Proceedings of the 2025 Winter Simulation Conference
E. Azar, A. Djanatliev, A. Harper, C. Kogler, and V. Ramamohan, eds.

A FORMAL AND DEPLOYABLE GAMING OPERATION TO DEFEND IT/OT NETWORKS

Ranjan Pal[1], Lillian Bluestein[2], Tilek Askerbekov[3], and Michael Siegel[1]

[1]MIT Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA, USA
[2]Department of EECS, Massachusetts Institute of Technology, Cambridge, MA, USA
[3]Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, USA

ABSTRACT

The cyber vulnerability terrain is largely amplified in critical infrastructure systems (CISs) that attract exploitative (nation-state) adversaries. This terrain is layered over an IT and IoT-driven operational technology (OT) network that supports CIS software applications and underlying protocol communications. Usually, the network is too large for both cyber adversaries and defenders to control every network resource under budget constraints. Hence, both sides strategically want to target 'crown jewels' (i.e., critical network resources) as points of control in the IT/OT network. Going against traditional CIS game theory literature that idealistically (impractically) model attacker-defense interactions, we are the first to formally model real-world adversary-defender strategic interactions in CIS networks as a simultaneous non-cooperative network game with an auction contest success function (CSF) to derive the optimal defender strategy at Nash equilibria. We compare theoretical game insights with those from large-scale Monte Carlo game simulations and propose CIS-managerial cyber defense action items.

1 INTRODUCTION

The modern critical infrastructure systems (CISs) such as an electric power grid, and a manufacturing planet are equipped with IT and IoT/CPS driven operational technology (OT) to promote increasingly proactive and data-driven approach to managing industrial operations. The primary (overlapping) benefits for CIS management to invest in such technology include: (a) real-time monitoring, response, and (automated) decision control of industrial and business processes, (b) improved operational visibility and asset tracking complementing remote work environments, (c) predictive sensor data driven maintenance to improve system reliability and equipment/process quality control, (d) data-driven energy optimization for reduced business operation costs, and (e) improved environmental, operational, and equipment safety to mitigate hazard externality and physical damage to people and equipments. It is not surprising then that the global IoT/CPS driven CIS market is projected (by *Statista*) to reach USD 275 billion by 2025, and to USD 450 billion by 2029 at a high CAGR of around 13.5%.

1.1 Cybersecurity Challenges in CISs

While on one hand, the IT and OT technology convergence brings in a large number of systems management benefits, it opens up a huge cyber vulnerability terrain spanned by hundreds and thousands of sensor and actuator devices. More specifically, large and complex (distributed) communication networks formed by sensor/actuator equipped CIS physical equipment have multiple critical vulnerable points in them. Research in applied computer science theory on systems networks have shown that in the worst case it is computationally infeasible to decipher all these critical points within practical time constraints (Pal et al. 2023; Pfleeger and Cunningham 2010; Pal et al. 2021; Pal et al. 2024). Add to this, budget constrained CIS managements (Dewri et al. 2007) in general are yet to invest a sufficient amount in cyber protection solutions and processes - partly because of their lack of awareness on cyber (increasing but insufficient) for a relatively new digitally new CIS industry. Moreover, there is a lack of seamless and easy-to-understand

cyber risk KPIs across top-down CIS management to enable the board and upper management to approve increased expenditure on cybersecurity improvement and cyber risk management. As a consequence a CIS is exposed to a considerable exploitation risk of zero-day or other unknown-known vulnerabilities. As examples (Stamp et al. 2009; Ten et al. 2011; Wang et al. 2013), adversaries could exploit such vulnerabilities to (a) gain root access of Human Machine Interface (HMI) devices in smart grid LANs operators to destabilize various aspects and critical parameters of the electrical system, including voltage levels, power flow, and circuit breaker status, (b) launch man-in-the-middle (MiTM) attacks to modify or falsify control data flow on communication links.

1.2 Cyber Risk Management Challenges in CISs

The fundamental requirement for CIS management en route effective and practically deployable cyber risk management (CRM) is to understand the series of sequential steps that adversaries use to launch different types of cyber attacks on ICS infrastructure. Such knowledge is usually obtained (a) from domain experts in the ICS industry, and/or (b) a well documented central database (designed) and maintained by organizations such as MITRE through their popular MITRE ATT&CK for ICS database that is leading database of tactics, techniques, and procedures (TTPs) populated from real-world observations over multiple ICS industries around the USA and the world.

Having gathered such information, an important step for both adversaries and defenders is to identify which resources within a CIS to target and how much budget to expend on them to execute the above-mentioned cyber attacks so as to gain high attack/defense impact in the CIS. This step is a challenge to both the cyber attack and the defense sides of a CIS because they are budget constrained - more so, the defender side. Alternatively, there is no sufficient budget to attack/defend all the possible resources of a CIS, and investing too little a budget to all resources may not serve the purpose in gaining control of the resource. Hence, the important strategic challenge question: *how should cyber risk managers allocate cyber defense (protection) budgets to CIS resources, i.e., the 'crown jewels' so as to maximize cybersecurity within a CIS, given that CIS adversaries will also deploy a similar allocation mindset?*

The answer to this question has implications to cyber risk management in general as it provides (a) a systematic recipe for engineering management of a CIS to spend its cyber protection budget on the most important resources, and (b) a simple quantitative and comparative way for the engineering management of a CIS to communicate with the upper management of to what extent different resource allocation strategies (i.e., strategic versus non-strategic) translate to business KPI in cyber adversarial environments, (c) a contribution to a more streamlined system-dependent (in contrast to being general) questionnaire (when compared to the status quo) cyber insurance companies provide their (potential) clients before deciding on coverage/pricing contractual parameters for CIS cyber risk management (CRM).

1.3 Research Motivation and Contributions

In this section we state our research motivation and lay down our contributions.

Research Motivation - Resource prioritization to make CIS more cyber resilient is not new in the practical industry. It is common knowledge from IT/OT consulting leaders such as *Dragos* that 'crown jewels' prioritization for improved cyber defense is popular in modern critical infrastructure settings. However, even for such systems the challenge is to ensure that cyber defense (protection) investments are apt, specifically in the presence of adversarial strategies - the logic behind such aptness has not been documented in industry reports. Alternatively, it is common knowledge that IT/OT cyber risk managers will protect certain critical CIS resources, but so will the adversaries. *What is not clear is how does such a 'fist fight' between a defender and an adversary over CIS resources drive the optimal defender investments in cyber defense? - after all one could defend certain resources, but could be out-defended on the same resources by adversaries.* In addition, in existing IT/OT cybersecurity literature the above-mentioned aptness logic has not been exhibited over the cyber vulnerability terrain that is layered over

an IT and operational technology (OT) network that supports CIS software applications and underlying protocol communications. In other words, *how does an underlying CIS network topology play a role in the amount of cyber defense investments under adversarial settings? It is evident that successfully defending certain topologically 'important' nodes will have a variable, non-linear, and non-monotonic effect on the overall cybersecurity of the network, when compared to some other network nodes.* **In this paper, we are motivated to answer these two questions.**

Research Contributions - We make the following research contributions in the paper.

- We propose a simultaneous, non-cooperative, and single shot adversary-defender game over an IT/OT CIS network topology where we assume that (a) the adversary is able to get sufficient leverage even if it successfully compromises one node in the network - such a scenario is common to malware-driven cyber attacks on critical infrastructure (e.g., ICSs) where a single-node compromise (e.g., such as in the *Colonial Pipeline* cyber incident of 2021) is enough to cause significant business service disruptions over time, and (b) the defender is interested to protect all nodes in the network - however may not have sufficient budget to protect all the nodes with success (i.e., an adversary might win control in a node battle despite a defender investing in cyber protection on the same node). The game is modeled over the practically realistic auction *contest success function* (CSF) that determines (as a function of adversary-defender investments on nodes) whether the adversary or the defender wins control over any network node (see Section 3).
- We analyse our proposed game in theory to derive and understand the Nash equilibria with respect to the amount of cyber defense investments on network nodes. Our closed form analysis on arbitrary network topologies (applicable on networks with no K_4 subgraph embeddings) reveals that the optimal and single cyber attack strategy at a mixed strategy Nash equilibria (that always exist for any non-cooperative game with closed and bounded strategy spaces) is always to spend resources on a single network node - except that this node is unknown to the defender and randomizes with the attacker (due to the mixed nature of Nash equilibria), and the defender needs to distribute its cyber protection (defense) resources to all nodes in the network. This type of game representing a randomized guerilla warfare strategy outcome is very practical based on multiple studies by the authors on how adversaries compromise CISs (see Section 4).
- The analysis in Section 4 showcases the insight on what is the best strategy for the adversary and defender in the game of CIS network control - however it does not state the impact of the network type and the player strategies on the degree of network cybersecurity. In Section 5, we design an extensive Monte Carlo simulation framework to understand how attacker and defender strategies in tandem affect the cybersecurity strength of a CIS IT/OT network that is defined as the number of network nodes that are compromised in an adversary-defender contest of control over the network. We assume (based on inputs from industry reports and personnel) that the randomized guerilla warfare strategy as the Nash equilibrium attacker strategy is spread across a few central nodes, i.e., 'crown jewels', of the CIS network, and the defender allocates its budget to a (overlapping) subset of central nodes of the CIS network. We study the influence of (a) the CIS network topology and (b) attack-defense investments on central network nodes, on network cybersecurity, and draw action items for CIS managers for effective strategic cyber defense (see Section 5).

We discuss related work in Section 2 and summarize our paper in Section 6.

2 RELATED WORK

In this section we briefly discuss existing work related to the game-theoretic setting in our research: (i) type of the non-cooperative network game fitting our CIS cybersecurity environment, (ii) sequence of game play between the players of the CIS network game, and (iii) decision logic on how control over a network node can be won by a player.

Type of Non-Cooperative Network Game - We start with emphasizing that the adversary-defender game on CIS networks is not an interdependent security game on networks, for which there is a huge amount of literature available (Laszka et al. 2014). In such games, each network node is a player whose selfish non-cooperative motive to invest in its own cyber protection influences such investments of other interdependent players in the network and the cybersecurity of the entire network. *In contrast, in our research the CIS network is owned by a single enterprise (player) and is the target of an adversary, i.e., our research deals with a two-player game, unlike that in an interdependent network security game*. In our game, each player aims to gain control over some (or all) nodes of the network. Such games have been modeled for critical infrastructure in the form of *Blotto* games, that have appeared in (Dziubiński 2013; Hart 2008; Macdonell and Mastronardi 2015; Roberson 2006; Thomas 2018; Weinstein 2012). These games aptly model the budget constraints of the two players on attack/defense investments in system resources - *however, unlike this work, they do not model the (CIS) network and its not feasible in cyber space to know budget of one player in practice by the other.*

Sequence of Play - Even for such two-player games, it is often the case that academic models in CIS networks (and in general overall) represent the adversary-defender interactions as a sequential game, where the defender (leader) moves first with the intention to maximize cyber protection, and the attacker (follower) moves second to maximize the damage atop this defender move. This results in the sequential game being formalized as a multi-level mathematical optimization problem (Arroyo and Galiana 2005; Salmeron et al. 2009; Yao et al. 2007; Acemoglu et al. 2016; Goyal and Vigier 2014; Pal and Prasanna 2016). *In our opinion this is an highly idealized setting for CISs, with no empirical or corporate evidence that cyber adversaries want to maximize damage and defenders want to minimize damage (as their intention).* Moreover, sequential two-player games in cyber settings are ones with incomplete and imperfect information, and (approximably) optimizing player strategies in such games is computationally intractable as the network scale grows (Daskalakis et al. 2009; Daskalakis 2013; Daskalakis and Papadimitriou 2015). *Hence, it is not even clear that the outcome of trying to solve such computationally difficult problems in informationally uncertain adversarial CIS environments is useful enough when compared to the resource cost needed to solve such problems.* Finally, and most importantly, based on multiple industry reports and communication with industry, this is not the way CIS defenders are strategically protecting their IT/OT networks. In practice, defender strategy (led by an enterprise cyber risk management team) strategically invests in cyber defense of certain 'crown jewels' in the CIS network whose information is incomplete to the adversary, and the latter having some CIS environment knowledge (e.g., when adversary is launching an APT attack) decides to attack an overlapping set of such 'crown jewels', whose knowledge is incomplete to the defender. This sequence repeats in rounds with feedback. In this paper we study a single game round.

Decision Logic of Player Node Control - Auction based node control has typically been one popular method of deciding resource (node) control among players of an attack-defense game. Winner-pay, chopstick-pay, and all-pay auctions for such a decision task has been proposed in (Ewerhart 2017; Ewerhart 2022; Szentes and Rosenthal 2003a; Szentes and Rosenthal 2003b; Siegel 2009). The auction winning success functions, popularly known as contest success functions (CSFs) are either deterministic or randomized. In the deterministic case, a player wins control of a resource (node) if its investments are greater than that of the opponent (Kovenock and Roberson 2018). In the randomized case (Clark and Konrad 2007), a player wins control of a resource (node) with a probability proportional to the ratio between its investment and the sum of the investments of both the players. However, for CIS settings that are equipped mostly with basic cybersecurity measures (according to status quo) it is more reasonable to assume the deterministic CSF (based on communication with corporates in the CIS industry).

3 A REALISTIC CYBER STRATEGIC GAME MODEL FOR CIS NETWORKS

In this section, we propose the setup of a realistic cyber strategic game of control and defense played between a defender of a CIS network and an adversary aiming to get control of certain critical network

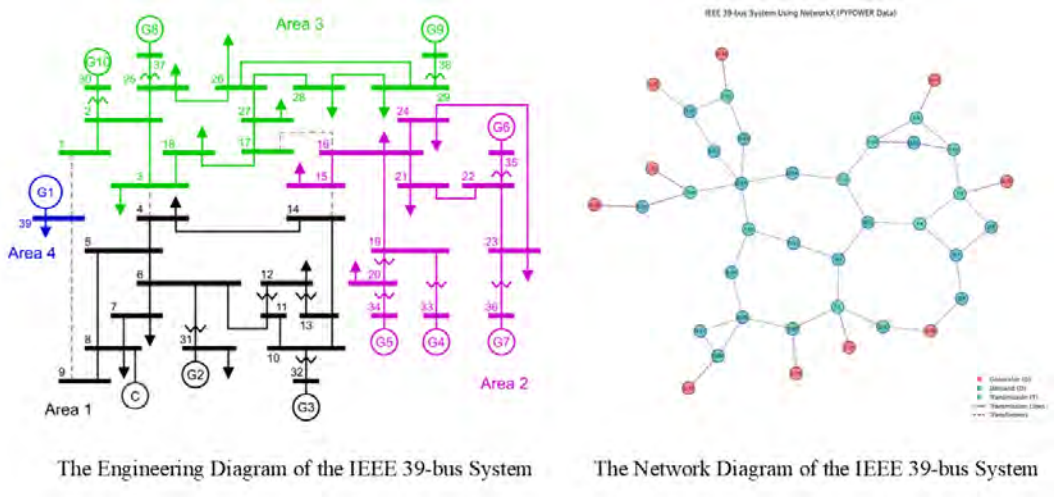

Figure 1: IEEE 39-bus system of New England (left). The IEEE 39-bus network via *pandapower* (right).

resources, i.e., CIS 'crown jewels'. We leave it to Section 4 to analyze the game at a Nash equilibrium to develop practical insights of cost effective and optimal cyber defense of CIS network 'crown jewels'.

The cyber strategic game setup consists of the description of (a) the CIS network structure, (b) the availability of strategic information to the defender and the adversary as applicable in reality, (c) the player utility/payoff functions that adhere to surveyed CIS industry leader inputs on how adversaries and defenders view game payoffs, and (d) the sequence of play between the adversary and the defender of a CIS network.

(a) The CIS Network Structure - We assume a mesh topological structure of an underlying CIS network. An example of a real world mesh network (without loss of generality) for a power grid CIS is shown in Figure 1. This is the standard IEEE 39 bus system that represents a simplified form of the New England power grid. Figure 1a. showcases the engineering diagram of the grid, whereas Figure 1b. is the network structure of the IEEE 39-bus system converted from Figure 1a. using the *pandapower* software that pipes in the IEEE 39-bus system data into the *NetworkX* Python-based software to output the system in an undirected network form.

A strong reason to model a mesh network for analysis as a 'universal' network is that most practical CIS topologies such as the tree and cluster topologies are special instances of a mesh network. In addition, most mesh networks can be decomposed into a series-parallel network structure (that is useful for graphical models to study the degree of network resiliency to component failures akin to flow of electricity in series-parallel circuits) on which our game theory analysis will be based upon in Section 4. A series-parallel network transformation of a given undirected graph G is possible in linear time (in the number of network nodes) via the seminal algorithm by the authors of (Valdes et al. 1979) if G does not have a K_4 clique embedded within it (Hassin and Tamir 1986). Consequently, it is important to know what is the likelihood of a K_4 being embedded in any graph in the family of connected mesh networks. In this paper, we show (as a novel contribution) via the following theorem the probability of a K_4 graph being embedded in any connected undirected graph (that subsumes the family of connected mesh networks) - with a low probability improving the generality of our results in our paper.

Theorem 1 *Given any undirected connected graph $G \in \mathcal{G}_{n,p}$ of n nodes representing a CIS network that is randomly generated using the popular Erdos-Renyi random process (Bollobás and Bollobás 1998) generating family $\mathcal{G}_{n,p}$. The probability that G consists of an embedded K_4 converges to 0 with $n \to \infty$ if $p << n^{-\frac{2}{3}}$; and converges to 1 with $n \to \infty$ if $p >> n^{-\frac{2}{3}}$. Hence $\exists$ threshold $p(n)$ (i.e., a measure of the degree of sparsity) that dictates the existence of a K_4 subgraph in G.*

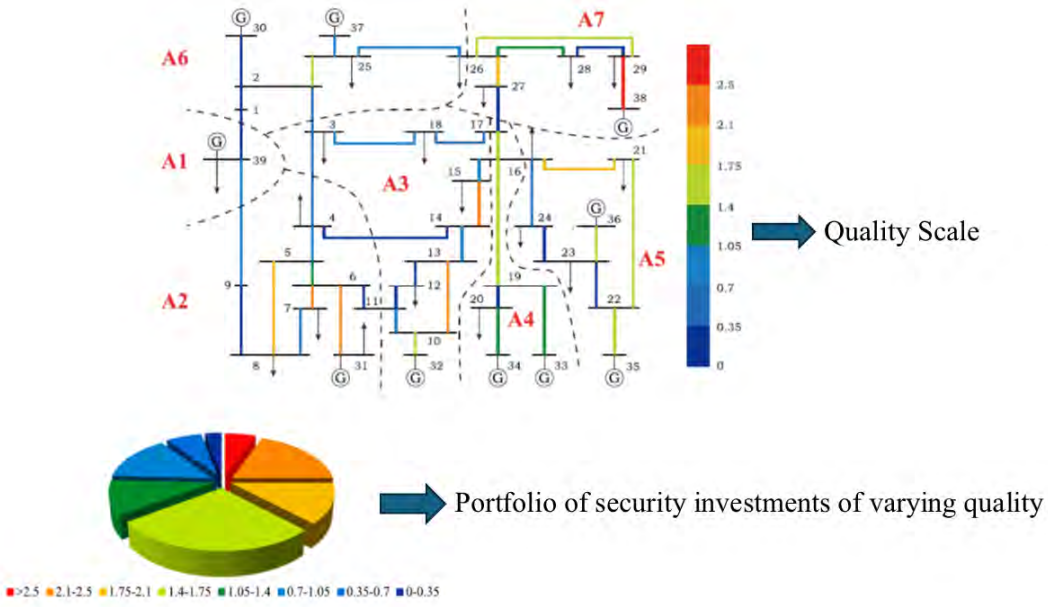

Figure 2: An illustration of a managerial portfolio of security investments on IEEE 39-bus network resources.

Proof Sketch - Define a random variable K = number of instances of K_4 in G and equals $\sum X_C$, where C ranges over the set of all 4-node subgraph of G, and X_C takes value of 1 if all pairs of vertices in C have an edge between them and takes a value 0 otherwise. The case of $p << n^{-\frac{2}{3}}$ is proved via the application of Markov's inequality. The case of $p >> n^{-\frac{2}{3}}$ is proved via applying the Chebyshev's inequality.

Theorem Implications - If a connected CIS network is relatively sparse with respect to the number of nodes (as is shown in Figure 1b) then there is a high likelihood of no K_4 subgraph embeddings in G. Many CIS networks exhibit this structure and hence a series-parallel network analysis suffices as a representative of a mesh network analysis.

(b) The Availability of Strategic Information - We assume the realistic setting where an external adversary has partial information about the CIS network topology. This is obtained, for example, when it launches an APT whose first step is to stealthily penetrate and laterally move inside the CIS network. Hence, the adversary can attack a list of critical network nodes, i.e., 'crown jewels', it perceives to be important. The defender is assumed to have complete view of the CIS network. The adversary does not have prior knowledge of the list of critical network nodes that the defender is going to protect (and vice-versa). However, for theoretical tractability, the players are assumed to know each other's payoff functions, and the range of investments each player makes to gain network resource control. Moreover, the players do not know each other's investment portfolio.

(c) The Player Utility/Payoff Functions - As a pre payoff mention context, the adversary has a portfolio of investments that is used to compromise the nodes of the mesh network by investing from its attack budget and so does the CIS network defender who has its own cyber defense portfolio that it uses in protecting the nodes of the same network (see Figure 2 adopted from industry studies). We assume in this paper that they allocate these investments in proportion to a network centrality metric (e.g., degree centrality, betweenness centrality, eigenvector centrality) that might be different for the adversary and the defender. Section 5 simulates in a Monte Carlo fashion these strategy mappings between the adversary and the defender for multiple graph topology types to derive the preferred strategy for the players that they can adhere to (as an outcome of investment strategy learning) in order to achieve a network game play equilibrium. The question here is: *what is the player payoff structure of this game play?*

We assume a weakest-link and best shot (series-parallel) network setting where the compromise of any resource, i.e., CIS network node, on the path of service from a source node to the destination node renders the path ineffective for service (the weakest-link part of the network). In cyber settings, this holds true as comprising a resource on a path is often enough to compromise the path (e.g., in APTs and DDoS attacks). We take for granted that any input undirected CIS network is first transformed into a series-parallel structure before this path compromise judgment is done. Consequently, for any path $A-B-C$ note that a node B could be a part of parallel sub-network (with all nodes, like B connected to C) where all nodes of that sub-network needs to be compromised in order to render a path from a service source A to the destination C to be ineffective (the best-shot part of the network). This parallel sub-network usually indicates CIS resource redundancy and/or manually operable network components that backup the failure of similar functioning digital components. The series-parallel design of the CIS network promotes resiliency-by-design on part of the network administrator.

We assume, as in practical reality, imperfect attack and defense on part of the adversary and the defender. Our version of imperfectness implies that an investment in a CIS network resource for gaining control does not guarantee control access. A player gains control of a network resource only if its investment on that resource is greater than that of the opponent. While this might not exactly be the case in reality, in scenarios when neither player is knowledgeable about the other's strategic investment amount it is prudent to be investing with the belief that more is better (a point endorsed by some CIS industry leaders). Moreover, often times in cyber settings that certain perceived critical network targets demand more control resources of the adversary and the defender. This is because critical resources are exposed to measures such as greater access control, being part of IT/OT segmented (virtual) networks, that make control takers invest more maintain/regain control. This is the guerrilla warfare strategy where an adversary tries to focus its efforts on a few important targets that the defender is unaware of (Kovenock and Roberson 2018).

In relation to utility/payoff functions for the players, let us initially define the variable $c^A_{i\in\mathscr{W}} = 1$ (for weakest-link sub-networks I in $\mathscr{W}$) if for sub-network I in a series-parallel network G, the adversary investment $x^A_{I,k}$ on *any* node k of I to gain/maintain control should be greater than $x^D_{I,k}$ - the defender investment on I to gain/maintain control. The value of $c^A_{I\in\mathscr{W}} = 0$, otherwise, i.e., $c^D_{I\in\mathscr{W}} = 1$. Ties are broken in favor of the defender (without loss of generality) if $x^A_{I,k} = x^D_{I,k}$ for any node k of I. Similarly, define the variable $c^A_{I\in\mathscr{B}} = 1$ (for best-shot sub-networks $\mathscr{B}$) if for sub-network I in a series-parallel network G, the adversary investment $x^A_{I,k}$ on *every* node k of I to gain/maintain control should be greater than $x^D_{I,k}$ - the defender investment on I to gain/maintain control. The value of $c^A_{I\in\mathscr{W}} = 0$, otherwise, i.e., $c^D_{I\in\mathscr{B}} = 1$. Ties are broken in favor of the defender (without loss of generality) if $x^A_{I,k} = x^D_{I,k}$ for every node k of I. We re-emphasize here that a sub-network in a series-parallel network is either a series connection of single nodes (the weakest-link reflection), or a parallel network of multiple nodes (the best-shot reflection). The payoff function for adversary A is given as $PF_A(\vec{x}^A,\vec{x}^D) = v_A \max\left(\{c^A_{I\in\mathscr{B}}\},\{c^A_{I\in\mathscr{W}}\}\right) - \sum_J \sum_{k\in|J|} x^A_{J,k}$, where $\mathscr{B}$ is the set of best-shot sub-networks in G; $\mathscr{W}$ is the set of weakest-link sub-networks in G; v_A is the per sub-network payoff if the adversary gains control; and $|J|$ is the number of nodes of sub-network J in G. Alternatively, the payoff function of the defender is $PF_D(\vec{x}^A,\vec{x}^D) = v_D\left(1-\max\left(\{c^A_{I\in\mathscr{B}}\},\{c^A_{I\in\mathscr{W}}\}\right)\right) - \sum_J \sum_{k\in|J|} x^D_{J,k}$, where v_D is the payoff to the defender if it control of all the sub-networks.

(d) The Sequence of Play Between Adversary and Defender - The game between the adversary and defender is one of incomplete information, where only the structure of the payoff function is public knowledge and all other strategic information is private knowledge. In such a scenario, a simultaneous game is equivalent to a sequential game of incomplete information. This is more so the case in realistic CISs where the adversary and defender usually do not continually monitor each other's actions due to lack of sufficient resources (an agenda set by most CIS upper managements who handle cybersecurity budgeting) to monitor the entire network. Hence, we assume a one-shot simultaneous game of network node control between the adversary and the defender adhering with much of reality. In this regard, we assume that in the one-shot game, where each player allocates a portfolio of attack/defense efforts on the various nodes of the CIS network, and a node target is won by the player who invests more in the target.

4 ANALYSIS OF GAME EQUILIBRIA

In this section, we analyze the game equilibria, and draw practical implications of such equilibria. We have the following result on the game equilibria strategies and their payoffs, when the defender (adversary) has a relative effort advantage over the adversary (defender) with respect to a stronger portfolio of effort allocation over the nodes of the CIS network. The proof of the result directly applies from the theory (and we omit it in this paper due to lack of space) in (Kovenock and Roberson 2018) that shows how n-variate investment distributions influence the scale of targets adversaries will invest in, and how much (based on the series-parallel structure of the CIS network). The specific nature of the game equilibria in the presence of a specific structure-dependent (e.g., investment on some central CIS network nodes) player strategy will be discussed in Section 5 with the help of Monte Carlo simulations (as a complement to the theorem result).

Theorem 2 *Let there be a set $I_{j\in\mathscr{B}}$ of best-shot sub-networks j in a CIS network. Similarly, let there be a set set $I_{j\in\mathscr{W}}$ of weakest-link sub-networks j in a CIS network. Let α_D denote the normalized relative effort of the CIS defender on the various best-shot and weakest-link sub-networks. Then, for $\alpha_D \geq 1$, we have the following mixed strategy Nash equilibrium for the adversary:*

$$P_A(\vec{x}^A) = 1 - \frac{1}{\alpha} + \frac{\sum_{j\in\mathscr{W}} \sum_{i\in I_j} x^A_{I_j}}{v_D} + \frac{\sum_{j\in\mathscr{B}} \min_{i\in I_j}\{x^A_{I_j}\}}{v_D},$$

where $\vec{x} \in \prod_{j\in\mathscr{W}}[0, v_A]^{n_j} \times \prod_{j\in\mathscr{B}} \left[0, \frac{v_A}{n_j}\right]^{n_j}$; $n_j | j \in \mathscr{B}$ being the number of best-shot sub-networks, $n_j | j \in \mathscr{W}$ being the number of weakest-link sub-networks, and $\alpha_D = \frac{v_D}{(v_A[\sum_{j\in\mathscr{W}} n_j + \sum_{j\in\mathscr{B}} \frac{1}{n_j}])}$. Under such a mixed strategy Nash equilibrium (there are many for $\vec{x}$ satisfying lying in the domain), the adversary payoff is zero. Similarly, for $\alpha_D \geq 1$, we have the following mixed strategy Nash equilibrium for the defender:

$$P_D(\vec{x}^D) = \sum_{m\in\mathscr{M}_\mathscr{B}} \frac{\min(\{x^D_I\} i \in \cup_{j\in\mathscr{W}} I_j, \{n_j x^D_{I_{j(m)}}\}_{j\in\mathscr{B}}}{v_A \prod_{j\in\mathscr{B}} n_j},$$

where $\mathscr{M}_\mathscr{B}$ is the set of all possible $|\mathscr{B}|$ tuples of best-shot CIS network targets with exactly one target i from each best-shot network $j \in \mathscr{B}$. Under such a mixed strategy Nash equilibrium (there are many for $\vec{x}$ satisfying lying in the domain), the defender payoff is $v_D(1 - \frac{1}{\alpha})$. In the case when $\alpha_D < 1$, we have the following mixed strategy Nash equilibrium for the adversary:

$$P_A(\vec{x}^A) = \frac{\sum_{j\in\mathscr{W}} \sum_{i\in I_j} x^A_{I_j}}{v_D} + \frac{\sum_{j\in\mathscr{B}} \min_{i\in I_j}\{x^A_{I_j}\}}{v_D},$$

where $\vec{x} \in \prod_{j\in\mathscr{W}}[0, v_A]^{n_j} \times \prod_{j\in\mathscr{B}} \left[0, \frac{v_A}{n_j}\right]^{n_j}$; $n_j | j \in \mathscr{B}$ being the number of best-shot sub-networks, $n_j | j \in \mathscr{W}$ being the number of weakest-link sub-networks, and $\alpha_D = \frac{v_D}{(v_A[\sum_{j\in\mathscr{W}} n_j + \sum_{j\in\mathscr{B}} \frac{1}{n_j}])}$. Under such a mixed strategy Nash equilibrium (there are many for $\vec{x}$ satisfying lying in the domain), the adversary payoff is $v_A(1 - \alpha_D)$. Similarly, for $\alpha_D \geq 1$, we have the following mixed strategy Nash equilibrium for the defender:

$$P_D(\vec{x}^D) = 1 - \alpha_D + \sum_{m\in\mathscr{M}_\mathscr{B}} \frac{\min(\{x^D_I\} i \in \cup_{j\in\mathscr{W}} I_j, \{n_j x^D_{I_{j(m)}}\}_{j\in\mathscr{B}}}{v_A \prod_{j\in\mathscr{B}} n_j}.$$

Practical Implications - The theorem states that the Nash equilibrium is not unique, given there is a mixed Nash equilibria for every strategy pair of the defender and the attacker indicating a portfolio of efforts on each node of a CIS network. Non-uniqueness here implies that a multivariate distribution of control investments over nodes is not node-specific, but all such allocation permutations result in the same

expected payoff to the player. For $\alpha_D \geq 1$, the expected payoff to the adversary is a constant zero in all these strategies at the Nash equilibrium. The defender gets a constant non-varying positive expected payoff (increasing in v_D and α_D) at any Nash equilibrium. For $\alpha_D < 1$, the expected payoff to the defender is a constant zero in all these strategies at the Nash equilibrium. The adversary gets a constant non-varying positive expected payoff (increasing in v_A and decreasing in α_D) at any Nash equilibrium. Hence, the defender/adversary only needs to ensure their strategies lie in the domain mentioned in the theorem **(an action item)**, and for every such mixed strategy (invariant of node allocation permutations) the expected payoff is the same. The normalized relative effort of the defender α_D is increasing in the relative valuation of the defender when compared to that of the adversary ($\frac{v_D}{v_A}$), and is decreasing in the size of the number of weakest-link and best-shot sub-networks - this indicating the size of the CIS network increasing the cyber-risk exposure for a limited security investment budget. As **an action item**, defenders should design CIS networks with lower weakest-link sub-networks and higher best-shot sub-networks (therby increasing the cost to compromise for the adversary). Given a defense portfolio by the defender, the rational adversary will focus on control efforts on the most critical (weakest-link) targets, and not invest enough in the other nodes of the CIS network. Such targets structurally map to various graph/network central CIS network nodes - something we will study in detail in Section 5 via Monte Carlo simulations. The analysis of such targets will be of interest to cyber insurance companies. The defender should (as **an action item**) invest more in the security of weakest-link network nodes under a limited security investment budget.

5 SIMULATION EVALUATION

In this section, we simulate a strategic CIS network game to observe the effect of network structure/topology dependent strategies on defense payoffs. The distinction between simulations and proposed theory is that the latter does not model specific graph centrality driven strategies by the players. While the theory shows existence of game equilibria, the simulations microscopically showcases how strategies influenced by network structure impacts equilibria payoffs.

5.1 Simulation Setup

We conduct experiments on (un)weighted graphs to compare how structural connectivity alone influences attack-defense dynamics, as well as how incorporating varying edge strengths and node vulnerabilities impacts strategic outcomes. We ran these simulations on three different (without loss of generality) graph topologies: *Erdos-Renyi* random mesh graphs, star graphs, and tree graphs. All graphs were generated using the *NetworkX* library. Additionally, two lower benchmark control strategies were included (for a comparative purpose): a 0-defense strategy to observe unrestricted attacker behavior and an "unintelligent" defense strategy to compare against more strategic allocations.

Each node in the CIS graph has simulation data structure attributes that track attack/defense status, including attack/defense investment units, centrality values, and whether the node has been attacked or compromised. Heterogeneous defense units practically map to tougher/lighter access control strategies. link segmentations (e.g., links and devices being part of virtual LANs) at application levels, and sophisticated/naive cryptography induced link/node protection solution costs. In weighted graphs, edges are statistically assigned weights representing context that effect the cost of attacks and defenses. As an example tougher access control strategies, link segmentations (e.g., links/devices on virtual LANs) at application levels, and cryptography induced link/node protection solution costs contribute to heterogeneous weights in a CIS graph.

A Monte Carlo simulation approach is used, conducting 1000 iterations per network configuration. The simulations are performed on 500-node graphs, as this size extrapolates effectively to larger network structures while remaining computationally feasible. The purpose of using Monte Carlo simulations is to capture variability in attack and defense outcomes. The attacker budget is fixed at 75 units, while the defense budget is fixed at 35 units (without loss of generality) - usually adversaries are more resourceful than the defenders. These values ensure a competitive dynamic where neither the attacker nor the defender

has an overwhelming advantage, allowing for meaningful strategic analysis. In weighted graphs, the cost of attacking or defending a node is modified to be proportional to its edge weights or aggregated vulnerability score. The attacker must consider the cost-effectiveness of targeting specific nodes, while the defender must allocate resources strategically to high impact resources.

We explore three centrality-based strategies to inform attack and defense behavior in our simulations: - *degree centrality* (in CIS networks, these are nodes with the highest number of connections represent critical access points, such as routers, servers, or influential users in a social network), *betweenness centrality* (in CIS networks such nodes act as key intermediaries in data flow, such as firewalls, gateway servers, or organizational liaisons), and *eigenvector centrality* (in CIS networks such nodes act as high-traffic servers). We also utilized a random non-centrality player strategy in order to represent a less centrality concentrated, baseline security investment approach. The experiments test various combinations of attack and defense strategies, including *degree versus degree*, *betweenness versus betweenness*, *eigenvector versus eigenvector*, and *random versus random*. Cross-strategy pairs (adhering to practical reality), such as *degree versus betweenness* or *eigenvector versus random*, are also explored.

Attack strategies consist of two phases: direct and indirect attacks. In the direct attack phase, the top 5% (without loss of generality and adhering to reality where adversaries usually target atmost 10% of system resources) of highest centrality nodes are attacked first, with each direct attack costing 1 unit per node. Once a node is infiltrated, adjacent nodes are targeted in the indirect attack phase, with each indirect attack costing 0.5 units per node (in adherence to practice where indirect compromises are cheaper). If an attack fails, re-attacking that node is not attempted. In the weighted graphs, direct attacks prioritize nodes with the highest centrality adjusted by weight, and indirect attacks consider edge weights when determining expansion targets. In weighted graphs, defense allocation is prioritized based on the centrality-weight product, and defense cost scales with edge weight, making strategic allocation more critical. The probability of successful node compromise in unweighted graphs varies based on the attack and defense allocations. Direct attacks have a 10% success rate if the node has 1 defense unit and 90% if it has 0 defense units. This is without loss of generality. Indirect attack success rates depend on the defense allocations of both the attacking and target nodes, with probabilities ranging from 25% to 90% (wlog). In weighted graphs, the probability of compromise is proportional to both the node status and edge weights, making certain attack paths more or less viable depending on link strength and node vulnerability.

5.2 Simulation Results Reflecting CIS Management Action Items

Our control strategies validated the experimental setup. The intelligent topology-dependent defense strategies consistently outperformed (see Figures 3(a), 3(d)) both the random and no-defense strategies (by approximately at least 20% and at most 80% respectively in median statistics). This, given that adversaries in practice usually have enough CIS information to target selected critical network nodes; otherwise defender performance on intelligent defense would be significantly higher. The best performance was observed in networks employing intelligent defense, followed by those using the random defense strategy, with the no-defense strategy resulting in the highest level of infiltration. **This confirms that strategic allocation of defense resources is crucial for network security.** Our findings also indicate that strategy selection significantly impacts network resilience. However, attacker infiltration was relatively more influenced by the underlying topology of the network rather than the specific attack-defense strategy pairing in use (see Figures 3(b), 3(e)). The median percentage of the network infiltrated remained consistent across all strategy mappings within a given topology, but it varied significantly between different topologies (see Figures 3(c), 3(f)). Tree topologies showed considerably higher resistance (by around 50%) to malicious CIS network node infiltration when compared to that in star and mesh topologies (in order). Mesh networks have maximum connectivity that renders them vulnerable to higher node compromise counts, whereas star networks are exposed to single points of failure. **This suggests (for CIS managers) that some network structures inherently provide stronger defense mechanisms, regardless of strategic allocation.**

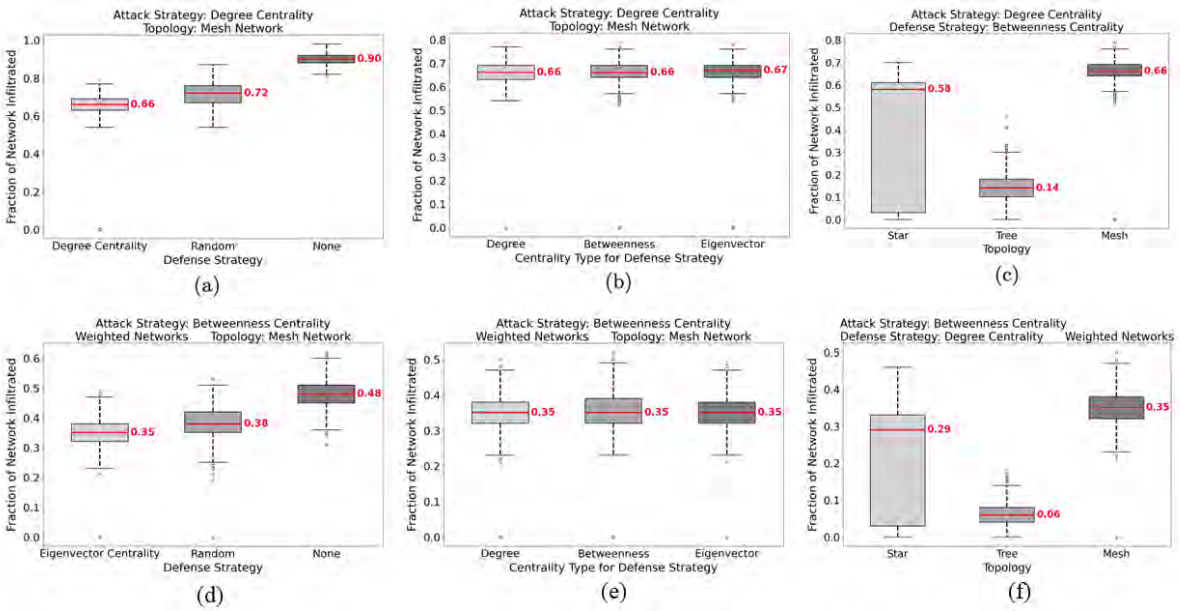

Figure 3: Simulation plots to study strategic topology-driven attack/defense control games in CIS networks.

6 PAPER SUMMARY

In this paper, we are the first to align with real world practice of formally modeling strategic adversarial interaction in a CIS (IT/OT) network as a simultaneous non-cooperative network game with an auction *contest success function* (CSF). We compare theoretical insights from game analysis with those from large-scale Monte Carlo simulations and propose CIS-managerial cyber defense action items. While theory promises an existence of game Nash equilibria, the simulations microscopically showcase how strategies influenced specifically by network structure impacts equilibria payoffs from strategic cyber defense actions.

ACKNOWLEDGEMENT

This study has been supported by funding from Cybersecurity at MIT Sloan (CAMS).

REFERENCES

Acemoglu, D., A. Malekian, and A. Ozdaglar. 2016. "Network security and contagion". *Journal of Economic Theory* 166:536–585.

Arroyo, J. M. and F. D. Galiana. 2005. "On the solution of the bilevel programming formulation of the terrorist threat problem". *IEEE transactions on Power Systems* 20(2):789–797.

Bollobás, B. and B. Bollobás. 1998. *Random graphs*. Springer.

Clark, D. J. and K. A. Konrad. 2007. "Asymmetric conflict: Weakest link against best shot". *Journal of Conflict Resolution* 51(3):457–469.

Daskalakis, C. 2013. "On the complexity of approximating a Nash equilibrium". *ACM Transactions on Algorithms (TALG)* 9(3):1–35.

Daskalakis, C., P. W. Goldberg, and C. H. Papadimitriou. 2009. "The complexity of computing a Nash equilibrium". *Communications of the ACM* 52(2):89–97.

Daskalakis, C. and C. H. Papadimitriou. 2015. "Approximate Nash equilibria in anonymous games". *Journal of Economic Theory* 156:207–245.

Dewri, R., N. Poolsappasit, I. Ray, and D. Whitley. 2007. "Optimal security hardening using multi-objective optimization on attack tree models of networks". In *Proceedings of the 14th ACM conference on Computer and communications security*, 204–213.

Dziubiński, M. 2013. "Non-symmetric discrete General Lotto games". *International Journal of Game Theory* 42:801–833.

Ewerhart, C. 2017. "Contests with small noise and the robustness of the all-pay auction". *Games and Economic Behavior* 105:195–211.

Ewerhart, C. 2022. "A "fractal" solution to the chopstick auction". *Economic Theory* 74(4):1025–1041.
Goyal, S. and A. Vigier. 2014. "Attack, defence, and contagion in networks". *The Review of Economic Studies* 81(4):1518–1542.
Hart, S. 2008. "Discrete colonel blotto and general lotto games". *International Journal of Game Theory* 36(3-4):441–460.
Hassin, R. and A. Tamir. 1986. "Efficient algorithms for optimization and selection on series-parallel graphs". *SIAM Journal on Algebraic Discrete Methods* 7(3):379–389.
Kovenock, D. and B. Roberson. 2018. "The optimal defense of networks of targets". *Economic Inquiry* 56(4):2195–2211.
Laszka, A., M. Felegyhazi, and L. Buttyan. 2014. "A survey of interdependent information security games". *ACM Computing Surveys (CSUR)* 47(2):1–38.
Macdonell, S. T. and N. Mastronardi. 2015. "Waging simple wars: a complete characterization of two-battlefield Blotto equilibria". *Economic Theory* 58(1):183–216.
Pal, R., P. Liu, T. Lu, and E. Hua. 2023. "How Hard is Cyber-Risk Management in IT/OT Systems? A Theory to Classify and Conquer Hardness of Insuring ICSs". *ACM Transactions on Cyber-Physical Systems (TCPS)* 6(4):1–31.
Pal, R., T. Lu, P. Liu, and X. Yin. 2021. "Cyber (re-) insurance policy writing is NP-hard in IoT societies". In *2021 Winter Simulation Conference (WSC)*, 1–12. IEEE.
Pal, R. and V. Prasanna. 2016. "The STREAM mechanism for CPS security the case of the smart grid". *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 36(4):537–550.
Pal, R., R. Sequeira, and S. Zeijlemaker. 2024. "How Hard is it to Estimate Systemic Enterprise Cyber-Risk?". In *2024 Winter Simulation Conference (WSC)*.
Pfleeger, S. and R. Cunningham. 2010. "Why measuring security is hard". *IEEE Security & Privacy* 8(4):46–54.
Roberson, B. 2006. "The colonel blotto game". *Economic Theory* 29(1):1–24.
Salmeron, J., K. Wood, and R. Baldick. 2009. "Worst-case interdiction analysis of large-scale electric power grids". *IEEE Transactions on power systems* 24(1):96–104.
Siegel, R. 2009. "All-pay contests". *Econometrica* 77(1):71–92.
Stamp, J., A. McIntyre, and B. Ricardson. 2009. "Reliability impacts from cyber attack on electric power systems". In *2009 IEEE/PES Power Systems Conference and Exposition*, 1–8. IEEE.
Szentes, B. and R. W. Rosenthal. 2003a. "Beyond chopsticks: Symmetric equilibria in majority auction games". *Games and Economic Behavior* 45(2):278–295.
Szentes, B. and R. W. Rosenthal. 2003b. "Three-object two-bidder simultaneous auctions: chopsticks and tetrahedra". *Games and Economic Behavior* 44(1):114–133.
Ten, C.-W., J. Hong, and C.-C. Liu. 2011. "Anomaly detection for cybersecurity of the substations". *IEEE Transactions on Smart Grid* 2(4):865–873.
Thomas, C. 2018. "N-dimensional Blotto game with heterogeneous battlefield values". *Economic Theory* 65(3):509–544.
Valdes, J., R. E. Tarjan, and E. L. Lawler. 1979. "The recognition of series parallel digraphs". In *Proceedings of the eleventh annual ACM symposium on Theory of computing*, 1–12.
Wang, L., S. Jajodia, A. Singhal, P. Cheng and S. Noel. 2013. "k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities". *IEEE Transactions on Dependable and Secure Computing* 11(1):30–44.
Weinstein, J. 2012. "Two notes on the Blotto game". *The BE Journal of Theoretical Economics* 12(1):000010151519351704 1893.
Yao, Y., T. Edmunds, D. Papageorgiou, and R. Alvarez. 2007. "Trilevel optimization in power network defense". *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 37(4):712–718.

AUTHOR BIOGRAPHIES

RANJAN PAL is a Research Scientist with the MIT Sloan School of Management, and an invited working group member of the World Economic Forum. His primary research interests lie in cyber risk and resilience management using interdisciplinary methods. He serves as an Associate Editor of the ACM Transactions on MIS. His email address is ranjanp@mit.edu.

LILLIAN BLUESTEIN is a student in the EECS department at MIT. She is also a researcher with Cybersecurity at MIT Sloan (CAMS) at the MIT Sloan School of Management. Her primary research interest lies in strategic cyber risk management using game theory for critical infrastructures and business networks. Her email address is lillianb@mit.edu.

TILEK ASKERBEKOV is a student in the Mathematics department at MIT, and an International Mathematical Olympiad (IMO) awardee. He is also a researcher with Cybersecurity at MIT Sloan (CAMS) at the MIT Sloan School of Management, contributing his expertise in graph theory to boost critical infrastructure cybersecurity. His email address is tilekmit@mit.edu.

MICHAEL SIEGEL is a Principal Research Scientist with the MIT Sloan School of Management. His primary research interest lies in cybersecurity management of information systems. He is the founding co-Director of the Cybersecurity at MIT Sloan (CAMS) center within the MIT Sloan School of Management. His email is msiegel@mit.edu.