Connectivity Maintenance in Uncertain Networks under Adversarial Attack

Jianzhi Tang[1], Luoyi Fu[2], Jiaxin Ding[2], Xinbing Wang[1,2] and Guihai Chen[2]
[1,2]Dept. of {Electronic Engineering, Computer Science}, Shanghai Jiao Tong University, China
{tangjianzhi, yiluofu, jiaxinding, xwang8}@sjtu.edu.cn, gchen@cs.sjtu.edu.cn

***Abstract*—This paper studies the problem of connectivity maintenance in adversarial uncertain networks, where a defender prevents the largest connected component from being decomposed by an attacker. In contrast with its deterministic counterpart, connectivity maintenance in an uncertain network involves additional testing on edges to determine their existence. To this end, by modeling a general uncertain network as a random graph with each edge associated with an existence probability and a testing cost, our goal is to design a general adaptive defensive strategy to maximize the expected size of the largest remaining connected component with minimum expected testing cost and, moreover, the strategy should be independent of the attacking patterns. The computational complexity of the connectivity maintenance problem is unraveled by proving its NP-hardness. To accurately tackle the problem, based on dynamic programming we first propose an optimal defensive strategy for a specific class of uncertain networks with uniform testing costs. Thereafter multi-objective optimization is adopted to generalize the optimal strategy for general uncertain networks through weighted sum of normalized size and cost. Due to the prohibitive price of an optimal strategy, two approximate defensive strategies are further designed to pursue decent performance with quasilinear complexity. We first derive a heuristic approach by quantifying the edge vulnerability through an analogy from the degree centrality in deterministic networks to the probability degree and connectivity weight in uncertain networks. For performance guarantee, we then devise an adaptive greedy policy incorporating the minimax rule from game theory, which minimizes the possible loss suffered by the defender in a worst-case scenario caused by the attacker and has an approximation ratio of $(1 - 1/e)$. Extensive experiments on both synthetic and real-world network datasets under diverse attacking patterns demonstrate the superiority of the proposed strategies over baselines.**

I. Introduction

Connectivity has long been the focus of concern in the field of networking. The investigation of network connectivity has a wide range of applications in real-life scenarios. In communication networks, the connectivity among devices reflects the reliability of data links and facilitates the design of wise routing strategies for efficient message transmission [1]. In social networks, the connectivity among users reflects the tightness of relation and is utilized to infer preference similarities for accurate recommendation [2]. In academic networks, the connectivity among scholars and papers is conducive to the analysis of collaboration and dependency among various research fields [3].

Despite the importance of connectivity, networked systems are vulnerable to adversarial attacks that aim to destroy the network connectivity. In these attacks, failure of nodes and links are caused by the attacker to compromise the network's ability to meet its quality-of-service (QoS) [4]. Recently, emerging works have been focusing on characterizing the impact of different attacking patterns on network connectivity, most of which assuming the network to be deterministic [5], [6], [7]. A variety of connectivity maintenance strategies have also been proposed based on the analysis of crucial nodes and links in maintaining the network connectivity under specific attacking strategies.

Unfortunately, a deterministic network fails to serve as a suitable model for most real-life networks, which are usually uncertain. Affected by multiple factors, the existence of links in an uncertain network is usually unfixed and full knowledge of the existence of all links at some point is usually unavailable. For instance, in a data center, due to the unreliability of data links, connection between a pair of nodes may frequently fail [8]. In a metropolitan localization network, communication between smartphones is restricted by their relative locations [9]. In an outdoor sensor network, connection between devices strongly depends on climatological conditions within the field [10]. In fact, over 90 percent of links in wireless sensor networks are unreliable [11]. All these observations motivate the modeling of an uncertain network as a random graph where each edge is assigned an existence probability, which can be estimated a priori through link detection over time or be generated from various probability models concerning specific types of networks and applications [12].

Compared with its deterministic counterpart, the major technique of designing efficient connectivity maintenance strategies in an uncertain network differs greatly. The main difference lies in that to eliminate the uncertainty of the network, we have to test the edges to find out whether they exist or not. However, such testing may involve far more complicated procedures than merely identifying the existence of an uncertain link. For example, in social networks, to unravel the genuine relation between a pair of users, we may need to apply advanced approaches such as graph matching or data mining to reinforce the judgement [13], which may incur large computational cost. Hence, it is desirable to design a strategy that maintains the connectivity of the network with minimum expected testing cost. Furthermore, a wise strategy should be adaptive, implying that the previous testing outcomes should be fully utilized for future edge selections.

In this paper, we are thus motivated to present a first look into the problem of connectivity maintenance in uncertain networks under adversarial attacks. Given a general uncertain

network modeled as a random graph with each edge associated with an existence probability and a testing cost, our goal is to design a general adaptive defensive strategy that incurs the maximum expected size of the largest remaining connected component with minimum expected testing cost. Moreover, the defensive strategy should be independent of the attacking patterns. To this end, we first investigate the computational complexity of the problem. By proving its NP-hardness, we show the difficulty of connectivity maintenance in an uncertain network. To characterize the features of an optimal solution, based on dynamic programming we first design an optimal defensive strategy for uncertain networks with uniform costs and thereafter generalize the strategy for general networks through weighted sum of normalized size and cost. Considering the prohibitive price of computing an optimal strategy, we further design two approximate defensive strategies to pursue decent performance with quasilinear complexity, in which the first one is a heuristic approach that quantifies the edge vulnerability through an analogy from degree centrality of nodes in deterministic networks to connectivity weight of edges in uncertain networks, and the second one is an adaptive greedy policy incorporating the minimax rule from game theory, which minimizes the possible loss suffered by the defender in a worst-case scenario caused by the attacker and has theoretical performance guarantee.

Our key contributions are summarized as follows:

- We formally define the problem of connectivity maintenance in adversarial uncertain networks by clarifying the general uncertain network model and the actions taken by the attacker and the defender, respectively. We prove the NP-hardness of the connectivity maintenance problem.
- We derive an optimal defensive strategy which gives us insights into the nature of the problem and the characteristics of the optimal solution. We further design two approximate strategies which, as concluded from experimental results, can both derive decent solutions with quasilinear computational complexity.
- All the proposed strategies are *general* and are independent of the attacking patterns. We validate the superiority of the proposed strategies over baselines through extensive experiments on both synthetic and real-world network datasets, under diverse attacking patterns.

The rest of this paper is organized as follows. Section II states related work. In Section III, we introduce network and adversary models and formulate the connectivity maintenance problem. In Section IV, we investigate the computational complexity of the problem. We propose the dynamic programming-based optimal defensive strategies in Section V. In Section VI, we propose two approximate defensive strategies and we evaluate the proposed strategies in Section VII. We conclude the paper in Section VIII.

II. Related Work

A. Uncertain Networks

Uncertain networks characterize the properties of most real-life networks, whose topologies may dynamically vary with time. The past few years have seen intensive studies focusing on different aspects of uncertain networks. Wu *et al.* investigates the robustness issues of a set of distributed optimization algorithms over uncertain network graphs [14]. Yu *et al.* proposed a distributed algorithm to accomplish local broadcast services in abstract MAC layer in dynamic networks [15]. Saha *et al.* devised a sampling-based algorithm with accuracy guarantee to compute the most probable shortest path in uncertain networks [16]. Cheng *et al.* studied the top-k vulnerable nodes detection problem in uncertain graphs and proposed a sampling-based approach [17]. In recent years, other types of works on uncertain networks include reliable topology design [18], performance analysis of unreliable wireless networks [19], and representative subgraphs extraction for acceleration of different querying processes [20].

B. Network Connectivity

As a fundamental yet essential problem in the field of networking, abundant works have made an effort to investigate network connectivity. Piltyay *et al.* performed the analysis of connectivity of wireless sensor network in heterogeneous 5G mobile systems [21]. Fukunaga *et al.* presented an adaptive algorithm with theoretical performance guarantee to find connected dominating sets in uncertain graphs [22]. Fu *et al.* proposed an optimal algorithm for source-destination connectivity determination in general uncertain networks [12]. For connectivity in adversarial networks, Abuzainab *et al.* studied the network connectivity in an adversarial internet of battlefield things [6]. Flaxman *et al.* analyzed the influence on network connectivity caused by adversarial deletion of partial nodes in a scale-free network [23]. Du *et al.* investigated the robustness of coupled networks under different targeted-attack strategies [5]. Nugraha *et al.* addressed cyber security issues considering connectivity on resilient graphs [7].

Although much effort has been devoted in both uncertain network and connectivity investigation, when it comes to connectivity analysis in adversarial networks, two deficiencies of prior art from our perspective are listed as follows:

- Most existing works model the adversarial network as a deterministic graph, while the rest mainly focus on uncertain networks with specific topologies. Such works are valuable to particular classes of networks (e.g. bipartite and scale-free graphs), but may lack the ability of generalization to general uncertain networks. Moreover, the heterogeneous testing cost is always ignored.
- Existing studies concentrate on the influence on connectivity caused by mere attack rather than a joint consideration of attack and defense which may generate general defensive strategies for effective connectivity maintenance.

To our best knowledge, this work is the first attempt to deign *general* defensive strategies for connectivity maintenance in *general* uncertain networks under adversarial attacks.

III. Models and Problem Formulation

A. Uncertain Network Model

An uncertain network is denoted by a random graph $\mathcal{G}(V, E, p, c)$, where V is the set of vertices, E is the set of

edges, $p : E \mapsto [0, 1]$ and $c : E \mapsto \mathbb{R}^+$ are the functions that assign each edge e its existence probability and testing cost respectively. The existence probabilities of different edges are independent [12].

A state of an uncertain network $\mathcal{G}$ at some point is characterized by an $|E|$-dimensional vector $\mathbf{s}$ representing the underlying deterministic network of $\mathcal{G}$ at that moment. The elements of $\mathbf{s}$ consist of 0 and 1, respectively implying the inexistence and the existence of the corresponding edge. We define $\mathbf{s}_i$ as the i-th component of state $\mathbf{s}$. The set of all possible states associated with $\mathcal{G}$ is denoted as $\mathcal{S}_{|E|} = \{0, 1\}^{|E|}$. During the whole process of connectivity maintenance, the state of $\mathcal{G}$ is assumed to be fixed unless edges are attacked.

B. Adversary Model

We define $\mathbf{s}^a$ and $\mathbf{s}^d$ as the network states observed by the attacker and the defender, respectively. The elements of both $\mathbf{s}^a$ and $\mathbf{s}^d$ consist of 0, 1 and *, where * implies the corresponding edge is untested.

Considering the nature of connectivity maintenance and following the state of the art, we cast the adversarial process as a multistage two-player zero-sum game, where at each stage the attacker acts as a leader and the defender acts as a follower [6]. The detailed actions made by the attacker and the defender are listed as follows.

1) Attacker: At stage t, the attacker selects a_t edges and tests their existence. For those inexistent chosen edges, the attack fails. For those existent chosen edges, the attack succeeds and the attacker destroys them permanently. An attack is observable if the defender is fully aware of its location and outcome. The goal of the attacker is to decrease, as many as possible, the existing edges in the uncertain network in order to destroy the connectivity of the whole network.

Based on the amount of prior knowledge of the uncertain network, the attacking strategies are classified into two general patterns:

- *Oblivious Attack.* The attacker has few knowledge of functions p and c in network $\mathcal{G}$. Hence, the attacker randomly selects each edge with equal probability at each stage, independent of the previous actions. Such an attacker is said to *move by nature* in game theory.
- *Adaptive Attack.* The attacker has some or much knowledge of functions p and c in network $\mathcal{G}$. With these information at hand, the attacker makes selections based on previous actions and the current state $\mathbf{s}^a$ at each stage, resulting in an organized attacking strategy.

2) Defender: The defender has full prior knowledge of functions p and c in network $\mathcal{G}$. At stage t, the defender selects d_t edges and tests their existence. For those inexistent chosen edges, the defender makes no further action. For those existent chosen edges, the defender applies sophisticated techniques (i.e. burst transmission on data links in communication networks and encryption of messages in military networks) to 'conceal' the existing edge from being attacked until the end of adversary. The goal of the defender is to hinder the attacks and to maintain the connectivity of the network as much as possible with minimum testing cost.

With perfect knowledge of the network, the defender always tends to follow an *adaptive defensive strategy*, which is a mapping π that maps a state $\mathbf{s}^d$ to an edge e in the set of untested edges in $\mathbf{s}^d$, indicating that the defender should select and test edge e when confronted with state $\mathbf{s}^d$. For completeness, we define that if all edges in a state $\mathbf{s}^d$ has been tested, then strategy π maps $\mathbf{s}^d$ to $\perp$, which indicates the end of defense.

An illustrative example of an adversarial process is shown in Figure 1. The notations that will be used throughout the paper are summarized in Table I.

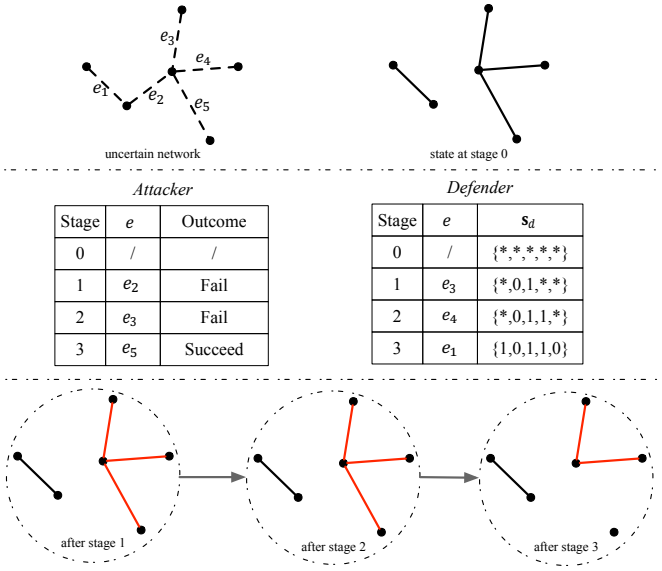


Fig. 1. An adversary example. Top: An uncertain network and its state before adversary. Medium: The edges selected by the attacker/defender at each stage and the respective outcome. Bottom: The evolution of network state during the process of adversary. The largest connected component is marked in red. In this example, the attack is observable and the size of the largest remaining connected component is 3.

C. Metrics and Problem Formulation

To characterize the network connectivity and to quantify the effect of the defense, we define the metric to be optimized and formulate the problem of connectivity maintenance as follows.

Definition 1. (Largest Remaining Connected Component) *The largest remaining connected component is the connected component with maximum number of vertices (i.e., the connected component of maximum size) at the end of adversary.*

Definition 2. (The Connectivity Maintenance Problem) *Given a general uncertain network $\mathcal{G}(V, E, p, c)$ and an attacker with arbitrary attacking strategy, the goal is to design a general adaptive defensive strategy π that incurs the maximum expected size of the largest remaining connected component with minimum expected testing cost.*

IV. Computational Complexity

Before elaborating the defensive strategy, we first investigate the computational complexity of the problem. We will show that, even if without the existence of an attacker, it is NP-hard for the defender to discover a connected component of

TABLE I
NOTATIONS AND DEFINITIONS

Notations	Definitions
$\mathcal{G}$	uncertain network
V	vertex set
E	edge set
p	existence probability function
c	testing cost function
$\mathbf{s}$	network state
$\mathbf{s}^a, \mathbf{s}^d$	state observed by attacker/defender
$\mathbf{s}_i$	i-th component of state $\mathbf{s}$
$\mathbf{s} \cdot e, \mathbf{s} \setminus e$	evolved state from $\mathbf{s}$ with e existent/inexistent
$\mathcal{S}$	set of network states
$\mathcal{S}_i$	set of network states with $\|i\|$ tested edges
$E_u^{\mathbf{s}}$	set of untested edges in state $\mathbf{s}$
a_t, d_t	number of edges attacked/defended at stage t
π	adaptive defensive strategy
u, f, F_{lc}	utility functions

certain size with a constrained testing cost. To this end, we first convert the connectivity maintenance problem into its decision version that asks for the existence of a defensive strategy with expected testing cost at most l and with the size of the discovered largest connected component at least k for a given uncertain network. We then prove in Theorem 1 that this decision version is NP-hard.

Theorem 1. *The decision version of the connectivity maintenance problem is NP-hard.*

Proof: We prove the NP-hardness by reduction from s-t reliability problem [24], which asks whether the probability of a node s being connected to a node t is larger than some value r in a graph G where all edges exist independently with probability $\frac{1}{2}$.

Given an instance of s-t reliability problem, we transform the graph G into an uncertain network $\mathcal{G}(V, E, p, c)$ through the following steps. We first traverse nodes in G assuming all edges exist and keep the size of the largest connected component no larger than k by edge deletion. Then, we assign each edge in G its corresponding existence probability $\frac{1}{2}$ and cost 1. Finally, We add an extra path $\mathcal{P}$ in G between node s and node t. Path $\mathcal{P}$ consists of k different nodes, including s and t. We set the existence probability of each of the $k-1$ edges on $\mathcal{P}$ as $\frac{1}{2}$ and the cost of each edge as $2^{|E|}/(k-1)$.

Denote r as the s-t reliability in G and l as the expected cost incurred by the optimal defensive strategy on $\mathcal{G}$. We will show that we can efficiently compute r if we know l and vice versa. Without loss of generality, we focus on the connected component consisting of nodes s and t. If s and t are not connected in G, then the defender has to at least test and conceal the connected component $\mathcal{P}$, leading to the first constraint $l \geq (1-r)2^{|E|}$. The other constraint $l \leq r|E| + (1-r)2^{|E|}$ holds since the expected cost of the optimal strategy will not exceed that of a clumsy strategy that first tests all the edges in G and then tests and conceals all the edges in $\mathcal{P}$ if nodes s and t are not connected in G. Combining these two constraints, we conclude that an s-t reliability $r = m/2^{|E|}$ exists if and only if there exists a strategy with expected cost l satisfying $2^{|E|} - l \leq m \leq \frac{2^{|E|}-l}{1-1-|E|/2^{|E|}}$, where m is an integer. We notice that the gap $(2^{|E|} - l)\left(\frac{|E|/2^{|E|}}{1-|E|/2^{|E|}}\right) \leq \frac{|E|}{1-|E|/2^{|E|}} = O(|E|)$ is linear with $|E|$.

Since the transformation and verification can both be done in polynomial time, we conclude that the decision version of connectivity maintenance problem is NP-hard. ■

V. OPTIMAL DEFENSIVE STRATEGY

Despite the NP-hardness, in order to gain some insights into the connectivity maintenance problem, it is still necessary and worthwhile to investigate the optimal solution. To this end, we first utilize Dynamic Programming (DP) to derive an optimal defensive strategy for a specific class of uncertain networks with uniform costs and thereafter generalize the optimal strategy for general uncertain networks through Multi-Objective Optimization (MOO).

A. Uncertain Networks with Uniform Costs

In uncertain networks where all the edges have the same testing cost, the only focus of the defender when designing defensive strategy is to choose the edge that maximizes the expected size of the largest remaining connected component. To this end, we consider dynamic programming [25] as an effective approach that directs the defender to compute the optimal strategy in a bottom-up fashion.

We first make some preliminary definitions and notations. For a given uncertain network observed by the defender, we divide the network state space $\mathcal{S}$ into $|E|$ disjoint subsets $\mathcal{S}_i (i = 0, 1, \cdots, |E|)$ based on the number of tested edges in the state. We name the states in the set $\mathcal{S}_{|E|}$ as terminating states and the states in the sets $\mathcal{S}_i (i = 0, 1, \cdots, |E|-1)$ as temporary states. Given a temporary state $\mathbf{s}$ and a selected edge e to test, $\mathbf{s} \cdot e$ and $\mathbf{s} \setminus e$ respectively denote the evolved state after finding e existent and inexistent.

In addition, we define an optimal utility function u that computes, for each temporary state, the expected size of the largest remaining connected component generated by the optimal defensive strategy starting from that state. For each terminating state, u computes the exact size of its largest connected component. For a defensive strategy π, u_π denotes its corresponding optimal utility function.

Algorithm 1 Optimal Defensive Strategy

Input: Uncertain network $\mathcal{G}(V, E, p, c)$ with constant c
Output: An optimal defensive strategy π

Initialize Compute $u_\pi(\mathbf{s})$ for all $\mathbf{s} \in \mathcal{S}_{|E|}$
for $i = |E| - 1$ to 0 **do**
  for all $\mathbf{s} \in \mathcal{S}_i$ **do**
    $E_u^{\mathbf{s}}$:= the set of untested edges in $\mathbf{s}$
    $e^* := \text{argmax}_{e \in E_u^{\mathbf{s}}} \{p(e)u_\pi(\mathbf{s} \cdot e) + (1 - p(e))u_\pi(\mathbf{s} \setminus e)\}$
    $u_\pi(\mathbf{s}) := p(e^*)u_\pi(\mathbf{s} \cdot e^*) + (1 - p(e^*))u_\pi(\mathbf{s} \setminus e^*)$
    $\pi(\mathbf{s}) := e^*$
  end for
end for
return π

According to the Bellman equation [25], we presents an optimal defensive strategy based on dynamic programming in Algorithm 1. The following theorems prove its correctness and investigate its time complexity.

Theorem 2. *For an uncertain network $\mathcal{G}(V, E, p, c)$ with constant c, Algorithm 1 yields an optimal defensive strategy.*

Proof: We prove the theorem by backward induction. Denote the optimal defensive strategy by π^*, and denote the defensive strategy generated in Algorithm 1 by π. For all states $\mathbf{s} \in \mathcal{S}_{|E|}$, it is obvious that $u_\pi(\mathbf{s}) = u_{\pi^*}(\mathbf{s})$. Now suppose that for all states $\mathbf{s} \in \mathcal{S}_i, i \geq k, u_\pi(\mathbf{s}) \geq u_{\pi^*}(\mathbf{s})$. To verify the optimality of π, we have to show that for all states $\mathbf{s} \in \mathcal{S}_{k-1}, u_\pi(\mathbf{s}) \geq u_{\pi^*}(\mathbf{s})$.

According to Algorithm 1, for a state $\mathbf{s} \in \mathcal{S}_{k-1}$, we have

$$\begin{aligned} u_\pi(\mathbf{s}) &= \max_{e \in E_u} \{p(e)u_\pi(\mathbf{s} \cdot e) + (1 - p(e))u_\pi(\mathbf{s} \setminus e)\} \\ &\geq p(\pi^*(\mathbf{s}))u_\pi(\mathbf{s} \cdot \pi^*(\mathbf{s})) + (1 - p(\pi^*(\mathbf{s})))u_\pi(\mathbf{s} \setminus \pi^*(\mathbf{s})) \\ &\geq p(\pi^*(\mathbf{s}))u_{\pi^*}(\mathbf{s} \cdot \pi^*(\mathbf{s})) + (1 - p(\pi^*(\mathbf{s})))u_{\pi^*}(\mathbf{s} \setminus \pi^*(\mathbf{s})) \\ &= u_{\pi^*}(\mathbf{s}), \end{aligned}$$

where the second inequality follows from the induction hypothesis. We have now shown that under every state $\mathbf{s}$, the defensive strategy π is optimal, which completes the proof. ■

Theorem 3. *For an uncertain network $\mathcal{G}(V, E, p, c)$ with constant c, the time complexity of Algorithm 1 is $O(|V|2^{|E|} + |E|3^{|E|})$, where $|V|$ and $|E|$ respectively denote the number of vertices and edges in $\mathcal{G}$.*

Proof: The total number of possible network states observed by the defender is $3^{|E|}$, including $2^{|E|}$ terminating states and $3^{|E|} - 2^{|E|}$ temporary states. To find the largest connected component of a terminating state, we have to loop through all the vertices, implementing either breadth-first or depth-first search whenever the loop reaches a vertex that has not already been included in a previously found connected component. This is implementable in $O((|V| + |E|))$ time. Also, selecting the optimal edge for each temporary state requires $O(|E|)$ time. Consequently, Algorithm 1 generates the optimal defensive strategy in $O((|V| + |E|)2^{|E|} + |E|(3^{|E|} - 2^{|E|})) = O(|V|2^{|E|} + |E|3^{|E|})$ time. ■

Remark: Algorithm 1 is perfectly suitable for Erdős-Rényi network (ER graph), the most commonly studied uncertain network topology. In an ER graph denoted by $G(n, p)$, any pair of n vertices are connected with an edge which exists independently with uniform probability p and the testing cost of each edge is uniform.

B. General Uncertain Networks

Now we generalize the optimal defensive strategy for general uncertain networks. In general networks, we aim to optimize two objectives simultaneously. On the one hand, we hope to maximize the expected size of the remaining largest connected component. On the other hand, we wish to minimize the total expected testing cost incurred by the strategy.

To design an exact algorithm that takes into account both objectives, we adopt the *weighted sum method* for Multi-Objective Optimization Problems (MOOP) [26]. We combine the two objectives into a single one by adding each objective pre-multiplied by a defender-supplied weight. The weights reflect the preference, for larger weight on cost implies the defensive strategy being economy-oriented, while larger weight on size implies the strategy being result-oriented.

Since cost and size differ in dimension, we first normalize them through min-max normalization, where a variable x is normalized to $x^* = (x - x_{min})/(x_{max} - x_{min}), x^* \in [0, 1]$. We define F_{lc} as a utility function that computes for each terminating state the size of its largest connected component and define the optimal utility function u for each temporary state $\mathbf{s}$ as

$$u(\mathbf{s}) = \max_{e \in E_u^{\mathbf{s}}} \{-\alpha \frac{c(e) - c_{min}}{c_{max} - c_{min}} + p(e)u(\mathbf{s} \cdot e) + (1 - p(e))u(\mathbf{s} \setminus e)\},$$

whereas for each terminating state,

$$u(\mathbf{s}) = \beta \frac{F_{lc}(\mathbf{s})}{|V|}.$$

Parameters c_{max} and c_{min} denote the maximum and minimum cost of all edges, $|V|$ denotes the total number of vertices in $\mathcal{G}$ (the maximum possible size of connected component), and α, β denote the positive weights given by the defender. Since we aim to decrease the cost, negative normalized cost is included.

Denote π as the defensive strategy adopted by the defender, and u_π as the optimal utility function associated with π. Algorithm 2 states the optimal weighted defensive strategy.

Algorithm 2 Optimal Weighted Defensive Strategy

Input: Uncertain network $\mathcal{G}(V, E, p, c)$, weights α and β
Output: An optimal weighted defensive strategy π

Initialize: Compute $u_\pi(\mathbf{s}) = \beta \frac{F_{lc}(\mathbf{s})}{|V|}$ for all $\mathbf{s} \in \mathcal{S}_{|E|}$
for $i = |E| - 1$ to 0 **do**
  for all $\mathbf{s} \in \mathcal{S}_i$ **do**
    $E_u^{\mathbf{s}}$:= the set of untested edges in $\mathbf{s}$
    $e^* := \text{argmax}_{e \in E_u^{\mathbf{s}}} \{-\alpha \frac{c(e) - c_{min}}{c_{max} - c_{min}} + p(e)u_\pi(\mathbf{s} \cdot e) + (1 - p(e))u_\pi(\mathbf{s} \setminus e)\}$,
    $u_\pi(\mathbf{s}) := -\alpha \frac{c(e^*) - c_{min}}{c_{max} - c_{min}} + p(e^*)u_\pi(\mathbf{s} \cdot e^*) + (1 - p(e^*))u_\pi(\mathbf{s} \setminus e^*)$,
    $\pi(\mathbf{s}) := e^*$.
  end for
end for
return π

The computational complexity of Algorithm 2 is also $O(|V|2^{|E|} + |E|3^{|E|})$. Proofs of the optimality (under the same weights) and complexity of Algorithm 2 directly follow from that of Algorithm 1.

Remark: It is noteworthy that, the proposed two DP-based algorithms generate the optimal defensive strategies regardless of the attacking strategies. In other words, the optimality of the two proposed strategies are independent of the attacking patterns adopted by the attacker. Bellman's Principle of Optimality takes credit for such independence, which indicates that starting from arbitrary state, the optimal strategy performs best among all defensive strategies.

VI. Approximate Defensive Strategy

While the two DP-based algorithms precisely characterize the features of the optimal defensive strategy, applying it into practice may generate huge computational complexity due to the NP-hard nature of our problem. Thus, it is of great necessity to design approximation algorithms that largely reduce the complexity while achieve comparable performance with regard to the optimal solution. In this section, we propose two approximate defensive strategy to strike a balance between optimality and complexity.

A. Heuristic Approach

We first present a heuristic approach that quantifies the edge vulnerability through an analogy from the centrality metrics of nodes in deterministic networks to that of edges in uncertain networks. In graph theory, the degree of a vertex v in a deterministic network, $\deg(v)$, is the number of edges incident upon v. In uncertain networks, we generalize this concept through the following definitions on *probability degree* of nodes and *connectivity weight* of edges.

Definition 3. (Probability Degree) *In an uncertain network $\mathcal{G}(V, E, p, c)$, the probability degree of a vertex v,* $\text{pdeg}(v)$*, is the sum of the existence probabilities of all edges incident upon v.*

Definition 4. (Connectivity Weight) *In an uncertain network $\mathcal{G}(V, E, p, c)$, the connectivity weight of an edge e, $w_{con}(e)$, is the sum of the probability degrees of its two endpoints.*

In the heuristic approach, the defender selects edges in a decreasing order of a ranking metric which combines the connectivity weight, existence probability and testing cost. We detail the procedure in Algorithm 3.

Algorithm 3 The Heuristic Approach

Input: Uncertain network $\mathcal{G}(V, E, p, c)$.
Output: An approximate defensive strategy π.

Initialize: Network state $\mathbf{s} := (*, *, \cdots, *)$, number of edges selected per stage d_t, set of untested edges $E_u^{\mathbf{s}} := E$, set of edges selected by the attacker $E_a := \emptyset$.
Compute $r(e) = w_{con}(e)p(e)/c(e)$ for each $e \in E$.
repeat at each stage:
  Update E_a and set $\mathbf{s}_e := 0$ for each $e \in E_a$.
  $E_u^{\mathbf{s}} := E_u^{\mathbf{s}} \setminus E_a$.
  for $i = 1$ to d_t **do**
    $\pi(\mathbf{s}) := \text{argmax}_{e \in E_u^{\mathbf{s}}} r(e)$.
    $\mathbf{s}_{\pi(\mathbf{s})} := 1$ if $\pi(\mathbf{s})$ exists and 0 otherwise.
    $E_u^{\mathbf{s}} := E_u^{\mathbf{s}} \setminus \{\pi(\mathbf{s})\}$.
  end for
until the end of adversary
return π

We now argue the rationality of the ranking metric $r(e)$. To start with, the definition of *connectivity weight* is quite straightforward, since the connectivity weight of an edge can be regarded as the expected number of edges connected to that edge. The edge with a larger connectivity weight tends to be more vulnerable (therefore crucial) in the network connectivity. In other words, if we conceal an edge with larger weight, we are likely to maintain a larger remaining connected component. Besides, a high existence probability of an edge is bound to increase the chance of a selected edge being existent, so that the defender will not likely 'miss the shot' when testing. In the contrary, the testing cost of an edge contributes negatively to the ranking, since the defender aims to minimize the total testing cost. An overall consideration of the aforementioned three factors results in the proposed ranking metric.

Compared with the two optimal strategies, the heuristic approach reduces the time complexity to $O(|E| \log |E|)$, since we only need to precompute and rank $r(e)$ for all edges initially. Despite the simplicity of implementation, as demonstrated in the experiments, this heuristic approach exhibits surprising superiority over other baselines.

B. Minimax-based Adaptive Greedy Policy

A weakness of the heuristic approach is the lack of performance guarantee. To design an approximate defensive strategy with theoretical approximation ratio, we combine the *minimax* rule from game theory with the *adaptive greedy policy* for adaptive stochastic maximization.

1) Adopting Minimax Rule: Since the connectivity maintenance problem can be cast as a two-player zero-sum game, it is intuitive to efficiently solve the problem by adopting the idea from game theory [27]. Considering the feature of our model, i.e., uncertainty of the network, we refer to the *minimax* rule, which is a decision rule for *mini*mizing the possible loss for a worst-case (*max*imum loss) scenario.

To begin with, we introduce the notion of the *Largest Potential Connected Component (LPCC)* to quantify the loss suffered by the defender.

Definition 5. (Largest Potential Connected Component) *The largest potential connected component of a temporary state* $\mathbf{s}$ *observed by the defender is the largest connected component formed by the untested edges and the edges successfully destroyed by the attacker (if observable).*

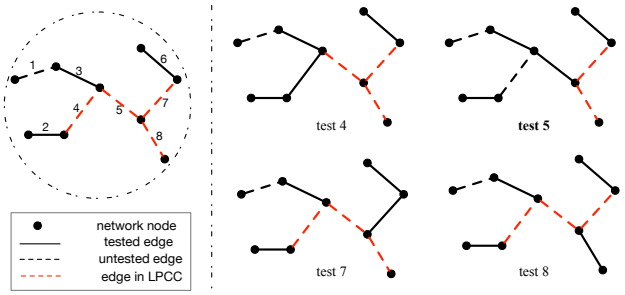


Fig. 2. An LPCC example. Left: The network state observed by the defender at current stage. Right: Four possible outcomes of changes in LPCC depending on the edge tested at next stage. In this example, edge 5 should be tested at next stage to decrease the size of the LPCC from 5 to 3.

For the defender, the worst-case scenario starting from a temporary state $\mathbf{s}$ is that the attacker has destroyed sufficient existing edges after multiple stages to make the largest connected component formed by the destroyed edges match the initial LPCC in size, indicating that the network connectivity

is destroyed to the maximum extent. Therefore, at each stage, the defender needs to minimize the size of the LPCC in order to minimize the possible loss for a worst-case scenario. An example to illustrate the selection rule for the defender is shown in Figure 2.

2) Applying Adaptive Greedy Policy: To implement the *minimax* rule, we apply the *adaptive greedy policy* for the adaptive stochastic maximization problem [28] which aims to maximize a utility function $f : S \to \mathbb{R}_{\geq 0}$ that depends on which edges we select and which state each edge is in. To start with, we introduce the following preliminaries in the language of the connectivity maintenance problem.

Definition 6. (Subrealization) *A state* $\mathbf{s}$ *is a subrealization of a state* $\mathbf{s}'$ *if* $\mathbf{s}_e = \mathbf{s}'_e$ *for all* $\mathbf{s}_e \neq *$. *Equivalently,* $\mathbf{s}$ *is a subrealization of* $\mathbf{s}'$ *if and only if, when viewed as relations,* $\mathbf{s} \subseteq \mathbf{s}'$.

Definition 7. (Conditional Expected Marginal Benefit) *Given a state* $\mathbf{s}$*, an untested edge* e *and a utility function* f*, the conditional expected marginal benefit of* e *conditioned on having observed* $\mathbf{s}$ *is* $\Delta(e|\mathbf{s}) := p(e)f(\mathbf{s}{\cdot}e) + (1-p(e))f(\mathbf{s}\backslash e) - f(\mathbf{s})$.

Definition 8. (Adaptive Monotonicity) *A utility function* $f : S \to \mathbb{R}_{\geq 0}$ *is adaptive monotone if the conditional expected marginal benefit of any untested edge in any state is nonnegative, i.e., for all* $\mathbf{s} \in \mathcal{S}$ *and all* $e \in E_u^{\mathbf{s}}$ *we have* $\Delta(e|\mathbf{s}) \geq 0$.

Definition 9. (Adaptive Submodularity) *A utility function* $f : S \to \mathbb{R}_{\geq 0}$ *is adaptive submodular if the conditional expected marginal benefit of any fixed edge does not increase as more edges are tested. Formally,* f *is adaptive submodular if for all temporary states* $\mathbf{s}$ *and* $\mathbf{s}'$ *such that* $\mathbf{s}$ *is a subrealization of* $\mathbf{s}'$ *(i.e.,* $\mathbf{s} \subseteq \mathbf{s}'$*), and for all* $e \in E_u^{\mathbf{s}'}$*, we have* $\Delta(e|\mathbf{s}) \geq \Delta(e|\mathbf{s}')$.

The goal of *adaptive stochastic maximization* is to find a policy π that maximizes the expected value of the utility function f which is both adaptive monotone and adaptive submodular, subject to limitations on the accumulated cost when selecting edges following π. To incorporate the idea of *minimax*, we define our utility function $f : S \to \mathbb{R}_{\geq 0}$ on state $\mathbf{s}$ as *the difference between the initial size of the LPCC and the size of the LPCC in* $\mathbf{s}$. We further notice that, due to the definition of LPCC, for a state $\mathbf{s}$ and an untested edge e in $\mathbf{s}$ observed by the defender, we must have $f(\mathbf{s}{\cdot}e) = f(\mathbf{s}\backslash e)$ and the conditional expected marginal benefit is thus simplified to $\Delta(e|\mathbf{s}) := f(\mathbf{s}\backslash e) - f(\mathbf{s})$. Theorem 4 demonstrates the adaptive monotonicity and the adaptive submodularity of the utility function f we defined.

Theorem 4. *The utility function* f *is both adaptive monotone and adaptive submodular.*

Proof: The adaptive monotonicity of f can be easily proved by noticing that the size of the LPCC in a state $\mathbf{s}$ will never increase when the defender selects an untested edge e, regardless of the existence of e.

To prove the adaptive submodularity of f, we consider three cases categorized by the position of the selected edge e. If e does not belong to the LPCC, then the removal of e will make no difference to the conditional expected marginal benefit, regardless of the stage where e is selected. If e belongs to the LPCC, then either the removal of e makes no difference to the size of the LPCC or the removal of e divides the LPCC into two components, in which case the conditional expected marginal benefit is the smaller size of the two. Obviously, if edge e is selected after multiple stages instead of at the current stage, the conditional expected marginal benefit will never increase, which completes the proof. ■

3) Minimax-based Adaptive Greedy Algorithm: According to the *Adaptive Greedy Policy*, at each stage the defender selects untested edges in descending order of $\Delta(e|\mathbf{s})/c(e)$. Under the same constraint on cost, such a policy has an approximation ratio of $(1-1/e)$, namely $f(\pi) > (1-1/e)f(\pi^*)$, where $f(\pi)$ and $f(\pi^*)$ denote the the final value of f when following policy π and optimal policy π^* respectively. We present the minimax-based adaptive greedy policy in Algorithm 4, which has a time complexity of $O(|E|\log|E|)$ due to the sort of untested edges at each stage.

Algorithm 4 The Minimax-based Adaptive Greedy Policy

Input: Uncertain network $\mathcal{G}(V, E, p, c)$.
Output: An approximate defensive strategy π.

Initialize: Network state $\mathbf{s} := (*, *, \cdots, *)$, number of edges selected per stage d_t, set of untested edges $E_u^{\mathbf{s}} := E$, set of edges selected by the attacker $E_a := \emptyset$, utility function f.
Compute the initial size of LPCC in $\mathbf{s}$.
repeat at each stage:
  Update E_a and set $\mathbf{s}_e := 0$ for each $e \in E_a$.
  $E_u^{\mathbf{s}} := E_u^{\mathbf{s}} \setminus E_a$.
  for $i = 1$ to d_t **do**
    $\pi(\mathbf{s}) := \text{argmax}_{e \in E_u^{\mathbf{s}}} \{\frac{f(\mathbf{s}\backslash e) - f(\mathbf{s})}{c(e)}\}$.
    $\mathbf{s}_{\pi(\mathbf{s})} := 1$ if $\pi(\mathbf{s})$ exists and 0 otherwise.
    $E_u^{\mathbf{s}} := E_u^{\mathbf{s}} \setminus \{\pi(\mathbf{s})\}$.
  end for
until the end of adversary
return π

Remark: The utility function f we define relaxes the model constraint in that the defender may not need to acquire full prior knowledge of function p in the network. In effect, we view Algorithm 4 as a framework for devising defensive strategies for a wide range of network models through the selection of sophisticated scenario-specific utility functions.

VII. Experiments

We now evaluate the performance of the proposed defensive strategies through extensive experiments on various datasets.

A. Experimental Setup

1) Datasets: We adopt one synthetic and two real-world datasets to construct the uncertain networks. The two real-world datasets respectively reflect the characteristics of social networks and communication networks, which are networks that are apt to adversarial attack in real-life scenarios. Descriptions of these datasets are listed as follows:

- **Erdős-Rényi Networks:** Two uncertain networks are constructed by ER graph models $G(6, 0.2)$ and $G(100, 0.02)$. The uniform testing cost of each edge in both networks is set to 1.
- **Facebook Ego Networks [29]:** This datasets consists of ego network (friends lists) with 333 nodes and 5038 edges from Facebook. We extract 18 ego networks, each with 100 nodes, to construct 18 uncertain networks.
- **EU Email Networks [30]:** This datasets consists of email data network with 265214 nodes and 420045 edges generated in a large European research institution from October 2003 to May 2005. We extract 18 email networks, each with 100 nodes, to construct 18 uncertain networks.

We turn the initial directed email network into an undirected one by creating an edge between nodes i and j if either there is a directed edge from i to j or from j to i in the initial dataset. For each uncertain network constructed from real-world datasets, Jaccard's coefficient [31] is adopted to assign each edge its existence probability. Specifically, for an edge $e = (u, v)$, $p(e) = |\mathcal{N}(u) \bigcap \mathcal{N}(v)|/|\mathcal{N}(u) \bigcup \mathcal{N}(v)|$, where $\mathcal{N}(u)$ denotes the set of neighbors of node u. The testing cost of each edge is generated from a Gaussian distribution with mean 30 and standard deviation 10 (negative part truncated).

2) Methodology: To measure the performance of different defensive strategies, for each uncertain network we generate 100 deterministic networks by sampling from the distribution of existence probabilities of edges. On each deterministic network, different defensive strategies are run 10 times, each time under a certain attacking strategy which is either an oblivious attack that randomly selects edges and is observable by the defender or an adaptive attack that selects edges in a decreasing order of their existence probabilities and is unobservable by the defender. The defense ends when the size of the largest remaining connected component stabilizes. The metrics of a strategy in an uncertain network, i.e., the expected size of the largest remaining connected component and the expected total testing cost, is approximated by the average of size and cost incurred by the strategy through 1000 trials.

3) Strategies in Comparison: We evaluate the performance of the proposed defensive strategies against two baselines, namely random defensive strategy and no-defense strategy. All strategies in comparison are listed as follows:

- **Optimal Defensive Strategy (OPT):** The optimal strategy generated by Algorithm 1 proposed in Section V. Due to its prohibitive computational complexity, OPT is simulated only for a 6-node Erdős-Rényi network.
- **Heuristic Approach (HEU):** The heuristic strategy generated by Algorithm 3 proposed in Section VI.
- **Minimax-based Adaptive Greedy Policy (MAG):** The adaptive greedy approach incorporating minimax rule generated by Algorithm 4 in Section VI.
- **Random Defensive Strategy (RAND):** The defender randomly selects edges to test at each stage of adversary.
- **No-defense Strategy (NOD):** The defender takes no defensive action during the whole process of adversary.

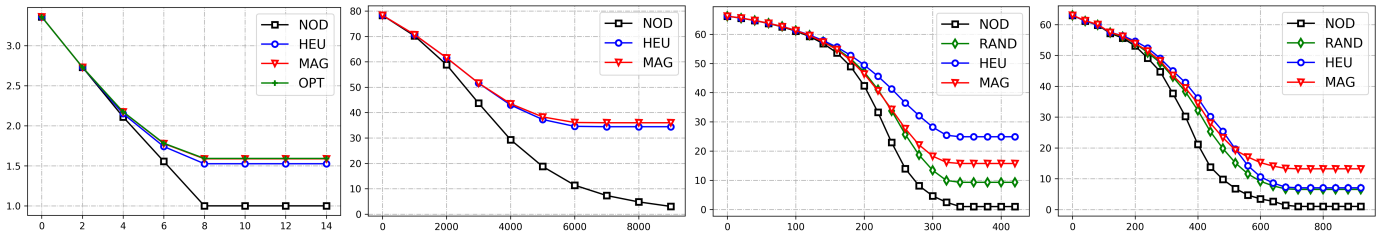
Due to the requirement of subjective defender-supplied weights, the optimal weighted defensive strategy generated by Algorithm 2 is not included in the comparison.

B. Performance Analysis

The optimality of OPT in ER networks is demonstrated in Figure 3(a), with an expected size 1.592 of the remaining largest connected component compared to NOD with size 1, HEU with size 1.526 and MAG with size 1.587. For large ER networks, Figure 3(b) shows the superiority of MAG over other baselines. We further notice that, HEU degrades to RAND in this case since all the edges in an ER network have the same existence probability and testing cost. Therefore, for uncertain networks with near uniform parameter setting, we speculate that it is relatively effective to maintain its connectivity through equal treatment of edges.

Tables II and III list the detailed outcomes in two real-world datasets under both oblivious and adaptive attack. The results are in the form of a/b where a denotes the ratio of the expected size of the largest remaining connected component to the average size of the initial largest connected component and b denotes the expected total testing cost. Bold and underlined figures are respectively the best results for a and b in a network. For a straightforward illustration, Figures 3(c) and 3(d) plot the process of an adversary in EU Email network under oblivious attack and an adversary in Facebook ego network under adaptive attack.

Under oblivious attack that is observable by the defender, HEU achieves superiority in both size and cost despite its ease of implementation. Such a phenomenon validates the notion of connectivity weight. The reason probably lies in that this heuristic approach fully utilizes the accessible knowledge of parameters in the uncertain network, which is unavailable for the attacker. MAG, on the other hand, also performs well in



(a) $G(6, 0.2)$ (b) $G(100, 0.02)$ (c) EU Email Network (d) Facebook Ego Network

Fig. 3. Experimental results with x-coordinate indicating the number of stages and y-coordinate indicating the expected size of largest remaining connected component. (a) Results in $G(6, 0.2)$ under oblivious attack with $a_t = 1$ and $d_t = 1$. (b) Results in $G(100, 0.02)$ under oblivious attack with $a_t = 1$ and $d_t = 1$. (c) An adversary process in EU Email network under oblivious attack. (d) An adversary process in Facebook ego network under adaptive attack.

TABLE II
EXPERIMENTAL RESULTS IN FACEBOOK EGO NETWORKS

Oblivious Attack	$a_t = 40, d_t = 1$			$a_t = 50, d_t = 1$			$a_t = 60, d_t = 1$		
	1	2	3	4	5	6	7	8	9
HEU	**0.427**/2569	**0.298**/4299	**0.140**/3240	**0.199**/2137	**0.354**/2136	**0.268**/2356	**0.204**/1808	**0.160**/2805	**0.201**/2041
MAG	0.254/3680	0.148/7126	0.129/3994	0.138/3064	0.194/2943	0.201/2926	0.109/2612	0.133/4823	0.138/2536
RAND	0.124/3640	0.079/6808	0.071/4068	0.063/3113	0.102/2963	0.107/2947	0.056/2683	0.072/4496	0.085/2701
NOD	0.016/——	0.017/——	0.018/——	0.017/——	0.016/——	0.016/——	0.017/——	0.019/——	0.024/——
Adaptive Attack	$a_t = 3, d_t = 1$			$a_t = 5, d_t = 1$			$a_t = 10, d_t = 1$		
	1	2	3	4	5	6	7	8	9
HEU	0.112/6371	0.086/5053	0.144/5115	0.102/3166	0.078/2823	0.090/3627	0.043/1340	0.045/856	0.042/828
MAG	**0.210**/10712	**0.165**/6975	**0.182**/7310	**0.153**/5868	**0.125**/5316	**0.145**/6129	**0.090**/3617	**0.072**/2769	**0.078**/2874
RAND	0.103/10655	0.108/6951	0.118/7522	0.079/5698	0.068/5207	0.081/6229	0.047/3679	0.048/2734	0.046/2951
NOD	0.016/——	0.019/——	0.020/——	0.018/——	0.017/——	0.019/——	0.017/——	0.018/——	0.017/——

TABLE III
EXPERIMENTAL RESULTS IN EU EMAIL NETWORKS

Oblivious Attack	$a_t = 40, d_t = 1$			$a_t = 50, d_t = 1$			$a_t = 60, d_t = 1$		
	1	2	3	4	5	6	7	8	9
HEU	**0.145**/1761	**0.196**/4340	**0.143**/4353	**0.154**/3398	**0.278**/2068	0.072/1112	0.087/1210	0.082/800	**0.203**/1636
MAG	0.113/4147	0.146/6750	0.105/7052	0.104/5074	0.178/3015	**0.087**/3166	**0.103**/2744	**0.087**/2707	0.147/2365
RAND	0.054/4098	0.078/6690	0.059/6756	0.051/5269	0.094/2903	0.049/3091	0.049/2709	0.044/2772	0.077/2400
NOD	0.014/——	0.018/——	0.016/——	0.016/——	0.017/——	0.015/——	0.016/——	0.015/——	0.016/——
Adaptive Attack	$a_t = 3, d_t = 1$			$a_t = 5, d_t = 1$			$a_t = 10, d_t = 1$		
	1	2	3	4	5	6	7	8	9
HEU	0.072/3833	0.075/4556	0.109/4618	0.052/2118	0.054/3262	0.044/1415	0.035/1451	0.045/902	0.041/751
MAG	**0.151**/6220	**0.191**/6778	**0.145**/7503	**0.111**/4514	**0.136**/6218	**0.092**/2552	**0.070**/3688	**0.063**/2266	**0.060**/2105
RAND	0.079/6256	0.116/6732	0.094/7229	0.062/4438	0.080/6036	0.058/2760	0.041/3600	0.046/2289	0.044/2253
NOD	0.017/——	0.020/——	0.017/——	0.017/——	0.016/——	0.020/——	0.014/——	0.020/——	0.018/——

preserving the largest connected component, but is liable to incur more cost than HEU.

Under adaptive attack that is unobservable by the defender, the advantage of HEU in preserving the network connectivity is largely weakened. In some drastic cases, the remaining size of HEU is even smaller than that of a trivial random strategy, which is likely due to the fact that the attacker is fully aware of the parameters of the network and thus each attack is well-targeted. Under these severe circumstances, MAG outperforms other strategies in size, which verifies that the incorporation of minimax rule serves its purpose of minimizing the loss in a worst-case scenario.

In general, we conclude that both HEU and MAG achieve decent performance in various datasets. For scenarios where the network knowledge of the defender far outweighs that of the attacker, HEU functions as a better approach that is both economic and efficient. For scenarios where the attacker is knowledgeable and tricky, MAG serves as a preferable policy which is both secure and effective.

VIII. CONCLUSION

In this paper, we investigate the problem of connectivity maintenance in adversarial uncertain networks. Given a general uncertain network modeled as a random graph with each edge associated with an existence probability and a testing cost, our goal is to design general adaptive defensive strategies to maximize the expected size of the largest remaining connected component at the end of adversary with minimum expected testing cost, regardless of the attacking strategies. The complexity of our problem is clarified by proving its NP-hardness. To address the problem, we first design optimal defensive strategies based on dynamic programming and multi-objective optimization. Due to the prohibitive complexity of computing an optimal strategy, we then design two approximate strategies respectively based on heuristic analogy of centrality metrics from deterministic networks to uncertain networks and adaptive greedy policy combined with minimax rule from game theory. The superiority of the proposed strategies over baselines is justified through extensive experiments.

ACKNOWLEDGMENT

This work was supported by National Key R&D Program of China 2018YFB2100302, NSF China (No. 42050105, 62020106005, 62061146002, 61960206002, 61822206, 61832013, 61829201), 2021 Tencent AI Lab Rhino-Bird Focused Research Program (No. JR202132), and the Program of Shanghai Academic/Technology Research Leader under Grant No. 18XD1401800.

REFERENCES

[1] N. Saeed, A. Celik, M.-S. Alouini, and T. Y. Al-Naffouri, "Performance analysis of connectivity and localization in multi-hop underwater optical wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 18, no. 11, pp. 2604–2615, 2018.

[2] E. G. Tajeuna, M. Bouguessa, and S. Wang, "Modeling and predicting community structure changes in time-evolving social networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 31, no. 6, pp. 1166–1180, 2018.

[3] Z. Tan, C. Liu, Y. Mao, Y. Guo, J. Shen, and X. Wang, "Acemap: A novel approach towards displaying relationship among academic literatures," in *Proceedings of the 25th international conference companion on world wide web*, 2016, pp. 437–442.

[4] T. N. Dinh and M. T. Thai, "Assessing attack vulnerability in networks with uncertainty," in *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2015, pp. 2380–2388.

[5] R. Du, G. Dong, L. Tian, and R. Liu, "Targeted attack on networks coupled by connectivity and dependency links," *Physica A: Statistical Mechanics and its Applications*, vol. 450, pp. 687–699, 2016.

[6] N. Abuzainab and W. Saad, "Dynamic connectivity game for adversarial internet of battlefield things systems," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 378–390, 2017.

[7] Y. Nugraha, A. Cetinkaya, T. Hayakawa, H. Ishii, and Q. Zhu, "Dynamic resilient network games considering connectivity," in *2020 59th IEEE Conference on Decision and Control (CDC)*. IEEE, 2020, pp. 3779–3784.

[8] P. Gill, N. Jain, and N. Nagappan, "Understanding network failures in data centers: measurement, analysis, and implications," in *Proceedings of the ACM SIGCOMM 2011 conference*, 2011, pp. 350–361.

[9] C. Bo, X.-Y. Li, T. Jung, X. Mao, Y. Tao, and L. Yao, "Smartloc: Push the limit of the inertial sensor based metropolitan localization using smartphone," in *Proceedings of the 19th annual international conference on Mobile computing & networking*, 2013, pp. 195–198.

[10] D. D. K. Rathinam, D. Surendran, A. Shilpa, A. S. Grace, and J. Sherin, "Modern agriculture using wireless sensor network (wsn)," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*. IEEE, 2019, pp. 515–519.

[11] S. Ji, R. Beyah, and Z. Cai, "Snapshot and continuous data collection in probabilistic wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 3, pp. 626–637, 2013.

[12] X. Fu, Z. Xu, Q. Peng, L. Fu, and X. Wang, "Complexity vs. optimality: Unraveling source-destination connection in uncertain graphs," in *IEEE INFOCOM 2017-IEEE Conference on Computer Communications*. IEEE, 2017, pp. 1–9.

[13] C.-F. Chiasserini, M. Garetto, and E. Leonardi, "De-anonymizing clustered social networks by percolation graph matching," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 12, no. 2, pp. 1–39, 2018.

[14] Z. Wu and Z. Li, "Distributed robust optimization algorithms over uncertain network graphs," *IEEE Transactions on Cybernetics*, 2020.

[15] D. Yu, Y. Zou, J. Yu, Y. Zhang, F. Li, X. Cheng, F. Dressler, and F. C. Lau, "Implementing the abstract mac layer in dynamic networks," *IEEE Transactions on Mobile Computing*, vol. 20, no. 5, pp. 1832–1845, 2020.

[16] A. Saha, R. Brokkelkamp, Y. Velaj, A. Khan, and F. Bonchi, "Shortest paths and centrality in uncertain networks," *Proceedings of the VLDB Endowment*, vol. 14, no. 7, pp. 1188–1201, 2021.

[17] D. Cheng, C. Chen, X. Wang, and S. Xiang, "Efficient top-k vulnerable nodes detection in uncertain graphs," *IEEE Transactions on Knowledge and Data Engineering*, 2021.

[18] M. Johnston, H.-W. Lee, and E. Modiano, "A robust optimization approach to backup network design with random failures," *IEEE/ACM Transactions on Networking*, vol. 23, no. 4, pp. 1216–1228, 2014.

[19] S. Zhao and X. Wang, "Node density and delay in large-scale wireless networks with unreliable links," *IEEE/ACM Transactions on Networking*, vol. 22, no. 4, pp. 1150–1163, 2013.

[20] P. Parchas, F. Gullo, D. Papadias, and F. Bonchi, "The pursuit of a good possible world: extracting representative instances of uncertain graphs," in *Proceedings of the 2014 ACM SIGMOD international conference on management of data*, 2014, pp. 967–978.

[21] S. Piltyay, A. Bulashenko, and I. Demchenko, "Wireless sensor network connectivity in heterogeneous 5g mobile systems," in *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*. IEEE, 2020, pp. 625–630.

[22] T. Fukunaga, "Adaptive algorithm for finding connected dominating sets in uncertain graphs," *IEEE/ACM Transactions on Networking*, vol. 28, no. 1, pp. 387–398, 2020.

[23] A. D. Flaxman, A. M. Frieze, and J. Vera, "Adversarial deletion in a scale-free random graph process," *Combinatorics, Probability and Computing*, vol. 16, no. 2, pp. 261–270, 2007.

[24] M. O. Ball, "Computational complexity of network reliability analysis: An overview," *Ieee transactions on reliability*, vol. 35, no. 3, pp. 230–239, 1986.

[25] R. E. Bellman and S. E. Dreyfus, *Applied dynamic programming*. Princeton university press, 2015.

[26] K. Miettinen, *Nonlinear multiobjective optimization*. Springer Science & Business Media, 2012, vol. 12.

[27] R. B. Myerson, *Game theory*. Harvard university press, 2013.

[28] D. Golovin and A. Krause, "Adaptive submodularity: Theory and applications in active learning and stochastic optimization," *Journal of Artificial Intelligence Research*, vol. 42, pp. 427–486, 2011.

[29] J. J. McAuley and J. Leskovec, "Learning to discover social circles in ego networks." in *NIPS*, vol. 2012. Citeseer, 2012, pp. 548–56.

[30] J. Leskovec, J. Kleinberg, and C. Faloutsos, "Graph evolution: Densification and shrinking diameters," *ACM transactions on Knowledge Discovery from Data (TKDD)*, vol. 1, no. 1, pp. 2–es, 2007.

[31] D. Liben-Nowell and J. Kleinberg, "The link-prediction problem for social networks," *Journal of the American society for information science and technology*, vol. 58, no. 7, pp. 1019–1031, 2007.