Leveraging Diversity for Achieving Resilient Consensus in Sparse Networks

Faiq Ghawash * **Waseem Abbas** *

* *Information Technology University, Lahore, Pakistan*
(e-mails: faiq.ghawash@itu.edu.pk, w.abbas@itu.edu.pk)

Abstract: A networked system can be made resilient against adversaries and attacks if the underlying network graph is structurally robust. For instance, to achieve distributed consensus in the presence of adversaries, the underlying network graph needs to satisfy certain robustness conditions. A typical approach to making networks structurally robust is to strategically add extra links between nodes, which might be prohibitively expensive. In this paper, we propose an alternative way of improving network's robustness, that is by considering heterogeneity of nodes. Nodes in a network can be of different types and can have multiple variants. As a result, different nodes can have disjoint sets of vulnerabilities, which means that an attacker can only compromise a particular type of nodes by exploiting a particular vulnerability. We show that, by such a diversification of nodes, attacker's ability to change the underlying network structure is significantly reduced. Consequently, even a sparse network with heterogeneous nodes can exhibit the properties of a structurally robust network. Using these ideas, we propose a distributed control policy that utilizes heterogeneity in the network to achieve resilient consensus in adversarial environment. We extend the notion of (r,s)-robustness to incorporate the diversity of nodes and provide necessary and sufficient conditions to guarantee resilient distributed consensus in heterogeneous networks. Finally we study the properties and construction of robust graphs with heterogeneous nodes.

Keywords: Resilient Consensus, Network Robustness, Distributed Algorithm

1. INTRODUCTION

A key aspect of networked and cooperative systems is that participating agents rely on local interactions to achieve complex global tasks such as area coverage, network formation and flocking (for instance, see Mesbahi and Egerstedt (2010); Ren et al. (2005)). The success of various distributed control algorithms depend on agents sharing true information with each other and updating their states according to the predefined update protocols. However, if a small subset of agents do not adhere to the designed control protocols and share incorrect information with neighbors, the overall performance of the system is adversely impacted, and the overall network objective might not be achieved. For instance, in the distributed consensus problem, which is one of the most widely studied problem in distributed computing and network control systems, a single malicious node can prevent all the other nodes from converging to a common state, which is the overall network objective. Consequently, resilience of distributed control algorithms to malicious agents is an important issue.

A typical approach to improving resilience of distributed algorithms in networks is to exploit the underlying network structure. In fact, it has been shown that highly connected and structurally robust networks are more resilient to adversarial intrusions. For instance, to achieve distributed consensus, there are algorithms that guarantee consensus in the presence of misbehaving nodes if the underlying network graph satisfies certain connectivity and robustness conditions, for instance LeBlanc et al. (2013); Park and Hutchinson (2017); Tseng and Vaidya (2015). A common aspect in all these solutions is that the underlying network must satisfy certain robustness and connectivity conditions, which ultimately result in highly dense graphs. Although these solutions perform well, the high connectivity requirements might limit the scope of these solutions, especially in sparse networks. For instance, in many practical scenarios, where the communication links are formed based on proximity, it might be difficult or prohibitively expensive to establish new communication links between agents. Thus, an interesting question is how can we improve the resilience of such distributed algorithms in sparse networks? In other words, how can we make sparse networks *act like* highly connected or robust networks without adding communications links?

In this paper, we propose an alternative way of improving network's robustness, that is by utilizing the notion of *diversity* of nodes. In simple words, diversity means that nodes in a network are of different types and have many variants. Nodes might be different based on their hardware implementation, software, resources etc. A consequence of having diverse implementations is that nodes might have disjoint vulnerability sets, and by exploiting a particular vulnerability, an attacker can only impact the nodes belonging to that particular type. Thus, diversification effectively limits the attacker's ability to compromise

a large number of nodes within the network, and hence improves the network's robustness. We modify a typically used notion of network robustness (as in LeBlanc et al. (2013)) to include the effect of nodes' diversity, and then utilize it to design a resilient distributed consensus algorithm that guarantees convergence even in sparse networks. Our main contributions are:

- We formalize the notion of (r,s)-*robustness with coloring* that takes into account the effect of nodes' diversity by assigning colors to nodes. Then, we show that the robustness properties of the graph, even a sparse one, can be significantly improved by appropriately introducing diversity of nodes instead of adding extra edges with in the network.
- We propose a resilient distributed consensus algorithm and determine conditions—in terms of (r,s)-robustness with coloring—that guarantee consensus among normal nodes in the presence of adversaries.
- We also discuss the construction of (r,s)-robust graphs with colors. Finally, we provide simulations that verify our results.

The concept of diversification of nodes has been employed previously in computer networks as an effective security mechanism (e.g. see O'Donnell and Sethu (2004); Newell et al. (2015); Alarifi and Du (2006)). Apart from diversification of nodes, an alternative approach to improve the structural robustness is by making few carefully chosen nodes as trusted (immune to attacks by hardening), for instance Dziubiński and Goyal (2013); Abbas et al. (2019). Trusted nodes can help to design distributed algorithms that achieve resilient consensus (Abbas et al. (2018)) and resilient estimation (Mitra et al. (2018)), however, the assumption of guaranteeing the true operation of trusted nodes at all times is highly optimistic, and may require large investment to harden such agents.

The rest of the paper is organized as follows: Section 2 provides a network model and formulates the problem. Section 3 discusses the diversity paradigm and introduces the notion of (r,s)-robustness with coloring. Section 4 presents a resilient distributed consensus algorithm with a detailed analysis. Section 5 discusses construction of robust heterogeneous networks. Section 6 provides simulation results, and finally, Section 7 concludes the paper.

2. NETWORK MODEL AND PROBLEM FORMULATION

A multi-agent system is modelled by an undirected graph $\mathcal{G}(\mathcal{V},\mathcal{E})$. The vertex set $\mathcal{V}$ corresponds to agents (e.g robots, sensors), whereas the the edge set $\mathcal{E}$ represents the communication model among the agents. An edge between node i and j shows the information exchange between nodes and is represented by $(i,j) = (j,i)$. The *neighbourhood* of node i is defined as $N(i) = \{j \in \mathcal{V} : (i,j) \in \mathcal{V}\}$, and the *closed neighborhood* is $N[i] = N(i) \cup \{i\}$. We use the terms nodes, vertices and agents interchangeably. At any time instant t, each node has a state value denoted by $x_i(t) \in \mathbb{R}$. Based on the application, the state value can be a sensor measurement, position variable, optimization parameter, opinion or any other quantity of interest. We assume that all nodes interact synchronously with each other. Our network is heterogeneous in the sense that nodes are of different types.

Node types   There are multiple types (or variants) of nodes in the network, and each node belongs to a specific type. We denote node types by a set of colors $\Gamma = \{C_1, C_2, \cdots, C_n\}$. All nodes of type i are assigned color C_i. Nodes can be of different types based on their hardware platforms, software, resources, or due to other implementation or functional features. Moreover, each node in the network is either *normal* or *adversarial* as defined below:

Normal nodes   A normal node is the one that always updates its state according to a predefined update rule based on the values of nodes in $N[i]$, for instance,

$$x_i(t+1) = f(\{x_j(t)\}), \; j \in N[i]. \qquad (1)$$

Adversarial nodes   Adversarial nodes are the ones that are compromised by an attacker (for instance, by exploiting vulnerabilities), and therefore, do not follow the state update rule (1). They can change their state values arbitrarily. We consider that all adversarial nodes must belong to the *same type*, that is, they all have the *same color*. Adversarial nodes may feed others with malicious and misleading information, thus preventing the network to achieve the required global objective. We note that a normal node knows the colors of its neighbors, but does not know the type (color) of adversarial nodes.

Threat models and scopes   If an adversary node shares the same state value at time t with all of its neighbors, then it is commonly known as a *malicious adversary*. Similarly, an adversarial node sending different values to different nodes in its neighbors at time t is commonly referred to as the *byzantine adversary*. The scope of the threat is usually defined in terms of the number of adversarial nodes in the network, for instance using *F-total* and *F-local* models LeBlanc et al. (2013). In our case, *F-total* model means that there are at most F adversarial nodes (of the same color) in the network. Similarly, *F-local* model means that the neighborhood of any node in the network contains at most F adversarial nodes of the same color.

2.1 Objective: Resilient Consensus

Here, our objective is to design a distributed control policy for the normal agents such that *agreement* and *safety* conditions are satisfied in the presence of adversarial agents. Agreement condition requires the asymptotic convergence of normal nodes state values to a common value (consensus), whereas safety condition requires that at all times, the state value of any normal node is within the interval defined by the maximum and minimum of the initial values of normal nodes. More precisely, to achieve resilient consensus, the following conditions must be satisfied:

(1) As $t \to \infty$, $x_i(t) = x_j(t) = x$ for all normal nodes i,j.
(2) Let $M[t]$ and $m[t]$ denotes the maximum and minimum values of normal nodes at any time step t. For all normal nodes $i \in \mathcal{V}$, $m[0] \leq x_i(t) \leq M[0]$

3. DIVERSITY FOR IMPROVING NETWORK'S STRUCTURAL ROBUSTNESS

Heterogeneity in networks has been studied in many different contexts by researchers across various disciplines. One such aspect is the diversification of nodes, which broadly means that nodes in a network are of different types, and have multiple variants. Our goal is to exploit diversity of nodes to effectively improve the network's structural robustness. In other words, we explore if it is possible to limit an attacker's ability to change the underlying network structure by having a variety of nodes. Diversification of nodes can be achieved by employing different operating systems, software packages, and hardware platforms. Owing to distinct implementations of such variants, they typically have disjoint exploitation sets and vulnerabilities. As a result, an attacker cannot compromise devices of different types (with disjoint vulnerabilities) by exploiting a particular vulnerability at a time. In fact, an attacker can only compromise devices belonging to the same type or class by exploiting a particular vulnerability specific to that class. This effectively limits attackers ability to attack nodes in the network. Thus, if we assign colors to nodes depending on the particular type they belong to, then the attacker can only attack nodes of the same color by exploiting the vulnerabilities corresponding to that particular type. Building on this simple yet key observation, we model the diversity of nodes to improve network's robustness in adversarial environment.

We consider that each node belongs to a specific node type, which is represented by a color, and each node is then assigned a unique color.

Definition 1 (*Coloring*) Let $\Gamma = \{C_1, C_2, \dots C_n\}$ be the set of colors, then *coloring* $\mathcal{C}$ is the assignment of colors from Γ to nodes in $\mathcal{V}$, that is

$$\mathcal{C} : \mathcal{V} \longrightarrow \Gamma \qquad (2)$$

The number of colors used in the heterogeneous network is represented by C. For the ease of notation, we denote the color assigned to node i by $\mathcal{C}_i$.

Definition 2 (*Mono-chromatic and Poly-chromatic Subsets*) A subset of nodes $S \subseteq \mathcal{V}$ where $|S| > 1$ is mono chromatic, if all nodes in S have the same color, that is $\mathcal{C}_i = \mathcal{C}_j$, $\forall i, j \in S$. Otherwise S is poly-chromatic.

To measure network robustness and quantify the effect of adversarial nodes on the overall performance of the network, we utilize the notion of $(r, s) - robustness$ as in LeBlanc et al. (2013). This notion has turned out to be very useful in analyzing the resilience of distributed algorithms, in particular distributed consensus, in adversarial set-ups. Next, we modify the notion of (r, s)-robustness to incorporate the diversification of nodes.

Definition 3 (*r-valid node*) For a positive integer r and a subset $S \subset \mathcal{V}$, a node $v \in S$ is an *r-valid node* if at least one of the following is satisfied:

(i) v has at least r mono-chromatic neighbors outside of S (that is, in $N(v) \setminus S$).
(ii) v has at least two neighbors with different colors outside of S.

Definition 4 (*(r,s)-robustness with coloring*) Let $r, s > 1$ be two positive integers, and S_1 and S_2 be non-empty, disjoint subsets of $\mathcal{V}$. Let $\mathcal{X}_{S_1}^r$ and $\mathcal{X}_{S_2}^r$ be the set of r-valid nodes in $\mathcal{S}_1$ and $\mathcal{S}_2$ respectively. A graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$ is *(r,s)-robust with coloring* if at least one of the following is always satisfied:

(i) $|\mathcal{X}_{S_1}^r| = |\mathcal{S}_1|$.
(ii) $|\mathcal{X}_{S_2}^r| = |\mathcal{S}_2|$.
(iii) $(\mathcal{X}_{S_1}^r \cup \mathcal{X}_{S_2}^r)$ is mono-chromatic and $|\mathcal{X}_{S_1}^r \cup \mathcal{X}_{S_2}^r| \geq s$.
(iv) $(\mathcal{X}_{S_1}^r \cup \mathcal{X}_{S_2}^r)$ is poly-chromatic.

The condition (iv) above requires at least two distinct colored r-valid nodes in $S_1 \cup S_2$. We note that if all nodes in the network are of the same color, then the above definition is exactly the notion of (r, s)-robustness defined in LeBlanc et al. (2013). An illustrations of conditions (iii) and (iv) are given in Figure 1.
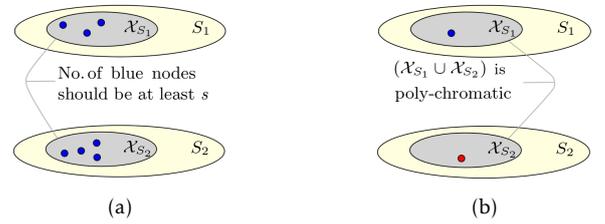

Fig. 1. Conditions (iii) and (iv) for (r, s)-robustness with coloring.

The main idea here is that a graph that is (r, s)-robust (with only one color) can be (r', s')-robust with (multiple) colors for $r' > r$ and $s' > s$. In other words, it is possible to make sparse networks highly robust with colors assigned appropriately to nodes. We also note that (r, s)-robustness can only be improved using colors if the underlying graph is at least $(2, 2)$-robust. Similarly, we define the notion of *r-robustness with coloring*, which will be used to analyze the resilient consensus in the case of F-local adversary model, as below:

Definition 5 (*r-robustness with coloring*) A graph is *r-robust with coloring*, if for any pair of non-empty disjoint subset $S_1, S_2 \subset V$, at least one of the subsets must contain a node that has at least r-neighbours of any color or at least three distinct color neighbours outside of its respective set.

It must be noted that r-robustness can only be improved using colors if the underlying graph is at least 3-robust. We also note that the notion of r-robustness with coloring and (r, s)-robustness with coloring differ with respect to the validity of node having poly-chromatic neighbourhood. Hence $(r, 1)$-robustness with coloring does not correspond to r-robustness with coloring except in networks with only one type of nodes. We explain the significance of colors and the notion of (r, s)-robustness with coloring in the examples below.

3.1 Examples

The graph in Figure 2(a) is $(2, 2)$-robust with one color. However, if we use three colors such that nodes in the set $\{1, 2, 3, 4, 5, 7\}$ are assigned color C_1, node 6 is assigned C_2, and node 8 has color C_3, then the graph becomes

(4, 4)-robust with three colors. Similarly, the graph in 2(b) is not (3, 3)-robust if all the nodes have the same color. By using three colors, the graph becomes (5, 5)-robust, for instance, if nodes in $\{1, 2, 5, 6, 9\}$ have color C_1, nodes in $\{7, 8, 10\}$ have C_2 and nodes in $\{3, 4\}$ are assigned C_3. Finally, the graph in Figure 2(c) is 3-robust which becomes 5-robust with three colors, where nodes in the sets $\{1, 4, 5, 6, 10, 11\}, \{2, 3\}$ and $\{7, 8, 9\}$ have colors C_1, C_2 and C_3 respectively.
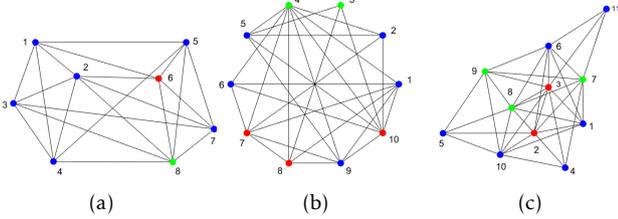

Fig. 2. (a) (4, 4)-robust graph with colors. (b) (5, 5)-robust graph with colors. (c) 5-robust graph with colors.

These examples emphasize that diversity of nodes in the network can be used to significantly improve the robustness of the network. A network can exhibit the properties of highly connected and structurally robust networks without adding additional communication links. Figure 3 shows the comparison of adding additional links to the nodes coloring (diversification) approach. It is observed that diversification could improve robustness in networks, especially in cases where adding communication links are prohibitively expensive or is not feasible. Moreover, it is interesting to note that multiple coloring schemes can be utilized to achieve the desired robustness.
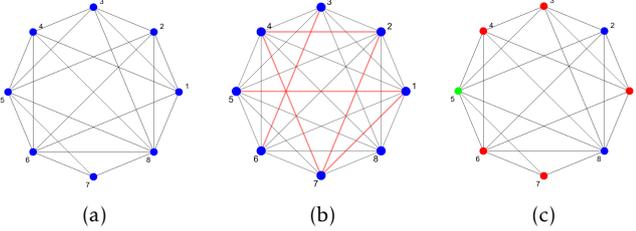

Fig. 3. (a) A (2, 2)-robust graph with one color nodes. (b) Six edges must be added to make the graph (4, 4)-robust. (c) Graph becomes (4, 4)-robust by appropriately introducing three colors.

4. RESILIENT CONSENSUS PROTOCOL WITH COLORING (RCP-C)

In this section, we present a distributed state update rule for normal nodes, which we term as *Resilient Consensus Protocol with Coloring* (RCP-C) that guarantees consensus among normal nodes in heterogeneous networks under certain robustness conditions discussed later. The main idea is that, at any time step t, node i collects values from all of its neighbors, but considers only a subset of them to update its state. We note that every node knows the colors of its neighbors, but does not know the color of adversarial nodes. The values of neighbors considered by i are explained below:

First, a node determines F largest and F smallest values corresponding to nodes in $N_i(t)$. Let such nodes be denoted by $\overline{\mathcal{R}}_i(t)$ and $\underline{\mathcal{R}}_i(t)$ respectively. The node i always considers values of nodes in $N_i(t) \setminus (\overline{\mathcal{R}}_i(t) \cup \underline{\mathcal{R}}_i(t))$. Here, F is a given parameter, and is an upper bound on the number of adversaries (under the F-total or F-local models). Second, based on the colors of nodes in $\overline{\mathcal{R}}_i(t)$ (respectively $\underline{\mathcal{R}}_i(t)$), node i groups values into various subsets. Then, i ignores all the values in the subset containing the maximum (minimum) value, and considers all the values in the remaining subsets.

Next, we formally present the steps in the algorithm below, and illustrate in Figure 4.

(1) At each time step t, node i receives state values from its neighbours $N_i(t)$.

(2) The neighbouring nodes $N_i(t)$ are categorized into two sets $\overline{N}_i(t)$ and $\underline{N}_i(t)$ based on their state values as follows:

$$\overline{N}_i(t) = \{l \in N_i(t) : x_l(t) > x_i(t)\}$$
$$\underline{N}_i(t) = \{l \in N_i(t) : x_l(t) < x_i(t)\}$$

Next, define $\overline{\mathcal{R}}_i(t) = \overline{N}_i(t)$ if $|\overline{N}_i(t)| < F$. Otherwise, $\overline{\mathcal{R}}_i(t)$ consists of the F nodes in $\overline{N}_i(t)$ with the highest state values. Similarly, define $\underline{\mathcal{R}}_i(t) = \underline{N}_i(t)$ if $|\underline{N}_i(t)| < F$. Otherwise $\underline{\mathcal{R}}_i(t)$ consists of the F nodes in $\underline{N}_i(t)$ with the lowest state values. Finally, we define

$$\mathcal{R}_i(t) = \underline{\mathcal{R}}_i(t) \cup \overline{\mathcal{R}}_i(t)$$

(3) Based on the number of colors in the neighborhood of node i, $\overline{\mathcal{R}}_i(t)$ is divided into different subsets, $\{\overline{V}_1^i(t), \overline{V}_2^i(t), \cdots \overline{V}_C^i(t)\}$, where $\overline{V}_k^i(t)$ contains the values in $\overline{\mathcal{R}}_i(t)$ corresponding to nodes with color C_k. Consider $\overline{V}_M^i(t)$ to be the subset containing the maximum value in $\overline{\mathcal{R}}_i(t)$. [1] Moreover, define

$$\overline{\mathcal{D}_i}(t) = \overline{\mathcal{R}}_i(t) \setminus \overline{V}_M^i(t).$$

Similarly, divide $\underline{\mathcal{R}}_i(t)$ into subsets, $\{\underline{V}_1^i(t), \cdots \underline{V}_C^i(t)\}$, and consider $\underline{V}_m^i(t)$ to be the subset containing the minimum value in $\underline{\mathcal{R}}_i(t)$. Then, define

$$\underline{\mathcal{D}_i}(t) = \underline{\mathcal{R}}_i(t) \setminus \underline{V}_m^i(t).$$

Finally, we define

$$\mathcal{D}_i(t) = \overline{\mathcal{D}}_i(t) \cup \underline{\mathcal{D}}_i(t).$$

(4) Each normal node i updates its value according to the following rule:

$$x_i(t+1) = \sum_{j \in [(N_i[t] \setminus \mathcal{R}_i(t)] \cup \mathcal{D}_i(t)} w_{ij}(t) x_j(t) \qquad (3)$$

Here, $w_{ij}(t)$ represents the weight that is assigned to the value of node j by node i at time step t [2]. An illustration of various steps of the algorithm is given in Figure 4.

The RCP-C differs from the conventional Weighted Mean Subsequent Reduced (WMSR) algorithm (LeBlanc et al. (2013)) in step-3. This step allows the algorithm to utilize the diversity of nodes in the network and extract useful information based on the colors (types) of nodes in the neighbourhood.

---

[1] Ties are broken arbitrarily.
[2] $\sum_{j=1}^n w_{ij} = 1$, where $w_{ij} \geq \alpha$ for some $0 < \alpha < 1$.
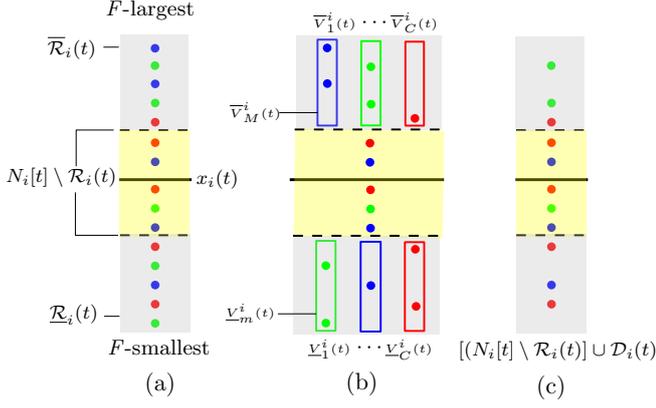
Fig. 4. Illustration of steps followed in RCP-C. (a) Node i computes F largest (and F smallest) values with respect to node's own value (Steps 1 and 2). (b) Based on the colors of neighbors, node i groups values in $\overline{\mathcal{R}}_i(t)$ (respectively $\underline{\mathcal{R}}_i(t)$) and ignores all the values in the group containing the maximum (minimum) value (Step 3). (c) All remaining values in (a) and (b) are considered in the update rule of node i (Step 4).

4.1 Analysis

Next, we analyze RCP-C algorithm, and provide necessary and sufficient conditions to guarantee resilient consensus in the presence of adversaries (F-total and F-local models) in heterogeneous networks. The main results are stated below.

Theorem 4.1. Let $\mathcal{G}(\mathcal{V}, \mathcal{E})$ be a time invariant heterogeneous network, in which each node is assigned a color from the coloring set $\Gamma = \{C_1, C_2, \cdots, C_n\}$, and each normal node follows RCP-C. Then,

(1) under the *F-total malicious model*, resilient asymptotic consensus is achieved if and only if the underlying graph topology is $(F+1, F+1)$-robust with colors.
(2) Similarly, under the *F-local malicious model*, resilient asymptotic consensus is achieved if the underlying graph topology is $(2F+1)$-robust with colors.

The proof of Theorem 4.1 is given in Appendix A.

5. CONSTRUCTION AND PROPERTIES OF HETEROGENEOUS ROBUST GRAPHS

In this section, first we discuss the construction of (r, s)-robust graphs with colors. Since the exact computation of (r, s)-robustness is computationally challenging, even if all the nodes are of the same color (as discussed in Zhang et al. (2015)), it is useful to develop approaches to grow networks by adding nodes while preserving robustness.

Theorem 5.1. Let $\mathcal{G}(\mathcal{V}, \mathcal{E})$ be an (r, s)-robust graph with colors. Then the graph $\mathcal{G}'(\mathcal{V} \cup \{u_{new}\}, \mathcal{E}')$ obtained by adding a new vertex u_{new} to $\mathcal{G}(\mathcal{V}, \mathcal{E})$ is also (r, s)-robust with colors if any of the following holds.

(1) u_{new} is adjacent to at least $r + s - 1$ mono-chromatic nodes.
(2) u_{new} is adjacent to at least $\max(r, s)$ nodes of color C_k and one node of any other color $C_j, j \neq k$.
(3) u_{new} is adjacent to at least three distinct color nodes.

The proof of Theorem 5.1 is given in Appendix B.

Similarly, it can be shown that the property of r-robustness with colors remain preserved if a new node is adjacent to r nodes of any color, or it is adjacent to three distinct color nodes in the existing graph.

Next, we analyze the robustness conditions that guarantee consensus of normal nodes implementing RCP-C if *all* the nodes of the same color are compromised. Here, note the difference with the earlier attack model in which at most F nodes of the same color could be adversaries (under the F-total or F-local set-up). For this, we need to introduce the notion of *mono-chromatic robust graphs*.

Definition 6 (*Mono-chromatic robust*) A graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$ with coloring $\mathcal{C}$ is mono-chromatic robust, if for any pair of non-empty disjoint subset $S_1, S_2 \subset \mathcal{V}$, at least one of the subsets contains a node that has at least three distinct color neighbours outside of its respective set.

Since every normal node has neighbors with multiple colors in a mono-chromatic robust graph, it always considers a value from a normal neighbor to update its state. A node will always have normal neighbor as all the adversarial nodes are of the same color. This gives us the following:

Theorem 5.2. Under RCP-C all normal nodes will reach resilient asymptotic consensus in the presence of any number of malicious adversaries of the same color if the underlying graph topology is mono-chromatic robust.

Proof of Theorem 5.2 is given in Appendix B.

Further, we analyze the requirement on minimum number of colors necessary to achieve mono-chromatic robust graphs and provide sharp bounds for some specific graph classes that can be made mono-chromatic robust by a careful assignment of colors to nodes. These graph classes include F-elemental graphs (discussed in Guerrero-Bonilla et al. (2017)) that are inherently $2F+1$-robust graphs and 3-robust graphs with certain conditions on the neighbourhood of each node.

Theorem 5.3. Given a graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$ with coloring $\mathcal{C}$, at least five colors ($C = 5$) are required to make the graph mono-chromatic robust. For F-elemental graphs ($F > 2$) the bound is sharp.

Proof of Theorem 5.3 is given in Appendix B.

Theorem 5.4. A 3-robust graph in which at least three nodes in the neighbourhood of each vertex are pairwise adjacent, then the number of colors required to make such $\mathcal{G}(\mathcal{V}, \mathcal{E})$ mono-chromatic robust is upper bounded by the chromatic number [3] of $\mathcal{G}(\mathcal{V}, \mathcal{E})$.

Proof of Theorem 5.4 is given in Appendix B.

Based on the above results, a mono-chromatic robust graph of n nodes can be constructed by starting with a complete graph on five nodes (K_5) graph and assigning each vertex a unique color. New nodes are added in the network by connecting them with three distinct color nodes in the existing network.

---

[3] Minimum number of colors assigned to nodes such that no two adjacent nodes have the same color.

6. SIMULATION RESULTS

To validate our proposed RCP-C algorithm in heterogeneous networks, we provide simulations for both *F*-total and *F*-local malicious models and compare our approach with existing WMSR algorithm in homogeneous networks. Under the *F*-total malicious model, we consider the network shown in Figure 5(a) which is $(2, 2)$-robust with one color. It means only one malicious node can be tolerated (using WMSR algorithm). Thus, if nodes $3, 7, 8$ are malicious, consensus is not achieved as shown in Figure 5(a). However, by an appropriate assignment of colors to nodes (as shown in Figure 5(b)), the same network becomes $(4, 4)$-robust with three colors and can handle up to three malicious nodes. If normal nodes implement RCP-C, consensus is guaranteed even with an attack of three malicious nodes as illustrated in Figure 5(b). Similarly, the network considered for F-local model simulation is shown in Figure 5(c). The network is 3-robust with one color and can tolerate at most 1 malicious node in the neighbourhood of any node. If we consider $F = 2$, and nodes 2 and 3 to be malicious, consensus is not achieved under WMSR algorithm. However, the same network becomes 5-robust with three colors as shown in Figure 5(d). Under RCP-C, normal nodes achieve resilient asymptotic consensus as illustrated in Figure 5(d).

(a) *F*-total model (WMSR)

(b) *F*-total model (RCP-C)

(c) *F*-local model (WMSR)

(d) *F*-local model (RCP-C)

Fig. 5. Comparison of WMSR and RCP-C under the *F*-total and *F*-local malicious models.

7. CONCLUSIONS

This paper proposed an alternative way to improve structural robustness in networks by incorporating the diversification of nodes. We showed that the attacker's ability to change the underlying network could be significantly reduced by deploying diverse nodes. This could effectively lead to a higher robustness in networks, even if they are sparse originally. To account for the robustness of heterogeneous network, we proposed the notion of (r, s)-robustness with coloring. We studied the resilient consensus problem and proposed a distributed algorithm that took into account the diversity of nodes in the network and provided conditions in terms of (r, s)-robustness with coloring to guarantee consensus in the presence of adversaries. In future, we would like to generalize the attack model by allowing multiple types of nodes to be attacked. Moreover, assigning appropriate types (colors) to nodes to achieve desired robustness is computationally challenging, and we aim to provide efficient algorithms for this problem.

8. ACKNOWLEDGMENTS

REFERENCES

Abbas, W., Laszka, A., and Koutsoukos, X. (2018). Improving network connectivity and robustness using trusted nodes with application to resilient consensus. *IEEE Trans. on Control of Network Systems*, 5(4).

Abbas, W., Laszka, A., and Koutsoukos, X. (2019). Diversity and trust to increase structural robustness in networks. In *American Control Conference (ACC)*. IEEE.

Alarifi, A. and Du, W. (2006). Diversify sensor nodes to improve resilience against node compromise. In *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, 101–112. ACM.

Dziubiński, M. and Goyal, S. (2013). Network design and defence. *Games and Economic Behavior*, 79, 30–43.

Guerrero-Bonilla, L., Prorok, A., and Kumar, V. (2017). Formations for resilient robot teams. *IEEE Robotics and Automation Letters*, 2(2).

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

Mesbahi, M. and Egerstedt, M. (2010). *Graph theoretic methods in multiagent networks*, volume 33. Princeton University Press.

Mitra, A., Abbas, W., and Sundaram, S. (2018). On the impact of trusted nodes in resilient distributed state estimation of lti systems. In *2018 IEEE Conference on Decision and Control (CDC)*, 4547–4552. IEEE.

Newell, A., Obenshain, D., Tantillo, T., Nita-Rotaru, C., and Amir, Y. (2015). Increasing network resiliency by optimally assigning diverse variants to routing nodes. *IEEE Transactions on Dependable and Secure Computing*, 12(6), 602–614.

O'Donnell, A.J. and Sethu, H. (2004). On achieving software diversity for improved network security using distributed coloring algorithms. In *Proceedings of the 11th ACM conference on Computer and communications security*, 121–131. ACM.

Park, H. and Hutchinson, S.A. (2017). Fault-tolerant rendezvous of multirobot systems. *IEEE transactions on robotics*, 33(3), 565–582.

Ren, W., Beard, R.W., and Atkins, E.M. (2005). A survey of consensus problems in multi-agent coordination. In *Proceedings of the 2005, American Control Conference, 2005.*, 1859–1864. IEEE.

Tseng, L. and Vaidya, N.H. (2015). Fault-tolerant consensus in directed graphs. In *Proceedings of the 2015 ACM Symposium on Principles of Distributed Computing*.

Zhang, H., Fata, E., and Sundaram, S. (2015). A notion of robustness in complex networks. *IEEE Trans. on Control of Network Systems*, 2(3).
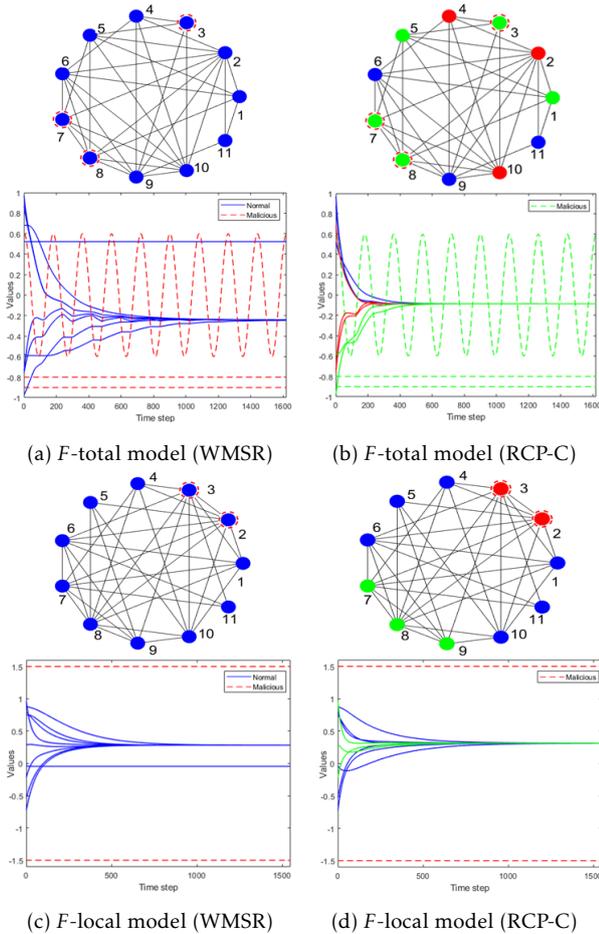
Appendix A. PROOFS

A.1 Proof of Theorem 4.1 (a)

In order to prove the theorem, we use similar arguments used in the proof of Theorem 1 in LeBlanc et al. (2013).

Proof: (**Necessity**) *Under the F-total malicious model* $(F + 1, F + 1)$*-robustness with coloring is a necessary condition.*

Let us consider a graph $\mathcal{G}$ that is not $(F + 1, F + 1)$-robust with coloring. Hence there would exist some non-empty disjoint subsets S_1 and S_2 which do not satisfy any of the conditions in Definition 4. Therefore, there would be at most F nodes in $S_1 \cup S_2$ that have two distinct color nodes or $F + 1$ neighbours outside of their respective set ($|\mathcal{X}_{S_1}^{F+1} \cup \mathcal{X}_{S_2}^{F+1}| \leq F$). Moreover, we also know that ($\mathcal{X}_{S_1}^{F+1} \cup \mathcal{X}_{S_2}^{F+1}$) is mono-chromatic otherwise condition (iv) in Definition 4 would be satisfied. As there can be F adversaries in the network under the F-total model, we assume that all valid nodes ($\mathcal{X}_{S_1}^{F+1} \cup \mathcal{X}_{S_2}^{F+1}$) are malicious. Moreover, we know that none of the conditions in Definition 4 is satisfied by $\mathcal{G}$. Hence for some $i \in \{1, 2\}$ $|\mathcal{X}_{S_i}^{F+1}| < |S_i|$, this implies that there would exist at least one normal node in both S_1 and S_2, say x_1 and x_2, that has at most F mono-chromatic neighbours outside of its respective set. Now consider that, all nodes in S_1 have state values a and state value in S_2 be b, where $b > a$. The state values of all nodes in $\mathcal{V} \setminus (S_1 \cup S_2)$ are assigned values in the interval (a, b). Malicious nodes keep their values constant throughout. Both x_1 and x_2 ignores all values (F or less) outside of their respective set. Hence consensus would not be achieved.

(**Sufficiency**) $(F + 1, F + 1)$*-robustness with coloring is a sufficient condition under F-total malicious model.*

Let $\mathcal{A}$ denotes the adversarial nodes in the network, then $\mathcal{N} = \mathcal{V} \setminus \mathcal{A}$ corresponds to the set of normal nodes. We define $M[t] = max_{i \in \mathcal{N}} x_i(t)$ and $m[t] = min_{i \in \mathcal{N}} x_i(t)$. We know that all nodes in $(N_i[t] \setminus \mathcal{R}_i(t)) \cup \mathcal{D}_i(t)$ contains values in the interval $[m[t], M[t]]$ and the update rule is defined as the convex combination of values in the interval. We deduce that $m[t]$ and $M[t]$ are monotone and bounded functions of t and thus both have some limits denoted by A_m and A_M respectively. In order to achieve consensus among the normal agents we need to show that $A_M = A_m$. We will assume that $A_M > A_m$ and then show that such an assumption leads to contradiction allowing us to prove $A_M = A_m$. Let $A_M > A_m$ and define a constant ϵ_o such that $A_M - \epsilon_o > A_m + \epsilon_o$. At any time instant t and for any positive number ϵ_i, we define

$$\mathcal{S}_M(t, \epsilon_i) = \{j \in \mathcal{V} : x_j(t) > A_M - \epsilon_i\} \quad (A.1)$$

$$\mathcal{S}_m(t, \epsilon_i) = \{j \in \mathcal{V} : x_j(t) < A_m + \epsilon_i\} \quad (A.2)$$

$\mathcal{S}_M(t, \epsilon_i)$ have all nodes whose state values are greater than $A_M - \epsilon_i$. Similarly $\mathcal{S}_m(t, \epsilon_i)$ have nodes with values less than $A_m + \epsilon_i$. It must be noted that $\mathcal{S}_M(t, \epsilon_i)$ and $\mathcal{S}_m(t, \epsilon_i)$ contain both the normal and malicious nodes. Now let $\mathcal{X}_M^{F+1}(t, \epsilon_i) \subseteq \mathcal{S}_M(t, \epsilon_i)$ be a subset of valid nodes, that is, each node in $\mathcal{X}_M^{F+1}(t, \epsilon_i)$ have $F+1$ mono-chromatic neighbours or two distinct color neighbours outside of $\mathcal{S}_M(t, \epsilon_i)$. Similarly $\mathcal{X}_m^{F+1}(t, \epsilon_i) \subseteq \mathcal{S}_m(t, \epsilon_i)$ be the subset of valid nodes in $\mathcal{S}_m(t, \epsilon_i)$.

Now fix $\epsilon < \frac{\alpha^N}{1 - \alpha^N}$ where $N = |\mathcal{N}|$ denotes total number of normal nodes and here $\epsilon_o > \epsilon > 0$. From the definition of convergence, we know that there exist a t_ϵ such that for any time instant $t > t_\epsilon$, $M[t]$ and $m[t]$ are bounded by $A_M + \epsilon$ and $A_m - \epsilon$.

Consider non-empty disjoint subsets $\mathcal{S}_M(t_\epsilon, \epsilon_o)$ and $\mathcal{S}_m(t_\epsilon, \epsilon_o)$. From the definition of ϵ_o, we note that $\mathcal{S}_M(t_\epsilon, \epsilon_o)$ and $\mathcal{S}_m(t_\epsilon, \epsilon_o)$ are disjoint. Since the graph $\mathcal{G}$ is $(F + 1, F + 1)$-robust with coloring and there can be at most F adversaries in the network. Hence there would always exist one normal valid node in $\mathcal{X}_M(t_\epsilon, \epsilon_o) \cup \mathcal{X}_m(t_\epsilon, \epsilon_o)$. Without loss of generality, we assume that such a valid node (say i) is in $\mathcal{X}_M(t_\epsilon, \epsilon_o) \cap \mathcal{N}$. Next, we show that

$$x_i(t_\epsilon + 1) \leq A_M - \epsilon_1, \epsilon_1 < \epsilon_o \quad (A.3)$$

In order to compute $x_i(t_\epsilon + 1)$, node i consider values of nodes in the set $(N[k] \setminus \mathcal{R}_i(t)) \cup D_i(t)$ (as defined in RCP-C Algorithm). As the node i has at least $F + 1$ mono-chromatic nodes or two distinct color neighbours outside of the set with values less than its own. Thus node i would always consider a value lesser than its own while computing $x_i(t_\epsilon + 1)$. The maximum value of such a neighbour is $A_M - \epsilon_o$ as it lies in $\mathcal{V} \setminus \mathcal{S}_M(t_\epsilon, \epsilon_o)$. The maximum value that node i, receives from its neighbours in $\mathcal{S}_M(t_\epsilon, \epsilon_o)$ is $M[t_\epsilon]$. Since the update rule is the convex combination of the state values of the neighbours and each combination coefficient is lower bounded by α. In the worst case, assigning the maximum weight to the highest value we get

$$x_i(t_\epsilon + 1) \leq (1 - \alpha)M(t_\epsilon) + \alpha(A_M - \epsilon_o)$$
$$\leq (1 - \alpha)(A_M + \epsilon) + \alpha(A_M - \epsilon_o)$$
$$\leq A_M - \alpha\epsilon_o + (1 - \alpha)\epsilon$$
$$= A_M - \epsilon_1$$

where $\epsilon_1 = \alpha\epsilon_o - (1 - \alpha)\epsilon$ and $\epsilon_1 < \epsilon_o$. We can repeat the same steps if node $i \in \mathcal{X}_m^{F+1}$. Hence

$$x_i(t_\epsilon + 1) \geq A_m + \epsilon_1 \quad (A.4)$$

As a consequence of the A.3 and A.4 at least one of the following is true

- The number of normal nodes in $\mathcal{S}_M(t + 1, \epsilon_1) \cap \mathcal{N}$ is strictly lesser than the normal nodes in $\mathcal{S}_M(t, \epsilon_o) \cap \mathcal{N}$ e.g $|\mathcal{S}_M(t + 1, \epsilon_1) \cap \mathcal{N}| < |\mathcal{S}_M(t, \epsilon_o) \cap \mathcal{N}|$.
- $|\mathcal{S}_m(t + 1, \epsilon_1) \cap \mathcal{N}| < |\mathcal{S}_m(t, \epsilon_o) \cap \mathcal{N}|$.

Note that $\mathcal{S}_M(t + 1, \epsilon_1)$ and $\mathcal{S}_m(t + 1, \epsilon_1)$ are disjoint as $\epsilon_1 < \epsilon_o$. Next, we define $\epsilon_j = \epsilon_{j-1} - (1 - \alpha)\epsilon$ for any $j \geq 1$. Note that $\epsilon_j < \epsilon_{j-1}$. Then for any time step $t_\epsilon + j$, the above analysis can be repeated as long as $\mathcal{S}_M(t_\epsilon + j, \epsilon_j)$ and $\mathcal{S}_m(t_\epsilon + j, \epsilon_j)$ contain normal nodes. Since the number of normal nodes are finite, there exist a time step $t_\epsilon + k$ such that at least one of the following is always satisfied:

(a) $\mathcal{S}_M(t_\epsilon + k, \epsilon_k) = \emptyset$, which implies that the maximum value of any normal node at time step $t_\epsilon + k$ is upper bounded by $A_M - \epsilon_k$, or

(b) $\mathcal{S}_m(t_\epsilon + k, \epsilon_k) = \emptyset$, which implies that the minimum value of the normal nodes is lower bounded by $A_m + \epsilon_k$.

If $\epsilon_k > 0$, then (a) implies a contradiction to the fact that $M[t]$ converges monotonically to A_M and (b) contradicts

to the fact that the $m[t]$ converges monotonically to A_m. Next, we show that $\epsilon_k > 0$.

$$\epsilon_k = \alpha\epsilon_{k-1} - (1-\alpha)\epsilon = \alpha^k \epsilon_o - (1-\alpha^k)\epsilon$$
$$\geq \alpha^N \epsilon_o - (1-\alpha^N)\epsilon \qquad (A.5)$$

Since $\epsilon < \frac{\alpha^N}{1-\alpha^N}$, we get $\epsilon_k > 0$ which gives the desired contradiction, thus proving that $A_M = A_m$. $\blacksquare$

A.2 Proof of Theorem 4.1 (b)

Proof: (**Sufficiency**) *$2F + 1$-robustness with coloring is a sufficient condition under the F-local malicious model.*
We can construct the sufficiency proof using the same approach and arguments as followed in proof of the Theorem 4.1 (a). Recall $\mathcal{N}$ denotes the set of all normal nodes. For F-Local malicious model, it must be noted that when considering the non-empty disjoint subsets $\mathcal{S}_M(t_\epsilon, \epsilon_o) \cap \mathcal{N}$ and $\mathcal{S}_m(t_\epsilon, \epsilon_o) \cap \mathcal{N}$ defined in the proof of Theorem 4.1 (a) (the main difference here is that we are considering only normal nodes), at least one of the set contains a node that has at least $2F + 1$ or three distinct color neighbours outside of its respective set as the underlying graph is $2F + 1$-robust with coloring. Recall that at most F (or less) monochromatic nodes can be compromised, thus there would exist a normal node in $(\mathcal{S}_M(t_\epsilon, \epsilon_o) \cap \mathcal{N} \cup \mathcal{S}_m(t_\epsilon, \epsilon_o) \cap \mathcal{N})$ that will utilize the value of at least one normal node value outside of $S_M(t_\epsilon, \epsilon_o)$ or $S_m(t_\epsilon, \epsilon_o)$ sets. $\blacksquare$

Appendix B. PROOFS

B.1 Proof of Theorem 5.1

Proof: Let S_1' and S_2' be any two non-empty disjoint subsets in $\mathcal{G}'$. For such S_i' where $i \in \{1, 2\}$, there can be three cases (a) $u_{new} \notin S_i'$ (b) $\{u_{new}\} = S_i'$ (c) $u_{new} \in S_i'$.

In the first case, since $\mathcal{G}$ is (r,s)-robust with coloring, hence at least one of the condition in Definition 4 is satisfied directly by S_1' and S_2' in $\mathcal{G}'$.
In case (b), under all three clauses of the theorem u_{new} would be a valid node hence condition (i) or (ii) is satisfied in Definition 4.
In (c), we can assume that $u_{new} \in S_2'$ without loss of generality. Let $S_1 = S_1'$ and $S_2 = S_2' \setminus \{u_{new}\}$. As the graph $\mathcal{G}$ is (r,s)-robust with coloring hence the subset S_1 and S_2 satisfy at least one of the conditions in Definition 4. If any of the conditions among (i), (iii) or (iv) is satisfied by S_1 and S_2 in graph $\mathcal{G}$ then same condition would be satisfied by S_1' and S_2' in $\mathcal{G}'$.
Now, let us assume condition (ii) is satisfied among all conditions in $\mathcal{G}$ which is $|\mathcal{X}_{S_2}^r| = |S_2|$. If $|\mathcal{X}_{S_2}^r|$ is poly-chromatic then (iv) gets satisfied so we can assume that S_2 consist of mono-chromatic valid nodes only. Moreover, since only condition (ii) is satisfied among all conditions in Definition 4 hence $|\mathcal{X}_{S_1}^r| + |\mathcal{X}_{S_2}^r| < s$ and $|\mathcal{X}_{S_2}^r| = |S_2|$. This implies that S_2 can have at most $s-1$ nodes.
Under the clause (i), if u_{new} in G' is connected to at least $r+s-1$ mono-chromatic nodes, then it must be connected to at least r mono-chromatic nodes outside S_2'. Similarly

under the clause (ii) of the theorem, if $u_{new} \in G'$ is connected to $\max(r,s)$ nodes of C_k and one node of C_j, then u_{new} would be connected to at least r mono-chromatic, or two distinct colors neighbours outside of S_2' making u_{new} a valid node. Under the clause (iii) of the theorem, if u_{new} in $\mathcal{G}'$ is connected to three distinct color nodes, it would always be connected to at least two distinct colors nodes outside of S_2'. $\blacksquare$

B.2 Proof of Theorem 5.2

Proof: The theorem can be proved using the same approach and arguments as followed in proof of the Theorem 4.1 (a). Note that $\mathcal{N}$ denotes the set of all normal nodes. For mono-chromatic robust graphs, it must be noted that when considering the non-empty disjoint subsets $S_M(t_\epsilon, \epsilon_o) \cap \mathcal{N}$ and $S_m(t_\epsilon, \epsilon_o) \cap \mathcal{N}$ defined in the proof of Theorem 4.1 (a), at least one of the set contains a node that has at least three distinct color neighbours outside of its respective set. As nodes of only one color are compromised, thus there would exist a normal node in $(\mathcal{S}_M(t_\epsilon, \epsilon_o) \cap \mathcal{N} \cup \mathcal{S}_m(t_\epsilon, \epsilon_o) \cap \mathcal{N})$ that will utilize the value of at least one normal node value outside of $S_M(t_\epsilon, \epsilon_o)$ or $S_m(t_\epsilon, \epsilon_o)$ sets. $\blacksquare$

B.3 Proof of Theorem 5.3

Proof: Let $\mathcal{G}(\mathcal{V}, \mathcal{E})$ be a colored r-robust graph with four colors ($C = 4$). Let S_1 and S_2 be any arbitrary non-empty disjoint subsets. Without loss of generality, for some $i \in \{1, 2\}$ and $j \in \{3, 4\}$, we consider $S_1 = \{l \in \mathcal{V} : C(l) \in C_i\}$ and $S_2 = \{l \in \mathcal{V} : C(l) \in C_j\}$. Then, there does not exist any node in S_1 or S_2 which has three distinct color neighbours outside of its respective set. Hence mono-chromatic robustness can never be achieved with lesser than five colors in the network.

Definition 7 (*F-elemental graph*) An F-elemental graph is a graph with $|\mathcal{V}| = 4F + 1$ nodes that is r-robust with $r = 2F + 1$ for some positive integer value of F.

(*Sharpness of bound for F-elemental graphs*) Given an F-elemental $\mathcal{G}(\mathcal{V}, \mathcal{E})$ graph ($F > 2$), the number of vertices are $|\mathcal{V}| = 4F + 1$ and there exist a set $\mathcal{V}' \subseteq \mathcal{V}$ ($|\mathcal{V}'| = 2F$) such that all nodes in $\mathcal{V}'$ are connected to all vertices in $\mathcal{V}$ (Guerrero-Bonilla et al., 2017, Proposition 1). Assign five distinct colors to nodes in $\mathcal{V}'$. Then there can be two cases

- For some $i \in \{1, 2\}$, $S_i \cap \mathcal{V}' = \emptyset$: Since each node in $\mathcal{V}'$ is connected to all vertices in $\mathcal{V}$. Then each node in S_i is adjacent to five distinct color nodes outside of their respective set allowing all of them to meet the condition in Definition 5.
- For some $i \in \{1, 2\}$, $S_i \cap \mathcal{V}' \neq \emptyset$: Without loss of generality, we can assume that $S_1 \cap \mathcal{V}' \neq \emptyset$. If $S_1 = \mathcal{V}'$ then all nodes in S_2 have five distinct color neighbours. If $|S_1 \cap \mathcal{V}'| < |S_1|$ then there would exist at least one node in S_1 or S_2 that has at least three distinct color nodes outside of its respective sets.

$\blacksquare$

B.4 Proof of Theorem 5.4

Proof: For a graph $\mathcal{G}$ which is 3-robust (all nodes are of the same color), for every pair of non-empty disjoint subsets S_1 and S_2 there exists a node v in $S_1 \cup S_2$ that has at least three neighbours outside of its respective set. Moreover, each vertex in $\mathcal{G}$ has at least three neighbours that are pair wise adjacent. By assigning color to the nodes in the graph such that no two adjacent nodes share the same color (proper coloring), v would always have three distinct color neighbours making $\mathcal{G}$ a mono-chromatic robust graph. ∎