This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2019.2917934, IEEE Transactions on Network and Service Management

Network Adaptations under Cascading Failures for Mission-Oriented Networks

Terrence J. Moore, *Member, IEEE*, Jin-Hee Cho, *Senior Member, IEEE*, and Ing-Ray Chen, *Member, IEEE*

Abstract—In the network science domain, a larger size of the giant component (i.e., the largest cluster of nodes) represents higher network resilience in terms of maximizing network availability in the presence of attacks. However, this does not necessarily represent how well the network provides promised services under attacks and/or failures. We aim to improve network resilience by introducing network adaptability (i.e., reconfiguration of a network topology), in addition to fault-tolerance. We develop a suite of strategies adopting processes from percolation theory, describing the process to percolate into a medium, for a tactical, mission-oriented network. This network is service-oriented, characterized by a number of task teams where each resource-restricted node aims to maximize resource utilization while completing multiple tasks without failure. We investigate how node failures can trigger overloads, leading to cascading failures. We consider various attack behaviors (infectious, non-infectious, random, or targeted) and analyze their effects. Through extensive simulations, we show the outperformance of the proposed adaptation strategy compared with the performance of the existing counterparts in terms of the size of the giant component, the utilization of resources, the number of alive task teams (or mission success ratio), and the adaptation cost for a large-scale, mission-oriented network under attack.

Index Terms—network resilience, fault tolerance, network adaptation, percolation theory, cascading failure.

1 Introduction

Correlated, cascading failures have been widely reported in large-scale telecommunication networks because of their significant impact in disrupting services. Typical examples include severe network disruptions introduced by either natural disasters or attacks by malicious activities, such as terrorist attacks or cyberattacks. The consequences of those disasters and/or attacks have affected many people's lives because resources are exhausted or due to the lack of assistance from limited rescue resources [34]. These examples also exemplify typical tactical situations in battlefields or disaster rescue operations that require high effectiveness and efficiency in allocating resources in order to provide seamless operational tasks or services in highly-deceptive, resource-restricted settings.

Maintaining high network resilience is critical in the presence of attacks and/or failures. To achieve this, a network should adapt to dynamics or sudden changes caused by the attacks or failures by responding to them in an agile manner. Network resilience has been substantially studied based on percolation theory that describes the behavior of connected nodes in a network, mimicking a fluid to percolate into a medium (see Section 2.2). In percolation theory, the key factor of network resilience is mainly fault tolerance with the large size of the giant component (i.e., the largest cluster size) with high network connectivity among remaining nodes. Hence, the key concern of past studies is to find the occupation probability as a critical value in various types of network models, including random graph networks, small-world networks, or scale-free networks [4, 38]. In these studies, a low value of the occupation probability, which means a high percolation threshold (i.e., a relative fraction of nodes to be removed before a phase transition showing a sudden drop of the size of the giant component) indicates high network resilience. However, this concept of network resilience only considers network connectivity-based fault tolerance without considering other aspects of network resilience.

Network resilience in general covers three aspects [13, 14, 33]: fault tolerance, adaptability, and recoverability. Most existing network science research considered only fault tolerance. In this work, we extend the concept of network resilience by embracing network adaptability, in addition to fault tolerance, in a mission-oriented (or service-oriented) network. In this context, nodes execute multiple tasks concurrently limited by their resource capacity and need to communicate with other nodes on the same team for task execution. We are interested in maximizing mission performance by using network adaptation strategies based on percolation theory. To do so, we propose a suite of adaptation strategies based on the process of site percolation (i.e., removing a node) or bond percolation (i.e., removing an edge) for mitigating the adverse effect of attacks or failures while maximizing mission performance. More specifically, our proposed network adaptation strategies aim at (1) maximizing the size of the giant component; (2) maximizing node resource utilization; (3) minimizing the cost of network adaptations (i.e., the number of shuffled edges); and (4) maximizing the number of active tasks that can continue execution despite attacks. We will limit the scope of this work to network adaptability and fault-tolerance and leave recoverability for our future research.

We make the following key **contributions** in this work:

- *Terrence J. Moore is with US Army Research Laboratory, Adelphi, MD, USA. Email: terrence.j.moore.civ@mail.mil. Jin-Hee Cho and Ing-Ray Chen are with the Department of Computer Science, Virginia Tech, Falls Church, VA, USA. E-mail: {jicho, irchen}@vt.edu.*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2019.2917934, IEEE Transactions on Network and Service Management

1) We extended the concept of network resilience beyond fault tolerance by considering network adaptability. As mentioned earlier, network resilience is defined in terms of the degree of a system's fault tolerance, adaptability, and/or recoverability [14] (see the detailed discussions on network resilience in Section 2.1), although most network resilience research in the network science mainly looked at the aspect of fault tolerance by measuring 'the size of the giant component' as the only indicator of network resilience. However, this may not be sufficient for service or mission-oriented networks, which aim to provide a requested service or achieve a given mission. In this work, we show how a network is configured in terms of a network topology (i.e., network adaptations to determine connections between nodes) that can make a more significant impact on service provision and/or quality under the service/mission-oriented networks.
2) We model a service or mission-oriented network based on a bi-partite network (i.e., two types of vertices exist such as an affiliation where a person belongs to an organization and his/her social network) in which a vertex is a group or a node. A node can execute multiple tasks by being associated with multiple groups, which requires direct communications between the node and member nodes in the same task group. Given this type of network structure, we investigate the impact of correlated, cascading failures (i.e., the process of a system being failed because the failure of a part of the system triggers that of other parts of the system because they are interconnected) due to overloaded nodes after a set of initial attacks are performed. We consider a set of "targeted attack" strategies and analyze the effects of various targeted attack strategies on network resilience of the network. The targeted attack strategies differ in the way the attacker targets a set of initial nodes to start the attack based on the node importance or criticality factors including degree, betweenness, resource, and number of assigned tasks.
3) We perform a thorough and comprehensive analysis to analyze the effects of node failure types (functional, overload, and security failure), attack processes (non-infectious vs. infectious), attack strategies (random vs. targeted), and adaptation strategies (random, minimum load, maximum load, or priority-aware load) on network resilience. In addition, we consider a service-oriented network characterized by a rich set of environmental and operational parameters including attack density, the maximum level of resources available, and the maximum number of groups a node can join. We compare our proposed adaptation strategies with a baseline model and existing counterparts for verification and validation.
4) Lastly, we demonstrate that the size of the giant component is not the only indicator to represent network resilience in a service-oriented or mission-oriented network. In particular, when the network is under attack, the number of surviving nodes in the largest connected component does not completely determine the mission performance in terms of the number of successfully completed tasks. That is, given the same number of non-compromised, active nodes, one network can provide better services than another. This leads to the critical question of what network characteristics can truly represent resilience against attacks. To investigate this, we examine the following network characteristics of a mission-oriented network executing our proposed adaptation strategies: (i) degree distribution; (ii) betweenness distribution; and (iii) clustering coefficient. Through this, we identify key network characteristics that can truly represent network resilience against attacks.

This work substantially extends from our preliminary work [12] in terms of the following aspects:

- We considered random attack behaviors and analyzed the effect of attack density on network resilience in our prior work [12]. In this work, we also considered targeted attack behaviors, including degree, betweenness, group, and resource attacks, and node/task behaviors, and analyzed their impact on the performance of the proposed scheme compared to other baseline counterparts.
- We also considered a more rich set of operation/environment parameters, including attack density, maximum available resources, and the maximum number of groups a node can join, as in a mission-oriented setting. These experiments and analyses are not presented in [12].
- In this work, we identified key network characteristics of a mission-oriented network following our proposed adaptation strategies that can truly represent network resilience against attacks. Identification of key network metrics that can represent network resilience is a critical contribution because it may provide an alternative metric to indicate network resilience beyond fault tolerance. This has not been addressed in our prior work [12] and any other prior work.

2 Background & Related Work

This section provides an overview of related work including: (1) network resilience; (2) percolation theory; and (3) network failures.

2.1 Network Resilience

Network resilience has been studied in many disciplines. Network resilience is commonly defined based on how remaining nodes are connected when faults or attacks are applied in a network, measuring communication reliability [15, 35]. Recently, Barabási [4] defined network resilience as the network's adaptability under internal or external errors that can change the network structure in order to provide normal services. The common aspect of these definitions indicates that when the network is well connected, it provides proper network services.

Most network science research has studied network resilience to indicate the degree of fault-tolerance in a network which is measured based on the size of the giant component. Percolation theory, discussed below, has been used to determine network breakdown point [2, 8, 52]. On the other hand, computer scientists investigate network resilience in a broader sense by considering network trustworthiness [13, 14, 33]. In particular, we observe the concept of network resilience in terms of fault tolerance,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2019.2917934, IEEE Transactions on Network and Service Management

adaptability, and recoverability via an in-depth literature survey of various disciplines [14, 33]. To be specific, network resilience is defined as the degree of a system being (1) functioning properly by providing normal services under the presence of failures and/or attacks (i.e., fault tolerance); (2) adapting system configurations to sudden changes (e.g., failures or attacks) for maintaining a normal system state (i.e., adaptability); and (3) quickly recoverable from any failure and/or attacks (i.e., recoverability). Other studies also considered network resilience in terms of tolerance and trustworthiness [46], adaptability or reconfigurability [10, 11, 23, 28, 29, 35, 43], fault tolerance [2, 8, 52], and recoverability [30, 40, 45]. Ganin et al. [20] proposed models to enhance resilience and efficiency in transportation networks, inspired by percolation theory, where the resilience considers recoverability of urban road systems. Kryven [27] proposed a generic analytic theory describing the effect of color-dependent bond percolation on the network structure and sizes of the giant component. Rocca et al. [41] proposed a strategy to avoid or mitigate a complete collapse of a system consisting of interdependent networks facing cascading failures by considering a reconnection probability reflecting recoverability. Wang et al. [48] provided a probabilistic solution of the site percolation based on generating functions for a wireless sensor network with community features. Yuan et al. [54] studied k-core percolation where a node fails when losing connections based on given threshold k in terms of network stability under random, localized, or targeted attacks in random and scale-free network models.

Network adaptability refers to a network's capability to adjust the network topology such as adjusting edges or distributing redundant information to seamlessly deal with sudden system or environmental changes [28]. Network adaptability has been studied in a sense that the effectiveness of the response to abnormal states is closely related to how quickly malicious behavior is reliably and efficiently detected [28, 35]. The network must also be capable of implementing appropriate defense mechanisms to handle sophisticated, diverse attack approaches [10, 11]. Network availability has been investigated to represent the degree of network resilience in disaster management [23, 43].

With respect to the above cited works, our work follows the network science approach in terms of utilizing percolation theory to study network behaviors under attacks. However, unlike network science research which traditionally considers network resilience as fault tolerance, we extend the concept of network resilience by embracing network adaptability, in addition to fault tolerance. Network adaptability thus far has not been studied based on percolation theory under cascading failures caused by targeted attacks.

2.2 Percolation Theory

Network resilience is frequently studied using percolation theory by measuring *the giant component*. This metric is commonly employed as a main metric to represent the degree of network resilience, mainly measuring network connectivity. The effect of various attack types, such as random attacks or targeted attacks, are investigated in this line of network resilience study based on percolation theory [25, 33]. Site percolation and bond percolation refer to the processes of eliminating nodes and edges, respectively. The effect of the percolation on the size of the giant component depends on the attacker's selection of an initial set of nodes or edges that would be removed from the network after attacks [36, 37].

Most network science approaches were interested in identifying a critical threshold of percolation as an indicator of network resilience [4, 38]. Different node or edge removal selection rules have been developed to model targeted attacks based on a node's centrality metric, such as degree or betweenness. Recent work investigated the effect of localized attacks (i.e., an epidemic process that compromises nodes initially in a localized region of the network) in order to obtain a critical percolation threshold [44].

In contrast to the network science approaches, computer scientists studied the concept of network resilience to manage network services. For example, epidemic attacks leading to cascading failures have been examined using percolation theory to identify a critical occupation probability (i.e., how many nodes are existing in a network) [22, 47], to investigate the size of the giant component in cyber-physical systems [26], and to develop a cost-effective method of immunization in an enterprise network [28]. Franceschetti et al. [17] leveraged percolation theory to obtain a lower bound of the bit rate per source-destination pair in wireless sensor networks. Chau et al. [9] found an optimal setting of enabling robust multi-path routing under networks or node outages. However, neither work cited above dealt with failures caused by cyberattacks. Although many works above have addressed network resilience by considering various types of attack behaviors, network resilience has been predominantly studied based on fault tolerance.

2.3 Network Failures

Network failures can be caused by the following aspects [33]: connectivity-based, cascading-based, and functionality-based network failures. Although we categorize the network failures with these three categories, they are interwoven to each other because nodes can become overloaded due to disconnectivity with other nodes or other nodes' functional failure, which may ultimately lead to cascading failures as well.

A *connectivity-based network failure* occurs when the network cannot maintain a certain portion of connected, active nodes. This type of failure is often studied using percolation theory to characterize the collapse of the giant component after a substantially large portion of nodes or edges are eliminated. The process of node removals is determined by the attack model, such as random attacks or targeted attacks, and it occurs on popular network models, such as the Erdös-Rényi random network [16], the Barabási-Albert scale free network [5], or the Watts and Strogatz small-world network [51].

A *cascading-based network failure* occurs when the failure of one or more nodes causes other nodes to fail, which then can cause the failure of other nodes, and so on [47]. This process is often considered as an epidemic process mimicking the transmission of a contagious disease. In addition to diseases, epidemic models have been applied to investigate failures in financial institutions, power grids, and communication networks. It has also been applied to describe the spread of malware or node capture or compromise in the cybersecurity domain [6]. Many factors impact cascading

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2019.2917934, IEEE Transactions on Network and Service Management

failures in a network; these factors include the behaviors of node neighbors, the failure impact region, and the failure propagation probability (i.e., an infection rate) [53].

A *functionality-based network failure* refers to the network failure when a large portion of nodes (or components) malfunction or become compromised. The result of this failure is that normal network services can no longer be provided. Freixas and Pons [19] studied the impact of functionality-based network failure in terms of the criticality and/or interdependency of nodes in the network. Often times, a node's criticality is measured by various types of centrality metrics [38]. Xu and Wang [53] also indicated cascading failures as the key effect of the functionality failures of nodes. Overloaded failures due to some of the nodes malfunctioning [32] can lead to functionality-based network failure as well. In addition, a network with multiple subcomponents (or modules) can face cascading failure [21, 39] because some subcomponents are shared by multiple nodes. A node's failure can introduce cascading failures because it can affect the overall service provision of its associated subcomponents [3].

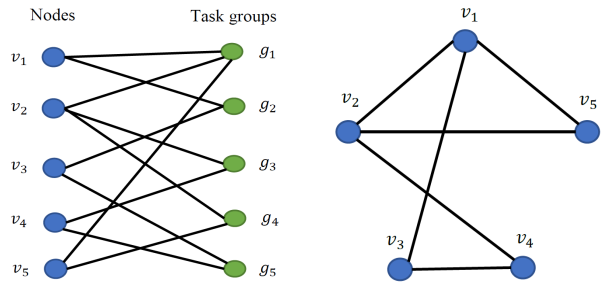
In our work, in order to perform a thorough analysis of our proposed adaptation strategies for network resilience, we consider all network failure types discussed above caused by various types of node failures (functional, overload, and security failure), attack processes (non-infectious vs. infectious), and attack strategies (random vs. targeted).

3 System Model

3.1 Network Model

A tactical mission-oriented network is a network wherein a number of entities or nodes are required to collectively accomplish a common mission consisting of multiple tasks. A typical example includes a military mission team or a rescue team executing multiple tasks where each task group has workload to process while some coordination between task groups is needed to successfully complete the common mission [7, 50]. In this mission team scenario, it is critical to maintaining connectivity between nodes for effective communications within a same group and/or across task groups. At the same time, as a node may participate in multiple task groups, the node should be capable of handling multiple tasks assigned without failure. Therefore, both communication connectivity between nodes across task groups and the node composition of each task group are critical factors, leading to a successful mission completion.

We model a mission-oriented network by using a bi-partite graph (or affiliation network), as exemplified in Fig. 1 (a). One set of vertices holds the tasks (or groups) the network is designed to execute while the other set of vertices holds the nodes that are assigned to various tasks. Fig. 1 (b) projects the bi-partite network in Fig. 1 (a) onto the network where a vertex is a node. This projection shows more directly which nodes are cooperating on some task and can potentially impact each other; however, the projection abstracts the details of which task or tasks a pair of nodes are cooperative. The bi-partite network is useful for keeping track of which nodes are assigned to which tasks and the one-mode projection is useful for keeping track of which nodes can affect a given node.



(a) *Bi-partite network with nodes and nodes' associated task groups.* (b) *Network topology based on shared affiliated groups.*

Fig. 1: Bi-partite network topology with nodes associated with multiple task groups.

We consider a network with a fixed number N of nodes and a fixed number N_g of tasks. Nodes are assigned to multiple task groups, where each group, denoted by g_k, provides a service k, for $k = 1, \ldots, N_g$. The set of nodes assigned to the group g_k is denoted by N_{g_k}. The set of groups that node i is assigned to is denoted by $\mathcal{M}_i$, for $i = 1, \ldots, N$. The topology of the network can change due to the failure of certain nodes (see Section 3.2) and due to changes in the assignment of nodes to tasks (i.e., edge adjustments) from applying the proposed network adaptation strategies, as shown in Section 4. Hence, the nodes assigned to the various tasks can change. For example, a node may not have enough resource to meet some task's workload demands, as described below, and leave the group. Alternatively, a node with available resource might be recruited to join another task to lessen the workload burden on existing task group nodes. It is also possible for tasks to fail, e.g., when no node is a member of the respective task group (see the 'group failure conditions' in Section 3.3). To emphasize this temporal aspect, we shall denote these sets of nodes and sets of groups as dependent on time t, i.e., as $N_{g_k}(t)$ and $\mathcal{M}_i(t)$, except where it inconveniences the expression.

A task group will be characterized by a profile as:

$$\Pr[g_k(t)] = [\mathrm{ID}(k), N_{g_k}(t), W_{g_k}, CR_{g_k}], \tag{1}$$

where the group's identifier is $\mathrm{ID}(k)$, the set of nodes assigned to the group at time t is $N_{g_k}(t)$, the workload required for the task is W_{g_k}, and the level of task criticality is CR_{g_k} affecting the task priority. This workload per group member, $w_{g_k}(t)$, will be equally distributed among the nodes assigned to the group, i.e.,

$$w_{g_k}(t) = \frac{W_{g_k}}{|N_{g_k}(t)|}. \tag{2}$$

Note that the workload for a group depends on the number of nodes assigned to that group. We assume that the workload, W_{g_k}, is constant across task groups. Higher CR_{g_k} represents a higher importance of group g_k where CR_{g_k} can be categorized high ($CR_{g_k} = 3$), medium ($CR_{g_k} = 2$), and low ($CR_{g_k} = 1$). CR_{g_k} is considered when the mission success ratio is estimated based on Eq. (7) [49]. The task criticality is uniformly selected at random for given task groups.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2019.2917934, IEEE Transactions on Network and Service Management

A node i will be characterized by its profile, described as:

$$\Pr[v_i] = [\text{ID}(i), \mathcal{M}_i(t), r_i], \tag{3}$$

where $\text{ID}(i)$ is node i's ID, $\mathcal{M}_i(t)$ is the set of tasks node i is assigned to at time t, and r_i is node i's maximum resource level. Note that r_i refers to i's maximum level to represent the resources associated with computation and communication. Node i's resource level will change where it can be represented by two aspects: the resource used and non-used, denoted by (ur_i, nur_i), respectively, where $r_i = ur_i + nur_i$. The total workload node i has at time t is given by:

$$\mathcal{W}_i(t) = \sum_{g_k \in \mathcal{M}_i} w_{g_k}(t), \tag{4}$$

where the workload per group member $w_{g_k}(t)$ is given in Eq. (2). Because of the workload requirement and the limited resource capacity for each node, then node i will be overloaded when $\mathcal{W}_i(t) > r_i$. Conversely, when $\mathcal{W}_i(t) < r_i$, then the node is underutilized. The desired network state aims to maximize the utilization of resources, i.e., minimize $r_i - \mathcal{W}_i(t) \geq 0$, while also maintaining network connectivity.

3.2 Node Failures

Three types of node failures can occur in our system model:

- *Functional failure*: A functional failure may result from physical destruction or malfunction of the node. The primary adverse effect of the failure is that the node can no longer provide the service it once provided. A secondary adverse effect is that its neighboring nodes, who were cooperating with the node on any ongoing tasks, risk being overloaded from the transfer of the workload demand previously met by the currently failed node.
- *Overload failure*: An overload failure results from an excessive workload placed on the node from a task service due to the sudden departure of one or more nodes. The departure of a neighboring node may be because of a failure or a neighboring node implementing an adaptation strategy due to overloading (see Section 4.2). A node is overloaded when the node's resources can no longer satisfy the workload requirements of the assigned tasks, i.e., when $\mathcal{W}_i(t) > r_i$. While the node can no longer provide the services it once provided, it is possible to still provide some level of service in the network, e.g., for fewer tasks. Any task group the node leaves may trigger cascading failures of its neighboring nodes in that task.
- *Security failure*: A security failure occurs when the node is directly compromised and captured by attackers. The attack may be from an initial (random or targeted) attack on the node originating from outside the network or from a neighboring node that has itself been compromised. This implies that a compromised node from a security failure can compromise its neighboring nodes. If the compromise is detected, then the node can be eliminated from the network, e.g., via rekeying (or changing a group key for each task). Clearly, a compromised node may not provide a proper service to its tasks. It can also compromise neighboring nodes, introducing the security failure to new tasks. Both scenarios may cascade through the network.

3.3 Group Failures

A group fails when it has no members (or nodes). As discussed in Section 3.2, nodes assigned to the task can fail via a functional or security failure. An overload leads to an increased workload for the remaining nodes in the task service group. A compromise leads to an increased risk of the remaining nodes being compromised or from an overload when the compromised node is detected and isolated. Either scenario increases the likelihood of the remaining nodes being overloaded. Our proposed adaptation strategies to increase resource utilization in response to these potential overloads are discussed in Section 4.

3.4 Cascading Failures

In this work, two attack processes are considered where they can lead to percolation-based cascading failures:

- *Non-infectious attacks*: In practice, non-infectious attacks are observed as the forms of a physical destruction of the part of a system (e.g., physical damage to cyber-physical systems [1]), non-functional servers attacked by denial-of-service (DoS) attacks (e.g., outside attackers performing DoS attacks [31]), or an unauthorized access by an inside attacker who illegally obtained access credentials [31]. The aspect of this attack type is that although the attack itself makes a given node completely down, there is no replicating infection towards other nodes. In our work, this non-infectious attack is modeled as follows. The attacker attacks a fraction ϕ of the nodes in the network through functional failures due to physical destruction or malfunction. The surviving nodes in the network experience an increased workload as a result, leading to overloading among the neighbors of the failed nodes, which may cascade through the network. As the fraction ϕ of failed nodes increases, it eventually reaches a threshold that breaks the network completely. This is a classic site percolation scenario [38].
- *Infectious attacks*: Unlike the scenario above, these nodes are compromised and can infect other nodes. Typical example scenarios include the spread of malwares or viruses. Botnets can spread malwares or viruses via mobile devices. A mobile device can use a mobile malware such as a Trojan horse, playing a role of a botclient to receive a command and control from a remote server [31]. In this work, we model this infectious attack as follows. A fraction ϕ of nodes are selected by the attacker to fail. We model this infection by an epidemic process based on the Susceptible-Infected-Removed (SIR) model [38]. Nodes in an infected state (I) can compromise nodes in the susceptible state (S) with rate β. The system includes a detection capability (e.g., an intrusion detection system or namely IDS), which can remove compromised nodes with rate γ into a quarantined or removed state (R), without recovery. This rate can be interpreted as an average delay of $1/\gamma$ to the detection and removal of a compromised node. This quarantining or removal can be accomplished, for example, by changing the secret key (rekeying) of each task group for which the compromised node is a member. The removal of the edges connected to the detected, infected node can be modeled by bond percolation. Note that this removal incurs a cost (e.g., cost to change a key) involved with the computation and communication cost

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2019.2917934, IEEE Transactions on Network and Service Management

for the tasks. To account for this cost, we estimate the adaptation cost based on the number of edges adjusted between the original network topology and the adapted network topology (see Section 5.1). This removal has the same adverse effect as that of the failed node, i.e., it increases the workload of the surviving task group nodes associated with the removed node increasing the potential for cascading failures that can be caused by nodes that are overloaded.

These two types of attacks (i.e., non-infectious or infectious) can be performed randomly or with a particular targeted entity. In practice, the attack type can be random or targeted depending on an attacker's intent. A random attack is the most common intentional threat with the aim of compromising people's software by spreading malwares, viruses, or worms. A targeted attack is to attack a particular entity, which has vulnerabilities or more value causing more disastrous impact on a system (e.g., a Web server) [42]. In this work, we consider a random attack by selecting a victim node randomly while choosing the victim node with high centrality or power to increase the impact of the performed attack (see Section 5.2.2).

Each node may learn about a previous attack so it can be immune to the past attack. However, considering a node's learning towards attacks is beyond the scope of this work and will be examined in our future work.

4 Network Adaptation Strategies

In this section, we first describe basic adaptation operations based on percolation process and then detail our proposed adaptation strategies. The operations include the removal of nodes and the removal and addition of edges. The strategies are motivated by the situations in which a task group needs to add a node so as not to be overloaded and a node needs to drop a task group so as not to be overloaded.

4.1 Adaptation Operations based on Percolation Process

The adaptation operations considered in this work include the following:

- *Removal of a compromised node*: A compromised member node of a task group can infect other member nodes in the same task group. These other nodes can then infect nodes in other tasks. In order to limit the network vulnerability and prevent the spreading of infection to other nodes (and tasks), a compromised node once detected must be isolated from the network. This is done by removing all edges of this compromised node, thereby removing this compromised node from every task group it was a member.
- *Removal of edges*: Two nodes are connected by an edge only if they are members of at least one common task group. The removal of an edge of two nodes indicates that they are no longer associated in any common task group. When a node is overloaded, it needs to reduce its workload by leaving a group. When this node leaves a task group, all the edges of this node with other nodes in the same group will be removed. However, if this node and another node are still associated with a separate task group, then the edge between those two nodes remains.
- *Addition of edges*: When a node has sufficient resources to take on additional workload, the node can join an existing task group. By joining a new group, this node establishes edge connectivity with all other members currently in the group if those edges did not exist already from membership in another group.

Algorithm 1 FindGroup

$i \leftarrow$ ID of an overloaded node
$M_i \leftarrow$ a set of groups to which node i belongs
$nur_i \leftarrow i$'s non-used, remaining resource
$w_{g_k} \leftarrow$ group g_k's per-node-workload
procedure FINDGROUP(i, M_i)
  for all group $g_k \in M_i$ **do**
    if $\mathcal{W}_i(t) - w_{g_k} \leq r_i$ **then**
      if `random-A` **then**
        groupID $\leftarrow$ a random j in M_i
      else if `min-LA` **then**
        groupID $\leftarrow j$ in M_i with maximum w_{g_k}
      else if `max-LA` **then**
        groupID $\leftarrow j$ in M_i with minimum w_{g_k}
      else if `pa-LA` **then**
        groupID $\leftarrow j$ in M_i with the lowest CR_{g_k}
      else // no adaptation
        groupID $\leftarrow 0$
      end if
    end if
  end for
  if groupID > 0 **then**
    remove edges between members in group $g_{groupID}$ and node i
  end if
end procedure

Algorithm 2 FindNode

$\mathcal{V} \leftarrow$ a vector of nodes v_i for $i = 1 \cdots N$ in a network
$k \leftarrow$ ID of an overloaded group
$M_i \leftarrow$ a set of groups i belongs to
$nur_i \leftarrow i$'s remaining resource
$w_{g_k} \leftarrow$ group g_k's per-node-workload
procedure FINDNODE(k, $\mathcal{V}$)
  for all $v_i \in \mathcal{V}$ **do**
    if $nur_i \geq w_{g_k}$ **then**
      if `random-A` **then**
        nodeID $\leftarrow$ a random v_i in $\mathcal{V}$
      else if `min-LA` **then**
        nodeID $\leftarrow v_i$ with maximum nur_i
      else if `max-LA` **then**
        nodeID $\leftarrow v_i$ with minimum nur_i
      else if `pa-LA` **then**
        if $CR_{g_k} == 3$ **then** ▷ high criticality task
          nodeID $\leftarrow v_i$ with maximum nur_i
        else if $CR_{g_k} == 2$ **then** ▷ mid criticality task
          nodeID $\leftarrow v_i$ selected randomly
        else $CR_{g_k} == 1$ ▷ low criticality task
          nodeID $\leftarrow v_i$ with minimum nur_i
        end if
      else // no adaptation
        nodeID $\leftarrow 0$
      end if
    end if
  end for

  if nodeID > 0 **then**
    add edges between members in group g_k and node $nodeID$
  end if
end procedure

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2019.2917934, IEEE Transactions on Network and Service Management

4.2 Adaptation Strategies

When a node is detected as functionally failed (i.e., suffering a functional failure) or compromised (i.e., suffering a security failure), it is removed from the network by following the process of site percolation, cutting all the edges of the node. The network topology must adapt to mitigate the degree of vulnerability from cascading failures. In this work, we devise two adaptation algorithms that determine how a node would leave a group (`FindGroup`) and how a node would join a group (`FindNode`), respectively.

- `FindGroup`: When a node is overloaded, it will make the selection of a group it wants to leave to avoid being overloaded by keeping $\mathcal{W}_i(t) \leq r_i$.
- `FindNode`: When a group detects a member node is leaving and there are overloaded member nodes in the group, the group will recruit a node to be a member of the group to help existing members reduce their per-node-workload, $w_{g_k}(t)$.

We consider three network adaptation strategies for executing `FindGroup` and `FindNode`:

1) Random Adaptation (`random-A`): (i) `FindGroup`: An overloaded node *randomly* selects a group to depart; and (ii) `FindNode`: an overloaded group *randomly* selects a node to draft as a member such that the given group can sufficiently reduce the workload of the overloaded node and the recruited node can deal with the workload the overloaded group assigns.
2) Minimum Load Adaptation (`min-LA`): (i) `FindGroup`: An overloaded node selects *a group with maximum workload* to depart; and (ii) `FindNode`: an overloaded group selects a node that has the maximum resource remaining (i.e., nur_i) as a new member such that the task group can sufficiently reduce the workload of other overloaded member nodes and the recruited node can deal with the workload the overloaded task group assigns. This adaptation aims at minimizing adaptation cost and maximizing the size of the giant component. On the other hand, this strategy places less emphasis on resource utilization.
3) Maximum Load Adaptation (`max-LA`): (i) `FindGroup`: An overloaded node selects *a group with minimum workload* to depart; and (ii) `FindNode`: An overloaded group selects a node that has minimum remaining resource (i.e., nur_i) as a member such that the group can reduce the workload of other overloaded nodes and the recruited node can still handle the workload from the overloaded group. This adaptation's goal is to *maximize* resource utilization with less emphasis on preserving the giant component size or minimizing adaptation cost.
4) Priority-Aware Load Adaptation (`pa-LA`): This scheme is devised to reflect the concept of the different importance of a task assigned to each group as an existing approach [49]. In order for this scheme to be applied in the context of mission-oriented networks concerned in this work, we implemented `pa-LA` as follows: (i) `FindGroup`: An overloaded node selects *a group with a lowest task criticality*, CR_{g_k}, among a candidate pool (i.e., a set of groups that can be dropped to make the node not overloaded) to depart; and (ii) `FindNode`: When an overloaded group has high criticality (i.e., $CR_{g_k} = 3$), it follows `min-LA`; for the overloaded group with $CR_{g_k} = 2$, it follows `random-A`; and for the overloaded group with $CR_{g_k} = 1$, it uses `max-LA`. The rational behind `pa-LA` is to maximize the mission success ratio (see Eq. (7)) while maximizing resource utilization.

We summarize the four adaptation strategies for executing `FindGroup` and `FindNode` in Algorithms 1 and 2. We will analyze the performance of the three adaptation strategies in Section 5, in comparison with that of baseline counterparts.

5 Results and Analysis

5.1 Metrics

We measure network resilience by the following performance metrics:

- *Size of the giant component* ($\mathcal{S}_g$): This is a traditional metric to represent network resilience (or robustness) in percolation theory [38] after attacks. This metric is estimated based on the total number of alive nodes over the total number of nodes initially deployed in a network. A higher $\mathcal{S}_g$ represents a higher degree of network connectivity.
- *Resource utilization ratio* ($\mathcal{U}_R$): This metric measures how efficiently resources are utilized in the network and is calculated by:

$$\mathcal{U}_R = \frac{\sum_{i=1}^{N} ur_i}{\sum_{i=1}^{N} r_i} \tag{5}$$

  where ur_i refers the resource used by node i during the mission period while r_i is the resource level initially given to node i. A higher resource utilization ratio means a better utilization of network resources.
- *Adaptation cost* ($\mathcal{C}_A$): This metric measures the cost associated with the network topology change in terms of the number of edges changed after a network adaptation strategy is applied in response to node failures due to attacks. This cost is obtained by:

$$\mathcal{C}_A = \frac{sum(|A-B|)}{sum(A+B)} \tag{6}$$

  where A is the original adjacency matrix and B is the resulting adjacency matrix after an adaptation strategy is applied. $sum(|A-B|)$ means the sum of the differences between A and B while $sum(|A+B|)$ indicates the sum of the additions between A and B. This formula determines the proportion of edge additions and removals normalized by the number of edges in the original network and the final network. A lower cost implies a higher efficiency.
- *Number of active task groups* ($\mathcal{N}_A$): This metric counts how many active task groups are successfully executed despite the presence of attacks. This metric captures network resilience in terms of the network's ability to provide normal, proper services against cascading failures caused by attacks. A higher number of this metric indicates a higher mission performance.
- *Mission success ratio* ($\mathcal{R}_s$): This metric measures how a given mission consisting of N_g tasks has been successfully completed and is estimated based on task criticality where

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2019.2917934, IEEE Transactions on Network and Service Management

a more critical task with higher CR_{g_k} is weighed more as follows:

$$\mathcal{R}_s = \sum_{k=1}^{N_g} \frac{\left[R_k \times CR_{g_k}\right]}{\sum_{k=1}^{N_g} CR_{g_k}} \quad (7)$$

where N_g is the total number of task groups available and R_k is a boolean variable indicating whether group k successfully completed its task, with 1 meaning yes; and 0 otherwise.

5.2 Experimental Setup

5.2.1 Initial Network Deployment

We consider multiple dynamic task teams given a common mission where the given mission-oriented tactical network consists of heterogeneous nodes, including sensors, robots, unmanned vehicles or other devices, dismounted soldiers or first response personnel or manned vehicles carrying sensors or handheld devices [7, 50]. We consider a medium-sized mission-oriented network, which is common in a military mission context with a total of $N = 200$ members where each member can join task groups to concurrently execute multiple tasks in the range of $[0, n_g]$ for $n_g = 10$. Each tactical group's workload is assigned differently in the range of $[0, W_g]$ for $W_g = 10$, which is a normalized workload, to reflect heterogeneous characteristics of each tactical task. Due to the nature of high hostility and potential security vulnerability in the given tactical environment, we consider an initial seeded attacker with 10% out of the total number of nodes but vary its ratio to investigate its impact on the performance of considered schemes, and consider a node's vulnerability to be compromised with probability $\beta = 0.3$. We assume that an IDS is in place where its detection capability is $\gamma = 0.9$ generating 10% (i.e., $\phi = 0.1$) of false positives or false negatives, which is fairly high in order to conservatively consider the performance of the proposed schemes under high hostility. To ensure high validity of the experimental results, we also ran our simulation $N_r = 1000$ times for each data point shown in our experimental results.

The initial task assignment is implemented as follows. For each node i an initial number, $n_{i,g}$, from the integer range $[1, n_g]$ is randomly chosen, then $n_{i,g}$ of the N_g tasks or group IDs are randomly selected, and node i is assigned to these tasks. After this task assignment is completed for every node, then the workload distribution per node is calculated for each task, each node's workload demand for the initial network is calculated, and the nodes are given a sufficient level of resources to deal with the workload demands. For example, node i has workloads given by the set of task groups it is affiliated with, denoted by $\mathcal{M}_i(0)$, according to Eq. (2) and its total workload is calculated as $\mathcal{W}_i(0)$ according to Eq. (4). An adequate resource for node i must satisfy $r_i > \mathcal{W}_i(0)$. We set $r_i = (1 + \alpha)\mathcal{W}_i(0)$, with $\alpha > 0$ providing node i with an extra portion α of resources.

5.2.2 Attack Processes and Strategies

We consider two types of attack processes:

- **Non-Infectious attacks** (NIA) cause nodes to fail due to functional failure (see Section 3.2), so they do not compromise their neighboring nodes. It follows the site percolation process (see Section 3.4).
- **Infectious attacks** (IA) cause nodes to fail due to security failure (see Section 3.2). Also compromised nodes can further compromise their neighboring nodes. It follows the epidemic process based on the Susceptible-Infected-Removed (SIR) model (see Section 3.4).

The impact of IA is more powerful than NIA. However, both attacks can introduce cascading failures due to overloaded nodes caused by attacks/failures.

Under either NIA or IA, we consider two attack strategies by which a fraction ϕ of nodes are initially selected to attack:

- **Random attacks** select nodes to fail or compromise at random. Detected failed/compromised nodes are being removed from the network.
- **Targeted attacks** select nodes based on the following importance/criticality criteria: (1) the highest degree [24] (called *degree attacks*); (2) the highest betweenness [18] (called *betweenness attacks*); (3) the highest number of groups a node is involved with (called *group attacks*); and (4) the highest level of a node's resource (called *resource attacks*).

5.2.3 Network Adaptation Strategies

After attacks are applied following site percolation as above, we study the performance of adaptation strategies, including `random-A`, `min-LA`, and `max-LA`, as described in Section 4.2, compared to no adaptation (`non-A`). The default design parameter values are listed in Table 1. The initial network deployment as described in Section 5.2.1 based on these parameter values has more than 10,000 edges with the average node degree being approximately 100, indicating a network that is densely connected. The results are collected based on 1000 times of simulation runs.

5.3 Performance Results & Analysis

In this section, we compare the performance of the proposed adaptation strategies and baseline counterparts. In particular, Sections 5.3.1 and 5.3.2 show the comparative performance analysis under various attack strategies (random vs. targeted attacks) and attack processes (non-infectious vs. infectious attacks) when homogeneous task groups with an equal importance (i.e., no task criticality considered) are given. Section 5.3.3 discusses the comparative performance analysis when heterogeneous task groups with a different importance are considered under random attacks. In this section, we consider a priority-aware load adaptation (`pa-LA`) to investigate its effect on mission success ratio defined in Eq. (7).

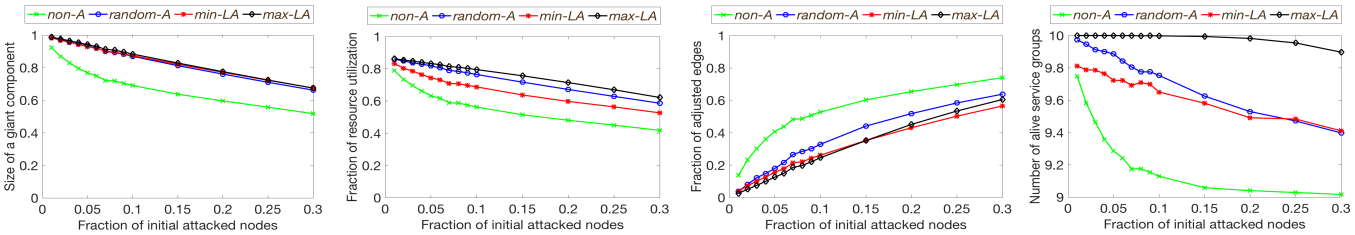
5.3.1 Performance Analysis under Random Attacks

Results under Non-Infectious Attacks: The effect of the initial proportion, ϕ, of randomly-selected failed nodes when attacks are non-infectious for the different adaptations are shown in Fig. 2. Since these are non-infectious attacks, the node failures are primarily due to the initial failures (i.e., the initial proportion ϕ) and the nodes overloaded from increased workloads caused by other failures. Therefore, the fraction of nodes in the giant component, $\mathcal{S}_g$, will be bounded above by $1-\phi$, as in Fig. 2 (a). Notice that there is a significantly larger $\mathcal{S}_g$ when any adaptation strategy is used, but there is no significant difference in terms of $\mathcal{S}_g$ between them. This explains that the size of the giant component is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2019.2917934, IEEE Transactions on Network and Service Management

TABLE 1: Key parameters, their meanings, and their default values.

Param.	Description	Val.
N	Total number of nodes in a network	200
N_g	Total number of groups available	10
n_g	Maximum number of task groups each node can join, in which n_g, as a task ID, is randomly chosen in the range of $[1, N_g]$ as an integer	5
ϕ	% of initial seeding attacks out of N	10%
α	% of the maximum level of the extra resource assigned for each node	30%
β	Probability that a node is compromised	0.3
γ	Probability that a compromised node is detected and accordingly eliminated	0.9
W_g	A group's maximum workload in which the workload for group g_k, denoted by W_{g_k}, is randomly chosen in the range of $[1, W_g]$ as a real number	10
N_r	Number of simulation runs	1000



(a) Size of the giant component (b) Resource utilization ratio (c) Adaptation cost (d) Number of alive service groups

Fig. 2: Performance comparison of adaptation strategies under different attack density, ϕ, when attacks are non-infectious.

not the only indicator representing network resilience and cannot explain how the resources of remaining nodes are used to provide normal, proper services.

Fig. 2 (b) shows how different ϕ affects node resource utilization, $\mathcal{U}_R$. Comparing with the results in Fig. 2 (a), it is evident that a higher giant component size does not show a clear relationship with a higher resource utilization of nodes. We observe the following performance order in terms of $\mathcal{U}_R$: `max-LA` $\geq$ `random-A` $\geq$ `min-LA` $\geq$ `non-A` (no adaptation). Based on Figs. 2 (a) and 2 (b), we can infer that the size of the giant component cannot fully explain the performance in resource utilization or mission performance (e.g., a number of alive service groups), which can partly represent the degree of network resilience as well.

The effect on the adaptation cost, $\mathcal{C}_A$, estimated by the fraction of edges adjusted, as in Eq. (6), is demonstrated in Fig. 2 (c). The performance order with regard to $\mathcal{C}_A$ is: `min-LA` $\geq$ `max-LA` $\geq$ `random-A` $\geq$ `non-A`. Note that the superior performance of `min-LA` and `max-LA` in giant component size, $\mathcal{S}_g$, and resource utilization, $\mathcal{U}_R$, does not require a high adaptation cost, $\mathcal{C}_A$. Finally, the effect on the number of active tasks, $\mathcal{N}_A$, is shown in Fig. 2 (d). The performance order of the adaptation strategies is: `max-LA` $\geq$ `random-A` $\geq$ `non-A` $\geq$ `min-LA`. `max-LA` evidently performs better than the other schemes in $\mathcal{N}_A$. `min-LA` does not perform better than `random-A` in terms of $\mathcal{N}_A$. Overall, `max-LA` performs the best among all for all metrics under non-infectious attacks where the effect of ϕ is restricted to functional failures without infections and with limited overloaded failures.

Results under Infectious Attacks (IA): Fig. 3 shows the effect of ϕ on the four metrics under infectious attacks when different adaptations and non-adaptation strategies are applied. The effect of ϕ on the size of the giant component, $\mathcal{S}_g$, as shown in Fig. 3 (a) is similar to the non-infectious scenario, shown in Fig. 2 (a), in that adaptation strategies show higher effectiveness than non-adaptation counterparts while performing almost equivalently among themselves. For resource utilization, $\mathcal{U}_R$, shown in Fig. 3 (b), among all adaptation strategies (`random-A`, `min-LA`, and `max-LA`) the best performer is `max-LA` and the worst is `min-LA`. We observe that `random-A` performs quite well under a hostile environment in which ϕ is high.

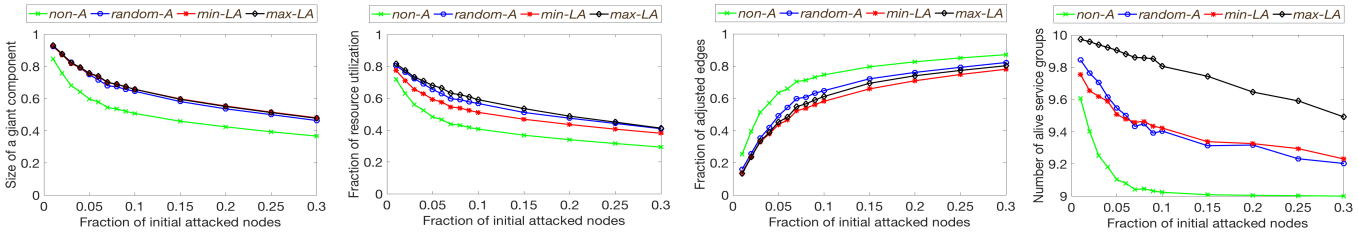
The effect of ϕ on the adaptation cost, $\mathcal{C}_A$, is shown in Fig. 3 (c). Similar to the non-infectious scenario, `min-LA` and `max-LA` incur less cost than `non-A` and `random-A`. As discussed in Section 4, `min-LA` focuses more on maintaining high connectivity with consideration of adaptation cost, so there is no surprise that it generates the greatest size of the giant component with the least adaptation cost. The effect of ϕ on the number of active tasks, $\mathcal{N}_A$, is shown in Fig. 3 (d). `max-LA` outperforms all other adaptation strategies although there is a performance degradation under infectious attacks compared to under non-infectious attacks.

5.3.2 *Performance Analysis under Targeted Attacks*

In this section, we investigate the effect of targeted attacks (see Section 5.2) on network resilience. In particular, we analyze the effect of targeted attack types (i.e., degree, betweenness, group, and resource attacks) on performance of `min-LA` and `max-LA`. Again we show the performance of `min-LA` and `max-LA` for both non-infectious attacks (NIA) and infectious attacks (IA).

After examining the effect of various targeted attack types on the four metrics in Section 5.1, we observe that except the number of alive groups metric ($\mathcal{N}_A$), other performance metrics, including the size of the giant component ($\mathcal{S}_g$), resource utilization ratio ($\mathcal{R}_U$), and adaptation cost ($\mathcal{C}_A$) do not show much sensitivity on different targeted attack types for either `min-LA` and `max-LA`. Therefore, below we report our findings in more detail for $\mathcal{N}_A$, which

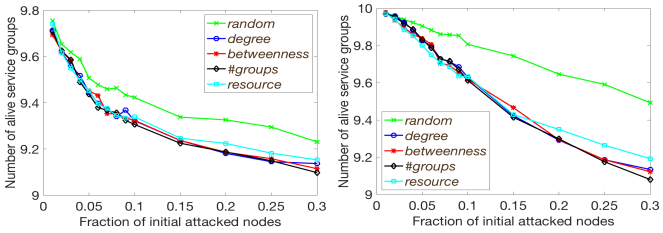
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2019.2917934, IEEE Transactions on Network and Service Management



(a) Size of the giant component (b) Resource utilization ratio (c) Adaptation cost (d) Number of alive service groups

Fig. 3: Performance comparison of adaptation strategies under different attack density, ϕ, when attacks are infectious.

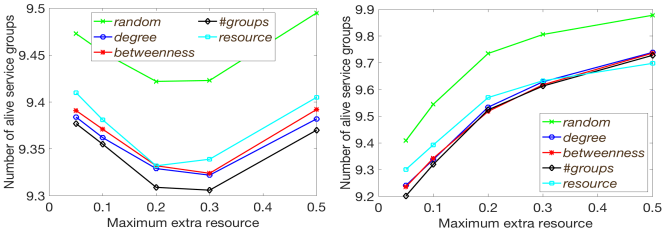
is a critical metric to represent mission performance in a mission-oriented network.



(a) `min-LA` under IA (b) `max-LA` under IA

Fig. 4: Effect of varying attack density, ϕ, on the number of alive groups, $\mathcal{N}_A$, with `min-LA` or `max-LA` under targeted, infectious attacks.

Effect of Varying Attack Density, ϕ: Fig. 4 shows the effect of ϕ on $\mathcal{N}_A$ under various targeted, infectious attacks when either `min-LA` or `max-LA` is used. In both adaptation strategies, the effect of IA is more severe than NIA (not shown for the case with NIA due to space constraint). In addition, targeted attacks significantly decrease $\mathcal{N}_A$ compared to random attacks. It is evident that `max-LA` outperforms `min-LA` across varying the fraction of initial attacked nodes and under different attacks. This implies that network adaptation aiming to maximize resource utilization can ultimately lead to better mission performance as it aims for maximizing the total number of completed tasks as a system goal while the individual node/group-level goal only concerns its task completion, which may take resources for other task groups to the completion.

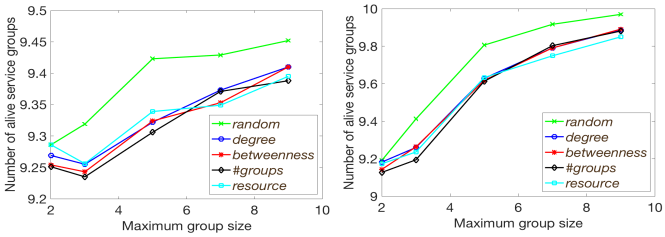


(a) `min-LA` under IA (b) `max-LA` under IA

Fig. 5: Effect of varying the maximum extra resource level, α, on the number of alive groups, $\mathcal{N}_A$, with `min-LA` or `max-LA` under targeted, infectious attacks.

Effect of Varying the Maximum Level of Extra Resource, α: Fig. 5 shows the effect of α (representing the percentage of extra resources provided to each node above each node's required level of resources) on $\mathcal{N}_A$ under `min-LA` or `max-LA` under infectious attacks. Similar to Fig. 4, the impact of random attacks is much less detrimental than targeted attacks. In addition, centrality-based attacks (i.e., degree and betweenness attacks) introduce higher adverse effect than characteristic-based attacks (i.e., resource and group attacks) under IA with the same reason explained in Fig. 4. It is noteworthy that for `min-LA` there exists an α level that will minimize $\mathcal{N}_A$. That is, a higher α does not necessarily increase $\mathcal{N}_A$. This implies that under `min-LA` extra resources do not lead to high resource utilization. The reason is that `min-LA` chooses a node or a group to maximize the individual utility rather than global system-level utility. As a result, nodes with maximum resources can be easily taken by another group without caring much about saving capable nodes for other groups.

The effect of α on other performance metrics, including $\mathcal{S}_g$, $\mathcal{R}_U$, and $\mathcal{C}_A$, is summarized as follows: Random attacks introduce less $\mathcal{C}_A$ and higher $\mathcal{R}_U$, compared to targeted attacks. Varying α does not show high sensitivity across all targeted attack types. In addition, the sensitivity of α is minimal due to less adaptation needed (i.e., less overloaded nodes with more resources) across all attack types.



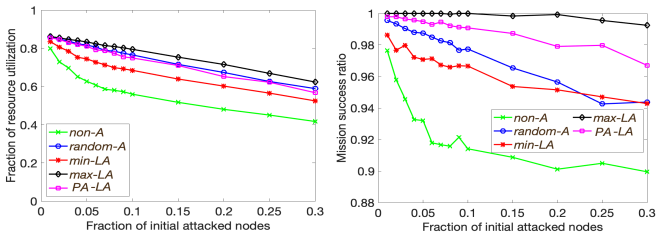
(a) `min-LA` under IA (b) `max-LA` under IA

Fig. 6: Effect of varying the maximum number of groups to join, n_g, on the number of alive groups, $\mathcal{N}_A$, with `min-LA` or `max-LA` under targeted, infectious attacks.

Effect of Varying the Maximum Number of Groups to Join, n_g: Fig. 6 shows the effect of n_g on $\mathcal{N}_A$ under `min-LA` or `max-LA` under targeted, infectious attacks. Under both `min-LA` and `max-LA`, as n_g increases $\mathcal{N}_A$ also increases. Different from the results observed in Figs. 4 and 5, among all targeted attack types, *resource attacks* (i.e., attacking nodes with more resources) impact $\mathcal{N}_A$ the most. This explains that as node resource levels are critical to maximizing $\mathcal{N}_A$. With increasing n_g, `max-LA` is more effective than `min-LA` to maximize $\mathcal{N}_A$. Based on our findings from Figs. 4 -6, we can conclude that team composition in terms of how to assign a node to a particular group considering the resource level is critical to maximizing mission performance (i.e., $\mathcal{N}_A$) in mission-oriented networks.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2019.2917934, IEEE Transactions on Network and Service Management

5.3.3 Performance Analysis under Tasks with Different Criticality Levels



(a) Resource utilization ratio (b) Mission success ratio

Fig. 7: Performance comparison of adaptation strategies under different attack density, ϕ, under random, non-infectious attacks when task groups are given with different levels of criticality.

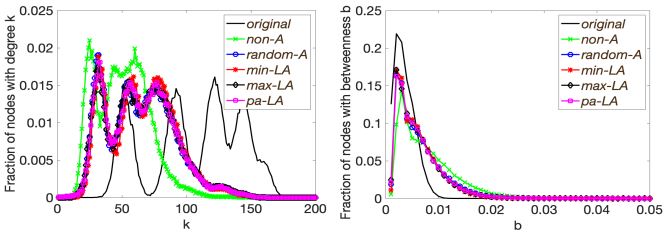
In this section, we compare the performance of the adaptation strategies against baseline counterparts particularly when task groups are heterogeneous with different levels of criticality. Among 10 task groups, the criticality level, CR_{g_k}, is assigned as high, medium, and low with the ratio of $2:3:5$. We also considered an additional scheme, called priority-aware load adaptation (`pa-LA`), as described in Section 4.2, to investigate the effect of considering different criticality levels of task groups on mission success ratio in Eq. (7). Fig. 7 shows the results based on the performance comparison of adaptation strategies and baseline counterparts, similar to Fig. 2, but under tasks groups with different levels of criticality. To investigate the impact of tasks with different levels of criticality, we use mission success ratio ($\mathcal{R}_s$) to compare the performance of adaptation strategies and baseline counterparts. In particular, `pa-LA` is examined to show its impact on $\mathcal{R}_s$ as it is priority-aware based on the criticality level of a given task group. Due to the space constraint, we only show the resource utilization and mission success ratio in Fig. 7.

Although the results shown in Fig. 7 are very similar to those in Fig. 2, as we considered the different levels of criticality in task groups, the focus of this experiment is how the priority-aware adaptation scheme (i.e., `pa-LA`), as an existing counterpart, performs compared to the proposed adaptation strategies (i.e., `max-LA` and `min-LA`) and the baseline counterparts (i.e., `non-A` and `random-A`). `pa-LA` also shows a fairly similar size of the giant component like other adaptation strategies and performs close to `random-A` in resource utilization and little less than `max-LA` in adaptation cost. Most interestingly, in terms of the mission success ratio, different from our expectation that `pa-LA` would perform better than `max-LA`, our proposed `max-LA` outperforms even `pa-LA`. This implies that even `max-LA` can maximally optimize the resource allocation even beyond the existing priority-aware scheme (i.e., `pa-LA`).

5.4 Analysis of Network Characteristics

In Section 5.3, we observed that across different adaptation strategies, there is little difference in the size of the giant component (i.e., $\mathcal{S}_g$). However, we observe that `max-LA` outperforms other adaptation strategies in the number of alive service groups (i.e., $\mathcal{N}_A$). In order to understand the reason why an adaptation strategy (e.g., `max-LA`) performs better than others, we examine three key "network characteristics" metrics associated with a network topology [38]: degree distribution, betweenness distribution, and clustering coefficient. A node's degree or betweenness typically represents its centrality or influence (or power) in a given network. The clustering coefficient metric mainly explains how nodes are connected to each other, showing the tendency of clustering together. This metric is mainly used to observe whether a given graph has a set of groups that are tightly connected. We adopt the *network average clustering coefficient* [51].

5.4.1 Degree & Betwenness Distributions



(a) Degree distribution (b) Betweenness distribution

Fig. 8: Degree and betweenness distributions after attack and adaptation under random attacks.

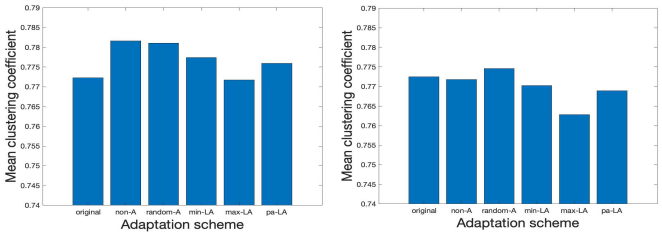
Fig. 8 plots the fraction of nodes with degree k or betweenness b (y-axis) vs. k or b (x-axis) to visually show the node degree or betweenness distribution in the resulting network after attack and adaptation under random attacks. We omit the results under other attacks as their trends are very similar and due to space constraint. The following observations regarding the differences among the original network and the networks after random attack under the adaptation (or non-adaptation) strategies also apply to the scenarios with targeted attacks.

Fig. 8 (a) shows the degree distributions of networks including an original network and a network after applying all comparing non-adaptation or adaptation strategies. In the original network, the four highest degrees are observed across various values of k. After attacks are applied, since some edges around the attacked nodes are removed, the ranges of degrees k are reduced in both non-adapted and adapted networks. All adapted networks have a wider range of distributions than the non-adapted network with `non-A`, particularly moving towards a high node degree direction due to some edges reconnected by `FindNode` or `FindGroup`. Among the adaptation strategies (i.e., `random-A`, `max-LA`, `min-LA`, and `pa-LA`), the difference in node degree distributions is very small, implying little sensitivity of the node degree distribution under different adaptation strategies.

Fig. 8 (b) shows the betweenness distributions of the original network, non-adapted network, and adapted networks under random attacks. We observe no significant sensitivity over different strategies except that the original network has lower betweenness than non-adapted and/or adapted networks. This is because the network after being attacked has fewer edges which can change nodes' betweenness due to the changed paths between nodes. Although these two distributions showed the changes of edges due to attacks applied, they do not show any significant sensitivity over different adaptation strategies.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2019.2917934, IEEE Transactions on Network and Service Management

5.4.2 Clustering Coefficient



(a) Random attacks (b) Resource attacks

Fig. 9: Clustering coefficient before and after attack under random or resource attacks.

Although Fig. 8 shows interesting results in terms of identifying different network characteristics between non-adaptation and adaptation strategies, they do not explain much why a particular scheme (i.e., `max-LA`) performs better than the rest of other schemes. In this section, we use a graph centrality metric, clustering coefficient (CC), to investigate this issue.

Fig. 9 plots the CC (y-axis) of the original topology and the resulting topology after applying various adaptation strategies (x-axis), under various attack types when attacks are non-infectious. Due to the space constraint, we only show the CC under random or resource attacks. Recall that the CC represents how nodes are closely clustered together. In Fig. 9, the bars represent the degree of the CC values for the original network and (non) adapted networks under different schemes. We found the high performing scheme (i.e., `max-LA`) in resource utilization and mission performance (i.e., the number of alive service groups or mission success ratio) shows the lowest CC among all, representing a less degree of being clustered between nodes in the adapted network using the `max-LA`. This implies that a less coupled network is less likely to trigger correlated failures (i.e., security and overload failures), leading to less cascading failures. Therefore, in order to minimize the effect of cascading failures for mission-oriented networks, nodes should not be tightly coupled together but just maintain a sufficient level of connectivity for providing normal network availability which leads to providing normal services properly.

In particular, a less tightly coupled network with low clustering coefficient generated by a resource-aware adaptation strategy will be less vulnerable to cascading failures caused by targeted attacks. In our experimental results, `max-LA` generates the lowest mean clustering coefficient among all adaptation strategies. This may explain why it outperforms all other adaptation strategies in terms of resource utilization and the number of alive service group.

5.5 Analysis of the Giant Component with Adaptation Strategies

In Section 5.3, we showed the size of the giant component is not significantly different under three different adaptation strategies, including `random-A`, `min-LA`, `max-LA`, and `pa-LA`. In this section, we mathematically prove why the size of the giant component is similar under different adaptation strategies following the procedures of estimating the size of the giant component in percolation theory. For simplicity, we consider non-infectious random attacks.

In this work, when the original network is attacked by a set of initial attackers, an IDS operates to detect the initial attackers with probability γ. Then, a set of edges connected to detected attackers are removed (i.e., bond percolation). When an adaptive strategy is used, some edges may be removed when a node drops a task group and some edges may be added when a group adds a node as a member to mitigate/avoid overloaded failures. Given a fraction of initial attackers, ϕ, the IDS is applied with detection probability γ, leading to removing nodes with probability $\phi(1-\gamma)$. As shown in Fig. 2, as long as a node belongs to any group, it belongs to the giant component. This means when the node has a remaining resource level to maintain the assigned workload from task groups involved, it is more likely to belong to the giant component, and vice-versa. We denote the average probability that a node does not belong to the giant component by u_r because of its resource level that triggers overloaded failure. Hence, we consider the following cases when node i does not belong to the giant component: (1) when the node is removed by an IDS after it is selected as an initial attacker with probability $\phi(1-\gamma)$ (i.e., functional failure in Section 3.2); or (2) when a node did not fail due to the initial attack but failed due to being overloaded even under network adaptations made with probability $(1-\phi+\gamma\phi)u_r$ (i.e., overloaded failure in Section 3.2).

The average probability any node i does not belong to the giant component, denoted by u, is:

$$u = \phi(1-\gamma) + (1-\phi+\phi\gamma)\sum_{r=1}^{\tau} p_r u_r \tag{8}$$

where $\sum_{r=1}^{\tau} p_r = 1$ and τ is the maximum number of resource intervals (or ranges of resource values) and a node's resource level is given based on τ different levels. Higher r represents a higher resource level in which p_r's refer to a resource distribution of nodes with resource level r. Note that in a given mission-oriented network considered in this work, the connection between nodes is based on a task group formation where a node's resource level is a critical factor for two nodes to be connected. For simplicity, taking $\sum_{r=1}^{\tau} p_r u_r$ as $g_r(u)$, u can be rewritten by $u = \phi(1-\gamma) + (1-\phi+\phi\gamma)g_r(u)$. Then, the size of the giant component, $S_g (= 1-u)$, is given by:

$$\begin{aligned} S_g &= 1 - \phi(1-\gamma) - (1-\phi+\phi\gamma)g_r(u) \\ &= (1-\phi+\phi\gamma)(1-g_r(u)) \end{aligned} \tag{9}$$

Eq. (9) proves that the size of the giant component is mainly affected by the attack intensity with ϕ and the quality of the IDS, γ. Another key impact is based on the resource distribution of nodes in the network. However, when adaptations are made regardless of a strategy, as long as additional edges are added or removed to deal with overloaded failures, the size of the giant component is the same because $g_r(u)$ is not sensitive to the assignment of nodes to different task groups. This is aligned with our finding in Section 5.3 that the size of the giant component can only partially represent the degree of network resilience particularly under service or mission-oriented networks.

6 Conclusions

In this paper, we extended the concept of network resilience by embracing network adaptability in addition to fault tolerance for service-oriented or mission-oriented networks. We developed three network adaptation strategies (`random-A`, `max-LA`, `min-LA`, and `pa-LA`) based on percolation theory to fend off cascading failures caused by targeted attacks. We performed a thorough and comprehensive analysis to analyze the effects of node failure types (functional, overload, and security failure), attack processes (non-infectious vs. infectious), attack strategies (random vs. targeted), and adaptation strategies (random, minimum load, maximum load, priority-aware load) on network resilience. Lastly, we identified key network characteristics that can truly represent network resilience against attacks.

The **key findings** obtained from this study include:

- In mission or service-oriented networks, the size of the giant component that solely measures network connectivity may not fully represent the degree of network resilience because other measurements, such as delivered service quality, cannot be properly measured only based on network connectivity. This is proven via our extensive simulation study along with a mathematical proof.
- Although resource-aware adaptation (i.e., `max-LA`) does not generate a larger size of the giant component, when compared to other counterparts, it is capable of increasing network resource utilization which is also a critical factor to increase mission performance, measured by the number of active task groups that can execute to completion in the presence of targeted attacks.
- The size of the giant component ($\mathcal{S}_g$), resource utilization ratio ($\mathcal{R}_U$), and adaptation cost ($\mathcal{C}_A$) do not show much sensitivity over various targeted attack types (i.e., degree attacks, betweenness attacks, group attacks, and resource attacks). However, the number of alive service groups ($\mathcal{S}_A$) exhibits high sensitivity, indicating that the number of alive service groups after attack is the key metric to represent mission performance in a mission-oriented network.
- Resource attacks (that target nodes with a high resource level) and group attacks (that target nodes with a large number of groups affiliated with) can significantly decrease the number of alive service groups when the attacks are non-infectious.
- Given a mission-oriented network with the same number of active, non-compromised nodes with the same level of resource utilization in executing a set of tasks, how to assign the resource by assigning the right nodes to the right groups is critical to maximize mission performance.
- `max-LA` generates the lowest mean clustering coefficient among all adaptation strategies. This may explain why it outperforms all other adaptation strategies in terms of resource utilization and the number of alive service group. This implies that a loosely coupled network is resilient against attacks while maximizing mission performance because it is less susceptible to cascading failures caused by targeted attacks. Our experimental results suggest that the "clustering coefficient" can be a key network characteristics metric representing network resilience.

References

[1] M. Alam, D. Yang, J. Rodriguez, and R. A. Abd-alhameed, "Secure device-to-device communication in lte-a," *IEEE Communications Magazine*, vol. 52, no. 4, pp. 66–73, April 2014.

[2] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, pp. 378–382, 2000.

[3] J. Bagrow, S. Lehmann, and Y.-Y. Ahn, "Robustness and modular structure in networks," *Network Science*, vol. 3, no. 4, pp. 509–525, 2015.

[4] A.-L. Barabási, *Network Science*, 1st ed. Cambridge University Press, 2016.

[5] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[6] L. Blume, D. Easley, J. Kleinberg, R. Kleinberg, and E. Tardos, "Which networks are least susceptible to cascading failures?" in *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, Oct 2011, pp. 393–402.

[7] M. R. Brannsten, F. T. Johnsen, T. H. Bloebaum, and K. Lund, "Toward federated mission networking in the tactical domain," *IEEE Communications Magazine*, vol. 53, no. 10, pp. 52–58, Oct. 2015.

[8] D. S. Callaway, M. E. Newman, S. H. Strogatz, and D. J. Watts, "Network robustness and fragility: Percolation on random graphs," *Physical Review Letters*, vol. 85, no. 25, pp. 5468–5471, 2000.

[9] C. Chau, R. J. Gibbens, R. E. Hancock, and D. Towsley, "Robust multipath routing in large wireless networks," in *2011 Proceedings IEEE INFOCOM*, April 2011, pp. 271–275.

[10] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 24–29, 2012.

[11] J.-H. Cho and J. Gao, "Cyber war game in temporal networks," *PLoS ONE*, vol. 11, no. 2, pp. 24–29, 2016.

[12] J.-H. Cho and T. Moore, "Percolation-based network adaptability under cascading failures," in *IEEE INFOCOM 2018*, April 2018.

[13] J.-H. Cho, P. M. Hurley, and S. Xu, "Metrics and measurement of trustworthy systems," in *IEEE Military Communications Conference (MILCOM)*, Nov. 2016, pp. 1237–1242.

[14] J.-H. Cho, S. Xu, P. Hurley, M. Mackay, T. Benjamin, and M. Beaumont, "STRAM: Measuring the trustworthiness of computer-based systems," *ACM Computing Surveys*, Jan. 2019, under press.

[15] C. Colbourn, "Network resilience," *SIAM Journal on Algebraic Discrete Methods*, vol. 8, no. 3, pp. 404–409, 1987.

[16] P. Erdös and A. Rényi, "On the evolution of random graphs," in *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, 1960, pp. 17–61.

[17] M. Franceschetti, O. Dousse, D. N. C. Tse, and P. Thiran, "Closing the gap in the capacity of wireless networks via percolation theory," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 1009–1018, March 2007.

[18] L. Freeman, "A set of measures of centrality based on betweenness," *Sociometry*, vol. 40, pp. 35–41, 1977.

[19] J. Freixas and M. Pons, "The influence of the node criticality relation on some measures of component importance," *Operations Research Letters*, vol. 36, no. 5, pp. 557–560, Sept. 2008.

[20] A. A. Ganin, M. Kitsak, D. Marchese, J. M. Keisler, T. Seager, and I. Linkov, "Resilience and efficiency in transportation networks," *Science Advances*, vol. 3, no. 12, 2017.

[21] M. Girvan and M. E. J. Newman, "Community structure in social and biological networks," *Proceedings of the National Academy of Sciences*, vol. 99, no. 12, pp. 7821–7826, June 2002.

[22] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "The

effect of eavesdroppers on network connectivity: A secrecy graph approach," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 712–724, Sept 2011.

[23] M. F. Habib, M. Tornatore, F. Dikbiyik, and B. Mukherjee, "Disaster survivability in optical communication networks," *Computer Communications*, vol. 36, no. 6, pp. 630–644, 2013.

[24] R. A. Hanneman and M. Riddle, *Introduction to social network methods*, Riverside, CA, University of California, Riverside, 2005, ch. Chapter 10: Centrality and power.

[25] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Computers & Security*, vol. 24, no. 1, pp. 31–43, 2005.

[26] Z. Huang, C. Wang, A. Nayak, and I. Stojmenovic, "Small cluster in cyber physical systems: Network topology, interdependence and cascading failures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 8, pp. 2340–2351, Aug. 2015.

[27] I. Kryven, "Bond percolation in coloured and multiplex networks," *Nature Communications*, vol. 10, no. 404, 2019.

[28] G. Liu, J. Zhang, and G. Chen, "An approach to finding the cost-effective immunization targets for information assurance," *Decision Support Systems*, vol. 67, pp. 40–52, Nov. 2014.

[29] A. M. Madni and S. Jackson, "Towards a conceptual framework for resilience engineering," *IEEE Systems Journal*, vol. 3, no. 2, pp. 181–191, June 2009.

[30] A. Majdandzic, B. Podobnik, S. V. Buldrev, D. Y. Kenett, S. Havlin, and H. E. Stanley, "Spontaneous recovery in dynamical networks," *Nature Physics*, vol. 10, pp. 34–38, 2014.

[31] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016.

[32] S. Mizutaka and K. Yakubo, "Overload network failures: An approach from the random-walk model," in *2013 International Conference on Signal-Image Technology Internet-Based Systems*, Dec. 2013, pp. 630–633.

[33] T. J. Moore and J.-H. Cho, *Applying Percolation Theory*. Springer International Publishing, 2019, pp. 107–133.

[34] B. Mukherjee, M. F. Habib, and F. Dikbiyik, "Network adaptability from disaster disruptions and cascading failures," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 230–238, May 2014.

[35] W. Najjar and J. L. Gaudiot, "Network resilience: a measure of network fault tolerance," *IEEE Transactions on Computers*, vol. 39, no. 2, pp. 174–181, Feb 1990.

[36] M. Newman and D. Watts, "Scaling and percolation in the small-world network model," *Physical Review E*, vol. 60, no. 6, pp. 7332–7342, 1999.

[37] M. Newman and R. Ziff, "Fast monte carlo algorithm for site or bond percolation," *Physical Review E*, vol. 64, no. 1, p. 016706, 2001.

[38] M. E. J. Newman, *Networks: An Introduction*, 1st ed. Oxford University Press, 2010.

[39] G. Palla1, I. Derényi, I. Farkas, and T. Vicsek, "Uncovering the overlapping community structure of complex networks in nature and society," *Nature*, vol. 435, 2005.

[40] J. L. H. R. S. Farr and T. M. Fink, "Easily repairable networks: reconnecting nodes after damage," *Physical Review Letters*, vol. 113, no. 13, p. 138701, 2014.

[41] C. E. L. Rocca, H. E. Stanley, and L. A. Braunstein, "Strategy for stopping failure cascades in interdependent networks," *Physica A: Statistical Mechanics and its Applications*, vol. 508, pp. 577–583, 2018.

[42] S. Ruj and A. Pal, "Analyzing cascading failures in smart grids under random and targeted attacks," in *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, May 2014, pp. 226–233.

[43] S. S. Savas, M. F. Habib, M. Tornatore, F. Dikbiyik, and B. Mukherjee, "Network adaptability to disaster disruptions by exploiting degraded-service tolerance," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 58–65, Dec. 2014.

[44] S. Shao, X. Huang, H. E. Stanley, and S. Havlin, "Percolation of localized attack on complex networks," *New Journal of Physics*, vol. 17, no. 2, p. 023049, 2015.

[45] L. Shekhtman, M. M. Danziger, and S. Havlin, "Recent advances on failure and recovery in networks," *Chaos, Solitons, and Fractals*, vol. 90, pp. 28–36, 2016.

[46] J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, June 2010.

[47] L. Sun and W. Wang, "Understanding blackholes in large-scale cognitive radio networks under generic failures," in *2013 Proceedings IEEE INFOCOM*, April 2013, pp. 728–736.

[48] F. Wang, B. Zhang, Q. Li, S. Chai, L. Cui, S. Zhang, and Z. Guan, "A study on the robustness and fragility of tree-based wireless sensor networks with community characteristics," in *2017 IEEE International Conference on Unmanned Systems (ICUS)*, Oct. 2017, pp. 307–312.

[49] Y. Wang, I. Chen, and J. Cho, "Trust-based task assignment in autonomous service-oriented ad hoc networks," in *2015 IEEE Twelfth International Symposium on Autonomous Decentralized Systems*, Mar. 2015, pp. 71–77.

[50] Y. Wang, I. Chen, J. Cho, and J. J. P. Tsai, "Trust-based task assignment with multiobjective optimization in service-oriented ad hoc networks," *IEEE Transactions on Network and Service Management*, vol. 14, no. 1, pp. 217–232, March 2017.

[51] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, p. 440442, 1998.

[52] F. Xing and W. Wang, "On the critical phase transition time of wireless multi-hop networks with random failures," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08, 2008, pp. 175–186.

[53] Y. Xu and W. Wang, "Characterizing the spread of correlated failures in large wireless networks," in *2010 Proceedings IEEE INFOCOM*, March 2010, pp. 1–9.

[54] X. Yuan, Y. Dai, H. E. Stanley, and S. Havlin, "k-core percolation on complex networks: Comparing random, localized, and targeted attacks," *Phys. Rev. E*, vol. 93, p. 062302, Jun. 2016.