag{34}$$

where $z^{j,a}_{k+1} = [V^j_{m,k+1}\ P^{j,a}_{m,k+1}\ Q^j_{m,k+1}\ P^j_{mn,k+1}\ Q^j_{mn,k+1}]^T$ contains the tampered injection power $P^{j,a}_{m,k+1}$. This in turn affects the estimated voltage amplitude and phase angle $\hat{V}^{j,a}_{m,k+1}$ and $\hat{\theta}^{j,a}_{m,k+1}$ of the corresponding attacked node m in subregion j.

2) Attack Type 2 occurs: based on the result $\hat{x}^{j,a}_{t1,k+1|k+1}$ caused by attack Type 1, when attack Type 2 is caused by attack Status 1 or attack Status 2, i.e., the data from state estimator j to the state estimator i is further tampered or blocked, and the state $\hat{x}^{j,*}_{t2,k+1|k+1} = (1-\mu^2_{k+1})T^2_{k+1}\hat{x}^{j,a}_{t1,k+1|k+1}$ contains false data (i.e., $\mu^2_{k+1} = 0,\ T^2_{k+1} \neq 0$) or suffers from data losses (i.e., $\mu^2_{k+1} = 0$). Then, according to (4), the subregion i and the attacked subregion j begin to exchange state data, i.e., $\hat{x}^{j,*}_{t2,k|k}$ containing false data due to attacks is transmitted to subregion i, so that all neighbor regions of subregion j receive the wrong state $\hat{x}^{j,*}_{t2,k+1|k+1}$ of subregion j.

Finally, the global state $\hat{x}^{a}_{k+1|k+1}$ with attack impact can be obtained by distributed state estimation, then the estimated measurement of all nodes can be expressed as

$$\hat{z}^{a}_{k+1|k+1} = H\hat{x}^{a}_{k+1|k+1} \tag{35}$$

where $\hat{z}^{a}_{k+1|k+1} = [\hat{V}_{m,k+1},\ \hat{P}^{a}_{m,k+1},\ \hat{Q}_{m,k+1},\ \hat{P}_{mn,k+1},\ \hat{Q}_{mn,k+1}]^T$ contains the estimated value $\hat{P}^{j,a}_{m,k+1}$ of the tampered injection power $P^{j,a}_{m,k+1}$.

Next, the estimated state $\hat{x}^{a}_{k+1|k+1}$ and measurement $\hat{z}^{a}_{k+1|k+1}$ of each node are sent to the control center as the original data for OPF. In the process of OPF, it is also necessary to meet the equilibrium constraint of power system and generator unit output constraints and other constraints, i.e., three constraints given in subsection 2.3, it follows that

$$\bar{P}^{tot}_{k} = \bar{P}^{TG}_{m,k} + \bar{P}^{CG}_{n,k} = \bar{P}^{load}_{k}$$

$$\bar{P}^{TG,\min}_{m,k} \leq \bar{P}^{TG}_{m,k} \leq \bar{P}^{TG,\max}_{m,k}, t \in S^T, m \in S^{TG}$$

$$\bar{P}^{CG,\min}_{n,k} \leq \bar{P}^{CG}_{n,k} \leq \bar{P}^{CG,\max}_{n,k}, t \in S^T, m \in S^{TG}$$

Remark 9: The hacker can attack any node connected to thermal power units, clean energy units or load. Considering that carbon emissions are only related to active power, only active injection power of the above three types of nodes due to attacks are considered. When the hacker attacks nodes connected to thermal power units, clean energy units or load, it will affect $\bar{P}^{TG}_{m,k}$, $\bar{P}^{CG}_{n,k}$ and $\bar{P}^{load}_{k}$ in power balance constraints, respectively.

Since the equilibrium constraint of power system is affected by attacks, OPF will produce the output $\bar{P}^{TG,a}_{m,k}$ of each thermal power unit when calculating power flow with carbon emission as the optimal target, i.e., min $\bar{E}^a = \sum_{m\in S^{TG}}\sum_{k\in S^T}\bar{E}_m\{P^{TG,a}_{m,k}\}$.

4.3.2. Carbon emissions analysis with compensation mechanism

The above analysis shows how hybrid attacks affect carbon emission of CPPSs without compensation mechanism. Then carbon emissions of CPPSs with compensation mechanisms can be analyzed. The difference between carbon emission analysis with and without compensation is the process of state data exchange.

When subregion j transmits the attacked states data $\hat{x}^{j,*}_{t2,k+1|k+1}$ to subregion i through the consensus term in (4), attack detection mechanism is performed by (18) in subregion j. If an alarm is triggered, then subregion j will be determined as a non-secure set. As described in (21), the Kalman predicted value $\tilde{x}^{j}_{k|k-1}$ of subregion j will replace $\hat{x}^{j,*}_{t2,k+1|k+1}$ and be transmitted to subregion i. At this point, the distributed state estimation method can be used to obtain the estimated voltage amplitude and phase angle value $\hat{V}^{j,com}_{m,k+1}$ and $\hat{\theta}^{j,com}_{m,k+1}$ of subregion j under compensation mechanism.

Finally, the global state $\hat{x}^{com}_{k+1|k+1}$ under compensation mechanism can be obtained by distributed state estimation, then the estimated measurement of all nodes can be expressed as

$$\hat{z}^{com}_{k+1|k+1} = H\hat{x}^{com}_{k+1|k+1} \tag{36}$$

Next, the estimated state $\hat{x}^{com}_{k+1|k+1}$ and measurement $\hat{z}^{com}_{k+1|k+1}$ of each node are sent to the control center as the original data for OPF to obtain the output $\bar{P}^{TG,com}_{m,k}$ of each thermal power unit under compensation mechanism. Then carbon emissions under compensation mechanism can be obtained by min $\bar{E}^{com} = \sum_{m\in S^{TG}} \sum_{k\in S^{T}} \bar{E}_m\{P^{TG,com}_{m,k}\}$.

Finally, the impact of different attacks on carbon emissions will be analyzed by experimental results. For example, three types of nodes, including nodes connected to clean energy units, nodes connected to thermal power units and load, are attacked respectively, and three types of nodes are attacked simultaneously to further analyze the impact of attacks on carbon emissions. Furthermore, to analyze the impact of attack intensity on carbon emissions, the estimated state and measurement of each node are increased or decreased by adjusting T^1_k and T^2_k, and OPF is then operated to obtain the output of each thermal power unit, and the impact of attack intensity on carbon emissions is finally analyzed. It should be noted that the impact of the attack on the state estimation is relieved after the compensation mechanism is adopted.

5. Experimental results and analysis

To validate the performance of the proposed DSSE method under hybrid attacks and the impact of hybrid attacks on carbon emissions and economic cost, experiments were operated using the IEEE 14-bus system and the data from actual power systems. The IEEE 14-bus system as shown in Fig.3 is employed, where the specific measurements of the nodes contained in 4 subregion are shown in Table I.

In Fig.3, 5 thermal power units are connected to the nodes $1, 2, 3, 6$ and 8, respectively, and their parameters are shown in Table II. Clean energy unit is connected to node 7 and the capacity is 80.49 MW. The total output of thermal power unit is 185.68 MW, i.e., the clean energy penetration rate is 30%. After ignoring the line loss, the total load of the system is 268.29 MW. And the conversion coefficient between power generation and carbon dioxide emission of thermal power unit is set to 0.83 [61].

5.1. Experimental analysis in IEEE 14-bus system

5.1.1. Distributed security state estimation

In this numerical simulation, distributed state estimation results under different conditions are used to evaluate the effectiveness and convergence of the proposed algorithm.

1) *Attack-free distributed security state estimation*: When hybrid attacks are not launched, Table 3 shows the actual value and estimated value of voltage amplitude and phase angle of each node. To better illustrate the effectiveness of distributed security state estimation under hybrid attacks, node 3 is taken as an example. Using the above proposed DSSE method, Fig.5 shows the attack-free estimation results of phase angle and amplitude of node 3. After a few iterations, the states of four subregions finally reach the consensus and converge to true value, which confirms the effectiveness and convergence of the proposed distributed method.

2) *Distributed security state estimation under hybrid attacks*: When the hacker launch hybrid attacks on subregion 2, Figs.6a) and b) show the estimation results of phase angle and amplitude of node 3. First, before hybrid attacks, the phase angle and amplitude estimations of node 3 in four subregions have been consistent and converge to true

Table 1
Partition table of IEEE 14-bus system

Subregion	Nodes	Measurements
1	1, 2, 3, 4, 5, 6	V_1, P_5, $P_{1,2}$, $P_{1,5}$, $P_{2,3}$, $P_{2,5}$, $P_{5,6}$, Q_5, $Q_{1,2}$, $Q_{1,5}$, $Q_{2,3}$, $Q_{2,4}$, $Q_{2,5}$, $Q_{5,6}$
2	2, 3, 4, 5, 7, 8, 9	V_4, P_4, P_7, $P_{3,4}$, $P_{4,5}$, $P_{4,7}$, $P_{4,9}$, $P_{7,8}$, $P_{7,9}$, Q_4, Q_7, $Q_{3,4}$, $Q_{4,5}$, $Q_{4,7}$, $Q_{4,9}$, $Q_{7,8}$, $Q_{7,9}$
3	4, 7, 9, 10, 11, 13, 14	V_9, P_9, P_{10}, $P_{9,10}$, $P_{9,14}$, $P_{10,11}$, $P_{13,14}$, Q_9, Q_{10}, Q_{14}, $Q_{9,10}$, $Q_{9,14}$, $Q_{10,11}$, $Q_{13,14}$
4	6, 10, 11, 12, 13, 14	V_6, P_{11}, P_{12}, P_{13}, $P_{6,11}$, $P_{6,12}$, $P_{6,13}$, $P_{12,13}$, Q_{11}, Q_{12}, Q_{13}, $Q_{6,11}$, $Q_{6,12}$, $Q_{6,13}$, $Q_{12,13}$

Table 2
Parameters of thermal power units

Units	P_1^{TG}	P_2^{TG}	P_3^{TG}	P_4^{TG}	P_5^{TG}
Node	1	2	3	6	8
$P_m^{TG,min}$	0	0	0	0	0
$P_m^{TG,max}$	332.4	140	100	100	100

Table 3
True value and estimated value of voltage amplitude and phase angle of each node in IEEE 14-bus system

Nodes	1	2	3	4	5	6	7
θ	0	-0.087	-0.223	-0.179	-0.153	-0.252	-0.231
$\hat{\theta}$	0	-0.087	-0.227	-0.182	-0.157	-0.254	-0.234
V	1.060	1.045	1.010	1.013	1.017	1.070	1.046
$\hat{V}$	1.059	1.041	1.025	1.021	1.019	1.063	1.041
Nodes	8	9	10	11	12	13	14
θ	-0.231	-0.259	-0.262	-0.259	-0.267	-0.268	-0.281
$\hat{\theta}$	-0.234	-0.261	-0.265	-0.262	-0.269	-0.270	-0.283
V	1.080	1.031	1.030	1.046	1.053	1.047	1.019
$\hat{V}$	1.084	1.030	1.034	1.039	1.046	1.040	1.023

value. Then, hybrid attacks are launched on subregion 2 at the instant 200. Since four subregions need exchange data, the estimations of phase angle and amplitude of node 3 in all subregions are affected by hybrid attacks and gradually deviate from true value. It will inevitably pose a threat on the stable operation of the system.

Next, the designed attack detection method is used to detect attacks, Fig.6c) shows attack detection results. The threshold is set as $3|R|$, which depends on the 3σ criterion in engineering application. When hybrid attacks are not launched, the proposed detection method does not exceed the set threshold. However, when hybrid attacks are launched on node 3 of subregion 2, the size of T_k is set as 1.5. The proposed detection method exceeds the set threshold, which triggers the alarm and threaten system running.

3) *Distributed security estimation with attack compensation mechanism*: When the abnormality of subregion 2 is detected, the attack compensation mechanism is adopted to relieve the impact of attacks, Fig.7 shows the phase angle and amplitude estimation results of node 3 in four subregions. Firstly, when hybrid attacks are launched, the estimations of phase angle and amplitude of node 3 in all subregion are affected and gradually deviate from their true values. Then, after successfully detecting hybrid attacks, at the instant $\eta_k^i = 0$, distributed state estimator continues to perform state estimation by using attack compensation mechanism. Finally, after compensation mechanism is adopted, the phase

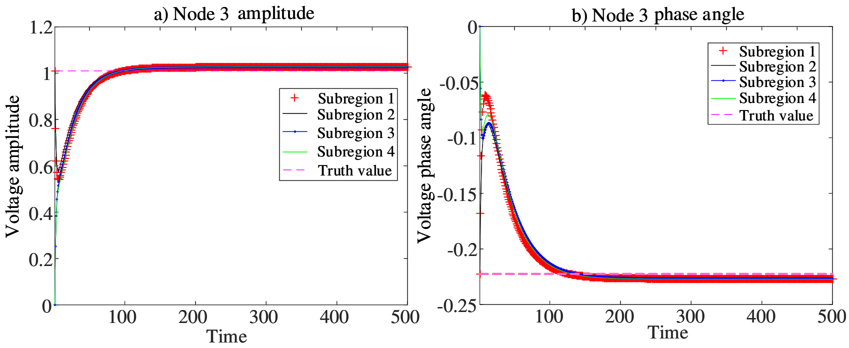


Figure 5: Estimation results of phase angle and amplitude of node 3 in 4 subregions.

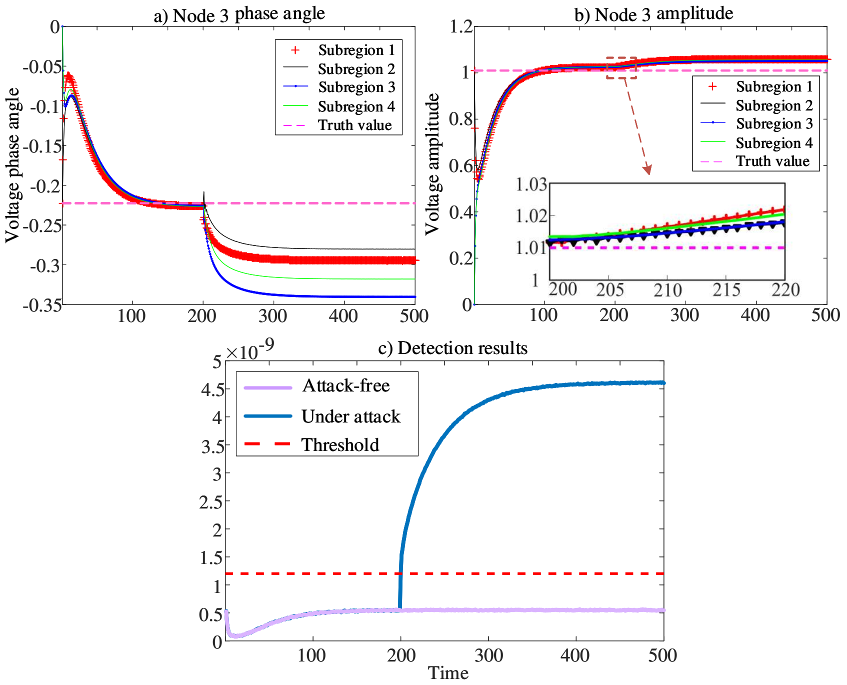


Figure 6: Estimation results of phase angle and amplitude of node 3 in 4 subregions and attack detection results under hybrid attacks. The detection threshold is $3|R| = 1.2$, which is based on the 3σ criterion of ensuring no false detection under attack-free.

angle and amplitude estimation results of node 3 in four subregions begin to gradually return to true value, which finally reach the consensus and converge to true value. The above process confirms the effectiveness and convergence of the proposed DSSE method.

Moreover, the mean absolute error (MAE) is used as an indicator to evaluate the performance of state estimation method, i.e., $MAE(\hat{x}_k^i) = \frac{1}{n}\sum_{n=1}^{N}\left|\hat{x}_{k|k}^i(n) - x_k(n)\right|$. Fig.8 shows the MAE of two methods under hybrid attacks. The proposed method has smaller MAE under hybrid attacks than the method in [12], which further confirms the effectiveness of the proposed method.

As attack intensity continues to increase, when the spectral radius of matrix $\Gamma_{k|k}$ is greater than 1 as shown in Fig.9c), i.e., $\rho(\Gamma_{k|k}) > 1$, the distributed state estimation results begin to diverge. Figs.9a) and 9b) show the estimation results of phase angle and amplitude of node 3 in 4 subregions when the spectral radius is greater than 1. First, before hybrid attacks, the phase angle and amplitude estimations of node 3 in four subregions have been consistent and

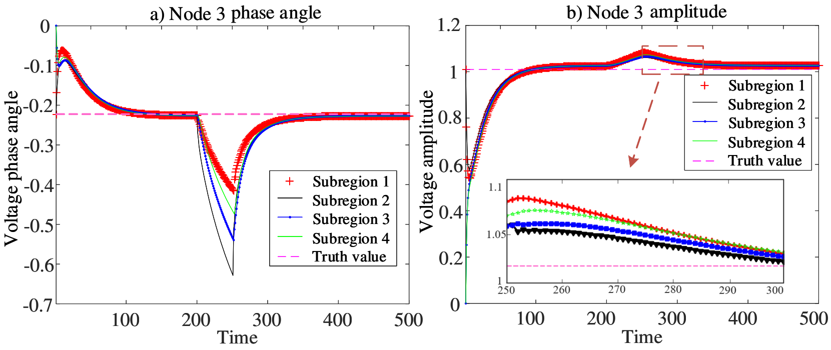


Figure 7: Estimation results of phase angle and amplitude of node 3 in 4 subregions under attack compensation mechanism.

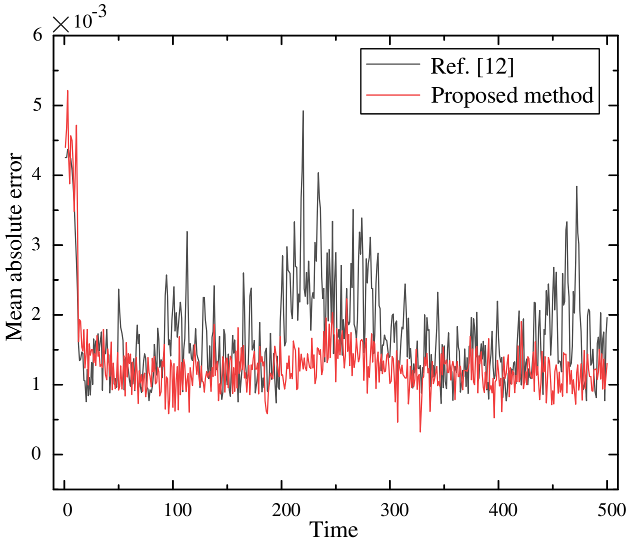


Figure 8: Mean absolute error of two methods under hybrid attacks.

converge to true value. Then, when hybrid attacks are launched at the instant 200, the excessive attack intensity does not cause phase angle and amplitude of node 3 to converge as shown in Fig. 7, which reveals that the convergence of distributed state estimation is destroyed when attack intensity increases to such an extent that the spectral radius of matrix $\Gamma_{k|k}$ is greater than 1.

5.1.2. Impact of hybrid attacks on carbon emissions and economic cost

In this numerical simulation, the impact of attacks on CPPSs carbon emissions and economic cost are analyzed by attacking different types of nodes.

1) *Attacking nodes connected to clean energy units*: Before considering attacking nodes connected to clean energy units, the impact of clean energy penetration rate on carbon emissions is analyzed. When clean energy penetration rate ranges from 5% to 30% and there is no hybrid attacks, Fig.10 shows the total output of thermal power units and clean energy units. It shows that under the constraint of power balance, the greater penetration rate of clean energy units will reduce power output of thermal power units, thus leading to the reduction of carbon emissions.

Then, when the node 7 connected to clean energy unit is attacked, Fig.11 shows the total output of clean energy units and thermal power units, and the overall carbon emission. The attack intensity is also introduced to describe how the attacker tampers with the value of the injection power P_7 of node 7. It is evident from Fig.11 that when attack intensity gradually increases, the outputs of clean energy units rapidly decrease until they become zeros. It should be noted that attack intensity of 0 means that attack compensation mechanism is used to relieve the impact of attacks. At

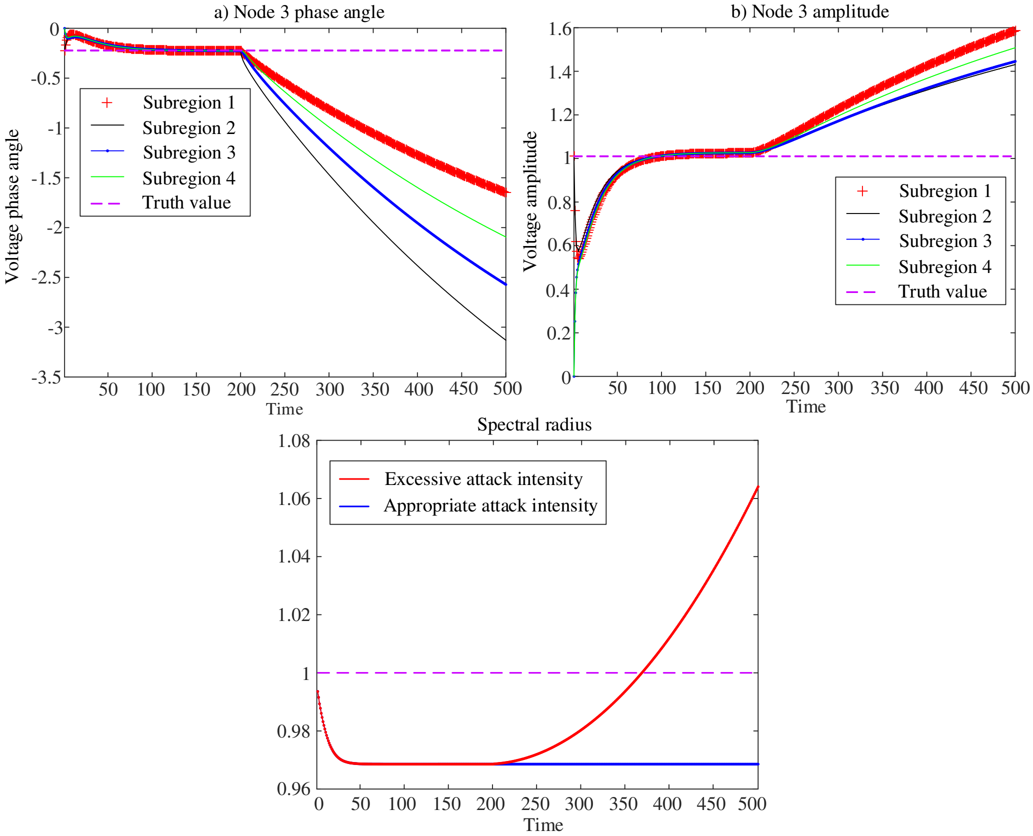


Figure 9: Estimation results of phase angle and amplitude of node 3 in 4 subregions when the spectral radius is greater than 1.

this time, thermal power units increase the output to incease system stability and meet power balance constraints. As the outputs of thermal power units increase, carbon emissions also increase rapidly. The output of each thermal power unit is listed in Table 4. and it is evident that the output of clean energy units gradually decreases due to the impact of attack, while thermal power units gradually increase their power outputs, leading to an increase in carbon emissions. This also confirms that attacking nodes connected to clean energy units will lead to an increase in carbon emissions.

2) *Attacking nodes connected to thermal power units*: When node 6 connected to thermal power unit is attacked and attack intensity ranges from 100% to 600%, Fig.12 shows the total output of thermal power units, the injection power of node 6, and the total carbon emission. Fig.12 reveals that when attack intensity gradually increases, i.e., the injection power of node 6 gradually increases due to the impact of the attack. At this time, when clean energy output is stable, thermal power unit needs to increase its output to maintain the constraint of power balance. Meanwhile, with the increase of the output of thermal power units, carbon emissions also gradually increase. And the output of each thermal power unit is described in Table 5. As can be seen from Table 5, the injection power of node 6 gradually increases under the influence of attack, while that of thermal power units gradually increases, leading to an increase in carbon emissions. This also confirms that attacking nodes connected to thermal power units will lead to an increase in carbon emissions.

3) *Attacking load nodes*: When load node 10 is attacked and attack intensity is from 100% to 600%, Fig.12 also shows the total output of thermal power units, injection power of node 10, and the total carbon emission. As can be seen from Fig.12, when attack intensity increases by multiple, i.e., the injection power of node 10 is increases by multiple. At this time, when the output of clean energy is stable, thermal power units still need to increase their output to maintain the constraint of power balance, resulting in the gradual increase of carbon emissions. And the output of each thermal power unit is described in Table 6. As seen from Table 6, the injection power of node 10 gradually increases under the attack, while thermal power units gradually increase their outputs, leading to an increase in carbon

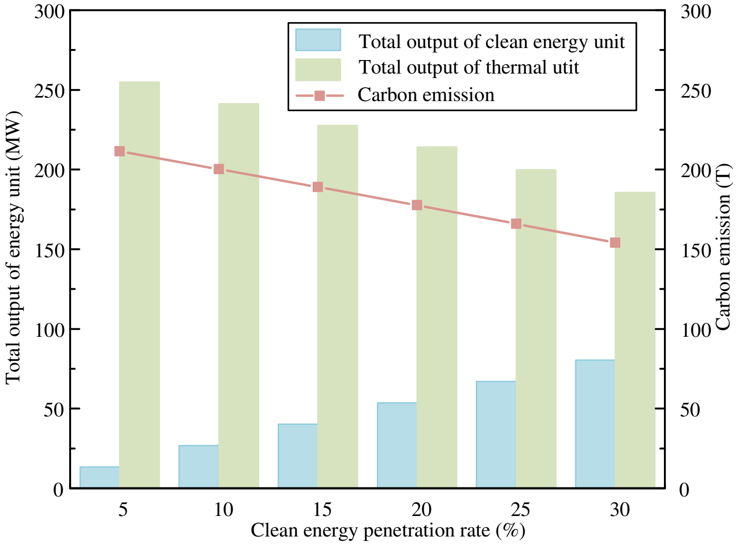


Figure 10: Total output of thermal power units and clean energy unit, and total carbon emission when the penetration rate ranges from 5% to 30%.

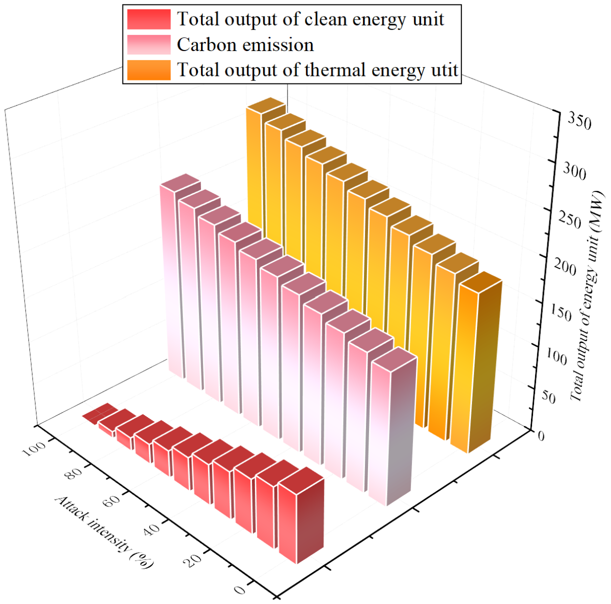


Figure 11: Total output of thermal power units and clean energy unit, and total carbon emission when node 7 is attacked and the attack intensity ranges from 0% to 100%.

emissions. This also confirms that attacking load nodes will lead to an increase in carbon emissions.

4) *Attacking all three types of nodes simultaneously*: When nodes 7, 6 and 10 are attacked, Fig.13 shows the total output of thermal power units, the injection power of nodes 7, 6, 10, and the total carbon emission. It should be noted that the attacker can increase or decrease the tampered value. To analyze the impact of the attack on the increase of carbon emissions, the injection power of node 7 is reduced and that of nodes 6 and 10 are increased.

As can be seen from Fig.13, when the hacker attacks the injected power of nodes 7, 6 and 10 simultaneously, clean energy output decreases and the total loads increases. Compared with attacking a single type of node, thermal power units need to further increase their outputs to maintain the constraint of power balance, resulting in a rapid increase

Table 4
Output of each thermal power unit and total carbon emission when attacking injection power P_7 of node 7 of clean energy generator

Attack intensity	P_7	P_1^{TG}	P_2^{TG}	P_3^{TG}	P_4^{TG}	P_5^{TG}	Total TGs output	Carbon emissions	Economic cost
0	80.49	156.27	29.42	0	0	0	185.68	154.11	4980.71
10%	72.44	163.38	30.79	0	0	0	194.17	161.16	5268.85
20%	64.39	170.51	32.18	0	0	0	202.69	168.23	5563.63
30%	56.34	177.68	33.57	0	0	0	211.25	175.34	5865.16
40%	48.29	183.87	34.78	1.09	0	0	219.73	182.38	6137.42
50%	40.25	185.98	35.17	6.61	0	0	227.75	189.03	6485.19
60%	32.18	188.09	35.56	12.20	0	0	235.84	195.75	6800.61
70%	24.15	190.20	35.95	17.78	0	0	243.93	202.46	7116.97
80%	16.10	192.32	36.34	23.40	0	0	252.07	209.22	7436.64
90%	8.05	193.61	36.59	26.84	0	3.15	260.19	215.96	7758.58
100%	0	194.33	36.72	28.74	0	8.50	268.29	222.68	8081.53

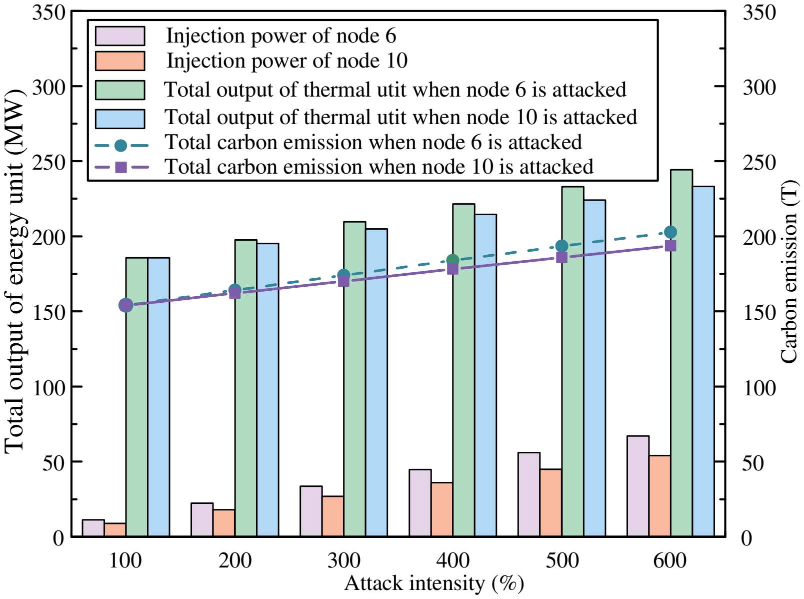


Figure 12: Total output of thermal power units, injection power of node 6, and total carbon emission when node 6 is attacked and the attack intensity ranges from 100% to 600%.

in carbon emissions. And the output of each thermal power unit is listed in Table 7. It is evident that the power outputs of clean energy units gradually decrease, and the injection power of nodes 6 and 10 gradually increases due to the impact of the attack, while thermal power units gradually increase their power outputs, leading to an increase in carbon emissions. In addition, compared with attacking a single node, attacking three nodes simultaneously causes the largest increase in carbon emissions.

Moreover, when attacking a single node and simultaneously attacking three nodes, a further comparative analysis is conducted on carbon emissions as shown in Fig.14. It can be seen that as attack intensity on different nodes reduces, the carbon emissions of CPPSs will also correspondingly reduce, and the reduction in carbon emission caused by cyber

Table 5
Output of each thermal power unit and total carbon emission when attacking injection power P_6 of node 6 of thermal power generator

Attack intensity	P_6	P_1^{TG}	P_2^{TG}	P_3^{TG}	P_4^{TG}	P_5^{TG}	Total TGs output	Carbon emissions	Economic cost
100%	11.20	156.27	29.41	0	0	0	185.68	154.11	4980.71
200%	22.40	166.28	31.34	0	0	0	197.62	164.02	5387.72
300%	33.60	176.37	33.29	0	0	0	209.66	174.02	5808.59
400%	44.80	184.85	34.92	1.81	0	0	221.59	183.92	6243.4
500%	56.00	188.00	35.50	9.49	0	0	233.00	193.39	6686.66
600%	67.20	189.54	35.78	13.26	5.76	0	244.33	202.79	7134.89

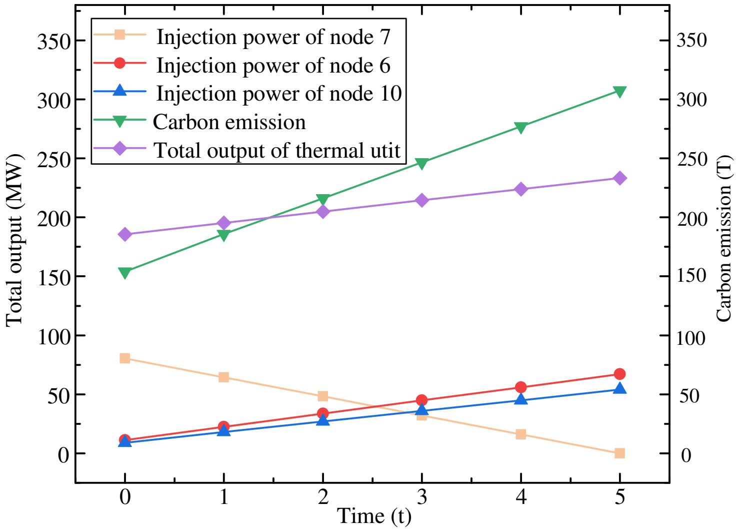


Figure 13: Total output of thermal power units, injection power of nodes 6, 7, 10, and total carbon emission when nodes 7, 6 and 10 are attacked.

attacks on different single nodes is also different. It is worth noting that when the attacker simultaneously attacks three nodes, the increase of carbon emissions will reach its maximum. However, as data compensation mechanism gradually relieves attack impact, carbon emissions caused by attacking different nodes are gradually reduced. Therefore, the proposed DSSE method can effectively reduce the impact of cyber attacks on carbon emissions.

Finally, when attacking a single node and simultaneously attacking three nodes, a further comparative analysis of economic cost is performed as shown in Fig.15. As can be seen from Fig.15, economic cost of CPPSs increases with the increase of attack intensity on a single node, and the degree of increase in economic cost caused by cyber attacks on different single nodes is also different. It is worth noting that under the same attack intensity, economic cost of attacking three nodes is greater than that of attacking a single node, which is consistent with the above analysis of carbon emissions.

5.2. *Experimental analysis in China power system*

A regional real power system in China is used to validate the proposed approach. The highest load of this power grid in history is 191.3MW, and there are about 250 00 residents with the highest annual electricity sales of 901 million kW·h. This real power system includes 28 buses (i.e., four power stations including two wind farms, two 220 KV substations, two 110 KV substations, etc.), 44 branches and 121 measurements. The system configuration is shown in Fig.16. The wind unit 1 is connected to node 9, and the wind unit 2 is connected to node 11, and their total output is

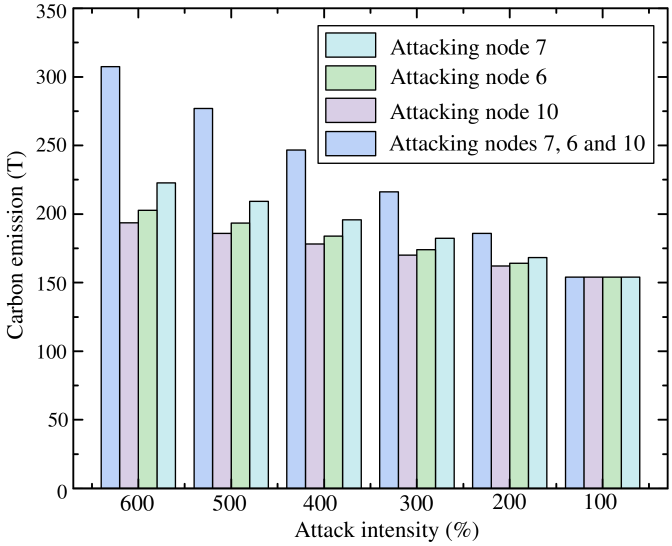


Figure 14: Carbon emissions of attacking a single node and simultaneously attacking three nodes.

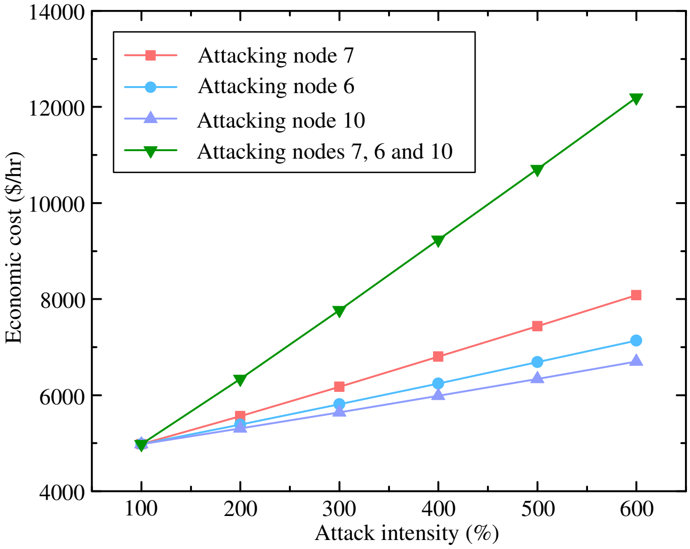


Figure 15: Economic cost of attacking a single node and simultaneously attacking three nodes.

68MW. The total output of thermal power unit is 123.3 MW, i.e., the clean energy penetration rate is 35.54%.

Specifically, node 9 connected to wind unit 1 is attacked, and random attack intensity is used to tamper with the injected power of node 9. Considering that power generation of wind unit 1 is greater than that of wind unit 2, the minimum attack intensity and maximum attack intensity are set as 10% and 60%.

When node 9 (i.e., wind unit 1) is attacked, Fig.17 shows the total output of thermal power units and clean energy unit, and total carbon emission. It is evident from Fig.17 that when attack intensity increases, the output of clean energy units decreases rapidly. At this time, thermal generation units increase their power outputs to maintain the stability of the total output to maintain power balance constraints. As thermal power units increase their outputs, carbon emissions also increase rapidly. Finnaly, the compensation mechanism is adopted to relieve the impact of the attack at time instant 9, and this leads to modify distributed state estimation results. OPF is operated based on the revised state estimation results, which reduces the output of thermal power units, thereby reducing carbon emissions.

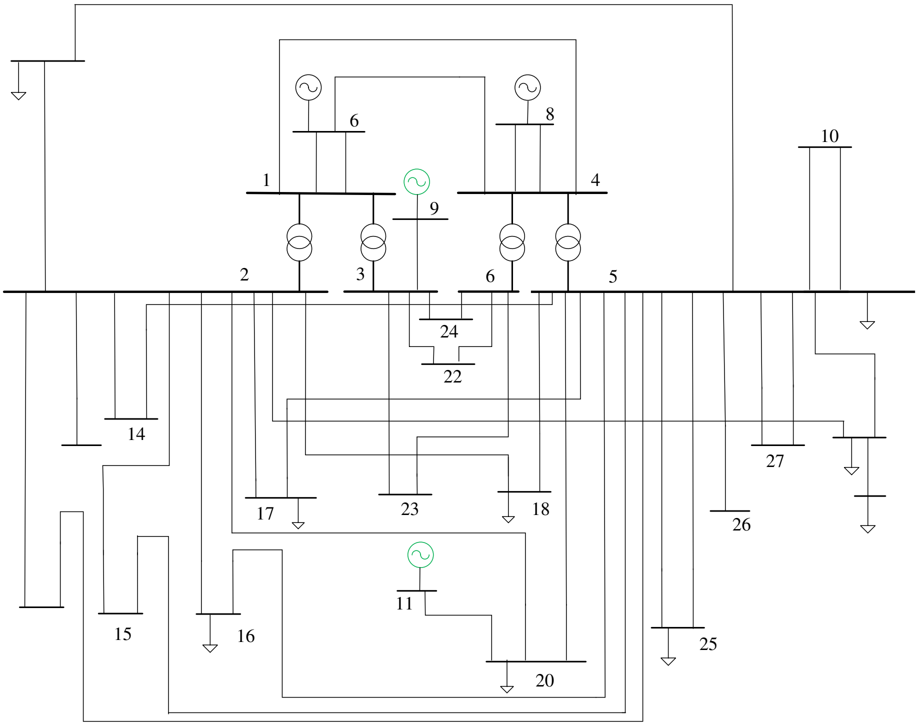


Figure 16: A regional real power system configuration in China.

Table 6
Output of each thermal power unit and total carbon emission when attacking injection power P_{10} of load node 10

Attack intensity	P_{10}	P_1^{TG}	P_2^{TG}	P_3^{TG}	P_4^{TG}	P_5^{TG}	Total TGs output	Carbon emissions	Economic cost
100%	9.00	156.27	29.41	0	0	0	185.68	154.11	4980.71
200%	18.00	164.27	30.96	0	0	0	195.23	162.04	5305.49
300%	27.00	172.35	32.53	0	0	0	204.88	170.05	5640.21
400%	36.00	180.50	34.12	0	0	0	214.61	178.13	5985.15
500%	45.00	185.08	34.99	3.94	0	0	224.02	185.94	6339.50
600%	54.00	187.52	35.44	10.3	0	0	233.26	193.61	6699.26

6. Discussion and conclusions

This paper has proposed a novel consensus-based DSSE method for analyzing the impact of hybrid attacks on carbon emissions and economic cost. The incomplete and non-authentic nature of the tampered data caused by hybrid attacks are formulated and their influence on distributed state estimation is analyzed. Then, a novel residual-based attack detection method is constructed in each subregion to determine whether the subregion is secure or non-secure, and a Kalman prediction-based attack compensation mechanism is designed for non-secure set to reconstruct distributed state estimation model. Furthermore, according to the reconstructed distributed state estimation model, a DSSE method under hybrid attacks is proposed and sufficient condition of its convergence is derived, and the impact of hybrid attacks on carbon emissions and economic cost are analyzed based on the proposed DSSE method. Finally, experimental results in IEEE 14-bus system and real power system demonstrate feasibility and effectiveness of pro-

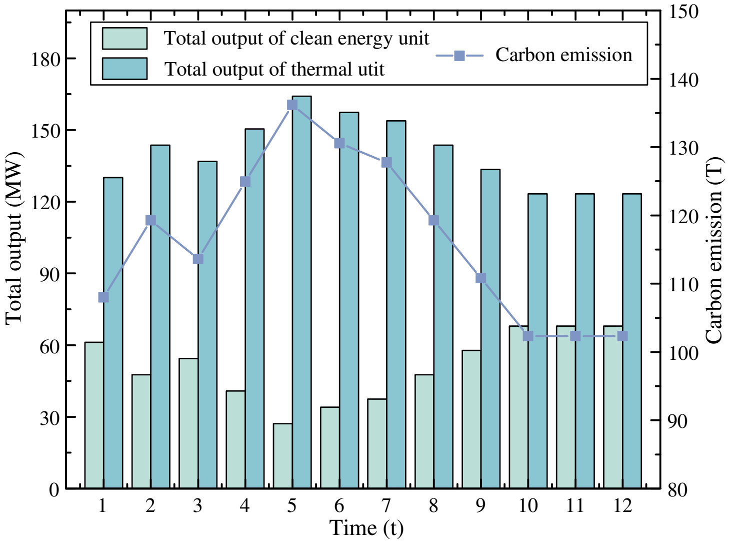


Figure 17: Total output of clean energy units and thermal power units, and total carbon emission when real power system are attacked.

Table 7
Output of each thermal power unit and total carbon emission when attacking injection power P_7, P_6 and P_{10}

P_7	P_6	P_{10}	P_1^{TG}	P_2^{TG}	P_3^{TG}	P_4^{TG}	P_5^{TG}	Total TGs output	Carbon emissions	Economic cost
80.49	11.20	9.00	156.27	29.41	0	0	0	185.68	154.11	4980.71
64.39	22.40	18.00	185.17	35.00	3.76	0	0	223.93	185.86	6335.68
48.29	33.60	27.00	194.1	36.65	26.82	2.90	0.03	260.50	216.22	7769.06
32.18	44.80	36.00	196.73	37.14	33.81	15.82	13.59	297.09	246.58	9232.05
16.10	56.00	45.00	198.93	37.55	39.61	27.57	30.07	333.72	276.99	10706.92
0	67.20	54.00	201.12	37.96	45.40	39.36	46.63	370.47	307.49	12195.67

posed DSSE method, and further validate that the proposed method can effectively relieve the negative impacts caused by hybrid attacks on state estimation under different attack intensity, thus relieving the impact of hybrid attacks on carbon emissions and economic cost.

However, the proliferation of clean energy and electric vehicles brings additional opportunities for the attacker, and the diversity and complexity of cyber attacks bring a huge threat to the security of CPPSs. The proposed DSSE method is essentially considered from the perspective of passive defense, i.e., cyber attacks can be detected and measures taken to relieve the impact of cyber attacks on the system only after the attacker have invaded the system, and malicious cyber attacks cannot be prevented at the root. Therefore, it is considered in the future work to further improve the security of CPPSs from the perspective of active defense by using signature and security certification, and make full use of clean energy to reduce carbon emissions. Moreover, considering some goals such as carbon emissions and economic cost, etc., game strategies between the attacker and the defender can also be investigated in the future.

Appendix

A *Example*

1) *Attack-free*: When neither attack Type 1 nor Type 2 occurs, state estimator j completes local state estimation of the states $x_2^j, x_3^j, x_4^j, x_5^j, x_7^j, x_8^j, x_9^j$ of nodes 2, 3, 4, 5, 7, 8, 9 contained in subregion j (i.e.,

attack-free subregion j in Fig. 3), and state estimator i also completes local state estimationof the states $x_1^i, x_2^i, x_3^i, x_4^i, x_5^i, x_6^i$ of nodes 1, 2, 3, 4, 5, 6 contained in subregion i. Then, the state estimator j transmits the states $x_2^j, x_3^j, x_4^j, x_5^j, x_7^j, x_8^j, x_9^j$ to state estimator i through communication network. Finally, subregion i obtains the states $x_1^i, x_2^i, x_3^i, x_4^i, x_5^i, x_6^i, x_7^i, x_8^i, x_9^i$ (i.e., attack-free subregion i in Fig. 3).

2) *Attack Type 1 occurs*: When attack Type 1 occurs, state estimator j also completes local estimation to obtain the node state data contained in subregion j. When attack Status 1 occurs, the data from subregion j to the corresponding local state estimator j is tampered, and nodes 2, 4 and 8 receive false data (i.e., Case 1: subregion j with false data in Fig. 3); When attack Status 2 occurs, the data from subregion j to the corresponding local state estimator j is blocked, so that nodes 2, 4 and 8 suffer from data losses (i.e., Case 2: subregion j with data losses in Fig. 3).

3) *Attack Type 2 occurs*: According to the above two Cases of attack Type 1, attack Type 2 also has two consequences. First, according to Case 1, i.e., the states x_2^j, x_4^j and x_8^j are corrupted with false data. When attack Status 1 occurs at this point, the data from state estimator j to state estimator i is tampered, the state x_7^i is further tampered, and state estimator i receives data of the states x_2^i, x_4^i, x_7^i, x_8^i containing false data. However, since subregion i contains nodes 2 and 4, the state x_2^i and x_4^i returns to normal through local estimation (i.e., Case 3: subregion i with false data in Fig. 3). Second, according to Case 2, i.e., the state data of x_2^j, x_4^j and x_8^j are lost. When attack Status 2 occurs at this point, the data transmission from state estimator j to the state estimator i is blocked, and state data of x_7^j is further lost, and state estimator i does not receive the states x_2^i, x_4^i, x_7^i and x_8^i. However, since subregion i contains nodes 2 and 4, the states x_2^i and x_4^i return to normal through local estimation (i.e., Case 4: subregion i with data losses in Fig. 3).

B *The exchanged state data description under hybrid attacks*

1) *Attack Type 1 occurs*: When attack Type 1 is caused by attack Status 1, the data from subregion j to the corresponding local state estimator j is tampered, so that the state $\hat{x}_{t1,k|k}^j$ is corrupted with false data. The corresponding model $\hat{x}_{s1,k|k}^{j,s1}$ can be described as [62]

$$\hat{x}_{t1,k|k}^{j,s1} = \varphi_k(T_k^1\hat{x}_{k|k}^j) + (1-\varphi_k)\hat{x}_{k|k}^j \tag{B.1}$$

where $t1$ represents attack Type 1, $s1$ represents attack Status 1, $T_k^1 = diag(\gamma_1, \gamma_2, \cdots, \gamma_n)$, $\gamma_i = d$ represents the i^{th} attacked communication channel, $d \in \mathbf{R}$ represents attack intensity, φ_k is a random variable with value of 0 or 1 (i.e., $\varphi_k = 1$ represents that FDIAs are successfully launched, $\varphi_k = 0$ otherwise).
When attack Type 1 is caused by attack Status 2, the data from subregion j to the corresponding local state estimator j is blocked, so that the state $\hat{x}_{t1,k|k}^j$ is lost. The corresponding model can be described as

$$\hat{x}_{t1,k|k}^{j,s2} = (1-\mu_k^1)\hat{x}_{k|k}^j \tag{B.2}$$

where $s2$ represents attack Status 2, μ_k^1 is a random variable with value of 0 or 1 (i.e., $\mu_k^1 = 1$ represents that DoSs are successfully launched, $\mu_k^1 = 0$ otherwise)
Therefore, when attack Type 1 is caused by attack Status 1 or attack Status 2, the attacked state $\hat{x}_{t1,k|k}^{j,a}$ of state estimator j is expressed as

$$\hat{x}_{t1,k|k}^{j,a} = (1-\mu_k^1)[\varphi_k(T_k^1\hat{x}_{k|k}^j) + (1-\varphi_k)\hat{x}_{k|k}^j] \tag{B.3}$$

2) *Attack Type 2 occurs*: When attack Type 2 is caused by attack Status 1, the data from state estimator j to state estimator i is tampered, so that the state $\hat{x}_{t2,k|k}^j$ is corrupted with false data. The corresponding model can be described as

$$\hat{x}_{t2,k|k}^{j,s1} = T_k^2\hat{x}_{t1,k|k}^{j,a} = T_k^2\{(1-\mu_k^1)[\varphi_k(T_k^1\hat{x}_{k|k}^j) + (1-\varphi_k)\hat{x}_{k|k}^j]\} \tag{B.4}$$

where $t2$ represents attack Type 2, T_k^2 is same as T_k^1.

When attack Type 2 is caused by attack Status 2, the data from state estimator j to state estimator i is blocked, so that the state $\hat{x}^{j}_{t2,k|k}$ is lost. The corresponding model can be described as

$$\hat{x}^{j,s2}_{t2,k|k} = (1-\mu^2_k)\hat{x}^{j,a}_{t1,k|k} \tag{B.5}$$

where μ^2_k is same as μ^1_k.

Therefore, when attack Type 2 is caused by attack Status 1 or attack Status 2, the attacked state $\hat{x}^{j,*}_{t2,k|k}$ of state estimator j is expressed as

$$\hat{x}^{j,*}_{t2,k|k} = (1-\mu^2_k)T^2_k\{(1-\mu^1_k)[\varphi_k(T^1_k\hat{x}^{j}_{k|k}) + (1-\varphi_k)\hat{x}^{j}_{k|k}]\} \tag{B.6}$$

References

[1] Zhang W, Li G, Guo F. Does carbon emissions trading promote green technology innovation in China? Appl Energy 2022;315:119012.

[2] Anasis J, Khalil M, Butenhoff C, Bluffstone R, Lendaris G. Optimal energy resource mix for the US and China to meet emissions pledges. Appl Energy 2019;238:92-100.

[3] Lai K, Illindala M, Subramaniam K. A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment. Appl Energy 2019;235:204-218.

[4] Zhao H, Jiang P, Chen Z, Ezeh C, Hong Y, Guo Y, Zheng C, Dzapo H, Gao X, Wu T. Improvement of fuel sources and energy products flexibility in coal power plants via energy-cyber-physical-systems approach. Appl Energy 2019;254:113554.

[5] Prinsloo G, Dobson R, Mammoli A. Synthesis of an intelligent rural village microgrid control strategy based on smartgrid multi-agent modelling and transactive energy management principles. Energy 2018;147:263-278.

[6] Hopuare M, Manni T, Laurent V, Maamaatuaiahutapu M. Investigating wind energy potential in Tahiti, French Polynesia. Energies 2022;15(6):1-13.

[7] Tan Z, Tan Q, Rong M. Analysis on the financing status of PV industry in China and the ways of improvement. Renew Sustain Energy Rev 2018;93:409-420.

[8] Zhang S, He Y. Analysis on the development and policy of solar PV power in China. Renew Sustain Energy Rev 2013;21:393-401.

[9] China Electricity Council. Report on analysis and forecast of China's power supply and demand in the first quarter of 2022. https://cec.org.cn/detail/index.html?3-308855.

[10] Liu J, Wang G, Zhao Z, Wei Q. Influence of large-scale new energy grid connection on China energy and power structure analysis model. Quarterly Journal of Indian Pulp and Paper Technical Association 2018;30(5):446-467.

[11] Qian T, Tang W, Wu Q. A fully decentralized dual consensus method for carbon trading power dispatch with wind power. Energy 2020;203:1-11.

[12] Li X, Jiang C, Du D, Li W, Fei M, Wu L. A novel state estimation method for smart grid under consecutive denial of service attacks. IEEE Syst J 2022;17(1):513-524.

[13] Saad A, Faddel S, Mohammed O. A secured distributed control system for future interconnected smart grids. Appl Energy 2019;243:57-70.

[14] Wang H, Meng A, Liu Y, Fu X, Cao G. Unscented Kalman Filter based interval state estimation of cyber physical energy system for detection of dynamic attack. Energy 2019;188:116036.

[15] Kurt M, Yilmaz Y, Wang X. Distributed quickest detection of cyber-attacks in smart grid. IEEE Trans on Information Forensics and Security 2018;13(8):2015-2030.

[16] Luo X, Wang X, Zhang M, Guan X. Distributed detection and isolation of bias injection attack in smart energy grid via interval observer. Appl Energy 2019;256:113703.

[17] Chen T, Cao Y, Chen X, Sun L, Zhang J, Amaratunga G. A distributed maximum-likelihood-based state estimation approach for power systems. IEEE Trans Instrum Meas 2021. DOI: 10.1109/TIM.2020.3024338.

[18] Robert M. Analysis of the cyber attack on the ukrainian power grid. Electricity Information Sharing and Analysis Center 2016.

[19] Condliffe J. Ukraines power grid gets hacked again, a worrying sign for infrastructure attacks. MIT Technology Review 2016.

[20] Orinoco Tribune. Breaking news: New attack on Venezuelan electrical grid produces localized short blackouts in Venezuela. https://orinocotribune.com/breaking-news-new-attack-on-venezuelan-electrical-grid-produces-localized-short-blackouts-in-venezuela/.

[21] An L, Yang G. Distributed secure state estimation for cyber physical systems under sensor attacks. Automatica 2019;107:526-538.

[22] Rana M, Bo R, Abdelhadi A. Distributed grid state estimation under cyber attacks using optimal filter and bayesian approach. IEEE Syst J 2021;15:1970-1978.

[23] Khalkhali MB, Vahedian A, Yazdi HS. Multi-target state estimation using interactive Kalman filter for multi-vehicle tracking. IEEE Trans Intell Transp Syst vol 2020;21:1131-1144.

[24] Ho C, Wu H, Chan S, Hou Y. A robust statistical approach to distributed power system state estimation with bad data. IEEE Trans Smart Grid 2020;11:517-527.

[25] Kurt MN, Yilmaz Y, Wang X. Secure distributed dynamic state estimation in wide-area smart grids. IEEE Trans Intell Transp Syst vol 2020;15:800-815.

[26] Du D, Li X, Li W, Chen R, Fei M, Wu L. ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks. IEEE Trans Syst Man Cybern Syst 2019;49:1698-1711.

[27] Du D, Zhu M, Li X, Fei M, Bu S, Wu L and Li K. A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems. J Mod Power Syst Clean Energy 2023;11(3);727-743.

[28] Li X, Jiang C, Du D, Wang R, Fei M, Li X, Tian Y. Optimization and control of cyber-physical power systems under dual-network interactive cascading failure. Control Eng Practice 2021;111:Article 104789.

[29] Zhang Y, Yagan O. Robustness of interdependent cyber-physical systems against cascading failures. IEEE Trans Autom Control 2020,65(2):711-726.

[30] Chen J, Liang G, Cai Z, Hu C, Xu Y, Luo F, Zhao J. Impact analysis of false data injection attacks on power system static security assessment. J Mod Power Syst Clean Energy 2016;4(3):496-505.

[31] ShangGuan X, He Y, Zhang C, Jin L, Jiang L, Wu M, Spencer J. Switching system-based load frequency control for multi-area power system resilient to denial-of-service attacks. Control Eng Practice 2021;107: Article 104678.

[32] Rahman M, Rana M, Pota H. Mitigation of frequency and voltage disruptions in smart grid during cyber-attack. J Control, Autom Elect Syst 2020;31:(2):412-421.

[33] Liu Y, Liu T, Sun H, Zhang K, Liu P. Hidden electricity theft by exploiting multiple-pricing scheme in smart grids. IEEE Trans Inf Forensic Secur 2020;15:2453-2468.

[34] Takiddin A, Ismail M, Zafar U, Serpedin E. Robust electricity theft detection against data poisoning attacks in smart grids. IEEE Trans. Smart Grid 2020;12(3):2675-2684.

[35] Lee L, Hu P. Vulnerability analysis of cascading dynamics in smart grids under load redistribution attacks. Int J Electr Power Energy Syst 2019;111:182-190.

[36] Zeng J, Bao R, McFarland M. Clean energy substitution: The effect of transitioning from coal to gas on air pollution. Energy Econ 2022;107:105816.

[37] Raza M, Lin B. Renewable energy substitution and energy technology impact in a transitional economy: A perspective from Pakistan. J Clean Prod 2022;360:132163.

[38] Wang R, Wen X, Wang X, Fu Y, Zhang Y. Low carbon optimal operation of integrated energy system based on carbon capture technology, LCA carbon emissions and ladder-type carbon trading. Appl Energy 2022;311:118664.

[39] Wang J, Yu Z, Zeng X, Wang Y, Li K, Deng S. Water-energy-carbon nexus: A life cycle assessment of post-combustion carbon capture technology from power plant level. J Clean Prod 2021;312:127727.

[40] Hu L, Wang Z, Han Q, Liu X. State estimation under false data injection attacks: Security analysis and system protection. Automatica 2018;87:176-183.

[41] Wang J, Chen C, Guan X. An overlapping distributed state estimation and detection method in smart grids. in: 2015 International Conference on Wireless Communications & Signal Processing (WCSP) 2015:1-5.

[42] Yang J, Zhang W, Guo F. Dynamic state estimation for power networks by distributed unscented information filter. IEEE Trans Smart Grid 2020;11(3):2162-2171.

[43] Yang W, Chen G, Wang X, Shi L. Stochastic sensor activation for distributed state estimation over a sensor network. Automatica 2014;50:2070-2076.

[44] Yang W, Yang C, Shi H, Shi L, G. Chen G. Stochastic link activation for distributed filtering under sensor power constraint. Automatica 2017;75:109-118.

[45] Persis C, Tesi P. Input-to-state stabilizing control under denial-of-service. IEEE Trans Autom Control, 2015; 60(11): 2930-2944.

[46] Varawala L, Hesamzadeh M, Dan G, Baldick R. A scalable formulation for look-ahead security-constrained optimal power flow. IEEE Trans Control Netw Syst 2022;9(1):138-150.

[47] Evangeline S, Rathikab P. Wind farm incorporated optimal power flow solutions through multi-objective horse herd optimization with a novel constraint handling technique. Expert Syst Appl 2022;194:116544.

[48] Xu J, Wang F, Lv C, Huang Q, Xie H. Economic-environmental equilibrium based optimal scheduling strategy towards wind-solar-thermal power generation system under limited resources. Appl Energy 2018;231:355-371.

[49] Tan Q, Ding Y, Ye Q, Mei S, Zhang Y, Wei Y. Optimization and evaluation of a dispatch model for an integrated wind-photovoltaic-thermal power system based on dynamic carbon emissions trading. Appl Energ 2019;253:113598.

[50] Tan Q, Ding Y, Zheng J, Dai M, Zhang Y. The effects of carbon emissions trading and renewable portfolio standards on the integrated wind-photovoltaic-thermal power-dispatching system: Real case studies in China. Energy 2021;222:1-15.

[51] Zhang D, Tang T, Ding Z, Qian F. Event-based resilient formation control of multiagent systems. IEEE Trans Cybern 2021;51:2490-2503.

[52] A. Ameli, A. Hooshyar, F. El-Saadany et al. Attack detection and identification for automatic generation control systems. IEEE Transactions on Power Systems 2018; 33(5): 4760-4774.

[53] X. Wang, X. Luo, M. Zhang et al. Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers. International Journal of Electrical Power and Energy Systems 2019;110:208-222.

[54] Huang J, Tang Y, Yang W, Li F. Resilient consensus-based distributed filtering: Convergence analysis under stealthy attacks. IEEE Trans Ind Inform 2020;16(7):4878-4888.

[55] H. Poor. An introduction to signal detection and estimation. New York: Springer-Verlag, 1994.

[56] Dayaratne T, Rudolph C, Liebman A, et al. Robust demand response for device scheduling under false data injection attacks in smart grid. 2020 IEEE PES Innovative Smart Grid Technologies Europe, The Hague, Netherlands, 2020.

[57] Musleh A, Chen G, and Dong Z. A survey on the detection algorithms for false data injection attacks in smart grids. IEEE Trans Smart Grid 2020;11(3):2218-2234.

[58] Luo X, Li Y, Wang X, et al. Interval observer-based detection and localization against false data injection attack in smart grids. IEEE Internet Things J 2021;8(2): 657-671.

[59] Debs AS, Larson RE. A dynamic estimator for tracking the state of a power system. IEEE Trans Power Apparatus Syst 1970;PAS-89(7):1670-1678.

[60] Yang W, Wang X, Shi H. Optimal consensus-based distributed estimation with intermittent communication. Int J Syst Sci 2011;42(9):1521-1529.

[61] Qin J, Wan Y, Yu X, Li F, Li C. Consensus-based distributed coordination between economic dispatch and demand response. IEEE Trans Smart Grid 2019;10(4):3709-3719.

[62] Yang W, Zhang X, Luo W, Zuo Z. Detection against randomly occurring complex attacks on distributed state estimation. Inf Sci: An Int J 2021;547:539-552.