ISA Transactions 149 (2024) 1–15

Contents lists available at ScienceDirect

ISA Transactions

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

Research article

Resilient distributed optimization for cyber–physical systems under adversarial environments: An event-based method

Zirui Liao [a,b,d], Shaoping Wang [a,b], Jian Shi [a,b,*], Ming Li [c], Yuwei Zhang [a,b], Zhiyong Sun [c]

[a] School of Automation Science and Electrical Engineering, Beihang University, Beijing, 100191, China
[b] Ningbo Institute of Technology, Beihang University, Ningbo, 315800, China
[c] Department of Electrical Engineering, Eindhoven University of Technology, Eindhoven, 5600MB, Netherlands
[d] Shenyuan Honors College, Beihang University, Beijing, 100191, China

ARTICLE INFO

Keywords:
Cyber–physical system
Distributed optimization
Event-triggering mechanism
Resilient algorithm

ABSTRACT

This work presents a resilient distributed optimization algorithm based on the event-triggering mechanism for cyber–physical systems (CPSs) to optimize an average of convex cost functions corresponding to multiple agents under adversarial environments. Two attack scenarios, including the f-total (each agent is affected by at most f malicious agents in the whole network) and the f-local (each agent is affected by at most f malicious agents in its in-neighbor set) attacks are considered. Subsequently, the convergence conditions under these two attack scenarios are provided, respectively, both of which guarantee that the state values of benign agents converge to a bounded error range. The optimality conditions are also presented by theoretical analysis, which guarantee that the state values of benign agents converge to a safety interval constructed by local optimal values under certain graph conditions, despite the misbehavior of malicious agents. In addition, four numerical examples are presented to show the effectiveness and superiority of the event-triggering resilient distributed optimization (RDO-E) algorithm. Compared to existing resilient algorithms, the proposed method achieves resilient distributed optimization with higher accuracy and less demanding communication overheads. Finally, by applying the proposed method to the multi-microgrid system, a resilient economic dispatch problem (REDP) is successfully solved, which validates the practical viability of the RDO-E algorithm.

1. Introduction

Cyber–physical systems (CPSs) have attracted extensive attention due to recent advances in automation science [1–5]. With highly integrated physical systems and cyber structures, CPSs represent the future generation of engineered systems [6,7]. The investigation of *distributed optimization* for CPSs has also become a research hotspot, which offers several advantages including higher scalability, stronger robustness, and higher efficiency in comparison to centralized patterns [8,9]. In the context of distributed optimization, multiple agents are equipped with local cost functions and aim to agree on a value that minimizes the average of these functions corresponding to one decision variable. Extensive scholarly work has been dedicated to the investigation and analysis of distributed optimization methods on the basis of consensus approach and subgradient descent technique [10–13]. In [10], a distributed subgradient descent (DGD) method was proposed to minimize a sum of convex cost functions corresponding to several nodes with a diminishing step-size. The work [11] extended the results in [10] for solving constrained distributed optimization problems in time-varying topologies. For fixed step-sizes, the work [12] developed a decentralized exact first-order algorithm (EXTRA). For second-order systems, a distributed Newton–Raphson algorithm was developed in [13] for addressing subgradient-based optimization problems.

However, the aforementioned distributed optimization methods are built on the predominant assumption that all agents seek for the global optimizer cooperatively, while the distributed nature and lack of global situational awareness make CPSs vulnerable to external malicious attacks or faults. Agents that may have suffered a malicious attack or may have encountered a fault would lose the capability of conducting the preset control protocols [14]. Typical malicious attack models include the f-total and f-local attack models [15,16]. Such attack models may undermine the benign agents in the network, destroy the achievement of distributed optimization among the benign individuals and even lead to the overall system paralysis [17]. As shown in Fig. 1, even a single malicious node has the ability to cause system crash. However, with the resilient algorithm (the word “resilient” represents a capability

* Corresponding author at: School of Automation Science and Electrical Engineering, Beihang University, Beijing, 100191, China.
E-mail addresses: by2003110@buaa.edu.cn (Z. Liao), shaopingwang@buaa.edu.cn (S. Wang), shijian@buaa.edu.cn (J. Shi), m.li3@tue.nl (M. Li), zhangyuwei@buaa.edu.cn (Y. Zhang), z.sun@tue.nl (Z. Sun).

https://doi.org/10.1016/j.isatra.2024.04.015
Received 1 September 2023; Received in revised form 12 April 2024; Accepted 13 April 2024
Available online 16 April 2024
0019-0578/

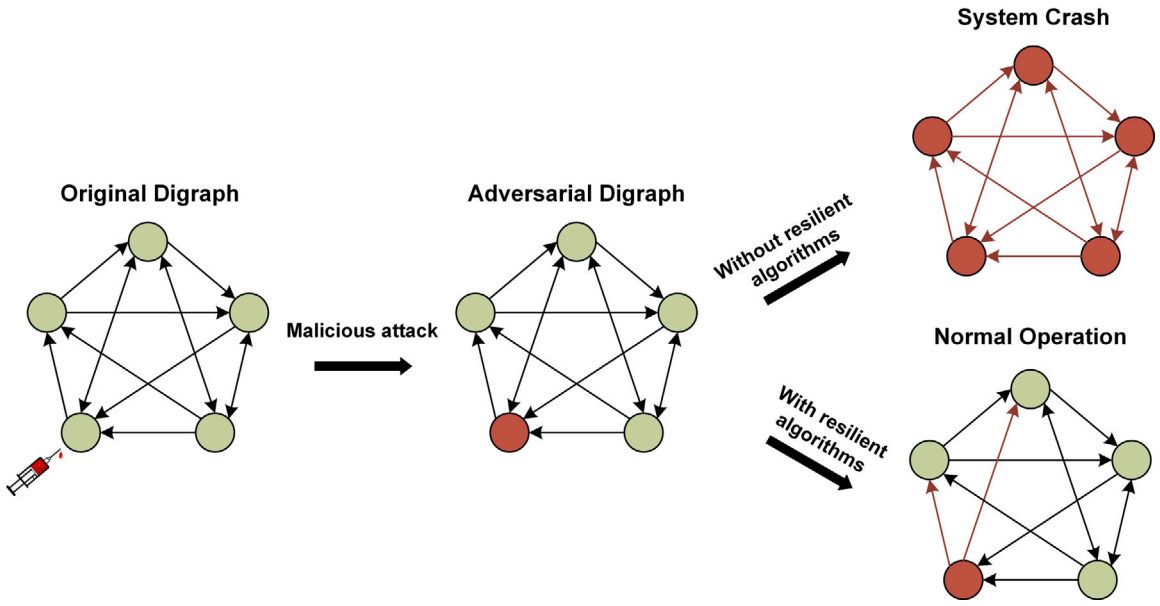


Fig. 1. A graphical example to illustrate the importance of resilient algorithms.

for agents to defend against malicious attacks and achieve a global objective), the benign agents can still function normally despite the influence of malicious agents. Thus, it is critical to study resilient control for CPSs by designing resilient algorithms, thereby achieving the desired goal in the presence of malicious attacks.

To overcome the impact of malicious attacks, the investigation of distributed optimization under adversarial environments was extended and the notion of *resilient distributed optimization* was further presented. Resilient distributed optimization ensures that the benign agents converge to the safety interval constructed by local optimal values under certain graph conditions, despite the misbehavior of a certain number of the malicious agents. In [18], the authors revealed that it is unattainable to design a distributed optimization algorithm that both finds optimal solutions without malicious attacks and is resilient under adversarial environments. Motivated by this essential constraint, the paper [18] combined the mean subsequence reduced (MSR) algorithm with subgradient descent technique and proposed a resilient version of the consensus-based distributed optimization algorithm to solve resilient distributed optimization problems. The work [19] considered distributed optimization problems of cyber–physical networks and presented a resilient consensus-based distributed optimization algorithm to deal with deception attacks. In [20], a novel filter method was introduced to relax the graph condition for achieving resilient distributed optimization. Trusted nodes were introduced in [21,22] and trust-based resilient distributed consensus algorithms were developed to overcome the impact of any number of malicious agents. Nevertheless, the aforementioned studies did not give full consideration to different attack scenarios, neither did they present complete convergence conditions under different attack models.

A common feature of most existing resilient distributed optimization strategies [18–20] is that they necessitate every agent in the network to interact with its neighbors frequently to access their current states for its own state update. This behavior costs massive communication resources and is sometimes unnecessary. In addition, it is quite difficult to guarantee that agents obtain the neighbors' information at each time step in practical scenarios. Motivated by these issues, this study seeks to mitigate the communication overheads for agents adopting the resilient distributed optimization algorithm [19] through an event-triggering mechanism. Event-based protocols have been widely applied to tackle miscellaneous control problems in the absence of malicious attacks [23–26]. Under adversarial environments, the paper [27] designed two event-triggering distributed protocols based on the idea of MSR to reduce communication overheads and achieve consensus. In the presence of false data injection threats, the authors in [28] developed an event-triggering output feedback model predictive control (MPC) scheme to provide valid system states for nonlinear MASs. Among these promising studies, the event-triggering mechanism is shown to be effective in reducing communication overheads for agents in the presence of malicious attacks. In the context of resilient distributed optimization, the CPS undertakes extensive communication overheads since the MSR algorithm and subgradient descent algorithm need to be implemented simultaneously. Therefore, it is essential to design appropriate event-based algorithms for resilient distributed optimization and reduce the heavy communication burden of CPSs.

Inspired by the above observations, this study proposes a resilient distributed optimization algorithm based on the event-triggering mechanism. The algorithm is designed to filter out some suspected state values sent from the nodes' in-neighbor set at each iteration. Two attack models are considered and their convergence and optimality properties are analyzed, respectively. The simulation results show that the proposed method is more accurate and consumes less communication resource than other event-based algorithms. To the best of our knowledge, this is the first attempt to adopt the event-triggering mechanism and the idea of attack tolerance to address the resilient distributed optimization problem, when the network is subject to the attack of malicious agent injection. The main contributions of this study are presented in the following:

1. With the introduction of a discrete-time event-based protocol, a novel event-triggering resilient distributed optimization (RDOE) algorithm is developed. Different from the resilient algorithms [16,27] that merely focus on the consensus problem, the proposed method guarantees that the benign agents converge to the safety interval constructed by local optimal values despite the influence of the malicious agents, thereby achieving resilient distributed optimization. Both convergence and optimality of the benign agents are ensured with reduced communication overheads.
2. Compared with the resilient distributed optimization methods [18–20], wherein only partial convergence conditions are stated, this study presents the necessary and sufficient convergence conditions for CPSs under f-total and f-local attack models. The optimality conditions under these two attack models are also implemented, respectively. These results enhance theoretical completeness.

Table 1
Nomenclature.

Variable	*Meaning*
$\mathcal{G}$	Digraph
$\mathcal{V}$	Node set
$\mathcal{E}$	Edge set
$\mathcal{V}_i^+$	Set of in-neighbors for agent i
$\mathcal{V}_i^-$	Set of out-neighbors for agent i
$\mathcal{Y}_S^r$	Subset of all agents possessing at least r in-neighbors outside $S \subseteq \mathcal{V}$
$f_i(x)$	Local cost function for agent i
$d_i(x)$	Subgradient of $f_i(x)$
$x_i(k)$	State value of agent i at time step k
$u_i(k)$	Control input of agent i at time step k
γ	Control gain
$\theta_{ij}(k)$	Weight of edge (j,i)
$\alpha(k)$	Step size at time step k
β	Lower bound of non-zero $\theta_{ij}(k)$
$\hat{x}_j(k)$	Auxiliary variable of agent j at time step k
c_0, c_1, δ	Positive scalars associated with triggering threshold
$\mathcal{M}$	Set of malicious agents
$\mathcal{B}$	Set of benign agents
f	Upper bound on the number of malicious agents
$\mathcal{R}_i^+(k)$	Set of retained in-neighbors for agent i after the RDO-E algorithm
c	Error range

3. In contrast to the existing distributed optimization algorithms [10,19] and event-based algorithms [23,27], the proposed RDO-E algorithm guarantees that the benign agents achieve resilient distributed optimization with a lower relative error and fewer trigger times. Furthermore, the proposed method is applicable to the resilient economic dispatch problem (REDP) in multi-microgrid systems, and the effectiveness of the RDO-E algorithm is validated by numerical results.

The other sections of this paper are arranged as follows. Section 2 introduces some preliminaries on graph theory, together with formulating the resilient distributed optimization problem. Section 3 presents the main results for achieving resilient distributed optimization under f-total and f-local attack models. We validate the main results through four numerical examples in Section 4. Eventually, Section 5 concludes this paper and prospects future research directions.

The notations used for this paper are listed in Table 1.

2. Preliminaries and problem formulation

2.1. Preliminaries on graphs

Consider a CPS described by a digraph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. The vertex set (or node set) is denoted as $\mathcal{V} = \{1, \ldots, n\}$, with $|\mathcal{V}|$ being its cardinality. The edge $(j,i) \in \mathcal{E}$ indicates that there exists a connection from agent j to agent i, which also implies that agent j is in the in-neighbor set $\mathcal{V}_i^+ = \{j \in \mathcal{V} | (j,i) \in \mathcal{E}\}$ of agent i. Moreover, we denote the out-neighbor set of agent i as $\mathcal{V}_i^- = \{j \in \mathcal{V} | (i,j) \in \mathcal{E}\}$.

In the context of resilient distributed optimization, two essential notions are set reachability and graph robustness, which are presented as follows, respectively.

Definition 1 ([15]). Consider a digraph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ and a nonempty subset $S \subseteq \mathcal{V}$. S is r-reachable if $\exists\, i \in S$ such that $\left|\mathcal{V}_i^+ \setminus S\right| \geq r$, where $r \in \mathbb{Z}_{>0}$.

Definition 2 ([15]). Consider a digraph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ and a nonempty subset $S \subseteq \mathcal{V}$. S is (r,s)-reachable if given $\mathcal{Y}_S^r = \left\{i \in S : \left|\mathcal{V}_i^+ \setminus S\right| \geq r\right\}$, then $\left|\mathcal{Y}_S^r\right| \geq s$, where $r, s \in \mathbb{Z}_{>0}$.

The notions of r-reachable and (r,s)-reachable set can be extended to graphs and the following definitions are derived.

Definition 3 ([16]). Consider a digraph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. $\mathcal{G}$ is r-robust if for each pair of nonempty, disjoint subsets $S_1, S_2 \subseteq \mathcal{V}$, at least one of them is r-reachable, where $r \in \mathbb{Z}_{>0}$.

Definition 4 ([16]). Consider a digraph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with n ($n \geq 2$) agents. $\mathcal{G}$ is (r,s)-robust if at least one of the conditions given below is satisfied specific to each pair of nonempty, disjoint subsets $S_1, S_2 \subseteq \mathcal{V}$:

$$(1)\left|\mathcal{Y}_{S_1}^r\right| = |S_1|, \quad (2)\left|\mathcal{Y}_{S_2}^r\right| = |S_2|, \quad (3)\left|\mathcal{Y}_{S_1}^r\right| + \left|\mathcal{Y}_{S_2}^r\right| \geq s,$$

where $r \in \mathbb{Z}^+$, $1 \leq s \leq n$, $\mathcal{Y}_{S_p}^r$ ($p = 1,2$) is the node set in S_p with at least r in-neighbors outside of S_p, which is expressed as $\mathcal{Y}_{S_p}^r = \left\{i \in S_p : \left|\mathcal{V}_i^+ \setminus S_p\right| \geq r\right\}$.

2.2. Formulation of distributed optimization problem

Before the problem formulation, we firstly present some basic properties for local cost functions. Consider a locally Lipschitz function $f_i(x) : \mathbb{R} \to \mathbb{R}$. The subgradient $d_i(x)$ of $f_i(x)$ satisfies

$$f_i(x) + d_i(x)\left(x' - x\right) \leq f_i\left(x'\right), \ \forall x' \in \mathcal{D}. \tag{1}$$

where $\mathcal{D} = \{x \in \mathbb{R} | f_i(x) < \infty\}$. Furthermore, $f_i(x)$ is said to be convex if

$$f_i(\omega x + (1-\omega)y) \leq \omega f_i(x) + (1-\omega) f_i(y), \ \forall x, y \in \mathbb{R}, \ \omega \in [0,1]. \tag{2}$$

Assumption 1. Each local cost function $f_i(x)$, $\forall i \in \mathcal{V}$ is locally Lipschitz and convex with bounded subgradients.

Consider a CPS comprised by n agents and described by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. For each agent $i \in \mathcal{V}$, its state update follows

$$x_i(k+1) = x_i(k) + u_i(k), \tag{3}$$

where $k \in \mathbb{Z}_{\geq 0}$, $x_i(k) \in \mathbb{R}$ is the state value and $u_i(k)$ is the control input. Assume that all agents endeavor to tackle the following optimization problem cooperatively:

$$\arg\min_x F(x) = \min \frac{1}{n} \sum_{i=1}^{n} f_i(x), \ i \in \mathcal{V}. \tag{4}$$

Note that each $f_i(x)$ in (4) satisfies Assumption 1. One common subgradient-based approach to solve problem (4) is

$$u_i(k) = \gamma \sum_{j \in \mathcal{V}_i^+(k)} \theta_{ij}(k)(x_j(k) - x_i(k)) - \alpha(k) d_i(k), \tag{5}$$

where γ is a control gain, $\alpha(k)$ is the step size, $d_i(k)$ is a subgradient for local cost function $f_i(x)$, which is well-defined due to Assumption 1, $\theta_{ij}(k)$ is the weight of edge (j,i).

Remark 1. Note that the problem (4) is an unconstrained distributed optimization problem. Nevertheless, some assumptions and conditions in the manuscript can be regarded as implicit constraints. For example, Assumption 1 requires each local cost function to be locally Lipschitz and convex, while Assumption 3 poses a constraint on the step size. In addition, the condition that the network should satisfy a certain attack model is also an implicit constraint. All these constraints are essential for implementing the proposed algorithm.

Remark 2. Although all agents in the CPS are modeled in one-dimensional space, the proposed algorithm can still be extended to higher-dimensional space with the help of Kronecker product. Some other tools like the convex analysis may also be required. Furthermore, the paper [29] provides an alternative way to achieve higher-dimensional resilient distributed optimization with the introduction of a distance filtering step. In three-dimensional space, it was proved in [29] that the state values of benign agents will asymptotically converge to a ball, while our extension ensures the asymptotic convergence to a hyperrectangle. Extending existing results to higher-dimensional space is also one of our next work plans.

To achieve distributed optimization under adversarial environments, the following assumptions are made.

Assumption 2. The edge weight satisfies $\theta_{ij}(k) \in [\beta, 1)$ if $(j,i) \in \mathcal{E}$ and otherwise $\theta_{ij}(k) = 0$, $\forall i, j \in \mathcal{V}$, where $\beta \in (0,1)$ refers to a fixed lower bound. Furthermore, we have $\theta_{ii}(k) = 1 - \gamma \sum_{j \in \mathcal{V}_i^+} \theta_{ij}(k)$, thus the control gain satisfies $\gamma \in (0, \beta / \max_i(\sum_{j \in \mathcal{V}_i^+} \theta_{ij}))$.

Assumption 3. The step size $\alpha(k)$ is diminishing and satisfies $\lim_{k\to\infty} \alpha(k) = 0$, $\sum_{k=1}^{\infty} \alpha(k) = \infty$.

Remark 3. The aforementioned three assumptions are essential for convergence and optimality analysis. Assumption 1 ensures that the subgradient of each cost function is upper bounded by some constant, which plays an important role in achieving consensus. Assumption 2 guarantees sufficient interaction between agents and avoids the situation where weights asymptotically vanish. Regarding Assumption 3, the condition $\lim_{k\to\infty} \alpha(k) = 0$ ensures the convergence of the CPS, while the condition $\sum_{k=1}^{\infty} \alpha(k) = \infty$ ensures the optimality of the CPS. A common choice for the step size $\alpha(k)$ is $\alpha(k) = \frac{1}{k+1}$, which satisfies all the conditions in Assumption 3. In fact, Assumptions 1–3 have been widely adopted in [18–20] to study resilient distributed optimization problems. Thus, they are also introduced in our work.

Note that frequent information transmission among agents in the network is required to implement the distributed optimization algorithm (5). For distributed optimization under adversarial environments, the communication burden will become heavier since extra resilient algorithms should be considered to overcome the influence of malicious attacks, and more communication resources will be consumed at each time step. Thus, the focus of this work is to design a resilient distributed optimization algorithm that consumes less demanding communication resources. Specifically, the event-triggering mechanism is introduced to guarantee that the information interaction among benign agents occurs only when specific conditions are satisfied.

2.3. Event-triggering mechanism

Various methods have been adopted to solve resilient distributed optimization problems in recent decades [19–21]. In these studies, agents in the network must communicate with their in-neighbors and update their state values according to the received information at each time step. Nevertheless, the frequent transmission of information among agents is sometimes unattainable due to resource limitations. To optimize network resource utilization, we develop the following event-triggering control protocol:

$$u_i(k) = \gamma \sum_{j \in \mathcal{V}_i^+(k)} \theta_{ij}(k) \left(\hat{x}_j(k) - x_i(k)\right) - \alpha(k) d_i(k), \tag{6}$$

where $\hat{x}_j(k) = x_j(t_l^j)$, $k \in [t_l^j, t_{l+1}^j)$, with $\{t_l^j\}$ being the sequence of the communication time for agent j. $\hat{x}_j(k) = x_j(t_l^j)$ is an auxiliary variable, which refers to the state value sent by agent j at the last communication time. Given the initial states $x_i(0)$ and $\hat{x}_j(0) = x_j(0)$, the distributed optimization will be achieved through the iteration of time step k. Note that the update of auxiliary variable $\hat{x}_j(k)$ depends on the event-triggering mechanism, and $\{t_l^j\}$ also depends on the trigger function. The method is designed in the discrete-time domain.

Now we introduce the design of the event-triggering mechanism and corresponding trigger function. The mechanism is applied to reduce the communication burden with respect to agents in the CPS. The benign agent i updates its state from $x_i(k)$ to $x_i(k+1)$ with the consideration of the auxiliary variable $\hat{x}_j(k)$, $\forall j \in \mathcal{V}_i^+$. The update of $\hat{x}_j(k)$ depends on whether the trigger condition is satisfied. The trigger function is designed as

$$\mathcal{T}_j(k+1) = |e_j(k+1)| - \tau(k+1) \tag{7}$$

where $e_j(k+1) = \hat{x}_j(k) - x_j(k+1)$ is the difference between the auxiliary variable of agent j at time step k and its state value at time step $k+1$,

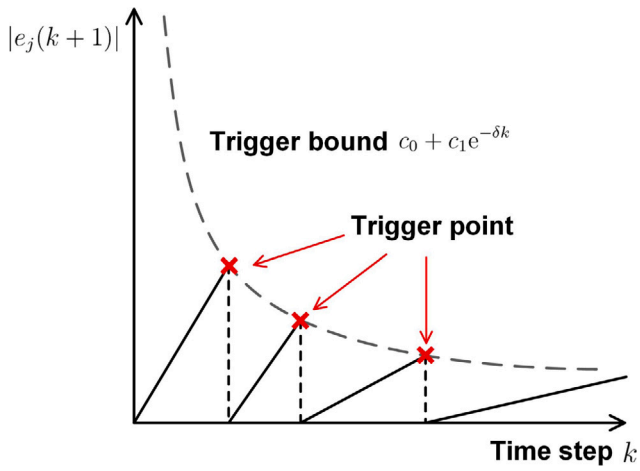


Fig. 2. Event-triggering communication mechanism.

$\tau(k+1) = c_0 + c_1 e^{-\delta(k+1)}$ is a threshold with $\delta, c_0, c_1 > 0$. Furthermore, we observe $\tau(k+1) < \tau(k)$, $\forall k \in \mathbb{Z}_{\geq 0}$.

Note that our event-triggered threshold $c_0 + c_1 e^{-\delta k}$ consists of a constant term c_0 and an exponential term $c_1 e^{-\delta k}$. As the iteration proceeds, the exponential term goes to zero, while the constant term is retained to facilitate a bounded consensus. As shown in Fig. 2, the most significant advantage of this setting is that it not only effectively ensures convergence but also significantly reduces communication overheads. In addition, the threshold $c_0 + c_1 e^{-\delta k}$ has been widely adopted in [23,30] to solve event-based control problems.

With the trigger function, the update of the auxiliary variable $\hat{x}_j(k+1)$ is expressed as

$$\hat{x}_j(k+1) = \begin{cases} x_j(k+1), & \text{if} \quad \mathcal{T}_j(k+1) > 0, \\ \hat{x}_j(k), & \text{otherwise.} \end{cases} \tag{8}$$

If the state value for agent j changes sufficiently, i.e., $\mathcal{T}_j(k+1) > 0$, agent j will update its auxiliary variable and transmit its latest auxiliary variable to agent i and other out-neighbors. Otherwise, agent i will utilize the auxiliary variable from the previous time step for state update and no information interaction will happen.

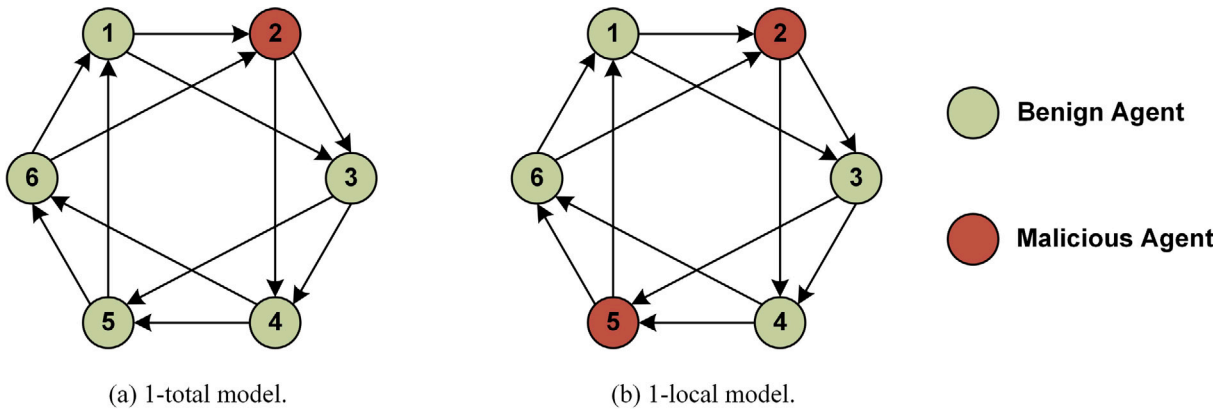
Note that the state update for each agent is synchronous, while the update of the auxiliary variable is asynchronous. Furthermore, the event-triggering condition (7) in continuous-time cases [23,30] may result in Zeno phenomenon, which is an essential problem to be addressed. Specifically, the threshold may approach zero when the CPS achieves consensus, and the triggering function may be activated infinitely within a finite time, leading to Zeno phenomenon. In our discrete-time setting, the minimum time interval between two consecutive triggered events is one, thus there is no concern for the Zeno behavior.

2.4. Attack models

In this paper, agents in the CPS are classified into benign agents and malicious agents, with the former collaborating with in-neighbors to achieve resilient distributed optimization and the latter transmitting wrong information to out-neighbors to interrupt the system update. Their precise definitions are presented as follows, respectively.

Definition 5 (*Benign agent [31]*)**.** An agent is said to be benign if it sends its current state $x_i(k)$ to all of its out-neighbors at each time step k and adopts the rule (6) for state update.

Definition 6 (*Malicious agent [31]*)**.** An agent is said to be malicious if it sends its current state $x_i(k)$ to all of its out-neighbors at each time step k, but adopts some other rule for state update at some time steps.



(a) 1-total model. (b) 1-local model.

Fig. 3. Illustrations of 1-total and 1-local attack models with six nodes.

Denote the sets of malicious and benign agents as $\mathcal{M}$ and $\mathcal{B}$, respectively. Then, we assume $\mathcal{M}\cap\mathcal{B}=\varnothing$ and $\mathcal{M}\cup\mathcal{B}=\mathcal{V}$. By invoking the definition of cardinality, the number of malicious and benign agents is denoted as $|\mathcal{M}|$ and $|\mathcal{B}|$, respectively. If some malicious agents exist in the network, we say that the CPS is under a malicious attack. To better describe the influence of malicious attacks, two attack models are defined according to the scope of threats and their illustrations are shown in Figs. 3(a) and 3(b), respectively.

Definition 7 (*f-total model [16]*)**.** A multi-agent network is said to be an f-total model if the whole network possesses at most f malicious agents, i.e., $|\mathcal{M}|\leq f$.

Definition 8 (*f-local model [16]*)**.** A multi-agent network is said to be an f-local model if the in-neighbor set of each agent i contains at most f malicious agents at each time step $k\in\mathbb{Z}_{\geq 0}$, i.e., $\left|\mathcal{V}_i^+(k)\cap\mathcal{M}\right|\leq f,\ \forall i\in\mathcal{V}$.

It is noteworthy that conventional methodologies implicitly assume that agents in the network operate reliably and work collaboratively to attain global optimization. Nevertheless, the growth in the number of agents in the network gives rise to specific concerns that lead to a breach of this assumption. As previously discussed, distributed optimization algorithms rely heavily on communication infrastructures, which create numerous vulnerabilities for cyber attacks. In such attacks, external adversaries may manipulate the transmitted information. It is evident that the attack undermines the performance of optimization algorithms by impeding benign agents from reaching the expected optimal value or manipulating the final optimal value to be false. More seriously, a single malicious agent may compel all agents to reach arbitrary optimal values by merely keeping this value constant, thus failing to achieve the global optimum.

Given the susceptibility of distributed algorithms to malicious attacks, which covertly alter the output and undermines the attainment of a global minimizer, an alternative approach is to devise an algorithm that yields a sub-optimal solution resilient to malicious attacks. The resulting solution is said to be the resilient optimal solution. To this end, a resilient distributed optimization algorithm based on the event-triggering mechanism will be developed in the following section.

Remark 4. In our setting, the agent identity is unknown to a benign agent, i.e., a benign agent does not know whether its neighbors are benign or malicious agents. Meanwhile, a malicious agent is able to identify other malicious agents and access the current and previous state values of neighboring agents.

3. Main results

3.1. Algorithm design

We design a resilient algorithm for addressing distributed optimization problems under adversarial environments, which is called the event-triggering resilient distributed optimization (RDO-E) algorithm. Each benign agent updates its state synchronously at each time step. Auxiliary variables are updated only when the trigger function (7) is activated, followed by information transmission to in-neighbors. The detailed procedures are shown in Algorithm 1.

Algorithm 1 Event-Triggering Resilient Distributed Optimization (RDO-E) Algorithm

1: Initialize the state value $x_i(0)$ and auxiliary variable $\hat{x}_i(0)$ for agent i randomly;
2: **for** $k=0,1,\ldots$ **do**
3: Receive $\{\hat{x}_j(k)\mid j\in\mathcal{V}_i^+(k)\}$ and arrange them in a list in ascending order;
4: **if** there are fewer than f auxiliary variables strictly smaller or larger than $x_i(k)$ **then**
5: Delete all these auxiliary variables;
6: **else**
7: Delete the f smallest and largest auxiliary variables in the list;
8: **end if**
9: Obtain $\mathcal{R}_i^+(k)$ as the set of retained in-neighbors for agent i;
10: Calculate the subgradient $d_i(k)$ according to (1);
11: Update the state value for agent i according to (3) and (6);
12: **if** the triggering function $\mathcal{T}_i(k+1)$ is activated ($\mathcal{T}_i(k+1)>0$) **then**
13: Update the auxiliary variable $\hat{x}_i(k+1)$ as $\hat{x}_i(k+1)=x_i(k+1)$;
14: Send $\hat{x}_i(k+1)$ to the out-neighbor set $\mathcal{V}_i^-(k)$ of agent i;
15: **else**
16: Set $\hat{x}_i(k+1)$ as $\hat{x}_i(k+1)=\hat{x}_i(k)$.
17: **end if**
18: **end for**

To show the principle of Algorithm 1 more intuitively, an illustration of Steps 4–8 is displayed in Fig. 4. Compared with $x_i(k)$, agent i removes the f smallest and largest values in the sorted list. If there are less than f values strictly larger or smaller than $x_i(k)$, then all of the values that are strictly larger or smaller than $x_i(k)$ will be removed. The removal of these suspicious values is achieved by setting $\theta_{ij}(k)=0$. Agent i will not utilize these removed data for state update, as they are considered malicious.

The main feature of the RDO-E algorithm is its attack tolerance, i.e., benign agents have no knowledge of the identities of abnormal information. Each benign agent only neglects the possibly misleading

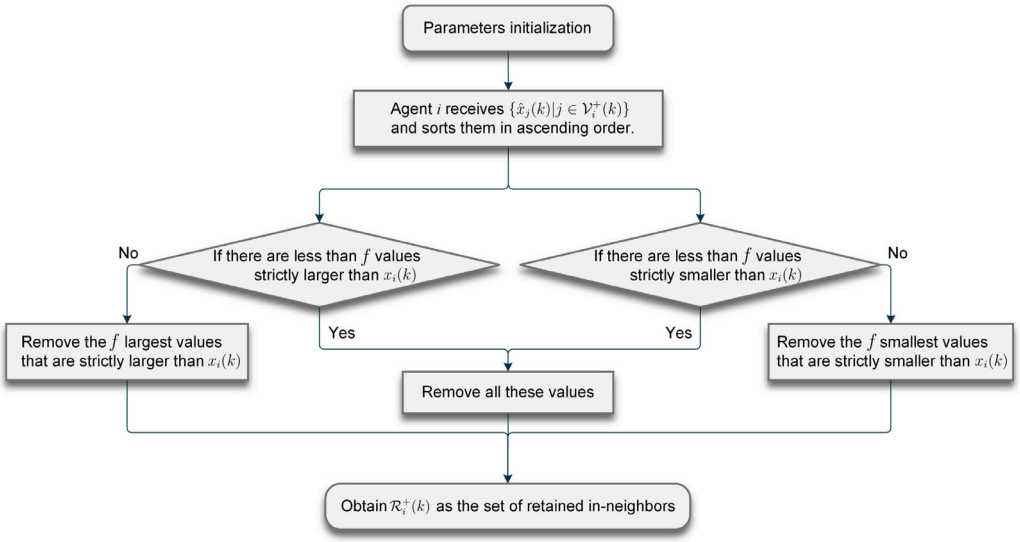


Fig. 4. Flowchart of the main steps of Algorithm 1.

information from its in-neighbors. Specifically, they eliminate f edges from in-neighbors with excessively large and small state values. Furthermore, following the communication rule regarding the algorithm, the update of auxiliary variables occurs only on the premise that the current state value makes enough variation and exceeds the prescribed threshold, and only in this case will the node send value to its neighboring agents. The event-triggering strategy can remarkably decrease the communication burden, which will be illustrated in Section 4.

3.2. Convergence analysis for the f-total malicious model

In this part, we will study the convergence property of the CPS involving the f-total attack scenario. Specifically, we provide the convergence conditions for CPSs to reach an agreement within the error range c under the f-total model. The following lemma is presented for the convenience of convergence analysis.

Lemma 1 (*11*). *Let $\{\varphi_k\}$ be a positive scalar sequence. Assume that $\lim_{k\to\infty}\varphi_k = 0$. For $\phi \in (0,1)$, it holds*

$$\lim_{k\to\infty}\sum_{l=0}^{k}\phi^{k-l}\varphi_l = 0. \tag{9}$$

Now, we are ready to give the necessary and sufficient conditions for the CPS to reach an agreement within the error range c under the f-total model.

Theorem 1. *Consider a CPS modeled by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. Let Assumptions 1–3 hold. Assume that each agent adopts the RDO-E algorithm for state update. Under the attack of f-total model, agreement within the error range c will be reached among benign agents if and only if the network is $(f+1, f+1)$-robust. Furthermore, the error range c will be achieved if c_0 satisfies*

$$c_0 \le \frac{\gamma^{n-1}\beta^n}{4n}c. \tag{10}$$

Proof (*Necessity*)**.** We consider the special case without the event-triggering mechanism (i.e., $c_0 = c_1 = 0$) and prove the necessity of the network condition by contradiction. Assume that the network is not $(f+1, f+1)$-robust. According to Definition 4, the following conditions hold:

$$\begin{aligned}&(1)\left|\mathcal{Y}_{\mathcal{S}_1}^{f+1}\right| < |\mathcal{S}_1|, \quad (2)\left|\mathcal{Y}_{\mathcal{S}_2}^{f+1}\right| < |\mathcal{S}_2|,\\ &(3)\left|\mathcal{Y}_{\mathcal{S}_1}^{f+1}\right| + \left|\mathcal{Y}_{\mathcal{S}_2}^{f+1}\right| \le f,\ \exists \mathcal{S}_1, \mathcal{S}_2 \subset \mathcal{V},\end{aligned} \tag{11}$$

where $\mathcal{S}_1$ and $\mathcal{S}_2$ are nonempty and disjoint node sets. Without loss of generality,[1] let the local cost functions for agents be

$$\begin{aligned}&\arg\min_x f_i(x) = x_1,\ \forall i \in \mathcal{S}_1\\ &\arg\min_x f_j(x) = x_2,\ \forall j \in \mathcal{S}_2\\ &\arg\min_x f_l(x) \in (x_1, x_2),\ \forall l \in \mathcal{V}\backslash(\mathcal{S}_1 \cup \mathcal{S}_2)\end{aligned}$$

with gradient being zero, where $x_1, x_2 \in \mathbb{R}$ and $x_1 < x_2$. Furthermore, suppose that the initial state values of agents meet

$$\begin{aligned}&x_i(0) = x_1,\ \forall i \in \mathcal{S}_1\\ &x_j(0) = x_2,\ \forall j \in \mathcal{S}_2\\ &x_l(0) \in (x_1, x_2),\ \forall l \in \mathcal{V}\backslash(\mathcal{S}_1 \cup \mathcal{S}_2).\end{aligned}$$

Since Condition (3) in (11) holds, we let all the agents in $\mathcal{Y}_{\mathcal{S}_1}^{f+1}$ and $\mathcal{Y}_{\mathcal{S}_2}^{f+1}$ be malicious and keep their state values constant, while the remaining agents are benign. By invoking Conditions (1) and (2) in (11), we know that the number of nodes in $\mathcal{S}_1/\mathcal{S}_2$ with at least $f+1$ in-neighbors is less than the number of nodes in $\mathcal{S}_1/\mathcal{S}_2$. Since we have made assumptions that all malicious agents are in $\mathcal{Y}_{\mathcal{S}_1}^{f+1}$ and $\mathcal{Y}_{\mathcal{S}_2}^{f+1}$ according to Condition (3), there exists at least one benign agent in $\mathcal{S}_1$ who has at most f in-neighbors outside $\mathcal{S}_1$. Similarly, we obtain that there exists at least one benign agent in $\mathcal{S}_2$ who has at most f in-neighbors outside $\mathcal{S}_2$. Therefore, both $\mathcal{S}_1$ and $\mathcal{S}_2$ possess at least one benign agent who has at most f in-neighbors outside of their respective sets. Through the RDO-E algorithm, these benign agents will remove f or less state values of these in-neighbors. Thus, for benign agents in $\mathcal{S}_1$, we deduce that

$$\begin{aligned}&x_i(k) + \gamma\sum_{j\in\mathcal{R}_i^+(k)}\theta_{ij}(k)\left(\hat{x}_j(k) - x_i(k)\right) = x_1\\ &\quad\text{and}\quad d_i(k) = 0,\ \forall i \in \mathcal{S}_1 \cap \mathcal{B},\ \forall k \ge 0.\end{aligned} \tag{12}$$

Similarly, for benign agents in $\mathcal{S}_2$, we have

$$\begin{aligned}&x_j(k) + \gamma\sum_{l\in\mathcal{R}_j^+(k)}\theta_{jl}(k)\left(\hat{x}_l(k) - x_j(k)\right) = x_2\\ &\quad\text{and}\quad d_j(k) = 0,\ \forall j \in \mathcal{S}_2 \cap \mathcal{B},\ \forall k \ge 0.\end{aligned} \tag{13}$$

[1] The generality here refers to the flexibility of $x_1, x_2 \in \mathbb{R}$, i.e., we can also let $x_1 > x_2$. The idea of proof is to consider a counterexample which satisfies all the prerequisites. Subsequently, we will obtain the contradiction, thereby deducing the necessary condition.

Synthesizing (12) with (13) yields that the state values of these benign agents will remain unchanged at x_1 or x_2, i.e.,

$$\begin{aligned} &x_i(k) = x_1,\ \forall i \in \mathcal{S}_1 \cap \mathcal{B},\ \forall k \geq 0 \\ &x_j(k) = x_2,\ \forall j \in \mathcal{S}_2 \cap \mathcal{B},\ \forall k \geq 0, \end{aligned} \tag{14}$$

which indicates that no agreement will be reached among benign agents.

(Sufficiency) For the sufficiency, we need to prove the convergence and derive the prescribed condition of c_0. Let

$$M(k) = \max_{i\in\mathcal{B}} \left\{x_i(k)\right\},\ m(k) = \min_{i\in\mathcal{B}} \left\{x_i(k)\right\}. \tag{15}$$

Furthermore, we define $L(k) = M(k) - m(k)$. If $L(k)$ asymptotically converges to the error range c, we say that the system reaches an approximate agreement.

In addition, we define $\sigma_j(k) = \hat{x}_j(k) - x_j(k)$. From (8), we further obtain

$$\sigma_j(k) = \begin{cases} 0, & \text{if} \quad \mathcal{T}_j(k) > 0, \\ \hat{x}_j(k-1) - x_j(k), & \text{otherwise.} \end{cases} \tag{16}$$

Notice that

$$\left|\sigma_j(k)\right| \leq \tau(k),\ \forall k \geq 0. \tag{17}$$

Thus, the update rule for agent $i \in \mathcal{B}$ is given by

$$x_i(k+1) = \theta_{ii}(k)x_i(k) + \gamma \sum_{j\in\mathcal{R}_i^+(k)} \theta_{ij}(k)\left(x_j(k) + \sigma_j(k)\right) - \alpha(k)d_i(k), \tag{18}$$

where $\theta_{ii}(k) = 1 - \gamma\sum_{j\in\mathcal{R}_i^+(k)}\theta_{ij}(k)$ and D is a positive scalar which satisfies $|d_i(k)| \leq D$. In view of the maximum state values defined in (15), the update rule (18) is upper bounded by

$$\begin{aligned} x_i(k+1) &\leq \theta_{ii}(k)M(k) + \gamma \sum_{j\in\mathcal{R}_i^+(k)} \theta_{ij}(k)\left(M(k) + \sigma_j(k)\right) + D\alpha(k) \\ &= M(k) + \gamma \sum_{j\in\mathcal{R}_i^+(k)} \theta_{ij}(k)\sigma_j(k) + D\alpha(k) \\ &\leq M(k) + \gamma \max_{j\in\mathcal{R}_i^+(k)} \left|\sigma_j(k)\right| + D\alpha(k) \\ &\leq M(k) + \gamma\tau(k) + D\alpha(k). \end{aligned} \tag{19}$$

Similarly, one obtains

$$x_i(k+1) \geq m(k) - \gamma\tau(k) - D\alpha(k). \tag{20}$$

Construct two sequences as

$$\overline{M}(k+1) = \overline{M}(k) + \gamma\tau(k) + D\alpha(k),\ \ \overline{m}(k+1) = \overline{m}(k) - \gamma\tau(k) - D\alpha(k), \tag{21}$$

where

$$\overline{M}(k) = M(k) - \hat{\mu},\ \ \overline{m}(k) = m(k) + \hat{\mu},\ \ \hat{\mu} = \mu L(k). \tag{22}$$

Another sequence is constructed as

$$\hat{\lambda}(k+1) = \xi\hat{\lambda}(k) - (1-\xi)\hat{\mu}, \tag{23}$$

where

$$\hat{\lambda}(k) = \lambda L(k),\ \ \xi = \gamma\beta. \tag{24}$$

Select the parameters λ and μ such that

$$\lambda + \mu = \frac{1}{2},\ \ 0 < \mu < \frac{\xi^n}{1-\xi^n}\lambda. \tag{25}$$

For any $\hat{\lambda}(k) \in \mathbb{R}$ and $k' \geq k$, let

$$\begin{aligned} &\overline{\mathcal{M}}(k,k',\hat{\lambda}(k)) = \left\{i \in \mathcal{V} : x_i(k') > \overline{M}(k) - \hat{\lambda}(k)\right\}, \\ &\underline{\mathcal{M}}(k,k',\hat{\lambda}(k)) = \left\{i \in \mathcal{V} : x_i(k') < \overline{m}(k) + \hat{\lambda}(k)\right\}. \end{aligned} \tag{26}$$

To capture the robust property of the network, it is expected to prove that $\overline{\mathcal{M}}(k,k',\hat{\lambda}(k))$ and $\underline{\mathcal{M}}(k,k',\hat{\lambda}(k))$ are nonempty and disjoint.

For the nonempty property, it follows from (22) that $M(k) > \overline{M}(k) - \hat{\lambda}(k)$. Similar analysis can be conducted on $m(k)$ to obtain $m(k) < \overline{m}(k) + \hat{\lambda}(k)$, which yields the nonempty property of these two sets. Furthermore, according to (15), both of these two sets contain at least one benign agent at time step k.

For the disjoint property, we need to prove $\overline{M}(k) - \hat{\lambda}(k) \geq \overline{m}(k) + \hat{\lambda}(k)$. By invoking (22), we have

$$\begin{aligned} &\overline{M}(k) - \hat{\lambda}(k) - (\overline{m}(k) + \hat{\lambda}(k)) \\ &= (M(k) - m(k)) - 2(\hat{\lambda}(k) + \hat{\mu}) \\ &= L(k) - 2(\lambda+\mu)L(k) \\ &= 0, \end{aligned} \tag{27}$$

where the last equation holds due to $\lambda + \mu = 1/2$. Therefore, we obtain that $\overline{\mathcal{M}}(k,k',\hat{\lambda}(k))$ and $\underline{\mathcal{M}}(k,k',\hat{\lambda}(k))$ are disjoint.

According to the aforementioned analysis, it has been proved that the sets $\overline{\mathcal{M}}(k,k',\hat{\lambda}(k))$ and $\underline{\mathcal{M}}(k,k',\hat{\lambda}(k))$ are nonempty and disjoint, with at least one benign agent in their respective sets. Since the underlying network is $(f+1,f+1)$-robust, at least one of the following condition holds:

$$(1)\left|\mathcal{Y}_{\mathcal{S}_1}^{f+1}\right| = |\mathcal{S}_1|,\quad (2)\left|\mathcal{Y}_{\mathcal{S}_2}^{f+1}\right| = |\mathcal{S}_2|,\quad (3)\left|\mathcal{Y}_{\mathcal{S}_1}^{f+1}\right| + \left|\mathcal{Y}_{\mathcal{S}_2}^{f+1}\right| > f.$$

It is noteworthy that no matter which condition holds, either $\overline{\mathcal{M}}(k,k',\hat{\lambda}(k))$ or $\underline{\mathcal{M}}(k,k',\hat{\lambda}(k))$ contains at least one benign agent who possesses at least $f+1$ in-neighbors outside of its respective set. Assume that the benign agent belongs to $\overline{\mathcal{M}}(k,k',\hat{\lambda}(k))$, i.e., $i \in \overline{\mathcal{M}}(k,k',\hat{\lambda}(k)) \cap \mathcal{B}$. We shall now revisit (18) and rewrite it as

$$\begin{aligned} x_i(k+1) = &\left(1 - \gamma \sum_{j\in\mathcal{R}_i^+(k)} \theta_{ij}(k)\right)x_i(k) + \gamma \sum_{j\in\mathcal{R}_i^+(k)\cap\overline{\mathcal{M}}} \theta_{ij}(k)x_j(k) \\ &+ \gamma \sum_{j\in\mathcal{R}_i^+(k)\setminus\overline{\mathcal{M}}} \theta_{ij}(k)x_j(k) + \gamma \sum_{j\in\mathcal{R}_i^+(k)} \theta_{ij}(k)\sigma_j(k) - \alpha(k)d_i(k), \end{aligned} \tag{28}$$

where $\overline{\mathcal{M}}(k,k',\hat{\lambda}(k))$ is abbreviated as $\overline{\mathcal{M}}$ for the convenience of expression. By invoking (15) and (22), the upper bound of (28) is given by

$$\begin{aligned} x_i(k+1) \leq &\left(1 - \gamma \sum_{j\in\mathcal{R}_i^+(k)} \theta_{ij}(k)\right)M(k) + \gamma \sum_{j\in\mathcal{R}_i^+(k)\cap\overline{\mathcal{M}}} \theta_{ij}(k)M(k) \\ &+ \gamma \sum_{j\in\mathcal{R}_i^+(k)\setminus\overline{\mathcal{M}}} \theta_{ij}(k)(\overline{M}(k) - \hat{\lambda}(k)) \\ &+ \gamma \sum_{j\in\mathcal{R}_i^+(k)} \theta_{ij}(k)\sigma_j(k) - \alpha(k)d_i(k) \\ = &\left(1 - \gamma \sum_{j\in\mathcal{R}_i^+(k)\setminus\overline{\mathcal{M}}} \theta_{ij}(k)\right)M(k) \\ &+ \gamma \sum_{j\in\mathcal{R}_i^+(k)\setminus\overline{\mathcal{M}}} \theta_{ij}(k)(\overline{M}(k) - \hat{\lambda}(k)) \\ &+ \gamma \sum_{j\in\mathcal{R}_i^+(k)} \theta_{ij}(k)\sigma_j(k) - \alpha(k)d_i(k). \end{aligned} \tag{29}$$

Replacing $M(k)$ with $\overline{M}(k) + \hat{\mu}$ and utilizing the limit of $\sigma_j(k)$ and $d_i(k)$, (29) is further upper bounded by

$$\begin{aligned} x_i(k+1) \leq &\left(1 - \gamma \sum_{j\in\mathcal{R}_i^+(k)\setminus\overline{\mathcal{M}}} \theta_{ij}(k)\right)(\overline{M}(k) + \hat{\mu}) \\ &+ \gamma \sum_{j\in\mathcal{R}_i^+(k)\setminus\overline{\mathcal{M}}} \theta_{ij}(k)(\overline{M}(k) - \hat{\lambda}(k)) \\ &+ \gamma \max_{j\in\mathcal{R}_i^+(k)} \left|\sigma_j(k)\right| + D\alpha(k) \\ \leq\ &\overline{M}(k) + (1-\gamma\beta)\hat{\mu} - \gamma\beta\hat{\lambda}(k) + \gamma\tau(k) + D\alpha(k) \\ =\ &\overline{M}(k+1) - \hat{\lambda}(k+1), \end{aligned} \tag{30}$$

which indicates that if a benign agent belongs to $\overline{\mathcal{M}}(k,k,\hat{\lambda}(k))$ at time step k, it will belong to $\mathcal{V}\backslash\overline{\mathcal{M}}(k,k+1,\hat{\lambda}(k+1))$ at time step $k+1$. Notice that inequality (30) also holds for benign agents that are in $\mathcal{V}\backslash\overline{\mathcal{M}}(k,k,\hat{\lambda}(k))$ at time step k. This fact implies that regardless of the state value for agent i, it will belong to $\mathcal{V}\backslash\overline{\mathcal{M}}(k,k+1,\hat{\lambda}(k+1))$ at the next time step. Similar conclusion can be conducted on $\underline{\mathcal{M}}(k,k+1,\hat{\lambda}(k+1))$. By recursion, we know that all benign agents will move out from $\overline{\mathcal{M}}(k,k+n,\hat{\lambda}(k+n))$ or $\underline{\mathcal{M}}(k,k+n,\hat{\lambda}(k+n))$ after n time steps, which means that either $\overline{\mathcal{M}}(k,k+n,\hat{\lambda}(k+n))\cap\mathcal{B}$ or $\underline{\mathcal{M}}(k,k+n,\hat{\lambda}(k+n))\cap\mathcal{B}$ is empty at time step $k+n$. Assume that $\overline{\mathcal{M}}(k,k+n,\hat{\lambda}(k+n))\cap\mathcal{B}$ is empty. Then, we have

$$x_i(k+n)\le\overline{M}(k+n)-\hat{\lambda}(k+n),\quad\forall i\in\mathcal{B},\tag{31}$$

which yields that

$$M(k+n)\le\overline{M}(k+n)-\hat{\lambda}(k+n).\tag{32}$$

We next show that $m(k+n)\ge\overline{m}(k+n)-\hat{\mu}$. For time step $k+n$, it follows from (20) that

$$\begin{aligned}m(k+n)&\ge m(k+n-1)-\gamma\tau(k+n-1)-D\alpha(k+n-1)\\&\ge m(k+n-1)-\gamma\tau(k+n-1)-D\alpha(k+n-1)-\hat{\mu}\\&=\overline{m}(k+n)-\hat{\mu}.\end{aligned}\tag{33}$$

To proceed with the convergence analysis, we need to derive recursive results at time step $k+n$ for sequences (21) and (23).

Let us first focus on $\overline{M}(k+n)$. It follows from (21) that

$$\overline{M}(k+n)=\overline{M}(k)+\sum_{l=0}^{n-1}\left(\gamma\tau(k+l)+D\alpha(k+l)\right).\tag{34}$$

Similarly, we have

$$\overline{m}(k+n)=\overline{m}(k)-\sum_{l=0}^{n-1}\left(\gamma\tau(k+l)+D\alpha(k+l)\right).\tag{35}$$

Now, let us turn our attention to $\hat{\lambda}(k+n)$. It follows from (23) that

$$\begin{aligned}\hat{\lambda}(k+n)&=\xi^n\hat{\lambda}(k)-(\xi^{n-1}+\cdots+\xi+1)(1-\xi)\hat{\mu}\\&=\xi^n\lambda L(k)-(1-\xi^n)\mu L(k)\\&=(\xi^n\lambda-(1-\xi^n)\mu)\,L(k).\end{aligned}\tag{36}$$

Combining the results of (32), (33), (34), (35), and (36) gives that:

$$\begin{aligned}L(k+n)&=M(k+n)-m(k+n)\\&\le\overline{M}(k+n)-\hat{\lambda}(k+n)-\overline{m}(k+n)+\hat{\mu}\\&=\overline{M}(k)-\overline{m}(k)+2\sum_{l=0}^{n-1}\gamma\tau(k+l)+2\sum_{l=0}^{n-1}D\alpha(k+l)\\&\quad-(\xi^n\lambda-(1-\xi^n)\mu)\,L(k)+\hat{\mu}\\&=(M(k)-\hat{\mu})-(m(k)+\hat{\mu})+2\gamma c_0n+2\gamma c_1\frac{1-\mathrm{e}^{-\delta n}}{1-\mathrm{e}^{-\delta}}\mathrm{e}^{-\delta k}\\&\quad+2D\sum_{l=0}^{n-1}\alpha(k+l)-(\xi^n\lambda-(1-\xi^n)\mu)\,L(k)+\hat{\mu}\\&=L(k)+2\gamma c_0n+2\gamma c_1\frac{1-\mathrm{e}^{-\delta n}}{1-\mathrm{e}^{-\delta}}\mathrm{e}^{-\delta k}-\mu L(k)\\&\quad+2D\sum_{l=0}^{n-1}\alpha(k+l)-(\xi^n\lambda-(1-\xi^n)\mu)\,L(k)\\&=(1-\xi^n(\lambda+\mu))L(k)+2\gamma c_0n+2\gamma c_1\frac{1-\mathrm{e}^{-\delta n}}{1-\mathrm{e}^{-\delta}}\mathrm{e}^{-\delta k}\\&\quad+2D\sum_{l=0}^{n-1}\alpha(k+l).\end{aligned}\tag{37}$$

Since $\alpha(k)$ is nonincreasing and $\lambda+\mu=1/2$, we further derive

$$L(k+n)\le(1-\frac{\xi^n}{2})L(k)+2\gamma c_0n+2\gamma c_1\frac{1-\mathrm{e}^{-\delta n}}{1-\mathrm{e}^{-\delta}}\mathrm{e}^{-\delta k}+2Dn\alpha(k).\tag{38}$$

Thus, for any $\varepsilon\in\mathbb{N}$, we have

$$\begin{aligned}L(k+\varepsilon n)\le(1-\frac{\xi^n}{2})^{\varepsilon}L(k)+\sum_{l=0}^{\varepsilon-1}(1-\frac{\xi^n}{2})^{\varepsilon-1-l}\\\times\left(2\gamma c_0n+2\gamma c_1\frac{1-\mathrm{e}^{-\delta n}}{1-\mathrm{e}^{-\delta}}\mathrm{e}^{-\delta(k+ln)}+2Dn\alpha(k+ln)\right).\end{aligned}\tag{39}$$

As ε goes to infinity, $\mathrm{e}^{-\delta(k+ln)}\to0$ and $\alpha(k+ln)\to0$. By invoking Lemma 1, we obtain

$$\lim_{\varepsilon\to\infty}L(k+\varepsilon n)\le2\gamma c_0n\sum_{l=0}^{\varepsilon-1}(1-\frac{\xi}{2})^{\varepsilon-1-l}=\frac{4c_0\gamma n}{\xi^n}=\frac{4c_0n}{\gamma^{n-1}\beta^n}\le c.\tag{40}$$

Since the aforementioned result holds for any $k\ge0$, we know

$$\lim_{k\to\infty}L(k)=\frac{4c_0n}{\gamma^{n-1}\beta^n}\le c\Rightarrow c_0\le\frac{\gamma^{n-1}\beta^n}{4n}c.\tag{41}$$

This completes the proof of convergence and the prescribed condition (10). ■

3.3. Convergence analysis for the f-local malicious model

In this part, we will study the convergence property of the CPS involving the f-local attack scenario, which represents a scalable number of malicious agents. The necessary and sufficient conditions are respectively presented for the CPS to reach an agreement within the error range c under the f-local malicious model.

Theorem 2. *Consider a CPS modeled by $\mathcal{G}=(\mathcal{V},\mathcal{E})$. Let Assumptions 1–3 hold. Assume that each agent adopts the RDO-E algorithm for state update. Under the attack of f-local model,*

(1) a necessary condition for reaching agreement within the error range c among benign agents is that the network is $(f+1)$-robust;
(2) if the network is $(2f+1)$-robust, then agreement within the error range c will be reached among benign agents. Furthermore, the error range c is achieved if c_0 satisfies

$$c_0\le\frac{\gamma^{n-1}\beta^n}{4n}c.\tag{42}$$

Proof (*Necessity*)**.** We also consider the special case without the event-triggering mechanism (i.e., $c_0=c_1=0$) and prove the necessity of the network condition by contradiction. Assume that the network is not $(f+1)$-robust. According to Definition 3, we can construct two nonempty and disjoint subsets $\mathcal{S}_1,\mathcal{S}_2\subseteq\mathcal{V}$, both of which are not $(f+1)$-reachable. This fact implies that each agent in $\mathcal{S}_1$ and $\mathcal{S}_2$ possesses at most f in-neighbors outside of their respective sets.

Let minimum solutions of the local cost functions for agents in $\mathcal{S}_1$ and $\mathcal{S}_2$ respectively be

$$\begin{aligned}&\arg\min_x f_i(x)=M',\ \forall i\in\mathcal{S}_1,\\&\arg\min_x f_j(x)=m',\ \forall j\in\mathcal{S}_2\end{aligned}$$

with gradient being zero, where

$$\begin{aligned}M'&=\max_{i\in\mathcal{V}}\left\{x_i(k)\right\},\\m'&=\min_{i\in\mathcal{V}}\left\{x_i(k)\right\}.\end{aligned}\tag{43}$$

Moreover, suppose that the state values of agents in $\mathcal{S}_1$ and $\mathcal{S}_2$ at time step k satisfy

$$\begin{aligned}&x_i(k)=M',\ \forall i\in\mathcal{S}_1\\&x_j(k)=m',\ \forall j\in\mathcal{S}_2,\end{aligned}$$

i.e., allocate the maximum and minimum state values to agents in $\mathcal{S}_1$ and $\mathcal{S}_2$, respectively. Through the RDO-E algorithm, however, the agents in $\mathcal{S}_1$ and $\mathcal{S}_2$ will never utilize any values outside their respective sets for update. Consequently, the state values of agents in $\mathcal{S}_1$ and $\mathcal{S}_2$

will remain unchanged at M' and m', respectively, and no agreement will be reached among benign agents.

(Sufficiency) For the sufficiency, we also consider the nonempty and disjoint subsets $\overline{\mathcal{M}}(k,k+n,\hat{\lambda}(k+n))\cap\mathcal{B}$ and $\underline{\mathcal{M}}(k,k+n,\hat{\lambda}(k+n))\cap\mathcal{B}$. Since the underlying network is $(2f+1)$-robust, we can assume that $\overline{\mathcal{M}}(k,k+n,\hat{\lambda}(k+n))\cap\mathcal{B}$ is $(2f+1)$-reachable. Through the RDO-E algorithm, at least one benign agent in $\overline{\mathcal{M}}(k,k+n,\hat{\lambda}(k+n))\cap\mathcal{B}$ will utilize at least one of its benign in-neighbors' state values from outside for update. Therefore, (18) is written as

$$\begin{aligned} x_i(k+1) &\le (1-\gamma\beta)M(k)+\gamma\beta(\overline{M}(k)-\hat{\lambda}(k))+\gamma\max_{j\in\mathcal{R}_i^+(k)}\left|\sigma_j(k)\right|+D\alpha(k)\\ &\le (1-\gamma\beta)(\overline{M}(k)+\hat{\mu})+\gamma\beta(\overline{M}(k)-\hat{\lambda}(k))+\gamma\tau(k)+D\alpha(k)\\ &= \overline{M}(k)+\gamma\tau(k)+D\alpha(k)-(\gamma\beta\hat{\lambda}(k)-(1-\gamma\beta)\hat{\mu})\\ &= \overline{M}(k+1)-\hat{\lambda}(k+1), \end{aligned} \tag{44}$$

which is consistent with (30). The subsequent deduction process is the same as that of Theorem 1 and thus omitted. ■

Remark 5. Note that the CPS reaches an agreement at the same error level under the conditions of Theorems 1 and 2. This is because the most significant difference between two theorems lies in diverse robustness requirements. These graph conditions have no influence on convergence accuracy. Furthermore, it is achievable to improve convergence accuracy by simply setting $c_0=0$. However, this operation may simultaneously reduce the convergence rate and increase the number of triggered events. This contradiction indicates a trade-off between reaching an agreement at a lower error level and consuming more communication overheads.

3.4. Optimality analysis

The aforementioned theorems merely guarantee that the final state value converges within the error range c under different attack models. In this part, we will further analyze the optimality of the CPS.

Suppose that each local cost function $f_i(x)$, $\forall i\in\mathcal{B}$ possesses a nonempty compact set of minimizers $\mathcal{X}_i^*$. Furthermore, define $m^*=\min_{i\in\mathcal{B}}\min\{x|x\in\mathcal{X}_i^*\}$ and $M^*=\max_{i\in\mathcal{B}}\max\{x|x\in\mathcal{X}_i^*\}$. The following theorem reveals that despite malicious attacks, the state values for benign agents will converge to the safety interval $\Psi=[m^*,M^*]$, which refers to the convex hull of local minimizers for all benign agents. Resilient distributed optimization is thereby guaranteed.

Theorem 3. *Consider a CPS modeled by $\mathcal{G}=(\mathcal{V},\mathcal{E})$. Let Assumptions 1–3 hold. Assume that each agent adopts the RDO-E algorithm for state update. Under the attack of f-total model, the state values of all benign agents will converge to the safety interval $\Psi=[m^*,M^*]$ if the underlying network is $(f+1,f+1)$-robust.*

Proof. Suppose that $\limsup_{k\to\infty}M(k)=M^*+\epsilon$ for the sake of a contradiction argument, where $\epsilon>0$. Since $\lim_{k\to\infty}(M(k)-m(k))=4c_0n/\gamma^{n-1}\beta^n$ according to Theorem 1 and $\lim_{k\to\infty}\alpha(k)=0$, there exists k_0 such that

$$M^*+\frac{\epsilon}{2}\le M(k_0)\le M^*+\frac{3\epsilon}{2}, \tag{45}$$

$$M(k)-m(k)\le\frac{\epsilon}{4},\quad\forall k\ge k_0, \tag{46}$$

and

$$D\alpha(k)\le\frac{\epsilon}{4},\quad\forall k\ge k_0 \tag{47}$$

hold. By invoking (45) and (46), we further obtain

$$m(k)\ge M(k)-\frac{\epsilon}{4}\ge M^*+\frac{\epsilon}{4}. \tag{48}$$

Since $f_i(x)$ is convex and the local optimal value x_i^* for cost function $f_i(x)$, $i\in\mathcal{B}$ satisfies $x_i^*\in[m^*,M^*]$, we know that $d_i(x)$ is diminishing and $d_i(k)\ge 0$, $\forall x>M^*$. Define $h=d_i(M^*+\frac{\epsilon}{4})>0$. Then, we have $d_i(k)\ge h>0$, $\forall i\in\mathcal{V}$, $\forall k\ge k_0$. Denote $k_1=\inf\left\{k>k_0\mid M(k)<M^*+\frac{\epsilon}{2}\right\}$ as the first time step when $M(k)<M^*+\frac{\epsilon}{2}$, $\forall k\ge k_0$. We shall prove that such k_1 exists by contradiction. For any $k\ge k_0$, it follows from (18) that

$$x_i(k+1)\le M(k)-h\alpha(k),\ \forall i\in\mathcal{B}, \tag{49}$$

which indicates that $M(k+1)\le M(k)-h\alpha(k)$. For any $k'\in\mathbb{N}^+$, it is further derived

$$\begin{aligned} M(k_0+k') &\le H(k_0)-h\sum_{l=k_0}^{k_0+k'-1}\alpha(l)\\ &\le M^*+\frac{3\epsilon}{2}-h\sum_{l=k_0}^{k_0+k'-1}\alpha(l). \end{aligned} \tag{50}$$

Due to $\sum_{k=1}^{\infty}\alpha(k)=\infty$, there exists some $\Delta k'$ such that $\sum_{l=k_0}^{k_0+\Delta k'-1}\alpha(l)>\frac{\epsilon}{h}$, which indicates $M(k_0+\Delta k')<M^*+\frac{\epsilon}{2}$. This leads to a contradiction, i.e., there exists $k_1=k_0+\Delta k'$ such that $M(k_1)<M^*+\frac{\epsilon}{2}$. Denote $k_1=\inf\left\{k>k_0\mid M(k)<M^*+\frac{\epsilon}{2}\right\}$. Then, we focus on $M(k)$ for all $k\in[k_1,k_2]$. If follows from (47) that

$$\begin{aligned} x_i(k_1+1) &= \theta_{ii}(k)x_i(k_1)+\gamma\sum_{j\in\mathcal{R}_i^+(k_1)}\theta_{ij}(k)\left(x_j(k)+\sigma_j(k)\right)-\alpha(k)d_i(k)\\ &\le M(k_1)+D\alpha(k_1)\\ &\le M^*+\frac{3\epsilon}{4}, \end{aligned} \tag{51}$$

which yields $M(k_1+1)\le M^*+\frac{3\epsilon}{4}$. Now, we discuss two cases distinguished by the magnitude relation between $M(k_1+1)$ and $M^*+\frac{\epsilon}{2}$. If $M(k_1+1)\ge M^*+\frac{\epsilon}{2}$, we can repeat the aforementioned analysis (49)–(51) and find that $M(k)$ is decreasing. Furthermore, there exists $k_2>k_1$ such that $M(k_2)<M^*+\frac{\epsilon}{2}$. It follows that $M(k)\le M^*+\frac{3\epsilon}{4}$, $\forall k\in[k_1,k_2]$ always holds. If $M(k_1+1)<M^*+\frac{\epsilon}{2}$, it is evident that $k_2=k_1+1$. In this situation, one also obtains $M(k)\le M^*+\frac{3\epsilon}{4}$, $\forall k\in[k_1,k_2]$.

By recursion, we define $k_l=\inf\left\{k>k_{l-1}\mid M(k)<M^*+\frac{\epsilon}{2}\right\}, l=3,4,\ldots$. Then, it is derived that $M(k)\le M^*+\frac{3\epsilon}{4}$, $\forall k\in[k_{l-1},k_l]$, $l=3,4,\ldots$ always holds. Consequently, we obtain $\limsup_{k\to\infty}x_i(k)\le M^*+\frac{3\epsilon}{4}$, which leads to a contradiction since we have assumed that $\limsup_{k\to\infty}M(k)=M^*+\epsilon$. This fact indicates $\limsup_{k\to\infty}x_i(k)\le M^*$. Similarly, we derive $\liminf_{k\to\infty}x_i\ge m^*$. Thus, the proof is complete. ■

Theorem 4. *Consider a CPS modeled by $\mathcal{G}=(\mathcal{V},\mathcal{E})$. Let Assumptions 1–3 hold. Assume that each agent adopts the RDO-E algorithm for state update. Under the attack of f-local model, the state values of all benign agents will converge to the safety interval $\Psi=[m^*,M^*]$ if the underlying network is $(2f+1)$-robust.*

Proof. The proof is similar to that of Theorem 3 and omitted here. ■

Remark 6. Although Theorems 3 and 4 ensure that the convergence value remains in the safety interval constructed by local optimal values, they do not guarantee accurate optimization under two attack scenarios. Rather than seeking for convergence to a safety interval, one may ask whether it is achievable that the CPS exactly converges to the global optimizer under adversarial environments. The paper [18] claimed that this goal is unattainable unless extra assumptions are made on agents' objective functions. Based on this fundamental result, the paper [32] showed that accurate optimization is achieved under adversarial environments if the $2f$-redundancy assumption is posed on the agents' objective functions. Nevertheless, the work [32] executed the analysis in a peer-to-peer network, while the attack scenario was limited to the f-total model. It was further revealed in [33] that the

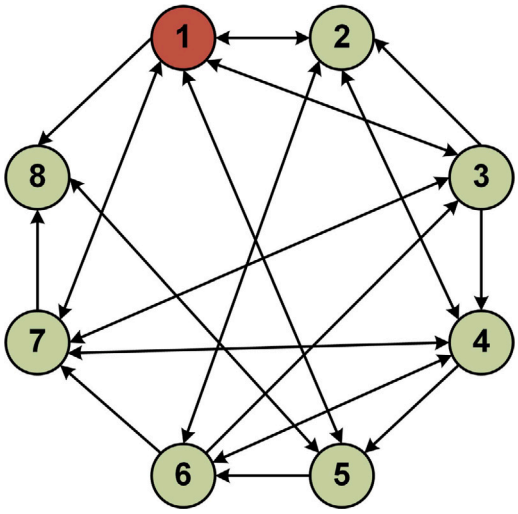


Fig. 5. A $(2,2)$-robust digraph with eight nodes.

assumption is a necessary condition for ensuring accurate optimization. Extending the results [32,33] to general networks and providing more complete optimality conditions remain open directions of research.

4. Case study

This part presents four numerical cases to validate the theoretical results and show the effectiveness, superiority, and practical viability of the RDO-E algorithm. Specifically, we first consider a CPS consisting of 8 agents and each agent $i \in \mathcal{V}$ possesses a local and confidential function $f_i(x) = p_i |x - q_i|$. It is evident that each $f_i(x)$ satisfies Assumption 1 and has a unique local optimal value $x_i^* = q_i$. Moreover, assume that all agents endeavor to tackle the following distributed optimization problem:

$$\arg\min_x F(x) = \frac{1}{8}\sum_{i=1}^{8} f_i(x_i) = \frac{1}{8}\sum_{i=1}^{8} p_i |x_i - q_i|. \tag{52}$$

The parameters for $f_i(x_i)$ are set as $[p_1, \ldots, p_8]^{\mathrm{T}} = [0.1, 0.2, 0.3, 0.4, 0.4, 0.3, 0.2, 0.1]^{\mathrm{T}}$ and $[q_1, \ldots, q_8]^{\mathrm{T}} = [-0.8, -0.6, -0.4, -0.2, 0.2, 0.4, 0.6, 0.8]^{\mathrm{T}}$, respectively. The initial state values for the CPS are denoted as $[x_1(0), \ldots, x_8(0)]^{\mathrm{T}} = [0, 2, 1, 0.5, 3, -0.5, -1, -2]^{\mathrm{T}}$. The safety interval is calculated as $\Psi = [-0.8, 0.8]$. Furthermore, we set the parameters concerning trigger function (7) as $c_0 = 5 \times 10^{-3}$, $c_1 = 0.05$, $\delta = 0.03$.

4.1. The f-total attack scenario

We firstly consider the f-total attack scenario. The network of the CPS is presented in Fig. 5, which is verified to be a $(2,2)$-robust graph. By invoking Theorem 1, the network is capable of tolerating at most 1 malicious agent in the whole network.

Thus, we postulate that the network is under the attack of 1-total attack model and let Agent 1 be malicious. It means that the attacker has manipulated Agent 1 and may change its state value arbitrarily. Furthermore, the malicious value will be transmitted over the underlying network to all out-neighbors of Agent 1. In this situation, it is impractical to solve (52) due to the persistent loss of information concerning $f_1(x)$ throughout the entire iteration process. Consequently, the remaining benign agents will collaboratively endeavor to tackle

$$\arg\min_x F_1(x) = \frac{1}{7}\sum_{\boldsymbol{i=2}}^{8} f_i(x_i) = \frac{1}{7}\sum_{i=2}^{8} p_i |x_i - q_i|. \tag{53}$$

If the influence of Agent 1 is neglected, we will obtain the optimal solution $x_i^* = 0.2$, $\forall i \in \mathcal{B}$ for problem (53) using the optimization algorithm in [10]. The result is illustrated in Fig. 6(a). Next, we involve Agent 1 into the network and set its state value as $x_1(k) = 1.5 \times \sin(0.02\pi k)$. It will try to prevent benign agents from converging to the optimal value. Fig. 6(b) displays the state values for the eight agents using the algorithm proposed in [10], which is not equipped with any defensive measures against malicious attacks. It can be seen that benign agents are incapable of achieving resilient distributed optimization. Instead, they follow the malicious agent in a sinusoidal motion, and the trajectories exceed the safety interval Ψ. The result implies that the malicious agent not only poses risks to the individual nodes, but also jeopardizes the safety and integrity of the whole system.

Subsequently, we apply the proposed RDO-E algorithm to the CPS and obtain the convergence result, as shown in Fig. 7(a). It is observed that despite the influence of Agent 1, the benign agents achieve resilient distributed optimization inside Ψ, which validates Theorems 1 and 3. Moreover, the event-triggering time in Fig. 7(b) indicates that the frequent information interaction between agents is significantly mitigated, thus the communication burden of the system is lightened.

4.2. The f-local attack scenario

In this part, we further consider the f-local attack scenario, which is a more common situation in practice (e.g., large-scale distributed networks). The network of the CPS is depicted in Fig. 8, which is verified to be a 3-robust graph. By invoking Theorem 2, the network is capable of tolerating at most 1 malicious agent in the in-neighbor set for each agent. Suppose that Agents 1 and 2 are malicious agents. It can be verified that the cyber–physical network satisfies the condition of 1-local attack model. The problem (52) remains unsolvable due to the information missing of Agents 1 and 2 during the iteration process. Thus, the remaining benign agents will collaboratively endeavor to tackle

$$\arg\min_x F_2(x) = \frac{1}{6}\sum_{\boldsymbol{i=3}}^{8} f_i(x_i) = \frac{1}{6}\sum_{i=3}^{8} p_i |x_i - q_i|. \tag{54}$$

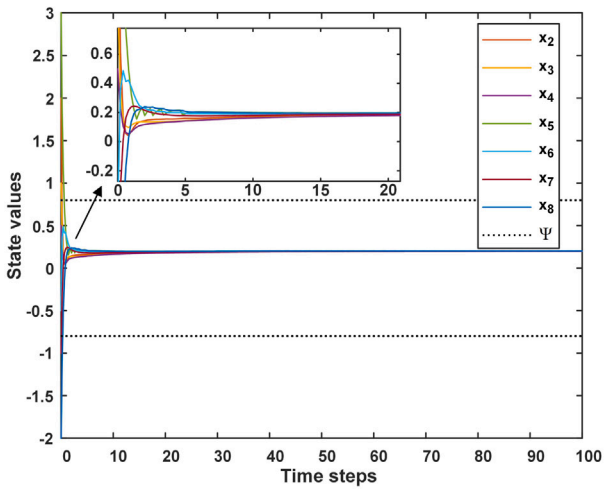
If we ignore the influence of Agents 1 and 2, we will obtain that the optimal solution for problem (54) is still $x_i^* = 0.2$, $\forall i \in \mathcal{B}$ using the optimization algorithm in [10], as shown in Fig. 9(a). Subsequently, we involve Agents 1 and 2 into the network and set their state values as $x_1(k) = 1.5 \times \sin(0.05\pi k)$ and $x_2(k) = rand(-1, 1)$, respectively, where $rand(-1, 1)$ refers to a random number belonging to $(-1, 1)$. Fig. 9(b) displays the convergence result adopting the algorithm proposed in [10] under the f-local attack model. Notice that the trajectories of the benign agents exhibit irregular movements and exceed the safety interval Ψ, which implies that the benign agents would be seriously affected by Agents 1 and 2. The result also indicates the necessity of resilient algorithms.

Now we apply the proposed RDO-E algorithm to the CPS and obtain the convergence result, as shown in Fig. 10(a). It can be observed that regardless of the misbehavior of two malicious agents, the benign agents achieve resilient distributed optimization inside Ψ, which validates Theorems 2 and 4. Furthermore, the result of event time instants is shown in Fig. 10(b), which indicates that the frequent information interaction between agents is mitigated, thus the substantial communication burden is lightened.

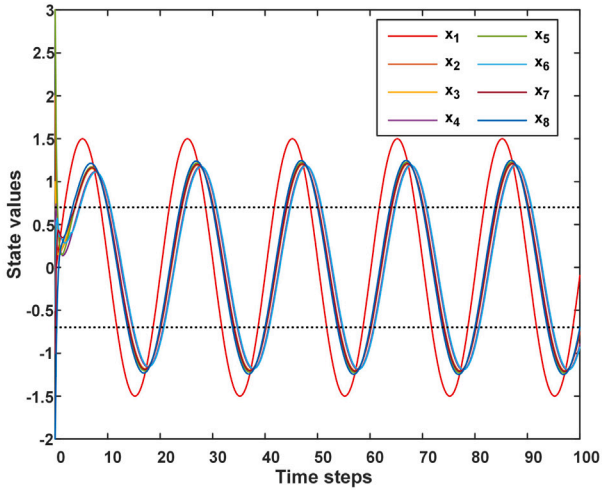
4.3. Comparison among different resilient algorithms based on the event-triggering mechanism

In order to show the superiority of the proposed RDO-E algorithm, a comparative analysis is conducted between the RDO-E algorithm and other established event-based resilient algorithms. Specifically, to equip the algorithms with the ability to achieve resilient distributed optimization, we modify the control protocol of the event-based resilient algorithm proposed in [23] as

$$u_i(k) = \gamma \sum_{j \in R_i^+(k)} \theta_{ij}(k)\left(\hat{x}_j(k) - \hat{x}_i(k)\right) - \alpha(k) d_i(k). \tag{55}$$

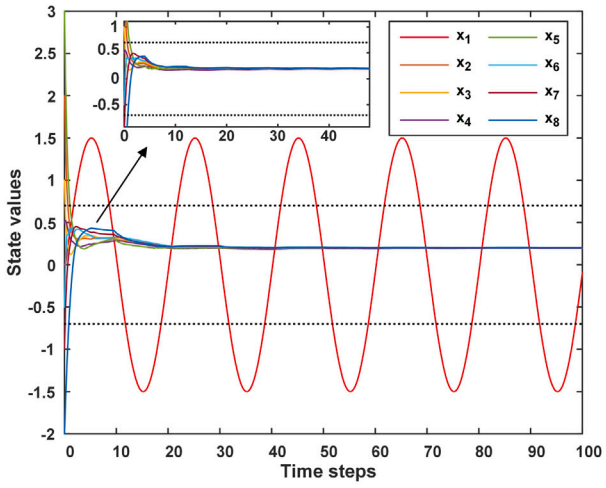


(a) Benign agents achieve RDO.

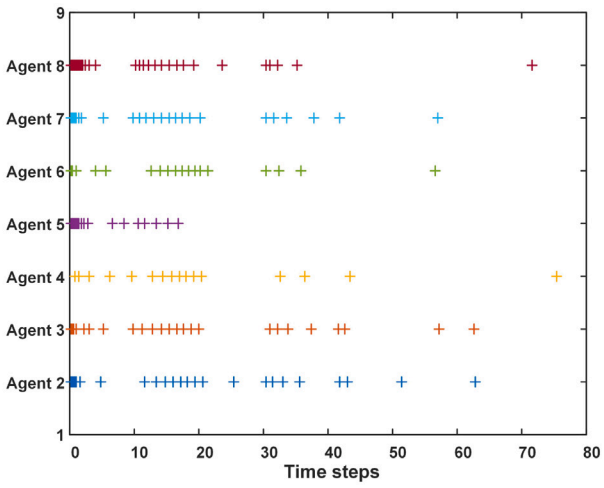


(b) Benign agents fail to achieve RDO.

Fig. 6. Convergence results using the algorithm proposed in [10]: (a) without the malicious attack; (b) with the malicious attack.



(a) Benign agents achieve RDO.



(b) Triggering behavior of the RDO-E algorithm.

Fig. 7. Convergence result and triggering behavior using the proposed RDO-E algorithm: (a) trajectories of agents; (b) event instants with the event function (7).

For event-based resilient algorithm [27], we let its control protocol the same as (55) and modify the update rule as

$$x_i(k+1) = \hat{x}_i(k) + u_i(k). \tag{56}$$

Other parameter settings and the event function are the same as the proposed RDO-E algorithm.

The simulation results using the event-based algorithm proposed in [23] are illustrated in Figs. 11(a) and 11(b). Although the six benign agents converge to the optimal value and achieve resilient distributed optimization inside the safety interval, As shown in Fig. 11(b), numerous event instants occur in the time interval $(0, 80)$ for agents 3, 4, 6, 7, and 8. It means that the CPS still needs to achieve resilient distributed optimization through frequent communication between agents.

Figs. 11(c) and 11(d) display the simulation results using the event-based algorithm proposed in [27]. Fig. 11(d) indicates that the event function (7) triggers occasionally, but Fig. 11(c) shows that the convergence value deviates from the optimal value $x_i^* = 0.2,\ \forall i \in \mathcal{B}$, which is unacceptable.

In order to facilitate a more intuitive comparison of method performance, we further calculate the number of triggered events for all benign agents in the simulation time steps and the relative errors of different algorithms, which are shown in Table 2. Note that three indicators are selected to evaluate the performance of various methods. The indicator "RDO" will be marked with ✓if a method achieves resilient distributed optimization, otherwise, it is marked with✗. The indicator "Event counts" is suitable for event-based algorithms to record the triggered events during the iteration process. Fewer event counts mean a lighter communication burden. The indicator "Relative error" describes the relative error between the convergence value for the CPS and the real optimal value. In addition, the algorithm [19] is selected as a benchmark algorithm, whose relative error is calculated as a reference.

Table 2
Comparison among different algorithms under the f-local attack model.

Algorithm	RDO	Event counts						Relative error
		ag.3	ag.4	ag.5	ag.6	ag.7	ag.8	
[10]	✗	\	\	\	\	\	\	\
[19]	✓	\	\	\	\	\	\	0.2%
[23]	✓	55	63	21	37	54	51	3.44%
[27]	✓	11	8	25	8	16	8	38.21%
RDO-E	✓	19	22	17	16	33	26	1.16%

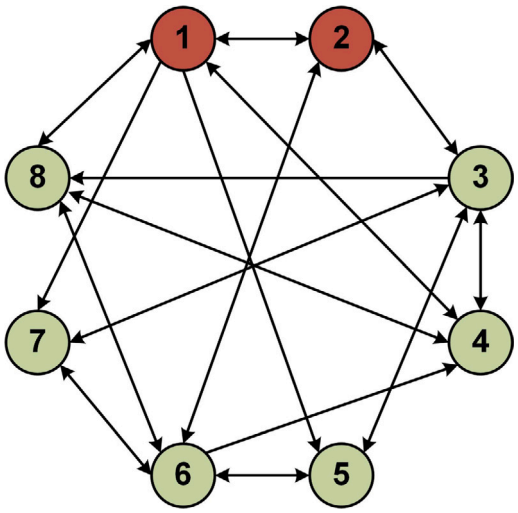


Fig. 8. A 3-robust digraph with eight nodes.

From Table 2, it is shown that the proposed RDO-E algorithm reaches the closest relative error to the algorithm [19] and triggers with fewer events. It means that the RDO-E algorithm balances algorithmic performance and event-triggering performance. Consequently, the proposed RDO-E algorithm is superior in achieving resilient distributed optimization with higher accuracy and lower communication overheads.

4.4. Application of the proposed algorithm to microgrids

In this subsection, we apply the proposed RDO-E algorithm to a multi-microgrid system and endeavor to tackle a resilient economic dispatch problem (REDP). A microgrid, consisting of intelligent devices, surpasses conventional power grids in terms of communication and processing capabilities [34]. It is a typical CPS and is widely recognized as the future infrastructure for power systems. Microgrids benefit from the use of distributed algorithms to determine the optimal solution for REDP, as opposed to centralized techniques. The goal of REDP is to optimize the power output of each distributed energy resource (DER) in order to minimize the overall generation cost, while fulfilling the output constraints of individual DERs and defending against malicious attacks.

Consider a multi-microgrid system described by Fig. 12(a), where multiple microgrids interconnect with each other through the network and can retrieve the voltages of DER from neighboring microgrids [35]. The network topology of the multi-microgrid system is depicted in Fig. 12(b), which is verified to be a 5-robust graph. By invoking Theorem 2, the network is capable of tolerating at most two malicious microgrids in the in-neighbor set of each microgrid.

Suppose that Grids 1 and 2 are malicious. It can be verified that the multi-microgrid network satisfies the 2-local attack model. The benign grids will try to solve the following REDP:

$$\begin{aligned} &\arg\min_{x} F_3(x) = \frac{1}{6}\sum_{i=3}^{8} f_i(x_i) = \frac{1}{6}\sum_{i=3}^{8}\left(p_i x_i^2 + q_i x_i + r_i\right) \\ &\text{subject to } \lim_{k\to\infty}\left|x_i(k) - x_j(k)\right| \le c, \quad \forall i,j \in \mathcal{B} \\ &\lim_{k\to\infty} x_i(k) \in \Psi = [m^*, M^*], \quad \forall i \in \mathcal{B}, \end{aligned} \tag{57}$$

where x_i is the output generation of Grid i, and $f_i(x_i) = p_i x^2 + q_i x + r_i$ is a specific local cost function corresponding to Grid i. The parameters for $f_i(x_i)$ are set as $[p_1, \ldots, p_8]^{\mathrm{T}} = [0.6, 0.3, 0.5, 0.8, 0.2, 0.5, 0.7, 0.4]^{\mathrm{T}}$, $[q_1, \ldots, q_8]^{\mathrm{T}} = [-10, -13, -6, -10, -5, -4, -7, -8]^{\mathrm{T}}$, and $[r_1, \ldots, r_8]^{\mathrm{T}} = [20, 30, 35, 10, 15, 25, 10, 15]^{\mathrm{T}}$. The initial output generations for grids are given by $[x_1(0), \ldots, x_8(0)]^{\mathrm{T}} = [0, 5, 10, 0, 12, 4, 0, 8]^{\mathrm{T}}$. The safety interval is calculated as $\Psi = [4, 12.5]$. Furthermore, we set the parameters concerning trigger function (7) as $c_0 = c_1 = 0.05$, $\delta = 0.03$.

Subsequently, we apply the proposed RDO-E algorithm into the multi-microgrid system and obtain the convergence result, as shown in Fig. 13(a). It is observed that despite the influence of Grids 1 and 2, the output generations of benign grids eventually converge within Ψ and approach the optimal value $x_i^* = 6.45$, $\forall i \in \mathcal{B}$ of the problem (57). This result means that the resilient economic dispatch problem has been successfully solved. Moreover, the triggering behavior in Fig. 13(b) indicates that the frequent information interaction between microgrids is significantly mitigated, thus the communication burden of the system is lightened.

5. Conclusion and future work

This study focuses on examining the resilient distributed optimization problem in CPSs when subject to f-total and f-local attack scenarios. To defend against malicious attacks, reduce communication overheads, and achieve resilient distributed optimization, an event-based RDO-E algorithm is developed. The convergence and optimality analyses for two attack models are conducted, respectively. The simulation results validate the theoretical analysis. For the f-total attack scenario, the proposed RDO-E algorithm ensures that the state values of benign agents converge to a safety interval determined by local optimal values if the cyber–physical network is $(f+1, f+1)$-robust. For the f-local attack scenario, despite two malicious agents exist in the network, the proposed RDO-E algorithm still guarantees that the state values of benign agents converge to the safety interval if the cyber–physical network is $(2f+1)$-robust. From the comparison results, it is shown that the proposed RDO-E algorithm effectively reduces the communication overheads and has a lower relative error than other event-based algorithms. In addition, the proposed method is applicable to multi-microgrid systems and has successfully tackled a resilient economic dispatch problem.

Future work will include the consideration of other malicious attacks and external disturbances, e.g., protocol attacks, communication delay, and noise. Extending the obtained results to higher-dimensional space would also be of significant theoretical and practical interest.

CRediT authorship contribution statement

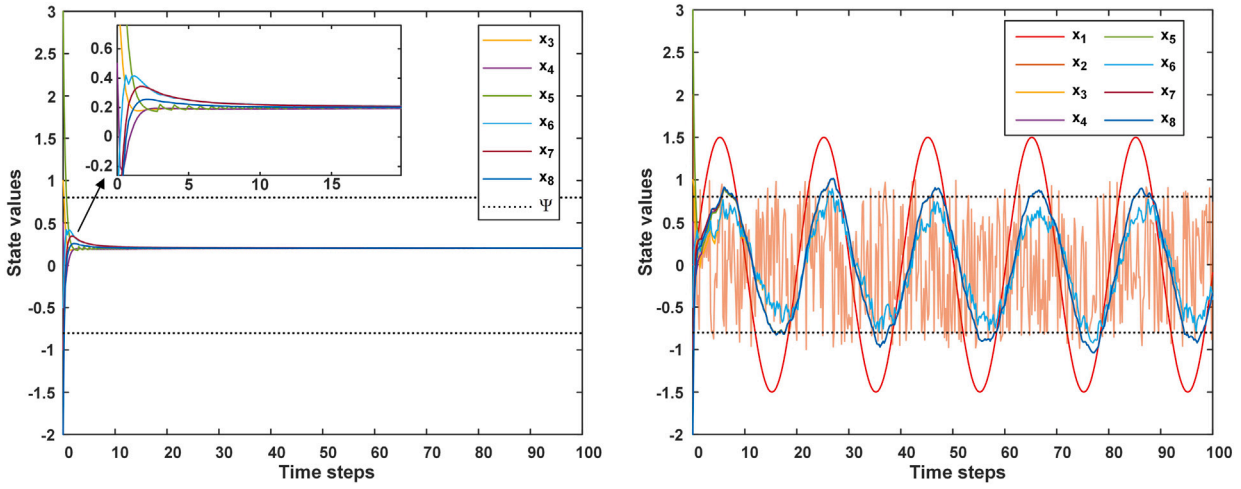
Zirui Liao: Writing – original draft, Writing – review & editing, Formal analysis, Investigation, Methodology. **Shaoping Wang:** Project administration, Supervision, Validation, Funding acquisition. **Jian Shi:** Supervision, Project administration. **Ming Li:** Investigation, Methodology, Writing – original draft. **Yuwei Zhang:** Validation, Investigation, Writing – original draft. **Zhiyong Sun:** Supervision, Methodology, Project administration, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

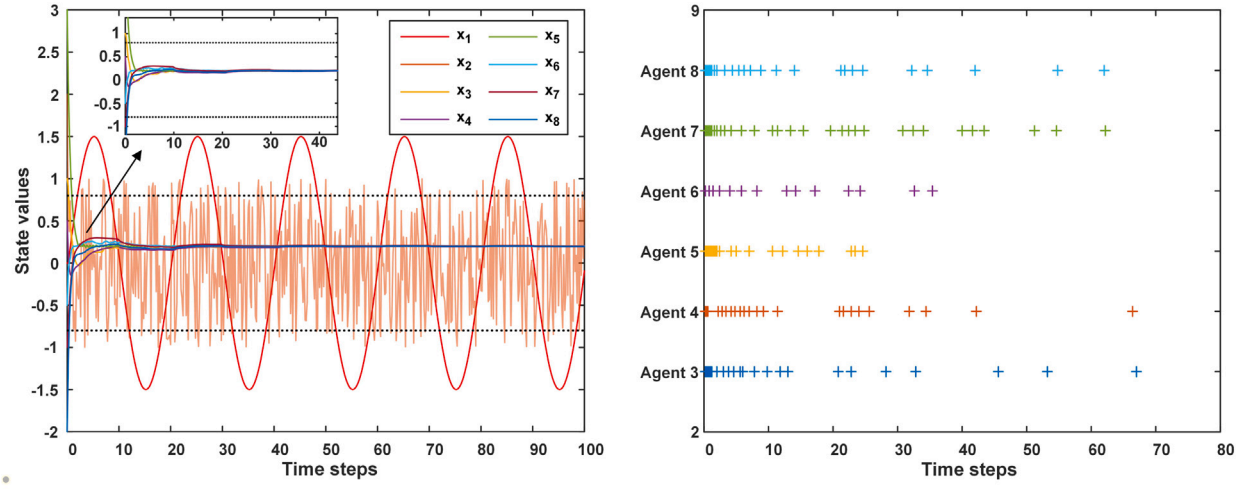
Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grants No. U2233212 and 62303030), the Beijing Municipal Natural Science Foundation (Grant No. L221008), the China Scholarship Council (Grant No. 202206020114), and the Outstanding Research Project of Shen Yuan Honors College (Grant No. 230122204).



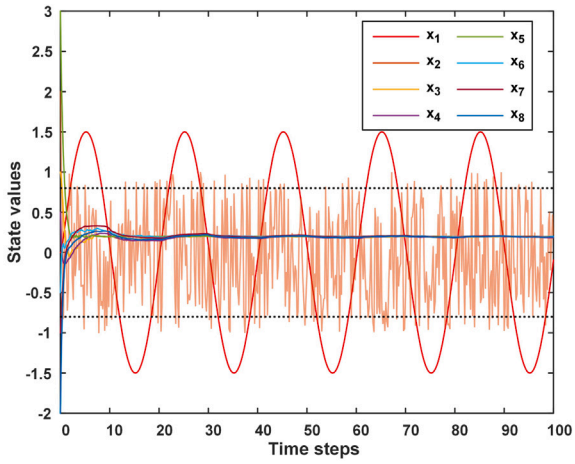
(a) Benign agents achieve RDO. (b) Benign agents fail to achieve RDO.

Fig. 9. Convergence results using the algorithm proposed in [10]: (a) without the malicious attack; (b) with the malicious attack.

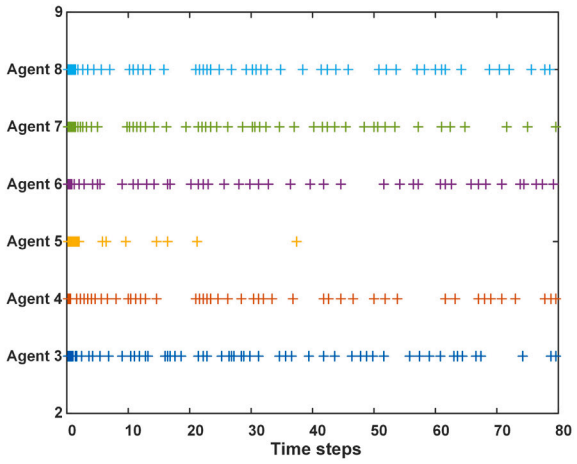


(a) Benign agents achieve RDO. (b) Triggering behavior of the RDO-E algorithm.

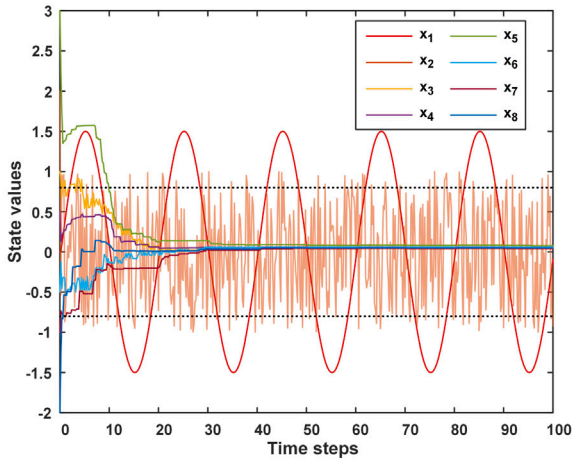
Fig. 10. Convergence result and triggering behavior using the proposed RDO-E algorithm: (a) trajectories of agents; (b) event instants with the event function (7).



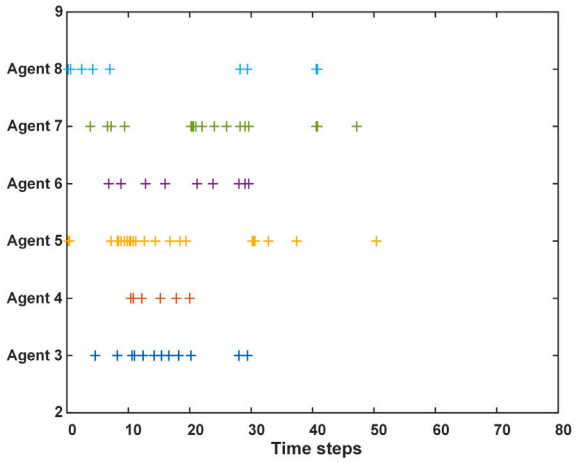
(a) Benign agents achieve RDO.



(b) Triggering behavior of the algorithm [23].

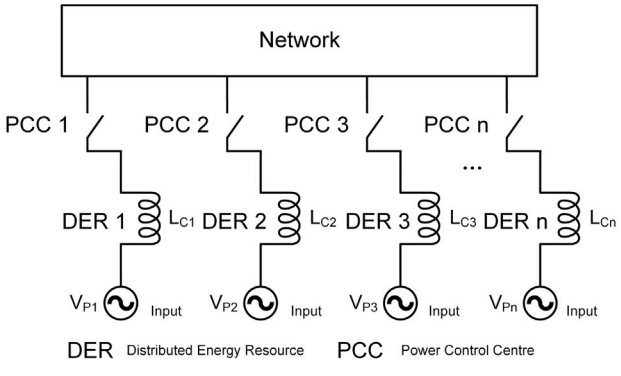


(c) Benign agents achieve RDO.

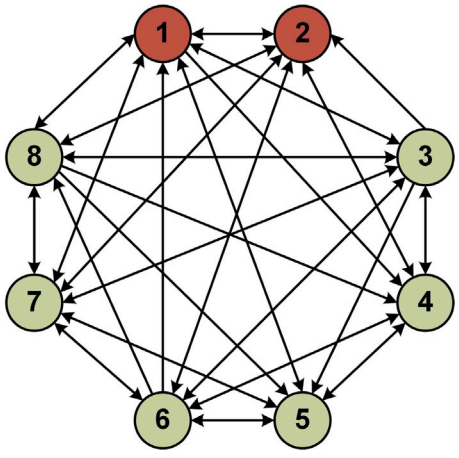


(d) Triggering behavior of the algorithm [27].

Fig. 11. Convergence results and triggering behaviors: (a) trajectories of agents using the algorithm proposed in [23]; (b) event instants using the algorithm proposed in [23]; (c) trajectories of agents using the algorithm proposed in [27]; (d) event instants using the algorithm proposed in [27].

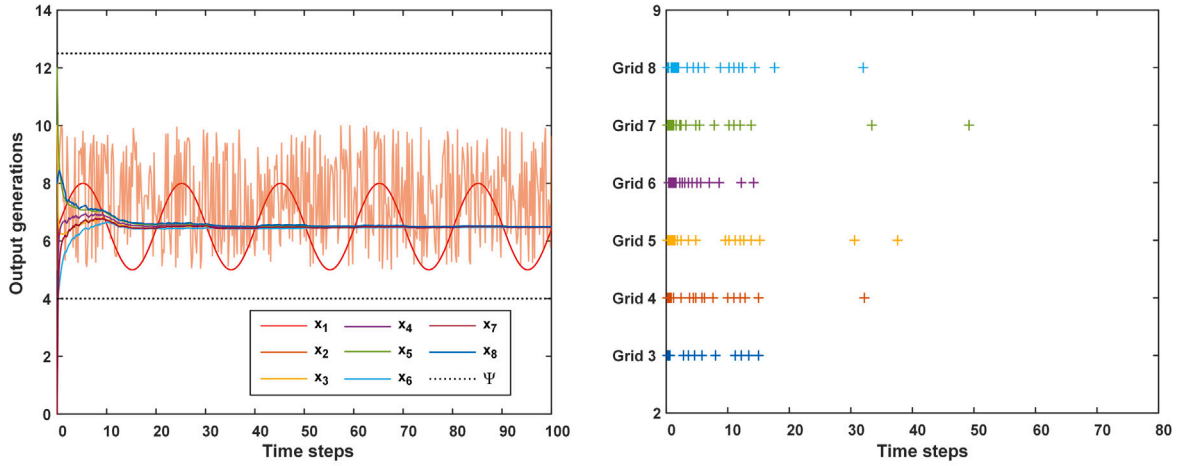


(a) A multi-microgrid system.



(b) A 5-robust digraph with eight grids.

Fig. 12. An illustration of the multi-microgrid system and its corresponding network topology.



(a) Benign microgrids tackle REDP. (b) Triggering behavior of the RDO-E algorithm.

Fig. 13. Convergence result and triggering behavior of the multi-microgrid system using the proposed RDO-E algorithm: (a) Output generations of microgrids; (b) event instants with the event function (7).

References

[1] Sun Z, Mou S, Anderson BDO, Cao M. Exponential stability for formation control systems with generalized controllers: A unified approach. Systems Control Lett 2016;93:50–7.

[2] Agrawal N, Kumar R. Security perspective analysis of industrial cyber physical systems (I-CPS): A decade-wide survey. ISA Trans 2022;130:10–24.

[3] Alur R. Principles of cyber-physical systems. MIT Press; 2015.

[4] Huang J, Fan J, Dinh TN, Zhao X, Zhang Y. Event-triggered interval estimation method for cyber–physical systems with unknown inputs. ISA Trans 2023;135:1–12.

[5] Gao X, Yang X, Meng L, Wang S. Fast economic dispatch with false data injection attack in electricity-gas cyber–physical system: A data-driven approach. ISA Trans 2023;137:13–22.

[6] Kim KD, Kumar PR. Cyber-physical systems: A perspective at the centennial. Proc IEEE 2012;100(Special Centennial Issue):1287–308.

[7] Zhang Y, Wang S, Heinrich MK, Wang X, Dorigo M. 3D hybrid formation control of an underwater robot swarm: Switching topologies, unmeasurable velocities, and system constraints. ISA Trans 2023;136:345–60.

[8] Yang T, Yi X, Wu J, Yuan Y, Wu D, Meng Z, et al. A survey of distributed optimization. Annu Rev Control 2019;47:278–305.

[9] Liao Z, Wang S, Shi J, Sun Z, Zhang Y, Sial MB. Cooperative situational awareness of multi-UAV system based on improved D-S evidence theory. Aerosp Sci Technol 2023;142:108605.

[10] Nedic A, Ozdaglar A. Distributed subgradient methods for multi-agent optimization. IEEE Trans Automat Control 2009;54(1):48–61.

[11] Nedic A, Ozdaglar A, Parrilo PA. Constrained consensus and optimization in multi-agent networks. IEEE Trans Automat Control 2010;55(4):922–38.

[12] Shi W, Ling Q, Wu G, Yin W. Extra: An exact first-order algorithm for decentralized consensus optimization. SIAM J Optim 2015;25(2):944–66.

[13] Varagnolo D, Zanella F, Cenedese A, Pillonetto G, Schenato L. Newton–Raphson consensus for distributed convex optimization. IEEE Trans Automat Control 2015;61(4):994–1009.

[14] Zuo S, Lewis FL, Davoudi A. Resilient output containment of heterogeneous cooperative and adversarial multigroup systems. IEEE Trans Automat Control 2019;65(7):3104–11.

[15] Zhang H, Sundaram S. Robustness of information diffusion algorithms to locally bounded adversaries. In: Proc. of the 2012 American control conference. 2012, p. 5855–61.

[16] LeBlanc HJ, Zhang H, Koutsoukos X, Sundaram S. Resilient asymptotic consensus in robust networks. IEEE J Sel Areas Commun 2013;31(4):766–81.

[17] Sundaram S, Gharesifard B. Consensus-based distributed optimization with malicious nodes. In: 2015 53rd annual allerton conference on communication, control, and computing. IEEE; 2015, p. 244–9.

[18] Sundaram S, Gharesifard B. Distributed optimization under adversarial nodes. IEEE Trans Automat Control 2018;64(3):1063–76.

[19] Fu W, Ma Q, Qin J, Kang Y. Resilient consensus-based distributed optimization under deception attacks. Internat J Robust Nonlinear Control 2021;31(6):1803–16.

[20] Xu C, Liu Q. A resilient distributed optimization algorithm based on consensus of multi-agent system against two attack scenarios. J Franklin Inst 2022;360(12):9096–114.

[21] Zhao C, He J, Wang Q. Resilient distributed optimization algorithm against adversarial attacks. IEEE Trans Automat Control 2019;65(10):4308–15.

[22] Xu C, Liu Q. A trust-based resilient consensus algorithm for distributed optimization considering node and edge attacks. Internat J Robust Nonlinear Control 2023;33(6):3517–34.

[23] Seyboth GS, Dimarogonas DV, Johansson KH. Event-based broadcasting for multi-agent average consensus. Automatica 2013;49(1):245–52.

[24] Gu Z, Yue D, Tian E. On designing of an adaptive event-triggered communication scheme for nonlinear networked interconnected control systems. Inform Sci 2018;422:257–70.

[25] Sun Z, Huang N, Anderson BDO, Duan Z. Event-based multiagent consensus control: Zeno-free triggering via $\mathcal{L}^p$ signals. IEEE Trans Cybern 2018;50(1):284–96.

[26] Li S, Liang K, He W. Fully distributed event-triggered secure consensus of general linear multi-agent systems under sequential scaling attacks. ISA Trans 2022;127:146–55.

[27] Wang Y, Ishii H. An event-triggered approach to quantized resilient consensus. Internat J Robust Nonlinear Control 2020;30(11):4188–204.

[28] Li Z, Xu H, Lin Z, Dong L, Chen Y. Event-triggered robust distributed output feedback model predictive control for nonlinear MASs against false data injection attacks. ISA Trans 2023;1–15.

[29] Kuwaranancharoen K, Xin L, Sundaram S. Byzantine-resilient distributed optimization of multi-dimensional functions. In: Proc. of the 2020 American control conference. IEEE; 2020, p. 4399–404.

[30] Xing L, Wen C, Guo F, Liu Z, Su H. Event-based consensus for linear multiagent systems without continuous communication. IEEE Trans Cybern 2016;47(8):2132–42.

[31] Wen G, Lv Y, Zheng WX, Zhou J, Fu J. Joint robustness of time-varying networks and its applications to resilient consensus. IEEE Trans Automat Control 2023;68(11):6466–80.

[32] Gupta N, Doan TT, Vaidya NH. Byzantine fault-tolerance in decentralized optimization under 2f-redundancy. In: 2021 American control conference. IEEE; 2021, p. 3632–7.

[33] Gupta N, Vaidya NH. Fault-tolerance in distributed optimization: The case of redundancy. In: Proceedings of the 39th symposium on principles of distributed computing. 2020, p. 365–74.

[34] Mao S, Dong Z, Schultz P, Tang Y, Meng K, Dong ZY, et al. A finite-time distributed optimization algorithm for economic dispatch in smart grids. IEEE Trans Syst Man Cybern A 2019;51(4):2068–79.

[35] Yassaie N, Hallajiyan M, Sharifi I, Talebi H. Resilient control of multi-microgrids against false data injection attack. ISA Trans 2021;110:238–46.