Decentralized network protection games in adversarial environments

Siddharth Pal *, Ertugrul N. Ciftcioglu†, Prithwish Basu *, Kevin S. Chan†, and Ananthram Swami†

*Raytheon BBN Technologies, Cambridge, MA 02138
†U.S. Army Research Lab, Adelphi, MD 20783

***Abstract*—We study network protection in a decentralized setting, where nodes can protect edges (or links) incident on it against an intelligent adversary capable of attacking edges. If an edge being attacked is not being defended the edge fails with a probability $0 < p < 1$ (no-defense attack probability); if it is defended by only a single node it fails with probability q (single-defense attack probability), $0 \leq q \leq p$; and, if it is defended by both the nodes the attack is successfully thwarted. We model the interaction between protecting nodes and the adversary as a game and study their equilibrium strategies. We note that in general the probability of an important link being defended by both of the nodes is higher compared to a less important link, such that a more important link fails with a lower probability. We also observe that the behavior of the adversary is radically different for the two different ranges of values of single-defense attack probability: $0 \leq q < \frac{p}{2}$ and $\frac{p}{2} < q \leq p$. We study the special scenarios of trees and connected communities and observe that in general the nodes will defend important links (such as cut edges) with high probability, while the adversary, in contrast to a centralized protection setting will attack less important links with a higher probability only in special scenarios.**

I. Introduction

Attacks on networks have been commonplace in history. To gain competitive advantage in war, armies and navies often attacked the supply lines of the enemy forces, (e.g., cargo ships or roads through mountainous terrain), to disrupt the latter's operation in an indirect manner. In modern times, individual or coordinated attacks typically occur on critical Internet infrastructure of a virtual enemy with a goal of causing denial of service (DoS). Since the defending party is anticipating an attack *somewhere in its network*, it needs to allocate its finite resources such as sentries or anti-virus software or load-balancing firewalls to protect its network. An adversary also knows that the defender will perform intelligent resource allocation, and therefore has to make a non-obvious decision about where to attack. This is distinctly different from protecting a network from an attack on a *random* asset. Several works have modeled this tension as a non-cooperative topology control game and have characterized the properties of its Nash equilibria [4], [3], [9], [10].

The typical model is a two-party game where the attacker and the defender are the two parties, and the defender has centralized control over how to allocate its resources to neutralize the attack. However, this does not capture the realistic scenarios, in which the defensive party is composed of multiple individuals (or agents) with selfish interests that are aligned with some global features of the network. For example, roughly speaking, the global Internet results from Internet Service Providers (ISP) connecting to other ISPs via *peering points*. The selfish incentive of each ISP is to protect the flows of its paid customers but this incentive can be met only if the global Internet survives, assuming that generally speaking, flows originating in each ISP are likely to traverse all ISPs. Therefore, in such a scenario, the desire that the Internet survives is shared by all ISPs, but they are willing to take only those actions that maximize their specific benefits which are computable on the post-attack Internet structure. The relative topological locations of each ISP within the global structure are different and can result in heterogeneous incentives, which in turn can result in a non-trivial game.

In this paper, we investigate a setting where individual nodes make decisions regarding which links to protect in a decentralized fashion against an external adversary who is capable of attacking any single link in the network. The aforementioned 2-player game now generalizes to an $n + 1$ player (or agent) game on a graph of n nodes. Typically a node can protect only the links incident upon it, but arguably it can also decide to pay for the protection of a link incident at a node located far away. The adversary is the $n + 1$-th player who is not affiliated with any node in the graph and can instead attack any link. Each node strives to selfishly optimize a certain network property of choice (e.g., minimize eccentricity, the maximum of the shortest path lengths to other nodes in the post-attack graph), whereas the adversary seeks to undermine it.

We consider several probabilistic models of defense in this paper and derive several analytical properties of Nash equilibria as a function of these probabilistic models. We also investigate interesting special cases and show that the decision

Emails: {siddharth.pal, prithwish.basu}@raytheon.com, ertugrulnc@ieee.org, {kevin.s.chan, ananthram.swami}.civ@mail.mil.

Research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Numbers W911NF-09-2-0053 and W911NF-16-2-0014. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on. This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

ISBN 978-3-901882-94-4 © 2017 IFIP

of deploying a mixed strategy (probabilistically distribute the protection over several links) depends on the relative location of the link in the graph and the selfish incentive of choice. For example, particularly vulnerable links such as *cut-edges* may get full protection for selfish incentives that depend on the global graph.

A. Related work

To the best of our knowledge we are the first to consider attack-defense games which consider selfish incentives among the "good guys" in the presence of a "bad guy". Aspnes et al. [2] and generalizations thereof [11] considered a somewhat similar *protection game* with n players trying to decide whether or not to pay for installing anti-virus software with a goal of protecting the network from a contagious virus. In their setting, however, while the n agents are strategically playing each other, the adversary (i.e. virus injector) is random and not strategic. Making the adversary strategic results in significant challenges in the game, which is the subject of this paper.

In Ciftcioglu et al. [4], [3], we studied a two-party game between a centralized defender and an adversary attacking a network, with the restriction that the topology must be within a set of policy compliant topologies. We observed that while the defender will defend the most important links with higher probability, the adversary will attack the less important links with higher probability. In this work, we note that these findings do not carry over completely to a decentralized scenario. Gueye et al. [10] consider network topology design in an adversarial environment, where a network manager chooses a spanning tree of the network and the adversary targets a specific set of links, with the network property of interest being connectivity. Laszka and Gueye [12] studied the vulnerability of network topologies and proposed security metrics for assessing the solutions as a two player game, with emphasis on network connectivity.

A significant body of work exists in the theoretical computer science literature focusing on static network topology redesign. Specifically, Watanabe and Nakamura [15] studied augmentation of static graphs for improved fault tolerance by improving connectivity; Demaine and Zadimoghaddam [5] studied the improvement of information flow properties by minimizing the diameter using shortcut edges; and, Myerson and Tagiku [14] studied the minimization of average shortest path lengths through network augmentation. Furthermore, network formation games [7] have been proposed to characterize how individual nodes should form connections to create a network in order to benefit from some property of the resultant network. Dijk et al. [6] and Laszka et al. [13] used a game setting to model protection against cyber-threats to prevent stealthy takeover of critical resource. In contrast, our work focuses on the tension that arises from the simultaneous actions of network protection and attack, in order to protect any particular network property of interest.

B. Contributions

We study a decentralized version of a network protection game in the presence of an adversary. We study the single shot game between the protecting nodes and the adversary and characterize the equilibrium strategies. Our primary contributions are summarized below:

1) We are the first to study a decentralized version of a network protection game involving a strategic adversary attacking links, with the individual nodes improving their own local network properties.

2) We analyze the equilibrium strategies of the protecting nodes and adversary, and observe that the nodes will protect important links with a higher probability; and in contrast to the centralized protection scenario, the adversary could attack more important links with higher probability because of the inherent decentralized nature of the setting.

3) We study canonical special cases: rooted trees and connected communities, and observe that while more important links are protected with higher probability, they could also be attacked with a higher probability under certain regimes. This is in contrast to the results obtained in the centralized scenario [4], [3].

The rest of the paper is organized as follows: In Section II, we describe the single shot game between the nodes protecting the network and the adversary. In the subsequent section, we characterize the resultant equilibria of the game, and establish properties of the strategies of the nodes and the adversaries. In Section IV we specifically consider two kinds of networks – trees and connected communities, and study the equilibrium strategies, followed by numerical results in Section V.

II. Decentralized Topology Control in Adversarial Environments

We assume that the attacker can attack only a single link in the current graph. We also assume that each node can only defend a single link which is incident on it. Generalizations are discussed later in the paper.

A. System Model

Some notation: For any graph G, the edge set of the graph is denoted as $E(G)$, and vertex set by $V(G)$.

1) State: The state space $\mathcal{S}$ is the set of all graphs with n nodes

$$\mathcal{S} = \{G \mid |V(G)| = n\},$$

while the system state is the current graph. Also, the set of neighbors of node i in $V(G)$ is denoted by $N_i(G)$. For ease of notation, we will replace $V(G)$ by $V := \{1, 2, \dots, n\}$.

2) Actions: The action space of the attacker and defender depend on the graph/state which is denoted as G in $\mathcal{S}$.

Decision making nodes: The action space for node i in graph G will be denoted as $\mathcal{A}_i(G) := \{(i, \ell), \ell \in N_i(G)\}$. Any node i in V can choose to protect/harden a link $e \in \mathcal{A}_i(G)$ among its connections in graph G. The joint action space of the individual nodes is represented as $\mathcal{A}_d(G) := \prod_{i \in V} \mathcal{A}_i(G)$, and the joint action space of all nodes except node i is represented as $\mathcal{A}_{-i}(G) := \prod_{j \in V, j \neq i} \mathcal{A}_j(G)$.

Attacker: The action space for the adversary in graph G will be denoted as $\mathcal{A}_a(G) := E(G)$. Therefore, the adversary is allowed to attack any existing link in the graph G.

3) State Transitions: We assume that the defending nodes and the adversary act simultaneously. For any edge $e = (k, \ell) \in E(G)$, if it is not defended by nodes k or ℓ, then it fails with probability p when attacked by the adversary. However, if only one of the two nodes defend the link, then the link is assumed to fail with probability q with $0 \leq q \leq p$. Furthermore, if both the nodes defend the link, we assume the link will stay protected even under attack. We define the state transition function as $T : \mathcal{S} \times \mathcal{A}_d \times \mathcal{A}_a \to \Delta(\mathcal{S})$

$$T(G, \mathbf{d}, e) = \begin{cases} G \setminus e, \text{ w.p. } p, & \text{if } e \neq d_k \text{ and } e \neq d_\ell \\ G \setminus e, \text{ w.p. } q, & \text{if } e = d_k \text{ and } e \neq d_\ell, \\ & \text{or } e \neq d_k \text{ and } e = d_\ell \\ G, \quad \text{w.p. } (1-p), & \text{if } e \neq d_k \text{ and } e \neq d_\ell \\ \quad \text{w.p. } (1-q), & \text{if } e = d_k \text{ and } e \neq d_\ell, \\ & \text{or } e \neq d_k \text{ and } e = d_\ell \\ \quad \text{w.p. } 1, & \text{if } e = d_k \text{ and } e = d_\ell \end{cases}$$

with d_k being the node being defended by node k, $\mathbf{d} = (d_i,\ i = 1, \ldots, n) \in \mathcal{A}_d$, $e = (k, \ell) \in \mathcal{A}_a$, and $\Delta(\mathcal{S})$ the probability simplex over the state space $\mathcal{S}$.

Here we consider two special cases: In the first case with $q = 0$, it is sufficient for one node to decide to protect a link, for it to be actually protected in the scenario of an attack from the adversary. In the case with $q = p$, both the nodes associated with an edge have to agree to protect a link, for it to be actually protected in the face of an attack.

B. Utilities

We define a global network property $\nu : \mathcal{G} \to \mathbb{R}$, for instance connectivity, average shortest path distance, diameter of a network. Furthermore, we also define local network property for each node i, e.g., eccentricity, centrality, given by $\nu_i : \mathcal{G} \to \mathbb{R}$. Next, we define payoff functions as $U_i : \mathcal{G} \times \mathcal{A}_d \times \mathcal{A}_a \to \mathbb{R}$ for each node i in V, and $U_a : \mathcal{G} \times \mathcal{A}_d \times \mathcal{A}_a \to \mathbb{R}$ for the adversary. We only require that the global and local network properties do not improve as edges are removed from a particular graph. While the individual nodes receives payoff for favourable local network property, the adversary tries to harm the global network property.

For graph G in $\mathcal{S}$, actions $\mathbf{d} \in \mathcal{A}_d$, and $a \in \mathcal{A}_a$, the payoff for a particular node i is

$$U_i(G, \mathbf{d}, a) = \nu_i(T(G, \mathbf{d}, a))$$

and for the adversary is set to be

$$U_a(G, \mathbf{d}, a) = -\nu(T(G, \mathbf{d}, a)).$$

Therefore the resultant Markov game is a 6-tuple – $\big(\mathcal{S}, \{\mathcal{A}_a(G),\ G \in \mathcal{S}\}, \{\mathcal{A}_d(G),\ G \in \mathcal{S}\}, \{U_i,\ i \in V\}, U_a, T\big)$. Observe that this is not a zero sum game except for very special choices of global and node-centric network properties. Since the game has finite number of players, and each player chooses its action from a finite action set, mixed Nash equilibrium is know to exist [8].

C. Mixed strategies and Nash equilibria

Mixed strategy of a defending node i is given as $\mathbf{r}_i = (\mathbf{r}_{G,i},\ G \in \mathcal{S})$, where $\mathbf{r}_{G,i} \in \Delta(\mathcal{A}_i(G))$. For simplicity, we denote the joint mixed strategies of the defending nodes as $\mathbf{r} = (\mathbf{r}_i,\ i = 1, \ldots, n)$, and that of all the nodes except node i as $\mathbf{r}_{-i}$. Mixed strategy of the adversary is given as $\mathbf{q} = (\mathbf{q}_G,\ G \in \mathcal{S})$, where $\mathbf{q}_G \in \Delta(\mathcal{A}_a(G))$.

A mixed strategy pair $(\mathbf{r}^*, \mathbf{q}^*)$ is a Nash equilibrium if neither player can improve their expected payoffs by deviating from their strategies, i.e., for all states G in S and nodes i

$$\mathbb{E}\left[U_i(G) | \mathbf{r}^*, \mathbf{q}^*\right] \geq \mathbb{E}\left[U_i(G) | \mathbf{r}, \mathbf{q}^*\right],$$

for all designer strategies $\mathbf{r}$, and

$$\mathbb{E}\left[U_a(G) | \mathbf{r}^*, \mathbf{q}^*\right] \geq \mathbb{E}\left[U_a(G) | \mathbf{r}^*, \mathbf{q}\right],$$

for all adversarial strategies $\mathbf{q}$.

Hence, $(\mathbf{r}_G^*, \mathbf{q}_G^*)$ is the mixed NE strategy pair at state G.

III. Properties of Nash equilibria

In this section we study some properties of mixed Nash equilibria of the resultant distributed game between the defending nodes and the adversary.

The expected payoff for the defending node i at the mixed NE $(\mathbf{r}_G^*, \mathbf{q}_G^*)$ is

$$\sum_{\mathbf{d} \in \mathcal{A}_d(G)} r_G^*(\mathbf{d}) \left(\sum_{a \in \mathcal{A}_a(G)} U_i(G, \mathbf{d}, a) q_G^*(a) \right).$$

and for the adversary is

$$\sum_{a \in \mathcal{A}_a(G)} q_G^*(a) \left(\sum_{\mathbf{d} \in \mathcal{A}_d(G)} U_a(G, \mathbf{d}, a) r_G^*(\mathbf{d}) \right).$$

We define

$$\begin{aligned} & Q_i^G(\mathbf{q}_G, \mathbf{r}_{G,-i}, m) \\ & = \sum_{a \in \mathcal{A}_a(G)} \sum_{\mathbf{d}_{-i} \in \mathcal{A}_{-i}(G)} U_i\left(G, (\mathbf{d}_{-i}, m), a\right) \mathbf{r}_{G,-i}(\mathbf{d}_{-i}) q_G(a) \\ & = \sum_{a \in \mathcal{A}_a(G)} \sum_{\mathbf{d}_{-i} \in \mathcal{A}_{-i}(G)} \sum_{G' \in S} T\left(G' | G, (\mathbf{d}_{-i}, m), a\right) \\ & \qquad \times \nu_i(G') \mathbf{r}_{G,-i}(\mathbf{d}_{-i}) q_G(a),\ m \in \mathcal{A}_i(G). \end{aligned}$$

Note that $Q_i^G(\mathbf{q}_G, \mathbf{r}_{G,-i}, m)$ is the expected payoff for node i playing action m when the other nodes are playing strategies given by $\mathbf{r}_G$ and the adversary is playing the mixed strategy $\mathbf{q}_G$; and, $T(G' | G, \mathbf{d}, a)$ is the probability of transitioning to state G' from state G under the actions $\mathbf{d}$ and a[2]. Next, we state a lemma that describes certain properties of the adversary pmf $\mathbf{q}_G^*$.

For a given graph G in $\mathcal{S}$, we can order the links as follows: For two links ℓ_1 and ℓ_2 in $E(G)$, link ℓ_1 is more important than ℓ_2 with respect to network property ν, i.e., $\ell_1 \succ_{G,\nu} \ell_2$ if $\nu(G \setminus \ell_1) \leq \nu(G \setminus \ell_2)$. For node i, and edge ℓ connected to

[2] We note that the expected utility of node i might also depend on the set of actions apart from its one-hop neighborhood.

i, we define $L_i(\ell) = \nu_i(G) - \nu_i(G \setminus \ell)$, which is the loss in network property when the edge is removed.

Lemma 3.1: Consider the mixed Nash equilibrium of the game $(\mathbf{r}^*_G, \mathbf{q}^*_G)$. For node i and for any two links $\ell_1 = (i,j), \ell_2 = (i,k)$ in $E(G)$:

(a) If $r^*_{G,i}(\ell_1), r^*_{G,i}(\ell_2) > 0$, we have

$$\begin{aligned} &L_i(\ell_1)q^*_G(\ell_1)\left[(p-q)-(p-2q)r^*_{G,j}(\ell_1)\right] \\ &\quad = L_i(\ell_2)q^*_G(\ell_2)\left[(p-q)-(p-2q)r^*_{G,k}(\ell_2)\right] \end{aligned} \tag{1}$$

(b) If $r^*_{G,i}(\ell_1) \notin \text{support}(\mathbf{r}^*_{G,i})$ and $r^*_{G,i}(\ell_2) > 0$, we have

$$\begin{aligned} &L_i(\ell_1)q^*_G(\ell_1)\left[(p-q)-(p-2q)r^*_{G,j}(\ell_1)\right] \\ &\quad \leq L_i(\ell_2)q^*_G(\ell_2)\left[(p-q)-(p-2q)r^*_{G,k}(\ell_2)\right] \end{aligned} \tag{2}$$

Furthermore, for both the above cases (i) for $q > \frac{p}{2}$: if $\ell_1 \succ_{G,\nu_i} \ell_2$ and $r^*_{G,j}(\ell_1) > r^*_{G,k}(\ell_2)$, then we must have $q^*_G(\ell_1) < q^*_G(\ell_2)$; and (ii) for $q < \frac{p}{2}$ if $\ell_1 \succ_{G,\nu_i} \ell_2$ and $r^*_{G,j}(\ell_1) < r^*_{G,k}(\ell_2)$, then we must have $q^*_G(\ell_1) < q^*_G(\ell_2)$.

Proof. From the principle of indifference, the expected payoffs for node i for defending links ℓ_1 and ℓ_2 should be equal otherwise the node would defend that link that yields an higher expected payoff. Therefore,

$$Q^G_i(\mathbf{q}^*_G, \mathbf{r}^*_{G,-i}, \ell_1) = Q^G_i(\mathbf{q}^*_G, \mathbf{r}^*_{G,-i}, \ell_2), \tag{3}$$

while the second part of the proof follows by noting that the expected payoff for defending link ℓ_2 should be no less than defending link ℓ_1. Details of the proof are given in Appendix VII. ■

Lemma 3.1 gives the relationship between the attack probabilities on two links $\ell_1 = (i,j)$ and $\ell_2 = (i,k)$ and the probabilities that they are being defended by the nodes j and k, respectively. As a consequence of the lemma, we observe that for $q > \frac{p}{2}$, if $\ell_1 \succ_{G,\nu_i} \ell_2$ and $r^*_{G,j}(\ell_1) > r^*_{G,k}(\ell_2)$ then the adversary attacks ℓ_2 with a higher probability than ℓ_1. The explanation behind this result is that if link ℓ_1 is defended with a higher probability by node j as compared to link ℓ_2 by node k, then the adversary will not gain much by attacking link ℓ_1 because that link will also be defended with a greater probability by node i given its importance to that particular node. However, a similar conclusion cannot be drawn if $r^*_{G,j}(\ell_1) < r^*_{G,k}(\ell_2)$, i.e., the relationship between the attack probabilities of links ℓ_1 and ℓ_2 cannot be determined qualitatively.

On the other hand, for $q < \frac{p}{2}$, if $r^*_{G,j}(\ell_1) < r^*_{G,k}(\ell_2)$ then the adversary attacks link ℓ_1 with a lower probability. This is rather counter-intuitive because given what we just discussed, the more a link is defended, lesser is the probability that it will be attacked by the adversary. However, since $q < \frac{p}{2}$, it is more likely that a link stays protected even when only one node is defending it. Since, $r^*_{G,j}(\ell_1) < r^*_{G,k}(\ell_2)$, and knowing fully well that link ℓ_1 is more important than ℓ_2 for node i, it presumably takes almost complete responsibility for the link, leading to a lesser return on attack for the adversary. On the other hand, when $r^*_{G,j}(\ell_1) > r^*_{G,k}(\ell_2)$, we cannot find relationship between the attack probabilities of links ℓ_1 and ℓ_2. This is in contrast to the centralized protection setting, where less important links are shown to be attacked with higher probability. As is evident, the lack of synchronization or decentralization among the node defenders allows the adversary to sometimes attack more important links with higher probability.

Also, observe that relationship between the attacker's probabilities of attacking two links can be established when either both the links are being defended by the relevant node, or the more important link for that node is not being defended. The latter situation leads to a relationship that the adversary should attack the more important with a lesser probability, because if that were not the case, the node in question would have defended the more important link. The situation when the more important link is being defended and a lesser one is not, does not lead to any relationship between the attack probabilities of the links.

Corollary 3.2: We consider the following special cases of Lemma 3.1: Consider the mixed Nash equilibrium of the game $(\mathbf{r}^*_G, \mathbf{q}^*_G)$. For node i and for any two links $\ell_1 = (i,j), \ell_2 = (i,k)$ in $E(G)$, we have the following cases

Case 1: For $q = 0$: If $r^*_{G,i}(\ell_1), r^*_{G,i}(\ell_2) > 0$,

$$\begin{aligned} &L_i(\ell_1)q^*_G(\ell_1)(1 - r^*_{G,j}(\ell_1)) \\ &\quad = L_i(\ell_2)q^*_G(\ell_2)(1 - r^*_{G,k}(\ell_2)), \end{aligned} \tag{4}$$

and if $r^*_{G,i}(\ell_1) \notin \text{support}(\mathbf{r}^*_{G,i})$ and $r^*_{G,i}(\ell_2) > 0$,

$$\begin{aligned} &L_i(\ell_1)q^*_G(\ell_1)(1 - r^*_{G,j}(\ell_1)) \\ &\quad \leq L_i(\ell_2)q^*_G(\ell_2)(1 - r^*_{G,k}(\ell_2)), \end{aligned} \tag{5}$$

Case 2: For $q = p$: If $r^*_{G,i}(\ell_1), r^*_{G,i}(\ell_2) > 0$,

$$L_i(\ell_1)q^*_G(\ell_1)r^*_{G,j}(\ell_1) = L_i(\ell_2)q^*_G(\ell_2)r^*_{G,k}(\ell_2), \tag{6}$$

and if $r^*_{G,i}(\ell_1) \notin \text{support}(\mathbf{r}^*_{G,i})$ and $r^*_{G,i}(\ell_2) > 0$,

$$L_i(\ell_1)q^*_G(\ell_1)r^*_{G,j}(\ell_1) \leq L_i(\ell_2)q^*_G(\ell_2)r^*_{G,k}(\ell_2), \tag{7}$$

Case 3: For $q = \frac{p}{2}$: If $r^*_{G,i}(\ell_1), r^*_{G,i}(\ell_2) > 0$,

$$L_i(\ell_1)q^*_G(\ell_1) = L_i(\ell_2)q^*_G(\ell_2) \tag{8}$$

and if $r^*_{G,i}(\ell_1) \notin \text{support}(\mathbf{r}^*_{G,i})$ and $r^*_{G,i}(\ell_2) > 0$,

$$L_i(\ell_1)q^*_G(\ell_1) \leq L_i(\ell_2)q^*_G(\ell_2) \tag{9}$$

Proof. The corollary follows directly from Lemma 3.1 by setting $q = 0, \frac{p}{2}, p$ in (1) and (2). ■

Corollary 3.2 considers three special cases. The case with $q = 0$, i.e., a link is protected even when one node defends the link, is a special case of $q < \frac{p}{2}$. This scenario clearly demonstrates that a more important link $\ell_1 = (i,j)$ for node i will be attacked with a lower probability compared to $\ell_2 = (i,k)$, if the other node j defends the link with a lower probability compared to k defending ℓ_1, in effect shifting most of the burden of defending the link ℓ_1 to node i. The scenario with $q = \frac{p}{2}$, i.e., both nodes are needed to protect the link, yields a straightforward relationship that if link ℓ_1 is more important than ℓ_2 for node i, and the opposite node j is also defending the link with a high probability, then the attack probability on the link will be low.

Finally, the case for $q = \frac{p}{2}$ yields a very interesting result that if a link ℓ_1 is more important than ℓ_2 for a node i, then the adversary will attack the more important link with lesser probability, irrespective of the strategies of the other concerned nodes j and k.

Going forward, we set the following notation: $L(\ell) = \nu(G) - \nu(G \setminus \ell)$, which denotes the reduction in the global network property due to the failure of link ℓ.

Lemma 3.3: Consider the mixed Nash equilibrium of the game $(\mathbf{r}_G^*, \mathbf{q}_G^*)$. For any two links $\ell_1 = (h, i), \ell_2 = (j, k)$ in $E(G)$:

(a) If $q_G^*(\ell_1), q_G^*(\ell_2) > 0$, we have

$$\begin{aligned}
&L(\ell_1)\Big[p(1 - r^*_{G,h}(\ell_1))(1 - r^*_{G,i}(\ell_1)) \\
&\quad + q\left(r^*_{G,h}(\ell_1)(1 - r^*_{G,i}(\ell_1)) + (1 - r^*_{G,h}(\ell_1))r^*_{G,i}(\ell_1)\right)\Big] \\
&= L(\ell_2)\Big[p(1 - r^*_{G,j}(\ell_2))(1 - r^*_{G,k}(\ell_2)) \\
&\quad + q\left(r^*_{G,j}(\ell_2)(1 - r^*_{G,k}(\ell_2)) + (1 - r^*_{G,j}(\ell_2))r^*_{G,k}(\ell_2)\right)\Big]
\end{aligned} \tag{10}$$

(b) If $q_G^*(\ell_1) \notin \text{support}(\mathbf{q}_G^*)$ and $q_G^*(\ell_2) > 0$, we have

$$\begin{aligned}
&L(\ell_1)\Big[p(1 - r^*_{G,h}(\ell_1))(1 - r^*_{G,i}(\ell_1)) \\
&\quad + q\left(r^*_{G,h}(\ell_1)(1 - r^*_{G,i}(\ell_1)) + (1 - r^*_{G,h}(\ell_1))r^*_{G,i}(\ell_1)\right)\Big] \\
&\leq L(\ell_2)\Big[p(1 - r^*_{G,j}(\ell_2))(1 - r^*_{G,k}(\ell_2)) \\
&\quad + q\left(r^*_{G,j}(\ell_2)(1 - r^*_{G,k}(\ell_2)) + (1 - r^*_{G,j}(\ell_2))r^*_{G,k}(\ell_2)\right)\Big]
\end{aligned} \tag{11}$$

Proof. First, we provide some notation: We define for $m \in \mathcal{A}_d(G)$,

$$\begin{aligned}
Q_a^G(\mathbf{r}_G, m) &= \sum_{\mathbf{d} \in \mathcal{A}_d(G)} U_i\left(G, \mathbf{d}, m\right) r_G(\mathbf{d}) \\
&= - \sum_{\mathbf{d} \in \mathcal{A}_d(G)} \sum_{G' \in S} T\left(G' | G, \mathbf{d}, m), a\right) \nu(G') r_G(\mathbf{d}),
\end{aligned}$$

which is the expected payoff for the adversary for attacking link m with the nodes following mixed strategies $\mathbf{r}_G$. As in Lemma 3.1, the first part of the proof follows by equating the expected payoff for the adversary for attacking links ℓ_1 and ℓ_2, i.e.,

$$Q_a^G(\mathbf{r}_G^*, \ell_1) = Q_a^G(\mathbf{r}_G^*, \ell_2),$$

while the second part of the proof follows by noting that the expected payoff for attacking link ℓ_1 should be no less than that for attacking link ℓ_2. The rest of the proof follows in a fashion similar to that of Lemma 3.1, and is therefore omitted. ■

Lemma 3.3 gives a relationship between the defence probabilities of links in the network. For instance, given two links ℓ_1 and ℓ_2, if ℓ_1 is more important with respect to the global network property ν, then the link will be protected with a greater probability. This follows by noting that

$$\begin{aligned}
&\Big[p(1 - r^*_{G,h}(\ell_1))(1 - r^*_{G,i}(\ell_1)) \\
&\quad + q\left(r^*_{G,h}(\ell_1)(1 - r^*_{G,i}(\ell_1)) + (1 - r^*_{G,h}(\ell_1))r^*_{G,i}(\ell_1)\right)\Big]
\end{aligned}$$

is the probability of failure of link ℓ_1 which has to be less compared to link ℓ_2, if link ℓ_1 is more important.

Lemma 3.4: For a link $\ell = (h, i)$ such that $q_G^*(\ell) = 0$, we must have $r^*_{G,h}(\ell) = r^*_{G,i}(\ell) = 0$.

Proof. This follows from noting that if a link is not being attacked, then the equilibrium strategy should be to leave the link unprotected. Because if that is not the case, a node (here h or i) can always improve by shifting some probability mass from defending the link ℓ to defending some other incident link that is being attacked. ■

Corollary 3.5: We consider the following special cases of Lemma 3.3: Consider the mixed Nash equilibrium of the game $(\mathbf{r}_G^*, \mathbf{q}_G^*)$. For any two links $\ell_1 = (h, i), \ell_2 = (j, k)$ in $E(G)$, we have the following cases when $q_G^*(\ell_1), q_G^*(\ell_2) > 0$ **Case 1:** For $q = 0$,

$$\begin{aligned}
&L(\ell_1)(1 - r^*_{G,h}(\ell_1))((1 - r^*_{G,i}(\ell_1)) \\
&\quad = L(\ell_2)((1 - r^*_{G,j}(\ell_2))((1 - r^*_{G,k}(\ell_2)),
\end{aligned} \tag{12}$$

Case 2: For $q = p$,

$$\begin{aligned}
&L(\ell_1)\left(1 - r^*_{G,h}(\ell_1) r^*_{G,i}(\ell_1)\right) \\
&\quad = L(\ell_2)\left(1 - r^*_{G,j}(\ell_2) r^*_{G,k}(\ell_2)\right)
\end{aligned} \tag{13}$$

Case 3: For $q = \frac{p}{2}$,

$$\begin{aligned}
&L(\ell_1)\left(2 - r^*_{G,h}(\ell_1) - r^*_{G,i}(\ell_1)\right) \\
&\quad = L(\ell_2)\left(2 - r^*_{G,j}(\ell_2) - r^*_{G,k}(\ell_2)\right)
\end{aligned} \tag{14}$$

Proof. The corollary follows directly from Lemma 3.3 by setting $q = 0, \frac{p}{2}, p$ in (10) and (11). ■

As we did in Corollary 3.2, we look at various special scenarios in Corollary 3.5. For $q = 0$, we observe that for a more important link (with respect to global property ν), the probability that it is not being defended by either of the nodes must be lower. This is because for $q = 0$, you can have a failure only when none of the involved nodes are defending the link. Furthermore, for $q = p$, a more important link will be jointly defended by the relevant nodes with a greater probability. Finally, for the $q = \frac{p}{2}$ scenario, the sum probability of defending a more important link will be greater for the concerned nodes.

IV. Case Studies

We consider two canonical special cases: rooted trees and connected communities, and investigate the defense probabilities of the nodes and the attack probabilities on the different kinds of edges.

A. Trees

Rooted trees as shown in Figure 1 have a single link going from a node to its parent with multiple possible offsprings. Suppose the node metric of interest is its reachability, i.e., the number of nodes reachable from a particular node, or eccentricity, and global network property of interest is the size of the largest connected component or the average shortest path length. A fair assumption in such scenarios is that, for any node, link to its parent node is more important for maintaining its local network property of reachability or eccentricity. Also, for the entire graph, edges closer to the root are more important because their removal would dislodge a large portion of the tree.

For $q = 0$, the equilibrium strategies for the nodes is to defend the link to its parent. This is foolproof and the adversary cannot attack the network in this scenario. However, for $q > 0$, there does not exist any foolproof strategy and the edges closer to the root gain priority and will be defended by the participating nodes with a greater probability. This follows directly from Lemma 3.3, which indicates that more important links will be defended by the involved nodes such that the failure probability will be less when attacked.

On the other hand, the adversary can be shown to attack more important links with less probability in certain scenarios. For instance, consider a tree where link $\ell_1 = (i, j)$ and $\ell_2 = (i, k)$, with node i being the parent of k and j being the parent of i. Under the local property of reachability or eccentricity, it is likely that $\ell_1 \succ_{G,\nu_i} \ell_2$, i.e., the link to its parent is more important for node i, and moreover if every node protects the link to its parent with greater mass, i.e., $r^*_{G,j}(\ell_1) < r^*_{G,k}(\ell_2)$, then from Lemma 3.1 we would have $q^*_G(\ell_1) < q^*_G(\ell_2)$ when $q \leq \frac{p}{2}$. When $q > \frac{p}{2}$, the attacker could attack more important links with higher probability unless the involved nodes defend the link with high probability, more specifically, the parent j needs to defend link ℓ_1 with higher probability compared to k defending link ℓ_2. The intuition behind this finding is that when q is small, there is not much opportunity for the adversary to attack more important links, which is not the case when $q > \frac{p}{2}$. Again this is in contrast to a centralized protection setting where links closer to the root would be attacked with a lower probability.

B. Connected dense communities

Figure 2 shows a topology with two communities connected to one another through hubs. We consider the node metric of average shortest path for a node (or reachability), and the global network property of interest could be the global eccentricity or the average path length.

From Lemma 3.3, it is clear that cut edges will be protected heavily by involved nodes because their removal would hurt the global network property the most. Also, edges connecting to hubs of local communities will be protected with a higher probability compared to other in-cluster edges. In the regime $q = \frac{p}{2}$, from Lemma 3.1 it follows that the adversary will attack the cut-edge with lower probability compared to other in-cluster edges, and attack in-cluster edges connecting to hubs with a lower probability than other in-cluster edges.

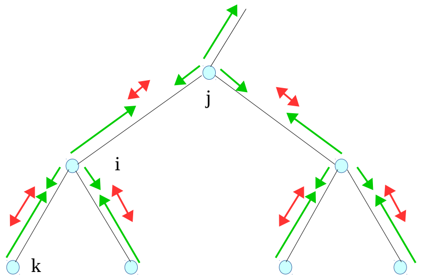

Fig. 1. Portion of a rooted tree shown with depiction of typical node defense and attack strategies when $q < \frac{p}{2}$. The defense strategies would be similar when $q > \frac{p}{2}$. (Green arrows correspond to protection of the adjacent links by the node where the arrow originates, and red arrows depict attack by the adversary; arrow lengths are proportional to the mixed strategy probabilities of the defense/attack on the link.)

A hub (say, node i) would value the cut-edge more than other edges connected to it. Similarly, another hub (node j) connected through the cut-edge $\ell_1 = (i, j)$, will protect it with high probability. Also, a peripheral node (say node k) would protect its link $\ell_2 = (k, i)$ to hub i with high probability. Hence, we cannot compare the defense probabilities $r^*_{G,j}(\ell_1)$ and $r^*_{G,k}(\ell_2)$, and therefore cannot use Lemma 3.1 to conclusively find relationship between the adversarial strategy for attacking links ℓ_1 or ℓ_2. On the other hand, consider a peripheral edge $\ell_3 = (k, m)$ or $\ell_4 = (k, n)$. Both edges are less important than edge ℓ_2 to node k, and furthermore if hub i defends link ℓ_2 with lower probability than node m defending link ℓ_3 or node n defending ℓ_4, we can use Lemma 3.1 to state that peripheral links like ℓ_3 and ℓ_4 will be attacked with more probability than links to hubs.

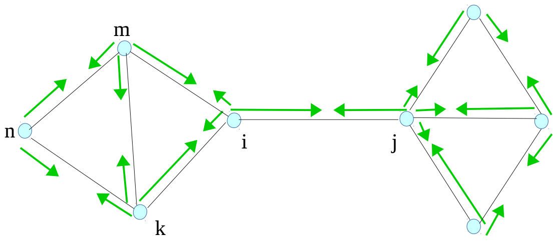

Fig. 2. Two communities connected through a cut-edge. The defense strategies of the nodes are depicted.

V. Numerical Results

In this section, we provide example numerical results validating the structural properties of the Nash equilibrium stated in Section III.

As an illustrative example, we first consider the scenario depicted in Fig. 3.

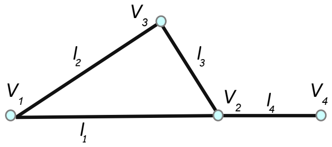

Fig. 3. A network with four nodes and four links.

TABLE I
General Payoff structure

	ℓ_1	ℓ_2	ℓ_3	ℓ_4
$L_1(.)$	0.6	0.5	0	0.5
$L_2(.)$	0.5	0	0.5	1
$L_3(.)$	0	0.5	0.6	0.5
$L_4(.)$	0.16	0	0.16	2
$\nu(G/\ell_i)$	4.3	4.5	4.3	3

TABLE II
Link Selection Probabilities, $q = p = 0.2$

	ℓ_1	ℓ_2	ℓ_3	ℓ_4
$r^*_{G,1}(\ell_i)$	0.7475	0.2525	–	–
$r^*_{G,2}(\ell_i)$	0.1809	–	0.157	0.6621
$r^*_{G,3}(\ell_i)$	–	0.2802	0.7198	–
$r^*_{G,4}(\ell_i)$	–	–	–	1
$q^*_G(\ell_i)$	0.3238	0.2787	0.3363	0.0611

TABLE III
Link Selection Probabilities, $q = \frac{p}{2} = 0.1$

	ℓ_1	ℓ_2	ℓ_3	ℓ_4
$r^*_{G,1}(\ell_i)$	0.9091	0.0909	–	–
$r^*_{G,2}(\ell_i)$	0	–	0.3636	0.6364
$r^*_{G,3}(\ell_i)$	–	0.4545	0.5455	–
$r^*_{G,4}(\ell_i)$	–	–	–	1
$q^*_G(\ell_i)$	0.2784	0.3712	0.2784	0.072

We initially consider the local network property for each node i, v_i, as the sum of the inverse of distances to each other node in the network; that is

$$\nu_i(T(G,\mathbf{d},a)) := \sum_{j\in G\setminus i} \frac{1}{d_{ij}}, \quad (15)$$

where d_{ij} is the number of hops on the shortest path between node i and node j, with $d_{ij} = \infty$ if there does not exist a path between v_i and v_j. We note that while these properties are *local* with respect to the particular node of concern, they may potentially depend on the whole topology, including links which are not directly connected to that node hence have no control over.

For the adversary, we chose a metric depending on the sum of inverses of all pair-to-pair shortest path lengths, i.e.,

$$U_a(T(G,\mathbf{d},a)) = -\nu_i(T(G,\mathbf{d},a)) := -\sum_{(k,l)\in G} \frac{1}{d_{kl}}. \quad (16)$$

We have selected these particular metrics for convenience since they are finite even when a subset of the nodes might be disconnected. These metrics are different ways of capturing local connectivity of a node embedded in a network, which might be applicable to the ISP scenario described in Section I.

Given these definitions, one can readily compute the importance of a link ℓ_i with respect to a particular node v_j, $L_j(\ell_i)$, i.e., $\nu_j(G) - \nu_j(G \setminus \ell_i)$ as shown in Table I, quantifying the significance of each link to a particular node.

On the other hand, for the adversary (Table I), $\nu(G) = 5$, $\nu(G\setminus\ell_1) = 4.\bar{3}$, $\nu(G\setminus\ell_2) = 4.5$, $\nu(G\setminus\ell_3) = 4.\bar{3}$, $\nu(G\setminus\ell_4) = 3$, implying that ℓ_4 is the link with most impact in terms of overall distance.

Solving the resulting games via the open source GAMBIT toolbox [1], we have for $p = q = 0.2$ the strategies in Table II, complying with Lemmas 3.1-3.3. Note that although links ℓ_1 and ℓ_3 are more important for the global network property with respect to link ℓ_2, they are attacked with a higher probability compared to link ℓ_2. This is *in contrast to the centralized setting* where more important links are attacked with lower probability.

When $q = \frac{p}{2} = 0.1$, we have the strategies in Table III, again complying with Lemmas 3.1- 3.3.

Finally, when $q = 0$, that is one node defending a link is sufficient to protect it, we have the probabilities in Table IV, which are again consistent with Lemmas 3.1- 3.3. Note that for this scenario there are four links and four nodes, and the resulting Nash equilibrium consists of pure strategies where the nodes and links have a one-to-one matching (as in an assignment problem) for defense, since defense by one node is sufficient. (see Fig. 4c). On the other hand, we observe that when $q > 0$, node v_2 significantly assists in the protection of ℓ_4 which is crucial in connecting v_4. We also observe the tendency of nodes to prioritize defending the links which are most important to themselves. On the other hand, contrary to intuition that the adversary would go for links which would increase its utility most (e.g. ℓ_4), we observe that it tends to go for links which do not increase its utility as much. Our intuition is that reminiscent of the centralized case [4], [3], i.e., the adversary expects that an important link is also likely to be protected better, hence it tries to attack links which might not be as well protected. Nevertheless, as we saw before, this does not always hold in the decentralized setting.

For the same network, we next consider the local network property of eccentricity for each node i, equal to $ecc_i(G) = \max_{j\in G\setminus i} d_{i,j}$. For the adversary, the network property is the sum of the eccentricities of all nodes, $\sum_{i\in G} ecc_i(G)$, equal to its utility $\nu(T(G,\mathbf{d},a))$. We consider the utility for node i as $\nu_i(T(G,\mathbf{d},a)) := -ecc_i(G)$.

We note that a significant difference between the previous

TABLE IV
Link Selection Probabilities, $p = 0.2, q = 0$

	ℓ_1	ℓ_2	ℓ_3	ℓ_4
$r^*_{G,1}(\ell_i)$	1	0	–	–
$r^*_{G,2}(\ell_i)$	0	–	1	0
$r^*_{G,3}(\ell_i)$	–	1	0	–
$r^*_{G,4}(\ell_i)$	–	–	–	1
$q^*_G(\ell_i)$	0.25	0.25	0.25	0.25

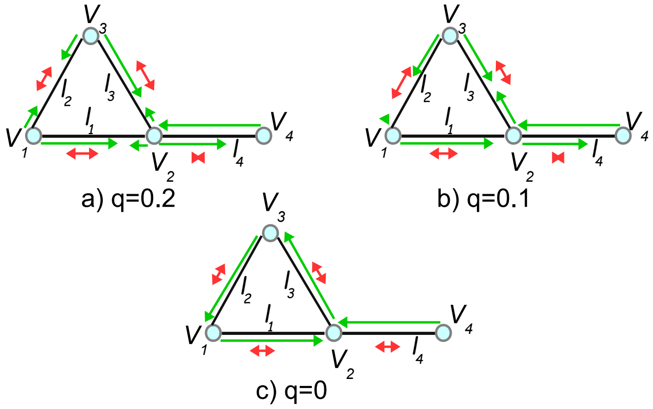

Fig. 4. Depiction of node protection actions, ($p = 0.2$, q varying)

TABLE V
LINK SELECTION PROBABILITIES, $q = p = 0.2$; ECCENTRICITY CASE

	ℓ_1	ℓ_2	ℓ_3	ℓ_4
$r^*_{G,1}(\ell_i)$	1	0	–	–
$r^*_{G,2}(\ell_i)$	0	–	0	1
$r^*_{G,3}(\ell_i)$	–	1	0	–
$r^*_{G,4}(\ell_i)$	–	–	–	1
$q^*_G(\ell_i)$	1	0	0	0

network properties is that a disconnected node leading to a distance of ∞ also prohibitively increases the costs for the individual nodes. In the topology considered, (with a link attack budget of 1,) this can only occur for node 4 when $q > 0$. as a result , in such scenarios, in order to avoid node v_4 being disconnected, we observe that node v_2 now adopts a pure strategy of protecting ℓ_4 to secure the link possibly at the expense of ℓ_1 and ℓ_3.

Specifically, for these network property costs based on eccentricity, we have $p = q = 0.2$ the strategies in Table V, and when $q = \frac{p}{2} = 0.1$, we have the strategies in Table VI. Finally, when q=0, that is one node defending a link is sufficient to protect it, we have the equilibrium in Table VII.

Next, we consider the network depicted in Figure 5, which is composed of two biconnected components with the extreme case of $p = 1$, $q = 0$, which means when a link is protected even by a single link, it is completely secured, but when a link is not protected at all, an adversary attack removes it. In such a case, considering node eccentricity as the local network property, and sum of all node eccentricities for the adversary, we observe that nodes adopt pure strategies, and v_1 protects ℓ_1, v_3 protects ℓ_3, v_5 protects ℓ_5 and v_6 protects ℓ_6. We note that ℓ_4 is protected by either both, or at least one of v_2 and v_4 for different equilibria. As provisioned, the secured portion of the network does not result in forests, but in a spanning tree (Fig. 6).

TABLE VI
LINK SELECTION PROBABILITIES, $q = \frac{p}{2} = 0.1$; ECCENTRICITY CASE

	ℓ_1	ℓ_2	ℓ_3	ℓ_4
$r^*_{G,1}(\ell_i)$	1	0	–	–
$r^*_{G,2}(\ell_i)$	0	–	0	1
$r^*_{G,3}(\ell_i)$	–	0.1875	0.8125	–
$r^*_{G,4}(\ell_i)$	–	–	–	1
$q^*_G(\ell_i)$	0	1	0	0

TABLE VII
LINK SELECTION PROBABILITIES, $p = 0.2, q = 0$; ECCENTRICITY CASE

	ℓ_1	ℓ_2	ℓ_3	ℓ_4
$r^*_{G,1}(\ell_i)$	1	0	–	–
$r^*_{G,2}(\ell_i)$	0	–	1	0
$r^*_{G,3}(\ell_i)$	–	1	0	–
$r^*_{G,4}(\ell_i)$	–	–	–	1
$q^*_G(\ell_i)$	0	0	1	0

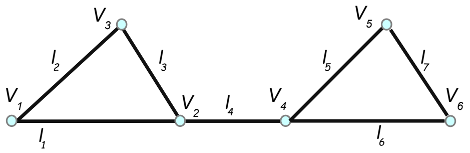

Fig. 5. Two triangles connected through a bridge.

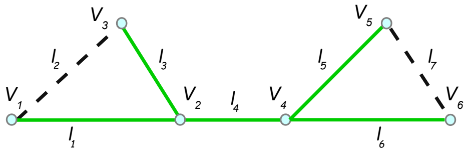

Fig. 6. Two triangles connected through a bridge: $p = 1$, $q = 0$, green links: secured links, dashed links: vulnerable links

VI. CONCLUSIONS

In this work, we have studied network protection in a decentralized setting, where nodes can protect edges in the face of a strategic adversary. We have studied the equilibrium properties of the resultant interaction and observe that, akin to a centralized protection scenario, the nodes will protect important links to the global network property with a higher probability. However, in contrast to the centralized protection setting, the adversary could potentially attack more important links with a higher probability, as demonstrated in Sections IV and V. We have stated certain rules that governs the behavior of the adversary, and observed that it varies significantly with the single-defense attack probability, q, in relation to the no-defense attack probability, p.

While in this paper, we have studied the fundamental properties of the outcome of the interaction between defending nodes and an intelligent adversary, future work will focus on developing protection strategies for the individual nodes. Already, it is evident from our research that the involved nodes should together protect important links in the network such that the probability of their failure is minimized under attack. Studying scenarios where the nodes can protect, and the adversary can attack multiple links is a topic of future research. We would also like to investigate cooperation between nodes while protecting the network using ideas from coalitional game theory.

VII. Appendix

Proof of Lemma 3.1:

For a node i in graph G connected to links $\ell_1 = (i,j)$ and $\ell_2 = (i,k)$, suppose $r^*_{G,i}(\ell_1), r^*_{G,i}(\ell_2) > 0$. From the principle of indifference, this implies that the expected payoff for node i for the pure strategies of defending edges ℓ_1 and ℓ_2 should be equal, otherwise the node would protect that edge that yields a higher expected payoff. Therefore,

$$Q_i^G(\mathbf{q}^*_G, \mathbf{r}^*_{G,-i}, \ell_1) = Q_i^G(\mathbf{q}^*_G, \mathbf{r}^*_{G,-i}, \ell_2) \tag{17}$$

The expected payoff $Q_i^G(\mathbf{q}^*_G, \mathbf{r}^*_{G,-i}, \ell_1)$ has the following terms – (a) the case where the attacked edge is neither ℓ_1 or ℓ_2, (b) the attacked edge is ℓ_1 or ℓ_2 but the defended edge by node i is neither ℓ_1 nor ℓ_2, (c) the attacked edge is ℓ_1 or ℓ_2 and the edge being defended by node i is also ℓ_1 or ℓ_2. Terms listed as (a) and (b) get cancelled on both sides of (17). Since, the terms that remain correspond to the scenarios when either edges ℓ_1 or ℓ_2 is attacked, the strategies of nodes other than i,j and k are irrelevant.

The left hand side of (17) can be expressed as

$$\begin{aligned}
&Q_i^G(\mathbf{q}^*_G, \mathbf{r}^*_{G,-i}, \ell_1)\\
&= \sum_{a\neq\ell_1,\ell_2} \sum_{\mathbf{d}_{-i}\in\mathcal{A}^G_{-i}} \mathbb{E}\left[U_i(G,(\mathbf{d}_{-i},\ell_1),a)\right] \mathbf{r}^*_{G,-i}(\mathbf{d}_{-i}) q^*_G(a)\\
&+ \sum_{\mathbf{d}_{-i}\in\mathcal{A}^G_{-i}:d_j\neq\ell_1} \mathbb{E}\left[U_i(G,(\mathbf{d}_{-i},\ell_1),\ell_1\right] \mathbf{r}^*_{G,-i}(\mathbf{d}_{-i}) q^*_G(\ell_1)\\
&+ \sum_{\mathbf{d}_{-i}\in\mathcal{A}^G_{-i}:d_j=\ell_1} \mathbb{E}\left[U_i(G,(\mathbf{d}_{-i},\ell_1),\ell_1\right] \mathbf{r}^*_{G,-i}(\mathbf{d}_{-i}) q^*_G(\ell_1)\\
&+ \sum_{\mathbf{d}_{-i}\in\mathcal{A}^G_{-i}:d_k\neq\ell_2} \mathbb{E}\left[U_i(G,(\mathbf{d}_{-i},\ell_1),\ell_2\right] \mathbf{r}^*_{G,-i}(\mathbf{d}_{-i}) q^*_G(\ell_2)\\
&+ \sum_{\mathbf{d}_{-i}\in\mathcal{A}^G_{-i}:d_k=\ell_2} \mathbb{E}\left[U_i(G,(\mathbf{d}_{-i},\ell_1),\ell_2\right] \mathbf{r}^*_{G,-i}(\mathbf{d}_{-i}) q^*_G(\ell_2).
\end{aligned} \tag{18}$$

For reasons discussed previously the first term in (18) does not need to be considered. Also, the individual terms in (18) can be written as

$$\begin{aligned}
&\sum_{\mathbf{d}_{-i}\in\mathcal{A}^G_{-i}:d_j\neq\ell_1} \mathbb{E}\left[U_i(G,(\mathbf{d}_{-i},\ell_1),\ell_1\right] \mathbf{r}^*_{G,-i}(\mathbf{d}_{-i}) q^*_G(\ell_1)\\
&= \left[q\nu_i(G\setminus\ell_1) + (1-q)\nu_i(G)\right] q^*_G(\ell_1)(1-r^*_{G,j}(\ell_1)), \qquad (19)\\
&\sum_{\mathbf{d}_{-i}\in\mathcal{A}^G_{-i}:d_j=\ell_1} \mathbb{E}\left[U_i(G,(\mathbf{d}_{-i},\ell_1),\ell_1\right] \mathbf{r}^*_{G,-i}(\mathbf{d}_{-i}) q^*_G(\ell_1)\\
&\qquad = \nu_i(G) q^*_G(\ell_1) r^*_{G,j}(\ell_1), \qquad (20)\\
&\sum_{\mathbf{d}_{-i}\in\mathcal{A}^G_{-i}:d_k\neq\ell_2} \mathbb{E}\left[U_i(G,(\mathbf{d}_{-i},\ell_1),\ell_2\right] \mathbf{r}^*_{G,-i}(\mathbf{d}_{-i}) q^*_G(\ell_2)\\
&= \left[p\nu_i(G\setminus\ell_2) + (1-p)\nu_i(G)\right] q^*_G(\ell_2)(1-r^*_{G,k}(\ell_2)) \qquad (21)\\
&\sum_{\mathbf{d}_{-i}\in\mathcal{A}^G_{-i}:d_k=\ell_2} \mathbb{E}\left[U_i(G,(\mathbf{d}_{-i},\ell_1),\ell_2\right] \mathbf{r}^*_{G,-i}(\mathbf{d}_{-i}) q^*_G(\ell_2)\\
&= \left[q\nu_i(G\setminus\ell_2) + (1-q)\nu_i(G)\right] q^*_G(\ell_2) r^*_{G,k}(\ell_2) \qquad (22)
\end{aligned}$$

We can obtain similar expressions for the right hand side of (17) which corresponds to the scenario when node i is defending ℓ_2. Using (19)-(22) in (17), we obtain

$$\begin{aligned}
&Q_i^G(\mathbf{q}^*_G, \mathbf{r}^*_{G,-i}, \ell_1) = Q_i^G(\mathbf{q}^*_G, \mathbf{r}^*_{G,-i}, \ell_2)\\
&\Rightarrow L_i(\ell_1) q^*_G(\ell_1)\left[(p-q) - (p-2q) r^*_{G,j}(\ell_1)\right]\\
&= L_i(\ell_2) q^*_G(\ell_2)\left[(p-q) - (p-2q) r^*_{G,k}(\ell_2)\right]
\end{aligned} \tag{23}$$

and the first part of the lemma follows after simple algebraic manipulations.

To prove the second part of the lemma, note that because link ℓ_2 is being defended by node i, whereas link ℓ_1 is not; the expected payoff for node i for the pure strategy of defending edge ℓ_2 should be no less than that for defending ℓ_1, i.e.,

$$Q_i^G(\mathbf{q}^*, \mathbf{r}^*_{G,-i}, \ell_1) \leq Q_i^G(\mathbf{q}^*, \mathbf{r}^*_{G,-i}, \ell_2).$$

Following similar steps as for the first part of the lemma leads to (2). ■

References

[1] Gambit: Software tools for game theory, gambit.sourceforge.net.

[2] J. Aspnes, K. Chang, and A. Yampolskiy. Inoculation strategies for victims of viruses and the sum-of-squares partition problem. In *Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '05, pages 43–52, 2005.

[3] E. N. Ciftcioglu, S. Pal, K. S. Chan, D. H. Cansever, A. Swami, A. Singh, and P. Basu. Topology design under adversarial dynamics. In *WiOpt*, May 2016.

[4] E. N. Ciftcioglu, S. Pal, K. S. Chan, D. H. Cansever, A. Swami, A. Singh, and P. Basu. Topology design games and dynamics in adversarial environments. In *IEEE Journal on Selected Areas in Communications*, volume 35, pages 628–642. IEEE, 2017.

[5] E. D. Demaine and M. Zadimoghaddam. Minimizing the diameter of a network using shortcut edges. In *Scandinavian Workshop on Algorithm Theory*, pages 420–431, 2010.

[6] M. V. Dijk, A. Juels, A. Oprea, and R. L. Rivest. Flipit: The game of stealthy takeover. volume 26, pages 655–713. Springer, 2013.

[7] A. Fabrikant, A. Luthra, E. Maneva, C. H. Papadimitriou, and S. Shenker. On a network creation game. In *Proceedings of Principles of Distributed Computing*, PODC '03, pages 347–351. ACM, 2003.

[8] D. Fudenberg and J. Tirole. Game theory, 1991. *Cambridge, Massachusetts*, 393:12, 1991.

[9] S. Goyal and A. Vigier. Attack, defence, and contagion in networks. *The Review of Economic Studies*, 81(4):1518–1542, 2014.

[10] A. Gueye, J. C. Walrand, and V. Anantharam. Design of network topology in an adversarial environment. In *Proceedings of the First International Conference on Decision and Game Theory for Security*, GameSec'10, pages 1–20, Berlin, Heidelberg, 2010. Springer-Verlag.

[11] V. S. A. Kumar, R. Rajaraman, Z. Sun, and R. Sundaram. Existence theorems and approximation algorithms for generalized network security games. In *Proceedings of IEEE International Conference on Distributed Computing Systems*, ICDCS '10, pages 348–357, 2010.

[12] A. Laszka and A. Gueye. Network topology vulnerability/cost trade-off: Model, application, and computational complexity. volume 11, pages 588–626. Taylor & Francis, 2015.

[13] A. Laszka, G. Horvath, M. Felegyhazi, and L. Buttyán. Flipthem: Modeling targeted attacks with flipit for multiple resources. In *International Conference on Decision and Game Theory for Security*, pages 175–194. Springer, 2014.

[14] A. Meyerson and B. Tagiku. Minimizing average shortest path distances via shortcut edge addition. In *APPROX-RANDOM*, volume 5687 of *LNCS*, pages 272–285. Springer, 2009.

[15] T. Watanabe and A. Nakamura. Edge-connectivity augmentation problems. *Journal of Computer and System Sciences*, 35(1), 1987.