On the non-resiliency of subsequence reduced resilient consensus in multiagent networks

Leon Khalyavin, Waseem Abbas

PII: S0947-3580(24)00180-8
DOI: https://doi.org/10.1016/j.ejcon.2024.101120
Reference: EJCON 101120

To appear in: *European Journal of Control*

Received date : 7 February 2024
Revised date : 19 September 2024
Accepted date : 20 September 2024

Please cite this article as: L. Khalyavin and W. Abbas, On the non-resiliency of subsequence reduced resilient consensus in multiagent networks. *European Journal of Control* (2024), doi: https://doi.org/10.1016/j.ejcon.2024.101120.

ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

00 (2024) 1–20

European Journal of Control

On the Non-resiliency of Subsequence Reduced Resilient Consensus in Multiagent Networks

Leon Khalyavin[a], Waseem Abbas[b]

[a]*Imperial College London, London, SW7 2AZ, UK*
[b]*University of Texas at Dallas, Richardson, TX 75080, USA*

Abstract

This paper studies resilient distributed consensus in networks lacking the structural robustness necessary for achieving consensus in the presence of misbehaving agents. Existing resilient consensus solutions, including widely adapted *weighted mean subsequence reduced (WMSR)* resilient consensus algorithm, present robustness conditions guaranteeing consensus among normal agents. However, when the graph is less robust than required, they only inform that agents fail to achieve consensus and do not evaluate the network performance comprehensively in such non-ideal scenarios. To address this limitation, we analyze the performance of resilient consensus in non-ideal situations by introducing the concept of *non-convergent nodes*. These nodes/agents cannot achieve consensus with any arbitrary agent due to the presence of misbehaving agents in the network. This notion enables ordering graphs that lack required robustness and facilitates the assessment of partial performance. Additionally, we demonstrate that among graphs with the same level of robustness (measured by their (r, s)-robustness), the number of non-convergent nodes varies significantly, indicating differing degrees of non-resilience. We also present numerical evaluation of results. Our approach quantifies the network performance under sub-optimal robustness conditions and offers a comprehensive resilience perspective.

Keywords: Resilient consensus, multiagent networks, graph robustness, distributed algorithms.

1. Introduction

In a networked multiagent system, the presence of a few adversarial or misbehaving agents can severely disrupt the system's behavior. Intelligent attacks targeting a subset of agents can impede the system from achieving its desired performance objectives. Consider the *distributed consensus* in multiagent systems, a canonical problem with several applications across various domains, including networked control systems, multi-robot systems, and sensor networks. The primary goal here is to ensure that all agents update their local states in a way that eventually converges to a common state. A simple *Linear Consensus Protocol (LCP)*, where each agent updates its state by averaging its neighbors' states, solves the problem (e.g., [1, 2, 3]). However, a single misbehaving agent–agent that does not adhere to the LCP–can prevent agents from achieving consensus (e.g., [4]). The primary objective of *resilient* network systems is to withstand such disruptive scenarios, guaranteeing the system's performance objectives despite misbehaving agents.

In a multiagent system, agents collect and incorporate data from neighbors while updating their states and making decisions. To achieve resilience against misbehaving agents, designing strategies that discard information from 'bad' neighbors during data aggregation and prioritize data from 'good' neighbors is crucial. Additionally, ensuring that each agent has a sufficient number of 'good' neighbors enhances resilience. Based on these principles, various resilient distributed strategies and algorithms have been proposed to tackle distributed optimization problems like consensus [4, 5, 6, 7, 8, 9, 10, 11, 12, 13], diffusion [14, 15, 16], estimation [17, 18, 19, 20], learning and optimization [21, 22, 23,

24, 25, 26, 27]. In particular, the *Weighted-Mean-Subsequence-Reduced (WMSR)* algorithm, presented in [4], stands out as a widely used resilient distributed consensus approach. By 'trimming' (ignoring) extreme values collected from neighbors during aggregation and leveraging structural conditions on the network graph, agents implementing the WMSR algorithm achieve consensus in the face of misbehaving agents. Considering the wide success of the trimming approach offered by the WMSR algorithm, several variants of WMSR have been proposed in the literature, for example, [4, 7, 28, 29, 9, 30, 31, 25, 32, 33, 20, 34, 35, 36, 37, 38]. Additionally, other approaches have been proposed that assign a 'score' to neighbor values and weight them accordingly when updating agent states. (e.g., [39, 13, 29, 14]).

In general, to study resilience in a distributed framework, we must consider three aspects: the algorithm, the structure of the network, and the adversarial attack. The algorithm refers to the state update protocol of the normal 'good' nodes in the network. The structure of the network refers to the interconnections among agents and describe information sharing among agents. Finally, the adversarial model describes the abilities of the misbehaving nodes and tries to approximate the scale of the attack on the network. Current resilient strategies for multiagent networks effectively address adversarial scenarios. In particular, the WMSR algorithm guarantees consensus among normal (i.e., non-adversarial) agents if the number of misbehaving agents is bounded by F and the network graph meets the required robustness condition, which depends on F.

However, the WMSR algorithm (and its variants) adopts an *all or nothing* approach to resilience, wherein meeting specific conditions ensures overall performance (consensus). Nevertheless, even the slightest deviation from these conditions can lead to significant performance degradation. For example, if there is one more adversary than permitted in the network, or if the graph slightly lacks the required robustness, agents may move arbitrarily far from their initial positions, leading to a deterioration in the performance of the resilient consensus algorithm. Consequently, analyzing the algorithm's performance under non-ideal situations becomes challenging, making it difficult to determine how many agents can achieve consensus. This challenge is exacerbated when the actual number of misbehaving agents exceeds the predefined threshold (F), necessitating the identification of agents that can or cannot achieve consensus. In more realistic scenarios, it is crucial to assess the partial performance of the network in non-ideal situations – that is, determining how many agents can still achieve consensus. Therefore, evaluating network performance in a continuous manner, rather than a binary 'objective achieved or not achieved' approach, becomes crucial. This requires exploring methods to rank networks based on their robustness, particularly when they fall short of desired resilience.

In this paper, we raise and study the following issue: *How can we evaluate the performance of the WMSR resilient consensus algorithm in a network that fails to meet the structural robustness threshold for guaranteeing consensus when facing F misbehaving agents?* To quantify the 'non-resilience' of such graphs, we introduce the concept of *non-convergent nodes*, which refers to agents in the network that fail to achieve consensus with any arbitrary agent in the network due to the presence of misbehaving agents (Section 3). This novel concept allows us to order graphs that lack the robustness criteria for resilience against F misbehaving agents, as Figure 1 illustrates. The graph G (green) in the figure guarantees consensus despite a single misbehaving agent (i.e., $F = 1$) due to its $(2, 2)$-robustness, as explained later in Section 2.1. In contrast, graphs G_1, G_2, G_3, and G_4 are all $(2, 1)$-robust and fail to meet the required robustness for resilience against a single misbehaving agent. Current resilience frameworks lack the ability to determine which of these four graphs is relatively better/worse than the others.

Using the concept of non-convergent nodes, we can rank graphs based on their 'non-resilience,' allowing us to evaluate partial performance by quantifying the number of non-convergent nodes. Subsequently, in the paper (Sections 3.1, 3.2, and 3.3), we show that there is significant variation in the number of non-convergent nodes among graphs with the same robustness. In particular, we examine various graph families categorized by their robustness and identify the graphs with the maximum and minimum number of non-convergent nodes within each family. Our results show that, within a single family of graphs, there can be graphs with no non-convergent nodes, as well as graphs where nearly all nodes are non-convergent. This underscores a substantial disparity in non-resilience even among graphs with the same robustness. The main contributions of the paper are summarized below:

- We introduce the idea of non-convergent nodes in graphs to characterize the degree of non-resilience against misbehaving agents. A non-convergent node refers to a normal node for which attacks exist, preventing it from converging to any arbitrary node in the graph. By applying this notion, we compare graphs that fail to meet the required graph robustness conditions for the WMSR resilient consensus algorithm with F misbehaving agents, enabling the evaluation of partial performance in such networks.

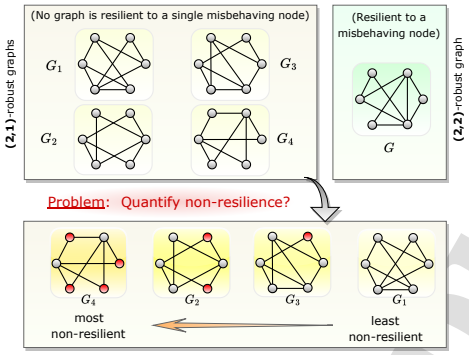


Figure 1: G is robust enough against a single misbehaving agent, whereas G_1, G_2, G_3, G_4 are not. By measuring the number of non-convergent nodes (red), we characterize the non-resilience in graphs whose robustness is below the required threshold.

- To assess the potential number of non-convergent nodes in networks under non-ideal robustness conditions, we systematically construct graphs designed to maximize the presence of such nodes. This analysis provides insight into the degree of non-resilience exhibited by networks failing to meet the required robustness criteria, as measured by the (r, s)-robustness metric. Specifically, we generate extremal cases for various (non-ideal) robustness conditions, including $(F+1, 1)$, (F, F), and $(F+1, F)$ scenarios, employing circulant graphs, complete graphs, and their combinations. By doing so, we quantify the worst-case deterioration in network performance when facing more misbehaving agents than initially anticipated during the network design phase.
- We provide a detailed numerical evaluation of our proposed approach, illustrating our results and highlighting potential research directions. Through illustrative examples and numerical simulations, we showcase the practical relevance of our findings and highlight the importance of considering non-ideal conditions in resilience analysis.

We note that resilience against misbehaving agents hinges on the choice of the distributed algorithm (state update rule). In our paper, we focus on the WMSR algorithm, a cornerstone in resilient distributed consensus. However, our approach is not restricted to the WMSR algorithm. Instead, it provides a framework that can readily be adapted to examine the performance of other resilient distributed algorithms in non-ideal scenarios. The rest of the paper is organized as follows: Section 2 introduces the preliminaries, provides an overview of the WMSR resilient consensus algorithm, and explains our problem. Section 3 is the main section introducing the notion of non-convergent nodes. It also presents graphs that, for given robustness specification, maximize the number of non-convergent nodes. Section 4 illustrates and experimentally evaluates the results. Finally, Section 5 concludes the paper.

2. Preliminaries and Resilient Distributed Consensus

We model a network of agents by an *undirected graph* $G = (V, E)$, where the vertex set V represents agents and the edge set E represents interactions and information exchange between agents. We use the terms vertex, node, and agent interchangeably. An (undirected) edge between nodes u and v is denoted by (u, v). The *neighborhood* of node u, denoted by $\mathcal{N}_u$, is $\{v \in V : (u, v) \in E\}$. The *degree* of node u is the number of nodes in $\mathcal{N}_u$. The cardinality of a subset of vertices $S \subseteq V$ is the number of nodes in S, and denoted by $|S|$.

Each agent $u \in V$ has a state $x_u(k) \in \mathbb{R}$ at time k that it updates according to a predefined state update rule while incorporating the state values of its neighbors in the update step. For the *distributed consensus* of agents, the goal is to design the state update rule guaranteeing the *safety* and *agreement* conditions stated below.

Definition 2.1. *(*Distributed consensus*) A network of agents $G = (V, E)$ achieves consensus if the following conditions are satisfied:*

1. *(Safety) Let* $x_{\min}(0)$ *and* $x_{\max}(0)$ *denote the minimum and the maximum of the initial states of nodes in G, respectively. Then,* $x_{\min}(0) \leq x_u(k) \leq x_{\max}(0), \quad \forall u \in V$*, and for all times k.*
2. *(Agreement) As* $k \to \infty$*,* $x_u(k) = x_v(k) = x$ *for all pairs of nodes* $u, v \in V$*.*

A simple state update rule, *Linear Consensus Protocol (LCP)*, solves the distributed consensus problem under conditions such as the network is connected. The LCP, defined below, has been extensively studied in the literature and widely applied.

$$x_u(k+1) = \sum_{v \in (\mathcal{N}_u \cup \{u\})} w_{uv}\, x_v(k), \tag{1}$$

where w_{uv} is some (positive) weight assigned by node u to the state value of v. Since G is undirected in our case, $w_{uv} = w_{vu}$. We consider that agents exchange state values with each other in a synchronous manner.

2.1. Resilient Distributed Consensus

It is well-known that (1) is not resilient to misbehaving nodes that deviate from the LCP update rule. In fact, a single misbehaving node can prevent the network from achieving consensus. Thus, distributed algorithms are designed to guarantee consensus despite misbehaving nodes. Misbehaving nodes in a network can manifest in different models, notably the *malicious* and *Byzantine* models. A **malicious** node disregards the LCP to update its state; however, it consistently sends the *same* state value to all of its neighbors at each time step k. On the other hand, a **Byzantine** node is one that not only disregards the LCP but can also send a different state value to each of its neighbors at each time step. Similarly, the influence of misbehaving nodes on the network is also determined by their numbers, leading to the formulation of models like the F*-total* and the F*-local*. In the F**-total** model, the maximum number of misbehaving nodes in the entire network is bounded by F. Conversely, in the F**-local** model, the maximum number of misbehaving nodes in the neighborhood of each node is at most F.

The *Weighted Mean Subsequence Reduced (WMSR)* algorithm in [4] offers a simple and efficient solution to the resilient distributed consensus problem. WMSR is a type of a 'trimming' algorithm, which essentially trims or ignores some of the extreme (largest and smallest) state values collected from its neighbors during the state update. The rationale is to prevent potentially malicious or Byzantine-influenced values from impacting the node's state. The main steps of the **WMSR algorithm** are as follows:

1. Each normal node u collects state values of neighbors at each time step k and sorts them.
2. It then removes the F largest (smallest) values strictly greater (smaller) than $x_u(k)$. If the number of values strictly greater (smaller) than $x_u(k)$ are less than F, then u removes all the values strictly greater (smaller) than its own value. Let the set of nodes in $\mathcal{N}_u$ whose state values are removed by u at the time step k are denoted by $\mathcal{R}_u(k)$.
3. The node u then updates its state according to the following:

$$x_u(k+1) \;=\; \sum_{v \in (\mathcal{N}_u \cup \{u\}) \setminus \mathcal{R}_u(k)} w_{uv}\, x_v(k). \tag{2}$$

The WMSR algorithm guarantees that normal nodes achieve distributed consensus despite misbehaving nodes, given that the underlying network graph fulfills certain robustness conditions. These conditions are defined using a graph robustness metric referred to as (r, s)**-robustness**. We define the (r, s)-robustness and related notions below, and then state relevant conditions on the graph (from [4]) guaranteeing resilient consensus despite misbehaving nodes.

Definition 2.2. (r-reachable set of S, $\mathcal{X}_S^r$) *Given a graph* $G = (V, E)$*, a subset* $S \subset V$*, and a positive integer* r*. A node* $x \in S$ *is* r-reachable *in* S *if it has at least* r *neighbors outside of* S*. The set of* r*-reachable nodes in* S *is*

$$\mathcal{X}_S^r = \{x \in S \,:\, |\mathcal{N}_x \setminus S| \geq r\}. \tag{3}$$

We now define the notion of (r, s)-robustness in graphs.

Definition 2.3. ((r, s)-robust graph [4]) *For positive integers* r *and* s*, a graph* $G = (V, E)$ *is* (r, s)*-robust if for* every *pair of non-empty disjoint subsets of nodes* $S_1, S_2 \subset V$*, at least one of the following conditions is satisfied.*

(i) $|\mathcal{X}^r_{S_1}| = |S_1|$ *(i.e., each node in* S_1 *has at least* r *neighbors outside of* S_1*),*

(ii) $|\mathcal{X}^r_{S_2}| = |S_2|$ *(i.e., each node in* S_2 *has at least* r *neighbors outside of* S_2*),*

(iii) $|\mathcal{X}^r_{S_1}| + |\mathcal{X}^r_{S_2}| \geq s$ *(i.e. the number of nodes in* S_1 *and* S_2 *having at least* r *neighbors outside of their respective sets is at least* s*).*

We illustrate these conditions in Figure 2.

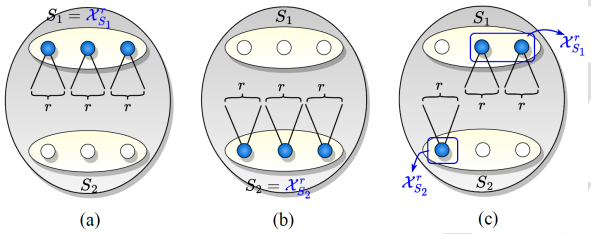


Figure 2: Three conditions for (r, s)-robustness. Blue nodes have at least r neighbors outside of their subset. (a) $|\mathcal{X}^r_{S_1}| = |S_1|$, (b) $|\mathcal{X}^r_{S_2}| = |S_2|$, (c) $|\mathcal{X}^r_{S_1}| + |\mathcal{X}^r_{S_2}| \geq s$.

LeBlanc et al. in [4] provide robustness conditions on the network graph to achieve resilient consensus under F-total/local and malicious/Byzantine models. For example, to guarantee consensus under the F**-total malicious** model, a *necessary and sufficient* condition is stated below.

Theorem 2.1. *[4] Consider a network* $G = (V, E)$ *with* $|V| = N$ *nodes, of which at most* F *nodes are malicious (i.e.,* F*-total malicious model). If each normal node implements the WMSR algorithm with parameter* F*, then the distributed consensus of normal nodes is achieved if and only if* G *is* $(F + 1, F + 1)$*-robust.*

It means that *any* graph that is not $(F + 1, F + 1)$-robust is not 'good enough' to achieve resilient consensus in a network with F malicious nodes, that is, we cannot guarantee that all normal nodes converge to a common state.

2.2. Main Question

In existing research, results for resilient distributed consensus generally offer a binary view: a network graph under a specific misbehavior model either satisfies the robustness criterion to guarantee all normal agents' convergence to a common point, or falls short. However, this dichotomous approach limits the possibility of a comparative analysis between network graphs that fail to meet the robustness criteria, thus leaving a gap in our understanding of the relative suitability of different graphs for consensus. Consider two distinct graphs, $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$, both of which are $(F + 1, F)$-robust. Under an F-total malicious model, both graphs fall short of the robustness necessary to confirm resilient consensus per the WMSR algorithm (Theorem 2.1). However, it is plausible that one graph demonstrates a relative advantage over the other in terms of achieving resilient distributed consensus. This raises an important question:

How can we evaluate the performance of a network that fails to meet the robustness threshold for guaranteeing consensus when facing F *misbehaving agents under different attack scenarios?*

To address this issue, the paper introduces the concept of *non-convergent* nodes within a network to measure a network's degree of non-resilience. As a result, we can assess the network's inadequacy for resilient consensus in scenarios where the network robustness falls short. This new methodology enables us to extend the analysis of network resilience beyond existing frameworks, allowing for comparative evaluation of networks that fall short of the required robustness. We demonstrate that networks of the same size and with the same (r, s)-robustness may exhibit varying quantities of non-convergent nodes. We focus on the constructions that lead to the maximum number of non-convergent nodes under a given (r, s)-robustness condition.

Remark 2.2. *This paper primarily focuses on the **F-total malicious** nodes model; however, the results can be readily adapted to other models, including the F-local and Byzantine models. Furthermore, although we consider the resilient consensus problem here, the approach remains applicable in other resilient distributed optimization setups (e.g., [25, 27, 40]), where the network must meet some connectivity or robustness conditions for resilience against misbehaving nodes.*

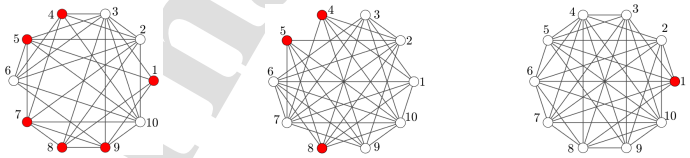
3. Quantifying Non-resilience of WMSR Resilient Consensus

In this section, we first define the concept of *non-convergent* nodes to quantify the degree of 'non-resilience' in networks failing to meet the required robustness condition. Then, we construct networks with the maximal number of non-convergent nodes. The goal is to demonstrate the significant variation in the number of non-convergent nodes across graphs with the same robustness. We recall that an (r, s)-robust network, where either r or s is smaller than $F + 1$, does not guarantee resilient consensus in the face of F malicious nodes. Therefore, to highlight the extent of non-resilience in networks under the F-total malicious model, we design (r, s)-robust graphs for different values of r and s while maximizing the number of non-convergent nodes. Finally, we demonstrate that graphs with the same (r, s)-robustness may have varying numbers of non-convergent nodes.

At the network level, the adversary aims to disrupt the convergence of all normal nodes at a common point by utilizing F malicious nodes. At the node level, the adversary's influence can be determined by its ability to prevent a normal node u from converging with another arbitrary normal node. For example, consider a normal node u in a network $G = (V, E)$. An attack consisting of F malicious nodes may exist, preventing u and some other normal node, say v, from converging; however, no such attack might be possible that hinders the convergence of u and a different normal node, say w. Hence, we evaluate the adversary's impact at the node level by measuring its ability to prevent a normal node u from converging with any other arbitrary normal node. This concept is formally defined as follows:

Definition 3.1. (Non-convergent node) *A normal node u is non-convergent (under the F-total model) if for every $v \in V \setminus \{u\}$ there is a set of at most F malicious nodes from $V \setminus \{u, v\}$ preventing u and v from converging at a common point. We denote the number of non-convergent nodes in G by $\alpha_F(G)$.*

If a graph is $(F + 1, F + 1)$-robust, there are no non-convergent nodes under the F-total malicious nodes model (by Theorem 2.1). However, when the graph's robustness is lower, that is, G is (r, s)-robust for $r, s < F + 1$, then the network may have multiple non-convergent nodes depending on the structure of G. A detailed illustration of a non-convergent node is presented in Section 4. Non-convergent nodes signify lack of guaranteed convergence to any other node, directly reflecting the network's vulnerability and non-resilience to F malicious nodes. As the robustness of the graph increases, the number of non-convergent nodes generally decreases. Figure 3 illustrates this, where none of the three graphs is $(4, 4)$-robust.



(a) $(4, 1)$-robust (b) $(4, 2)$-robust (c) $(4, 3)$-robust

Figure 3: The number of non-convergent nodes (highlighted red) in (a), (b), and (c) are 6, 3, and 1, respectively.

However, it is important to note that graphs with the same (r, s)-robustness can still have different numbers of non-convergent nodes, as discussed in Section 4 (Figure 10). Thus, graphs with the same (r, s)-robustness can exhibit varying levels of ability (or inability) to handle adversarial attacks, as indicated by the number of non-convergent nodes. To systematically study this, we consider various graph families in which all graphs within a given family have the same (r, s)-robustness for some r and s. We then examine the maximum and minimum values of $\alpha(G)$ within each family. This approach will reveal the extent of variation in the number of non-convergent nodes among graphs with identical (r, s)-robustness. To formalize this, we define the following:

Definition 3.2. *Let $\mathbb{G}(N, r, s)$ represent the family of all graphs consisting of N nodes that are (r, s)-robust. For a positive integer F, we define*

$$\overline{\alpha_F}\left(\mathbb{G}(N, r, s)\right) = \max_{G \in \mathbb{G}(N,r,s)} \alpha_F(G), \tag{4}$$

$$\underline{\alpha_F}\left(\mathbb{G}(N, r, s)\right) = \min_{G \in \mathbb{G}(N,r,s)} \alpha_F(G), \tag{5}$$

where $\alpha_F(G)$ is the number of non-convergent nodes in G under the F-total model.

Since $\overline{\alpha_F}$ in (4) represents the maximum number of non-convergent nodes a graph can have within a given family, it characterizes the worst-case scenario from a non-resilience perspective. Conversely, $\underline{\alpha_F}$ represents the best-case scenario. Here, we consider three distinct graph families: $\mathbb{G}(N, F+1, 1)$, $\mathbb{G}(N, F, F)$, and $\overline{\mathbb{G}}(N, F+1, F)$. Note that all these families contain graphs lacking the necessary robustness to be resilient against F malicious nodes. We explain the choice of these cases below.

- $\mathbb{G}(N, F, F)$: This family contains (F, F)-robust graphs that demonstrate resilience up to $F-1$ malicious agents. This case, therefore, assesses the existence of non-convergent nodes when the network faces one additional malicious node beyond its design capacity.
- $\mathbb{G}(N, F+1, F)$: This family contains $(F+1, F)$-robust graphs, which are positioned closely to the ideal $(F+1, F+1)$-robust graphs; however, they fail to ensure resilience against F malicious nodes. Our examination here revolves around understanding the potential number of non-convergent nodes in graphs that narrowly miss meeting the desired robustness criteria.
- $\mathbb{G}(N, F+1, 1)$: This group contains $(F+1, 1)$-robust graphs, which are considered because the parameter r in (r, s)-robustness generally takes precedence in the partial order that determines relative robustness. So, we consider the case where r condition is satisfied (i.e., $r = F+1$); however, the s condition is completely relaxed.

These diverse cases offer valuable insights into the trade-offs and implications of varying levels of graph robustness, shedding light on the nuanced relationship between structural properties and resilience in distributed consensus scenarios. Note that if a graph G is $(\hat{r}, \hat{s})$-robust for some $\hat{r}$ and $\hat{s}$, then it must also be (r, s)-robust for $r \leq \hat{r}$ and $s \leq \hat{s}$. Thus, $\mathbb{G}(N, \hat{r}, \hat{s}) \subseteq \mathbb{G}(N, r, s)$ for $\hat{r} \geq r$ and $\hat{s} \geq s$. For instance, consider a family $\mathbb{G}(N, F, F)$, and a graph G, where G is an $(F+1, F+1)$-robust graph with N nodes. Since G must also be (F, F)-robust, $G \in \mathbb{G}(N, F, F)$. More generally, $\mathbb{G}(N, F+1, F+1) \subseteq \mathbb{G}(N, F, F)$. Furthermore, an $(F+1, F+1)$-robust graph G will not have any non-convergent node, and therefore, $\alpha_F(G) = 0$, which means $\underline{\alpha_F}\left(\mathbb{G}(N, F+1, F+1)\right) = 0$. This directly implies that $\underline{\alpha_F}\left(\mathbb{G}(N, F, F)\right) = 0$. By a similar argument and observing that $\overline{\mathbb{G}}(N, F+1, F+1) \subseteq \mathbb{G}(N, F+1, F)$, and $\mathbb{G}(N, F+1, \overline{F+1}) \subseteq \mathbb{G}(N, F+1, 1)$, we deduce, $\underline{\alpha_F}\left(\mathbb{G}(N, F+1, F)\right) = 0$ and $\underline{\alpha_F}\left(\mathbb{G}(N, F+1, 1)\right) = 0$.

Next, we focus on finding the maximum number of non-convergent nodes a graph can have within a graph family, i.e., $\overline{\alpha_F}\left(\mathbb{G}(N, F+1, 1)\right)$, $\overline{\alpha_F}\left(\mathbb{G}(N, F, F)\right)$, and $\overline{\alpha_F}\left(\mathbb{G}(N, F+1, F)\right)$. For this, we construct $(F+1, 1)$, (F, F), and $(F+1, F)$-robust graphs with the maximal number of non-convergent nodes under the F-total malicious nodes model. Our constructions leverage the circulant graph, empty graph, and graph join operations, which we define below.

Definition 3.3. (Circulant graph) *A circulant graph $C_{N_c}^{1,2,\cdots,M}$ is an undirected graph with N_c nodes, denoted by $\{u_0, u_1, \cdots, u_{N_c-1}\}$, where each u_i is adjacent to $u_{i \pm j \pmod{N_c}}$ for all $j \in \{1, \cdots, M\}$.*

We note that the degree of each node in $C_{N_c}^{1,2,\cdots,M}$ is $2M$.

Definition 3.4. (Empty graph) *An* empty graph*, denoted by $\mathcal{E}_N$, is a graph with N nodes and an empty edge set.*

Definition 3.5. (Graph Join) *Given two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, the join graph, denoted by $G_1 \oplus G_2 = (V_1 \cup V_2, E_1 \cup E_2 \cup \{(a, b) : \ a \in V_1, \ b \in V_2\})$. In other words, each node u in G_1 is adjacent to all the nodes in G_2.*

Figure 4 illustrates the circulant graph $C_7^{1,2}$ (blue), empty graph $\mathcal{E}_2$ (gray) and their join $\mathcal{G} = \mathcal{E}_2 \oplus C_7^{1,2}$.

3.1. $(F+1,1)$-robust Graphs

In this sub-section, we consider the graph family $\mathbb{G}(N, F+1, 1)$ and examine the $(F+1,1)$-robustness condition that is considerably less restrictive compared to the $(F+1, F+1)$-robustness (which guarantees the absence of non-convergent nodes as well as resilient consensus despite F malicious nodes). We show that there are $(F+1,1)$-robust graphs, wherein almost all the nodes are non-convergent, thus, showing that $\overline{\alpha_F}(\mathbb{G}(N, F+1, 1))$ is close to N.

Lemma 3.1. *For given integers $F \geq 2$ and $N_c \geq 2F+1$, the graph $\mathcal{G} = \mathcal{E}_2 \oplus C_{N_c}^{1,\cdots,F-1}$ is $(F+1,1)$-robust.*

Proof. Let U and V denote the set of nodes in $C_{N_c}^{1,\cdots,F-1}$ and $\mathcal{E}_2$, respectively. Let S_1 and S_2 be two disjoint non-empty sets of nodes in $\mathcal{G}$. We show that at least one of these subsets is $(F+1)$-reachable. There are three cases.

(a) At least one of the subsets contains nodes from V only. Without the loss of generality (w.lo.g.), assume $S_1 \subseteq V$. Since $|U| = N_c \geq 2F+1$ and each $v \in S_1$ is adjacent to all nodes in U, we get $\mathcal{X}_{S_1}^{F+1} = S_1$ (recall Definition 2.3).

(b) At least one of the subsets, say S_1, contains nodes from U only, i.e., $S_1 \subseteq U$. There are two choices for S_2.

(b-1) $S_2 \cap V = \emptyset$: In this case, at least one of the subsets S_1 and S_2 have at most F nodes as $|U| \geq 2F+1$. W.l.o.g., assume $|S_1| \leq F$. Each node in U, and hence in S_1, has at $2F-2$ neighbors in U. Thus, each $u \in S_1$ has at least $(2F-2)-(F-1) = F-1$ neighbors in $U \setminus S_1$. Also, each $u \in S_1$ is adjacent to both nodes in V. Thus, $u \in S_1$ has at least $F-1+2 = F+1$ neighbors outside of S_1, thus, the subset S_1 is $(F+1)$-reachable.

(b-2) $S_2 \cap V \neq \emptyset$: If $|S_1| \leq F$, then S_1 is $(F+1)$-reachable by the above case (b-1). So, assume $|S_1| \geq F+1$. Since $V \cap S_2 \neq \emptyset$, let $v \in (S_2 \cap V)$. Note that v is adjacent to all nodes in S_1, which means the subset S_2 is $(F+1)$-reachable.

(c) S_1 and S_2 contain nodes from both U and V. Let $v_1 \in (S_1 \cap V)$ and $v_2 \in (S_2 \cap V)$. Since $|U| \geq 2F+1$, at least one of the subsets $S_1 \cap U$ and $S_2 \cap U$ has at most F nodes. Assume w.l.o.g. that $|S_1 \cap U| \leq F$. Then, v_1 has at least $F+1$ neighbors outside of S_1 (as v_1 is adjacent to all the nodes in U). As a result, S_1 is $(F+1)$-reachable. This completes the proof.

■

Figure 4 illustrates an example of such a graph for $F = 3$ and $N_c = 7$. Next, we show that all except two nodes in the graph considered in Lemma 3.1 are non-convergent, thereby showing that $\overline{\alpha_F}(\mathbb{G}(N, F+1, 1)) \geq N-2$.

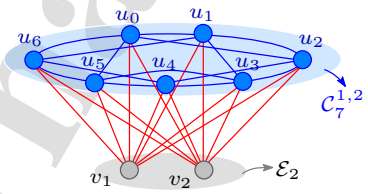


Figure 4: $\mathcal{G} = \mathcal{E}_2 \oplus C_7^{1,2}$ is (4, 1)-robust.

Theorem 3.2. *For given integers $F \geq 2$ and $N \geq 2F+3$, let $\mathbb{G}(N, F+1, 1)$ be a family of all $(F+1,1)$-robust graphs with N nodes, then*

$$\overline{\alpha_F}(\mathbb{G}(N, F+1, 1)) \geq N-2.$$

Proof. We prove the statement by showing that there exists a graph in $\mathbb{G}(N, F+1, 1)$ that has $N-2$ non-convergent nodes. For this, let $N_c = N-2$, and consider the graph $\mathcal{G} = \mathcal{E}_2 \oplus C_{N_c}^{1,\cdots,F-1}$, which is $(F+1,1)$-robust by Lemma 3.1. Let $U = \{u_0 \cdots, u_{N_c-1}\}$ denote the set of nodes in $C_{N_c}^{1,\cdots,F-1}$ and $V = \{v_1, v_2\}$ denote the two nodes in $\mathcal{E}_2$. Note that

$|U| + |V| = N$. We will show that each $u_i \in U$ is a non-convergent node under the F-total attack model. First, we show that $\mathcal{G}$ is not $(F+1, F+1)$-robust.

Consider two disjoint subsets S_1 and S_2, where $S_1 = \{u_0, \cdots, u_{F-1}\} \cup \{v_1\}$, and $S_2 = (U \setminus S_1) \cup \{v_2\}$. Note that each $u_j \in U$ has $2(F-1)$ neighbors in U. Also, each $u_i \in S_1 \cap U$ has at most $F-1$ neighbors in $U \setminus S_1$ and only one neighbor in $V \setminus S_1$. Thus, each node in $S_1 \cap U$ has at most F neighbors outside of S_1. Since v_1 is adjacent to all nodes in $U \setminus S_1$ and $|U \setminus S_1| \geq F+1$, we have $\mathcal{X}_{S_1}^{F+1} = \{v_1\}$. Similarly, each $u_j \in S_2 \cap U$ has at most F neighbors outside of S_2. Also, v_2 has at most F neighbors outside of S_2 (as $|S_1| = F+1$ and v_2 is not adjacent to $v_1 \in S_1$). Thus, $\mathcal{X}_{S_2}^{F+1} = \emptyset$, which means $|\mathcal{X}_{S_1}^{F+1} \cup \mathcal{X}_{S_2}^{F+1}| = 1 < F+1$, and $\mathcal{G}$ is not $(F+1, F+1)$-robust.

Next, we proceed to show that the number of non-convergent nodes in $\mathcal{G}$ is $N-2$, i.e., $\alpha_F(\mathcal{G}) = N-2$. For this, assign some value $a \in \mathbb{R}$ to all the nodes in S_1, and some value $b > a$ to all the nodes in S_2. Let $v_1 \in S_1$, which is the only node having $F+1$ neighbors outside of S_1, be the malicious node, and all the remaining nodes in S_1 and S_2 are normal. Then, each normal node has at most F neighbors outside of its respective subset (i.e., S_1 and S_2). It means each normal node in S_1 has at most F neighbors with values strictly greater than the node's value. Similarly, each normal node in S_2 has at most F neighbors with values strictly smaller than the node's value. By implementing the WMSR algorithm, each normal node in $S_1 \cup S_2$ removes values from all of its neighbors that are outside of its respective subset, and hence, never updates its value. This means normal nodes in S_1 and S_2 maintain the values a and b, respectively, and do not converge at a common value.

In particular, consider $u_0 \in S_1$, and observe that it does not converge to any of the nodes in $S_2 = \{u_F, \cdots, u_{N_c-1}, v_2\}$. Now, we select again two disjoint nonempty subsets, S_1' and S_2', as following:

Let $S_1' = \{u_0, u_{N_c-F+1}, \cdots, u_{N_c-1}\} \cup \{v_2\}$ (i.e., in S_1', include the nodes in U that are on the 'left' of u_0 compared to the previous case of S_1, where nodes to the 'right' of u_0 were included). Note that $|S_1'| = F+1$. Moreover, let $S_2' = (U \setminus S_1') \cup \{v_1\}$, and assume $v_2 \in S_1'$ to be the malicious node. Then, by the same argument used above (i.e., in the case of S_1 and S_2), we can ensure that u_0 does not converge to any of the nodes in S_2'. Since $S_2 \cup S_2' = (U \cup V) \setminus \{u_0\}$, we ensure that for every node pair (u_0, x), where $x \in (U \cup V) \setminus \{u_0\}$, there is an attack of at most F nodes such that u_0 and x do not converge. It means that u_0 is a non-convergent node. By the symmetry of the graph and applying the same arguments as above to other nodes in U implies that all the nodes in U, where $|U| = N-2$, are non-convergent, which means $\alpha_F(\mathcal{G}) = N-2$. This directly implies that $\overline{\alpha_F}(\mathbb{G}(N, F+1, 1)) \geq N-2$, which completes the proof. ∎

Thus, in the family $\mathbb{G}(N, F+1, 1)$, there exist $(F+1, 1)$-robust graphs with a total of N nodes, where, as $N \to \infty$, the ratio of non-convergent nodes to N approaches 1. Conversely, there are also maximally $(F+1, 1)$-robust graphs that do not have any non-convergent nodes. This highlights a significant disparity in the number of non-convergent nodes among $(F+1, 1)$-robust graphs. Therefore, while $(F+1, 1)$-robustness is a useful measure of a graph's resilience, it does not fully capture the extent of non-resilience, as quantified by the number of non-convergent nodes.

3.2. (F, F)-robust Graphs

Next, we consider (F, F)-robust graphs, which ensure resilience to $F-1$ malicious nodes. Our objective is to examine the maximum number of non-convergent nodes in a graph when it faces an additional malicious node beyond its resilience threshold. In particular, we investigate the scenario where the graph is subjected to F malicious nodes, surpassing its initial resilience threshold of $F-1$. Our goal is to construct (F, F)-robust graphs with the maximum number of non-convergent nodes, enabling us to explore $\overline{\alpha_F}(\mathbb{G}(N, F, F))$. Before presenting the graph construction, we state the following observation related to circulant graphs.

Observation 3.3. *Consider a circulant graph $C_{N_c}^{1,2,\cdots,\lceil \frac{F}{2} \rceil - 2}$, where $F \geq 5$ and $N_c \geq F+1$. Let i be some positive integer, where $3 \leq i \leq \frac{F+2}{2}$. If S is a subset of nodes in the circulant graph, where $F - i \leq |S| \leq N_c - (1+i)$, then, at least one of the following is true.*

(i) The number of nodes in S that are adjacent to at least $(i-2)$ nodes outside of S is at least $F+2-2i$, i.e., $|\mathcal{X}_S^{i-2}| \geq F+2-2i$.

(ii) All nodes in S are adjacent to at least $i-2$ nodes outside of S, i.e., $|\mathcal{X}_S^{i-2}| = |S|$.

Figure 5 illustrates the observation through examples. Consider a circulant graph $C_{10}^{1,2}$ with $F = 8$ and $N_c = 10$. For $i = 4$, Figure 5(a) shows a set S of size 4. There are two $(F + 2 - 2i = 2)$ nodes in S, shown in red, such that each of them has two $(i - 2 = 2)$ neighbors outside of S. Similarly, in Figure 5(b), we consider $i = 3$ and a set of nodes S of size 5. By Observation 3.3, there exist four $(F + 2 - 2i = 4)$ nodes in S (red colored), each of which has at least $i - 2 = 1$ neighbor outside of S.

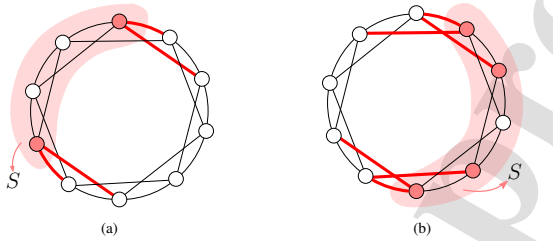


Figure 5: (a) A set S of four nodes contains two nodes (red), each of which has two neighbors outside of S. (b) A set S contains five nodes, of which four nodes (red) have at least one neighbor outside of S.

Next, we present our construction of (F, F)-robust graphs.

Lemma 3.4. *For integers $F > 4$ and $N \geq 2F + 3$, the graph $\mathcal{G} = \mathcal{K}_{F+2} \oplus C_{N-(F+2)}^{1,\cdots,\lceil \frac{F}{2} \rceil - 2}$, which is the join of complete graph $\mathcal{K}_{F+2}$ and circulant graph $C_{N-(F+2)}^{1,\cdots,\lceil \frac{F}{2} \rceil - 2}$, is (F, F)-robust.*

Proof. Let U and V denote the set of nodes in $C_{N-(F+2)}^{1,\cdots,\lceil \frac{F}{2} \rceil - 2}$ and $\mathcal{K}_{F+2}$, respectively. Let S_1 and S_2 be two disjoint non-empty sets of nodes in the given $\mathcal{G}$. There are three cases:

(a) One of the subsets contains nodes from V only. W.l.o.g, assume $S_1 \subseteq V$. Since $|U| \geq F + 1$ and each $v \in S_1$ is adjacent to all nodes in U, we get $\mathcal{X}_{S_1}^F = S_1$.

(b) One of the subsets contains nodes from U only. W.l.o.g, assume $S_1 \subseteq U$: Since $|V| \geq F + 2$ and each $u \in S_1$ is adjacent to all nodes in V, we get $\mathcal{X}_{S_1}^F = S_1$.

(c) Both S_1 and S_2 contain nodes from U and V. We have further two cases.

(c-1) One of the subsets, say S_1 has at most $(F-1)$ nodes: In this case, consider $|S_1 \cap V| = \nu_1$, then $|S_1 \cap U| \leq F-1-\nu_1$. Let $v \in S_1 \cap V$. The number of neighbors of v outside of S_1 are:

$$\begin{aligned} &= ((F + 2) - \nu_1) \ + \ (|U| - |S_1 \cap U|) \\ &\geq (F + 2 - \nu_1) \ + \ ((F + 1) - (F - 1 - \nu_1)) \\ &= F + 4. \end{aligned}$$

Similarly, let $u \in S_1 \cap U$. Note that u has $2\left(\lceil \frac{F}{2} \rceil - 2\right)$ neighbors in U. Then, the number of neighbors of u outside of S_1 are:

$$\begin{aligned} &\geq ((F + 2) - \nu_1) \ + \ (2\,(\lceil F/2 \rceil - 2) - ((S_1 \cap U) - 1)) \\ &\geq (F + 2 - \nu_1) \ + (F - 4 - (F - 1 - \nu_1 - 1)) \\ &= F. \end{aligned}$$

Thus, each node in S_1 has at least F neighbors outside of S_1, i.e., $\mathcal{X}_{S_1}^F = S_1$.

(c-2) Both subsets S_1 and S_2 have at least F nodes:

In this case, if at least one of the subsets, say S_1, has at most two nodes from V. Then, since $|V \setminus S_1| \geq F$ and each node in S_1 is adjacent to all nodes in V, we have $\mathcal{X}^F_{S_1} = S_1$. So, we consider that both S_1 and S_2 contain at least three nodes from V. We will next compute $|\mathcal{X}^F_{S_1}|$ and $|\mathcal{X}^F_{S_2}|$, and show that $|\mathcal{X}^F_{S_1}| + |\mathcal{X}^F_{S_2}| \geq F$.

For this, let $|S_1 \cap V| = \nu_1$ and $|S_2 \cap V| = \nu_2$.

Since each node in $S_1 \cap V$ (resp. $S_2 \cap V$) is adjacent to all the nodes in S_2 (resp. S_1), where $|S_2| \geq F$, we have $|\mathcal{X}^F_{S_1}| \geq \nu_1$. Similarly, $|\mathcal{X}^F_{S_2}| \geq \nu_2$. So, if $\nu_1 + \nu_2 \geq F$, we have $|\mathcal{X}^F_{S_1}| + |\mathcal{X}^F_{S_2}| \geq F$, and we are done. Thus, we assume,

$$\nu_1 + \nu_2 \leq F - 1. \tag{6}$$

Also, note that since $|V| = F + 2$, one of the subsets, say S_1, must contain at most $\frac{F+2}{2}$ nodes from V, i.e., $|S_1 \cap V| \leq \frac{F+2}{2}$. So, we get

$$3 \leq \nu_1 \leq \frac{F+2}{2}. \tag{7}$$

Using the above details and (6), we also get

$$3 \leq \nu_2 \leq F - 1 - \nu_1. \tag{8}$$

Next, we consider $|S_1 \cap U| = \mu_1$, and $|S_2 \cap U| = \mu_2$.

Observe that $F - \nu_1 \leq \mu_1$ (as $|S_1| \geq F$). Similarly, $F - \nu_2 \leq \mu_2$. Consequently, we get an upper bound on μ_1, i.e., $\mu_1 \leq |U| - (F - \nu_2)$. Using (6),

$$|U| - (F - \nu_2) \leq |U| - (1 + \nu_1),$$

thus, $\mu_1 \leq |U| - (1 + \nu_1)$. We write the upper and lower bounds on μ_1 again,

$$F - \nu_1 \leq \mu_1 \leq |U| - (1 + \nu_1). \tag{9}$$

Similarly, the bounds on μ_2 are,

$$F - \nu_2 \leq \mu_2 \leq |U| - (F - \nu_1). \tag{10}$$

Next, we compute $\mathcal{X}^F_{S_1}$ and $\mathcal{X}^F_{S_2}$.

Since $(S_1 \cap V) \subseteq \mathcal{X}^F_{S_1}$, we have $|\mathcal{X}^F_{S_1}| \geq |\mathcal{X}^F_{S_1} \cap V| = \nu_1$. Note that each $u \in (S_1 \cap U)$ is adjacent to at least $(F+2) - \nu_1$ nodes in $V \setminus (S_1 \cap V)$. So, if $u \in (S_1 \cap U)$ is adjacent to at least $\nu_1 - 2$ nodes in $U \setminus S_1$, then $u \in \mathcal{X}^F_{S_1}$ (as u will have at least F neighbors outside of S_1). Now consider (7), (9), and use Observation 3.3 (plugging $i = \nu_1$), we deduce that the number of nodes in $S_1 \cap U$, each of which is adjacent to at least $\nu_1 - 2$ nodes in $U \setminus S_1$ is at least $F - 2(\nu_1 - 1)$. This gives

$$\begin{aligned} |\mathcal{X}^F_{S_1}| &= |\mathcal{X}^F_{S_1} \cap V| + |\mathcal{X}^F_{S_1} \cap U| \\ &\geq \nu_1 + (F - 2(\nu_1 - 1)) \\ &= F + 2 - \nu_1. \end{aligned} \tag{11}$$

Similarly, considering (8), (10), and applying a similar argument as for $\mathcal{X}^F_{S_1}$, we obtain

$$|\mathcal{X}^F_{S_2}| = |\mathcal{X}^F_{S_2} \cap V| + |\mathcal{X}^F_{S_2} \cap U| \geq F + 2 - \nu_2. \tag{12}$$

Now, from (11) and (12), we get

$$\begin{aligned} |\mathcal{X}^F_{S_1}| + |\mathcal{X}^F_{S_2}| &\geq (F + 2 - \nu_1) + (F + 2 - \nu_2) \\ &= 2F + 4 - (\nu_1 + \nu_2) \end{aligned} \tag{13}$$

Using (6),

$$|\mathcal{X}^F_{S_1}| + |\mathcal{X}^F_{S_2}| \geq 2F + 4 - (F-1) = F + 3, \tag{14}$$

which is the desired result. This completes the proof. ∎

Figure 6 illustrates $\mathcal{G} = \mathcal{K}_{F+2} \oplus C^{1,\cdots,\lceil \frac{F}{2} \rceil - 2}_{N-(F+2)}$ for $F = 5$ and $N = 14$.

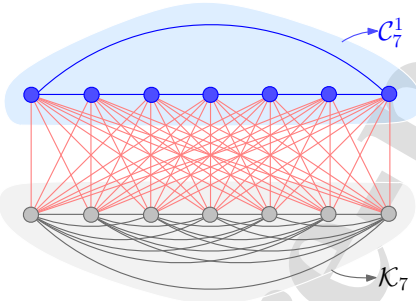


Figure 6: $\mathcal{G} = \mathcal{K}_7 \oplus C^1_7$ is (F, F)-robust graph for $F = 5$.

The following result presents the number of non-convergent nodes in (F, F)-robust graphs constructed above.

Theorem 3.5. *For given integers $F > 4$ and $N \geq 2F + 3$, let $\mathbb{G}(N, F, F)$ be a family of all (F, F)-robust graphs with N nodes, then*

$$\overline{\alpha_F}(\mathbb{G}(N, F+1, 1)) \geq N - (F+2).$$

Proof. We will construct a graph $\mathcal{G} \in \mathbb{G}(N, F, F)$ with $\alpha_F(\mathcal{G}) = N - (F+2)$, thus showing $\overline{\alpha_F}(\mathbb{G}(N, F+1, 1)) \geq N - (F+2)$. For this, consider $\mathcal{G} = \mathcal{K}_{F+2} \oplus C^{1,\cdots,\lceil \frac{F}{2} \rceil - 2}_{N-(F+2)}$, which is (F, F)-robust by Lemma 3.4. Let $V = \{v_1, \cdots, v_{F+2}\}$ denote the set of nodes in $\mathcal{K}_{F+2}$, and $U = \{u_1, \cdots, u_{N-(F+2)}\}$ be the set of nodes in $C^{1,2,\cdots,\lceil \frac{F}{2} \rceil - 2}_{N-(F+2)}$. Note that each $u_i \in U$ has $2(\lceil \frac{F}{2} \rceil - 2)$ neighbors in U.

For the non-convergent nodes, first, we show that the graph is not $(F+1, F+1)$-robust. Let S_1 be a set consisting of a single node from U, say $u \in U$, and $F-1$ nodes from V. Also, let S_2 be the set of remaining nodes, i.e., $S_2 = (U \cup V) \setminus S_1$. Note that $|S_1| = F$, so $\mathcal{X}^{F+1}_{S_2} = \emptyset$. Also, $u \in S_1$ has $3 + 2(\lceil \frac{F}{2} \rceil - 2) = 2\lceil \frac{F}{2} \rceil - 1 \leq F$ neighbors outside of S_1. At the same time, each $v \in (S_1 \cap V)$ has at least $F+1$ neighbors outside of S_1. Thus, $\mathcal{X}^{F+1}_{S_1} = S_1 \setminus \{u\}$, and $|\mathcal{X}^{F+1}_{S_1}| = F - 1 < |S_1|$. As a result, none of the three conditions for $(F+1, F+1)$-robustness are satisfied by sets S_1 and S_2, the considered graph is not $(F+1, F+1)$-robust.

Now, assume that the set of malicious nodes contains $\mathcal{X}^{F+1}_{S_1} \cup \mathcal{X}^{F+1}_{S_2}$. Note that $|\mathcal{X}^{F+1}_{S_1} \cup \mathcal{X}^{F+1}_{S_2}| \leq F$. Also, $u \in S_1$ is the only normal node in S_1 as $u \notin \mathcal{X}^{F+1}_{S_1}$. Now, assign value a to all nodes in S_1, and value $b > a$ to nodes in S_2. Note that all normal nodes in S_1 and S_2 have at most F neighbors outside of their respective sets, and as per the WMSR algorithm, each normal node in S_1 and S_2 removes F values outside of its respective set. Thus, $u \in S_1$, and other normal nodes in S_2 never update their values. Thus, u never converges to another normal node and is a non-convergent node. This scenario can be replicated for every node in U while applying the same arguments; thus, the number of non-convergent nodes in the graph is $|U| = N - (F+2)$, i.e. $\alpha_F(\mathcal{G}) = N - (F+2)$. This directly implies that $\overline{\alpha_F}(\mathbb{G}(N, F, F)) \geq N - (F+2)$, which completes the proof. ∎

For the graph $\mathcal{G} = \mathcal{K}_7 \oplus C^1_7$ in Figure 6, the (blue) nodes corresponding to the circulant graph, C^1_7, are the non-convergent nodes under the F-total model for $F = 5$.

3.3. (F+1,F)-robust Graphs

In this sub-section, we consider $\mathbb{G}(N, F+1, F)$ and examine $(F+1, F)$-robust graphs, which are slightly less robust than the desired $(F+1, F+1)$-robust graphs. As before, the goal is to design graphs with the maximum number of non-convergent nodes and obtain $\overline{\alpha_F}(\mathbb{G}(N, F+1, F))$. For this we state the following result.

Lemma 3.6. *For given integers $F \geq 3$ and $N \geq 3F$, the graph $\mathcal{G} = \mathcal{E}_{N-2F} \oplus C_{2F}^{1,\cdots,F-1}$ is $(F+1, F)$-robust.*

Proof. First, we will show the result for $N = 3F$, and then extend the result to $N > 3F$.

Assume $N = 3F$. Let U and V denote the set of nodes in $C_{2F}^{1,\cdots,F-1}$ and $\mathcal{E}_F$, respectively. Let S_1 and S_2 be two disjoint non-empty sets of nodes in the given $\mathcal{G}$. There are following cases for the choices of S_1 and S_2.

(a) At least one of S_1 and S_2 contains nodes from V only: W.l.o.g., let $S_1 \cap U = \emptyset$ (i.e., $S_1 \subseteq V$). Then, each node in S_1 has $2F$ neighbors outside of S_1, and $\mathcal{X}_{S_1}^{F+1} = S_1$.

(b) Both S_1 and S_2 contain nodes from U:

In this case, $S_1 \cap U \neq \emptyset$ and $S_2 \cap U \neq \emptyset$. Let

$$|S_1 \cap U| = \nu.$$

Since each node in U has a degree $2F-2$, each $u \in (S_1 \cap U)$ has $(2F-2) - (\nu - 1) = 2F - 1 - \nu$ neighbors in $U \setminus S_1$. Based on ν, we have the following sub-cases.

(b-1) $\nu \leq F-2$: In this case, for each $u \in S_1 \cap U$, the number of neighbors in $U \setminus S_1$ is:

$$2F - 1 - \nu \geq 2F - 1 - (F-2) = F + 1,$$

which means $\mathcal{X}_{S_1}^{F+1} \cap U = S_1 \cap U$. Similarly, since each $v \in S_1 \cap V$ is adjacent to all nodes in U, and $|U \setminus S_1| \geq F+1$, we have $\mathcal{X}_{S_1}^{F+1} \cap V = S_1 \cap V$. Thus, $\mathcal{X}_{S_1}^{F+1} = (S_1 \cap V) \cup (S_1 \cap U) = S_1$.

(b-2) $\nu \geq F+2$: This implies that $|S_2 \cap U| \leq F-2$. As a result, we apply the sub-case (b-1) on S_2 and get $\mathcal{X}_{S_2}^{F+1} = S_2$.

(b-3) $\nu = F-1$: In this case, note that $|U \setminus S_1| = F+1$. We have two scenarios: First, if $S_1 \cap V = V$ (i.e., S_1 contains all nodes in V), then each $v \in (S_1 \cap V)$ is adjacent to $F+1$ nodes in $U \setminus S_1$. Thus, $(S_1 \cap V) \subseteq \mathcal{X}_{S_1}^{F+1}$. Since $|S_1 \cap V| = |V| = F$, we have $\mathcal{X}_{S_1}^{F+1} \geq F$. Second, if $(S_1 \cap V) \neq V$, then there is at least one node in $V \setminus S_1$. This means that each $u \in S_1 \cap U$ is adjacent to at least one node in $V \setminus S_1$. Also, note that each $u \in (S_1 \cap U)$ has $2F - 1 - (F-1) = F$ neighbors in $U \setminus S_1$. Thus, each $u \in (S_1 \cap U)$ hast at least $F+1$ neighbors outside S_1, implying $(S_1 \cap U) \subseteq \mathcal{X}_{S_1}^{F+1}$. Moreover, each $v \in (S_1 \cap V)$ is adjacent to all nodes $U \setminus S_1$ (where $|U \setminus S_1| = F+1$), thus $(S_1 \cap V) \subseteq \mathcal{X}_{S_1}^{F+1}$. As a result, we get $\mathcal{X}_{S_1}^{F+1} = S_1$.

(b-4) $\nu = F$: Since $|U| = 2F$, we have $|S_2 \cap U| \leq F$. If $|S_2 \cap U| \leq F-1$, we apply the argument in sub-case (b-3) above on S_2. So, consider $|S_2 \cap U| = F$. Now, since $|V| = F$, at least one of the following is true: (i) $|V \setminus S_1| \geq \lceil \frac{F}{2} \rceil$, (ii) $|V \setminus S_2| \geq \lceil \frac{F}{2} \rceil$. W.l.o.g., we assume (i) is true. It means that each $u \in (S_1 \cap U)$ has at least $\lceil \frac{F}{2} \rceil$ neighbors in $V \setminus S_1$. Also, each $u \in (S_1 \cap U)$ has $2F - 1 - F = F - 1$ neighbors in $U \setminus S_1$. Noting that $F \geq 3$, we deduce that each $u \in (S_1 \cap U)$ has at least $F+1$ neighbors outside S_1. Since $|S_1 \cap U| = F$, we have $|\mathcal{X}_{S_1}^{F+1}| \geq F$.

(b-5) $\nu = F+1$: In this case $|S_2 \cap U| \leq F-1$, thus, we apply the sub-case (b-3) on S_2.

All the above cases establish that the graph $\mathcal{E}_F \oplus C_{2F}^{1,\cdots,F-1}$ is $(F+1, F)$-robust. Now, we add a new node v to $\mathcal{E}_F \oplus C_{2F}^{1,\cdots,F-1}$ such that v is adjacent to all nodes in U (i.e., nodes in the circulant graph). This gives the graph $\mathcal{E}_{F+1} \oplus C_{2F}^{1,\cdots,F-1}$. Since the new node v is adjacent to $2F$ nodes in the existing graph, the $(F+1, F)$-robustness of $\mathcal{E}_F \oplus C_{2F}^{1,\cdots,F-1}$ implies that the new graph $\mathcal{E}_{F+1} \oplus C_{2F}^{1,\cdots,F-1}$ is also $(F+1, F)$-robust (by [4, Theorem 5]). By the same argument, we add $N - 3F$ vertices to $\mathcal{E}_F \oplus C_{2F}^{1,\cdots,F-1}$ to get $\mathcal{G} = \mathcal{E}_{N-2F} \oplus C_{2F}^{1,\cdots,F-1}$, which is $(F+1, F)$-robust. ∎

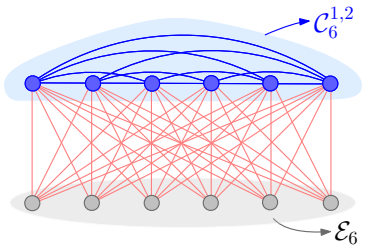


Figure 7: $\mathcal{G} = \mathcal{E}_6 \oplus \mathcal{C}_6^{1,2}$ is $(F+1, F)$-robust graph for $F = 3$.

Figure 7 illustrates $\mathcal{G} = \mathcal{E}_{N-2F} \oplus \mathcal{C}_{2F}^{1,\cdots,F-1}$ for $F = 3$ and $N = 12$. Next, we compute the number of non-convergent nodes in the graphs in Lemma 3.6, thereby obtaining a lower bound on $\overline{\alpha_F}(\mathbb{G}(N, F+1, F))$.

Theorem 3.7. *For given integers $F \geq 3$ and $N \geq 2F+3$, let $\mathbb{G}(N, F+1, F)$ be a family of all $(F+1, F)$-robust graphs with N nodes, then*

$$\overline{\alpha_F}(\mathbb{G}(N, F+1, F)) \geq N - 2F.$$

Proof. We show that there exists $\mathcal{G} \in \mathbb{G}(N, F+1, F)$ with $N - 2F$ non-convergent nodes. For this, consider $\mathcal{G} = \mathcal{E}_{N-2F} \oplus \mathcal{C}_{2F}^{1,\cdots,F-1}$, which is $(F+1, F)$-robust by Lemma 3.6. Let $V = \{v_1, \cdots, v_{F+2}\}$ be the set of nodes in $\mathcal{E}_{N-2F}$, and $U = \{u_1, \cdots, u_{2F}\}$ be the set of nodes in $\mathcal{C}_{2F}^{1,2,\cdots,F-1}$. We will show that each $v_i \in V$ is a non-convergent node.

For this, first, we show that $\mathcal{G}$ is not $(F+1, F+1)$-robust. Consider two nonempty disjoint subset of nodes in $\mathcal{G}$. Let $S_1 = \{v_1\} \cup \{u_1, u_2, \cdots, u_F\}$, and S_2 be the set of remaining nodes, i.e., $S_2 = (V \cup U) \setminus S_1$. We now compute $\mathcal{X}_{S_1}^{F+1}$ and $\mathcal{X}_{S_2}^{F+1}$. Note that each $u_i \in S_1$ is adjacent to at least $2(F-1) - (F-1) = F-1$ nodes in $U \setminus S_1$. Also, each $u_i \in S_1$ is adjacent to $(N-2F) - 1 \geq F-1$ nodes in $V \setminus S_1$. Thus, $u_i \in S_1$ is adjacent to at least $2(F-1)$ nodes outside S_1. Since $F \geq 3$, we have $2(F-1) \geq F+1$, and $(S_1 \cap U) \subseteq \mathcal{X}_{S_1}^{F+1}$. Moreover, $v_1 \in (S_1 \cap V)$ is adjacent to exactly F nodes outside of S_1. Thus, $\mathcal{X}_{S_1}^{F+1} = S_1 \cap U$, i.e., $|\mathcal{X}_{S_1}^{F+1}| = F$. As for S_2, each $v_i \in (S_2 \cap V)$ is adjacent to only F nodes outside S_2 (which are the nodes in $S_1 \cap U$). Further, each $u_j \in (S_2 \cap U)$ is adjacent to $2(F-1)$ nodes in U, of which $F-1$ nodes are in $S_2 \cap U$. Thus, each $u_j \in (S_2 \cap U)$ is adjacent to $F-1$ nodes in $U \setminus S_2$. Also, each such u_j is adjacent to one node in $V \setminus S_2$. Thus, each $u_j \in (S_2 \cap U)$ is adjacent to $(F-1)+1 = F$ nodes outside S_2, which means $\mathcal{X}_{S_2}^{F+1} = \emptyset$. In other words, $|\mathcal{X}_{S_1}^{F+1}| + |\mathcal{X}_{S_2}^{F+1}| = F$, and $\mathcal{G}$ is not $(F+1, F+1)$-robust.

Now, assign some real value $a \in \mathbb{R}$ to all nodes in S_1, and some value $b > a$ to nodes in S_2. Moreover, assume that nodes in $\mathcal{X}_{S_1}^{F+1} = S_1 \cap U$ are malicious. Since $|S_1 \cap U| = F$, the number of malicious nodes is F. Note that all normal nodes in S_1 and S_2 have at most F neighbors outside of their respective sets. Thus, following the WMSR algorithm, each normal node in S_1 and S_2 removes F values outside of its respective set, and hence never updates its value. In particular, $v_1 \in S_1$ does not converge to any normal node in $S_2 = (V \setminus \{v_1\}) \cup (U \setminus \{u_1, \cdots, u_F\})$. Now, by selecting $S_1 = \{v_1\} \cup \{u_{F+1}, \cdots, u_{2F}\}$, and $S_2 = (V \cup U) \setminus S_1$, we can ensure, by the same arguments as above, that there is an attack of F nodes (i.e., $\{u_{F+1}, \cdots, u_{2F}\}$) preventing v_1 to converge to any of the (normal) nodes in $\{u_1, \cdots, u_F\}$. As a result, for each node $x \in (V \cup U) \setminus \{v_1\}$, there is an attack of F nodes guaranteeing that v_1 and x do not converge, implying that v_1 is a non-convergent node. Finally, noting the symmetry of nodes in $\mathcal{G}$, we can replicate the same arguments as above to show that each $v_i \in V$ is non-convergent. Since $|V| = N - 2F$, we get the desired result, i.e., $\alpha_F(\mathcal{G}) = N - 2F$. This directly implies that $\overline{\alpha}_F(\mathbb{G}(N, F+1, F)) \geq N - 2F$. ∎

These results demonstrate that even among graphs with the same robustness, there can be significant variation in the number of non-convergent nodes. Consequently, in scenarios where robustness is insufficient, these graphs may exhibit varying levels of partial performance. Next, based on the previous discussions, we state a sufficient condition for a node to be a non-convergent node. In proofs of Theorems 3.2, 3.5, and 3.7, the main idea to design an F-total attack that prevents a normal node u from converging with another normal node v is as follows: First, we identify two disjoint empty sets of nodes, S_1 and S_2, wherein u and v belong to different sets. Moreover, S_1 and S_2 do not satisfy any of the three conditions in Definition 2.3. We then construct an attack involving a maximum of F malicious nodes

to ensure that the nodes in S_1 and S_2 do not converge. By leveraging this strategy, we can effectively state a *sufficient condition* for a node to be *non-convergent*.

Proposition 3.8. *In a graph $G = (V, E)$, a node $u \in V$ is non-convergent (under the F-total malicious model) if for every $v \in V \setminus \{u\}$, there exist a pair of non-empty disjoint subsets $S_1, S_2 \subset V$ such that*

1. *$|\mathcal{X}_{S_1}^{F+1}| < |S_1|$, and $|\mathcal{X}_{S_2}^{F+1}| < |S_2|$, and $|\mathcal{X}_{S_1}^{F+1}| + |\mathcal{X}_{S_2}^{F+1}| < F + 1$, (i.e., S_1 and S_2 do not satisfy the $(F + 1, F + 1)$-robustness criteria in Definition 2.3.)*
2. *u and v belong to distinct subsets, i.e., if $u \in S_1$, then $v \in S_2$ and vice versa.*
3. *Neither of u and v have $F + 1$ neighbors outside of their respective subsets.* ■

We demonstrate the above proposition through an example.

Example: Consider the graph in Figure 8, which is $(3, 3)$-robust. Under the F-total malicious model, where $F = 3$, nodes in $\{v_2, v_3, v_6, v_7\}$ are non-convergent as they satisfy the conditions in Proposition 3.8. We explain the non-convergence of v_6. Consider a pair of subsets, $S_1 = \{v_4, v_5, v_6\}$ and $S_2 = \{v_1, v_2, v_3, v_7, v_8\}$ in Figure 8(a). These subsets meet the first condition in Proposition 3.8. Notably, node $v_5 \in S_1$ is the only node with four $(F + 1 = 4)$ neighbors outside its subset S_1. Consequently, there exists an attack (involving v_5) that prevents v_6 from converging to any of the nodes in S_2. For the non-convergence of v_6, we further need to show that there is also an attack that prevents convergence of v_6 with nodes $v_4, v_5 \in S_1$. For this, consider subsets S_1 and S_2 in Figure 8(b), where $S_1 = \{v_1, v_6, v_7, v_8\}$ and $S_2 = \{v_2, v_3, v_4, v_5\}$. Note that v_6 is in a different subset than v_4 and v_5, and none of these nodes have four neighbors outside their respective sets, satisfying the conditions in the proposition. As a result, we can guarantee that node v_6 does not converge to v_4 and v_5, confirming its non-convergence.

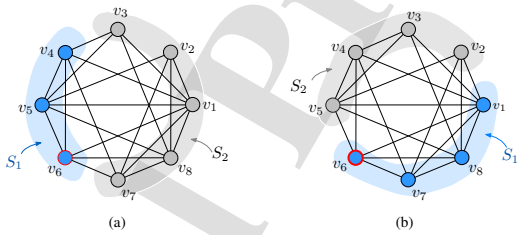


Figure 8: G is $(3, 3)$-robust and v_6 is non-convergent for $F = 3$.

Remark 3.9. *We note that the concept of non-convergence for a node is defined in relation to the attack model. Specifically, a node u is considered non-convergent if, for every other node v in the graph, an 'attack' can be constructed that prevents nodes u and v from 'converging at a common point'. In this paper, as highlighted in Remark 2.2, we have focused on the F-*total malicious *attack model, where non-convergence is defined under this specific scenario. However, this notion of an 'attack' can be adapted to other models, leading to corresponding modifications in the definition of non-convergence. Similarly, since distributed consensus is the optimization task considered in this work, non-convergent nodes are defined in terms of* convergence at a common point*. This definition can be adjusted to suit other optimization tasks by replacing 'converging at a common point' with the specific goal of the task.*

4. Illustrations and Simulations

In this section, we have two main goals: (1) to illustrate the notion of a non-convergent node. (2) To demonstrate how the number of non-convergent nodes in a graph changes as we alter the graph's robustness.

For an illustration of a non-convergent node, consider $G = (V, E)$ in Figure 9, which is $(4, 3)$-robust (but not $(4, 4)$-robust). Assuming $F = 3$ and F-total malicious attack, G has four non-convergent nodes, $\{v_7, v_8, v_9, v_{10}\}$. For instance, considering v_7, we show that for every other $v_i \in V$, there is an attack consisting of $F = 3$ malicious nodes ensuring that v_7 and v_i do not converge. In Figure 9(a), we design an attack involving v_1, v_2 and v_3. Their state trajectories are

shown in red in Figure 9(c). The state of v_7 is in green, and the states of the remaining nodes are in blue. As a result of this attack, none of the nodes in $\{v_4, v_5, v_6, v_8, v_9, v_{10}\}$ and v_7 converge at the same state. Next, we need to show that there is an attack that can prevent v_7 from converging to any of the nodes in $\{v_1, v_2, v_3\}$. Figure 9(d) demonstrates such a situation. Hence, for every node pair (v_7, v_i), we have an attack guaranteeing that v_i and v_7 do not converge, establishing that v_7 is a non-convergent node.

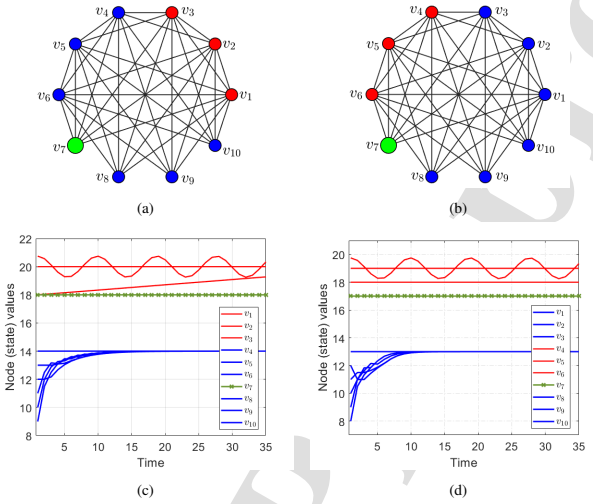


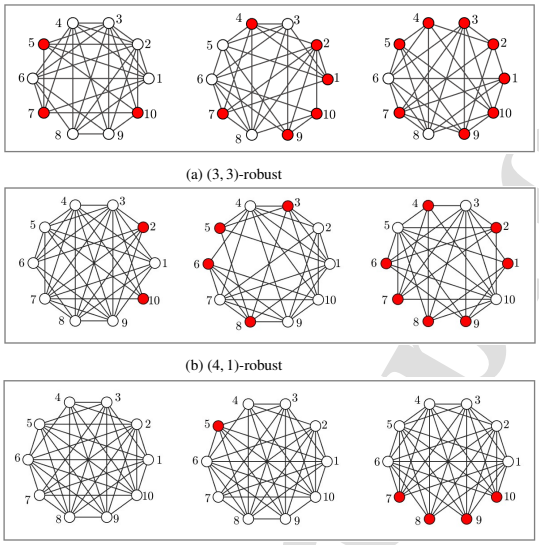
Figure 9: v_7 (green) is a non-convergent node. For every node $v_i \neq v_7$, there is an attack consisting of $F = 3$ nodes (as in (c) and (d)) preventing v_7 and v_i from converging to a common point.

Figure 10 presents different graphs, none of which is $(4, 4)$-robust. Consequently, these graphs cannot guarantee resilient consensus when faced with $F = 3$ malicious nodes, rendering them 'non-resilient' to three malicious nodes. Despite this common non-resilience, the impact varies between graphs, which we measure in terms of the number of non-convergent nodes in each graph. For instance, Figure 10(a) shows three $(3, 3)$-robust graphs, each having a different number of non-convergent nodes (red) and hence, a varying level of non-resilience. Similarly, Figures 10(b) and 10(c) present examples of $(4, 1)$- and $(4, 3)$-robust graphs, respectively. Each of these graphs contains a distinct number of non-convergent nodes.

In addition to the specific examples provided, we generated 50 instances each of $(3, 3)$-robust, $(4, 1)$-robust, and $(4, 3)$-robust graphs using the Erdős-Rényi model for $N = 10$ and $N = 14$.[1] For each graph, we calculated the number of non-convergent nodes under the F-total model with $F = 3$. The expected number of non-convergent nodes was then determined by averaging the results across the 50 graph instances with the same N and robustness. Table 1 presents these results as the expected fraction of non-convergent nodes in a graph.

Generally, the parameter r in the (r, s)-robustness takes precedence in determining the relative robustness of graphs [4]. Similarly, for the same value of r, an (r, s_1)-robust graph is relatively more robust than an (r, s_2)-robust graph, where $s_1 > s_2$. We observe (as in Table 1) that graphs with relatively higher robustness generally have fewer non-convergent nodes, given the same value of F. Finally, Figure 11(a) shows a $(2, 2)$-robust graph consisting of $N = 12$ nodes. The $(2, 2)$-robustness of G implies that resilient consensus is guaranteed in the presence of a single malicious node, and hence, none of the nodes in G is non-convergent. However, if we increase F (i.e., the number of malicious nodes), the number of non-convergent nodes also increases, as Figure 11(b) illustrates. This example demonstrates an increasing non-resilience of the graph to the presence of malicious nodes.

[1] Here, the robustness of each graph is maximal. We use maximal to mean the highest level of robustness that the graph can achieve without moving to the next level of robustness. For example, a $(3, 3)$-robust graph considered is not $(4, 1)$-robust. Similarly, the $(4, 1)$-robust graphs considered are maximally robust in that they are not $(4, 2)$-robust.



(a) $(3,3)$-robust

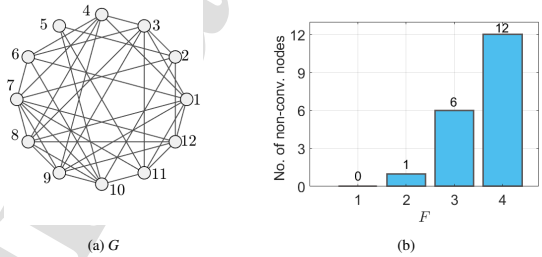
(b) $(4,1)$-robust

(c) $(4,3)$-robust

Figure 10: Non-convergent nodes (colored red) in $(3,3)$-robust, $(4,1)$-robust, and $(4,3)$-robust graphs.

Table 1: The fraction of non-convergent nodes in graphs with various robustness considering $F = 3$ malicious nodes.

	(# of non-convergent nodes)/N		
N	$(3,3)$-robust	$(4,1)$-robust	$(4,3)$-robust
10	0.65	0.38	0.01
14	0.68	0.43	0.07



(a) G (b)

Figure 11: (a) $(2,2)$-robust graph. (b) Number of non-convergent nodes increases with F.

5. Discussion and Conclusion

In traditional designs of resilient algorithms for multiagent systems, the primary focus has been characterizing conditions, such as network graph robustness and connectivity, guaranteeing the network objective despite misbehaving agents. However, in cases where these conditions are not satisfied, assessing the network's partial performance becomes challenging. Our novel concept of non-convergent nodes provides a quantifiable measure of how worse a

network with suboptimal robustness might perform, or in other words, how non-resilient the networks can be. For the WMSR resilient consensus algorithm, we demonstrated that graphs with the same (r, s)-robustness value can exhibit varying degrees of non-resilience, as evidenced by different numbers of non-convergent nodes. By departing from the conventional binary perspective of network resilience–hinging on either success or failure (network objective achieved or not achieved, respectively) in the face of misbehaving agents–our approach offers a more comprehensive view of network resilience. There are several promising directions for future research. One area of focus is characterizing non-convergent nodes and relating them to other graph parameters. For example, our experiments revealed that nodes with the smallest degrees often tend to be non-convergent, which aligns with expectations. However, we also observed instances where higher-degree nodes were non-convergent, even when smaller-degree nodes were not. For example, consider the graph in Figure 12, which is $(2, 2)$-robust but not $(3, 3)$-robust. We identified the non-convergent nodes as v_2, v_5, v_7 (highlighted in red) under the F-total model with $F = 3$. Notably, node v_5 is non-convergent despite having a degree of 6, while nodes v_1 and v_8, each with a degree of 4, are not non-convergent. This suggests a more complex relationship between non-convergent nodes and node degrees that warrants further exploration.

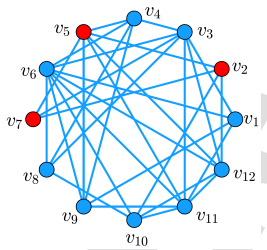


Figure 12: A $(2, 2)$-robust graph with non-convergent nodes (red) under the F-total model with $F = 3$.

Similarly, there are other notions of node resilience, such as bribing resistance [41], and it will be interesting to explore connections between them. Another limitation of the current work lies in the computational challenges of identifying non-convergent nodes. This complexity arises from the inherent connection between non-convergent nodes and (r, s)-robustness, a problem known to be coNP-complete [42]. Efficient methods and analytical tools for the computation of non-convergent nodes are currently lacking, and we aim to address these gaps in future work by leveraging recent advances in computing (r, s)-robustness in graphs (e.g., [43, 44, 45]). Additionally, while our approach was specifically applied to the WMSR algorithm, it has the potential for broader application across other algorithms and problem settings. In conclusion, this work opens avenues for assessing the network performance under sub-optimal robustness conditions, enabling more thorough evaluations and enhancing the design of resilient multiagent systems.

Acknwledgements

The authors wish to acknowledge Amazon Robotics for the support of L. Khalyavin in this research.

References

[1] A. Jadbabaie, J. Lin, and A. S. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Transactions on automatic control*, vol. 48, no. 6, pp. 988–1001, 2003.
[2] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, 2007.
[3] W. Ren, R. W. Beard, and E. M. Atkins, "Information consensus in multivehicle cooperative control," *IEEE Control systems magazine*, vol. 27, no. 2, pp. 71–82, 2007.
[4] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 4, pp. 766–781, 2013.
[5] S. M. Dibaji and H. Ishii, "Consensus of second-order multi-agent systems in the presence of locally bounded faults," *Systems & Control Letters*, vol. 79, pp. 23–29, 2015.

[6] D. M. Senejohnny, S. Sundaram, C. De Persis, and P. Tesi, "Resilience against misbehaving nodes in asynchronous networks," *Automatica*, vol. 104, pp. 26–33, 2019.

[7] J. Usevitch and D. Panagou, "Resilient leader-follower consensus to arbitrary reference values in time-varying graphs," *IEEE Transactions on Automatic Control*, vol. 65, no. 4, pp. 1755–1762, 2020.

[8] Y. Wang, H. Ishii, F. Bonnet, and X. Défago, "Resilient consensus for multi-agent systems under adversarial spreading processes," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 5, pp. 3316–3331, 2022.

[9] H. Ishii, Y. Wang, and S. Feng, "An overview on multi-agent consensus under adversarial attacks," *Annual Reviews in Control*, vol. 53, pp. 252–272, 2022.

[10] J. Yan, X. Li, Y. Mo, and C. Wen, "Resilient multi-dimensional consensus in adversarial environment," *Automatica*, vol. 145, 2022.

[11] G. Ramos, D. Silvestre, and C. Silvestre, "General resilient consensus algorithms," *International Journal of Control*, vol. 95, no. 6, pp. 1482–1496, 2022.

[12] W. Abbas, M. Shabbir, J. Li, and X. Koutsoukos, "Resilient distributed vector consensus using centerpoint," *Automatica*, vol. 136, 2022.

[13] L. Ballotta, G. Como, J. S. Shamma, and L. Schenato, "Can competition outperform collaboration? the role of misbehaving agents," *IEEE Transactions on Automatic Control*, vol. 69, no. 4, pp. 2308–2323, 2024.

[14] J. Li, W. Abbas, and X. Koutsoukos, "Resilient distributed diffusion in networks with adversaries," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 6, pp. 1–17, 2019.

[15] T. Yu, R. C. de Lamare, and Y. Yu, "Robust resilient diffusion over multi-task networks against byzantine attacks: Design, analysis and applications," *IEEE Transactions on Signal Processing*, vol. 70, pp. 2826–2841, 2022.

[16] M. Safi, S. M. Dibaji, and M. Pirani, "Resilient coordinated movement of connected autonomous vehicles," *European Journal of Control*, vol. 64, p. 100613, 2022.

[17] A. Mitra, J. A. Richards, S. Bagchi, and S. Sundaram, "Resilient distributed state estimation with mobile agents: overcoming byzantine adversaries, communication losses, and intermittent measurements," *Autonomous Robots*, vol. 43, pp. 743–768, 2019.

[18] A. Mitra and S. Sundaram, "Byzantine-resilient distributed observers for LTI systems," *Automatica*, vol. 108, p. 108487, 2019.

[19] L. An and G.-H. Yang, "Byzantine-resilient distributed state estimation: A min-switching approach," *Automatica*, vol. 129, p. 109664, 2021.

[20] Y. Chen, S. Kar, and J. M. Moura, "Resilient distributed estimation: Sensor attacks," *IEEE Transactions on Automatic Control*, vol. 64, no. 9, pp. 3772–3779, 2018.

[21] J. Li, W. Abbas, and X. Koutsoukos, "Byzantine resilient distributed multi-task learning," *Advances in Neural Information Processing Systems*, vol. 33, pp. 18215–18225, 2020.

[22] Z. Yang and W. U. Bajwa, "Byrdie: Byzantine-resilient distributed coordinate descent for decentralized learning," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 5, no. 4, pp. 611–627, 2019.

[23] Z. Yang, A. Gang, and W. U. Bajwa, "Adversary-resilient distributed and decentralized statistical inference and machine learning: An overview of recent advances under the byzantine threat model," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 146–159, 2020.

[24] A. Mitra, J. A. Richards, and S. Sundaram, "A new approach to distributed hypothesis testing and non-bayesian learning: Improved learning rate and byzantine resilience," *IEEE Transactions on Automatic Control*, vol. 66, no. 9, pp. 4084–4100, 2020.

[25] S. Sundaram and B. Gharesifard, "Distributed optimization under adversarial nodes," *IEEE Transactions on Automatic Control*, vol. 64, no. 3, pp. 1063–1076, 2018.

[26] L. Su and N. H. Vaidya, "Byzantine-resilient multiagent optimization," *IEEE Transactions on Automatic Control*, vol. 66, no. 5, pp. 2227–2233, 2020.

[27] C. Zhao, J. He, and Q.-G. Wang, "Resilient distributed optimization algorithm against adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 65, no. 10, pp. 4308–4315, 2019.

[28] D. Saldana, A. Prorok, S. Sundaram, M. F. Campos, and V. Kumar, "Resilient consensus for time-varying networks of dynamic agents," in *2017 American control conference (ACC)*, pp. 252–258, IEEE, 2017.

[29] M. Pirani, A. Mitra, and S. Sundaram, "Graph-theoretic approaches for analyzing the resilience of distributed control systems: A tutorial and survey," *Automatica*, vol. 157, 2023.

[30] V. Renganathan, K. Fathian, S. Safaoui, and T. Summers, "Spoof resilient coordination in distributed and robust robotic networks," *IEEE Transactions on Control Systems Technology*, vol. 30, no. 2, pp. 803–810, 2021.

[31] S. M. Dibaji and H. Ishii, "Resilient consensus of second-order agent networks: Asynchronous update rules with delays," *Automatica*, vol. 81, pp. 123–132, 2017.

[32] H. Rezaee, T. Parisini, and M. M. Polycarpou, "Resiliency in dynamic leader–follower multiagent systems," *Automatica*, vol. 125, 2021.

[33] W. Abbas, A. Laszka, and X. Koutsoukos, "Improving network connectivity and robustness using trusted nodes with application to resilient consensus," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 4, pp. 2036–2048, 2018.

[34] Y. Shang, "Resilient consensus of switched multi-agent systems," *Systems & control letters*, vol. 122, pp. 12–18, 2018.

[35] K. Saulnier, D. Saldana, A. Prorok, G. J. Pappas, and V. Kumar, "Resilient flocking for mobile robot teams," *IEEE Robotics and Automation letters*, vol. 2, no. 2, pp. 1039–1046, 2017.

[36] G. Wen, Y. Lv, W. X. Zheng, J. Zhou, and J. Fu, "Joint robustness of time-varying networks and its applications to resilient consensus," *IEEE Transactions on Automatic Control*, 2023.

[37] J. Wu, Y. Zhu, Y. Zheng, and H. Wang, "Resilient bipartite consensus of second-order multiagent systems with event-triggered communication," *IEEE Systems Journal*, 2021.

[38] X. Lu and Y. Jia, "Bipartite byzantine-resilient event-triggered consensus control of heterogeneous multi-agent systems," *International Journal of Robust and Nonlinear Control*, vol. 33, no. 1, pp. 282–310, 2023.

[39] G. Ramos, D. Silvestre, and C. Silvestre, "A discrete-time reputation-based resilient consensus algorithm for synchronous or asynchronous communications," *IEEE Transactions on Automatic Control*, vol. 69, no. 1, pp. 543–550, 2023.

[40] J. Zhu, Y. Lin, A. Velasquez, and J. Liu, "Resilient distributed optimization," in *American Control Conference (ACC)*, pp. 1307–1312, 2023.

[41] G. Ramos, D. Silvestre, and C. Silvestre, "Node and network resistance to bribery in multi-agent systems," *Systems & Control Letters*, vol. 147, p. 104842, 2021.

[42] H. Zhang, E. Fata, and S. Sundaram, "A notion of robustness in complex networks," *IEEE Transactions on Control of Network Systems*, vol. 2, no. 3, pp. 310–320, 2015.
[43] J. Usevitch and D. Panagou, "Determining *r*-and (*r*, *s*)-robustness of digraphs using mixed integer linear programming," *Automatica*, vol. 111, p. 108586, 2020.
[44] J. Jiang, Y. Wu, Z. Zhang, N. Zheng, and W. Meng, "Determining *r*-and (*r*, *s*)-robustness of multiagent networks based on heuristic algorithm," *Neurocomputing*, vol. 598, p. 128025, 2024.
[45] Y. Yi, Y. Wang, X. He, S. Patterson, and K. H. Johansson, "A sample-based algorithm for approximately testing *r*-robustness of a digraph," in *61st IEEE Conference on Decision and Control (CDC)*, pp. 6478–6483, 2022.

Declaration of interests

☒ 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.

☐ The author is an Editorial Board Member/Editor-in-Chief/Associate Editor/Guest Editor for *[Journal name]* and was not involved in the editorial review or the decision to publish this article.

☐ The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: