Homomorphic Encryption based Resilient Distributed Energy Management under Cyber-attack of Micro-grid with Event-triggered Mechanism

Huifeng Zhang, *Senior Member, IEEE,* Chengqian Yu, Meilian Zeng, Tao Ye, Dong Yue, *Fellow, IEEE,*
Chunxia Dou, *Senior Member, IEEE,* Xiangpeng Xie, *Senior Member, IEEE,*
Gerhard P. Hancke, *Life Fellow, IEEE*

***Abstract*—Privacy disclosures and malevolent data intrusions targeting adversarial agents pose significant menaces to cyber-physical systems, a reality that extends to the intricate realm of micro-grid energy management. This paper proposes a homomorphic encryption based resilient distributed algorithm with an event-triggered mechanism to address this problem. Due to the potential information disclosure issue, exchange information is encrypted to an arbitrary neighbor and decrypted with a private key to protect agents. Considering the potential security attacks on adversary agents, an event-trigger based resilient distributed optimization with trusted agents (ETRDO-T) is proposed. It ensures the convergence of distributed algorithms, as well as relives the communication burden caused by homomorphic encryption. The simulation results, it can be seen that even under data attacks from malicious nodes, this method can effectively protect privacy information in information exchange while ensuring the convergence of energy management.**

***Index Terms*—malicious data attack, cyber-physic system, homomorphic encryption, event-trigger, distributed algorithm.**

I. Introduction

MICRO-GRIDS have attracted increasing attention due to their convenient utilization of diverse distributed energy resources, including wind power, solar energy, and battery storage [1], [2]. The economic operation of micro-grid is an important issue that many researchers are concerned about, while system security and stability are met in the cyber-physical environment. Conventionally, centralized control is utilized to collect all necessary information to a control center to solve the economic problem [3], [4], [5]. With the integration of distributed energy into microgrid infrastructure, the centralized approach overly depends on single-point cyber security and has tight limits on compute power and communication capacity [6]. A distributed approach offers superior scalability, flexibility, and resilience for micro-grid control, contrasting with the limitations of a centralized method. This paradigm shift not only enhances system performance but also aligns with the evolving demands of modern energy management. As microgrids become more prevalent, communication-based distributed control is becoming more and more crucial in networked microgrids for coordinating a large number of heterogeneous and spatially dispersed distributed energy resources. These distributed energy resources have improved efficiency, privacy-preserving, scalability, and reliability when compared to traditional centralized control [7]. Reference [8] develops a reinforcement learning technique to address load scheduling and energy management problems, creating a multiagent-based distributed energy management model.

Given the escalating frequency of cyber intrusions over recent decades, cyber security has attracted considerable attention during energy management of power systems, and a distributed smart-grid control mode, with its decentralized nature and extensive information communication, may be better suited to address the cyber-attack issue. By emphasizing scalar local cost functions, the scholarly literature [9] advances efforts in addressing the envisaged Byzantine resilient multi-agent optimization challenge. It also studies Byzantine perturbation-resistant optimization in the absence of a central coordinating agent and describes convex coefficient structures that can achieve the global

H. Zhang is with the institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Jiangsu Province, China, 210023, e-mail: zhanghuifeng_520@163.com (Corresponding author)

C. Yu is with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Jiangsu Province, China, 210023, e-mail: 1222056208@njupt.edu.cn

M. Zeng is with the institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Jiangsu Province, China, 210023, e-mail: meilianzeng659@163.com

T. Ye is with the institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Jiangsu Province, China, 210023, e-mail: 1020051524@njupt.edu.cn

D. Yue is with the institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Jiangsu Province, China, 210023, e-mail: medongy@vip.163.com (Corresponding author)

C. Dou is with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications,Jiangsu Province, China, 210023, e-mail: cxdou@ysu.edu.cn

X. Xie is with the institute of Advanced Technology, Nanjing University of Posts and Telecommunications,Jiangsu Province, China, 210023, e-mail: xiexiangpeng1953@163.com

G. P. Hancke is with Nanjing University of Posts and Telecommunications, Jiangsu Province, China, and also with University of Pretoria, South Africa, e-mail: g.hancke@ieee.org

objective. The literature [10] delves into the exploration of the distributed robust economic dispatch quandary within the realm of integrated energy systems amidst cyber assaults, develops a protocol that protects privacy, and propose a distributed resilient economic dispatch methodology for orchestrating energy management within integrated energy systems amidst the presence of deviant units. To describe the adversaries, cyber security, and system dynamics of consensus-based distributed economic dispatch, the literature [11] suggests an all-encompassing framework known as the resilient collaborative distributed energy management system. To enhance the robustness of the system against both non-collusive and collusive false data injection attacks that are prevalent, thereby fortifying its resilience, a reputation-driven distributed approach for detecting and mitigating such threats is proposed. In the literature [12], the issue of cyberattacks is addressed using a distributed optimum frequency control technique that is durable, resilient, and capable of dynamic power adjustment and quick frequency recovery. In [6], a modified attack resilient method with a weighted mean subsequence reduction algorithm is suggested to mitigate potential vulnerabilities stemming from false data injection attacks. In [13], it proposes an adaptive load frequency control method in which the controller gains can be readily changed on the basis of the intensity of the assault. Using IEC 62351–7:2017 network and system management as a foundation, the references [14] showcase the first microgrid security monitoring platform design and implementation. The literature [15] proposition involves a jump-style trial-and-discard protocol, coupled with the construction of an impulsive closed-loop model that is agnostic to the specifics of the attack model. This model aims to address issues of node congestion and mitigate Denial of Service (DoS) attacks effectively. This unified framework combines the effects of DoS attacks with the proposed protocol to ensure the necessary dynamic output feedback performance. Though cyber attack issues can be addressed by these above distributed methods, the information exchange process can lead to privacy information disclosure of energy investors and load consumers. Hence, this paper utilizes a homomorphic encryption technique to address this problem during information exchange. Employing this method serves as an efficacious means for safeguarding the privacy of a load/power agent within the realm of energy management. The study proposed by the authors in [16] presents a groundbreaking private collaborative distributed energy management system, employing a novel primal-dual subgradient distributed optimization methodology alongside a homomorphic encryption algorithm. It is then used for the distributed and private solution of the AC optimum power flow issue. In the literature [17], the issue of individual agent privacy leaking is addressed by a proposed distributed optimum power flow method that preserves privacy using partly homomorphic encryption. However, homomorphic encryption can bring high communication complexity during information exchange, affecting the optimal control efficiency in energy management.

It is well recognized that reducing the communication load issue with an event-triggered method may be rather successful [18], [19], [20], [21], [22], [23], [24]. Therefore, this paper integrates an event-triggered mechanism into an distributed optimization algorithm designed to alleviate the communication overhead stemming from the utilization of homomorphic encryption. In comparison to existing work in the literature, the principal contribution of this manuscript can be succinctly encapsulated as follows:

(1) With consideration of the privacy-preserving issue, a Pailler cryptosystem is employed to an improved information exchange process with additive homomorphism and multiplicative homomorphism, which encrypts agents' state information and decrypts its neighbors' information with a private key to ensure privacy security of each agent;

(2) To tackle the issue of cyber-attacks and communication overload in cyber-physical micro-grid systems, a robust distributed optimization method using an event-triggered mechanism is suggested. Based on the connected dominating set conditions, each agent can converge well with less communication number even under adversarial attacks;

(3) The suggested resilient distributed optimization technique has been shown to have both good convergence and optimality, and the tolerable effect of the adversarial attack is also deduced in a cyber-physical micro-grid system, which also guides the verification results in the simulation results.

The subsequent sections of this manuscript are structured as follows: Section II presents the cyber-physical systems oriented energy management framework for the micro-grid, and the proposed resilient distributed method is provided in section III. Section IV presents a resilient distributed optimization algorithm utilizing homomorphic encryption, augmented with an event-trigger mechanism. Convergence and optimality properties of this algorithm are rigorously established in Section V. Simulation outcomes are delineated in Section VI, followed by conclusive remarks in Section VII.

II. Cyber-Physical systems based energy management model of micro-grid

A. Cyber-network model with homomorphic encryption of information exchange

As the physical system based energy management develops into the cyber-physical systems, the privacy protection and cyber-attack issue can be very important issues for energy management, while those existing literatures seldom take both privacy protection and cyber-attack into consideration. To address this problem, this paper considers the homomorphic encryption for privacy protection and adversary nodes for cyber-attack in the cyber-physical systems based energy management model as follows:

1) Topology information of cyber-network: As illustrated in the literature [25], a cyber-network for electricity can be conceptualized through the framework of a graph $G =$

(v, e), where $v = \{v_1, v_2, \cdots, v_N\}$ represents the node set of cyber-network, $e \subseteq v \times v$ denotes the edge set of cyber-network, N is the number of nodes in cyber-network. For two arbitrary nodes i and $j \neq i$ in node set, $(i, j) \in e$ represents the connection state between node i and node j, it can be expressed with adjacent matrix $A = [a_{ij}]_{N \times N}$ as follows:

$$a_{ij} = \begin{cases} > 0, & (i,j) \in e \\ 0, & (i,j) \notin e \end{cases} \tag{1}$$

2) Homomorphic encryption of information exchange: In this study, the utilization of homomorphic encryption is implemented to enhance data privacy safeguards within smart grid systems, mitigating the risk of inadvertent disclosure of sensitive information during data exchange processes, especially during data aggregation and analysis, which can be computed without decryption, ensuring data security and privacy. Although quantum key distribution provides unconditional security in theory, its practical deployment faces technical and cost challenges, especially in large-scale network environments such as smart grids. In addition, quantum key distribution suffers from the side channel problem [26]. In order to protect the data while allowing complex computations, encryption methods need to satisfy both additive and multiplicative features. Homomorphic encryption has additive and multiplicative properties, leading to distributed optimization that can use homomorphic encryption, whereas quantum key distribution methods do not satisfy this property and their encryption process is more complex. In contrast, homomorphic encryption schemes are easier to implement. Homomorphic encryption schemes are able to perform complex analysis and processing tasks directly on the encrypted data without the need for key distribution and management, as is the case with quantum key distribution [27], thus simplifying the operational process and reducing the overall complexity of the system. Since the system load may involve the privacy of the load users, information security must be considered during the information processing. Homomorphic encryption is a cryptographic technique that maintains the encrypted state of a ciphertext while computation is performed on it. This means that even in the encrypted state, we can perform computation on the data without decrypting it. Generally, homomorphic encryption consists of additive homomorphism and multiplicative homomorphism. Since two ciphertexts can be combined to form a single plaintext, this is known as additive homomorphism, which can be described as follows:

$$D(E(a) \bigoplus E(b)) = a + b \tag{2}$$

where $E(\cdot)$ represents encryption primitive, $D(\cdot)$ denotes decryption primitive. Multiplicative homomorphism can be described similarly as follows:

$$D(E(a) \bigotimes E(b)) = a \times b \tag{3}$$

In this paper, Pailler cryptosystem is utilized for key generation, encryption and decryption, which can be referred in Literature [28].

B. Physical model of optimal operation

With consideration of networked graph, the node set v consists of n_g distributed power generators and n_d demand consumers, they can also be described as v_g and v_d, and then it has $v = v_g \cup v_d$. The economic cost of power generation at each unit $i \in v_g$ can be expressed in the following form:

$$C_i(P_{g,i}) = \alpha_{1,i} P_{g,i}^2 + \alpha_{2,i} P_{g,i} + \alpha_{3,i} \tag{4}$$

where $\alpha_{1,i}$, $\alpha_{2,i}$ and $\alpha_{3,i}$ represent the cost coefficients of power generation at ith power generator, $P_{g,i}$ denotes power output of ith power generator. In terms of demand, the utility function of load consumer $j \in v_d$ can be expressed in the following form:

$$U_j(P_{l,j}) = \begin{cases} \mu_j P_{l,j} - \zeta_j P_{l,j}^2, & P_{l,j} \leq \frac{\mu_j}{2\zeta_j} \\ \frac{\mu_j^2}{4\zeta_j}, & P_{l,j} > \frac{\mu_j}{2\zeta_j} \end{cases} \tag{5}$$

where $\beta_{1,j}$, $\beta_{2,j}$ and $\beta_{3,j}$ represent the utility coefficients of jth load consumer, $P_{l,j}$ denotes system load of jth consumer, μ_j and ζ_j are the cost efficients of jth consumer. Therefore, the societal well-being of a micro-grid can be articulated as follows:

$$\min F = \sum_{i \in v_g} C_i(P_{g,i}) - \sum_{j \in v_d} U_j(P_{l,j}) \tag{6}$$

In addition, $P_{g,i}$ and $P_{l,j}$ must satisfy some limits as:

$$\begin{cases} P_{g,i}^{min} \leq P_{g,i} \leq P_{g,i}^{max} \\ P_{l,j}^{min} \leq P_{l,j} \leq P_{l,j}^{max} \end{cases} \tag{7}$$

where $P_{g,i}^{min}$ and $P_{g,i}^{max}$ represent upper and lower limits output bounds of ith power generator, $P_{l,j}^{min}$ and $P_{l,j}^{max}$ denote the upper and lower limits adjustable load of jth load consumer. Furthermore, it is imperative to ensure equilibrium between the exigencies of load demand and the capacity of generation, thereby upholding the essential balance of power within the system:

$$\sum_{i \in v_g} P_{g,i} - P_{loss} = \sum_{j \in v_d} P_{l,j} \tag{8}$$

where P_{loss} represents the transmission loss, which can be defined as:

$$P_{loss} = \sum_{i \in v_g} \sum_{k \in v_g} B_{ik} P_{g,i} P_{g,k} + \sum_{i \in v_g} B_{0i} P_{g,i} + B_{00} \tag{9}$$

where B_{ik}, B_{0i} and B_{00} represent the coefficients of transmission loss.

C. The malicious data attack on adversary node

On the demand side of micro-grid, consumers' load information will upload to the load aggregator, which can be tampered by malicious data attack. Each load aggregator can be taken as a controller/cyber-physical node, some conditions must be satisfied during information exchange.

(1) **Privacy preservation:** Private state information x_i of arbitrary node i can not be delivered to other node $j (j \neq i)$, and node j also can not deliver its private state information

to other nodes including node i.

(2) **Three nodes:** The cyber-physical nodes include three types: normal nodes, trusted nodes and adversarial nodes. The attacker may be able to gain access to the normal nodes. Trusted nodes have an elevated level of safeguarding and are impervious to assault. Adversarial nodes contains Byzantine/malicious attackers, which know the update mechanism for normal nodes alongside the network architecture.

(3) **Connected dominating set:** Here are some definitions about the connected dominating set formed by trusted nodes in graph $G = (v, e)$:

Definition 1: A set C of graph $G = (v, e)$ can be called a connected dominating set if two conditions can be satisfied: 1) All nodes in C form a connected graph; 2) An arbitrary node $i \notin C$ has at least one neighbor in C.

Definition 2: A graph $G_1 = (v_1, e_1)$ can be called a subgraph of $G = (v, e)$, if $v_1 \subseteq v$ consists of mere trusted nodes and normal nodes, and its edge set $e_1 \subseteq e$ consists of all connections between trusted nodes and all directed edges originating from trusted nodes towards neighboring normal nodes.

III. Distributed optimization algorithm for cyber-physical economic dispatch model

Given the computational capabilities inherent to each power generator/load aggregator, the optimization algorithm may be crafted in a distributed manner without altering its intended essence. The Lagrangian function can be created as:

$$\begin{aligned} L_\lambda = &\sum_{i\in v_g} C_i(P_{g,i}) - \sum_{j\in v_d} U_j(P_{l,j}) + \lambda_1(\sum_{i\in v_g} P_{g,i} - P_{loss} \\ &- \sum_{j\in v_d} P_{l,j}) + \sum_{i\in v_g} \lambda^+_{2,i}(P^{min}_{g,i} - P_{g,i} + d^+_{i,1}) \\ &+ \sum_{i\in v_g} \lambda^-_{2,i}(P_{g,i} - P^{max}_{g,i} + d^-_{i,2}) \\ &+ \sum_{j\in v_d} \lambda^+_{3,j}(P^{min}_{l,j} - P_{l,j} + d^+_{j,3}) \\ &+ \sum_{j\in v_d} \lambda^-_{3,j}(P_{l,j} - P^{max}_{l,j} + d^-_{j,3}) \end{aligned} \tag{10}$$

where λ_1, $\lambda^+_{2,i}$, $\lambda^-_{2,i}$, $\lambda^+_{3,j}$ and $\lambda^-_{3,j} > 0$ represent the Lagrangian operators, $d^+_{i,1}$, $d^-_{i,2}$, $d^+_{j,3}$ and $d^-_{j,3} > 0$ denote the control parameters. The gradient can be deduced as:

$$\begin{cases} \frac{\partial L_\lambda}{\partial P_{g,i}} = \nabla C_i(P_{g,i}) + \lambda_1(1 - 2\sum_{k\in v_g} B_{ik}P_{g,k} - B_{0,i}) \\ -\lambda^+_{2,i} + \lambda^-_{2,i} \\ \frac{\partial L_\lambda}{\partial P_{l,j}} = -\nabla U_j(P_{l,j}) - \lambda_1 - \lambda^+_{3,j} + \lambda^-_{3,j} \end{cases} \tag{11}$$

Define λ_i as the marginal outlay entailed by each power generator, which can be explicated as follows:

$$\lambda_i = \frac{2\alpha_{1,i}P_{g,i} + b_{g,i}}{B_{0,i} + 2\sum_{k\in v_g} B_{i,k}P_{g,k} - 1}, \quad i \in v_g \tag{12}$$

where parameter $b_{g,i}$ denotes $\alpha_{2,i} - \lambda^+_{2,i} + \lambda^-_{2,i}$, and it must satisfy $B_{0,i} + 2\sum_{k\in v_g} B_{i,k}P_{g,k} \neq 1$. Define λ_j as the increment utility of load aggregator, it can be described as:

$$\lambda_j = \begin{cases} \mu_j + 2\zeta_j P_{l,j} + b_{l,j}, \quad P_{l,j} \leq \frac{\mu_j}{2\zeta_j} \ \& \ j \in v_d \\ 0, \quad P_{l,j} > \frac{\mu_j}{2\zeta_j} \ \& \ j \in v_d \end{cases} \tag{13}$$

where parameter $b_{l,j} = \lambda^-_{3,j} - \lambda^+_{3,j}$. Without loss of generality, it mainly considers the situation when $\lambda_i \neq 0$ $(i \in v_g)$ and $\lambda_j \neq 0$ $(j \in v_d)$.

IV. Homomorphic encryption based resilient distributed optimization algorithm with event-trigger mechanism

A. Homomorphic encryption based distributed privacy preservation algorithm

In the course of the information exchange phase within the framework of a distributed consensus algorithm, homomorphic encryption is employed to ensure the privacy security of each agent. For each agent $i \in N$ (N represents agents set) and its arbitrary neighbor $k \in N_i$ (N_i denotes neighbor set of agent i), the weight denoting the interaction intensity between agent i and agent k is defined as a_{ik}. Suppose state of agent i and agent k are λ_i and λ_k, public key and private key operator of agent i are ε_1 and ε_2, the confidential interaction protocol can be seen in Fig.1 as follows:

(1) Agent i will encrypt its negative state information $-\lambda_i$ with public key ε_1 as $\varepsilon_1(-\lambda_i)$, and send public key ε_1 to its neighbor agent k.

(2) Encrypt state information λ_k with public key ε_1 as $\varepsilon_1(\lambda_k)$, and compute the difference between two agents as:

$$\varepsilon_1(\lambda_k) + \varepsilon_1(-\lambda_i) = \varepsilon_1(\lambda_k - \lambda_i) \tag{14}$$

(3) Agent k generates weight parameter $a_{k\to i}$, which is merely known by agent k. Then, multiply it with the difference value as:

$$\varepsilon_1(a_{k\to i}(\lambda_k - \lambda_i)) = (\varepsilon_1(\lambda_k - \lambda_i))^{a_{k\to i}} \tag{15}$$

(4) Agent k transfer $\varepsilon_1(a_{k\to i}(\lambda_k - \lambda_i))$ to agent i, then agent i will decrypt it with private key D_1 and multiply the decrypted information with generated weight parameter $a_{i\to k}$, which is also merely known to agent i. The procedure can be described as:

$$\varepsilon_1(a_{k\to i}(\lambda_k - \lambda_i)) \xrightarrow{D_1} a_{k\to i}(\lambda_k - \lambda_i) \xrightarrow{a_{i\to k}} a_{i\to k}a_{k\to i}(\lambda_k - \lambda_i) \tag{16}$$

Here, the weight value a_{ik} can be designed as $a_{i\to k}a_{k\to i}$, and $\Delta\lambda_{ik}$ can be described as $a_{ik}(\lambda_k - \lambda_i)$.

B. Resilient distributed optimization with event-triggered mechanism

This paper introduces a robust distributed optimization framework utilizing homomorphic encryption, coupled with an event-triggered mechanism, to mitigate cybersecurity challenges in energy management. To relive the communication and computation burden caused by homomorphic

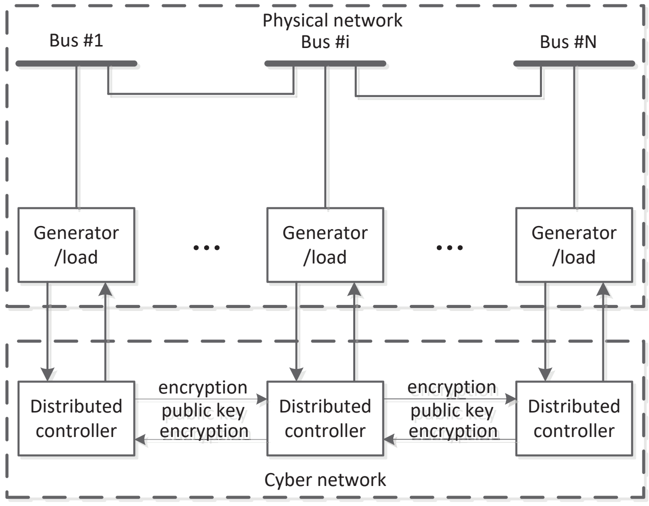


Fig. 1. The structure of cyber-physic network of micro-grid

encryption, the event-triggered mechanism is involved into the distributed optimization. To tackle with the cyber-attack on the malicious nodes, the malicious nodes are recognized firstly with the deviation between trusted nodes and current nodes during the coordinated optimization process, and then a resilient distributed optimization strategy can be made to avoid the cyber-attack on the malicious nodes.

Combined with distributed optimization strategy, here it can improve the iteration algorithm as:

$$\lambda_i(k+1) = \lambda_i(k) + \sum_{j\in N_i} a_{ij}(\lambda_j(k) - \lambda_i(k)) - \gamma_k \nabla f_i(\lambda_i(k)) \tag{17}$$

where γ_k represents step size parameter, the objective function $f_i(\lambda_i(k))$ of agent i satisfies $\sum_{i\in v_g} f_i(\lambda_i(k)) - \sum_{i\in v_d} f_i(\lambda_i(k)) = L_\lambda(\lambda_i(k))$, $\nabla f_i(\lambda_i(k))$ denotes the derivation of $f_i(\lambda_i(k))$. $P_{g,i}(k)$ and $P_{l,j}(k)$ can be deduced as follows:

$$\begin{cases} P_{g,i}(k+1) = \\ \quad \underset{P_{g,i}^{min} \le P_{g,i}(k) \le P_{g,i}^{max}}{\arg\min} [C_i(P_{g,i}(k)) - \lambda_i(k) P_{g,i}(k)],\ i \in v_g \\ P_{l,j}(k+1) = \\ \quad \underset{P_{l,j}^{min} \le P_{l,j}(k) \le P_{l,j}^{max}}{\arg\min} [\lambda_j(k+1) P_{l,j}(k) - U_j(P_{l,j}(k))],\ j \in v_d \end{cases} \tag{18}$$

The iteration algorithm of $P_{g,i}(k)$ and $P_{l,j}(k)$ and its convergence analysis have been provided in many existing publications. Then, the above iteration algorithm can be rewritten as follows:

$$\lambda_i(k+1) = \frac{1}{|R_i(k)|} \sum_{j\in R_i(k)} \lambda_j(k) - \gamma_k \nabla f_i(\lambda_i(k)) \tag{19}$$

where $|R_i(k)|$ represents the cardinality of set $R_i(k)$. Suppose set $R_i(k)$ is defined as:

$$R_i(k) = \{j|\lambda_i^{min} \le \lambda_j(k) \le \lambda_i^{max},\ j \in N_i \cup \{i\}\} \tag{20}$$

where λ_i^{min} and λ_i^{max} represent the minimum and maximum information bound of ith agent. For an arbitrary neighbor node j of node i, it participates iteration process merely when node j satisfies the requirement of set R_i^k. Here, this paper mainly focuses on the information exchange security under cyber-attack on adversary node. Event-triggered communication is taken into consideration, and it provides an ETRDO-T algorithm based on [29], trusting a subset of agents to fend off adversarial assaults. Each normal node in ETRDO-T is limited by its own boundaries and the states of its nearby trustworthy nodes. Meanwhile, each node sends its value to its neighbors if and only if the variation between its previous state and current state sent to its neighbors is greater than the preset threshold. Let it satisfy $\sum_{k=0}^{\infty} \gamma_k = \infty, \sum_{k=0}^{\infty} \gamma_k^2 < \infty$ and $\gamma_{k+1} \le \gamma_k$. $\tilde{\lambda}_{ij}(k)$ represents the state that agent i sends to its neighbor agent j at the k-th iteration of agent i. The trusted neighbor set of node i is denoted by $T_i = \{j|j \in N_i, j \in V_t\}$. In ETRDO-T, node i sorts $\tilde{\lambda}_{ji}(k)$ for all $j \in T_i \cup \{i\}$ and obtains the upper and lower limits states represented by $\tilde{\lambda}_i^{max}(k) = \max\ \{\tilde{\lambda}_{ji}(k)|j \in T_i \cup \{i\}\}$ and $\tilde{\lambda}_i^{min}(k) = \min\ \{\tilde{\lambda}_{ji}(k)|j \in T_i \cup \{i\}\}$, respectively. Combined with event-triggered mechanism and power balance deviation, it can deform the agents update formula as follows:

$$\begin{aligned} \lambda_i(k+1) = \lambda_i(k) + & \frac{1}{\left|\tilde{R}_i(k)\right|} \\ & \times \sum_{j\in\tilde{R}_i(k)} \left[\tilde{\lambda}_{ji}(k) - \lambda_i(k)\right] - \gamma_k \nabla f_i + \eta \xi_i(k) \\ = & \frac{1}{\left|\tilde{R}_i(k)\right|} \sum_{j\in\tilde{R}_i(k)} \lambda_j(k) - \gamma_k \nabla f_i \\ & + \frac{1}{\left|\tilde{R}_i(k)\right|} \sum_{j\in\tilde{R}_i(k)} e_{ji}(k) + \eta \xi_i(k) \end{aligned} \tag{21}$$

where $\tilde{R}_i(k)$ can be expressed as:

$$\tilde{R}_i(k) = \{j|\tilde{\lambda}_i^{min}(k) \le \tilde{\lambda}_{ji}(k) \le \tilde{\lambda}^{max}(k),\ j \in N_i \cup \{i\}\} \tag{22}$$

where $\tilde{\lambda}_{ji}(k)$ can be expressed as:

$$\tilde{\lambda}_{ji}(k) = \begin{cases} \lambda_j(k), & if \quad k \in k_i^t \\ \tilde{\lambda}_{ji}(k-1), & otherwise \end{cases} \tag{23}$$

where the deviation term $e_{ji}(k)$ can be describe as:

$$e_{ji}(k) = \begin{cases} \tilde{\lambda}_{ji}(k) - \lambda_j(k), & if \quad i \in N_j \\ 0, \quad otherwise \end{cases} \tag{24}$$

k_i^t represents the triggering time, it can be described as:

$$k_i^{t+1} = \min\{k > k_i^t| \parallel \tau_i(k) \parallel \ge a * e^{-b(k-k_0)}\} \tag{25}$$

where a and b denote the parameters of triggering function. With consideration of potential cyber-attack on adversary node, resilient distributed optimization algorithm can be improved on the basis of trusted nodes. Then let $e_i(k) =$

$\frac{1}{\left|\tilde{R}_i(k)\right|} \sum\limits_{j\in\tilde{R}_i(k)} e_{ji}(k) + \eta\xi_i(k)$, where η satisfied $0 < \eta < 1$ and $\xi_i(k)$ can be expressed as follows:

$$\begin{cases} \xi_i(k+1) = \sum\limits_{j\in N_i} a_{ij}\xi_j(k) + \Delta P(k) - \Delta P(k+1) \\ , \quad i \in v_g \\ \xi_i(k+1) = \sum\limits_{j\in N_i} a_{ij}\xi_j(k) + P_{L,i}(k+1) - P_{L,i}(k) \\ , \quad i \in v_d \end{cases} \tag{26}$$

where $\Delta P(k)$ denotes the power balance deviation, which can be described as:

$$\Delta P(k) = \sum_{i\in v_g} P_{g,i}(k) - P_{loss}(k) - \sum_{j\in v_d} P_{l,j}(k) \tag{27}$$

where $P_{loss}(k)$ can be calculated by transmission loss function of $P_{g,i}(k)$. By referring to [29], we know the transition matrix $\mathbf{M(k)} \in R^{N_0\times N_0}$ exists exactly. The above iteration algorithm of $\lambda_i(k)$ can be reformulated in a vector version as follows:

$$\mathbf{\Lambda}(k+1) = \mathbf{M}(k)\mathbf{\Lambda}(k) + \mathbf{E}(k) - \gamma_k\mathbf{F}^{'}(k) \tag{28}$$

where vector $\mathbf{\Lambda}(k) = [\lambda_1(k), \lambda_2(k), \cdots, \lambda_{N_0}]^T$, and matrix $\mathbf{M}(k) = [m_{ij}]_{N_0\times N_0}$, $\mathbf{E}(k) = [e_1(k), e_2(k), \cdots, e_{N_0}(k)]^T$, gradient vector $\mathbf{F}^{'}(k) = [\nabla f_1, \nabla f_2, \cdots, \nabla f_{N_0}]^T$. Then we can obtain that,

$$\begin{aligned} \Lambda(k+1) &= \mathbf{M}(k)\Lambda(k) - \gamma_k\mathbf{F}'(k) + \mathbf{E}(k) \\ &= \mathbf{M}(k)\mathbf{M}(k-1)\cdots\mathbf{M}(0)\Lambda(0) \\ &- \sum_{t=0}^{k}\mathbf{M}(k)\cdots\mathbf{M}(t+1)\gamma_t\mathbf{F}'(t) \\ &+ \sum_{t=0}^{k}\mathbf{M}(k)\cdots\mathbf{M}(t+1)\mathbf{E}(t) \\ &= \Phi(k,0)\Lambda(0) - \sum_{t=1}^{k+1}\Phi(k,t)\gamma_{t-1}\mathbf{F}'(t-1) \\ &+ \sum_{t=1}^{k+1}\Phi(k,t)\mathbf{E}(t-1) \end{aligned} \tag{29}$$

where $\Phi(k,t)$ is a backward product of $\mathbf{M}(k)$ and $\Phi(k,t)$ defines as follows:

$$\Phi(k,t) = \begin{cases} \prod\limits_{i=t}^{k}\mathbf{M}(i), & t < k \\ \mathbf{M}(k), & t = k \\ I_{n_0}, & t = k+1 \end{cases} \tag{30}$$

V. Convergence Analysis of Proposed Resilient Distributed Algorithm

A. Preparation for convergence analysis

By refering to [29] and [30], we present the following lemma forthwith.

Lemma 1 : If the presumption remains valid, under ETRDO-T, $\Phi(k,t)$ has the following attributes.

- For $\Phi(k,t)$, there holds $\lim_{k\geq t, k\to\infty}\Phi(k,t) = 1\psi^T(t)$, In this formulation, $\psi(t)$ represents a stochastic vector contingent upon the variable t.
- For any $\Phi(k,t)$, $|\Phi_{ij}(k,t) - \psi_i(t)| \leq (1-\varphi^{n_0})^{\left\lceil\frac{k-t+1}{n_0}\right\rceil}$.

By refering to [30], we make the following assumption: *Assumption* 2 : Consider a scenario wherein all actors, both non-faulty agents and faulty agents cease computing ∇f_i after some iteration $\bar{k}$, i.e., after $\bar{k}$ gradient is replaced by 0.

Remark 1 : Assumption 2 means that the values of all agents will not change after iteration $\bar{k}$. Then we can obtain that $\mathbf{E} = \mathbf{0}$ [31]. On the other hand, the values of all agents will not change implies that the threshold has no effect on the convergence of ETRDO-T. Therefore, in the later proof process, we assume that after iteration $\bar{k}$, the event trigger threshold is set to 0.

Since $k > \bar{k}, \nabla f_i = 0$ and $\mathbf{E} = \mathbf{0}$, for $k > \bar{k}$, according to lemma 1, applying restrictions to (3) yields on each sides, it can obtain:

$$\begin{aligned} &\lim_{k\to\infty}\Lambda(k+1) = \lim_{k\to\infty}\Phi(k,0)\Lambda(0) - \\ &\sum_{t=1}^{\bar{k}}\lim_{k\to\infty}\Phi(k,t)\gamma_{t-1}\mathbf{F}'(t-1) + \sum_{t=1}^{\bar{k}}\lim_{k\to\infty}\Phi(k,t)\mathbf{E}(t-1) \\ &= \mathbf{1}\psi^T(0)\Lambda(0) - \sum_{t=1}^{\bar{k}}\gamma_{t-1}\mathbf{1}\psi^T(t)\mathbf{F}'(t-1) + \sum_{t=1}^{\bar{k}}\mathbf{1}\psi^T(t)\mathbf{E}(t-1) \\ &= \left[\left\langle\psi^T(0), \Lambda(0)\right\rangle - \sum_{t=1}^{\bar{k}}\left\langle\psi^T(t), \gamma_{t-1}\mathbf{F}'(t-1) + \mathbf{E}(t-1)\right\rangle\right]\mathbf{1} \end{aligned} \tag{31}$$

The above illustrates where ETRDO-T's ultimate value will fall, it can be seen that all elements of $\lim_{k\to\infty}\Lambda(k+1)$ equal to a constant expressed as $y(\bar{k})$, where $y(\bar{k}) = \left\langle\psi^T(0), \Lambda(0)\right\rangle - \sum\limits_{t=1}^{\bar{k}}\left\langle\psi^T(t), \gamma_{t-1}\mathbf{F}'(t-1) + \mathbf{E}(t-1)\right\rangle$. According to (31), we have

$$\begin{aligned} y(\bar{k}) &= \left\langle\psi^T(0), \Lambda(0)\right\rangle \\ &\quad - \sum_{t=1}^{\bar{k}-1}\left\langle\psi^T(t), \gamma_{t-1}\mathbf{F}'(t-1) - \mathbf{E}(t-1)\right\rangle \\ &\quad - \left\langle\psi^T(\bar{k}), \gamma_{\bar{k}-1}\mathbf{F}'(\bar{k}-1) - \mathbf{E}(\bar{k}-1)\right\rangle \\ &= y(\bar{k}-1) - \left\langle\psi^T(\bar{k}), \gamma_{\bar{k}-1}\mathbf{F}'(\bar{k}-1) - \mathbf{E}(\bar{k}-1)\right\rangle \end{aligned} \tag{32}$$

We use $\{y(k)\}_{k=0}^{\infty}$ to represent the sequence generated by (32). In order to evaluate where ETRDO-T eventually converges, we propose the following lemma auxiliary proof.

Lemma 2 : Let $\{a_k\}_{k=0}^{\infty}$, $\{b_k\}_{k=0}^{\infty}$ and $\{c_k\}_{k=0}^{\infty}$ be nonnegative sequences. Suppose that $a_{k+1} \leq a_k - b_k + c_k, \forall k > 0$, and $\sum_{k=0}^{\infty} c_k < \infty$. Then, $\sum_{k=0}^{\infty} b_k < \infty$ and $\{a_k\}_{k=0}^{\infty}$ converges to a nonnegative value.

Proof : The demonstration of lemma 2 can be found in [30].

Lemma 3 : If the presumption remains valid, under ETRDO-T, $\forall x \in R, k \geq 0$, it can obtain the following inequality:

$$\begin{aligned}
&|y(k+1)-\lambda|^2 \leq |y(k)-\lambda|^2 + \\
&4\gamma_k L \sum\nolimits_{j\in V_n\cup V_t} \psi_j(k+1)\,|y(k)-\lambda_j(k)| \\
&-2\gamma_k \sum\nolimits_{j\in V_n\cup V_t} \psi_j(k+1)((f_j(y(k))-f_j(\lambda)) \\
&+2E(k)\sum\nolimits_{j\in V_n\cup V_t} \psi_j(k+1)\,(y(k)-\lambda) \\
&+\sum\nolimits_{j\in V_n\cup V_t} (\gamma_k \nabla f_j - e_j(k))^2
\end{aligned} \tag{33}$$

Proof: The proof of Lemma 3 can be demonstrated in Appendix A.

Lemma 4 : Let $u = \min_{i\in V_n\cup V_t}\lambda_i(0)$ and $U = \max_{i\in V_n\cup V_t}\lambda_i(0)$. If Assumption 1 holds, $\forall i \in V_n \cup V_t$, We have the following inequality

$$\begin{aligned}
&|y(k)-\lambda_i(k)| \leq N_0 \max\{|u|,|U|\}\left(1-\varphi^{N_0}\right)^{\left\lceil \frac{k}{N_0}\right\rceil} \\
&+N_0 L \sum_{t=1}^{k-1} \alpha_{t-1}\left(1-\varphi^{N_0}\right)^{\left\lceil \frac{k-t}{N_0}\right\rceil} + 2(\gamma_{k-1}L + E(k-1))
\end{aligned} \tag{34}$$

Proof: The lemma 4 can be proved in Appendix.B.

B. Convergence Analysis

Referring to [29], the collection of functions is supplied in order to assess where the final value of ETRDO-T will belong. $\mathcal{C}(\mu,\nu) = \{g(\lambda) | g(\lambda) = \sum_{i\in V_t}\beta_i f_i(\lambda), \beta_i \geq 0, \sum_{i\in V_t}\beta_i = 1, \sum_{i\in V_t} I\{\beta_i \geq \mu\} = \nu\}$. Then $Y(\mu,\nu)$ is defined as follows:

$$Y(\mu,\nu) = \cup_{g(\lambda)\in\mathcal{C}(\mu,\nu)} \arg\min_{x\in R} g(\lambda) \tag{35}$$

It should be point out that the idea of the proposition of lemma 3 and lemma 4 is inspired by [29] and [30]. However, the contents of lemma 3 and lemma 4 vary since we now have to take into account how event-triggered communication affects convergence because it was introduced in ETRDO-T. Let $\tilde{\lambda} \in Y(\mu,\nu)$, where $\mu \leq \varphi^d, \nu = N_2$. One has that $Y(\mu,\nu)$ is a convex set if $\mu \leq \varphi^d, \nu = N_2$. Based on Lemma 3, it can be concluded:

$$\begin{aligned}
&\left|y(k+1)-\tilde{\lambda}\right|^2 \leq \left|y(k)-\tilde{\lambda}\right|^2 + \\
&4\gamma_k L \sum\nolimits_{j\in V_n\cup V_t} \psi_j(k+1)\,|y(k)-\lambda_j(k)| \\
&-2\gamma_k \sum\nolimits_{j\in V_n\cup V_t} \psi_j(k+1)((f_j(y(k))-f_j(\lambda)) \\
&+2E(k)\sum\nolimits_{j\in V_n\cup V_t} \psi_j(k+1)\left(y(k)-\tilde{\lambda}\right) \\
&+\sum\nolimits_{j\in V_n\cup V_t} (\gamma_k \nabla f_j - e_j(k))^2
\end{aligned} \tag{36}$$

Then the following definitions are given:

$$\begin{cases}
a_k = \left|y(k)-\tilde{\lambda}\right|^2 \\
b_k = 2\gamma_k \sum\limits_{j\in V_n\cup V_t} \psi_j(k+1)((f_j(y(k))-f_j(\tilde{\lambda})) \\
c_k = 4\gamma_k L \sum_{j\in V_n\cup V_t} \psi_j(k+1)\,|y(k)-\lambda_j(k)| \\
\quad +2E(k)\sum_{j\in V_n\cup V_t} \psi_j(k+1)\left(y(k)-\tilde{\lambda}\right) \\
\quad +\sum_{j\in V_n\cup V_t} (\gamma_k \nabla f_i - e_j(k))^2
\end{cases} \tag{37}$$

Obviously, $a_{k+1} \leq a_k - b_k + c_k$, a_k and c_k are nonnegative sequence. Moreover, by referring to [29], we have b_k is also a nonnegative sequence. For lemma 2, it requires to discuss the boundedness of $\sum_{k=0}^{\infty} c_k$.

Lemma 5 : If the presumption remains valid, under ETRDO-T, it can obtain:

$$\sum\nolimits_{k=0}^{\infty} c_k < \infty \tag{38}$$

Proof: The proof of lemma 5 can be fined in Appendix C.

Combine (37), (38) and lemma 2, it can obtain $\sum_{k=0}^{\infty} b_k < \infty$, i.e.,

$$\sum_{k=0}^{\infty} 2\gamma_k \left[\sum_{j\in V_n\cup V_t} \psi_j(k+1)\left[f_j(y(k)) - f_j(\tilde{\lambda})\right]\right] < \infty \tag{39}$$

Since $\sum\limits_{k=0}^{\infty} \gamma_k = \infty$, suppose that $\lim\limits_{i\to\infty} y(k) \notin Y(\mu,\nu)$ and it can obtain:

$$\lim_{j\to\infty} f_j(y(k)) - f_j(\tilde{\lambda}) \neq 0 \tag{40}$$

contradicts with $\sum_{k=0}^{\infty} b_k < \infty$, namely, $\lim\limits_{i\to\infty} y(k) \in Y(\mu,\nu)$. Recall (31) and (32), it is known that $y(\bar{k})$ is the limit of $\lambda_i(k)$, $i \in V_n \cup V_t$. For $\{y(k)\}_{k=0}^{\infty}$, when $k \geq \bar{k}$, $y(k) = y(\bar{k})$. Therefore, it can obtain:

$$\lim\nolimits_{k\to\infty} |y(k) - \lambda_i(k)| = 0 \tag{41}$$

Thus, it can get $\lim\limits_{i\to\infty} \lambda_i(k) \in Y(\mu,\nu)$, which means that the convergence analysis is completed.

VI. CASE STUDY

The proposed scheme is implemented on an IEEE 9-bus system and an IEEE 39-bus system to testify its efficiency under privacy protection and cyber-attack environment. In these two experimental frameworks, the power generator and system load nodes are categorized into three distinct classes: trusted nodes, conventional nodes, and adversarial nodes, all nodes have been labeled with different color, which can be found in Fig.2 and Fig.3. Trusted nodes are set as known and adversary nodes are unknown. In the algorithm, each normal node will be constrained by its own boundaries as well as the state of neighboring trusted nodes. Also, each node sends values only to its neighbors and when the change in its previous state and current state from the values sent by its neighbors is greater than a preset threshold, the node will be considered as an attack node. Through the combination of event triggering mechanism and power balance bias, the agent update formula can be modified to protect private information while dealing with security attacks. The coordination procedure of ETRDO-T is executed employing homomorphic encryption technique to safeguard the privacy of individual nodes.

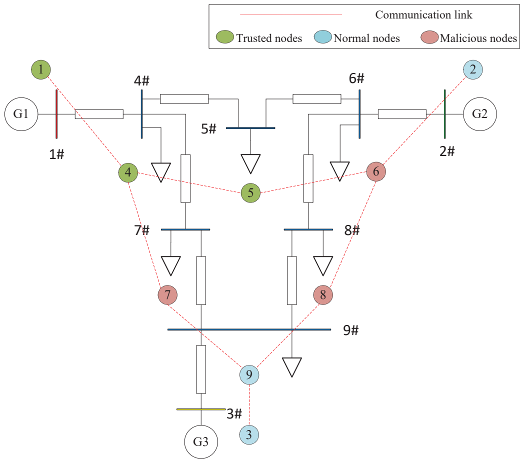


Fig. 2. The cyber-physical structure of IEEE 9-bus system

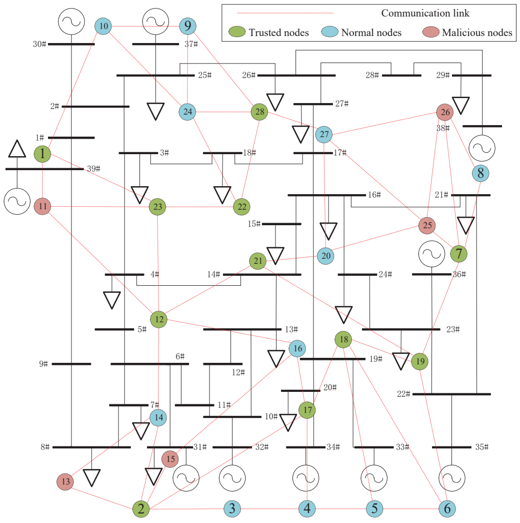


Fig. 3. The cyber-physical structure of IEEE 39-bus system

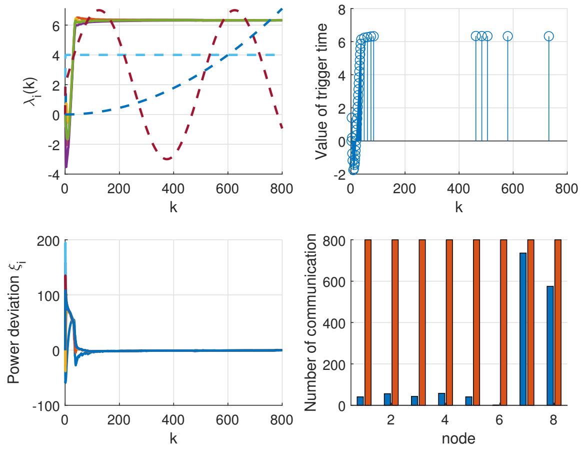


Fig. 4. The optimization process of proposed method on IEEE 9-bus system

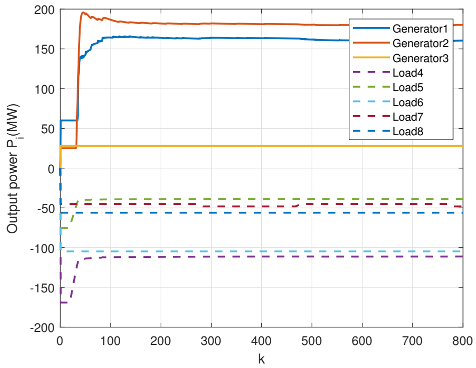


Fig. 5. The power output of proposed method on IEEE 9-bus system

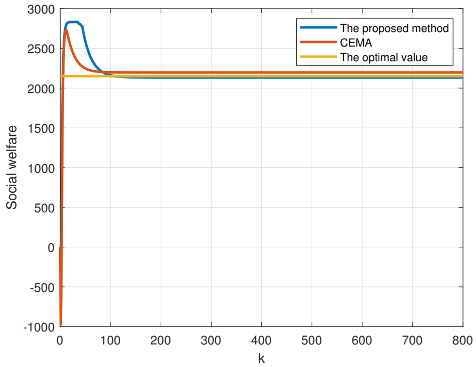


Fig. 6. The social welfare comparison with other methods on IEEE 9-bus system

A. The results analysis on IEEE 9-bus system

Due to cyber-attacks targeting adversary nodes, it is evident that the coordinated information, denoted as λ_i for adversary agents, fails to converge, in stark contrast to the effective convergence observed among the remaining five agents over the course of 100 iterations, as depicted in Fig.4. Combined with trusted agents, all the power generator agents and load demand agents can still finish distributed energy management tasks. The deviation control parameter ξ for each agent exhibits robust convergence to zero within 100 iterations, indicative of stringent adherence to all constraint limits. Within 100 iterations, the value of trigger time has stabilized, indicating that the states of the nodes in the system are close to the optimal solution and that changes in these states no longer trigger the preset thresholds. As a result, nodes no longer need to update their states or exchange information with neighboring nodes, indicating that the system has converged to a stable state. The number of information interactions under the event-triggered mechanism is significantly less than that under the traditional cycle, indicating that the event-triggered mechanism can sufficiently reduce the number of communications, save communication energy, and help improve the real-time reliability of the algorithm. In Fig.5, power output and system load can still converge within 100 iterations even under cyber-attack on adversary nodes, demand load is conceptualized as a negative power output for the sake of simplicity. In contrast to the prevailing energy management algorithm (CEMA) delineated in literature, [31], the proposed method can also perform well as CEMA even under a cyber-attack on adversary nodes, which is shown in Fig.6.

B. The results analysis on IEEE 39-bus system

The scalability of the suggested solution is additionally validated using the IEEE 39-bus system within the framework of this manuscript, and the optimization process is shown in Fig. 7. All trusted and normal nodes converge well, while the those malicious nodes cannot converge well. Since malicious nodes update their states differently from other nodes, their states cannot be optimized by normal local cost functions and neighbor relationships. Instead, their states may oscillate or keep increasing during the iteration process. In Fig. 7, five malicious nodes cannot converge throughout the optimization process. The power deviation of all trusted and normal nodes also converges to zero, and the total power mismatch still converges to zero, which indicates that all constraint limits are well satisfied. The method proposed in this paper employs an event-triggered mechanism, which triggers the communication based on the changes in the system state instead of communicating according to fixed time intervals, hence reducing the communication burden. It reduces the number of required communications and saves the communication energy compared to traditional periodic communication, ensuring the system's ability to converge in energy management and perform well even in the case of malicious data attacks by malicious nodes. In Fig.8, all the power outputs converge well within 500 iterations, including those of malicious nodes. Compared to CEMA, the approach delineated in this manuscript excels even amidst network assaults and also converges well to the optimum in Fig.9.

VII. Conclusion

With consideration of a cyber-attack on a cyber-physical system of distributed micro-grid energy management, this paper introduces an advanced algorithm for distributed optimization, leveraging homomorphic encryption techniques alongside a sophisticated event-triggered mechanism to ensure resilience. In microgrid energy management, homomorphic encryption is used to protect private information during information exchange. In addition, distributed algorithms combining homomorphic encryption algorithms and malicious data attacks from adversary nodes. This combined approach cannot only protects the privacy information, but also ensures that the convergence capability of energy management can be realized even in the case of malicious data attacks on the adversary nodes. Backed by theoretical underpinnings and corroborated by simulation outcomes, it has been ascertained that the suggested approach adeptly safeguards the integrity of energy administration amidst cyber intrusions targeting adversary nodes, safeguard each agent's personal information as well, and the incorporation of an event-triggered mechanism can effectively mitigate the

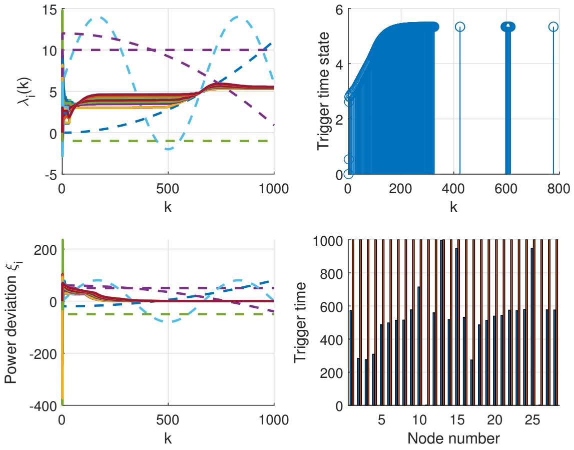


Fig. 7. The optimization process of proposed method on IEEE 39-bus system

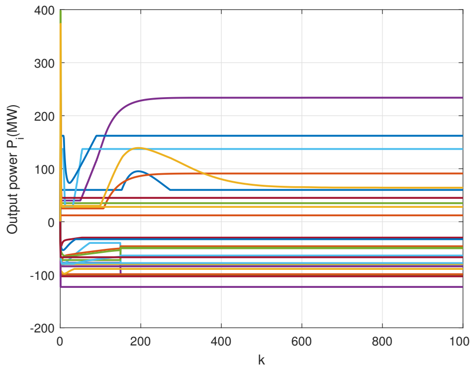


Fig. 8. The power output of proposed method on IEEE 39-bus system

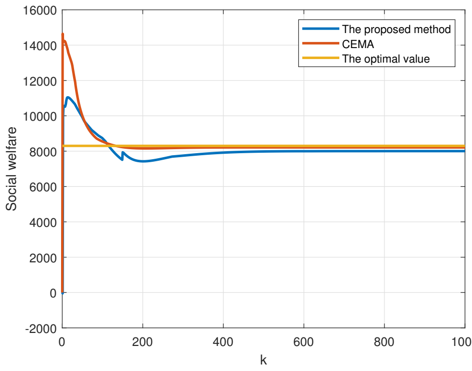


Fig. 9. The social welfare comparison with other methods on IEEE 39-bus system

communication overhead through the utilization of homomorphic encryption, and the proposed method still shows better performance and converges to the optimal value even under cyber-attacks on adversary nodes. The prevailing research endeavors primarily concentrate on distributed optimization algorithms fortified with homomorphic cryptographic techniques, designed to withstand attacks, while incorporating sophisticated event-triggered mechanisms, and future research will focus on exploring more efficient energy management approach for different cyber-attack models, communication networks, and better privacy-preserving techniques.

Appendix

A. Proof of lemma 3

Recall (31), it can obtain:

$$\begin{aligned}
&|y(k+1)-\lambda|^2 \\
&= \left|y(k) - \left\langle \psi^T(k+1), \gamma_k \mathbf{F}'(k) - \mathbf{E}(k) \right\rangle - \lambda\right|^2 \\
&= |y(k)-\lambda|^2 + \left|\left\langle \psi^T(k+1), \gamma_k \mathbf{F}'(k) - \mathbf{E}(k) \right\rangle\right|^2 \\
&- 2\left\langle \psi^T(k+1), \gamma_k \mathbf{F}'(k) - \mathbf{E}(k) \right\rangle (y(k)-\lambda)
\end{aligned} \tag{42}$$

For the second term on the right of inequality (42), we can make the following scaling:

$$\begin{aligned}
&\left|\left\langle \psi^T(k+1), \gamma_k \mathbf{F}'(k) - \mathbf{E}(k) \right\rangle\right|^2 \\
&\overset{a}{\leq} \left\|\psi^T(k+1)\right\|^2 \left\|\gamma_k \mathbf{F}'(k) - \mathbf{E}(k)\right\|^2 \\
&\overset{b}{\leq} \left\|\gamma_k \mathbf{F}'(k) - \mathbf{E}(k)\right\|^2 \\
&= \sum_{j \in V_n \cup V_t} \left(\gamma_k \nabla f_i - e_j(k)\right)^2
\end{aligned} \tag{43}$$

Inequality (a) follows from Cauchy-Schwarz inequality. Inequality (b) follows because $\left\|\psi^T(k+1)\right\|^2 = \sum_{j \in V_n \cup V_t} \psi_j^2(k+1) \leq \sum_{j \in V_n \cup V_t} \psi_j(k+1) = 1$.

Now consider the third term on the right of (42):

$$\begin{aligned}
&- 2\left\langle \psi^T(k+1), \gamma_k \mathbf{F}'(k) - \mathbf{E}(k) \right\rangle (y(k)-\lambda) \\
&= -2\gamma_k \sum_{j \in V_n \cup V_t} \psi_j(k+1) \nabla f_j \times (y(k)-\lambda) \\
&+ 2 \sum_{j \in V_n \cup V_t} \psi_j(k+1) e_j(k) (y(k)-\lambda)
\end{aligned} \tag{44}$$

By referring to [21], it provides the following inequality directly:

$$\begin{aligned}
&- 2\gamma_k \sum_{j \in V_n \cup V_t} \psi_j(k+1) \nabla f_j \times (y(k)-\lambda) \\
&\leq 4L\gamma_k \sum_{j \in V_n \cup V_t} \psi_j(k+1) \left|y(k) - \lambda_j(k)\right| \\
&- 2\gamma_k \sum_{j \in V_n \cup V_t} \psi_j(k+1) \left(f_j(y(k)) - f_j(\lambda)\right)
\end{aligned} \tag{45}$$

Combine (42), (43), (44), and (45), lemma 3 holds. ■

B. proof of lemma 4

Recall (29), for $k > 0$,

$$\begin{aligned}
\Lambda(k) = \Phi(k-1,0)\Lambda(0) - \sum_{t=1}^{k} \Phi(k-1,t)\gamma_{t-1}\mathbf{F}'(t-1) \\
+ \sum_{t=1}^{k} \Phi(k-1,t)\mathbf{E}(t-1)
\end{aligned} \tag{46}$$

Then each $\lambda_i(k)$ can be written as

$$\begin{aligned}
\lambda_i(k) =& \sum_{j=1}^{N_0} \Phi_{ij}(k-1,0)\lambda_j(0) \\
&- \sum_{t=1}^{k}\sum_{j=1}^{N_0} \Phi_{ij}(k-1,t)\left(\gamma_{t-1}\nabla f_j(t-1) - e_j(t)\right)
\end{aligned} \tag{47}$$

Recall (31), $y(k)$ can be written as

$$\begin{aligned}
y(k) =& \left\langle \psi^T(0), \Lambda(0) \right\rangle \\
&- \sum_{t=1}^{k} \left\langle \psi^T(t), \gamma_{t-1}\mathbf{F}'(t-1) - \mathbf{E}(t-1) \right\rangle \\
=& \sum_{j=1}^{N_0} \psi_j(0)\lambda_j(0) \\
&- \sum_{t=1}^{k}\sum_{j=1}^{N_0} \psi_j(t)\left(\gamma_{t-1}\nabla f_j(t-1) - e_j(t-1)\right)
\end{aligned} \tag{48}$$

Combine (47) and (48), it can obtain that

$$\begin{aligned}
&|y(k) - \lambda_i(k)| \\
=&\Bigg| \sum_{j=1}^{N_0} \left(\psi_j(0) - \Phi_{ij}(k-1,0)\right)\lambda_j(0) + \sum_{t=1}^{k}\sum_{j=1}^{N_0} \\
&\left(\Phi_{ij}(k-1,t) - \psi_j(t)\right)\left(\gamma_{t-1}\nabla f_j(t-1) - e_j(t-1)\right)\Bigg| \\
\leq& \left| \sum_{j=1}^{N_0} \left(\psi_j(0) - \Phi_{ij}(k-1,0)\right)\lambda_j(0) \right| \\
&+ \Bigg| \sum_{t=1}^{k}\sum_{j=1}^{N_0} \left(\Phi_{ij}(k-1,t) - \psi_j(t)\right) \\
&\times \left(\gamma_{t-1}\nabla f_j(t-1) - e_j(t-1)\right) \Bigg|
\end{aligned} \tag{49}$$

It first considers the first term to the right of the inequality, according to lemma 1, it can obtain:

$$\begin{aligned}
&\left|\sum_{j=1}^{N_0}\left(\psi_j(0)-\Phi_{ij}(k-1,0)\right)\lambda_j(0)\right|\\
\leq&\sum_{j=1}^{N_0}\left|\psi_j(0)-\Phi_{ij}(k-1,0)\right|\left|\lambda_j(0)\right|\\
\leq&\sum_{j=1}^{N_0}\left(1-\varphi^{N_0}\right)^{\left\lceil\frac{k}{N_0}\right\rceil}\max\left\{|u|,|U|\right\}\\
=&N_0\max\left\{|u|,|U|\right\}\left(1-\varphi^{N_0}\right)^{\left\lceil\frac{k}{N_0}\right\rceil}
\end{aligned}\tag{50}$$

Then, the second term on the right side of the inequality can obtain:

$$\begin{aligned}
&\left|\sum_{t=1}^{k}\sum_{j=1}^{N_0}\left(\Phi_{ij}(k-1,t)-\psi_j(t)\right)\left(\gamma_{t-1}\nabla f_j(t-1)-e_j(t-1)\right)\right|\\
\leq&\sum_{t=1}^{k-1}\sum_{j=1}^{N_0}\left|\Phi_{ij}(k-1,t)-\psi_j(t)\right|\left|\gamma_{t-1}\nabla f_j(t-1)-e_j(t-1)\right|\\
&+\Bigg|\left(\gamma_{k-1}\nabla f_i(k-1)-e_i(k-1)\right)\\
&-\sum_{j=1}^{N_0}\psi_j(t)\gamma_{k-1}\nabla f_j(k-1)-e_j(k-1)\Bigg|\\
\leq&\sum_{t=1}^{k-1}\sum_{j=1}^{N_0}|\Phi_{ij}(k-1,t)-\psi_j(t)|\gamma_{t-1}L+2(\gamma_{k-1}L+\Pi(k-1))\\
\leq&N_0L\sum_{t=1}^{k-1}\gamma_{t-1}\left(1-\varphi^{N_0}\right)^{\left\lceil\frac{k-t}{N_0}\right\rceil}+2(\gamma_{k-1}L+\Pi(k-1))
\end{aligned}\tag{51}$$

Where $\Pi(k)$ is the upper bound of $e_i(k)$. Combine (49), (50) and (51), lemma 4 holds.

C. proof of lemma 5

The Proof of lemma 5 can be presented as follows:

$$\begin{aligned}
\sum_{k=0}^{\infty}c_k=&\sum_{k=0}^{\infty}4\gamma_kL\sum_{j\in V_n\cup V_t}\psi_j(k+1)\left|y(k)-\lambda_j(k)\right|\\
&+\sum_{k=0}^{\infty}2E(k)\sum_{j\in V_n\cup V_t}\psi_j(k+1)\left(y(k)-\tilde{\lambda}\right)\\
&+\sum_{k=0}^{\infty}\sum_{j\in V_n\cup V_t}\left(\gamma_k\nabla f_j(k)-e_j(k)\right)^2
\end{aligned}\tag{52}$$

Recall remark 1, after $\bar{k}$ iterations, $\nabla f_i(k)=0$, $e_i(k)=0$ and $E(k)$ can be regarded as 0. Thus, it can obtain:

$$\begin{aligned}
&\sum_{k=0}^{\infty}\sum_{j\in V_n\cup V_t}\left(\gamma_k\nabla f_j(k)-e_j(k)\right)^2\\
=&\sum_{k=0}^{\bar{k}}\sum_{j\in V_n\cup V_t}\left(\gamma_k\nabla f_j(k)-e_j(k)\right)^2<\infty
\end{aligned}\tag{53}$$

Then, it can obtain:

$$\begin{aligned}
&\sum_{k=0}^{\infty}2E(k)\sum_{j\in V_n\cup V_t}\psi_j(k+1)\left|y(k)-\tilde{\lambda}\right|\\
=&\sum_{k=0}^{\bar{k}}2E(k)\sum_{j\in V_n\cup V_t}\psi_j(k+1)\left|y(k)-\tilde{\lambda}\right|<\infty
\end{aligned}\tag{54}$$

Since $\sum_{j\in V_n\cup V_t}\psi_j(k+1)=1$, by lemma 4, it can obtain for all $i\in V_n\cup V_t$.

$$\begin{aligned}
&\sum_{j\in V_n\cup V_t}\psi_j(k+1)\left|y(k)-x_j(k)\right|\\
\leq&\sum_{j\in V_n\cup V_t}\psi_j(k+1)\Bigg(n_0\max\left\{|u|,|U|\right\}\left(1-\varphi^{n_0}\right)^{\left\lceil\frac{k}{n_0}\right\rceil}\\
&+n_0L\sum_{t=1}^{k-1}\alpha_{t-1}(1-\varphi^{n_0})^{\left\lceil\frac{k-t}{n_0}\right\rceil}+2(\alpha_{k-1}L+\Pi(k-1))\Bigg)\\
=&n_0\max\left\{|u|,|U|\right\}\left(1-\varphi^{n_0}\right)^{\left\lceil\frac{k}{n_0}\right\rceil}\\
&+n_0L\sum_{t=1}^{k-1}\alpha_{t-1}(1-\varphi^{n_0})^{\left\lceil\frac{k-t}{n_0}\right\rceil}+2(\alpha_{k-1}L+\Pi(k-1))
\end{aligned}\tag{55}$$

By utilizing the fact that $\frac{1}{2}(x^2+y^2)\geq xy$, it can be concluded that

$$\sum_{k=0}^{\infty}4\alpha_kL\sum_{j\in V_n\cup V_t}\psi_j(k+1)\left|y(k)-x_j(k)\right|<\infty\tag{56}$$

Similar to that in [21], the comprehensive evidence is not included here. Combine (52), (53), (54) and (56), lemma 5 holds. ■

REFERENCES

[1] S. Raimondi Cominesi, M. Farina, L. Giulioni, B. Picasso, and R. Scattolini, "A two-layer stochastic model predictive control scheme for microgrids," *IEEE Transactions on Control Systems Technology*, vol. 26, no. 1, pp. 1–13, Jan 2018.

[2] H. Zhang, D. Yue, C. Dou, and G. P. Hancke, "Resilient optimal defensive strategy of micro-grids system via distributed deep reinforcement learning approach against fdi attack," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–11, 2022.

[3] Y. Wen, C. Y. Chung, X. Liu, and L. Che, "Microgrid dispatch with frequency-aware islanding constraints," *IEEE Transactions on Power Systems*, vol. 34, no. 3, pp. 2465–2468, 2019.

[4] H. Zhang, D. Yue, W. Yue, K. Li, and M. Yin, "Moea/d-based probabilistic pbi approach for risk-based optimal operation of hybrid energy system with intermittent power uncertainty," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–11, 2019.

[5] L. E. Sokoler, P. J. Dinesen, and J. B. Jørgensen, "A hierarchical algorithm for integrated scheduling and control with applications to power systems," *IEEE Transactions on Control Systems Technology*, vol. 25, no. 2, pp. 590–599, March 2017.

[6] W. Zhang, T. Qian, X. Chen, K. Huang, W. Tang, and Q. Wu, "Resilient economic control for distributed microgrids under false data injection attacks," *IEEE Transactions on Smart Grid*, pp. 1–1, 2021.

[7] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab, and A. Abusorrah, "Distributed control and communication strategies in networked microgrids," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2586–2633, 2020.

[8] E. Foruzan, L. Soh, and S. Asgarpoor, "Reinforcement learning approach for optimal distributed energy management in a microgrid," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5749–5758, 2018.

[9] L. Su and N. H. Vaidya, “Byzantine-resilient multiagent optimization,” *IEEE Transactions on Automatic Control*, vol. 66, no. 5, pp. 2227–2233, 2021.

[10] B. Huang, Y. Li, F. Zhan, Q. Sun, and H. Zhang, “A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks,” *IEEE Transactions on Industrial Informatics*, vol. 18, pp. 880–890, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:235848031

[11] Z. Cheng and M.-Y. Chow, “Resilient collaborative distributed energy management system framework for cyber-physical dc microgrids,” *IEEE Transactions on Smart Grid*, vol. 11, pp. 4637–4649, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:225048327

[12] Y. Liu, Y. Li, Y. Wang, X. Zhang, H. B. Gooi, and H. Xin, “Robust and resilient distributed optimal frequency control for microgrids against cyber attacks,” *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2021.

[13] Y. Zhang, C. Peng, C. Cheng, and Y.-L. Wang, “Attack intensity dependent adaptive load frequency control of interconnected power systems under malicious traffic attacks,” *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1223–1235, 2023.

[14] M. Karanfil, D. E. Rebbah, M. Debbabi, M. Kassouf, M. Ghafouri, E.-N. S. Youssef, and A. Hanna, “Detection of microgrid cyberattacks using network and system management,” *IEEE Transactions on Smart Grid*, vol. 14, no. 3, pp. 2390–2405, 2023.

[15] H. Yang, C. Peng, and Z. Cao, “Attack-model-independent stabilization of networked control systems under a jump-like tod scheduling protocol,” *Automatica*, vol. 152, p. 110982, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0005109823001358

[16] Z. Cheng, F. Ye, X. Cao, and M.-Y. Chow, “A homomorphic encryption based private collaborative distributed energy management system,” *IEEE Transactions on Smart Grid*, pp. 1–1, 2021.

[17] T. Wu, C. Zhao, and Y.-J. A. Zhang, “Privacy-preserving distributed optimal power flow with partially homomorphic encryption,” *IEEE Transactions on Smart Grid*, pp. 1–1, 2021.

[18] H. Zhang, Z. Chen, T. Ye, D. Yue, X. Xie, X. Hu, C. Dou, G. P. Hancke, and Y. Xue, “Security event-trigger-based distributed energy management of cyber-physical isolated power system with considering nonsmooth effects,” *IEEE Transactions on Cybernetics*, pp. 1–12, 2023.

[19] Y.-W. Wang, Y. Lei, T. Bian, and Z.-H. Guan, “Distributed control of nonlinear multiagent systems with unknown and nonidentical control directions via event-triggered communication,” *IEEE Transactions on Cybernetics*, vol. 50, no. 5, pp. 1820–1832, 2020.

[20] L. Ding, L. Y. Wang, G. Y. Yin, W. X. Zheng, and Q.-L. Han, “Distributed energy management for smart grids with an event-triggered communication scheme,” *IEEE Transactions on Control Systems Technology*, vol. 27, no. 5, pp. 1950–1961, 2019.

[21] S. Hu, D. Yue, X. Xie, Y. Ma, and X. Yin, “Stabilization of neural-network-based control systems via event-triggered control with nonperiodic sampled data,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 3, pp. 573–585, 2018.

[22] E. Tian, Z. Wang, L. Zou, and D. Yue, “Chance-constrained $h_{infinty}$ control for a class of time-varying systems with stochastic nonlinearities: The finite-horizon case,” *Automatica*, vol. 107, pp. 296–305, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0005109819302584

[23] H. Zhang, D. Yue, C. Dou, K. Li, and X. Xie, “Event-triggered multiagent optimization for two-layered model of hybrid energy system with price bidding-based demand response,” *IEEE Transactions on Cybernetics*, pp. 1–12, 2019.

[24] L. Ding, Q. Han, X. Ge, and X. Zhang, “An overview of recent advances in event-triggered consensus of multiagent systems,” *IEEE Transactions on Cybernetics*, vol. 48, no. 4, pp. 1110–1123, April 2018.

[25] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, “Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems,” *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2375–2385, 2015.

[26] M. Sasaki, “Quantum key distribution and its applications,” *IEEE Security & Privacy*, vol. 16, no. 5, pp. 42–48, 2018.

[27] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014, theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304397514004241

[28] M. Ruan, H. Gao, and Y. Wang, “Secure and privacy-preserving consensus,” *IEEE Transactions on Automatic Control*, vol. 64, no. 10, pp. 4035–4049, 2019.

[29] C. Zhao, J. He, and Q.-G. Wang, “Resilient distributed optimization algorithm against adversarial attacks,” *IEEE Transactions on Automatic Control*, vol. 65, no. 10, pp. 4308–4315, 2020.

[30] L. Su and N. Vaidya, “Byzantine multi-agent optimization: Part ii,” 2015.

[31] C. Zhao, J. He, P. Cheng, and J. Chen, “Consensus-based energy management in smart grid with transmission losses and directed communication,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2049–2061, 2017.

Huifeng Zhang (M’16-SM’22) received Ph.D. degree from Huazhong University of Science and Technology, Wuhan, China, in 2013. From 2014 to 2016, he was a Post-Doctoral Fellow with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. From 2017 to 2018, He was granted as visiting research fellow by China Scholarship Council to study in Queens University Belfast and University of Leeds, UK. He is currently an Associate Professor at the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His current research interest includes electrical power management, optimal operation of power system, distributed optimization, and multi-objective optimization.

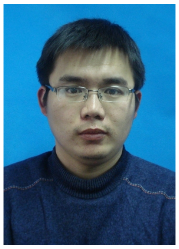
Chengqian Yu is currently pursuing the M.Sc. degree in control science and engineering with Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include event-triggered control and distributed optimization.

Meilian Zeng is currently pursuing the M.Sc. degree in electronic information major with Nanjing University of Posts and Telecommunications, Nanjing, China. Her research interests include privacy preservation and distributed optimization in power systems.

Tao Ye received the M.Sc. degree in control science and engineering with Nanjing University of Posts and Telecommunications, Nanjing, China, in 2023. His research interests include optimal operation of power system.

Dong Yue (SM'08-F'20) received the Ph.D. degree from the South China University of Technology, Guangzhou, China, in 1995. He is currently a Professor and the Dean with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China, and also a Changjiang Professor with the Department of Control Science and Engineering. His current research interests include analysis and synthesis of networked control systems, multiagent systems, optimal control of power systems, and internet of things. Prof. Yue is currently an Associate Editor of the IEEE Control Systems Society Conference Editorial Board and the International Journal of Systems Science.

Chunxia Dou (M'18-SM'21) received the B.S. and M.S. degrees in automation from the Northeast Heavy Machinery Institute, Qiqihaer, China, in 1989 and 1994, respectively, and the Ph.D. degree in Institute of Electrical Engineering from Yanshan University, Qinhuangdao, China, in 2005. Since 2016, she has been a Professor in Institute of Advanced Technology, Nanjing University of Posts and Telecommunications. Her current research interests include multi-agent based control, event-triggered hybrid control, distributed coordinated control, and multi-mode switching control and their applications in power systems, Microgrids and smart grids.



Xiangpeng Xie (M'16-SM'23) received the B.S. and Ph.D. degrees from Northeastern University, Shenyang, China, in 2004 and 2010, respectively, both in engineering. From 2012 to 2014, he was a Post-Doctoral Fellow with the Department of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan, China. He is currently a Professor with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His current research interests include fuzzy modeling and control synthesis, state estimations, optimization in process industries, and intelligent optimization algorithms.

Gerhard P. Hancke (M'88-SM'00-F'16) received the B.Sc. and B.Eng. degrees, in 1970, and the M.Eng. degree in Electronic Engineering, in 1973, from the University of Stellenbosch, South Africa, and the Ph.D. degree from the University of Pretoria, South Africa, in 1983. He is a Professor with the University of Pretoria, South Africa and recognized internationally as a pioneer and leading scholar in industrial wireless sensor networks research. He initiated and co-edited the first Special Section on Industrial Wireless Sensor Networks in the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS in 2009 and the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS in 2013. Prof. Hancke has been serving as an Associate Editor and Guest Editor for the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE ACCESS, and previously the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS. Currently, he is a Co-Editor-in-Chief for the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS.