Resilient distributed optimization under mobile malicious attacks

Yuan Wang * **Changxin Liu** ** **Hideaki Ishii** *** **and Karl Henrik Johansson** **

* *Department of Robotics, Hunan University, Changsha, China. yuanw@hnu.edu.cn*
** *Division of Decision and Control Systems, School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, and Digital Futures, Stockholm, Sweden. changxin@kth.se, kallej@kth.se*
*** *Department of Computer Science, Tokyo Institute of Technology, Yokohama, Japan. ishii@c.titech.ac.jp*

Abstract: This article addresses the distributed optimization problem in the presence of malicious adversaries that can move within the network and induce faulty behaviors in the attacked nodes. We first investigate the vulnerabilities of a consensus-based secure distributed optimization protocol under mobile adversaries. Then, a modified resilient distributed optimization algorithm is proposed. We develop conditions on the network structure for both complete and non-complete directed graph cases, under which the proposed algorithm guarantees that the estimates by regular nodes converge to the convex combination of the minimizers of their local functions. Simulations are carried out to verify the effectiveness of our approach.

Keywords: Fault-tolerant distributed optimization, multi-agent systems, network security, mobile adversary agents.

1. INTRODUCTION

Along with the development of information and communications technology, distributed computation over wireless networks has received increasing attention. It features using a group of computing units/agents whose local computations are coordinated by real-time peer-to-peer communication, thereby solving large-scale problems efficiently while being robust to node failures. This work considers the finite-sum distributed optimization problem, which finds broad applications in distributed control, sensor fusion, and federated learning (Yang et al., 2019).

Large-scale systems operating over wireless works including distributed optimization are vulnerable to cyber-attacks such as false data injections (FDI), denial-of-service (DoS) and eavesdropping attacks (Ishii et al., 2022). Those attacks deteriorate the performance and even threaten the operation of distributed systems. To this end, tailored distributed optimization algorithms resilient to specific types of attacks have been proposed lately. In this work, our focus is placed on the FDI attack which falsifies the transmitted signals among agents without being detected (Dibaji et al., 2017; Sundaram and Gharesifard, 2019). We should point out that related works in the literature mostly assumed a time-invariant set of malicious agents. By contrast, we consider more powerful attacks in distributed optimization systems, where a fixed number of adversaries are able to move within the system and manipulate the behaviors of agents.

Since the distributed consensus-seeking protocol is the fundamental tool to design distributed optimization algorithms, next we provide a brief review of both resilient consensus and distributed optimization algorithms.

Resilient Consensus: Resilient distributed consensus or agreement-seeking algorithms have been studied for a long time; see (Dolev et al., 1986; Kieckhafer and Azadmanesh, 1992) for a few early works. However, the algorithms have not been adapted to sparse networks and analyzed based on the graph robustness until the last decade (Dibaji et al., 2017; LeBlanc et al., 2013; Zhang et al., 2015). The core mechanism therein to defend FDI attacks is known as the mean subsequence reduced (MSR) algorithm, where every regular agent removes a number of extreme values from the set of messages received from its neighbors at each round. Under proper conditions on the graph, the regular agents with the MSR algorithm reach asymptotic consensus (LeBlanc et al., 2013). Note that the aforementioned works considered the compromised agents to be the same throughout the consensus-seeking process. Wang et al. (2022) considered a mobile attack model in which a fixed number of adversaries may switch their targets, and developed modified MSR algorithms to handle the effects due to switching.

⋆ This work was supported in part by the Knut and Alice Wallenberg Foundation, Wallenberg Scholar under Grant 66469; by a Distinguished Professor Grant from the Swedish Research Council (Org: JRL, project no: 3058); by the Swedish Foundation for Strategic Research; and by JSPS under Grant-in-Aid for Scientific Research Grant No. 22H01508.

Resilient Distributed Optimization: Sundaram and Gharesifard (2019) considered the distributed scalar optimization problem in the presence of malicious agents. A resilient algorithm is developed based on the MSR-based consensus and the subgradient methods. Under proper assumptions on the attack model and communication graph, the authors proved that the estimates by regular agents converge to the convex hull of their local minimizers. The algorithm was extended to the multi-dimensional case in (Kuwarananchareon et al., 2020). Recently, Wu et al. (2022) proposed a general robust aggregation rule and incorporated it into distributed stochastic optimization to defend FDI attacks. In another line of research, Gupta and Vaidya (2020) coined the notion of redundancy in objective functions (later extended by Zhu et al. (2022)) and used it to develop the condition that ensures full resilience in distributed optimization, that is, convergence to the consensual optimum of regular agents.

The contribution of this work is threefold: First, we show that the secure version of the consensus-based distributed optimization protocol under static adversary model (Sundaram and Gharesifard, 2019) is fragile under the mobile malicious adversary model. Second, we propose a novel secure distributed optimization protocol for the regular nodes under a mobile malicious model. The protocol is modified from the resilient approach based on the Local Filtering (LF) algorithm (Sundaram and Gharesifard, 2019). Third, we consider networks in both complete and non-complete graphs, and characterize the necessary connectivity structures for the proposed modified LF protocol such that the regular nodes' states converge to the convex hull of the minimizers of their local functions, regardless of the behaviors of a certain number of the adversarial nodes.

This paper is organized as follows. We formulate the problem and present some preliminaries in Section 2. Aiming at the mobile malicious model, our algorithm and its theoretical properties are developed in Section 3. Section 4 provides a few numerical examples and Section 5 concludes the paper.

2. PROBLEM FORMULATION

2.1 General notations

Let $\mathbb{R}, \mathbb{N}$ be the real, and natural numbers, $\mathbf{1}= [1, 1, \ldots, 1]'$, $\mathbf{0}= [0, 0, \ldots, 0]'$. The Euclidean norm on $\mathbb{R}^n$ is written by $||\cdot||$. A nonnegative matrix $A \in \mathbb{R}^{n\times n}$ is called row-stochastic if its rows are probability vectors. A probability vector is a numerical vector whose entries are real numbers between 0 and 1 and add up to 1.

Consider a directed network $\mathcal{G}(\mathcal{V}, \mathcal{E})$ consisting of n nodes, where the set of nodes is $\mathcal{V} = \{1, \ldots, n\}$, and the set of edges is $\mathcal{E} = \mathcal{V}\times\mathcal{V}$. An edge $(j, i) \in \mathcal{E}$ means that the node j can send a value to node i, and this edge is called the in-coming edge of node i, and the out-going edge of node j. Let $\mathcal{N}_i^- = \{j \in \mathcal{V} : (j, i) \in \mathcal{E}\}$ be the set of in-coming neighbors of node i, and $\mathcal{N}_i^+ = \{j \in \mathcal{V} : (i, j) \in \mathcal{E}\}$ be the set of out-going neighbors of node i. In this paper, the degree d_i of node i is the cardinality of $\mathcal{N}_i^-$.

2.2 Distributed optimization and consensus

A typical objective for distributed optimization is to solve the following minimization problem by local computation and peer-to-peer communication:

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

For each node i, there is a local cost function $f_i : \mathbb{R} \to \mathbb{R}$ that is assumed to be convex with bounded subgradients, and hence globally Lipschitz. As a popular approach to solve the distributed optimization problem, the agents combine the consensus dynamics and the gradient flow to find the minimizer (Nedić and Ozdaglar, 2009; Nedić et al., 2010). Specifically, at each time $k \in \mathbb{N}$, the agents have a temporary local solution $x_i(k)$ for problem (1). Each agent sends $x_i(k)$ to its neighbors and updates its state by

$$x_i(k+1) = a_{ii}(k)x_i(k) + \sum_{j\in\mathcal{N}_i^-} a_{ij}(k)x_j(k) - \alpha_k d_i(k), \tag{2}$$

where $a_{ij}(k)$ is the weight that satisfies $a_{ii}(k) + \sum_{j\in\mathcal{N}_i^-} a_{ij}(k) = 1$, and there exists a constant γ such that $a_{ij} \in [\gamma, 1]$ for all node i. The quantity $d_i(k)$ is the subgradient of f_i evaluated at $a_{ii}(k)x_i(k) + \sum_{i\in\mathcal{N}_i^-} a_{ij}(k)x_j(k)$. The step-size sequence is written as $\{\alpha_k\}_{k\in\mathbb{N}}$ in (2).

Problem (1) can be solved by (2) if the network topology is strongly connected, and the weights are doubly stochastic (Nedić et al., 2010).

Definition 1. (Double Stochasticity) The weights are called doubly stochastic, if for all $i \in \mathcal{V}$ and $k \in \mathbb{N}$, it holds $a_{ii}(k)+\sum_{j\in\mathcal{N}_i^-} a_{ij}(k) = 1$, and $a_{ii}(k)+\sum_{j\in\mathcal{N}_i^+} a_{ji}(k) = 1$.

Proposition 1. Suppose the network is strongly connected, the weights are doubly stochastic, and all local functions f_i have bounded subgradients. Consider the update rule (2) and let $\sum_{k=1}^{n} \alpha_k = \infty$, $\sum_{k=1}^{n} \alpha_k^2 < \infty$. Then, the minimizer x^* of problem (1) is asymptotically achieved, i.e., $\lim_{k\to\infty} |x_i(k) - x^*| = 0$ for all $i \in \mathcal{V}$.

The above result shows that a perfect global optimizer can be distributively attained if there is no attack. However, in the presence of attacks, such perfect global optimizer x^* is vulnerable to malicious node that may deviate the nodes from the prescribed update rule. Since achieving a perfect global optimizer under malicious attacks is hard (Su and Vaidya, 2021), one of the main objectives of distributed optimization under malicious attacks is to develop secure distributed algorithms such that the influence of the malicious nodes is mitigated. Here, we address a variant of the secure distributed optimization problem from (Sundaram and Gharesifard, 2019), where the states of regular nodes reach consensus in the convex hull of regular local minimizers rather than the ideal global optimizer x^*.

2.3 Mobile malicious model

In this article, we examine multi-agent systems operating in unpredictable or even hostile environments. Some of the agents are unreliable and/or adversarial. Such agents improperly implement the provided algorithm and may even update their states arbitrarily in an effort to obstruct the ongoing consensus process. For these faulty agents,

we present a new mobile malicious model. Informally, this class has the following three features: a) Adversarial agents have the ability to broadcast their false states to their neighbors, meaning that every adversarial agent's neighbors receive the same information from it. b) Over time, the malicious agents' identities may change. That is, at specific time instants, an attacker may transform a regular agent into a malicious one. c) A malicious agent may recover and become regular. When an attacker switches to a different non-adversarial agent, the original attacked agent is considered to be in the cured status.

To proceed, we introduce the following notations. At each time k, the set $\mathcal{V}$ of nodes is partitioned into two subsets: The set $\mathcal{R}(k)$ of regular agents and the set $\mathcal{A}(k)$ of adversarial agents. Moreover, we have $|\mathcal{R}(k)|+|\mathcal{A}(k)| = n$. In the static malicious model, both sets $\mathcal{R}(k)$ and $\mathcal{A}(k)$ remain invariant over time.

The upper bound as well as the faulty behaviors of the adversarial agents are defined below.

Definition 2. (F-total) The mobile adversarial set $\mathcal{A}(k)$ follows the F-total model if $|\mathcal{A}(k)| \leq F$ for all k, where $F \in \mathbb{N}$.

Definition 3. (Malicious nodes) An adversarial node $i \in \mathcal{A}(k)$ is said to be malicious if it makes updates in its value $x_i(k)$ arbitrarily and sends the same value to all of its neighbors.

Under the mobile adversary model, the adversaries may switch their targets, but we limit their influence by bounding the total number of them in the network over time. In addition, even though the adversarial nodes can arbitrarily send their states, we assume that they cannot change the local function f_i. Otherwise, it is clear that the distributed optimization problem cannot be solved after n steps, since the local functions of all agents may be corrupted.

We present the model of mobile malicious activities. This model is based on the literature in computer science for the Byzantine attack (Buhrman et al., 1995). We present the version modified for the scenario of malicious adversaries case. Here, each agent executes three steps during each round: Send out its own state, collect the states of its neighbors, and then update its state. The three steps are carried out by all agents simultaneously.

(Buhrman's model (Buhrman et al., 1995)): Only at the sending step in each round k the adversary is allowed to move away from an attacked agent i. In such a round, agent i broadcasts its corrupted state to its neighbors as $x_i(k)$, but it instantly recovers; as a result, agent i collects and updates its state like any other regular nodes. Due to this, agent i will be categorized as regular in this round k, meaning that $i \in \mathcal{R}(k)$. We have $j \in \mathcal{A}(k)$ if the adversary switched from agent i to agent j after i sends out its state. Note that there are at most F incorrect values in the network at any given round. An illustration of such mobile behavior can be found in Fig 1.

2.4 Attacking the Local Filtering (LF) dynamics

The objective of this paper is to develop distributed algorithms for the regular agents in the system to solve the optimization problem with secure guarantees under the

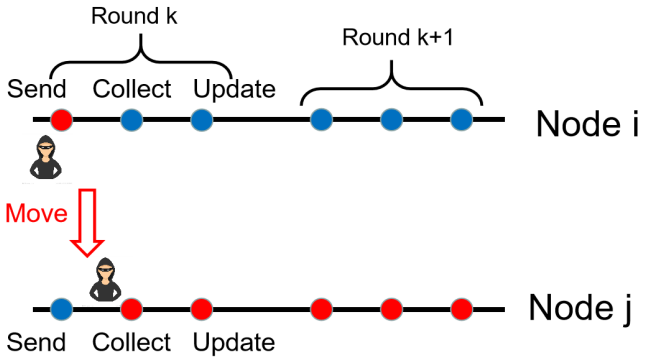

Fig. 1. Mobile malicious model model where $i \in R(k)$ and $j \in A(k)$.

mobile malicious model. This problem is an extension of that studied in (Sundaram and Gharesifard, 2019), which is limited to the static adversary model.

Definition 4. (Resilient optimization) If for any possible sets and behaviors of the mobile malicious nodes in $\mathcal{A}(k)$ and any initial state values of the regular nodes, the following conditions are satisfied, then the resilient optimization is solved in multi-agent system:

1) (Consensus condition) The regular nodes $\forall i, j \in \mathcal{R}(k)$ eventually take the same value as $\lim_{k\to\infty} |x_i(k) - x_j(k)| = 0$.
2) (Safety condition) Set the interval $\mathcal{S} \subset \mathbb{R}$ containing the local minimizers of all regular nodes. Then, it holds $\lim_{k\to\infty} x_i(k) \in \mathcal{S}$ for all $\forall i \in \mathcal{R}(k)$.

In particular, solving the resilient distributed optimization problem means that, if the sequence of step-sizes decreases to zero and is not summable (a typical condition in gradient-based optimization dynamics (Nedić et al., 2010)), the states of the regular nodes stay within the safety region that is bounded by regular local minimizers, regardless of the influences by the adversarial nodes.

One approach to solve the resilient distributed optimization problem under *static adversarial model* is the Local Filtering (LF) dynamics in (Sundaram and Gharesifard, 2019). The LF dynamics provide a safety guarantee such that the states of the regular nodes converge to the convex hull of the minimizers of the local cost functions. As a very brief introduction for the LF dynamics, each regular node executes three basic steps: Send, collect, and update. At time (or round) k, first, a regular agent i broadcasts its current value $x_i(k)$ to its neighboring agents. Second, it collects the values of the in-coming neighbor nodes $x_j(k)$ for $j \in \mathcal{N}_i^-$. Third, after discarding the most extreme neighbor values, its value is updated to $x_i(k+1)$. For the third step of state update, the update rule is given by

$$x_i(k+1) = a_{ii}(k)x_i(k) + \sum_{j\in\mathcal{M}_i^-(k)} a_{ij}(k)x_j(k) - \alpha_k d_i(k), \tag{3}$$

where $\mathcal{M}_i^-(k) \subset \mathcal{N}_i^-$ is the set of in-neighbors of node i whose states were retained. The value removal for node i is to remove the F largest and F smallest values that are larger and smaller than its own value, respectively. If there are fewer than F values higher (resp. lower) than its own value, node i removes all of those values.

However, we can demonstrate that if the conventional LF dynamics for the static F-total model are applied directly, mobile adversary agents can quickly demolish resilient optimization (for numerical simulations showing such properties, see Section 4).

Proposition 2. Suppose the local objective functions at each node are convex with bounded subgradients, but otherwise completely arbitrary, and the step-size $\alpha_k \to 0$ as $k \to \infty$. Suppose Γ is the LF algorithm that solves the resilient optimization problem under F-total static adversarial model. Then, a single mobile adversary can cause all the nodes' solutions to be outside of the safety interval $\mathcal{S}$ when they run algorithm Γ.

3. MODIFIED RESILIENT OPTIMIZATION ALGORITHM

Here, we present the modified LF dynamics with mobile malicious agents. It will be shown that this algorithm is effective to deal with Buhrman's malicious model.

Algorithm 1. (Modified LF dynamics). At each round k, regular node $i \in \mathcal{R}(k)$ executes the following three steps:

1. (Send) Node i sends its current value $x_i(k)$ to all neighbors.
2. (Collect) Node i collects the neighbor values $x_j(k), j \in \mathcal{N}_i^-$.
3. (Update) Node i updates the value $x_i(k+1)$ by:
   (a) Sorting all received values (include its own value) in a descending order.
   (b) Removing the F largest values and the F smallest values. The remained set of agent values are written by $\mathcal{M}_i^+(k) \subset \{i\} \cup \mathcal{N}_i^-$.
   (c) Updating its value by
   $$x_i(k+1) = \sum_{j \in \mathcal{M}_i^+(k)} \hat{a}_{ij}(k) x_j(k) - \alpha_k d_i(k), \quad (4)$$
   where $\{\alpha_k\}_{k \in \mathbb{N}}$ is a sequence of non-negative step-size, and $d_i(k)$ is a subgradient of f_i evaluated at $\sum_{j \in \mathcal{M}_i^+(k)} \hat{a}_{ij}(k) x_j(k)$. The weight $a_{ij}(k)$ satisfies $\sum_{j \in \mathcal{M}_i^+(k)} \hat{a}_{ij}(k) = 1$, and furthermore, there exists a constant γ such that $\hat{a}_{ij}(k) \in [\gamma, 1]$ for all node i and $k \in \mathbb{Z}_+$.

The possibility that agent i may not use its own value makes this method special. This is due to the fact that in Step 3, $2F$ values are eliminated regardless of the agent i's value. In contrast, the amount of values to be deleted in the typical techniques for the static adversary models in (LeBlanc et al., 2013; Sundaram and Gharesifard, 2019) depends on the current value of agent i. In particular, only those larger (respectively, smaller) than $x_i(k)$ are eliminated if agent i's value is among the largest (respectively, the smallest) F.

3.1 Convergence result for complete graph

Here, we first present the convergence properties of the modified LF dynamics (4) for networks in the complete graph form. More general graphs will be treated in the next subsection. In particular, we provide the necessary and sufficient conditions for complete graphs under F-total mobile malicious adversaries.

Theorem 1. Consider the multi-agent system whose network $\mathcal{G}$ forms a complete graph. Suppose that the mobile malicious agents follow the F-total and Buhrman's model, and the local objective functions f_i at each node are convex with subgradients bounded by some constant L, the step-size $\alpha_k \to 0$ as $k \to \infty$. Then, the regular nodes using Algorithm 1 reach consensus if and only if $n \geq 2F + 1$.

From the technical viewpoint, the proof of Theorem 1 can be seen as a natural extension of that in (Wang et al., 2022), which deals with the resilient consensus problem under the mobile adversary model. In both problems, the condition $N \geq 2F + 1$ is a tight one and hence consistent. Adding the subgradient term with a vanishing step-size $\alpha_k \to 0$ keeps the convergence properties for regular nodes. We further remark that the advantage of this analysis approach is that it can be extended to non-complete graph cases as we discuss in the next subsection.

3.2 Convergence result for non-complete graph

Next, we demonstrate the effectiveness of the modified LF algorithm for the non-complete graph case and provide a sufficient condition on the graph structure for resilient optimization under the mobile malicious model.

Theorem 2. Consider the multi-agent system under the network $\mathcal{G}$ where the mobile malicious agents follow the F-total and Buhrman's model. Suppose that the local objective functions f_i at each node are convex with subgradients bounded by some constant L, the step-size $\alpha_k \to 0$ as $k \to \infty$. Then, the regular agents using Algorithm 1 reach consensus if the following conditions are satisfied:

C1 $n \geq 4F + 4$.
C2 For every node i, the number of neighbors satisfies $|\mathcal{N}_i^-| \geq 2F + 1 + \frac{n}{2}$.

For comparison, Theorem 6.4 in (Sundaram and Gharesifard, 2019) shows convergence findings for the LF algorithm under the F-total static malicious model. It states that the regular nodes are guaranteed to reach consensus if and only if the network is a $(F+1, F+1)$-robust graph (see definition of robust graph in (Sundaram and Gharesifard, 2019)). However, according to our result under the F-total mobile malicious model, if conditions C1 and C2 are met, the network will always be $(2F + 1)$-robust (and not vice versa). It is known that $(2F + 1)$-robust graphs have more connections than $(F + 1, F + 1)$-robust graphs. In order to counter the more harmful mobile attacks, the regular agents must remove $2F$ neighbor values, which may include their own values. Comparing with the conventional LF algorithm, more values are removed at the removal step, and therefore, in our problem setting, a denser graph condition is necessary in order to guarantee the consensus.

3.3 Asymptotic safety result

In the previous subsections, we provided graph properties that guarantee consensus for the regular nodes under Algorithm 1. In this subsection, we provide a safety guarantee on these dynamics under additional conditions on the step-sizes, as detailed in the following theorem.

Theorem 3. Consider the multi-agent system under the mobile malicious agents following the F-total Buhrman's model. Suppose that one of the following conditions holds.

D1) The network is a complete graph, and $n \geq 2F+1$.
D2) The network satisfies C1 and C2 in Theorem 2.

Suppose that all regular nodes use Algorithm 1, and the local objective functions f_i at each node i are convex with subgradients bounded by some constant L, and each node i has a nonempty compact set of local minimizers $\mathcal{M}_i \subset \mathbb{R}$. Let $\overline{M} = \max\{x | x \in \mathcal{M}_i, i \in \mathcal{V}\}$ and $\underline{M} = \min\{x | x \in \mathcal{M}_i, i \in \mathcal{V}\}$. If the step-sizes satisfy $\sum_{k=1}^{\infty} \alpha_k = \infty$, $\sum_{k=1}^{\infty} \alpha_k^2 < \infty$, then $\limsup_{k\to\infty} x_i(k) \leq \overline{M}$ and $\liminf_{k\to\infty} x_i(k) \geq \underline{M}$ for all $i \in \mathcal{R}(k)$.

According to the safety result under the static malicious model (Theorem 7.1 in (Sundaram and Gharesifard, 2019)), the regular agents converge to the convex hull of the local minimizers of regular agents $i \in \mathcal{R}$. We can observe that all agents $i \in \mathcal{V}$ decide the safety area $\mathcal{S} = [\underline{M}, \overline{M}]$ in Theorem 3. The convex hull of regular agents' local function minimizers exhibits time-varying behavior because mobile malicious actors may change their positions. For any $i \in \mathcal{R}(k)$, it is evident that the safety area $\mathcal{S} = [\underline{M}, \overline{M}]$ contains all local function minimizers of regular agents because the local function $f_i(x)$ cannot be altered by malicious agents.

As shown in Theorem 3, the modified LF dynamics guarantee consensus within the convex hull of the local minimizers and prevent the adversarial nodes from driving the states of the regular nodes to arbitrarily large values under the appropriate conditions on the network topology. However, a single malicious node can still prevent the regular nodes from converging to a constant value under certain classes of step-sizes. This is different from the safety results in (Wang et al., 2022), where the regular nodes converge to a constant value. Note that the convergence to a constant in modified LF dynamics (Algorithm 1) does not hold even with a single mobile malicious node.

As a simple example, we consider a 3-node complete graph. The local functions of nodes are $f_1(x) = (x-1)^2$, $f_2(x) = (x-2)^2$, $f_3(x) = (x-3)^2$. Suppose that initially the mobile malicious node is node 1 and it does not move for a long time. The malicious node sends out a constant value that is much smaller than those of the regular nodes. Then, based on Theorems 6.4 and 7.1 in (Sundaram and Gharesifard, 2019) under static model, the states of nodes 2 and 3 converge in the area $(2, 3)$. Then, let the malicious node move to node 3 and stay there for a sufficiently long time. Then, the states of nodes 1 and 2 converge in the area $(1, 2)$. If such movements are conducted repeatably, the regular states oscillate within the area $(1, 3)$ and do not converge to a constant.

4. NUMERICAL EXAMPLES

Numerical simulations are performed with two communication networks, that is, a complete graph and a non-complete graph.

Complete Graph: First, we test both the conventional LF algorithm and the proposed modified LF algorithm under a 10-node complete graph. Partition the nodes into two groups $\mathcal{V}_1$ and $\mathcal{V}_2$. For Group $\mathcal{V}_1$ (respectively $\mathcal{V}_2$), set the objective function to be $f_i = (x-4)^2, i \in \mathcal{V}_1$ (respectively $f_i = (x-6)^2, i \in \mathcal{V}_2$). Therefore, the safety area is

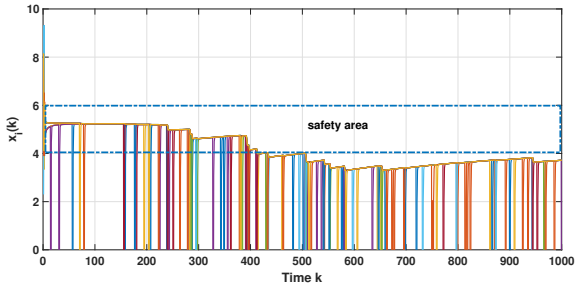

Fig. 2. Conventional LF dynamics under a single mobile malicious node.

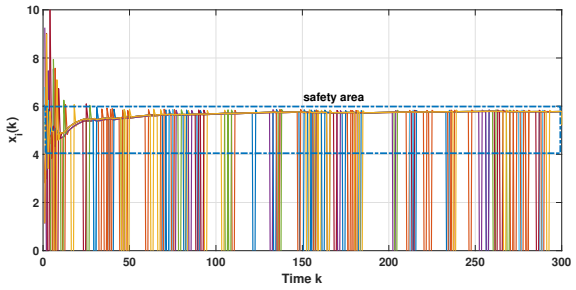

Fig. 3. Modified LF dynamics under complete graph with mobile malicious model, $F = 4$.

$\mathcal{S} = [4, 6]$. Initially, the regular nodes randomly take their values in $[0, 10]$, and let step-size $\alpha_k = 1/k$. Moreover, the mobile strategy of the malicious nodes is to move randomly in the whole network at each time. The malicious nodes $i \in \mathcal{A}(k)$ take the constant value $x_i(k) = -10$. The goal of the mobile malicious nodes is to mislead all regular nodes outside the safety area $\mathcal{S}$.

In Fig. 2, we display the conventional LF dynamics under a single mobile malicious node. It shows that all regular nodes are outside the safety area after time $k = 500$. As we analysed in Proposition 2, when the mobile malicious node left, the cured node is equipped with the corrupted negative value. Such values are used in the following updates based on the LF algorithm, which eventually misleads all regular nodes outside the safety area. As a comparison, we check the performance of the proposed modified LF algorithm. Based on Theorem 1, we know that a 10-node graph may tolerant at most four mobile malicious agent. Therefore, we set $F = 4$. Four nodes are initially chosen as malicious nodes, and they follow the aforementioned mobile strategy. The system dynamics is shown in Fig. 3, where we can check that all regular nodes eventually reach consensus in the safety area.

Non-complete Graph: Our focus of another experiment setup is to determine how well the proposed protocol performs under practical settings when the assumptions introduced in Theorem 2 may not hold. Specifically, we use randomly generated networks where the connectivity requirements are in general difficult to check due to the size of the network. For the network topology, we generated one hundred random geometric graphs with 100 nodes located in an area of 100×100 randomly under the uniform distribution. Each agent has a communication range determined by the radius $r = 40$, within which it can communicate with all agents. The network topology

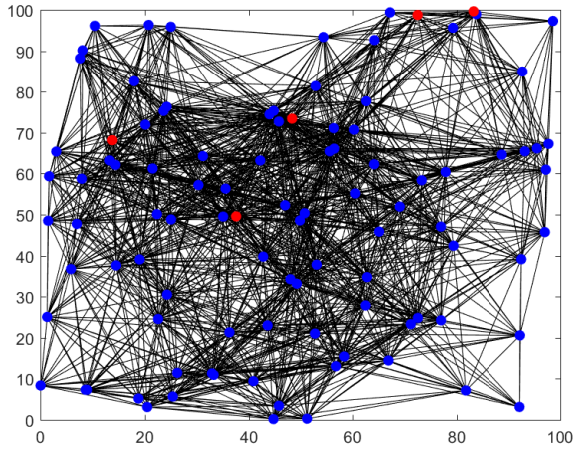

Fig. 4. Network topology $\mathcal{G}_1$ with $F = 5$.

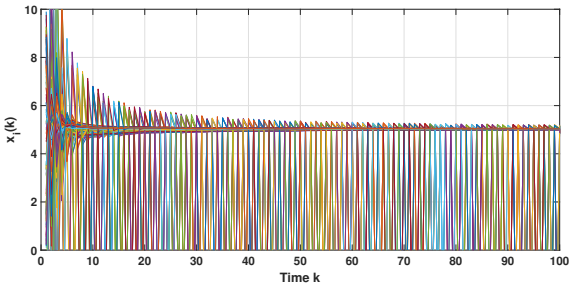

Fig. 5. Modified LF dynamics under graph $\mathcal{G}_1$ with mobile malicious model, $F = 5$.

$\mathcal{G}_1$ is shown in Fig. 4. The regular agents are drawn in blue while the initial malicious agents are in red. Here, five malicious agents are introduced.

The system dynamics for the modified LF algorithm under graph $\mathcal{G}_1$ is depicted in Fig. 5. The regular agents asymptotically reach consensus in the safety interval $\mathcal{S} = [4, 6]$, despite the influences of mobile malicious behaviors. In addition, the topology $\mathcal{G}_1$ does not meet the condition D2 in Theorem 2. Therefore, comparing with the non-complete networks discussed in Theorem 2, the proposed modified LF dynamics can practically solve the resilient optimization problem in a wider range of networks.

5. CONCLUSION

In this paper, we have considered the multi-agent distributed optimization problem in the presence of mobile misbehaving agents and have developed a resilient algorithm to mitigate their influence on the regular agents. Particularly, a modified LF algorithm has been suggested in a mobile malicious model. Through theoretical investigations under networks in both complete and non-complete graph forms, we have characterized the criteria on the required graph structures for the protocol to perform the resilient optimization with safety guarantees. We have further investigated the performance of the proposed resilient optimization algorithms for non-complete networks where the theoretical assumptions might not hold using numerical simulations. For future, we plan to devise more general algorithms for various mobile adversary models. Additionally, it is important to consider communication time delays and asynchronous update behaviors.

REFERENCES

Buhrman, H., Garay, J.A., and Hoepman, J.H. (1995). Optimal resiliency against mobile faults. *Twenty-Fifth International Symposium on Fault-Tolerant Computing. Digest of Papers*, 83–88.

Dibaji, S.M., Ishii, H., and Tempo, R. (2017). Resilient randomized quantized consensus. *IEEE Transactions on Automatic Control*, 63(8), 2508–2522.

Dolev, D., Lynch, N.A., Pinter, S.S., Stark, E.W., and Weihl, W.E. (1986). Reaching approximate agreement in the presence of faults. *Journal of the ACM (JACM)*, 33(3), 499–516.

Gupta, N. and Vaidya, N.H. (2020). Resilience in collaborative optimization: Redundant and independent cost functions. *arXiv preprint arXiv:2003.09675*.

Ishii, H., Wang, Y., and Feng, S. (2022). An overview on multi-agent consensus under adversarial attacks. *Annual Reviews in Control*.

Kieckhafer, R. and Azadmanesh, M. (1992). Fault-tolerant convergent voting in large sparsely connected networks. In *Proc. Complex Syst Eng'g Synth. and Assessment Tech. Workshop*, 31–51.

Kuwaranancharoen, K., Xin, L., and Sundaram, S. (2020). Byzantine-resilient distributed optimization of multi-dimensional functions. In *Proc. American Control Conference (ACC)*, 4399–4404.

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

Nedić, A. and Ozdaglar, A.E. (2009). Distributed subgradient methods for multi-agent optimization. *IEEE Transactions on Automatic Control*, 54, 48–61.

Nedić, A., Ozdaglar, A.E., and Parrilo, P.A. (2010). Constrained consensus and optimization in multi-agent networks. *IEEE Transactions on Automatic Control*, 55, 922–938.

Su, L. and Vaidya, N.H. (2021). Byzantine-resilient multiagent optimization. *IEEE Transactions on Automatic Control*, 66, 2227–2233.

Sundaram, S. and Gharesifard, B. (2019). Distributed optimization under adversarial nodes. *IEEE Transactions on Automatic Control*, 64, 1063–1076.

Wang, Y., Ishii, H., Bonnet, F., and Défago, X. (2022). Resilient real-valued consensus in spite of mobile malicious agents on directed graphs. *IEEE Transactions on Parallel and Distributed Systems*, 33, 586–603.

Wu, Z., Chen, T., and Ling, Q. (2022). Byzantine-resilient decentralized stochastic optimization with robust aggregation rules. *arXiv preprint arXiv:2206.04568*.

Yang, T., Yi, X., Wu, J., Yuan, Y., Wu, D., Meng, Z., Hong, Y., Wang, H., Lin, Z., and Johansson, K.H. (2019). A survey of distributed optimization. *Annual Reviews in Control*, 47, 278–305.

Zhang, H., Fata, E., and Sundaram, S. (2015). A notion of robustness in complex networks. *IEEE Transactions on Control of Network Systems*, 2(3), 310–320.

Zhu, J., Lin, Y., Velasquez, A., and Liu, J. (2022). Resilient distributed optimization. *arXiv preprint arXiv:2209.13095*.