Extended Horizons: Multi-hop Awareness in Network Games

Raman Ebrahimi and Parinaz Naghizadeh

University of California, San Diego, La Jolla, CA 92093, USA
{raman,parinaz}@ucsd.edu

Abstract. Network/interdependent security games have been extensively used in the literature to gain insights into how firms make optimal security decisions when accounting for spillovers of risks from other firms with whom they have risk interdependencies. We extend these models by proposing *K-hop network (security) games*, in which agents have *extended awareness* of network effects: an agent in a K-hop network game accounts for not only its immediate neighbors (those with whom it directly has joint operations or shared infrastructure), but also the spillover of the (security) risks from agents up to K-hops away from it. We first establish an equivalence between our proposed K-hop network games and a one-hop game played on an appropriately defined adjacency matrix. Then, through analytical results and numerical examples, we illustrate how subtle changes in a network can significantly alter equilibrium behaviors when accounting for multi-hop risk spillovers, emphasizing the dependency of agents' efforts on the nature of their dependencies (complement vs. substitute nature of efforts), agents' different levels K of awareness of the network effects, and the reactive vs. passive nature of lower awareness (lower K) agents to those with higher awareness (higher K). Our findings show that extended awareness of network effects can, in general, benefit agents by allowing them to optimize their security planning and resource allocation, but that decision makers who are less sophisticated and lack this awareness can suffer, and that consequently, overall investment levels in security may deteriorate.

Keywords: Network Games · Interdependent Security Games · Strategic Awareness.

1 Introduction

The study of strategic interactions in networked environments has received significant attention in the literature on game theory and its applications to cybersecurity; see [5,13,18] for surveys. In this context, *network (security) games* (also known as *interdependent security games*) are often used to model scenarios where each node represents a strategic decision-maker or firm, and each connection signifies an interdependence in the firms' security state or operations. Traditionally, these models are used to gain (qualitative) insight into the strategic security investments of decision-makers who consider how the actions

of their immediate (one-hop) neighbors could expose them to spillover security risks (e.g., [7,9,10,17,25,34]). These studies can inform us about the extent of free-riding of agents on each other's effort due to network effects, its impact on equilibrium suboptimality (in terms of social welfare or other notions of cumulative security costs), and potential interventions to alleviate it.

As cyber-physical systems become more complex and interconnected, it is crucial for decision makers to better understand how their interdependence on others should shape their organization's security budgeting and investments, and to do so *beyond their immediate neighbors*. The 2021 Kaseya Attack [21,23] illustrates this clearly. Attackers initially compromised Kaseya's VSA software, then used it to distribute ransomware to Managed Service Providers (MSPs) and their clients. This attack affected over 1,500 organizations, including schools, supermarkets, and a national railway. The disruption to the railway, for example, potentially impacted other businesses reliant on its services, highlighting the far-reaching (multi-hop) effects of one firm's security decisions on other firms in the system. Similarly, the 2021 Colonial Pipeline attack [2] exhibits multi-hop risk dependencies: the ransomware attack led to a shutdown of the pipeline, causing fuel shortages and rising prices. This affected not just consumers but also businesses dependent on fuel, such as airlines and logistics companies. A formal model of network games in which agents are aware of, and best-respond to, the efforts of not only their immediate neighbors, but also of agents multiple hops away, has potential to capture such events, and offer richer insights into strategic behavior and potential security interventions.

Motivated by this, in this paper, we extend the framework of network (security) games considered in prior work (e.g., [3,6,11,16,19,20,32]) to encompass the influence of multi-hop neighbors. These neighbors can be in the same network or can be neighbors in a multiplex network. By incorporating awareness of multi-hop security dependencies, we aim to provide a more comprehensive understanding of how strategic influences propagate through the network and affect agents' decisions to free-ride on others (and potentially underinvest in security which is a public good).

Formally, we propose a model of *K-hop network (security) games*, in which agents have *extended* awareness of network effects: an agent in a K-hop network game considers, or is aware of, the spillover of the (security) efforts of agents up to K-hops away from it when selecting its own effort. We then explore the implications of such extended awareness on agents' strategic security decision making by looking into the Nash equilibria that arise as agents' awareness of the network (the K in the K-hop game) increases. We begin by using illustrative examples to show that these changes are impacted by three factors: (1) the nature of the agents' dependencies (complement vs. substitute nature of efforts), (2) agents' different levels K of awareness of the network effects, and (3) the reactive vs. passive nature of lower awareness (lower K) agents to those with higher awareness (higher K). Accordingly, we provide analytical equilibrium characterizations and comparisons for two settings:

1. *The Nash equilibrium when all agents have K-hop awareness, for general K.* Specifically, for a general K-hop network game, we show that the game is equivalent to a one-hop network game played on a new network interdependency matrix $\hat{G}$, constructed from the original game matrix G, in a way that the links $\hat{g}_{ij}$ between agents i and j account for the spillovers across all paths of length at most K to agent i from agent j.
2. *A mixture of one aware (e.g., $K = 2$) and $N - 1$ unaware (e.g., $K = 1$) agents in games of pure strategic substitutes/complements.* For this case, we show that in a game of strategic substitutes, the agent can free-ride more on others by increasing its awareness compared to other agents. This means that awareness can benefit the aware agent by allowing it to attain the same security outcomes while lowering its effort (and therefore, overall increasing its utility), but that at the same time, it will hurt the other unaware and passive agents, as they will be (incorrectly) assuming that the aware agent is exerting higher effort than it truly is. We also provide a lower bound for the effort of an agent with two-hop awareness in a game of strategic complements, constructed from the agent's efforts in one-hop awareness games.

Finally, we explore the K-hop equilibrium structure and provide numerical experiments for special network structures (e.g., Stars, Directed Acyclic Graphs, and Random Graphs).

To summarize, our main contributions include: (i) proposing a new model to capture extended network awareness in network security games, (ii) showing an equivalence between our proposed K-hop games and a one-hop game played on an appropriately defined adjacency matrix, and (iii) elaborating on the impacts of K-hop awareness on agents' security efforts, as well as on the equilibrium's quality (in terms of agents sum of efforts), both analytically and through numerical experiments. Our findings show that extended awareness of network effects can, in general, benefit agents by allowing them to optimize their security planning and resource allocation, but that decision makers who are less sophisticated and lack this awareness can suffer, and that consequently, overall investment levels in security are highly dependant on network structure and they may improve or deteriorate.

The remainder of this paper is organized as follows. We review the work most closely related to our paper in Section 1.1. In Section 2, we review the commonly studied model of (one-hop) network security games, and then introduce our proposed model of K-hop network games. We analyze the equilibria of this model in Section 3, and illustrate our findings on special network structures and using numerical experiments in Section 4. We conclude with directions for future work in Section 5.

1.1 Related Work

Game-theoretical studies of security decision making on networks have adopted different modeling choices. We contrast the interdependent/network security

game models we consider here, with two other prominent models: network interdiction games, and attack graph models. Network interdiction games focus on the strategic disruption of networks facing adversarial attackers, by identifying and neutralizing critical nodes or links to impede the adversary's operations [26,28,29]. Attack graphs, on the other hand, model the possible pathways an attacker could take to compromise a network, helping defenders understand potential vulnerabilities and prioritize defenses [1,15,24,27,33]. Network security games in general, and our model included, do not consider the potential evolving or stepping-stone nature of attacks, but rather the equilibrium state. That is, unlike network interdiction games and attack graph models, an agent in a network security game model decides on its security investments once, as a best-response to an equilibrium state of the network, before attacks are launched, and does not adjust any links or investments in response to an evolving attack in the graph.

Our work is most closely related to the literature on network games. Some previous works on general network games (not restricted to the security context) include [11,16,19,20,22,31,32,35]. [19] has specifically discussed the existence and uniqueness Nash equilibrium for security decision making using linear influence networks while [20,22] have looked at existence, uniqueness, and stability of one-hop network games where necessary and sufficient conditions for guaranteed uniqueness are introduced. [11] characterizes the price of anarchy in the strategic form game and compares the benefits of improving security technology and improving incentives, and shows that improving technology alone may not offset the price of anarchy. [16] has summarized the modeling assumptions and categorized the equilibrium solutions in interdependent security games, [31,35] explore the bounded rationality of players using quantal response model and prospect theory. Our framework can also be seen as a discussion of boundedly rational agents (those who lack awareness of all network risk spillovers affecting them).

Access to information about other firms' security decisions, and decisions regarding information sharing, can significantly impact firms' security posture, as noted by [4]. Despite the potential benefits, various concerns such as confidentiality often hinder information sharing. To address this, legislation such as the Cybersecurity Information Sharing Act of 2015 [8] and guidance from the National Institute of Standards and Technology (NIST) [12] encourage firms to share intelligence.

In relation to our paper, we suggest that information shared by firms can also be viewed as a means of increasing their network awareness, providing them information about other firms' security behavior and of potential multi-hop risk spillovers (in our terminology, helping them change from passive to reactive agents, even if they do not possess multi-hop awareness). Specifically, we argue that lack of awareness can hurt decision makers when other agents have extended network awareness; mandating or incentivizing information sharing can help alleviate such issues.

2 Model

2.1 One-hop Model

We consider a network of N interconnected decision-makers; these can include device owners/operators, various divisions within a larger organization, or different sectors of the economy. We specify this network using a graph $\mathcal{G} \coloneqq \langle \mathcal{V}, G \rangle$ with the N agents as the set of vertices $\mathcal{V}$, and a weighted and directed interdependency matrix G specifying their connections, where $g_{ij} \in \mathbb{R}$ captures the dependence of agent i's security outcomes on agent j's security efforts (as detailed shortly).

Each agent i selects an *effort* $x_i \in \mathbb{R}_{\geq 0}$; this could represent the agent's investment in security (hardware, software, employee training, etc.). This effort impacts not only the agent itself, but also other agents in the network, as captured by the interdependency matrix G. Specifically, when $g_{ij} \geq 0$, we call i and j's relationship a strategic *substitute*; this means that if agent j is better protected, it is less likely that it is compromised and used to launch an attack on agent i, and as a result, i can invest less in security and achieve the same security outcomes. In contrast, $g_{ij} \leq 0$ is a strategic *complement* relation; meaning, if agent j increases its security effort, it is less likely to be attacked, making agent i more likely to be the target of an attack instead, so that i has to invest more in security in order to achieve the same security outcome.

The agent's utility is determined by its own action, as well as the actions of its one-hop neighboring agents. Let $\mathbf{x} \in \mathbb{R}^{N \times 1}$ denote the vector of all agents' actions. Then, agent i's utility is given by:

$$u_i(\mathbf{x}; G) = b_i(x_i + \sum_{j=1}^{N} g_{ij} x_j) - c_i x_i \ , \tag{1}$$

where $b_i(\cdot) : \mathbb{R} \to \mathbb{R}$ is a twice-differentiable, strictly increasing, and strictly concave *benefit function*, which has as its argument the *aggregate effort* experienced by the agent from its one-hop neighbors in the graph, and $c_i > 0$ is the *unit cost* of effort for agent i.

The (one-hop) network game involving a set of N agents, their efforts $\mathbf{x}$, and their utility functions $u_i(\mathbf{x}; G)$, has been extensively analyzed in previous studies (e.g., [3, 6, 11, 19, 20]). These games are known as games of *linear best-replies*, where the Nash equilibrium $\mathbf{x}^*$ is characterized by a set of linear best-response equations:

$$x_i^* = \max\{0, q_i - \sum_{j \in \mathcal{N}_i} g_{ij} x_j^*\}, \tag{2}$$

where q_i satisfies $b_i'(q_i) = c_i$. This condition ensures that the agent's effort is optimal, balancing marginal benefits and costs. The best-response (2) indicates that agent i exerts an effort x_i^* to reach the aggregate effort level q_i, considering the spillover $\sum_j g_{ij} x_j^*$ from its one-hop neighbors' efforts at equilibrium. If the

combined effort from neighboring agents already meets or exceeds q_i, agent i will exert no additional effort.

We next propose an extension of this model: K-hop network (security) games, in which agents are more "aware" as they account for the impacts of actions taken by those further away in the network on their security.

2.2 K-hop Model

We consider the same set of agents on the same network but with an *extended* awareness: an agent in a K-hop network game considers, or is aware of, the spillover of the (security) efforts of other agents up to K-hop away when selecting its effort.

Formally, the utility of an agent i with K-hop awareness is given by:

$$u_i^{(K)}(\mathbf{x}; G) = b_i(\, x_i + \sum_{k=1}^{K} \sum_{j=1}^{N} g_{ij}^{(k)} x_j \,) - c_i x_i \ , \tag{3}$$

where for agents i and j, $g_{ij}^{(k)}$ is the element in the i^{th} row and j^{th} column of the k^{th} power of the adjacency matrix G, and captures the impact of an agent j who is k-hops away on agent i's utility. By summing over the possible k's (from 1 to K), we are considering the impact of all possible effort spillovers from neighbors within k-hops of agent i on its utility.

This model also leads to a network game of linear best-replies. The Nash equilibrium $\mathbf{x}^*_{(K)}$ for agents with K-hop awareness is determined by:

$$x^*_{i_{(K)}} = \max\{0, q_i - \sum_{k=1}^{K} \sum_{j=1}^{N} g_{ij}^{(k)} x^*_{j_{(K)}}\} \tag{4}$$

Note that this model captures the commonly studied network security game model of Section 2.1 when $K = 1$. As K increases, the agent has more awareness of other agents further away in the network. As a special case, for $K \to \infty$, we say the agent attains *omni-vision*, as the agent will be accounting for, and best-responds to, the efforts of all other (reachable) agents in the network and all paths through which risk spillovers can propagate and reach it. For this setting, if all agents have omni-vision, agent i's utility (3) at the ∞-hop game's Nash equilibrium is given by:

$$u_i^{(\infty)}(\mathbf{x}^*_{(\infty)}; G) = b_i\Big(\big((I + G + G^2 + G^3 + \ldots)\mathbf{x}^*_{(\infty)}\big)_i\Big) - c_i x_i \ , \tag{5}$$

Let $S \coloneqq I + G + G^2 + G^3 + \ldots$. It is easy to see that $S(I - G) = I$, or $S = (I - G)^{-1}$, provided that S converges. It is known that $\lim_{k\to\infty} G^k = 0$ if and only if $\rho(G) < 1$, where $\rho(G)$ is the spectral radius of G; absolute convergence of S is guaranteed under this condition [30,36]. Using this relation, in our analysis of K-hop games in Section 3.1, we will establish a relation between the K-hop game's Nash equilibrium characterization and the matrix $(I - G)^{-1}$.

3 Impacts of Extended Awareness: Nash Equilibria of K-hop Network Games

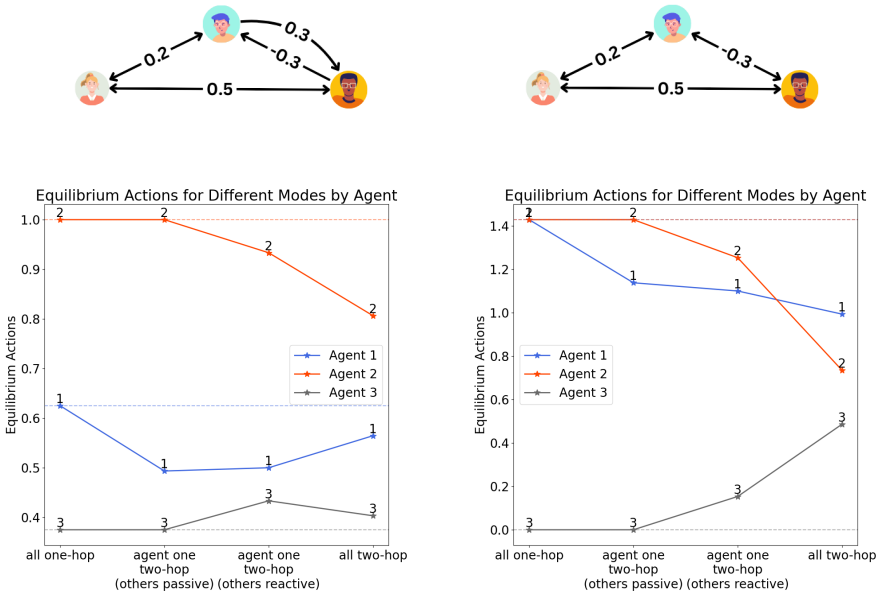
In this section, we explore the implications of agents' extended awareness on their strategic security decision making by looking into the Nash equilibria that arise as agents' awareness of the network (the K in the K-hop game) increases.

Warm-up: no awareness ($K = 0$) to one-hop awareness ($K = 1$). In order to illustrate the impacts of extended awareness, we start with a warm-up case: increasing awareness from $K = 0$ (no awareness; ignoring all network effects) to $K = 1$ (the commonly studied one-hop network security game). The equilibrium of the $K = 0$ game is $\mathbf{x}^* = \mathbf{q}^*$ (i.e., each agent i investing at its respective indifference point q_i). When awareness is upgraded to $K = 1$, the new optimal effort levels depend on whether only some or all agents access a higher awareness. We first consider the case where only one agent (*w.l.o.g.*, agent $i = 1$) can upgrade its awareness from $K = 0$ to $K = 1$: the equilibrium will be $x_1^* = \max\{0, q_1 - \sum_j g_{1j} q_j\}$, and $x_j^* = q_j, \forall j \neq 1$. We can see that the change in agent 1's effort depends on the nature of the game graph. For instance, for games of strategic substitutes (resp. complements) where $g_{ij} \geq 0, \forall j$ (resp. $g_{ij} \leq 0, \forall j$), agent 1 lowers (resp. increases) its efforts and its free riding increases (resp. decreases) as the agent becomes aware of its dependence on other agents. At the other extreme, if all agents can upgrade their awareness from $K = 0$ to $K = 1$, the NE is given by the fixed point of best-responses in (2); again, depending on the substitute/complement effects, the effort of each agent i may increase or decrease compared to the $K = 0$ case.

An illustrative example: one-hop ($K = 1$) to two-hop awareness ($K = 2$). From the above warm-up case, we can see that the impacts of increasing awareness on agents' efforts depend on (1) the strategic or complement nature of their dependencies, and (2) the potential differences in the awareness levels of agents. In the following numerical example, we highlight the same effects when awareness increases from immediate neighbors ($K = 1$) to two-hop away neighbors ($K = 2$), and further show that an additional consideration arises: (3) whether agents with lower awareness are *passive* or *reactive*. In the *passive* case, less aware agents (here, those with 1-hop awareness) best-respond assuming all other agents have lower awareness, too. *Reactive* (but still less aware) agents, on the other hand, best-respond to the observed level of effort of all agents, including the higher-awareness agents. The rationale is that these lower awareness agents assume any higher awareness agents are behaving sub-optimally without attributing a reason to their (perceived) sub-optimal efforts.

Example 1. Consider two network games represented by the adjacency matrices $A = \begin{pmatrix} 0 & 0.3 & 0.2 \\ -0.3 & 0 & 0.5 \\ 0.2 & 0.5 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & -0.3 & 0.2 \\ -0.3 & 0 & 0.5 \\ 0.2 & 0.5 & 0 \end{pmatrix}$, and with $\mathbf{q} = [1, 1, 1]^T$.

The only difference between the two networks is in edge g_{12}. As illustrated by Figure 1 we can see that by changing only this one link in the network, the



(a) Network A of agents (top) and their actions (bottom)

(b) Network B of agents (top) and their actions (bottom)

Fig. 1: Two different scenarios arise for two largely similar networks as levels of awareness increase.

equilibrium in each scenario (all one-hop aware, only agent 1 two-hop aware and others passive/reactive, and all two-hop aware) changes.

Focusing on Figure 1a first, we can see that agent 1 can free-ride more by being two-hop aware. If other agents are unaware themselves but reactive to agent 1's two-hop awareness, they adjust their efforts according to agent 1's lowered investment, agent 2 by decreasing its effort due to the negative link and agent 3 by increasing its own effort due to the positive link. If these agents manage to acquire resources to also become two-hop away, then agent 1 will increase its effort since agents 2 and 3 will also free-ride more by becoming two-hop aware.

Looking at Figure 1b next, we see a different change in the equilibrium, even though, compared to Figure 1a, the networks are not very different. Specifically, when other agents become reactive to agent 1's 2-hop awareness, they will have two different reactions: (i) agent 2 will also start free-riding more due to the negative link, (ii) agent 3 tries to make up for this with a higher effort. Lastly, when all agents have two-hop awareness, agents 1 and 2 will free-ride more, and agent 3 will try to make up for this by its own effort.

Motivated by the above examples, we next provide analytical results for two settings: Section 3.1 characterizes the equilibrium when all agents have K-hop awareness for general K, while Section 3.2 considers a mixture of one aware (e.g.,

$K = 2$) and $N - 1$ unaware (e.g., $K = 1$) agents in games of pure strategic substitutes/complements, and the impacts of the unaware agents' passive behavior on the ability of the one aware agent to free-ride on them.[1]

3.1 All K-hop Aware Agents

In this section, we consider games where all agents are aware of their K-hop neighbors (and are reactive). We start with the scenario $K < \infty$, which represents a case in which agents may not have the resources to be aware of all reachable agents and, at best, only take some into account. We also discuss the special case of $K \to \infty$; this case is important as it represents an ideal scenario where agents have unlimited resources and can best-respond to all reachable agents regardless of how distant they are, which we call *omni-vision*. We compare the two cases, and illustrate the differences using an example at the end of the subsection.

Nash equilibria of K-hop network games. In the following proposition, we identify an equivalence between the Nash equilibria of such K-hop games and that of a one-hop game with a specific adjacency matrix.

Proposition 1. *If $\rho(G) < 1$, then best-response of agents in a K-hop network game is the same as the best-response of agents in a one-hop game on a network with adjacency matrix $\hat{G} = (I - G)^{-1}(I - G^{K+1}) - I$.*

Proof. If $\rho(G) < 1$ we can define $S_K \coloneqq I + G + G^2 + \ldots + G^K = (I - G)^{-1}(I - G^{K+1})$, we can write agent i's K-hop best-response (4) as:

$$\begin{aligned} x^*_{i_{(K)}} &= \max\{0, q_i - \sum_{j=1}^{N} [S_K - I]_{ij}\, x^*_{j_{(K)}}\} \\ &= \max\{0, q_i + x^*_{i_{(K)}} - \sum_{j=1}^{N} [(I - G)^{-1}(I - G^{K+1})]_{ij}\, x^*_{j_{(K)}}\} \end{aligned} \tag{6}$$

which is equivalent to the best-response (2) of a one-hop game on a network with adjacency matrix $(I - G)^{-1}(I - G^{K+1}) - I$.

In Proposition 1, we are constructing a new network interdependency matrix $\hat{G}$ from the original matrix G in a way that the links $\hat{g}_{ij}$ between agents i and j account for the spillovers across all paths of length at most K to agent i from agent j in the original game.

The following corollary considers the special case of an ∞-hop game where all agents have omni-vision, i.e., they are aware of, and best-respond to, the efforts of all other agents.

[1] We will illustrate similar impacts when $K \geq 2$ and in general games of mixed strategic complements/substitutes through numerical experiments in Section 4.

Corollary 1. *If $\rho(G) < 1$, then the best-response of agents in a ∞-hop network game is the same as the best-response of agents in a one-hop game on a network with adjacency matrix $\hat{G} = G(I - G)^{-1}$.*

The proof follows from noting that if $\rho(G) < 1$, then $\lim_{K\to\infty} G^{K+1} = 0$, and that the infinite sum $S = I + G + G^2 + \ldots$ can be re-written $S - I = G(I + G + G^2 + \ldots) = GS = G(I - G)^{-1}$.

By reducing a K-hop game to a one-hop game on an appropriately transformed network, analysts can more easily predict and manage the propagation of risks and the strategic interactions between different entities in the network. This reduction allows for the application of existing tools and methodologies designed for one-hop games, which are often more mature and better understood. For example, this approach can be applied to verify the uniqueness of the Nash equilibrium in a K-hop network game which we know the Nash equilibrium of the one-hop network game is unique.

3.2 Mixture of Aware and Unaware Agents

The previous subsection analyzed the K-hop game's Nash equilibrium when all agents can attain K-hop awareness. However, it may not be possible for all agents to attain this awareness. One reason could be limited resources to gather intelligence about other agents' security decisions or the high cost of processing all available information. For instance, higher-level agents in a hierarchical network are expected to have full knowledge of the branches below them, but they may only have limited awareness due to the constraints of the human mind [14].

Motivated by this, we consider a scenario in which only one agent is able to upgrade its awareness (e.g., best-responding to both immediate and 2-hop away neighbors), while others are passive and remain at a lower awareness level (e.g., considering only their immediate neighbors). We discuss the change in the effort of the aware agent, and its ability to free-ride on others given their passive and unaware strategies. We present this analysis for two special network structures: games of strategic substitutes and games of strategic complements, where $g_{ij} \geq 0$ and $g_{ij} \leq 0$, respectively, for all i, j. The former captures networks where a security compromise of one agent negatively impacts others connected to it (due to, e.g., the spread of the attack or disruption of joint operations). The latter is most closely related to networks where attackers are interested in identifying the weakest targets.

We start with the impacts of one agent unilaterally upgrading its awareness in a game of strategic substitutes.[2]

Proposition 2. *Consider a network game of strategic substitutes, where agent i has K-hop awareness, while agents $j \neq i$ have $K' < K$ awareness. Then, agent i's effort will be lower compared to a game where it also had K'-awareness if and only if there is at least one agent l with effort $x^*_{l,(K')} > 0$ is $K' < k \leq K$ hops*

[2] The results of Proposition 2 also hold for the case of general networks if all paths with distance K have an even number of complement (negative weight) edges.

away from agent i. If no such agent exists, agent i's effort will be the same as the game where it also had K'-awareness.

Proof. When agent i is aware of up to K-hop neighbors in its best-response, while other agents are only aware of others at most $K' < K$ hops away, we can write:

$$x^*_{i_{(k)}} = \max\{0, q_i - \sum_{j=1}^{N}\sum_{l=1}^{K'} g_{ij}^{(l)} x^*_{j_{(K')}} - \sum_{j=1}^{N}\sum_{l=K'+1}^{K} g_{ij}^{(l)} x^*_{j_{(K')}}\} \tag{7}$$

For a game of strategic substitutes, we know $g_{ij}^{(l)} \geq 0$ for all l. Therefore we can conclude that $\sum_{j=1}^{N}\sum_{l=K'+1}^{k} g_{ij}^{(l)} x^*_{j_{(K')}} \geq 0$ and will strictly be positive if at least one agent with positive effort is reachable with $K' < k \leq K$ hops.

Proposition 2 states that if an agent becomes more aware than others in a game of strategic substitutes, it can (weakly) increase its free-riding on others. As a special case, if for the aware agent $x^*_{i_{(K')}} = 0$ at some K', then $x^*_{i_{(K)}} = 0$ for all $K > K'$. This means that awareness can benefit the aware agent by allowing it to attain the same security outcomes while lowering its effort (and therefore, overall increasing its utility), but that at the same time, it will hurt the other unaware and passive agents, as they will be (incorrectly) assuming that the aware agent is exerting higher effort than it truly is.

For *games of strategic complements*, on the other hand, we cannot make a statement as general as Proposition 2, since the sign of all entries of the powers of the adjacency matrix will be alternating, i.e., $g_{ij}^{(2n-1)} \leq 0$, $g_{ij}^{(2n)} \geq 0$ for all i and j. In other words, even though the odd-hop away neighbors maintain a strategic complement relation to agent i's effort, neighbors even number of hops away are turned into *strategic substitutes* from the viewpoint of agent i. That said, we can comment on the efforts at equilibrium when awareness increases from K to $K+1$ hops. Specifically, by defining $\bar{g}_i$ as the impact of agent i's most influential neighbor, i.e., $\bar{g}_i = \{g_{ij} : |g_{ij}| \geq |g_{ik}|, \forall k\}$, we can state the following result.

Proposition 3. *Consider a game of strategic complements where agent i has two-hop awareness while agents $j \neq i$ have one-hop awareness. Then agent i's effort will be lower compared to a game where it also had one-hop awareness, assuming $q_i > 0$, at most by $\bar{g}_i \sum_j \sum_k g_{kj} x^*_j$.*

Proof. Since $q_i > 0$, we can write $x^*_{i_{(1)}} = q_i - \sum_{j=1}^{N} g_{ij} x^*_{j_{(1)}} \geq 0$ and accordingly write $x^*_{i_{(2)}}$ as:

$$\begin{aligned} x^*_{i_{(2)}} &= \max\{0, q_i - \sum_{j=1}^{N}(g_{ij} + \sum_{k=1}^{N} g_{ik}g_{kj}) x^*_{j_{(1)}}\} \\ &= \max\{0, x^*_{i_{(1)}} - \sum_{j=1}^{N}\sum_{k=1}^{N} g_{ik}g_{kj} x^*_{j_{(1)}}\} \end{aligned} \tag{8}$$

Further, since we know $g_{ij} \leq 0$ we can further write $\sum_{k=1}^{N} g_{ik} g_{kj} x_j^* \leq \bar{g}_i \sum_k g_{kj} x_j^*$ where $\bar{g}_i$ is the element with largest absolute value in row i, i.e. most influential neighbor of agent i. Therefore, we can write:

$$x_{i_{(1)}}^* - \bar{g}_i \sum_{j=1}^{N} \sum_{k=1}^{N} g_{kj} x_{j_{(1)}}^* \leq x_{i_{(2)}}^* \leq x_{i_{(1)}}^* \tag{9}$$

The second term on the LHS bound in (9) is non-negative, confirming that for this setting, upgrading the awareness will not make the agents put in more effort.

The term $\sum_{j=1}^{N} \sum_{k=1}^{N} g_{kj} x_j^*$ could be interpreted in the network as the sum of the spillovers of all agents if they all had one-hop awareness. Therefore, the amount that agent i can free-ride by having two-hop awareness, compared to one-hop awareness, is bounded by the sum of spillovers of all agents over the network, weighted by the most influential neighbors of the agents.

We next take advantage of the knowledge of specific network structures and numerical experiments to discuss the more general cases and remove the constraints on edge weights.

4 Special Network Structures

In this section, we examine specific network structures and analyze each, both analytically and numerically. We identify equilibria in synthetic networks where all agents have K-hop awareness with varying K. We employ the sum of efforts as a baseline metric to assess the "quality" of the game. This evaluation is further extended by comparing $\sum_i q_i$ with the outcomes from games incorporating K-hop awareness, represented by $\sum_i x_{i_{(K)}}^*$. Our analysis begins with elementary graph configurations, such as cycles and star graphs, before advancing to a more general case of directed acyclic graphs.

One-way Cycle: It is relatively easier to understand the changes in the efforts of the agents in cycle graphs. Consider a directed one-way cycle graph with similar connections between agents, meaning that each agent i only has an outgoing link to agent $i+1$ with weight g. For this case, we have $g_{i,i-1} = 0$. This way, the best-response of agents will come down to:

$$x_{i_{(k)}}^* = \max\{0, q_i - \sum_{l=1}^{k} g^l x_{i+l_{(k)}}^*\} \tag{10}$$

As previously noted, for $g > 0$, it holds that $x_{i_{(k)}}^* \leq x_{i_{(k')}}^*$ for $k > k'$. Conversely, if $g < 0$, oscillations occur due to the alternating sign of the summation term in (10). For $|g| < 1$, these oscillations will converge as the number of considered hops grows, $\lim_{n\to\infty} g^n = 0$. However, if $|g| > 1$, the powers of g will diverge, also with alternating signs. In cases of high awareness levels, an agent

may completely free-ride and have, $x^*_{i_{(2k-1)}} = 0$, if aware of an even number of hops and exert significant effort, $x^*_{i_{(2k)}} \gg 0$, when aware of an odd number of hops. This analysis underscores that even in a straightforward case of a one-way cycle with uniform link weights, the increase in agents' awareness can lead to a range of outcomes.

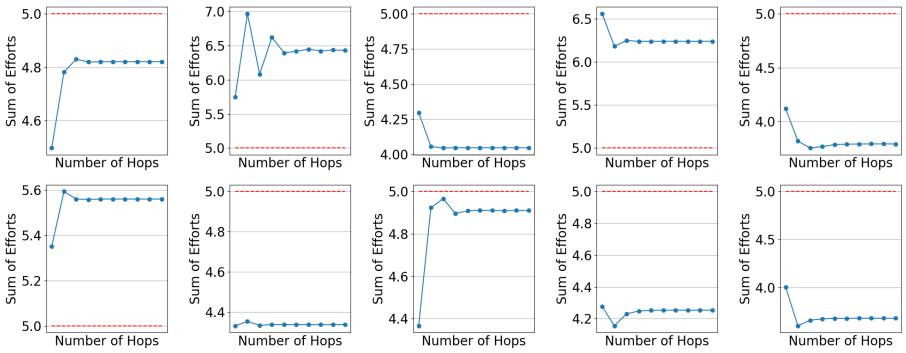


Fig. 2: Game quality comparison for 10 randomly generated one-way cycle networks with 5 K-hop aware agents (K from 1 to 10) with the no awareness case (dashed red line).

To relax the conditions on the connections in this case, with the aim to comment on the impact of network structure, we work with randomly generated weights within the range $(-1, 1)$ and calculate the equilibrium. In Figure 2, each data point represents the game quality on a randomly generated network of 5 agents for when agents are aware of K-hops with K going from 1 to 10. We can see that after a few hops the game quality converges, however, we can see that game quality can be either above or below the starting point which is no awareness. This indicates that by considering more hops, the spillovers are becoming less and less important. Also, the jump in game quality after going from one-hop to two-hop is significant.

Star Network: Another simple structure that can be of interest is star networks. Star networks have been studied in various applications, such as the structure of the internet [37]. Consider an undirected star network with the central node labeled as 1, and the remaining nodes are only connected to the central node. This way we have one node with $n-1$ connections and $n-1$ nodes with 1 connection, the adjacency matrix of this network will have the form $G = \begin{pmatrix} 0 & g_{1\cdot}^T \\ g_{1\cdot} & \mathbf{0} \end{pmatrix}$ and $G^2 = \begin{pmatrix} \|g_{1\cdot}\|_2^2 & 0 \\ 0 & g_{1\cdot} g_{1\cdot}^T \end{pmatrix}$, where the bottom right block is an $n-1 \times n-1$ matrix with i^{th} row being: $[g_{12}g_{1i}, g_{i3}g_{1i}, \ldots, g_{ii}^2, \ldots, g_{1n}g_{1i}]$.

Therefore, the agents' efforts after considering two hops will be as follows:

$$x^*_{1_{(2)}} = \max\{0, q_1 - g_{1\cdot}^T \mathbf{x}^*{}_{(2)} - \|g_{1\cdot}\|_2^2 x^*_{1_{(2)}}\} \tag{11}$$

$$x^*_{i_{(2)}} = \max\{0, q_i - g_{1i}(x^*_{1_{(2)}} + \sum_k g_{1k} x^*_{k_{(2)}})\} \tag{12}$$

We can see for the central agent, the rebound of its own effort ($\|g_{1\cdot}\|_2^2 x^*_{1_{(2)}}$) is allowing it to free-ride more and have a lower effort, while $q_1 - g_{1\cdot}^T \mathbf{x}^*{}_{(2)}$ is similar to one-hop awareness, with the only difference of accounting for other agents being two-hop aware. The case for non-central agents is rather simple as well. The two-hop spillovers are weighted by the two-hop neighbors' connection to the central agent and then summed with the effort of the only one-hop neighbor of agent i, agent 1. Again, for an easier conclusion, we turn to numerical simulation on synthetic networks with edge weights randomly generated in the range $(-1, 1)$ with 5 agents.

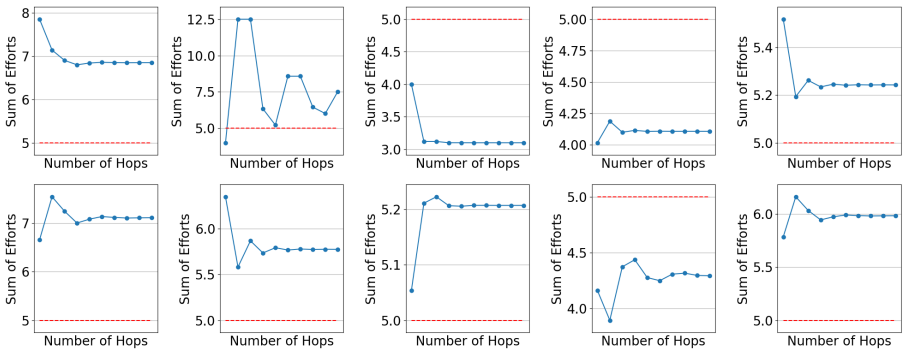


Fig. 3: Game quality comparison for 10 randomly generated star networks with 5 K-hop aware agents (K from 1 to 10) with the no awareness case (dashed red line).

As seen in Figure 3, in terms of game quality, this case is very similar to the case of the one-way cycle, even though the effort profiles can be very different.

Directed Acyclic Graph: Hierarchical structures are pervasive across various domains seen in technological systems, such as the Internet, organizational structures, and software architectures. Directed Acyclic Graphs (DAGs) are a specific type of hierarchical network characterized by a directed graph with no cycles, meaning there is a unidirectional flow from one node to another without returning to the starting node.

These types of networks can be represented by upper triangular adjacency matrices with zero diagonals, given that loops are not allowed. Normally, in

hierarchical matrices, the higher nodes have the full awareness of the sub-network below them, we can use k-hop model to capture this property of these networks.

For these networks, we can iteratively calculate all equilibrium efforts by starting from the bottom of the hierarchy (agents that have no outgoing links) and moving upwards. This is possible because The k^{th} power of an upper triangular matrix with zero diagonals is an upper triangular matrix with zero diagonal and $k-1$ zero superdiangonals above.[3]

We can see that for a hierarchical network with n agents, the lowest positioned agent will not be able to take a strategic effort since $G^n = \mathbf{0}$. the following example illustrates how this iterative procedure works:

Example 2. Consider a hierarchical network with the adjacency matrix $G = \begin{pmatrix} 0 & g_{12} & g_{13} \\ 0 & 0 & g_{23} \\ 0 & 0 & 0 \end{pmatrix}$ where we know $G^2 = \begin{pmatrix} 0 & 0 & g_{12}g_{23} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and $G^k = 0$ for $k \geq 3$. For the scenario where each agent is aware of two hops, we can write (assuming $q_i > 0\,,\, \forall i$):

$$x^*_{3_{(2)}} = q_3 \tag{13}$$

$$x^*_{2_{(2)}} = \max\{0, q_2 - g_{23}q_3\} \tag{14}$$

$$x^*_{1_{(2)}} = \max\{0, q_1 - g_{12}x^*_{2_{(2)}} - (g_{13} + g_{12}g_{23})q_3\} \tag{15}$$

As seen in these equations, we can start from the lowest nodes to find the equilibrium for these types of networks. For tree graphs, this model is equivalent to each agent considering the whole branch below them and not being aware of the branches above or parallel. Starting from the lowest nodes, we can find their equilibrium effort independently from other nodes (13), then we move to the nodes in the higher branches (14), and (15) until we know all the efforts in the network.

The numerical experiments for DAGs are more intriguing than previous cases. For these networks, we increased the number of agents to 10 and the range of edge weights to $(-2.5, 2.5)$. With these changes, we see that, as expected, all cases will converge. Even though this is not guaranteed for DAGs, all the random cases have higher game quality than the no awareness scenario. Also, the damping rate fluctuations in Figure 4 depend on the edge weights; if the edge weights are large, then they can continue on as many hops as there are agents; however, the fluctuations will definitely end since there exists a k for which $G^k = 0$.

[3] We can write the elements of the second power of A as $[A^2]_{ij} = \sum_k a_{ik}a_{kj}$. Given $a_{i\cdot} = [0, 0, ..., 0, a_{i,i+1}, ..., a_{in}]$ and $a^T_{\cdot j} = [a_{1j}, ..., a_{j-1,j}, 0, 0, ..., 0]$ we can easily see for $j = i+1$ we have $[A^2]_{ij} = 0$ since the first i elements of $a_{i\cdot}$ are zero and the last $n - j + 1 = n - i$ elements of $a_{\cdot j}$ are zero, similarly for $j < i + 1$. We can continue this process for higher powers of A and show the results.

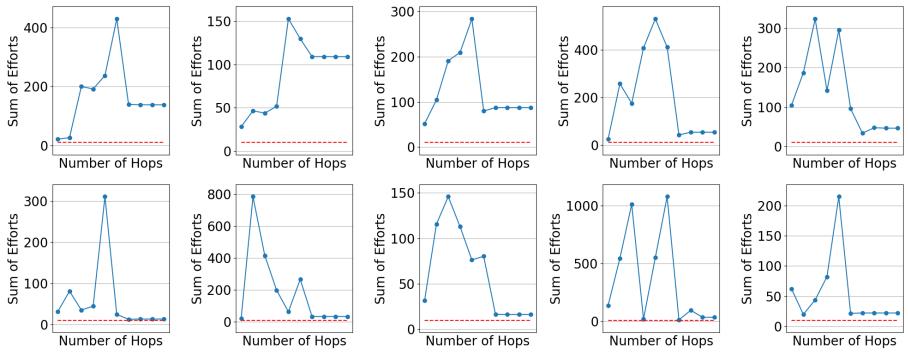


Fig. 4: Game quality comparison for 10 randomly generated DAGs with 10 K-hop aware agents (K from 1 to 10) with the no awareness case (dashed red line).

5 Conclusion

In this study, we extend the traditional framework of network security games by introducing K-hop network games, where agents possess extended awareness of risk spillovers up to K hops away. Our analysis highlights several key findings:

We demonstrate that agents' strategic security decisions and equilibrium behaviors are significantly influenced by their level of awareness. Increasing awareness results in changes in optimal effort levels, contingent upon the network structure and the nature of dependencies (complements vs. substitutes). In strategic substitutes games, agents with higher awareness can lower their efforts and increase free-riding, particularly if they are aware of agents with positive efforts within their extended network. In strategic complements games, the benefits of increased awareness from one-hop to two-hop are bounded, with efforts potentially decreasing for two-hop awareness but not leading to increased efforts compared to one-hop awareness scenario. Our examination of specific network structures shows varied impacts of increased awareness on agents' efforts. In one-way cycles, we analytically showed that efforts can oscillate with awareness levels, while in star networks, due to two-hop awareness, central agents can free-ride more compared to one-hop awareness. In hierarchical DAGs, agents' efforts are determined iteratively from the lowest to the highest nodes. Our numerical experiments indicate that the overall game quality, measured by the sum of agents' efforts, can both improve and deteriorate with increased awareness. The extent and direction of this change depend on network structure and edge weights.

In conclusion, extended awareness in network security games enables agents to optimize their security investments more effectively, but also exposes potential pitfalls for less aware agents. These insights can inform better policies and resource allocation strategies, emphasizing the necessity for sophisticated awareness in managing K-hop risk dependencies.

Future research can expand on these findings by exploring more complex and dynamic network structures, where agents' awareness levels may change over time. Further studies could also consider the impact of partial or evolving awareness, where agents gradually gain or lose information about their network environment. These extensions would enhance our understanding of strategic interactions in networks and contribute to the development of more robust models for predicting and optimizing agents' efforts in various domains.

Acknowledgments. This work is supported in part by the NSF under award CCF-2416311

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Abdallah, M., Naghizadeh, P., Hota, A.R., Cason, T., Bagchi, S., Sundaram, S.: Behavioral and game-theoretic security investments in interdependent systems modeled by attack graphs. IEEE Transactions on Control of Network Systems **7**(4), 1585–1596 (2020). https://doi.org/10.1109/TCNS.2020.2988007
2. Beerman, J., Berent, D., Falter, Z., Bhunia, S.: A review of colonial pipeline ransomware attack. In: 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW). pp. 8–15 (2023). https://doi.org/10.1109/CCGridW59191.2023.00017
3. Bramoullé, Y., Kranton, R., D'amours, M.: Strategic interaction and networks. American Economic Review **104**(3), 898–930 (2014)
4. Brown, S., Gommers, J., Serrano, O.: From cyber security information sharing to threat management. In: Proceedings of the 2nd ACM workshop on information sharing and collaborative security. pp. 43–49 (2015)
5. Do, C.T., Tran, N.H., Hong, C., Kamhoua, C.A., Kwiat, K.A., Blasch, E., Ren, S., Pissinou, N., Iyengar, S.S.: Game theory for cyber security and privacy. ACM Comput. Surv. **50**(2) (may 2017). https://doi.org/10.1145/3057268, https://doi.org/10.1145/3057268
6. Ebrahimi, R., Naghizadeh, P.: United we fall: On the nash equilibria of multiplex and multilayer network games (2024)
7. Ettredge, M.L., Richardson, V.J.: Information transfer among internet firms: the case of hacker attacks. Journal of Information Systems **17**(2), 71–82 (2003)
8. Fischer, E.A., Liu, E.C., Rollins, J., Theohary, C.A.: The 2013 cybersecurity executive order: Overview and considerations for congress. Congressional Research Service Washington (2013)
9. Hinz, O., Nofer, M., Schiereck, D., Trillig, J.: The influence of data theft on the share prices and systematic risk of consumer electronics companies. Information & Management **52**(3), 337–347 (2015)
10. Jeong, C.Y., Lee, S.Y.T., Lim, J.H.: Information security breaches and it security investments: Impacts on competitors. Information & Management **56**(5), 681–695 (2019). https://doi.org/https://doi.org/10.1016/j.im.2018.11.003, https://www.sciencedirect.com/science/article/pii/S037872061830435X

11. Jiang, L., Anantharam, V., Walrand, J.: How bad are selfish investments in network security? IEEE/ACM Transactions on Networking **19**(2), 549–560 (2011). https://doi.org/10.1109/TNET.2010.2071397
12. Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C., et al.: Guide to cyber threat information sharing. NIST special publication **800**(150), 35 (2016)
13. Kiennert, C., Ismail, Z., Debar, H., Leneutre, J.: A survey on game-theoretic approaches for intrusion detection and response optimization. ACM Comput. Surv. **51**(5) (aug 2018). https://doi.org/10.1145/3232848, https://doi.org/10.1145/3232848
14. Klingberg, T.: Limitations in information processing in the human brain: neuroimaging of dual task performance and working memory tasks. In: Cognition, emotion and autonomic responses: The integrative role of the prefrontal cortex and limbic structures, Progress in Brain Research, vol. 126, pp. 95–102. Elsevier (2000). https://doi.org/https://doi.org/10.1016/S0079-6123(00)26009-3, https://www.sciencedirect.com/science/article/pii/S0079612300260093
15. Lallie, H.S., Debattista, K., Bal, J.: A review of attack graph and attack tree visual syntax in cyber security. Computer Science Review **35**, 100219 (2020). https://doi.org/https://doi.org/10.1016/j.cosrev.2019.100219, https://www.sciencedirect.com/science/article/pii/S1574013719300772
16. Laszka, A., Felegyhazi, M., Buttyán, L.: A survey of interdependent information security games. ACM Computing Surveys (CSUR) **47**(2), 1–38 (2014)
17. Liang, X., Xiao, Y.: Game theory for network security. IEEE Communications Surveys & Tutorials **15**(1), 472–486 (2013). https://doi.org/10.1109/SURV.2012.062612.00056
18. Manshaei, M.H., Zhu, Q., Alpcan, T., Bacşar, T., Hubaux, J.P.: Game theory meets network security and privacy. ACM Comput. Surv. **45**(3) (jul 2013). https://doi.org/10.1145/2480741.2480742, https://doi.org/10.1145/2480741.2480742
19. Miura-Ko, R.A., Yolken, B., Mitchell, J., Bambos, N.: Security decision-making among interdependent organizations. In: the 21st IEEE Computer Security Foundations Symposium. pp. 66–80. IEEE (2008)
20. Naghizadeh, P., Liu, M.: Provision of public goods on networks: on existence, uniqueness, and centralities. IEEE Transactions on Network Science and Engineering **5**(3), 225–236 (2018)
21. Osborne, C.: Updated kaseya ransomware attack faq: What we know now (2021), https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/
22. Parise, F., Ozdaglar, A.: A variational inequality framework for network games: Existence, uniqueness, convergence and sensitivity analysis. Games and Economic Behavior **114**, 47–82 (2019). https://doi.org/https://doi.org/10.1016/j.geb.2018.11.012, https://www.sciencedirect.com/science/article/pii/S0899825618301891
23. Paul, K.: Who's behind the kaseya ransomware attack–and why is it so dangerous? (2021), https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers.
24. Qi, Y., Gu, Z., Li, A., Zhang, X., Shafiq, M., Mei, Y., Lin, K.: Cybersecurity knowledge graph enabled attack chain detection for cyber-physical systems. Computers and Electrical Engineering **108**, 108660 (2023). https://doi.org/https://doi.org/10.1016/j.compeleceng.2023.108660, https://www.sciencedirect.com/science/article/pii/S004579062300085X
25. Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., Wu, Q.: A survey of game theory as applied to network security. In: 2010 43rd Hawaii International

Conference on System Sciences. pp. 1–10 (2010). https://doi.org/10.1109/HICSS.2010.35

26. Sanjab, A., Saad, W., Başar, T.: Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game. In: 2017 IEEE International Conference on Communications (ICC). pp. 1–6 (2017). https://doi.org/10.1109/ICC.2017.7996862
27. Shandilya, V., Simmons, C.B., Shiva, S.: Use of attack graphs in security systems. Journal of Computer Networks and Communications **2014**(1), 818957 (2014)
28. Smith, J.C., Song, Y.: A survey of network interdiction models and algorithms. European Journal of Operational Research **283**(3), 797–811 (2020). https://doi.org/https://doi.org/10.1016/j.ejor.2019.06.024, https://www.sciencedirect.com/science/article/pii/S0377221719305156
29. Sreekumaran, H., Hota, A.R., Liu, A.L., Uhan, N.A., Sundaram, S.: Multi-agent decentralized network interdiction games. arXiv preprint arXiv:1503.01100 (2015)
30. Stewart, G.W.: Matrix Algorithms. Society for Industrial and Applied Mathematics (1998). https://doi.org/10.1137/1.9781611971408, https://epubs.siam.org/doi/abs/10.1137/1.9781611971408
31. Thakoor, O., Jabbari, S., Aggarwal, P., Gonzalez, C., Tambe, M., Vayanos, P.: Exploiting bounded rationality in risk-based cyber camouflage games. In: Zhu, Q., Baras, J.S., Poovendran, R., Chen, J. (eds.) Decision and Game Theory for Security. pp. 103–124. Springer International Publishing, Cham (2020)
32. Varian, H.: System reliability and free riding. In: Economics of information security, pp. 1–15. Springer (2004)
33. Wang, L., Singhal, A., Jajodia, S.: Measuring the overall security of network configurations using attack graphs. In: Barker, S., Ahn, G.J. (eds.) Data and Applications Security XXI. pp. 98–112. Springer Berlin Heidelberg, Berlin, Heidelberg (2007)
34. Wang, T., Wang, Y.Y., Yen, J.C.: It's not my fault: The transfer of information security breach information. Journal of Database Management **30**, 18–37 (07 2019). https://doi.org/10.4018/JDM.2019070102
35. Yang, R., Kiekintveld, C., Ordonez, F., Tambe, M., John, R.: Improving resource allocation strategy against human adversaries in security games. In: IJCAI Proceedings-International Joint Conference on Artificial Intelligence. vol. 22, p. 458. Barcelona (2011)
36. Young, N.: The rate of convergence of a matrix power series. Linear Algebra and its Applications **35**, 261–278 (1981). https://doi.org/https://doi.org/10.1016/0024-3795(81)90278-0, https://www.sciencedirect.com/science/article/pii/0024379581902780
37. Zegura, E., Calvert, K., Donahoo, M.: A quantitative comparison of graph-based models for internet topology. IEEE/ACM Transactions on Networking **5**(6), 770–783 (1997). https://doi.org/10.1109/90.650138