Preventive-Reactive Defense Tradeoffs in Resource Allocation Contests

Keith Paarporn, *Member, IEEE*, Shouhuai Xu, *Senior Member, IEEE*

***Abstract*— The connectivity enabled by modern computer networking technologies introduces vulnerabilities to adversarial attacks. Although it is ideal to be able to prevent all possible cyber attacks, this is not possible or feasible in practice and society must accept that attacks are inevitable. While many works study optimal security policies to minimize the chance of successful attacks, there are many unexplored territories. In this letter, we formulate and investigate a new problem, namely the tradeoff between the effort or resource that should be spent on preventing attacks (i.e., *preventive* defense) and the effort or resource that should be spent on recovering from attacks (i.e., *reactive* defense). We formulate the problem as a resource allocation game between the defender and the attacker, where they decide how to allocate resources to defend and attack a set nodes (e.g., computers), respectively. The game unfolds in two phases. (i) Allocate preventive resources to reduce the probabilities that the nodes are successfully compromised by the attacker. (ii) The compromised nodes undergo a recovery process, which can be sped up with the allocation of more reactive defense resources. Our results completely characterize the Nash equilibria of this game, revealing the defender's optimal allocation of preventive versus reactive resources.**

***Index Terms*— Game theory, Optimization, Agents-based systems, Stochastic systems**

I. Introduction

THE scale and connectivity of modern networked infrastructures introduces vulnerabilities that can be exploited by malicious entities. In particular, the security of computer networks is a persistent concern, despite tremendous advancements in cybersecurity mechanisms such as cryptosystems, intrusion detection systems, and firewalls. Indeed, cyber attacks cannot be completely prevented for reasons that include undecidability (e.g., there is no universal method or tool that can determine whether any piece of code is malicious or not) [1] and human factors [2].

In principle, it would be ideal to prevent as many attacks from succeeding as possible by employing *preventive* defense mechanisms, such as access control and firewalls. However, this can incur prohibitively high costs to an infrastructure's operator and inconveniences to users (e.g., every Internet access is thoroughly vetted). A complementary approach is to employ *reactive* defenses, in addition to preventive defenses, to recover systems from compromised states to secure states. The intuition is that some attacks are too costly to prevent from happening in the first place, and it may be more cost-effective to tolerate their occurrence and deal with their compromises afterwards. This naturally leads to a tradeoff between the amount of effort that should be spent on preventive defense and the effort that should be spent on reactive defense. Understanding this tradeoff is currently under-developed, as there have been numerous calls to incorporate these two security aspects in a single decision-making paradigm [3]–[9].

In this letter, we investigate preventive-reactive defense tradeoffs by appealing to *contest theory*, which studies competitive resource allocation with a variety of model formulations [10], [11]. In its basic form, players compete over a set of valuable items by allocating their limited resources to them. Some of these variations, such as the well-known *Colonel Blotto game* and *Tullock contest*, have recently been applied to numerous problems relating to cybersecurity [12]–[14], wireless communications [15], and network security [16]–[22]. These works leverage this flexible framework to generate specific insights regarding optimal resource allocation decisions for defenders. However, they primarily focus on strategies that maximize prevention, and neglect to consider how resources should be employed to improve reactive mechanisms in the event that an attack successfully bypasses the preventive measures.

We formulate a resource allocation contest between a defender and an attacker. The main question we seek to address is: *what amount of the total resource budget should the defender devote to preventive versus reactive security?* To draw insights into this question, we consider two distinct temporal phases. In phase 1, the attacker wages attacks against the defender's nodes (e.g., computers), where the attack success on each node is probabilistic and depends on the defender's allocation of preventive resources. In phase 2, the compromised nodes undergo a recovery process, which can be sped up with the allocation of more reactive resources. The defender's objective is to choose a policy for allocating preventive and reactive resources so as to minimize the total expected time the nodes spend in compromised states; the attacker's objective is to maximize it.

To the best of our knowledge, the inclusion of a reactive phase is novel to the theoretic formulation of contests. The main contribution of this letter is the characterization of the optimal amount of resources that the defender invests in preventive and reactive phases. In doing so, we also provide the optimal (i.e., equilibrium) resource allocations among the

The authors are with the Department of Computer Science at University of Colorado, Colorado Springs, CO 80918 USA. Contact: {kpaarpor,sxu}@uccs.edu.

This work is supported in part by NSF grants #ECCS-2346791 and #2115134 as well as a DoD/UC2 grant.

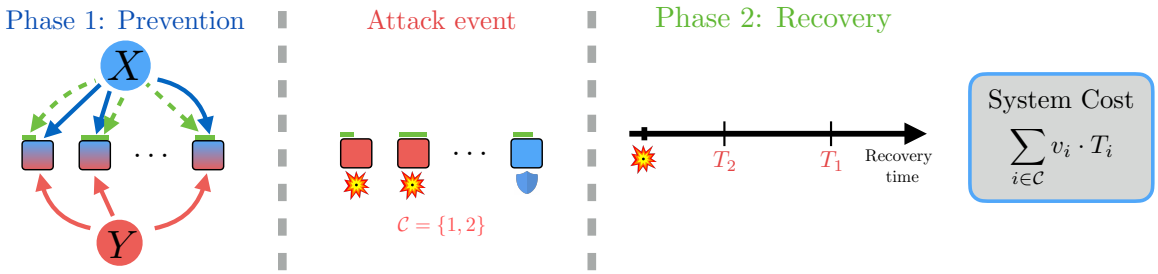

Fig. 1: The two-phase resource allocation contest model. (Left) In phase 1, the defender allocates two types of resources to nodes – preventive defense (represented as blue arrows) and reactive defense (represented as green bars). Simultaneously, the attacker allocates its limited resources. The allocation of preventive resources diminishes the probability each node becomes compromised. (Center) The attack event results in a subset of nodes becoming compromised. (Right) In phase 2, the compromised nodes undergo a recovery process. The time T_i it takes node i to recover is stochastically determined and can be reduced with the allocation of more reactive defense resources. The cost to the defender is a weighted sum of recovery times, where the weight v_i can be interpreted as the value of node i.

nodes in both phases. These results contribute to understanding the tradeoffs between robustness and resilience properties under a more holistic approach to decision-making for security.

In Section II, we formulate our two-phase contest model. Section III presents our main result (Theorem 3.1), which determines the defender's optimal investments in reactive and preventive resources. Section IV contains all technical details and proofs necessary to establish the main result. Section V gives concluding remarks.

II. Model

We formalize the problem as a two-player game between a defender $\mathcal{D}$ and attacker $\mathcal{A}$. The defender has a limited budget $X > 0$ of resources to invest into both preventive and reactive defense. The defender $\mathcal{D}$ is tasked with allocating resources among a set of nodes $\mathcal{N} = \{1, \dots, n\}$. A feasible strategy for $\mathcal{D}$ is a pair of vectors $(\boldsymbol{x}^{(1)} = (x_1^{(1)}, \dots, x_n^{(1)}), \boldsymbol{x}^{(2)} = (x_1^{(2)}, \dots, x_n^{(2)}))$ that satisfies $x_i^{(1)}, x_i^{(2)} \geq 0$ for all $i \in \mathcal{N}$ and $\boldsymbol{x}^{(1)} + \boldsymbol{x}^{(2)} \in \Delta(X)$, where

$$\Delta(X) := \left\{ \boldsymbol{z} \in \mathbb{R}^{|\mathcal{N}|} : z_i \geq 0 \ \forall i \in \mathcal{N} \text{ and } \sum_{i \in \mathcal{N}} z_i \leq X \right\}. \tag{1}$$

We will denote $\Delta^2(X)$ as the set of all such feasible pairs $\boldsymbol{x} = (\boldsymbol{x}^{(1)}, \boldsymbol{x}^{(2)})$. We will refer to $\boldsymbol{x}^{(1)}$ as the *protection vector* and $\boldsymbol{x}^{(2)}$ as the *recovery vector*. Given any feasible pair $(\boldsymbol{x}^{(1)}, \boldsymbol{x}^{(2)}) \in \Delta^2(X)$, $X_1 := \sum_{i \in \mathcal{N}} x_i^{(1)}$ and $X_2 := \sum_{i \in \mathcal{N}} x_i^{(2)}$ are the amount of resources devoted to preventive and reactive defenses, respectively. The attacker $\mathcal{A}$ has a resource budget $Y > 0$ that it invests for launching attacks on the nodes. A feasible strategy for $\mathcal{A}$ is any vector $\boldsymbol{y} \in \Delta(Y)$. Given resource allocations $(\boldsymbol{x}^{(1)}, \boldsymbol{x}^{(2)})$ and $\boldsymbol{y}$ from both players, the following sequence of events occurs in two phases.

Phase 1: The decisions $\boldsymbol{x}^{(1)}$ and $\boldsymbol{y}$ influence the probabilities that a node becomes compromised. We consider the probability that node $i \in \mathcal{N}$ becomes compromised is given by a ratio-form contest success function (CSF) [23], [24], which is commonly used to model breach probabilities in cybersecurity applications [14], [25]:

$$p_i(x_i^{(1)}, y_i^{(1)}) := \frac{y_i^{(1)}}{y_i^{(1)} + x_i^{(1)}}. \tag{2}$$

This is also referred to in the literature as the *Tullock* CSF. The probability that node i remains secure (i.e. not compromised) from the attack is $1 - p_i$. From (2), the outcomes for each node are independent of each other – a common assumption in the contests literature [23]. Consequently, the probability that the set of nodes $\mathcal{C} \subseteq \mathcal{N}$ become compromised is precisely

$$q_{\mathcal{C}}(\boldsymbol{x}^{(1)}, \boldsymbol{y}) := \left(\prod_{i \in \mathcal{C}} \frac{y_i}{y_i + x_i^{(1)}} \right) \left(\prod_{i \notin \mathcal{C}} \frac{x_i^{(1)}}{y_i + x_i^{(1)}} \right). \tag{3}$$

Regarding the informational capability of $\mathcal{D}$, we make the following assumption.

Assumption 1. *The defender cannot observe the set of nodes $\mathcal{C}$ that become compromised.*

Hence, $\mathcal{D}$ cannot base its decision $\boldsymbol{x}^{(2)}$ on knowing the compromised nodes, and the selection of the recovery vector $\boldsymbol{x}^{(2)}$ effectively occurs at the same time as the selection of $\boldsymbol{x}^{(1)}$. This is reasonable in cybersecurity scenarios, as many studies on the competitive control over computer networks assume a defender does not know the infection status of its nodes [26].

Phase 2: Given node i is compromised, it takes a random time $T_i(x_i^{(2)}) \geq 0$ for the compromise to be detected and recover i to a secure state. We model T_i as an exponential random variable with a rate parameter $r_i(x_i^{(2)})$ that increases in $x_i^{(2)}$. We note that the exponential distribution is a common choice to model recovery times (e.g. in compartmental contagion dynamics like SIS or SIR [27]).

In particular, $T_i(x_i^{(2)}) \sim \text{Exp}(r_i(x_i^{(2)}))$ with rate parameter $r_i(x_i^{(2)})$ defined by

$$r_i(x_i^{(2)}) := \frac{x_i^{(2)} + \delta_i}{x_i^{(2)} + \delta_i + \epsilon_i}, \tag{4}$$

where $\delta_i \geq 0$ indicates any existing reactive defense resources that node i is equipped with and $\epsilon_i > 0$ is an environmental parameter that determines how effective the reactive defense

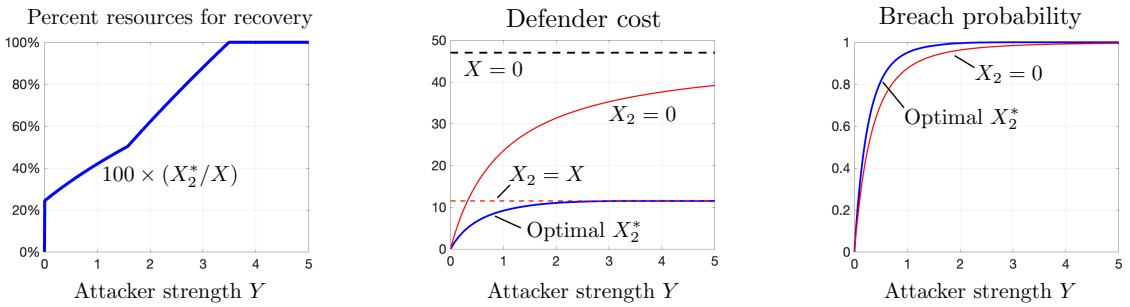

Fig. 2: Illustrations of the main result, Theorem 3.1, with $X = 1$, $\boldsymbol{v} = [1, 2, 3]$, $\boldsymbol{\epsilon} = [0.5, 0.3, 0.8]$, and $\boldsymbol{\delta} = [0.02, 0.05, 0.6]$. (a) The percentage of resources the defender devotes to reactive defense in equilibrium as the adversary's budget Y increases. (b) Expected costs to the defender when it uses equilibrium strategy (solid blue), invests all resources into reactive defense (dashed red), invests no resources into reactive defense (solid red), and has no resources at all (dashed black). (c) The probability that at least one of the nodes becomes compromised when the defender uses its equilibrium strategy (solid blue), or invests no resources into reactive defense (solid red).

resources $x_i^{(2)}$ are in terms of reducing expected recovery time. The recovery rate has a unit upper bound $r_i < 1$ across all nodes; note that this is without loss of generality because any heterogeneity may be absorbed in the importance parameters v_i. The cost experienced by the defender is given by

$$J_{\mathcal{D}} := \sum_{i \in \mathcal{C}} v_i \cdot T_i(x_i^{(2)}), \tag{5}$$

where $v_i > 0$ indicates node i's importance (e.g.) to the service of a network. Intuitively, the cost is the sum total of the amount of time each node spends in the compromised state weighted by its importance. The cost to the attacker is the negative, $J_{\mathcal{A}} = -J_{\mathcal{D}}$. A diagram of the complete model setup is shown in Figure 1. The defender seeks to minimize its ex-ante expected total cost,

$$\bar{J}_{\mathcal{D}}(\boldsymbol{x}, \boldsymbol{y}) := \mathbb{E}_{\mathcal{C} \sim q(\boldsymbol{x}^{(1)}, \boldsymbol{y})} \left[\sum_{i \in \mathcal{C}} v_i \cdot \mathbb{E}[T_i(x_i^{(2)})] \right], \tag{6}$$

and the attacker seeks to maximize the defender's cost. Because each node becomes compromised with an independent probability p_i and the expected recovery time for $i \in \mathcal{N}$ does not depend on the compromised set $\mathcal{C}$, the expected total cost can be expressed as

$$\bar{J}_{\mathcal{D}}(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i \in \mathcal{N}} \frac{y_i^{(1)}}{y_i^{(1)} + x_i^{(1)}} \cdot v_i \left(1 + \frac{\epsilon_i}{\delta_i + x_i^{(2)}} \right). \tag{7}$$

This defines a two-player strategic-form game that we denote by $\mathcal{G}(\Delta^2(X), \Delta(Y), \Gamma)$, where $\Gamma = \{v_i, \delta_i, \epsilon_i\}_{i \in \mathcal{N}}$ is the tuple of environmental parameters. An *equilibrium* of the game is any pair $(\boldsymbol{x}^*, \boldsymbol{y}^*)$ that satisfies

$$\bar{J}_{\mathcal{D}}(\boldsymbol{x}, \boldsymbol{y}^*) \geq \bar{J}_{\mathcal{D}}(\boldsymbol{x}^*, \boldsymbol{y}^*) \geq \bar{J}_{\mathcal{D}}(\boldsymbol{x}^*, \boldsymbol{y}) \tag{8}$$

for every $\boldsymbol{x} \in \Delta^2(X)$ and $\boldsymbol{y} \in \Delta(Y)$.

III. Main Results

Before presenting the main Theorem, we will follow (without loss of generality) a re-ordering of the indices of $\mathcal{N}$ according to

$$\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_n, \tag{9}$$

where $\alpha_i := \frac{\delta_i}{\sqrt{\epsilon_i v_i}}$. We also define parameters $V := \sum_{i \in \mathcal{N}} v_i$, and for $k = 1, \ldots, n$, $E_k := \sum_{j > k} \frac{\epsilon_j v_j}{\delta_j}$, $D_k := \sum_{j \leq k} \delta_j$, $S_k := (\sum_{j \leq k} \sqrt{\epsilon_j v_j})^2$, and $C_k := \frac{S_k}{V + E_k}$.

Our main result below establishes the amount of resources the defender devotes to reactive defenses in its equilibrium strategy.

Theorem 3.1. *The game $\mathcal{G}(\Delta^2(X), \Delta(Y), \Gamma)$ admits a unique equilibrium, where the defender's optimal amount of resources X_2^* to invest into reactive defense is given as follows.*

1) If $Y \leq f_1(0)$ or $Y = 0$, then $X_2^* = 0$.

2) If $Y \geq f_\ell(X)$, then $X_2^* = X$, where ℓ is the unique index satisfying

$$\ell = \arg\max \{k = 1, \ldots, n : g(\alpha_k) \leq X\} \tag{10}$$

and function $g : \mathbb{R}_+ \to \mathbb{R}_+$ is defined as

$$g(t) := \sum_{i \in \mathcal{N}} \max \{t \sqrt{\epsilon_i v_i} - \delta_i, 0\}. \tag{11}$$

3) If $f_k(g(\alpha_k)) < Y \leq f_k(g(\alpha_{k+1}))$ for $k \in \{1, \ldots, \ell\}$, then

$$X_2^* = \sqrt{C_k^2 + C_k(D_k + X + Y)} - (C_k + D_k). \tag{12}$$

The optimal amount of resources to invest into preventive defense is $X_1^* = X - X_2^*$. Here, we define

$$f_k(X_2) := \frac{V + E_k + S_k/(X_2 + D_k)}{S_k/(X_2 + D_k)^2} - (X - X_2) \tag{13}$$

for $k = 1, 2, \ldots, n$.

Section IV contains the full proof of this result. The first item of the Theorem indicates that no resources should be invested in reactive defense if the adversary is sufficiently weak, meaning that the attacker cannot succeed and thus recovery is not necessary. The threshold for defining "sufficiently weak" depends on the system's parameters. We note that this threshold can be negative, in which case the inequality is never satisfied. In this case the defender will always invest some resources in reactive defense because the attacker has a chance to succeed even if all defensive efforts are allocated to prevention. The second item indicates that the defender should invest all of its resources into reactive defense if the adversary

is sufficiently strong. In this case, the defender should not waste any resources on preventive defense. The third item specifies, in all other cases, how the defender should split its investments between prevention defense and reactive defense.

Figure 2 illustrates these results on a three-node example case study. When $Y = 0$, the defender is indifferent to any amount $X_2 \in [0, X]$ because no attack occurs. However, an interesting observation in Figure 2(a) is that for small $Y > 0$, the optimal percent investment starts increasing immediately from $\sim$25%. One might have expected the percentage to be 0, since it is much easier to prevent breaches when the attacker has negligible strength. In Figure 2(c), the probability that at least one of the nodes become compromised is shown. By using the optimal investment X_2^*, we observe the tradeoff that the defender makes, namely sacrificing preventive security in order to minimize the overall cost.

IV. Analysis

This section provides a sequence of technical Lemmas that are necessary to establish the proof of Theorem 3.1. Our approach is as follows: we first show that $\mathcal{G}(\Delta^2(X), \Delta(Y), \Gamma)$ is a zero-sum game with convex-concave structure (Lemma 4.1), allowing us to cast the problem of finding the equilibrium as a min-max optimization. We then proceed to explicitly solve the optimization problem (Lemmas 4.3 and 4.4) by first appealing to known results in the literature (Lemma 4.2). The final proof of Theorem 3.1 is provided at the end of the section.

Lemma 4.1. *The cost function $\bar{J}_{\mathcal{D}}(\boldsymbol{x}, \boldsymbol{y}) : \Delta^2(X) \times \Delta(Y) \to \mathbb{R}$ is continuous, convex in $\boldsymbol{x}$ for any fixed $\boldsymbol{y}$, and concave in $\boldsymbol{y}$ for any fixed $\boldsymbol{x}$.*

Proof. We focus on the proof for fixed $\boldsymbol{y} \in \Delta(Y)$ as the proof for fixed $\boldsymbol{x}$ is similar. The Hessian matrix of $\bar{J}_{\mathcal{D}}$ with respect to $\boldsymbol{x}$ is the following $2n \times 2n$ symmetric matrix represented in block form:

$$H_{\boldsymbol{x}} := \left[\begin{array}{c|c} D^{(1)} & M \\ \hline M & D^{(2)} \end{array}\right]. \tag{14}$$

Each of the blocks are $n \times n$ diagonal matrices with non-negative entries. We have $D^{(1)} = \operatorname{diag}\left(\left\{\frac{2y_i}{(y_i+x_i^{(1)})^3} v_i \left(1 + \frac{\epsilon_i}{\delta_i + x_i^{(2)}}\right)\right\}_{i\in\mathcal{N}}\right)$, $D^{(2)} = \operatorname{diag}\left(\left\{\frac{y_i}{y_i+x_i^{(1)}} \frac{2\epsilon_i v_i}{(\delta_i+x_i^{(2)})^3}\right\}_{i\in\mathcal{N}}\right)$, and $M = \operatorname{diag}\left(\left\{\frac{y_i}{(y_i+x_i^{(1)})^2} \frac{\epsilon_i v_i}{(\delta_i+x_i^{(2)})^2}\right\}_{i\in\mathcal{N}}\right)$. The eigenvalues of $H_{\boldsymbol{x}}$ are real-valued and are the solutions $s \in \mathbb{R}$ to

$$\det(sI_{2n} - H_{\boldsymbol{x}}) = 0. \tag{15}$$

Note that $sI_{2n} - H_{\boldsymbol{x}}$ is also a block matrix,

$$sI_{2n} - H_{\boldsymbol{x}} = \left[\begin{array}{c|c} sI_n - D^{(1)} & -M \\ \hline -M & sI_n - D^{(2)} \end{array}\right]. \tag{16}$$

Using the determinant identity $\det(sI_{2n} - H_{\boldsymbol{x}}) = \det((sI_n - D^{(1)})(sI_n - D^{(2)}) - M^2) = 0$, we observe that the latter matrix is diagonal with entries that are quadratic in s:

$$h_i(s) := s^2 - (D_i^{(1)} + D_i^{(2)})s + (D_i^{(1)} D_i^{(2)} - M_i^2), \ i \in \mathcal{N}. \tag{17}$$

The constant term is non-negative since matrix $D^{(1)}D^{(2)} - M^2$ is diagonal with non-negative entries,

$$\frac{(y_i)^2}{(y_i + x_i^{(1)})^4} \frac{\epsilon_i v_i^2}{(\delta_i + x_i^{(2)})^3} \left(4 + 3\frac{\epsilon_i}{\delta_i + x_i^{(2)}}\right) \geq 0. \tag{18}$$

We conclude that each of the $h_i(\cdot)$ satisfies $h_i(0) \geq 0$ and $h_i'(0) \leq 0$. Therefore, $s < 0$ cannot be a solution to any $h_i(s) = 0$, $i \in \mathcal{N}$. ∎

Consequently, the Minimax Theorem asserts that the game $\mathcal{G}(\Delta^2(X), \Delta(Y), \Gamma)$ admits a unique equilibrium cost; i.e., in any Nash equilibrium, the cost to the defender is given by

$$\min_{\boldsymbol{x}\in\Delta^2(X)} \max_{\boldsymbol{y}\in\Delta_{\mathcal{N}}(Y)} \bar{J}_{\mathcal{D}}(\boldsymbol{x}, \boldsymbol{y}). \tag{19}$$

Equation (19) provides a min-max optimization problem whose solution will yield the equilibrium payoff and strategy for the defender.

In order to solve (19), we first consider a simpler game in which the attacker and defender's strategy is respectively a vector of allocations $\boldsymbol{x} \in \Delta(X)$ and $\boldsymbol{y} \in \Delta(Y)$, and $w_i > 0$ denotes the cost to the defender if node i becomes compromised. The cost function to the defender is

$$\sum_{i\in\mathcal{N}} \frac{y_i}{y_i + x_i} \cdot w_i, \tag{20}$$

and the attacker's cost is the negation. Let us denote this game by $\mathcal{G}^0(\Delta(X), \Delta(Y), \{w_i\}_{i\in\mathcal{N}})$. In other words, $\mathcal{G}_0$ is the game consisting of only phase 1 of $\mathcal{G}$. The following well-known result describes its equilibrium.

Lemma 4.2 ([24]). *The game $\mathcal{G}^0(\Delta(X), \Delta(Y), \{w_i\}_{i\in\mathcal{N}})$ admits a unique Nash equilibrium $(\boldsymbol{x}^*, \boldsymbol{y}^*) \in \Delta(X) \times \Delta(Y)$, where*

$$x_i^* = \frac{w_i}{\sum_{j\in\mathcal{N}} w_j} X \quad \text{and} \quad y_i^* = \frac{w_i}{\sum_{j\in\mathcal{N}} w_j} Y \tag{21}$$

for all $i \in \mathcal{N}$. The equilibrium cost to the defender is given by

$$J_{\mathcal{D}}^0(X; \boldsymbol{w}) := \frac{Y}{Y + X} \sum_{i\in\mathcal{N}} w_i. \tag{22}$$

We observe that our formulation $\mathcal{G}(\Delta^2(X), \Delta(Y), \Gamma)$ resembles $\mathcal{G}^0$ with the difference that in our formulation, the defender has an opportunity to influence the values of the w_i's through its allocation of recovery resources $\boldsymbol{x}^{(2)}$. Namely, the weights are given by

$$w_i(x_i^{(2)}) := v_i \left(1 + \frac{\epsilon_i}{x_i^{(2)} + \delta_i}\right). \tag{23}$$

The next Lemma leverages this observation to refine optimization problem (19).

Lemma 4.3. *The equilibrium cost to the defender in*

$\mathcal{G}(\Delta^2(X), \Delta(Y), \Gamma)$ *is*

$$\min_{X_2 \in [0,X]} \min_{\boldsymbol{x}^{(2)} \in \Delta(X_2)} \frac{Y}{Y + X - X_2} \sum_{i \in \mathcal{N}} w_i(x_i^{(2)}). \tag{24}$$

Proof. From (19), the equilibrium cost of $\mathcal{G}(\Delta^2(X), \Delta(Y), \Gamma)$ is

$$\begin{aligned} &\min_{\boldsymbol{x} \in \Delta^2(X)} \max_{\boldsymbol{y} \in \Delta_{\mathcal{N}}(Y)} \bar{J}_{\mathcal{D}}(\boldsymbol{x}, \boldsymbol{y}) \\ &= \min_{X_2 \in [0,X]} \min_{\boldsymbol{x}^{(2)} \in \Delta(X_2)} \left[\min_{\boldsymbol{x}^{(1)} \in \Delta(X - X_2)} \max_{\boldsymbol{y} \in \Delta_{\mathcal{N}}(Y)} \bar{J}_{\mathcal{D}}(\boldsymbol{x}, \boldsymbol{y}) \right] \\ &= \min_{X_2 \in [0,X]} \min_{\boldsymbol{x}^{(2)} \in \Delta(X_2)} J^0_{\mathcal{D}}(X - X_2; \{w_i(x_i^{(2)})\}_{i \in \mathcal{N}}) \end{aligned} \tag{25}$$

where $J^0_{\mathcal{D}}$ is given in (22). ∎

In addition to finding the equilibrium cost of $\mathcal{G}(\Delta^2(X), \Delta(Y), \Gamma)$, solving the optimization problem (24) also reveals the optimal amount of resources to invest into reactive defense X_2^* as well as the allocation of the X_2^* resources over the nodes. Thus, we first focus on solving inner minimization problem of (24). That is, for a fixed X_2, find the allocation of reactive defense resources that solves

$$\min_{\boldsymbol{x}^{(2)} \in \Delta(X_2)} \frac{Y}{Y + X - X_2} \sum_{i \in \mathcal{N}} w_i(x_i^{(2)}). \tag{26}$$

Its solution is characterized below.

Lemma 4.4. *Suppose $X_2 \in [0, X]$ is fixed. The solution to* (26) *is given by*

$$x_i^{(2)*} = \begin{cases} \frac{\sqrt{\epsilon_i v_i}}{\sum_{j \le k} \sqrt{\epsilon_j v_j}} (X_2 + \sum_{j \le k} \delta_j) - \delta_i, & \text{for } i \le k \\ 0, & \text{for } i > k \end{cases} \tag{27}$$

for $i = 1, \ldots, n$, where $k \in \{1, 2, \ldots, n\}$ is the unique index for which $g(\alpha_k) \le X_2 < g(\alpha_{k+1})$ with $\alpha_{n+1} := \infty$, and $g(\cdot)$ is defined in (11)*. The optimal value of* (26) *is*

$$\frac{Y}{Y + X - X_2} \left(V + E_k + \frac{S_k}{X_2 + D_k} \right). \tag{28}$$

Proof. The optimal choice is also a solution to the problem

$$\min_{\boldsymbol{x}^{(2)} \in \Delta(X_2)} \sum_{i \in \mathcal{N}} \frac{\epsilon_i v_i}{x_i + \delta_i}, \tag{29}$$

which is obtained by removing additive constants and common factors. This is a convex problem since the objective and constraint set $\Delta(X_2)$ are convex. Slater's condition also holds. Thus, the Karush-Kuhn-Tucker (KKT) conditions are necessary and sufficient for optimality. In addition to the constraint $\boldsymbol{x}^{(2)} \in \Delta(X_2)$, we need $\forall i \in \mathcal{N}$,

$$-\frac{\epsilon_i v_i}{(x_i + \delta_i)^2} - \lambda_i + \lambda = 0, \tag{30}$$

where $\lambda_i \ge 0$ is the multiplier associated with the non-negativity constraint $-x_i \le 0$ and $\lambda \ge 0$ is the multiplier associated with the budget constraint $\sum_{i \in \mathcal{N}} x_i - X_2 \le 0$. The complementary slackness conditions must also hold, i.e., $\lambda_i x_i = 0$ for all $i \in \mathcal{N}$ and $\lambda(\sum_{i \in \mathcal{N}} x_i - X_2) = 0$. From condition (30), we observe two cases are possible

1) If $\lambda < \frac{\epsilon_i v_i}{\delta_i^2}$, then we have $\lambda_i^* = 0$ and $x_i^* = \sqrt{\frac{\epsilon_i v_i}{\lambda}} - \delta_i$.
2) If $\lambda \ge \frac{\epsilon_i v_i}{\delta_i^2}$, then we have $x_i^* = 0$ and $\lambda_i^* \ge 0$.

Consequently, we also observe that $\lambda \neq 0$, for otherwise the budget constraint would be violated. Thus, it must hold that $\sum_{i \in \mathcal{N}} x_i^* = X_2$, i.e., all of the budget is used. Therefore, the budget constraint must be satisfied with equality:

$$g(t) := \sum_{i \in \mathcal{N}} \max\{t\sqrt{\epsilon_i v_i} - \delta_i, 0\} = X_2, \tag{31}$$

where the variable $t := 1/\sqrt{\lambda}$. The function $g(t)$ is piece-wise linear and strictly increasing at any point t such that $g(t) > 0$. It is also unbounded from above and continuous. Thus, there exists a unique solution to the above equation.

For easier exposition, we will assume that the arrangement of indices (9) is ordered strictly, i.e. $\alpha_1 < \alpha_2 < \cdots < \alpha_n$ [1]. These are the values of t at which the piecewise-linear parts $t\sqrt{\epsilon_i v_i} - \delta_i$ become active in $g(t)$. The function g can then be written in the form

$$g(t) = \begin{cases} 0, & \text{if } t \in [0, \alpha_1) \\ \sum_{j \le k} t\sqrt{\epsilon_j v_j} - \delta_j, & \text{if } t \in [\alpha_k, \alpha_{k+1}), \\ & \quad k = 1, \ldots, n-1 \\ \sum_{j \in \mathcal{N}} t\sqrt{\epsilon_j v_j} - \delta_j, & \text{if } t > \alpha_n. \end{cases} \tag{32}$$

There exists an index $k^* \in \{1, \ldots, n\}$ for which $g(\alpha_{k^*}) < X_2 \le g(\alpha_{k^*+1})$, where we define $\alpha_{n+1} := \infty$. From (31), we can recover the value $t^* = \frac{X_2 + \sum_{j \le k^*} \delta_j}{\sum_{j \le k^*} \sqrt{\epsilon_j v_j}}$. This implies $\lambda_i^* = 0$ for all $i = 1, \ldots, k^*$, giving $\frac{\sqrt{\epsilon_i v_i}}{\sum_{j \le k^*} \sqrt{\epsilon_j v_j}} (X_2 + \sum_{j \le k^*} \delta_j) - \delta_i$, and $x_i^* = 0$ for all $i = k^* + 1, \ldots, n$. Substituting these into the objective of (26) yields expression (28). ∎

With the value of the inner problem established by (28), we complete the solution of (24) to establish Theorem 3.1.

Proof of Theorem 3.1. We leverage Lemma 4.4 to express problem (24) as

$$\min_{X_2 \in [0,X]} L(X_2), \tag{33}$$

where $L : [0, X] \to \mathbb{R}$ is defined as

$$L(X_2) := L_k(X_2) \text{ for } g(\alpha_k) \le X_2 < g(\alpha_{k+1}),\ k = 1, \ldots, \ell \tag{34}$$

with $L_k(X_2) := \frac{Y}{Y + X - X_2} \left(V + E_k + \frac{S_k}{X_2 + D_k} \right)$ and ℓ being defined in (10). In words, $L(X_2)$ is the minimum cost the defender can ensure when spending X_2 resources on reactive defense. We claim that function $L(X_2)$ is convex and continuously differentiable on $(0, X)$ because each $L_k(X_2)$ is convex, $L_k(g(\alpha_{k+1})) = L_{k+1}(g(\alpha_{k+1}))$, and $L_k'(g(\alpha_{k+1})) = L_{k+1}'(g(\alpha_{k+1}))$. Therefore, L attains its minimum value for a unique $X_2^* \in [0, X]$. Its derivative is

$$L'(X_2) = \frac{Y}{Y + X - X_2} \left(\frac{V + E_k + \frac{S_k}{X_2 + D_k}}{Y + X - X_2} - \frac{S_k}{(X_2 + D_k)^2} \right). \tag{35}$$

The condition $L'(0) \ge 0$ implies that $L(X_2)$ is strictly increasing, and therefore $X_2^* = 0$. This condition corresponds to item 1) in Theorem 3.1. The condition $L'(X) \le$

[1] This is without loss of generality as identical arguments in the proof still apply to non-strict orderings.

0 implies that $L(X_2)$ is strictly decreasing on $[0, X]$, and therefore $X_2^* = X$. This condition corresponds to item 2) in Theorem 3.1. If neither of these conditions hold, then it must be true that $L'_k(X_2^*) = 0$ for some $k \in \{1, \dots, \ell\}$ and $X_2^* \in [g(\alpha_k), g(\alpha_{k+1}))$. This implies that the condition $L'_k(g(\alpha_k)) \leq 0$ and $L'_k(g(\alpha_{k+1})) \geq 0$ must hold, which correspond to item 3) in Theorem 3.1. In this case, X_2^* is calculated by solving

$$\frac{V + E_k + \frac{S_k}{X_2 + D_k}}{Y + X - X_2} - \frac{S_k}{(X_2 + D_k)^2} = 0. \tag{36}$$

Using a change of variable $Z := X_2 + D_k$, we multiply the above equation by the positive factor $Z^2(Z - (D_k + X + Y))$ to obtain a quadratic equation

$$Z^2 + 2C_k Z - C_k(D_k + X + Y) = 0, \tag{37}$$

where we denote $C_k = \frac{S_k}{V_k + E_k}$. The roots are

$$Z = -C_k \pm \sqrt{C_k^2 + C_k(D_k + X + Y)}, \tag{38}$$

of which only the '+' root is positive. We therefore obtain

$$X_2^* = \sqrt{C_k^2 + C_k(D_k + X + Y)} - (C_k + D_k). \tag{39}$$

■

This concludes the proof of the main result, Theorem 3.1.

V. Conclusion

We have examined fundamental tradeoffs between investing in preventive versus reactive defense. We formulated a resource allocation contest game between a defender and an attacker with two distinct temporal phases. In phase 1, the defender's preventive resources reduces the probability that nodes can become compromised by the attacker. In phase 2, the compromised nodes undergo a recovery process that can be sped up with more reactive resources. Our analysis characterizes the Nash equilibrium strategies, which reveal the defender's optimal investment in preventive versus reactive defense efforts given limited resources. An interesting extension to this letter is to consider resources that may regenerate over time. This highlights the dynamic nature of making resource allocation decisions.

References

[1] F. Cohen, "On the implications of computer viruses and methods of defense," *Comput. Secur.*, vol. 7, no. 2, pp. 167–184, 1988.

[2] T. Longtchi, R. M. Rodriguez, L. Al-Shawaf, A. Atyabi, and S. Xu, "Internet-based social engineering psychology, attacks, and defenses: A survey," *Proceedings of IEEE*, vol. 112, no. 3, pp. 210–246, 2024.

[3] Q. Zhu and T. Başar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 46–65, 2015.

[4] S. Xu, "Cybersecurity dynamics: A foundation for the science of cybersecurity," in *Proactive and Dynamic Network Defense*. Springer, 2019, vol. 74, pp. 1–31.

[5] I. Linkov and A. Kott, "Fundamental concepts of cyber resilience: Introduction and overview," *Cyber resilience of systems and networks*, pp. 1–25, 2019.

[6] J. Chen, C. Touati, and Q. Zhu, "A dynamic game approach to strategic design of secure and resilient infrastructure network," *IEEE Transactions on Information Forensics and security*, vol. 15, pp. 462–474, 2019.

[7] Y. Han, W. Lu, and S. Xu, "Preventive and reactive cyber defense dynamics with ergodic time-dependent parameters is globally attractive," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2517–2532, 2021.

[8] V. S. Mai, R. J. La, and A. Battou, "Optimal cybersecurity investments using sis model: Weakly connected networks," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE, 2022, pp. 6097–6102.

[9] Q. Zhu and T. Başar, "Disentangling resilience from robustness: Contextual dualism, interactionism, and game-theoretic paradigms," *IEEE Control Systems Magazine*, vol. 44, no. 3, pp. 95–103, 2024.

[10] M. Vojnović, "Contest theory," *Commun. ACM*, vol. 60, no. 5, pp. 70–80, apr 2017. [Online]. Available: https://doi.org/10.1145/3012008

[11] D. Kovenock and B. Roberson, "Conflicts with multiple battlefields," in *The Oxford Handbook of the Economics of Peace and Conflict*, M. Garfinkel and S. Skaperdas, Eds. Oxford: Oxford University Press, 2012.

[12] P. H. Chia and J. Chuang, "Colonel blotto in the phishing war," in *Decision and Game Theory for Security: Second International Conference, GameSec 2011, College Park, MD, Maryland, USA, November 14-15, 2011. Proceedings 2*. Springer, 2011, pp. 201–218.

[13] A. Gupta, G. Schwartz, C. Langbort, S. S. Sastry, and T. Başar, "A three-stage colonel blotto game with applications to cyberphysical security," in *2014 American Control Conference*, 2014, pp. 3820–3825.

[14] D. Iliaev, S. Oren, and E. Segev, "A tullock-contest-based approach for cyber security investments," *Annals of Operations Research*, vol. 320, no. 1, pp. 61–84, 2023.

[15] M. Hajimirsaadeghi and N. B. Mandayam, "A dynamic colonel blotto game model for spectrum sharing in wireless networks," in *2017 55th Annual Allerton conference on communication, control, and computing (Allerton)*. IEEE, 2017, pp. 287–294.

[16] S. Guan, J. Wang, H. Yao, C. Jiang, Z. Han, and Y. Ren, "Colonel Blotto games in network systems: Models, strategies, and applications," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 637–649, 2020.

[17] A. Ferdowsi, W. Saad, and N. B. Mandayam, "Colonel blotto game for sensor protection in interdependent critical infrastructure," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2857–2874, 2021.

[18] D. Shishika, Y. Guan, M. Dorothy, and V. Kumar, "Dynamic defender-attacker blotto game," in *2022 American Control Conference (ACC)*. IEEE, 2022, pp. 4422–4428.

[19] A. Aghajan, K. Paarporn, and J. R. Marden, "A general lotto game over networked targets," in *2022 IEEE 61st Conference on Decision and Control (CDC)*, 2022, pp. 5974–5979.

[20] ——, "Equilibrium characterizations of multi-resource lotto games," *IFAC-PapersOnLine*, vol. 56, no. 2, pp. 2805–2810, 2023.

[21] ——, "Extension theorems for general lotto games with applications to network security," *IEEE Transactions on Control of Network Systems*, vol. 11, no. 1, pp. 185–196, 2023.

[22] G. Díaz-Garcia, F. Bullo, and J. R. Marden, "Beyond the 'enemy-of-my-enemy'alliances: Coalitions in networked contest games," in *2023 62nd IEEE Conference on Decision and Control (CDC)*. IEEE, 2023, pp. 2220–2225.

[23] S. Skaperdas, "Contest success functions," *Economic theory*, vol. 7, pp. 283–290, 1996.

[24] A. Robson, "Multi-item contests," *Working paper No. 446, The Australian National University*, 2005.

[25] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, nov 2002. [Online]. Available: https://doi.org/10.1145/581271.581274

[26] M. Van Dijk, A. Juels, A. Oprea, and R. L. Rivest, "Flipit: The game of "stealthy takeover"," *Journal of Cryptology*, vol. 26, pp. 655–713, 2013.

[27] P. Van Mieghem, "The n-intertwined sis epidemic network model," *Computing*, vol. 93, no. 2, pp. 147–169, 2011.