This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2954363, IEEE Transactions on Automatic Control

Resilient Distributed Optimization Algorithm against Adversarial Attacks⋆

Chengcheng Zhao, *Member, IEEE*, Jianping He, *Member, IEEE*, and Qing-Guo WANG, *Senior Member, IEEE*

***Abstract*—As the cyber-attack is becoming one of the most challenging threats faced by Cyber-Physical Systems (CPS), investigating the effect of cyber-attacks on distributed optimization and designing resilient algorithms are of both theoretical merits and practical values. Most existing works are established on the assumption that the maximum tolerable number of attacks, which depends on the network connectivity (N-CON), is known by all normal agents. All normal agents will use the maximum number of attacks to decide whether the received information will be used for iterations. In this paper, we relax this assumption and propose a novel resilient distributed optimization algorithm. The proposed algorithm exploits the trusted agents which cannot be compromised by adversarial attacks and form a connected dominating set in the original graph to constrain effects of adversarial attacks. It is shown that local variables of all normal and trusted agents converge to the same value under the proposed algorithm. Further, the final solution belongs to the convex set of minimizers of the weighted average of local cost functions of all trusted agents. The upper bound of the distance between the final solution and the optimal one has also been provided. Numerical results are presented to demonstrate the effectiveness of the proposed algorithm.**

***Index Terms*—Distributed Optimization, Adversarial Attacks, Connected Dominating Set, Trusted Agents, Resilient Algorithm**

I. Introduction

The cyber-attack has become one of the most challenging threats faced by CPS [2], which can make existing distributed algorithms vulnerable or even invalid and thus lead to system damage and even paralysis [3]. Therefore, it is necessary to investigate effects of cyber-attacks on distributed algorithms and improve their resilience to enhance CPS cyber-securities. We consider distributed optimization, where multiple agents aim to minimize the average of their local cost functions corresponding to one decision variable. With several potential advantages of strong robustness, high scalability, and computation efficiency compared to centralized one, distributed optimization has been widely used in CPS for various purposes, such as machine learning [4] and energy management [5]. To meet application requirements, much attention has been paid to distributed algorithm design and their performance analysis [6]. However, most these works are built on the hypothesis that the network surrounding is benign without any intruder.

For distributed optimization, adversarial attacks are divided into malicious and Byzantine attacks according to the threat scope of the attacker [7]. Especially, malicious attacks intend to disrupt the network functions by sending the same arbitrary state to their neighbors during the periodic information exchange, while Byzantine attacks are able to send different arbitrary states to different neighbors. Typical malicious attacks include DoS and false data injection. Note that the privacy attacks, e.g., eavesdropping attack, are not considered, since such attacks will not disrupt the network function. Consensus under adversarial attacks has been studied extensively. Denote the maximum amount of tolerable attacks by F. Analysis on the relationship of F, the number of total agents, and N-CON[1] has been provided for consensus under adversarial attacks and a sequence of resilient consensus algorithms were developed in [8], [9]. The key idea in most of these existing algorithms is to avoid utilizing malicious states broadcast by adversarial agents to guaranteed that the final state is within the interval of the smallest initial state and the largest one. To relax the assumption on F, Abbas *et al.* [10] proposed a resilient consensus algorithm with trusted agents (RCP-T), under which the number of tolerable attacks can be arbitrarily large. For general distributed optimization under malicious attacks, Sundaram *et al.* proposed a resilient algorithm by removing F largest and smallest states at each iteration, under which the final solution will belong to the convex hull of the set of all normal agents' local minimizers [3]. Moreover, considering the complete graph and Byzantine attacks, Su *et al.* proposed a series of resilient algorithms by removing F largest and smallest states [11], [12]. Authors also demonstrated that the final state belongs to the well-defined set of optimal solutions of the constrained optimization problem, i.e., minimizing the weighted average of all uncompromised agents' functions subject to constraints that a constant number of weights are lower bounded by a constant weight. It should be pointed out that most these algorithms are only effective when F is known and is strictly dependent on N-CON. To relax this limitation, Sundaram *et al.* [7] proposed the local filtering consensus-based algorithm to bear F local adversarial

⋆The preliminary result of this work was presented in part at the 13th IEEE International Conference on Control and Automation (IEEE ICCA 2017) [1]. This work was supported in part by NSF61973218, NSF61903328, and CPSF511200-X91902. Qing-Guo WANG acknowledges the financial support of the National Research Foundation of South Africa (Grant Numbers: 113340, 120106), which partially funded his research on this work.

Chengcheng Zhao is with State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou, China (email: zccsq90@gmail.com).

Jianping He is with the Department of Automation, Shanghai Jiao Tong University, Shanghai, China (email: jianpinghe.zju@gmail.com).

Qing-Guo WANG, Institute for Intelligent Systems, Faculty of Engineering and the Built Environment, University of Johannesburg, South Africa. (email: wangq@uj.ac.za).

[1]N-CON means the least number of agents or edges that can be cut from the network to make the rest network unconnected.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2954363, IEEE Transactions on Automatic Control

attacks, where the network has to be at least $(F+1, F+1)$-robust. Nonetheless, the effectiveness of the algorithm is still restricted by N-CON.

To relax the assumption on F, we design a resilient distributed optimization algorithm by exploiting trusted agents (RDO-T). The idea of RDO-T is inspired by (RCP-T), under which the number of tolerable attacks can be any large and the final state belongs to the interval of the largest and smallest initial states. The differences between our work and [10] are two-fold: 1) In the iteration process, the differential of local cost function is utilized for state update, which makes the convergence analysis inapplicable; 2) Since the dynamic of states of all normal and trusted agents is a nonlinear process, how to evaluate the optimality of the final state of RDO-T under adversarial attacks is more complex and challenging. Compared to our previous work [1], the explicit definition is provided for the graph composed by normal and trusted agents, a detailed model for adversarial attacks has been added, and the justifications on assumptions and the problem of interests have been changed to make it more clear. Further, we have provided more specific theoretical results to make the performance analysis more complete and rigorous, e.g., a tighter set is given to constrain the final point. Moreover, more simulation results and potential research topics are provided. The main contributions of this work are summarized as follows:

1. We investigate the problem of distributed optimization under adversarial attacks when the backbone of the network is protected, where the tolerable number of adversarial agents is unknown and can be arbitrarily large.
2. We design RDO-T, where the trusted agents induce a dominating connected set of the original network to overcome adversarial attacks. Under RDO-T, the normal agent only use states bounded by the largest and smallest state among its neighbors and itself for iterations.
3. We show that under RDO-T, consensus is achieved by all normal and trusted agents and the final solution is bounded by the convex set of minimizers of weighted average of all trusted agents' local cost functions. Under RDO-T, the variation of the final solution from the optimal one is also analyzed.

The remainder of this paper is organized as follows. Section II provides the models and formulates the problem, before the detailed resilient distributed optimization algorithm and the performance analysis are presented in Section III. Section IV verifies the main results through numerical results, while discussions regarding potential research directions are introduced in Section V. Conclusion is given in Section VI.

II. Preliminaries and Problem Formulation

A. Network Model

Consider a network with n ($n \geq 3$) agents having unique identifications (ID) denoted by $\{1, \cdots, n\}$. An undirected connected graph $G = (V, E)$ is utilized to represent the communication topology of the network, where V is the set of N nodes (agents) and $E \subset V \times V$ is the edge set. Since the network is undirected, we have that $(j, i) \in E \Leftrightarrow (i, j) \in E$. We omit self loops in G just for the notational convenience. In fact, each agent is able to obtain its local information. The neighbor set of node i is defined as $N_i = \{j \in V \,|\, (j, i) \in E\}$ and $|N_i|$ is its cardinality. In this paper, we consider a connected network and there exists only one clique.

We divide nodes into three types, i.e., normal nodes, trusted nodes, and adversarial nodes. Specifically, normal nodes may crash or be compromised by the attacker. Trusted nodes have a higher security level, which cannot crash or be compromised by the attacker. Adversarial nodes include malicious or Byzantine attackers, which are aware of the network structure. Meanwhile, the adversarial nodes know the update rule of normal nodes, which can be easily realized through a period of latent probe [13]. The sets of normal nodes, trusted nodes, and adversarial nodes are denoted by V_n, V_t, and V_a, respectively. Let $n_1 = |V_n|$, $n_2 = |V_t|$, and $n_a = |V_a|$ represent their cardinalities, respectively. Suppose that each node is able to identify the trusted nodes among their neighbors. To simplify the notation, we denote $n_0 = n_1 + n_2$ and IDs of all trusted and normal agents are among $\{1, \cdots, n_0\}$. Let $A \in \mathbb{R}^{n_0 \times n_0}$ be the adjacency matrix corresponding to the graph composed of all normal and trusted nodes, where $a_{ij} = 1$ if and only if $(i, j) \in E$ and $a_{ij} = 0$, otherwise. Meanwhile, we use $D \in \mathbb{R}^{n_0 \times n_0}$ to represent the diagonal matrix with $D_{ii} = |N_i|$. We provide the definition of the connected dominating set by referring to [14], which plays a key role in the defense strategy design. The subgraph $G_1 = (V_1, E_1)$, and the assumption satisfied by trusted nodes are also given.

***Definition** 1:* A set C of graph $G = (V, E)$ is a connected dominating set (CDS) if each node which does not belong to C has at least one neighbor in C and all nodes in C form a connected graph.

***Definition** 2:* $G_1 = (V_1, E_1)$ is the subgraph of G, where $V_1 = V_t \cup V_n$ and $E_1 \in E$ includes all edges connecting trusted nodes and all directed edges from trusted nodes to neighbor normal ones. The diameter of graph G_1 is denoted as d.

***Assumption** 1:* Trusted agents induce a CDS of $G = (V, E)$.

***Remark** 1:* Although Assumption 1 seems strong, we believe that it is reasonable to assume that the attacker has limited resources to compromise agents. Therefore, we make an assumption that trusted agents cannot be compromised by the attacker. Further, if the attacker is able to do anything to all nodes, it seems impossible to design defense mechanisms that guarantee network functionality. In practice, the security of trusted agents can be enhanced by computing hardening or redundant backup [15]. As a result, the attacker needs more resources to compromise trusted agents compared to compromising normal ones. Moreover, the identity authentication technology can be applied to ensure that all agents are capable of identifying neighboring trusted agents [16].

Actually, Assumption 1 can be treated as the problem of finding a CDS of the graph. Although introducing Assumption 1 brings extra cost, numerous approximate algorithms have been proposed for finding a CDS in a graph, which even can be solved in a distributed way [17]. Moreover, CDS has been widely used in the routing protocol design for mobile ad hoc networks. For example, a CDS is commonly utilized for constructing the virtual backbone for mobile wireless sensor networks to solve the broadcasting storm problem [18].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2954363, IEEE Transactions on Automatic Control

Assumption 1 could be true for these networks once the security enhancement is implemented to these nodes of a CDS.

B. Distributed Optimization under Adversarial Attacks

Let $f_i(x) : \mathbb{R} \to \mathbb{R}$, be the local cost function of agent i, where x is the global variable. Suppose that each $f_i(x), \forall i \in V$, is convex, continuously differentiable ($f_i'(x)$ denotes the gradient) and is also Lipschitz continuous, i.e., $f_i'(x) \leq L$, where L is a constant. It is assumed that the optimal point set $\arg\min f_i(x)$, is nonempty, bounded and closed. Distributed optimization problem is formulated as,

$$\min \frac{1}{n} \sum_{i=1}^{n} f_i(x). \tag{1}$$

Let $x_i(k)$ be the state of local variable x_i of node i at iteration k. The state vector of all normal and trusted nodes at iteration k is denoted by $\mathbf{x}(k) = [x_1(k), \cdots, x_{n_0}(k)]^{\mathrm{T}} \in \mathbb{R}^{n_0}$. In this paper, suppose that each node would like to keep its local cost function confidential, and static, synchronous communication model is set for all nodes.

Attack model: Consider that the attacker is able to make compromised nodes update states arbitrarily and broadcast different states to different neighbors. In order to tolerate such attacks, we have to consider the worst case, i.e., compromised nodes change local cost functions and follow the iteration rule like normal nodes. It is difficult to judge whether adversarial agents behave normally and thus solving problem (1) by following the consensus-based gradient descent algorithm (CGDA) does not work anymore. As a result, for all normal and trusted nodes, the problem becomes cooperatively minimizing the average of their local cost functions, i.e.,

$$\min \frac{1}{n_0} \sum_{i \in V_n \cup V_t} f_i(x). \tag{2}$$

Problem (2) cannot be solved exactly in a distributed way [19], i.e., the optimal solution of problem (2) cannot be achieved in a fully distributed way. The reason is that if each node keeps its local cost function confidential, normal or trusted nodes cannot detect and identify the compromised nodes through local interactions. As a result, it is desirable to solve the approximate version of problem (2), i.e., minimizing the weighted average of all trusted agents' local cost functions.

C. Problem of Interests

It is worth noting that relaxing the dependence of the number of tolerable adversarial nodes on N-CON is a very difficult and challenging problem [19]. To enhance the security of the network, it is a good choice to protect the backbone of the original network from the attacker, which means that nodes in a CDS need to be secure. Under this protection framework, we consider a powerful attacker, which means that the tolerable number of compromised agents is unknown by other nodes and the compromised nodes can behave arbitrarily. We then aim to find a way to guarantee the resilience of the distributed optimization under such powerful attacks. Although some assumptions are required, it is meaningful to design a framework to defend the function of distributed optimization even for the powerful attack scenarios. Therefore, it is practical and promising to design a resilient algorithm for solving the approximate version of problem (2) to overcome adversarial attacks under Assumption 1, where F can be an arbitrary number. Moreover, how to guarantee the consensus of local variables and how to evaluate the optimality of the final solution of the resilient algorithm are also interesting issues.

III. Main Results

A. Algorithm Design

We provide a RDO-T algorithm by entrusting a subset of agents to overcome adversarial attacks in this section, where each normal node only uses neighbor's states bounded by neighboring trusted nodes and itself. Thus, the resilience is guaranteed for the distributed optimization even when the amount of adversarial nodes is arbitrarily large. Let $f_i'(k) = f_i'(x_i(k))$ and $\{\alpha_0, \cdots, \alpha_\infty\}$ be the sequence of stepsizes, which satisfies $\sum_{k=0}^{\infty} \alpha_k = \infty$, $\sum_{k=0}^{\infty} \alpha_k^2 < \infty$ and $\alpha_{k+1} \leq \alpha_k$. $\sum_{k=0}^{\infty} \alpha_k = \infty$ and $\alpha_{k+1} \leq \alpha_k$ are used to ensure that states of nodes converge to the same optimizer in steady-state. Meanwhile, $\sum_{k=0}^{\infty} \alpha_k^2 < \infty$ is to make the algorithm applicable for general convex functions [20]. The details of RDO-T are given in Algorithm 1. In

Algorithm 1 (RDO-T)

Initialization: Each node i initializes $x_i(0)$ randomly.

Loop:

1. Each node i obtains the set $R_i(k)$, i.e., $R_i(k) = \{j | x_i^m(k) \leq x_j(k) \leq x_i^M(k), j \in N_i \cup \{i\}\}$.
2. Each node i updates $x_i(k+1)$ according to (3),

$$x_i(k+1) = \frac{1}{|R_i(k)|} \sum_{j \in R_i(k)} x_j(k) - \alpha_k f_i'(k), \tag{3}$$

where $|R_i(k)|$ denotes the cardinality of $R_i(k)$.

3. $|x_i(k) - x_j(k)|$, $j \in T_i$ for each node i is less than the prescribed error threshold, the loop terminates.

Output: $x_i(k)$, $\forall i, j \in V_n \cup V_t$.

Algorithm 1, after receiving the message from neighbors, each node i identifies the set of all neighboring trusted nodes, i.e., $T_i = \{j \,|\, j \in N_i, j \in V_t\}$. Then, node i sorts $x_j(k)$ for all $j \in T_i \cup \{i\}$ and obtains the maximum and minimum states represented by $x_i^M(k) = \max\{x_j(k) \,|\, j \in T_i \cup \{i\}\}$ and $x_i^m(k) = \min\{x_j(k) | j \in T_i \cup \{i\}\}$, respectively. It is pointed out here that RDO-T can also be used in directed strongly connected networks as long as the CDS is well defined. Moreover, it is noted that the CDS needs to be pre-implemented for RDO-T. The number of trusted nodes in CDS depends on N-CON, the total number of nodes in G, and the degree distribution [14].

B. Convergence and Optimality of RDO-T

To evaluate the performance of RDO-T, we first establish the existence of the transition matrix for all normal and trusted nodes at each iteration. The transition matrix is utilized to characterize the process of changing from one state of all normal and trusted nodes to another. The backward product of the transition matrices and its properties are then given. Meanwhile, we provide the convex set of the minimizers of the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2954363, IEEE Transactions on Automatic Control

weighted average of all trusted agents' functions inspired by to [19] and show that the final solution under RDO-T belongs to this set.

1) Existence of Transition Matrix: In what follows, we prove the existence of transition matrix under RDO-T and analyze its properties, which are crucial to subsequent analysis.

***Lemma** 1:* If Assumption 1 holds, under RDO-T, there exists $M(k) \in \mathbb{R}^{n_0 \times n_0}$ for all k such that

$$\mathbf{x}(k+1) = M(k)\mathbf{x}(k) - \alpha_k f'(k), \tag{4}$$

where $f'(k) = [f'_1(k), \cdots, f'_{n_0}(k)]^{\mathrm{T}}$ and $M(k) = [M_{ij}(k)]_{n_0 \times n_0}$ has the following properties, $\forall i \in V_t \cup V_n$:

i) $M(k)$ is a row stochastic matrix, i.e., $\sum_{j=1}^{n_0} M_{ij}(k) = 1$;
ii) $M_{ij}(k) \neq 0$ if and only if $(j,i) \in E_1 \cup \{(i,i)\}$;
iii) $\forall M_{ij}(k) \neq 0$, $M_{ij}(k) \geq \varphi = \frac{1}{d_M+1}$, $d_M = \max\{|N_i|\}$.

Proof: The proof can be found in Appendix A. ∎

2) Backward Product and Its Properties: According to (4),

$$\begin{aligned}\mathbf{x}(k+1) =& M(k)\mathbf{x}(k) - \alpha_k f'(k)\\ =& M(k)\cdots M(0)\mathbf{x}(0) - \sum_{t=0}^{k}(M(k)\cdots M(t+1))\alpha_t f'(t)\\ =& \Phi(k,0)\mathbf{x}(0) - \sum_{t=1}^{k+1}\Phi(k,t)\alpha_{t-1}f'(t-1),\end{aligned} \tag{5}$$

where $\Phi(k,t), t \leq k+1$, is the backward product with $\Phi(k,k) = M(k)$ and $\Phi(k,k+1) = \mathrm{I}_{n_0}$. I_{n_0} is an identity matrix of size $n_0 \times n_0$. By referring to [11], [21] and [12], we provide the following lemma directly.

***Lemma** 2:* If Assumption 1 holds, under RDO-T, $\Phi(k,t)$ has the following properties:

i) There are n_2 columns in $\Phi(t+n_0-1,t)$ lower bounded by $\varphi^d\mathbf{1}$ component-wise for all t, where $\mathbf{1} \in \mathbb{R}^{n_0}$, is a vector with all elements equal to 1;
ii) For $\Phi(k,t)$, there holds $\lim_{k\geq t, k\to\infty}\Phi(k,t) = \mathbf{1}\psi^{\mathrm{T}}(t)$, where $\psi(t)$ is a stochastic vector dependent on t;
iii) For any $\Phi(k,t)$, $|\Phi_{ij}(k,t) - \psi_i(t)| \leq (1-\varphi^{n_0})^{\lceil\frac{k-t+1}{n_0}\rceil}$;
iv) For any fixed t, n_2 nonzero entries in $\psi(t)$ are lower bounded by φ^d, i.e., there are n_2 nonzero entries $i \in \{1,\cdots,n_0\}$ such that, $\psi_i(t) \geq \varphi^d$.

***Remark** 2:* From Lemma 2, we see that the convergence and the final solution of the backward product are concluded, which make the convergence analysis of RDO-T possible. Moreover, as the lower bound of the final solution is provided in property iv), we can exploit this result to analyze where the final solution will belong under the proposed algorithm.

3) The Convex Optimal Set $Y(\mu,\nu)$: To evaluate where the final value of RDO-T will belong, the collection of functions is provided by referring to [19]. The collection is denoted by $C(\mu,\nu) = \{g(x)|g(x) = \sum_{i\in V_t}\beta_i f_i(x), \beta_i \geq 0, \sum_{i\in V_t}\beta_i = 1, \sum_{i\in V_t}\mathbf{I}\{\beta_i \geq \mu\} = \nu\}$, where $\mathbf{I}\{\cdot\}$ is the indicator function. For any given μ and ν, $C(\mu,\nu)$ is a valid function. Then, we define

$$Y(\mu,\nu) = \cup_{g(x)\in C(\mu,\nu)}\arg\min_{x\in\mathbb{R}} g(x). \tag{6}$$

***Lemma** 3:* If $\mu = \varphi^d$ and $\nu = n_2$, $Y(\mu,\nu)$ is a convex set.

It should be pointed out that since the proposed algorithm in this paper is totally different from that in [11], the bounds of the parameters μ and ν are different.

4) Convergence and Optimality Analysis: Based on the above results, we prove that the convergence of RDO-T is guaranteed and the final solution will always belong to the minimizer of some weighted average of local cost functions of all trusted agents. The main idea of the proof is inspired by theoretical results in [12], but RDO-T and parameters are different so that the proof is different. We first provide $y(k)$ to which the local variable $x_i(k)$ will converge and then prove that $y(k)$ will converge to the convex set $Y(\mu,\nu)$ defined before. Assuming that for $k \geq \bar{k}$, $f'_i(k) = 0$, $\forall i \in V_t \cup V_n$, we have

$$\begin{aligned}&\mathbf{x}(k+\bar{k})\\ =&\Phi(k,\bar{k}-1)\mathbf{x}(\bar{k}-1) - \sum_{t=1}^{\bar{k}}\Phi(k,t)(\alpha_{t-1}f'(t-1))\\ =&\Phi(k,\bar{k})[\Phi(\bar{k},\bar{k}-1)\mathbf{x}(\bar{k}-1) - \sum_{t=1}^{\bar{k}}\Phi(\bar{k}-1,t)(\alpha_{t-1}f'(t-1))]\\ =&\Phi(k,\bar{k})\mathbf{x}(\bar{k}).\end{aligned} \tag{7}$$

Taking limits on both sides of (7) yields

$$\begin{aligned}\lim_{k\to\infty}\mathbf{x}(k+\bar{k}) =& \lim_{k\to\infty}\Phi(k,0)\mathbf{x}(0) - \sum_{t=1}^{\bar{k}}\lim_{k\to\infty}\Phi(k,t)(\alpha_{t-1}f'(t-1))]\\ =&\mathbf{1}\psi^{\mathrm{T}}(0)\mathbf{x}(0) - \sum_{t=1}^{\bar{k}}\alpha_{t-1}\mathbf{1}\psi^{\mathrm{T}}(t)f'(t-1)\\ =&[\langle\psi^{\mathrm{T}}(0),\mathbf{x}(0)\rangle - \sum_{t=1}^{\bar{k}}\alpha_{t-1}\langle\psi^{\mathrm{T}}(t),f'(t-1)\rangle]\mathbf{1},\end{aligned} \tag{8}$$

where $\langle,\rangle$ is the symbol for inner product of two vectors. We see that the limit of vector $\mathbf{x}(k+\bar{k})$ is a vector with all elements equal to one constant denoted by $y(\bar{k})$. Then, let $\mathbf{y}(\bar{k}) = [y(\bar{k}),\cdots,y(\bar{k})]^{\mathrm{T}} \in \mathbb{R}^{n_0}$. According to (8), we have

$$\begin{aligned}y(\bar{k}) =&\langle\psi^{\mathrm{T}}(0),\mathbf{x}(0)\rangle - \sum_{t=1}^{\bar{k}-1}\alpha_{t-1}\langle\psi^{\mathrm{T}}(t),f'(t-1)\rangle\\ &-\langle\alpha_{\bar{k}-1}\langle\psi^{\mathrm{T}}(\bar{k}),f'(\bar{k}-1)\rangle\\ =&y(\bar{k}-1) - \alpha_{\bar{k}-1}\langle\psi^{\mathrm{T}}(\bar{k}),f'(\bar{k}-1)\rangle.\end{aligned} \tag{9}$$

Denote $\{y(k)\}_{k=0}^{\infty}$ as the sequence obtained by (9) and $\{x_i(k)\}_{k=0}^{\infty}$ as the local variable sequence of node $i, i \in V_n \cup V_t$ acquired from (8).

***Theorem** 1:* If Assumption 1 holds, $\mu = \varphi^d, \nu = n_2$ and $\lim_{k\to\infty}\alpha_k = 0$, RDO-T achieves convergence and the final solution will belong to $Y(\mu,\nu)$, i.e.,

$$\lim_{k\to\infty}x_i(k) = \lim_{k\to\infty}x_j(k) \in Y(\mu,\nu), \forall i,j \in V_n \cup V_t. \tag{10}$$

Proof: The proof can be found in Appendix B. ∎

***Remark** 3:* Note that there is no requirement on the number of tolerable adversarial nodes in RDO-T and no condition on adversarial nodes is needed to guarantee the convergence and optimality. Hence, RDO-T is effective even when the number of adversarial nodes is very large. It means that the amount of adversarial nodes has no relationship with N-CON and when N-CON is small, RDO-T is still resilient for the distributed optimization against adversarial attacks. Further, as the key idea of RDO-T is distinct from these in existing works, μ and ν are different. In RDO-T, the resilience is guaranteed by entrusting a CDS of nodes in the network and μ, ν rely on the diameter of $G_1 = (V_1, E_1)$ and the number of trusted nodes.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2954363, IEEE Transactions on Automatic Control

5) Optimality Evaluation: Distributed optimization problem with adversarial attacks undergoes three steps in the above solving process. Let x^*, $\hat{x}^*$, and $\tilde{x}^*$ be the optimal solution of problem (1), (2), and $\min_x C(\mu, \nu)$, respectively. Then, we have

$$\frac{1}{n}\sum_{i=1}^{n} f_i'(x^*) = 0, \frac{1}{n_0}\sum_{i=1}^{n_0} f_i'(\hat{x}^*) = 0, \sum_{i\in V_t}\beta_i f_i'(\tilde{x}^*) = 0. \quad (11)$$

In the following part, we analyze the relationship between x^*, $\hat{x}^*$, $\tilde{x}^*$, and $f_i(x)$, $\forall i \in V$, and how the value of the final objective function varies from the optimal one.

***Lemma** 4:* If $\sum_{i=n_0+1}^{n} f_i'(x^*) \le 0$, $\hat{x}^* - x^* \ge 0$, and otherwise, $\hat{x}^* - x^* > 0$, i.e., the direction of the variance of the optimal solution under adversarial attacks is determined by the sum of derivatives of the compromised nodes' functions at the original optimal solution. Moreover, if $\beta_i \ge \frac{1}{n_0}$, $\forall i \in V_t$, when $\sum_{i\in V_n} f_i'(\hat{x}^*) \ge 0$, $\hat{x}^* - \tilde{x}^* \ge 0$, and otherwise, $\hat{x}^* - \tilde{x}^* < 0$.

Proof: The proof can be found in Appendix C. ∎

In order to obtain the distance between x^* and $\hat{x}^*$, and the distance between $\hat{x}^*$ and $\tilde{x}^*$, it is supposed that $\forall i \in V$, $f_i(x) \in C^2$, i.e., $f_i(x)$ is twice differentiable and $0 < C_1 \le f_i''(x) \le C_2$.

***Lemma** 5:* For problem (1) under adversarial attacks, if $\forall i \in V$, $f_i(x)$ is Lipschitz continuous, twice differentiable, and $0 < C_1 \le f_i''(x) \le C_2$, we have

$$\frac{|\sum_{i=n_0+1}^{n} f_i'(x^*)|}{n_0 C_2} \le |x^* - \hat{x}^*| \le \frac{|\sum_{i=n_0+1}^{n} f_i'(x^*)|}{n_0 C_1}, \quad (12)$$

$$\frac{|\sum_{i\in V_n} f_i'(\hat{x}^*)|}{n_0|\sum_{i\in V_t}(\frac{1}{n_0} - \beta_i)C_2|} \le |\hat{x}^* - \tilde{x}^*| \le \frac{|\sum_{i\in V_n} f_i'(\hat{x}^*)|}{n_0|\sum_{i\in V_t}(\frac{1}{n_0} - \beta_i)C_1|} \quad (13)$$

Proof: We provide the proof in Appendix D. ∎

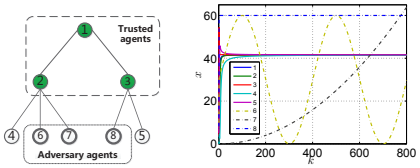
***Lemma** 6:* For problem (1) under adversarial attacks, if $\forall i \in V$, $f_i(x)$ is Lipschitz continuous, twice differentiable, and $0 \le f_i''(x) \le C_2$, we have

$$\begin{aligned} &|\frac{1}{n}\sum_{i=1}^{n} f_i(x^*) - \frac{1}{n_0}\sum_{i=1}^{n_0} f_i(\hat{x}^*)| \\ &\le |\frac{1}{n}\sum_{i=n_0+1}^{n} f_i(x^*)| + \frac{n-n_0}{n_0}|\frac{1}{n}\sum_{i=1}^{n_0} f_i(x^*)| + |(\hat{x}^* - x^*)L|, \end{aligned} \quad (14)$$

$$\begin{aligned} &|\frac{1}{n_0}\sum_{i=1}^{n_0} f_i(\hat{x}^*) - \sum_{i\in V_t}\beta_i f_i(\tilde{x}^*)| \\ &\le |\frac{1}{n_0}\sum_{i=1}^{n_1} f_i(\hat{x}^*)| + |\sum_{i\in V_t}(\frac{1}{n_0} - \beta_i) f_i(\hat{x}^*)| + n_2 L|\tilde{x}^* - \hat{x}^*|. \end{aligned} \quad (15)$$

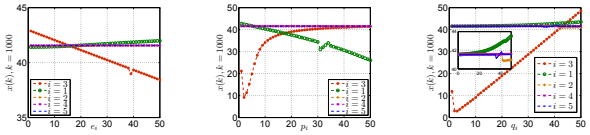
Proof: The proof is provided in Appendix E. ∎

***Remark** 4:* Algorithm 2 is given as: Trusted agents run the standard CGDA, and normal agents simply take the average of their trusted neighbors' local estimates). Under Algorithm 2, states of trusted agents will converge to the minima of $\frac{1}{n_2}\sum_{i\in V_t} f_i(x)$. As normal agents always follow their neighboring trusted agents and their states will converge to the same minimizer. Note that normal agents do not affect the final solution under Algorithm 2, but it is desirable to use the states of normal agents to solve problem (2). Meanwhile, more neighbors' states can be used in RDO-T, which may accelerate the convergence rate. Therefore, RDO-T will be more promising.



(a) an example (b) convergence

Fig. 1. A network example and performance evaluation



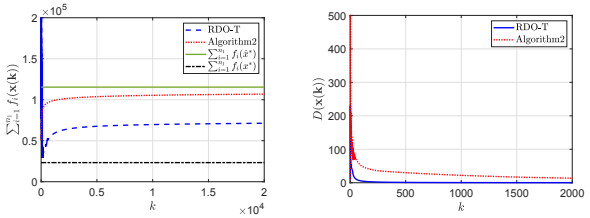
(a) Effect of e_i (b) Effect of p_i (c) Effect of q_i

Fig. 2. Effect of function parameters on the final value $x(k)$

IV. Numerical Results

In this section, we investigate the effectiveness of RDO-T through numerical results. Consider a network shown in Fig. 1(a) with $n = 8$ nodes including 3 adversarial, 3 trusted and 2 normal nodes. We set $f_i(x) = p_i\sqrt{e_i^2 + (x - q_i)^2}$, $\forall i \in V$ with different parameters e_i, $p_i > 0$, and q_i from intervals [8, 20], [0, 70], [-50, 80], respectively. First, we investigate the performance of RDO-T under no attacks. The optimal solution of (1) is $x^* = 2.90$, while the final value of the global variable under RDO-T becomes 41.58. The value of $\sum_{i\in}^{n_0} f_i(x)$ converges to 9316.4, while the optimal one is 7232.4. Due to step 1 and 2 in RDO-T, the positions of non-zero elements in system matrix is asymmetric. Further, since the parameters α_k goes to zero with iterations, it is not guaranteed that the derivative of the objective function goes to zero with k. Meanwhile, the final solution depends on the initial state, the specified function expressions, and the iterations k, implying that the final solution can be much deviated from the optimal one.

We then explore how RDO-T performs under adversarial attacks. For $k \ge 1$, adversarial nodes update their states as $x_6(k) = 30\sin(0.005\pi x_i(k-1)*k)+30$, $x_7(k) = (k/100)^2$, $x_8(k) = 60$. From Fig. 1(b), we see that all local variables of normal agents and trusted agents will converge under adversarial attacks. Furthermore, as N-CON shown in Fig. 1(a) is 1, the existing algorithm in [12] cannot tolerate one adversarial node. Meanwhile, the protocol proposed in [7] will also



(a) Optimality (b) Convergence Speed

Fig. 3. Comparisons of RDO-T and Algorithm 2

be invalid since the network is not (2,2)-robust[2]. Compared to these works, RDO-T is effective even when the number of adversarial nodes is arbitrary. We also investigate how parameters e_i, p_i and q_i affect the final value of $x_i(k)$, which demonstrates how different local cost functions impact the final value of $x(k)$. It is observed from Fig. 2 that node $i = 3$ will affect $x_i(\infty)$ more than other normal and trusted nodes. For different parameters of the same node, the tendencies of the effects are different.

Further, we consider two scenarios, i.e., a 50m×50m square with $n = 30$, and a large network with 200 nodes deployed in a 100m × 100m square. The communication radius of each node is 20m, nodes' positions are randomly selected in the square, and e_i, p_i, q_i are set from [1, 20], [0, 2800], [-100, 200]. After protecting a CDS, we randomly select 20 adversarial nodes. First, for the smaller network, let $\arg\min \frac{1}{n_2} \sum_{i\in V_t} f_i(x)$ ($\hat{x}* = 56.1682$) be largely deviated to $\arg\min \frac{1}{n_0} \sum_{i\in V_n\cup V_t} f_i(x)$ ($x* = 2.7377$). It is observed from Fig. 3(a) that under RDO-T, the final solution can be closer to the optimal solution of problem (2) by using more neighbors' states compared to Algorithm 2. For the large network, let $\hat{x}^*$ be near to x^*, and then more neighbors' states can be used by trusted and normal agents with a large probability. It is observed from Fig. 3(b) ($D(\mathbf{x}(k)) = \max(\mathbf{x}(k)) - \min(\mathbf{x}(k))$) that RDO-T may converge faster than Algorithm 2. It is because that using bounded states broadcast by adversarial nodes could enhance the connectivity of the network among normal and trusted nodes.

V. Discussions

Here, we give some potential and interesting topics, including attack modeling and practical applications.

Effect of Specific Attacks: For general attacks, we only provide a general bound for the final solution. But if we can identify the specific behavior of attacks, the effect of the attack on the convergence and optimality of distributed optimization can be analyzed in a more specific way. For instance, if the attacker compromises agents and launches Denial of Service attack, then the remaining nodes still minimize the average of their local cost functions subject to one global variable. The problem turns out to be that how the optimal solution will change compared with the original one. To solve this problem, the first step is to classify the behavior of attacks appropriately. Then, finding an effective way to characterize impact of the local cost function on the optimal solution will also be an interesting topic. The potential solution is to find a valid function space, which is based on the local minima.

Challenges in Practical Applications: Theoretically, it is usually claimed that under adversarial attacks, distributed optimization problem reduces to that all uncompromised agents cooperatively minimize the average of their local cost functions. But in practice, the problem transformation may not be rational. For example, distributed optimization algorithms have been investigated for DC-OPF problem with multiple regions. Considering that there is one compromised regional operator, although uncompromised operators can solve the transformed problem to certain extent, the compromised operator can still inject power to the transmission line arbitrarily. Thus, attack detection and identification are more important. Some algorithms have been proposed to intrusion detection and isolation (DIS) for distributed optimization under attacks, which are based on the detection theory, hypothesis testing and the trends of gradient variations [22]. Most existing works focus on DIS for specific attacks or particular algorithm scenario, where numerous extra iterations are required or more states of variables need to be transmitted during the iteration process. Thus, designing resilient optimization algorithms for real applications, where misbehaving nodes can be detected and identified effectively and efficiently, is of significance.

[2]For $G = \{V, E\}$, (r, s)-robust for some natural numbers r, s means that any pairs of nonempty subsets $S_1, S_2 \subset V$, at least one of the following conditions holds: 1) Each node in S_1 has at least r neighbors outside S_1; 2) Each node in S_2 has at least r neighbors outside S_2; 3) There exist at least s nodes in $S_1 \cup S_2$ that each has at least r neighbors outside their respective sets.

VI. Conclusion

In this paper, we developed a resilient distributed optimization algorithm under adversarial attacks by endowing a certain CDS of nodes with the high security. We proved that the convergence is guaranteed and the final solution will definitely join in the set of minimizers of the weighted average of all trusted agents' functions. We also found that how far the final solution will deviate from the optimal one is affected by normal and trusted agents' local cost functions. When the number of adversarial attacks is large and unknown, RDO-T is still resilient. It means that when N-CON is small, RDO-T is still effective. Furthermore, we found that when N-CON is large, protecting a small amount of agents with the high security is enough for RDO-T. Simulation results demonstrated the effectiveness of RDO-T and several discussions regarding potential research problems were also provided.

References

[1] C. Zhao, J. He, and Q.-G. Wang. Resilient distributed optimization algorithm against adversary attacks. In *Proc. IEEE ICCA*, pages 473–478. IEEE, 2017.

[2] F. Pasqualetti, F. Dörfler, and F. Bullo. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11):2715–2729, 2013.

[3] S. Sundaram and B. Gharesifard. Consensus-based distributed optimization with malicious nodes. In *Proc. Allerton*, pages 244–249. IEEE, 2015.

[4] L. Su and N. Vaidya. Robust multi-agent optimization: coping with byzantine agents with input redundancy. In *Proc. Symposium on Stabilization, Safety, and Security of Distributed Systems*, pages 368–382. Springer, 2016.

[5] 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*, 8(5):2049–2061, 2017.

[6] A. Nedic and A. Ozdaglar. Distributed optimization over time-varying directed graphs. *IEEE Transactions on Automatic Control*, 60(3):601–615, 2015.

[7] S. Sundaram and B. Gharesifard. Distributed optimization under adversarial nodes. *arXiv preprint arXiv:1606.08939*, 2016.

[8] F. Pasqualetti, A. Bicchi, and F. Bullo. Consensus computation in unreliable networks: A system theoretic approach. *IEEE Transactions on Automatic Control*, 57(1):90–104, 2012.

[9] H. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram. Resilient asymptotic consensus in robust networks. *IEEE Journal on Selected Areas in Communications*, 31(4):766–781, 2013.

[10] W. Abbas, Y. Vorobeychik, and X. Koutsoukos. Resilient consensus protocol in the presence of trusted node. In *Proc. ISRCS*, pages 1–7. IEEE, 2014.

[11] L. Su and N. Vaidya. Byzantine multi-agent optimization: Part ii. *arXiv preprint arXiv:1507.01845*, 2015.

[12] L. Su and N. Vaidya. Fault-tolerant distributed optimization (part iv): constrained optimization with arbitrary directed networks. *arXiv preprint arXiv:1511.01821*, 2015.

[13] K. Huang, M. Siegel, and M. Stuart. Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys (CSUR)*, 51(4):70, 2018.

[14] Y. Caro, D. West, and R. Yuster. Connected domination and spanning trees with many leaves. *SIAM Journal on Discrete Mathematics*, 13(2):202–211, 2000.

[15] C. Kopp. Hardening your computing assets. *Asia/Pacific Open Systems Review. Computer Magazine Group, NSW under the title of Information WarfarePart*, 2, 1997.

[16] K. T. Nguyen, M. Laurent, and N. Oualha. Survey on secure communication protocols for the internet of things. *Ad Hoc Networks*, 32:17–31, 2015.

[17] J. Wu and H. Li. On calculating connected dominating set for efficient routing in ad hoc wireless networks. In *Proc. DIAL-M*, pages 7–14. ACM, 1999.

[18] B. Liu, W. Wang, D. Kim, Y. Li, S-S. Kwon, and Y. Jiang. On practical construction of quality fault-tolerant virtual backbone in homogeneous wireless networks. *IEEE/ACM Transactions on Networking*, 26(1):412–421, 2018.

[19] L. Su and N. Vaidya. Byzantine multi-agent optimization: Part i. *arXiv preprint arXiv:1506.04681*, 2015.

[20] R. Xin and U. A. Khan. A linear algorithm for optimization over directed graphs with geometric convergence. *IEEE Control Systems Letters*, 2(3):315–320, 2018.

[21] N. Vaidya. Matrix representation of iterative approximate byzantine consensus in directed graphs. *arXiv preprint arXiv:1203.1888*, 2012.

[22] N. Ravi, A. Scaglione, and A. Nedić. A case of distributed optimization in adversarial environment. In *Proc. ICASSP*, pages 5252–5256. IEEE, 2019.

APPENDIX

A. Proof of Lemma 1

Proof: Due to the loop in RDO-T, node $i \in V_n \cup V_t$ only utilizes $x_j(k), j \in R_i(k)$, which are bounded by the maximum and minimum states among node i and its trusted neighbors. Hence, $R_i(k) \subseteq N_i$, that is, $\frac{1}{|R_i(k)|} \geq \frac{1}{|N_i|+1}$. We divide the states that each normal or trusted node i will utilize for state update at iteration k into three sets, i.e., the set of states of neighboring trusted nodes (denoted by $S_i(k)$), the set composed of its own state ($\{x_i(k)\}$), and the set of states of its neighboring adversarial nodes and normal nodes ($\bar{S}_i(k)$). Then, the state update process can be characterized by,

$$\sum_{j\in R_i(k)} \frac{x_j(k)}{|R_i(k)|} = \frac{1}{|R_i(k)|}\Big(\sum_{j\in S_i(k)} x_j(k) + x_i(k) + \sum_{j\in \bar{S}_i(k)} x_j(k)\Big) \tag{16}$$

Then, we divide the proof into two cases, i.e., $\bar{S}_i(k) = \emptyset$ and $\bar{S}_i(k) \neq \emptyset$. **Case 1**: If $\bar{S}_i(k) = \emptyset$, then there holds $M_{ij}(k) = \frac{1}{|R_i(k)|}$ for $(j,i) \in E_1$ or $j = i$, i.e., Lemma 1 holds. **Case 2**: If $\bar{S}_i(k) \neq \emptyset$, there exists at least one normal or adversarial node in $R_i(k)$. Here, we consider the case when there is only one normal or adversarial node $s \in V_a$ in $R_i(k)$, which means that $x_s(k)$ satisfies $x_i^m(k) \leq x_s(k) \leq x_i^M(k)$ according to Step 1 and 2 in RDO-T. Hence, there must exist $0 \leq \rho \leq 1$ such that $x_s(k) = \rho x_i^m(k) + (1-\rho)x_i^M(k)$. Based on (3), we have

$$\begin{aligned}\frac{\sum_{j\in R_i(k)} x_j(k)}{|R_i(k)|} &= \frac{1}{|R_i(k)|}\Big(\sum_{j\in S_i(k)} x_j(k) + x_i(k) + x_s(k)\Big)\\ &= \frac{\big(\sum_{j\in S_i(k)} x_j(k) + x_i(k) + \rho x_i^m(k) + (1-\rho)x_i^M(k)\big)}{|R_i(k)|},\end{aligned} \tag{17}$$

Then, we consider the case when there is only one node j_1 (j_2) in $S_i(k)\cup\{i\}$ such that $x_{j_1}(k) = x_i^m(k)$ ($x_{j_2}(k) = x_i^M(k)$) and give $R_i^1(k) = R_i(k)\backslash\{S_i(k)\cup j_1 \cup j_2\}$. As $x_i^m(k) \in x_j(k)$, $j \in R_i(k)$ and $x_i^M(k) \in x_j(k)$, $j \in R_i(k)$, one obtains from (17) that

$$\begin{aligned}&\frac{1}{|R_i(k)|}\Big(\sum_{j\in S_i(k)} x_j(k) + x_i(k) + \rho x_i^m(k) + (1-\rho)x_i^M(k)\Big)\\ &= \frac{1}{|R_i(k)|}\Big(\sum_{j\in R_i^1(k)} x_j(k) + (1+\rho)x_{j_1}(k) + (2-\rho)x_{j_2}(k)\Big).\end{aligned} \tag{18}$$

From the above equation, we infer that $M_{ij}(k) = \frac{(1+\rho)}{|R_i(k)|}$, $j = j_1$, $M_{ij}(k) = \frac{(2-\rho)}{|R_i(k)|}$, $j = j_2$ and $M_{ij}(k) = \frac{1}{|R_i(k)|}$, $j \in R_i^1(k)$, which means that ii) and iii) hold. Since $|R_i^1(k)| + (1+\rho) + (2-\rho) = |R_i(k)|$, $M(k)$ is a row stochastic matrix, i) holds. Similarly, we obtain the same conclusion for more than one normal or adversarial node and more than one node with maximum and minimum states in $R_i(k)$. Thus, i) holds. Combining (18) with $R_i(k)$ and E_1, we have ii) and iii). ■

B. Proof of Theorem 1

We obtain the following lemmas by referring to [11].

Lemma 7: Let $\{a_k\}_{k=0}^{\infty}$, $\{b_k\}_{k=0}^{\infty}$, and $\{c_k\}_{k=0}^{\infty}$ be non-negative sequences. Suppose that $a_{k+1} \leq a_k - b_k + c_k, \forall k \geq 0$, and $\sum_{k=0}^{\infty} c_k < \infty$. Then, $\sum_{k=0}^{\infty} b_k < \infty$ and the sequence $\{a_k\}_{k=0}^{\infty}$ converges to a non-negative value.

Lemma 8: If Assumption 1 holds, under RDO-T, $\forall x \in \mathbb{R}$ and $\forall k \geq 0$, then the following relation holds,

$$\begin{aligned}|y(k+1) - x|^2 \leq |y(k) - x|^2 &+ 4L\alpha_k \sum_{j\in V_n\cup V_t} \psi_j(k+1)|y(k) - x_j(k)|\\ &- 2\alpha_k \sum_{j\in V_n\cup V_t} \psi_j(k+1)(f_j(y(k)) - f_j(x)) + \alpha_k^2 n_0 L^2\end{aligned} \tag{19}$$

Let $H = \max_{i\in V_n\cup V_t} x_i(0)$ and $h = \min_{i\in V_n\cup V_t}$. Then a bound is obtained by the following lemma.

Lemma 9: If Assumption 1 holds, under RDO-T, $\forall i \in V_n \cup V_t$, we have

$$\begin{aligned}&|y(k) - x_i(k)|\\ &\leq n_0 \max\{|h|, |H|\}(1-\varphi^{n_0})^{\lceil \frac{k}{n_0} \rceil} + n_0 L \sum_{t=1}^{k-1} \alpha_{t-1}(1-\varphi^{n_0})^{\lceil \frac{k-t}{n_0} \rceil} + 2\alpha_{k-1}L\end{aligned} \tag{20}$$

$$\lim_{k\to\infty} |y(k) - x_i(k)| = 0. \tag{21}$$

Proof: We first prove the convergence of $y(k)$ and $\lim_{k\to\infty} y(k) \in Y(\mu,\nu)$. Let $\tilde{x} \in Y(\mu,\nu)$, where $\mu \leq \varphi^d, \nu = n_2$. According to Lemma 8, one obtains that,

$$\begin{aligned}|y(k+1) - \tilde{x}|^2 \leq |y(k) - \tilde{x}|^2 &+ 4L\alpha_k \sum_{j\in V_n\cup V_t} \psi_j(k+1)|y(k) - x_j(k)|\\ &- 2\alpha_k \sum_{j\in V_n\cup V_t} \psi_j(k+1)(f_j(y(k)) - f_j(\tilde{x})) + \alpha_k^2 n_0 L^2.\end{aligned}$$

Given the following definition,

$$\begin{aligned}a_k &= |y(k) - \tilde{x}|^2\\ b_k &= 2\alpha_k\Big[\sum_{j\in V_n\cup V_t} \psi_j(k+1)f_j(y(k)) - \sum_{j\in V_n\cup V_t} \psi_j(k+1)f_j(\tilde{x})\Big]\\ c_k &= 4L\alpha_k \sum_{j\in V_n\cup V_t} \psi_j(k+1)|y(k) - x_j(k)| + \alpha_k^2 n_0 L^2,\end{aligned} \tag{22}$$

we have $a_k \geq 0$, $c_k \geq 0$ directly. Moreover, by referring to Lemma 2, one infers that $\tilde{x}$ is the optimal solution of the optimization problem $\min_x \sum_{j\in V_n\cup V_t} \psi_j(k+1)f_j(x)$. As a result,

$$\sum_{j\in V_n\cup V_t} \psi_j(k+1)f_j(y(k)) - \sum_{j\in V_n\cup V_t} \psi_j(k+1)f_j(\tilde{x})) \geq 0. \tag{23}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2954363, IEEE Transactions on Automatic Control

As $\alpha_k \geq 0$, $\forall k$, we conclude that $b_k \geq 0$. Hence, $\{a_k\}_{k=0}^{\infty}$, $\{b_k\}_{k=0}^{\infty}$, $\{c_k\}_{k=0}^{\infty}$ are nonnegative sequences. According to Lemma 9, one obtains that

$$\begin{aligned} c_k &= 4L\alpha_k \sum_{j\in V_n\cup V_t} \psi_j(k+1)|y(k)-x_j(k)| + \alpha_k^2 n_0 L^2 \\ &\leq 4L\alpha_k \sum_{j\in V_n\cup V_t} \psi_j(k+1)(n_0\max\{|h|,|H|\}(1-\varphi^{n_0})^{\lceil\frac{k}{n_0}\rceil} \\ &\quad + n_0 L\sum_{t=1}^{k-1}\alpha_{t-1}(1-\varphi^{n_0})^{\lceil\frac{k-t}{n_0}\rceil} + 2\alpha_{k-1}L) + \alpha_k^2 n_0 L^2. \end{aligned} \tag{24}$$

By utilizing the fact that $\frac{1}{2}(\alpha_k^2+\alpha_{k-1}^2) \geq \alpha_{k-1}\alpha_k$, we conclude that $\sum_{k=0}^{\infty} c_k < \infty$. The detailed proof is omitted here, which is similar to that in [11]. Applying Lemma 7, one has for any $\tilde{x} \in Y(\mu,\nu)$, $\{a_k\}_{k=0}^{\infty}$ converges, and

$$\begin{aligned} \sum_{k=0}^{\infty} b_k = \sum_{k=0}^{\infty} 2\alpha_k[&\sum_{j\in V_n\cup V_t} \psi_j(k+1) f_j(y(k)) \\ &- \sum_{j\in V_n\cup V_t} \psi_j(k+1) f_j(\tilde{x}))] < \infty. \end{aligned} \tag{25}$$

Suppose that $\lim_{k\to\infty} y(k) \notin Y(\mu,\nu)$, and we have

$$\lim_{k\to\infty} \sum_{j\in V_n\cup V_t} \psi_j(k+1) f_j(y(k)) - \sum_{j\in V_n\cup V_t} \psi_j(k+1) f_j(\tilde{x})) \neq 0, \tag{26}$$

contradicts with (25), where the fact $\sum_{k=0}^{\infty} \alpha_k = \infty$ is utilized. Hence, one obtains that $\lim_{k\to\infty} y(k) \in Y(\mu,\nu)$. Combining with Lemma 9, we complete the proof. ■

C. Proof of Lemma 4

Proof: From (11), one obtains,

$$\begin{aligned} &\sum_{i=1}^{n} f_i'(x^*) - \sum_{i=1}^{n_0} f_i'(\hat{x}^*) = 0, \\ &\sum_{i=1}^{n} f_i'(x^*) - \sum_{i=1}^{n_0} f_i'(\hat{x}^*) = \sum_{i=1}^{n_0}(f_i'(x^*) - f_i'(\hat{x}^*)) + \sum_{i=n_0+1}^{n} f_i'(x^*). \end{aligned} \tag{27}$$

When $\hat{x}^* \leq x^*$, due to the convexity of $f_i(x)$, there holds $f_i'(x^*) - f_i'(\hat{x}^*) \geq 0$. If $\sum_{i=n_0+1}^{n} f_i'(x^*) \geq 0$, we have $f_i'(x^*) - f_i'(\hat{x}^*) \geq 0$, $\forall i \in V_t \cup V_n$, and thus $\hat{x}^* \leq x^*$. Due to the same reason, if $\sum_{i=n_0+1}^{n} f_i'(x^*) < 0$, one infers $f_i'(x^*) - f_i'(\hat{x}^*) \leq 0$, $\forall i \in V_t \cup V_n$, and thus $\hat{x}^* > x^*$. From (11), one obtains,

$$\begin{aligned} &\frac{1}{n_0}\sum_{i=1}^{n_0} f_i'(\hat{x}^*) - \sum_{i\in V_t} \beta_i f_i'(\tilde{x}^*) \\ &= \sum_{i\in V_t}(\frac{1}{n_0} - \beta_i)(f_i'(\hat{x}^*) - f_i'(\tilde{x}^*)) + \sum_{i\in V_n} \frac{f_i'(\hat{x}^*)}{n_0} = 0. \end{aligned} \tag{28}$$

We first consider the case $\beta_i \geq \frac{1}{n_0}$, $\forall i \in V_t$. If $f_i'(\hat{x}^*) - f_i'(\tilde{x}^*) \geq 0$, $\sum_{i\in V_n} f_i'(\hat{x}^*) \geq 0$; If $f_i'(\hat{x}^*) - f_i'(\tilde{x}^*) \leq 0$, $\sum_{i\in V_n} f_i'(\hat{x}^*) \leq 0$. If the sign of $\sum_{i\in V_t}(\frac{1}{n_0} - \beta_i)(f_i'(\hat{x}^*) - f_i'(\tilde{x}^*))$ is the same as $f_i'(\hat{x}^*) - f_i'(\tilde{x}^*)$, we can conclude: Iff (if and only if) $f_i'(\hat{x}^*) - f_i'(\tilde{x}^*) \geq 0$, $\sum_{i\in V_n} f_i'(\hat{x}^*) \leq 0$; Iff $f_i'(\hat{x}^*) - f_i'(\tilde{x}^*) < 0$, $\sum_{i\in V_n} f_i'(\hat{x}^*) > 0$. If the sign of $\sum_{i\in V_t}(\frac{1}{n_0} - \beta_i)(f_i'(\hat{x}^*) - f_i'(\tilde{x}^*))$ is the opposite of $f_i'(\hat{x}^*) - f_i'(\tilde{x}^*)$, one obtains: Iff $f_i'(\hat{x}^*) - f_i'(\tilde{x}^*) \geq 0$, $\sum_{i\in V_n} f_i'(\hat{x}^*) \geq 0$; Iff $f_i'(\hat{x}^*) - f_i'(\tilde{x}^*) < 0$, $\sum_{i\in V_n} f_i'(\hat{x}^*) < 0$. ■

D. Proof of Lemma 5

Proof: Since $f_i(x)$ is twice differentiable and $0 < C_1 \leq f_i''(x) \leq C_2$, we have

$$|f_i'(x^*) - f_i'(\hat{x}^*)| \leq C_2|x^* - \hat{x}^*|. \tag{29}$$

According to (27), it can be inferred

$$\sum_{i=1}^{n_0}(|f_i'(x^*) - f_i'(\hat{x}^*)|) = |-\sum_{i=n_0+1}^{n} f_i'(x^*)|. \tag{30}$$

Combining (29) and (30), one has $|\sum_{i=n_0+1}^{n} f_i'(x^*)| \leq n_0 C_2|x^* - \hat{x}^*|$. Hence, there holds $|x^* - \hat{x}^*| \geq \frac{|\sum_{i=n_0+1}^{n} f_i'(x^*)|}{n_0 C_2}$. For the same reason, we have $|x^* - \hat{x}^*| \leq \frac{|\sum_{i=n_0+1}^{n} f_i'(x^*)|}{n_0 C_1}$. Considering the deviation of $\hat{x}^*$ from $\tilde{x}^*$, from (28), one obtains

$$|\sum_{i\in V_t}(\frac{1}{n_0} - \beta_i)(f_i'(\hat{x}^*) - f_i'(\tilde{x}^*))| = |-\frac{1}{n_0}\sum_{i\in V_n} f_i'(\hat{x}^*)|. \tag{31}$$

Due to the convexity of $f_i(x)$, $\forall i \in V$, $f_i(x)$ is twice differentiable and $0 < C_1 \leq f_i''(x) \leq C_2$, there holds

$$|\sum_{i\in V_t}(\frac{1}{n_0} - \beta_i)(f_i'(\hat{x}^*) - f_i'(\tilde{x}^*))| \leq |\sum_{i\in V_t}(\frac{1}{n_0} - \beta_i)C_2(\hat{x}^* - \tilde{x}^*)|.$$

Therefore, $|-\frac{1}{n_0}\sum_{i\in V_n} f_i'(\hat{x}^*)| \leq |\sum_{i\in V_t}(\frac{1}{n_0} - \beta_i)C_2(\hat{x}^* - \tilde{x}^*)|$. Thus, we conclude the lower bound of $|\hat{x}^* - \tilde{x}^*|$ as that in (13). Due to the same reason, one obtains the upper bound in (13). ■

E. Proof of Lemma 6

Proof: Due to the convexity of function $f_i(x)$, one infers $f_i(\hat{x}^*) \geq f_i(x^*) + f_i'(x^*)(\hat{x}^* - x^*)$. As a result, there holds

$$\begin{aligned} &|\frac{1}{n}\sum_{i=1}^{n} f_i(x^*) - \frac{1}{n_0}\sum_{i=1}^{n_0} f_i(\hat{x}^*)| \\ &\leq |\frac{1}{n}\sum_{i=1}^{n} f_i(x^*) - \frac{1}{n_0}\sum_{i=1}^{n_0}(f_i(x^*) + f_i'(x^*)(\hat{x}^* - x^*))| \\ &\leq |\sum_{i=n_+n_2+1}^{n} \frac{f_i(x^*)}{n}| + |\sum_{i=1}^{n_0}(\frac{1}{n} - \frac{1}{n_0})f_i(x^*) - \sum_{i=1}^{n_0}\frac{f_i'(x^*)(\hat{x}^* - x^*)}{n_0}|. \end{aligned} \tag{32}$$

Meanwhile, one has

$$\begin{aligned} &|\frac{n_0 - n}{nn_0}\sum_{i=1}^{n_0} f_i(x^*) - \frac{(\hat{x}^* - x^*)}{n_0}\sum_{i=n_0+1}^{n} f_i'(x^*)| \\ &\leq |\frac{n_0 - n}{nn_0}\sum_{i=1}^{n_0} f_i(x^*)| + |\frac{(\hat{x}^* - x^*)}{n_0}(n - n_0)L| \\ &\leq \frac{n - n_0}{n_0}|\frac{1}{n}\sum_{i=1}^{n_0} f_i(x^*)| + |(\hat{x}^* - x^*)L|, \end{aligned} \tag{33}$$

where we use $|f_i'(x)| \leq L$ and $\sum_{i=n_0+1}^{n} f_i'(x^*) + \sum_{i=1}^{n_0} f_i'(x^*) = 0$. As a result, (14) holds. For the same reason, it can be obtained

$$\begin{aligned} &|\sum_{i=1}^{n_0}\frac{f_i(\hat{x}^*)}{n_0} - \sum_{i\in V_t}\beta_i f_i(\tilde{x}^*)| \\ &\leq |\sum_{i=1}^{n_0}\frac{f_i(\hat{x}^*)}{n_0} - \sum_{i\in V_t}\beta_i(f_i(\hat{x}^*) + f_i'(\hat{x}^*)(\tilde{x}^* - \hat{x}^*))| \\ &\leq |\sum_{i=1}^{n_1}\frac{f_i(\hat{x}^*)}{n_0}| + |\sum_{i\in V_t}(\frac{1}{n_0} - \beta_i)f_i(\hat{x}^*)| + |\sum_{i\in V_t}\beta_i f_i'(\hat{x}^*)(\tilde{x}^* - \hat{x}^*)| \\ &\leq |\sum_{i=1}^{n_1}\frac{f_i(\hat{x}^*)}{n_0}| + |\sum_{i\in V_t}(\frac{1}{n_0} - \beta_i)f_i(\hat{x}^*)| + n_2 L|\tilde{x}^* - \hat{x}^*|. \end{aligned} \tag{34}$$

Hence, we have completed the proof. ■