Topology design under adversarial dynamics

Ertugrul N. Ciftcioglu∗†, Siddharth Pal†, Kevin S. Chan†, Derya H. Cansever§, Ananthram Swami†, Ambuj Singh¶, and Prithwish Basu†

∗IBM Research, Yorktown Heights, NY 10598
†U.S. Army Research Lab, Adelphi, MD 20783
§Army CERDEC, Aberdeen Proving Ground, MD 21001
¶University of California Santa Barbara, Santa Barbara, CA 93106

Abstract—We study the problem of network topology design within a sequence of policy-compliant topologies as a game between a designer and an adversary. At any time instant, the designer aims to operate the network in an optimal topology within this policy compliant sequence with respect to a desired network property. Simultaneously, the adversary counters the designer trying to force operation in a suboptimal topology. We show the existence of various mixed strategy equilibria in this game and systematically study its structural properties. We study the effect of parameters, and characterize the steady state behavior of the underlying Markov chain. While the intuitive adversarial strategy here is to attack links appearing early in the topology sequence, the Nash Equilibrium strategy is for the designer to defend the earlier links and for the adversary to attack the later links. We validate these properties through two use cases with example sets of network topologies.

I. INTRODUCTION

Networks are used to transport objects or information of a specific type between different nodes that are interconnected by means of links. Examples include vehicles in a road network, data packets in the Internet, messages in an online social network, signals in a biological network, electricity in power grids, etc. While networks often grow in a self-organized fashion or based on some natural user demand, they often need to be systematically designed so that they can provide a certain functionality to its users. Sometimes, an existing network needs to be redesigned by adding new links to augment its topology. Such network topology redesign has received significant attention in the graph theory and network science literature. However, the research till date has focused on augmentation of static graphs for optimizing a plethora of network properties [1], [2], [3].

In the real world, however, networks suffer from dynamics caused by the environment, which is usually random and varies over time, or by an intelligent adversary who is determined to disrupt the network. In this paper, we consider an adversarial setting in which a network designer continually attempts to grow the network to a denser state over time, whereas the adversary simultaneously attempts to thwart those attempts. This has applications in cyber-infrastructure design and design of agile command and control networks. The extent to which a designer is allowed to alter a network may be limited by policy, thus bounding the set of allowed topologies within which the system needs to operate. This is because the allowed topologies may reflect organizational and operational constraints and may lead to unintended consequences if not complied with. Also, the designer can grow the network from one allowed topology to another by adding links in a certain policy-compliant order in order to honor precedence constraints (illustrated in Fig. 1).

We assume that if an adversary attacks a certain link and the designer does not defend it simultaneously, then the link will be disabled with a certain probability and the designer may not be able to restore it immediately. Hence, it would then be forced by policy to “fall back” to one of the allowed topologies using the remaining links unaffected by the adversarial attack. Under such circumstances, the designer needs to strategically consider how much of a potential hit in the network property she is willing to take while balancing it with the cost of defending a link or growing the network to an even larger size. The adversary, similarly, takes the designer’s strategy space into account in order to devise her own best strategy in order to inflict maximum damage. For instance, suppose a group of users wants to achieve a secure collaborative mission using a wireless network. The collaboration is organized along a logical organizational command-and-control topology overlaid on a wireless network underlay, e.g., as sketched in [4].

These communications are assumed to be secured by long predetermined secret keys which are difficult to compromise. However, to increase the operational tempo, new logical links (or shortcuts) are added to the organizational topology. Since these shortcut links are ephemeral, they are secured only by short pairwise secret keys certified by a certificate authority (CA) at the start of the mission. The shortcut links are typically added in a certain order of precedence, e.g., a logical link is established between two salesmen (S) only after one has been

Figure 1. A sequence of allowed topologies with the densification property.
established between their respective managers (M). Thus if the M-M link’s key is compromised, its certificate as well as the S-S link’s certificate will have to be revoked. To ensure such hierarchical means of secure communication, CA issues certificates based on existing certificate chains. If a compromise or vulnerability is found in a certificate within a certificate chain, any links secured with that or any intermediate certificate is considered to be compromised. Therefore, in order to maintain secure communications, the network must operate with any links generated with the remaining certificate chain. At some later time, the network administrator may choose to issue new certificates based on the remaining valid certificates.

Scenarios such as the one proposed above can be naturally modeled within a non-cooperative game theoretic framework where both the designer and adversary are attempting to maximize their own utility, defined as a function of the network property under consideration as well as the costs incurred to support or attack a certain portion of the network topology. In this paper, we analyze the network design game in an adversarial environment. Analyzing the evolution of the network in such a setting involves integration of several modules. First, the equilibrium mixed strategies of the designer and adversary are characterized for each stage, which results in a probability mass function on the set of actions for each player. Next, utilizing the equilibrium mixed strategies, we characterize the one-step transition probabilities between the different possible topologies. Finally, we use the one-step transition probability matrix to characterize the steady state probabilities of the different topologies.

Throughout this study, we identify conditions on several system parameters under which the network can grow, and several structural properties of the equilibrium mixed strategies.

The following are the main contributions of the paper: 1) modeling and formulation of a topology selection game for adversarial environments, 2) analysis of the dynamic game and characterization of requirements on system parameters as a function of network properties, along with several structural properties of the equilibrium strategies, and 3) characterization of steady state system behavior that results from the tension between the designer’s strategies to grow the network connectivity and the adversary’s strategies to shrink it.

A. Organization of the paper

In this paper, we analyze the network design game in an adversarial environment. Analyzing the evolution of the network in such a setting involves integration of several modules. First, the equilibrium mixed strategies of the designer and adversary are characterized for each stage, which results in a probability mass function on the set of actions for each player. Next, utilizing the equilibrium mixed strategies, we characterize the one-step transition probabilities between the different possible topologies. Finally, we use the one-step transition probability matrix to characterize the steady state probabilities of the different topologies.

Throughout this study, we identify conditions on several system parameters under which the network can grow, and several structural properties of the equilibrium mixed strategies.

The following are the main contributions of the paper: 1) modeling and formulation of a topology selection game for adversarial environments, 2) analysis of the dynamic game and characterization of requirements on system parameters as a function of network properties, along with several structural properties of the equilibrium strategies, and 3) characterization of steady state system behavior that results from the tension between the designer’s strategies to grow the network connectivity and the adversary’s strategies to shrink it.

B. Related work

Static network topology redesign has received a lot of attention in the theoretical computer science literature. Specifically, it has focused on augmentation of static graphs for improved fault tolerance (maximization of connectivity [1]) or information flow properties (minimization of diameter [2], eccentricity and average shortest path length [3]). In contrast, here we focus on the tension that arises from the simultaneous actions of network (re)design and attack.

Network formation games have been proposed to characterize how individuals connect to others to create networks in order to selfishly benefit from some property of the resulting network [5]. However, games between adversaries and designers are not considered in that framework.

Recently, there has been significant interest in developing game theoretic formulations for scenarios where adversaries and designers compete for a resource [6] or multiple resources [7]. However, they do not consider topology design issues. Gueye et al. consider network topology design in an adversarial environment [8]. In their setting, the network manager chooses a spanning tree of the network and the adversary targets a specific set of links, where the network property of interest is connectivity. In particular, they show that at a Nash equilibrium, the adversary targets a critical set of vulnerable links. While our formulation considers general network properties, we also incorporate the possibility of link addition not considered in [8]. Ma et al. study the continual process of infrastructure protection where the adversary and the designer interact to produce dynamic states affecting their best actions [9]. They use zero-sum Markov games to model such interactions subject to underlying uncertainties of events and actions. They too do not consider the problem of network augmentation.

To the best of our knowledge, ours is the first work that focuses on the situation where a system could exist in one of several allowed topology states with the designer dynamically attempting to improve the topology and an intelligent adversary continually attempting to thwart those attempts. Recently, we have considered another problem of topology control among a set of allowed topologies in a time-varying contested environment [10], where the environment disrupted random links regardless of their importance. In contrast, the current work considers the presence of an intelligent adversary, which would specifically target links in order to inflict maximal damage to the network property under consideration.

II. TOPOLOGY DESIGN IN ADVERSARIAL ENVIRONMENTS

We consider a model where the network designer wants to or can only operate in a finite number of policy-compliant topologies. Moreover, these topologies possess a hierarchical ordering such that there is a strict subset relation between topologies of successive indices, and the topologies densify as topology index increases. In our model each successive topology differs by one link, i.e., \( G_0 \subset G_1 \subset G_2 \ldots \subset G_K \). Given such a setting, we consider a two-player topology selection/control game where the designer (or defender) wants to maintain a denser network which yields desirable network properties (e.g., low path lengths, low network diameter, high connectivity etc.), while an adversary tries to disrupt the new links in order to maximally damage network functionality. We consider successive series of actions, hence an evolution, where the objective of each user is to maximize its own time average payoff (or minimize costs for the designer).

A. System Model

1) State: We denote the state by the topology index, \( k \). We assume that there are at most \( K+1 \) different topology states,
and a sequence of $K$ links $l_1, \ldots, l_K$ is already known to both designer and adversary. The difference between states $j - 1$ and $j$ is link $l_j$.

2) Actions: Assuming we are currently at state $k$, we consider the following set of actions:

**Designer:** Defend link $l_i$, $i \in 1, \ldots, k$ or add new link $l_{k+1}$ ($k+1$ possible actions). We assume that the designer cannot add and protect a new link at the same time.

**Adversary:** Attack existing link $l_j$ where $j \leq k$, or anticipated (simultaneously formed) link $l_{k+1}$ ($k+1$ possible actions). Note that in our model, we assume that links in the original topology $G_0$ are well protected and as such, they are not subject to attacks by the adversary. We also assume that the designer and the attacker act simultaneously at each stage of the game.

3) State Transitions: If the designer protects the link that was attacked, then the state remains the same, at $k$. If the designer does not protect the attacked link, then we assume that the adversary is successful with probability $p$. If the attack succeeds, then the attacked link $l_j$ is disabled and the state decreases to the highest allowed (policy-compliant) state, i.e. $j - 1$. The transition to the next step only depends on the current state and the actions, along with the attack success probability $p$, specifically

$$s(t+1) = \begin{cases} a(t) - 1, & \text{w.p. } p, \text{if } a(t) \neq d(t) \\ s(t), & \text{w.p. } (1 - p), \text{if } a(t) = d(t) \\ s(t) + 1, & \text{w.p. } 1 - p, \text{if } d(t) = s(t) + 1 \end{cases}$$

where $a(t)$ and $d(t)$ denote the index of the associated link that the adversary and designer choose at step $t$, i.e. link $l_{a(t)}$ and link $l_{d(t)}$. Accordingly, it is a Markov game.

4) Costs: We consider two types of costs.

**Network Property Costs:** The network property costs depend on the topology with examples such as eccentricity, centrality, and connectivity. While it is difficult to characterize the behavior of all such properties, we expect the typical pattern that network property costs are convex, decreasing in increasing topology state with diminishing returns. We denote the network property cost for topology index $k$ by $g_k$.

**Operational Costs:** We differentiate between the costs of attacking an existing link and an anticipated link for the adversary. Since an existing link is likely to be more robust, we assume that the cost $\beta$ for attacking an existing link is greater than $\alpha$, the cost for attacking an anticipated link. These costs may be constant or depend on the number of links that are disabled (due to backtracking). For the designer, we denote the cost of protecting an existing link by $\delta$ and that of adding a new link by $\gamma$. The cost for adding a new link might be typically higher than that for protecting an existing link. Throughout the paper, we also consider scenarios where these costs ($\alpha$, $\beta$, $\gamma$, $\delta$) may be zero, and characterize both strategies and specify conditions on the remaining system parameters under which the network can grow.

**B. Game Formulation**

Our initial formulation is a non-zero sum game where the designer tries to minimize total costs (network property cost $g_k$ plus operational $z_k \in \{\gamma, \delta\}$ due to protection/addition), while the adversary tries to maximize the cost to the designer minus the attack cost. It is more convenient to define reward for the designer as the negative of the cost, and the aim is to maximize the “reward” or “payoff”. The expected payoff matrix can be expressed as shown in Table I. Here $g_0 > \ldots > g_{k-1} > g_k$. It can be seen that in general a pure strategy Nash equilibrium does not exist (by inspection) except in certain special scenarios. Hence, players typically adopt mixed strategies. Both players would aim to select strategies such that the other player cannot differentiate between its actions while calculating their expected utility (also known as equalizer strategy in game theory), thus resulting in a mixed strategy. Next, we provide a special condition on the attack success probability (along with an assumption on the network costs) which leads to the interesting case when the designer always decides to add a link and grow the network (a pure strategy).

### III. Properties of Strategies and Nash Equilibria

In this section, we first characterize several key structural properties for equilibrium strategies.

**A. Characterization of structural properties**

**Lemma III.1.** Suppose that the network property cost $g_k$ is concave decreasing in $k$, and adding a new link is not costlier than protecting an existing link ($\gamma \leq \delta$). Then, at current state $k$, for $p < \frac{1}{k+1}$, the designer adopts the pure strategy of always adding links. On the other hand, if network property cost $g_k$ is convex decreasing in $k$, it is not possible to spot any pure strategy for the designer by inspection if $p > \frac{1}{k+1}$. In general, regardless of the network property cost behavior, if $p < \frac{1}{k+1}$, the designer has the pure strategy of adding $l_{k+1}$.

**Proof.** The designer chooses the pure strategy of always adding links if that strategy dominates all other strategies. This implies the conditions: $g_k + \delta > pg_i + (1 - p)g_{k+1} + \gamma$, $i = 0, \ldots, k - 1$, indicating that the costs incurred in protecting a link is greater than the cost incurred in adding link ($k + 1$), while the adversary attacks link $i$. The most restrictive of these conditions in terms of $p$ is the first one since the network property cost is decreasing. If $g_0 \ldots g_k$ are concave decreasing, the negative of these $-g_0 \ldots - g_k$ are concave increasing. Let $s = \frac{1}{k+1}$, and denote the continuous relaxation of $-g_k$ as $G(k)$. We invoke the well-known Jensen’s inequality to obtain:

$$G(s \cdot 0 + (1 - s)(k + 1)) = G(k) > sG(0) + (1 - s)G(k + 1)$$

$$\implies -g_k > -\frac{1}{k+1}g_0 - \frac{k}{k+1}g_{k+1},$$

proving the second part of the Lemma. On the other hand, if $g_0 \ldots g_k$ is concave decreasing, the negatives of these are convex increasing and inequality (4) is reversed: $-g_k < -\frac{1}{k+1}g_0$.

\footnote{It is also possible to consider an arbitrary weighted sum of the two cost components $\lambda g_k + (1 - \lambda)z_k$ for any $\lambda \in [0, 1]$ depending on prioritization.}
$k+1$ links, which along with $\gamma \leq \delta$ implies that it is always optimal to grow the network. Hence, if $p < \frac{1}{k+1}$, the first part of the lemma is proven. Regardless of the network property cost being convex or concave decreasing in $k$, simple calculations reveal that if \((1-p)g_k < g_{k+1} > 1\) it is more beneficial for the designer to add $l_{k+1}$ than defending $l_{d_1}$; if \((1-p)g_k < g_{k+1} > 1\), then designer will always add $l_{k+1}$ rather than defend any link, which happens when $p < \frac{g_k - g_{k+1}}{g_{k+1} - g_k}$.

In the rest of the section, the properties are stated under the assumption that the adversary cannot attack an anticipated link. Accordingly, we can simply assume the attack cost $\beta$ is 0. We also assume for clarity that the designer costs for protecting an existing link and adding a new link ($\delta, \gamma$) are both 0.

Now, consider a mixed Nash equilibrium at state $k = (r_k^*, q_k^*)$; where the designer strategy $r_k^* = (r_k^*(1), \ldots, r_k^*(k), r_k^*(k+1))$ and the adversary strategy $q_k^* = (q_k^*(1), \ldots, q_k^*(k))$. Here, $r_k^*(j)$ is the probability allocated to strategy $j$ (defend link for $j \leq k$) for the designer while at state $k$, and $q_k^*(j)$ is the probability allocated to strategy $j$ (attack link for $j \leq k$) for the designer while at state $k$. According to the payoffs tabulated in Table I:

For an adversary action $a \in \mathbb{N}_k$ and designer action $d \in \mathbb{N}_{k+1}$ at state $k$ let the expected payoff for the designer and the adversary be denoted as $U^*_1(d,a)$ and $U^*_2(d,a)$ respectively (with $\alpha = 0$). Therefore the expected payoff for the designer at the mixed NE $\left(r_k^*, q_k^*\right)$ is

$$\sum_{d=1}^{k+1} r_k^*(d) \left( \sum_{a=1}^{k} U^*_1(d,a) q_k^*(a) \right).$$

We define

$$Q^k_k(q_k^*(m), m) = \sum_{a=1}^{k} U^*_1(d,a)q_k^*(a), \quad m = 1, 2, \ldots, k.$$  

Note that $Q^i_k(q_k^*, m)$ is the expected payoff for the designer playing action $m$ when the adversary is playing the mixed strategy $q_k^*$. Next, we state a lemma that describes certain properties on the adversary pmf $q_k^*$.

**Lemma III.2.** Consider a mixed NE of the game $(r_k^*, q_k^*)$:

1) For $d_1, d_2 \in \text{support}(r_k^*)$ with $k+1 > d_2 > d_1$, we must have

$$g_{d_1-1} - g_k \leq q_k^*(d_1) \leq g_{d_2-1} - g_k q_k^*(d_2)$$

which necessarily implies $q_k^*(d_2) \geq q_k^*(d_1)$.

2) For any $d_3 \notin \text{support}(r_k^*)$ and $d_1 \in \text{support}(r_k^*)$

$$q_k^*(d_3) \leq \frac{g_{d_1-1} - g_k}{g_{d_2-1} - g_k} q_k^*(d_1).$$

If $d_3 < d_1$, then $q_k^*(d_3) \leq q_k^*(d_1)$.

The lemma is proved in the Appendix. The first part implies that in the equilibrium scenario for two links that are being defended, a lower indexed link must be attacked with a lower probability. If that is not the case, i.e., the lower indexed link is attacked with a higher probability, then rather than defending the higher indexed link, the designer would put its resources defending the lower indexed link. According to Lemma III.2(2), if a lower indexed link is not being defended then that would imply that the attack probability is really low, at least lower than a higher indexed link being defended. The expected payoff for the adversary at the mixed NE $(r_k^*, q_k^*)$ is

$$\sum_{a=1}^{k} q_k^*(a) \left( \sum_{d=1}^{k+1} U^*_1(d,a) r_k^*(d) \right).$$

As before, we define

$$Q_k^k(r_k^*(m), m) = \sum_{d=1}^{k+1} U^*_2(d,m) r_k^*(d), \quad m = 1, 2, \ldots, k+1.$$  

Next, we state a lemma which characterizes the properties of the designer pmf $r_k^*$.

**Lemma III.3.** For a mixed NE of the game $(r_k^*, q_k^*)$, we have

1) For $a_1, a_2 \in \text{support}(q_k^*)$ with $k+1 > a_2 > a_1$, $\left| g_{a_2-1} - g_k \right| \left( 1 - r_k^*(a_2) \right) = \left| g_{a_1-1} - g_k \right| \left( 1 - r_k^*(a_1) \right)$

which necessarily implies $r_k^*(a_1) \geq r_k^*(a_2)$.

2) For any $a_3 \notin \text{support}(q_k^*)$ and $a_1 \in \text{support}(q_k^*)$

$$r_k^*(a_3) \geq 1 - \frac{g_{a_1-1} - g_k}{g_{a_3-1} - g_k} \left[ 1 - r_k^*(a_1) \right].$$

If $a_3 < a_1$, then $r_k^*(a_3) \geq r_k^*(a_1)$.

We do not prove the above lemma here, because the involved steps are very similar to that of Lemma III.2. The first part implies that in the equilibrium scenario for two different links being attacked, a lower indexed link will be defended with a greater probability. This is understandable, because, if the lower indexed link was defended with a lower probability, then it would be beneficial for the adversary to only attack the lower indexed link, rather than attacking both the links. And, according to Lemma III.3(2), if a lower indexed link is not being attacked, then that would mean the lower indexed link is being defended heavily, at least with a probability greater than a higher indexed link being attacked.

Next, we state a number of key results that are obtained from the two previous lemmas.
Proposition III.4. Consider a mixed NE of the game \((r^*_k, q^*_k)\).

1) When ordered by link index the adversary pmf \(q^*_k\) is monotonically increasing on the set support\((r^*_k)\). Similarly, the designer pmf \(r^*_k\) is monotonically decreasing on the set support\((q^*_k)\).

2) The designer will not defend an unattacked link, i.e., \(r^*_k(d) = 0\) whenever \(q^*_k(d) = 0\) for \(d < k + 1\).

3) If link \(l_d\) is being both attacked and defended, i.e., \(r^*_k(d), q^*_k(d) > 0\) then all lower indexed links will be defended, i.e., \(r^*_k(0) > 0, d_1 < d\).

4) If link \(l_d\) is not being defended, i.e., \(r^*_k(a) = 0\), then no higher indexed links will be defended, i.e., \(r^*_k(a_1) = 0\) for all \(a_1 > a\).

Proof.

1) Rewording of Lemma III.3(1) and Lemma III.2(1).

2) Clearly, the expected payoff will always be greater for the designer when she does not defend the unattacked link. Intuitively, this makes sense because a designer can always do better by not defending a link that is not being attacked, and shifting the probability mass elsewhere to those links which are being attacked.

3) Follows from Lemma III.3. Again, intuitively this makes sense because if a lower indexed link \(l_d\) is not being defended, then the adversary can do better by attacking \(l_d\) instead of \(l_d\).

4) It is readily shown using first principles that the equilibrium strategy of the designer cannot be such that a higher indexed link is being defended while a lower indexed link is not.

Next, we state a theorem that defines the structure of the adversary and the designer pmfs more precisely.

Theorem III.5. Consider a mixed NE \((r^*_k, q^*_k)\). Then, there exists a link \(\ell^*\) such that \(r^*_k(\ell^*) = 0\) for all \(\ell^* < \ell^* \leq k\), and \(r^*_k(\ell^* > 0, q^*_k(\ell^*) > 0\), and \(q^*_k\) is monotonically decreasing and increasing respectively, and \(q^*_k(\ell^*) = 0\) for \(\ell^* > \ell^* + 1\) (see Fig. 2).

Proof. First we show that there exists a link \(\ell\) such that \(r^*_k(\ell), q^*_k(\ell) > 0\). By Prop. III.4(2), there are only three possibilities for \(\ell \in \mathbb{N}_k\): (i) \(r^*_k(\ell) = 0\) and \(q^*_k(\ell) = 0\), (ii) \(r^*_k(\ell) = 0\) and \(q^*_k(\ell) > 0\), and (ii) \(r^*_k(\ell) > 0\) and \(q^*_k(\ell) > 0\). Therefore, it is clear that the set of links \{\(\ell \mid r^*_k(\ell), q^*_k(\ell) > 0\)\} is non-empty.

Let \(\ell^* = \max\{\ell \mid r^*_k(\ell), q^*_k(\ell) > 0\}\). From Prop. III.4(3), \(r^*_k(\ell^*) > 0\) for all \(\ell^* \leq \ell^*\). Therefore by Lemma III.2, we conclude \(q^*_k\) is monotonically increasing on \([1, \ell^*]\). Also, \(q^*_k\) has full support on \([1, \ell^*]\), because for some \(\ell^* < \ell^*\), \(q^*_k(\ell'') = 0\) then that would violate Prop. III.4(2). Therefore, Lemma III.3 implies that the designer pmf \(r^*_k\) will be monotonically decreasing on \([1, \ell^*]\). Since we cannot have the scenario where \(r^*_k(\ell) > 0\) and \(q^*_k(\ell) = 0\), therefore by definition of \(\ell^*, r^*_k(\ell^* + 1) = 0\). From Prop. III.4(4-5), we get \(r^*_k(\ell') = 0\) for \(\ell' > \ell^*\).

We have established the structure of the designer pmf \(r^*_k\) and the adversary pmf \(q^*_k\) on \([1, \ell^*]\). Now, for \(\ell' > \ell^*\), none of the links are being defended. So, using simple arguments it is easy to show that it is not optimal for the adversary to have any positive mass on any link \(\ell' > \ell^* + 1\).

B. Evaluating Mixed Strategies

Here, we focus on few instances of state \(k\), and characterize the mixed strategy probabilities as a function of network property costs, operational costs and attack success probabilities. While the cases we present are rather small for ease of exposition, they provide intuition for more general cases.

State 0: In State 0, we are at the base topology, and both designer and adversary each have only one strategy; the designer tries to grow the topology to \(G_1\) by adding \(l_1\), and the adversary tries to attack the “anticipated” (in this case with certainty) \(l_1\). The state transitions to 1 with probability \(1 - p\), while it stays at 0 with probability \(p\).

State 1: In State 1, both the designer and adversary now have two possible strategies; to act on the existing \(l_1\), or anticipated \(l_2\). First, we note that \(\alpha < \beta\) is necessary for strategy 2 not to be dominated for the adversary, and \(\beta - \alpha < p(g_0 - g_1)\) for strategy 1 also not being dominated for that case for the adversary. The designer selects \(r^*_k\) as the equalizer strategy such that the expected payoff of the adversary is independent of the link to attack, resulting in \((r^*_1(1), r^*_2(2)) = (1 - \frac{\beta - \alpha}{(1-p)(g_1-g_2)+p(g_0-g_1)}, 1 - \frac{\beta - \alpha}{(1-p)(g_1-g_2)+p(g_0-g_1)})\). We also note that \(\beta - \alpha\) directly impacts the possibility of growing the network from state 1. Now, the adversary selects \(q_1\) so that the expected payoff of the designer is independent of the designer’s chosen link as \((q^*_1(1), q^*_1(2)) = (1 - \frac{\beta - \alpha}{(1-p)(g_2-g_1)+p(g_0-g_1)}, 1 - \frac{\beta - \alpha}{(1-p)(g_2-g_1)+p(g_0-g_1)})\). Note that the adversary allocates a nonzero probability of attacking the anticipated link as well.
Finally, the self transition $\gamma_{k,k}$ occurs in all of the other cases, which can also be expressed as

$$\gamma_{k,k} = \sum_{j=1}^{k} [r^*_q(j)q^*_k(j) + (1-p)(1-r^*_q(j)q^*_k(j))] + r^*_q(k+1)q^*_k(k+1)p.$$ 

The first term in the summation corresponds to cases when the designer protects the attacked links, and the second term corresponds to failed attacks despite the link was not protected. Finally, the last term outside the summation corresponds to the case when the designer tries to grow the network by adding links. The probabilities can be expressed as such for any different $k = \{0, 1, 2, ..., K-1, K\}$ to form the state transition probability matrix.

### D. Stationary Probabilities

Given the state transition matrix $P$ below, we can obtain the stationary probabilities $\pi$ from the balance equation: $\pi P = \pi$.

$$P = \begin{pmatrix}
\gamma_{0,0} & \gamma_{0,1} & 0 & \ldots & 0 \\
\gamma_{1,0} & \gamma_{1,1} & \gamma_{1,2} & \ldots & 0 \\
\gamma_{2,0} & \gamma_{2,1} & \gamma_{2,2} & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\gamma_{K-1,0} & \gamma_{K-1,1} & \gamma_{K-1,2} & \cdots & \gamma_{K-1,K} \\
\gamma_{K,0} & \gamma_{K,1} & \gamma_{K,2} & \cdots & \gamma_{K,K}
\end{pmatrix}. \quad (5)
$$

Note that $P$ almost has a lower triangular form, which can be exploited to obtain closed-form expressions for the stationary probabilities, along with the constraint $\sum_{j=0}^{K} \pi_j = 1$.

In the next section, we characterize the mixed strategy Nash Equilibrium for several exemplar topology control scenarios and then describe the steady state probabilities using the methods described in this section. We also validate the key monotonicity results proved in this section.

### IV. Case Studies

In this section, we present several case studies to illustrate the theoretical methodologies and results presented earlier in the paper. Each of these case studies considers different network topologies and network property costs, and focuses on demonstrating the effect of varying parameters.

#### A. Effect of Attack Success Probability

First, to solely demonstrate the effect of attack success probability, we assume that the operational costs $\delta, \gamma, \beta, \alpha$ are all equal to 0. As a basic model, we consider a set of four allowed topologies. The base topology $G_0$ is a set of three cliques $K_{n/3}$ that are disconnected from each other – this models three organizations with no links between them. The richer topologies are denoted by $G_i = G_{i-1} \cup l_i$ for $i \in \{1, 2, 3\}$. We consider an exemplar graph property, specifically, the harmonic mean of path lengths, which is a measure of how short the paths are on average, while not being unbounded for disconnected networks. It can be easily shown that $g_0(n) = \frac{9n(n-1)}{2(n-3)}$, $g_1(n) = \frac{27n(n-1)}{11n^2 - 21n + 18}$, $g_2(n) = \frac{135n(n-1)}{71n^2 - 66n + 189}$, and $g_3(n) = \frac{9n(n-1)}{5n^2 - 3n + 18}$. The $g_i$’s converge quickly, for reasonable values of $n$, to $g_0 = 3, g_1 = 2.45, g_2 = 1.9, g_3 = 1.8$, and are monotonically decreasing in $k$. We now use the methods proposed in Section III to compute the optimal game theoretic attack/defense/growth strategies for each state in the game.
on the first two links and ignore the third link. Such behavior is consistent with the structure of the game. Finally, for \( p = 1 \), all the probability mass is at \( G_0 \).

### B. Effects of Varying Operational Costs

Here, we consider the network property of eccentricity of a given node \( u \), which is the maximum length of shortest paths from \( u \) to all other nodes in the network. In [12] it has been observed that the eccentricity \( e(k) \) of a network augmented with \( k \) links following a greedy algorithm obeys an approximate scaling law such as \( e(k) \approx \min(u, c + \frac{k}{2}) \). We consider this network property cost with \( u = 32, c = 14, y = 9 \) from [12]. In order to gain insights from operational costs, we fix the costs for defending and attacking existing links as equal to \( \delta = \beta = 1 \), and vary the costs involved with the additional link. Next, we assume that the cost to add a new link is larger than that to protect an existing link, hence we set \( \gamma = 1.25 \). Finally, we vary the cost for attacking an anticipated link \( \alpha \) in Fig. 4, where we depict the maximum attainable network state depending on \( \alpha \).

In addition to confirming the effect of varying attack success probability on maximum network growth, Fig. 4 reveals an interesting phenomenon: When the adversary is capable of performing with lower operational costs \( \alpha \) (hence seemingly has an advantage compared with the case with higher \( \alpha \)), the network can surprisingly evolve to larger sizes, eventually. While Fig. 4 only reveals the largest network state to which the network is able to evolve, we note that the actual expected value of network property costs for the designer may also decrease with smaller \( \alpha \). For instance, when \( p = 0.1 \), with \( \alpha = 1 \) the steady state probabilities are \( \pi = (0.0181, 0.0584, 0.1522, 0.7713) \) resulting in average network property cost of 17.8501. On the other hand, with \( \alpha = 0.5 \), the steady state probabilities are \( \pi = (0.0034, 0.01, 0.0248, 0.0379, 0.0783, 0.8063, 0.0393) \) resulting in average network property cost of 16.063. While this observation seems rather counter-intuitive, we attribute it to the following reason: When anticipated attack cost \( \alpha \) is not lower than the cost to attack an existing link \( \beta \), the “attack anticipated link strategy” is dominated and the adversary...
focuses on existing links instead. As a result, especially when network property costs tend to experience diminishing returns and saturation, the designer tends to spend all of its budget to protect the existing links to avoid backtracking, and does not attempt to grow the network further. On the other hand, when \( \alpha < \beta \), in line with our discussion in III.B, the adversary also tends to attack the anticipated link with nonzero probability. Due to this shift in probability mass, the existing links are in less danger and the designer also takes its chances in growing the network, resulting in the possibility of further extra growth.

V. CONCLUDING REMARKS

In this paper, we proposed a game theoretic formulation of the dynamic topology control problem under an adversarial action which succeeds probabilistically. We characterized several structural properties of the mixed strategy Nash Equilibrium. For graph properties that decrease monotonically with link addition, at equilibrium, the designer should put more effort on defending links added earlier than later, whereas the attacker’s best strategy is the opposite. We also give conditions on the attack success probability for the existence of pure equilibrium. In this work, we concentrated on analyzing the optimal attack/defense/growth strategies on a given set of allowed topologies. The design of a set of allowed topologies that favors the designer is a topic of future research. Note that we have considered a myopic setting where actions are based only on the current state. A future direction of interest is future-aware multi-stage games for topology control.

APPENDIX

Proof of Lemma III.2

1) If there exists \( 1 \leq d_1 < d_2 \leq k \) such that \( r_k^*(d_1), r_k^*(d_2) > 0 \) then we must have \( Q_k^1(q_k^*, d_1) = Q_k^1(q_k^*, d_2) \). Otherwise, the designer would do better by not playing the pure strategy which yields lower payoff. Therefore,

\[
Q_k^1(q_k^*, d_1) = Q_k^1(q_k^*, d_2)
\]

which implies \( q_k^*(d_2) = \frac{g_{d_1} - g_k}{g_{d_2} - g_k} q_k^*(d_1) \). For \( d_2 > d_1 \), we have \( \frac{g_{d_1} - g_k}{g_{d_2} - g_k} > 1 \) and the first part of the lemma follows.

2) Consider \( d_3 \notin \text{support}(r_k^*) \) and \( d_1 \in \text{support}(r_k^*) \). Since \( d_3 \notin \text{support}(r_k^*) \), we must have the expected payoff for the designer playing \( d_3 \) to be no greater than playing \( d_1 \), i.e., \( Q_k^1(q_k^*, d_3) \leq Q_k^1(q_k^*, d_1) \).

\[
Q_k^1(q_k^*, d_3) \leq Q_k^1(q_k^*, d_1)
\]

\[
\Rightarrow \sum_{a \neq d_1, d_3} U_k^1(d_3, a) q_k^*(a) + U_k^1(d_1, d_3) q_k^*(d_3)
\]

\[
+ U_k^1(d_3, d_1) q_k^*(d_1) \leq U_k^1(d_1, d_3) q_k^*(d_3)
\]

\[
+ \sum_{a \neq d_1, d_3} U_k^1(d_1, a) q_k^*(a) + U_k^1(d_1, d_1) q_k^*(d_1)
\]

\[
\Rightarrow - \sum_{a \neq d_1, d_2} [pg_{d_1} - (1 - p)g_k] q_k^*(a) - g_k q_k^*(d_1)
\]

\[
- [pg_{d_2} - (1 - p)g_k] q_k^*(d_2)
\]

\[
= - \sum_{a \neq d_1, d_2} [pg_{a} - (1 - p)g_k] q_k^*(a)
\]

\[
- [pg_{d_2} - (1 - p)g_k] q_k^*(d_1) - g_k q_k^*(d_2)
\]

\[
\Rightarrow q_k^*(d_2) [g_{d_2} - g_k] = q_k^*(d_1) [g_{d_1} - g_k]
\]

\[
\Rightarrow q_k^*(d_2) \geq q_k^*(d_1), \quad d_1 \in \text{support}(r_k^*)
\]

References


