COST-EFFICIENT NETWORK PROTECTION GAMES AGAINST UNCERTAIN TYPES OF CYBER-ATTACKERS

Zhifan Xu, *Melike Baykal-Gürsoy*

Industrial and Systems Engineering, Rutgers University
Piscataway, NJ, USA
zhifan.xu@rutgers.edu, gursoy@soe.rutgers.edu

ABSTRACT

This paper considers network protection games for a heterogeneous network system with N nodes against cyber-attackers of two different types of intentions. The first type tries to maximize damage based on the value of each networked node, while the second type only aims at successful infiltration. A defender, by applying defensive resources to networked nodes, can decrease those nodes' vulnerabilities. Meanwhile, the defender needs to balance the cost of using defensive resources and potential security benefits. Existing literature shows that, in a Nash equilibrium, the defender should adopt different resource allocation strategies against different types of attackers. However, it could be difficult for the defender to know the type of incoming cyber-attackers. A Bayesian game is investigated considering the case that the defender is uncertain about the attacker's type. We demonstrate that the Bayesian equilibrium defensive resource allocation strategy is a mixture of the Nash equilibrium strategies from the games against the two types of attackers separately.

***Index Terms*—** Network protection, non-zero-sum game, Bayesian game.

1. INTRODUCTION

Modern cyber-network systems, such as computer networks and wireless communication networks, are under threat from increasing amounts of cyber-attacks. An unexpected cyber-attack may cause leakage of sensitive data, disruption in industrial controllers, or even casualties. Game theory-based models have been used to guide optimal defensive resources allocation against intelligent attackers in various scenarios [1, 2], including intrusion detection systems [3, 4] and physical layer security for wireless networks [5, 6, 7].

It is usually assumed that cyber-attackers will prefer some nodes in the network over other nodes. For example, Chen and Leneutre [8] proposed a game-theoretic model to find the optimal target selection strategy for intrusion detection in heterogeneous networks with each networked node containing security assets of different values. Wu et al. [9] investigated a two-stage intrusion detection resources allocation game for a network consisting of nodes of different importance. However, some attackers may have different intentions, such as the infiltration type attacker discussed in [10, 11] that treats all networked nodes equally. Garnaev *et al.* [12] discussed defensive resources allocation strategies when the attacker may be of maximal damage or infiltration type. The research in [13] also incorporates the cost of defensive resources and shows that optimal defensive resources allocation strategies have completely different forms against different types of attackers.

It is of great interest in the security community to investigate defense strategies when the type of attacker is unknown *a priori*. Zhang *et al.* [14] defined a *Ambiguous Security Game* using the D-S theory for a leader-follower game where there are attackers (followers) with different payoff functions but the defender (leader) doesn't know the probability of which type of attacker will show up. Chen *et al.* [15] applied the principle of Pareto optimality in repeated security games in which the defender can handle different types of attackers simultaneously. In this paper, we focus on the case that the incoming attacker is either of maximal damage type according to a known payoff function, or of infiltration type that treats every node equally. We proposed a Bayesian Nash game where the defender has a prior belief about the type of incoming attackers. The equilibrium is derived in closed form. It will be shown that the defender will fight against maximal damage type attacker on nodes with high value, while against infiltration type attacker on other nodes.

To the best of our knowledge, the research that is most relevant to this paper is [12], which also considers those two types of attackers but ignores the cost of defense. This paper will show that the cost of defense plays a key role.

2. FORMULATION OF THE PROBLEM

Consider a heterogeneous networked system with N nodes. The importance of each node is valued as $C_1, \dots, C_N$, re-

This material is based upon work supported by the National Science Foundation (Grant No.1901721).

spectively. Such networked system structures may correspond to varieties of information and communication networks, for example, a database cluster of N servers, or an OFDM wireless network with orthogonal sub-carriers. A cyber attacker is targeting some of the nodes, while an agent working as the defender tries to minimize the effect of attacks at the same time. For the sake of simplicity, assume that $C_1 > \cdots > C_N$, and the value of C_i's are known by both defender and attackers.

A strategy of the attacker is a normalized vector $\boldsymbol{y} = (y_1, ..., y_N)$ such that $y_i \geq 0,\ \forall i$, and also $\sum_{i=1}^N y_i = 1$, where y_i is the attack resource applied at node i. Similarly, a strategy of the defender is a normalized vector $\boldsymbol{x} = (x_1, ..., x_N)$ such that $x_i \geq 0,\ \forall i = 1$, where x_i is the defense resource applied at node i. Let $\sum_{i=1}^N x_i \leq 1$ so that the defender can decide not to use all defensive resources when it is not cost-effective. Moreover, let $G_i(x_i) = g_i x_i$ be the cost of defending node i, where $g_i > 0$ denotes the unit cost of applying defensive resources at node i [16, 9].

Let $p_i(x_i, y_i) \in [0, 1]$ be the vulnerability of node i. Equivalently, we can consider $p_i(x_i, y_i)$ as the probability of node i being destroyed. It should satisfy: 1) $p_i(x_i, y_i)$ is decreasing w.r.t $x_i \geq 0$; 2) $p_i(x_i, y_i)$ is increasing w.r.t. $y_i \geq 0$; 3) the vulnerability is 0 when node i is not attacked, that is, $p_i(x_i, 0) = 0$. In this paper, a linear representation for vulnerability is adopted as suggested in [12], that is,

$$p_i(x_i, y_i) = (1 - d_i x_i) y_i,\ \ \forall i = 1, ..., N,$$

where $d_i \in (0, 1)$ stands for the effectiveness of applying defensive resources at node i. Let $R_i(x_i, y_i) = p_i(x_i, y_i) C_i$ denote the expected damage at node i, thus it is proportional to node i's vulnerability and importance.

The defender wants to minimize the expected damage to the whole network caused by a cyber attack while maintaining a reasonable level of defense expenditure. Thus, if the defender knows the attacker's type, he needs to maximize the following utility function

$$\begin{aligned} u^D(\boldsymbol{x}, \boldsymbol{y_h}) &= -\sum_{i=1}^N R_i(x_i, y_{h_i}) - \sum_{i=1}^N G_i(x_i) \\ &= -\sum_{i=1}^N y_{h_i} C_i + \sum_{i=1}^N (y_{h_i} d_i C_i - g_i) x_i, \end{aligned} \tag{1}$$

where $h \in \{\mathrm{I}, \mathrm{II}\}$ stands for the type of the attacker. Here we call the maximal damage type attacker as the Type I attacker, and call the infiltration type attacker as the Type II attacker.

This paper considers the situation in which the defender and the attacker take action simultaneously. Hence, if the defender knows the attacker's type h, then $(\boldsymbol{x}^*, \boldsymbol{y}_{\boldsymbol{h}}^*)$ is a NE strategy pair if and only if

$$\begin{aligned} u^D(\boldsymbol{x}^*, \boldsymbol{y}_{\boldsymbol{h}}^*) &\geq u^D(\boldsymbol{x}, \boldsymbol{y}_{\boldsymbol{h}}^*),\ \ \forall \boldsymbol{x}, \\ u_h^A(\boldsymbol{x}^*, \boldsymbol{y}_{\boldsymbol{h}}^*) &\geq u_h^A(\boldsymbol{x}^*, \boldsymbol{y_h}),\ \ \forall \boldsymbol{y_h}, \end{aligned}$$

The next two sections show the analytical results from [13] about the NE structures when the defender is against different types of attackers.

2.1. The attacker aims to inflict maximal damage

When the attacker wants to inflict maximal expected damage, she maximizes the following utility function

$$u_{\mathrm{I}}^A(\boldsymbol{x}, \boldsymbol{y_{\mathrm{I}}}) = \sum_{i=1}^N R_i(x_i, y_{\mathrm{I}_i}) = \sum_{i=1}^N (1 - d_i x_i) C_i y_{\mathrm{I}_i}. \tag{2}$$

Define

$$\phi_i = \begin{cases} \sum_{j=1}^i \frac{C_j - C_i}{d_j C_j},\ \ \forall i \leq N, \\ \infty,\ \ \ i = N+1, \end{cases} \qquad \psi_i = \begin{cases} \sum_{j=1}^i \frac{g_j}{d_j C_j},\ \ \forall i \leq N, \\ \infty,\ \ \ i = N+1, \end{cases}$$

and let k be a positive integer such that $\phi_k < 1 < \phi_{k+1}$, m be a non-negative integer such that $\psi_m < 1 < \psi_{m+1}$.

If $k \leq m$, then the game has a unique NE $(\boldsymbol{x}^*, \boldsymbol{y}_{\mathbf{I}}^*)$ that

$$x_j^* = \begin{cases} \frac{\frac{1}{d_j C_j}}{\sum_{i=1}^k \frac{1}{d_i C_i}} (1 - \sum_{i=1}^k \frac{C_i - C_j}{d_i C_i}), & \forall j \leq k, \\ 0, & \forall k < j \leq N, \end{cases} \tag{3}$$

$$y_{\mathrm{I}_j}^* = \begin{cases} \frac{\frac{1}{d_j C_j}}{\sum_{i=1}^k \frac{1}{d_i C_i}} (1 - \sum_{i=1}^k \frac{g_i - g_j}{d_i C_i}), & \forall j \leq k, \\ 0, & \forall k < j \leq N. \end{cases} \tag{4}$$

If $m < k$, then the game has a unique NE $(\boldsymbol{x}^*, \boldsymbol{y}_{\mathbf{I}}^*)$ that

$$x_j^* = \begin{cases} \frac{C_j - C_{m+1}}{d_j C_j}, & \forall j \leq m, \\ 0, & \forall m < j \leq N, \end{cases} \tag{5}$$

$$y_{\mathrm{I}_j}^* = \begin{cases} \frac{g_j}{d_j C_j}, & \forall j \leq m, \\ 1 - \sum_{i=1}^m \frac{g_i}{d_i C_i}, & j = m+1, \\ 0, & \forall j > m+1. \end{cases} \tag{6}$$

Note that we assume $\phi_k \neq 1$ and $\psi_m \neq 1$ for the sake of simplicity. Also, the NE strategy $(\boldsymbol{x}^*, \boldsymbol{y}_{\mathbf{I}}^*)$ has the following properties summarized as lemma.

Lemma 1. *If $y_{\mathrm{I}_i}^* > 0$, then $x_j^* > 0,\ \forall j < i$.*

Lemma 2. *If $x_i^* > 0$, then $y_{\mathrm{I}_i}^* > 0$.*

Apparently, in both case (a) and case (b), the defender and the attacker will focus on nodes with the highest C_i's. By definition of ψ_i, $m < k$ implies that cost of defense g_j is large compared to $d_j C_j$ for some node j. Thus, in case (b), $\sum_{i=1}^N x_i^* < 1$, which means the defender keep some resources unused because it is not cost-effective.

2.2. The attacker aims to infiltrate the network

When the attacker tries to infiltrate the network, ignoring the difference of C_is, the attacker tries to maximize

$$u_{\mathrm{II}}^A(\boldsymbol{x}, \boldsymbol{y_{\mathrm{II}}}) = C \sum_{i=1}^N p_i(x_i, y_{\mathrm{II}_i}) = C \sum_{i=1}^N (1 - d_i x_i) y_{\mathrm{II}_i}, \tag{7}$$

where C is a constant replacing all C_i's. Define $\xi_N = \sum_{j=1}^N \frac{g_j}{d_j C_j}$. The NE strategy pair $(\boldsymbol{x}^*, \boldsymbol{y}_{\mathbf{II}}^*)$ also has different closed form solutions in two cases.

If $\xi_N < 1$, then the game has a unique equilibrium strategy $(\boldsymbol{x}^*, \boldsymbol{y}^*_{\mathbf{II}})$, for all $j \le N$,

$$x^*_j = \frac{\frac{1}{d_j}}{\sum_{i=1}^N \frac{1}{d_i}}, y^*_{\mathrm{II}_j} = \frac{\frac{1}{d_j C_j}}{\sum_{i=1}^N \frac{1}{d_i C_i}}\Big(1 - \sum_{i=1}^N \frac{g_i - g_j}{d_i C_i}\Big). \quad (8)$$

If $\xi_N > 1$, then the game has a unique equilibrium strategy $(\boldsymbol{x}^*, \boldsymbol{y}^*_{\mathbf{II}})$, for all $j \le N$,

$$x^*_j = 0, \quad y^*_{\mathrm{II}_j} \le \frac{g_j}{d_j C_j}. \quad (9)$$

Note that we assume $\xi_N \neq 1$ for the sake of simplicity. The NE strategy $(\boldsymbol{x}^*, \boldsymbol{y}^*_{\mathbf{II}})$ has the following property as lemma.

Lemma 3. *If $\xi_N > 1$, then $x^*_i = 0, \ \forall i = 1, ..., N$; if $\xi_N < 1$, then $x^*_i > 0, \ \forall i = 1, ..., N$.*

When facing a Type II attacker, the defender switches from protecting all nodes to not protecting any node as ξ_N becomes greater than 1. $\xi_N > 1$ actually implies that it is not cost-effective to protect the network since cost of defense g_j is large compared to $d_j C_j$ for some node j.

3. A BAYESIAN GAME WITH UNCERTAINTY ABOUT ATTACKER'S TYPE

The last section has shown that the defender should take completely different defensive resource allocation strategies against different types of attackers. Consider a scenario in which at any instance, the defender encounters either a Type I or a Type II attacker. However, the defender can not observe the attacker's type ahead of time, but he may have historical information about the frequency of each type of attack. Let the probability of facing a Type I attacker is $\alpha \in (0, 1)$, and of facing a Type II attacker is $1 - \alpha$.

The expected payoff of the defender, u^D, under a mixed policy triple $(\boldsymbol{x}, \boldsymbol{y}_{\mathrm{I}}, \boldsymbol{y}_{\mathrm{II}})$, is

$$\begin{aligned} u^D(\boldsymbol{x}, \boldsymbol{y}_{\mathrm{I}}, \boldsymbol{y}_{\mathrm{II}}) &= \alpha \cdot u^D(\boldsymbol{x}, \boldsymbol{y}_{\mathrm{I}}) + (1-\alpha) u^D(\boldsymbol{x}, \boldsymbol{y}_{\mathrm{II}}) \\ &= \sum_{i=1}^N x_i \left[\alpha y_{\mathrm{I}_i} + (1-\alpha) y_{\mathrm{II}_i}\Big) d_i C_i - g_i\right] \\ &- \sum_{i=1}^N \Big(\alpha y_{\mathrm{I}_i} + (1-\alpha) y_{\mathrm{II}_i}\Big) C_i. \end{aligned} \quad (10)$$

Meanwhile, every attacker knows her own type. Thus, the defender is playing a Bayesian game with uncertain attacker types. Let $(\boldsymbol{x}^*, \boldsymbol{y}^*_{\mathbf{I}}, \boldsymbol{y}^*_{\mathbf{II}})$ be the Bayesian equilibrium, then

$$v^D_B \equiv u^D(\boldsymbol{x}^*, \boldsymbol{y}^*_{\mathbf{I}}, \boldsymbol{y}^*_{\mathbf{II}}) \ge u^D(\boldsymbol{x}, \boldsymbol{y}^*_{\mathbf{I}}, \boldsymbol{y}^*_{\mathbf{II}}), \ \forall \boldsymbol{x} \in X,$$

$$v^A_{\mathrm{I}} \equiv u^A_{\mathrm{I}}(\boldsymbol{x}^*, \boldsymbol{y}^*_{\mathbf{I}}) \ge u^A_{\mathrm{I}}(\boldsymbol{x}^*, \boldsymbol{y}_{\mathbf{I}}), \ \forall \boldsymbol{y}_{\mathbf{I}} \in Y,$$
$$v^A_{\mathrm{II}} \equiv u^A_{\mathrm{II}}(\boldsymbol{x}^*, \boldsymbol{y}^*_{\mathbf{I}}) \ge u^A_{\mathrm{II}}(\boldsymbol{x}^*, \boldsymbol{y}_{\mathbf{II}}), \ \forall \boldsymbol{y}_{\mathbf{II}} \in Y,$$

where v^D_B, v^A_{I} and v^A_{II} denote the game value of the defender, Type I and Type II attackers, respectively. A computational way to find $\boldsymbol{x}^*$ is to solve a black-box optimization problem

$$\begin{aligned} \min_{\boldsymbol{x} \in X} \quad & w^D - u^D(\boldsymbol{x}, \boldsymbol{y}^*_{\mathbf{I}}, \boldsymbol{y}^*_{\mathbf{II}}) \\ \text{s.t.} \quad & \boldsymbol{y}^*_{\mathbf{I}} = \arg\max_{y_{\mathrm{I}} \in Y} u^A_{\mathrm{I}}(\boldsymbol{x}, \boldsymbol{y}_{\mathbf{I}}), \\ & \boldsymbol{y}^*_{\mathbf{II}} = \arg\max_{y_{\mathrm{II}} \in Y} u^A_{\mathrm{II}}(\boldsymbol{x}, \boldsymbol{y}_{\mathbf{II}}), \\ & w^D = \max_{\boldsymbol{x}' \in X} u^D(\boldsymbol{x}', \boldsymbol{y}^*_{\mathbf{I}}, \boldsymbol{y}^*_{\mathbf{II}}), \end{aligned} \quad (11)$$

and $\boldsymbol{x}^*$ is found when the objective function reaches global optimum 0. Such a problem may be solved by Genetic Algorithms [17] or Tabu Search [18, 19]. However, those algorithms are not guaranteed to converge to the global optimum.

This paper provides the closed-form solution of $\boldsymbol{x}^*$ by analyzing the Bayesian equilibrium's structures. The following lemma reveals a nodes-sharing property for Type I and Type II attackers. The equilibrium target sets of two attackers have at most one node in common.

Lemma 4. *For the Bayesian NE $(\boldsymbol{x}^*, \boldsymbol{y}^*_{\mathbf{I}}, \boldsymbol{y}^*_{\mathbf{II}})$, if $y^*_{\mathrm{I}_i} > 0$, then $y^*_{\mathrm{II}_j} = 0, \ \forall j < i$.*

Proof. Let S^A_i be a pure policy of attacker such that all attack resources are allocated to nodes i. Given $y^*_{\mathrm{I}_i} > 0$, it holds that

$$u^A_{\mathrm{I}}(\boldsymbol{x}^*, S^A_i) \ge u^A_{\mathrm{I}}(\boldsymbol{x}^*, S^A_j), \quad \forall j = 1, ..., N,$$

implying $C_i - x^*_i d_i C_i \ge C_j - x^*_j d_j C_j, \quad \forall j = 1, ..., N$. This inequality, then, provides the following bound on the payoff function of Type II attacker under the pure policy of attacking nodes j, i.e., $u^A_{\mathrm{II}}(\boldsymbol{x}^*, S^A_j)$, as

$$\begin{aligned} u^A_{\mathrm{II}}(\boldsymbol{x}^*, S^A_j) &= C(1 - x^*_j d_j) \le C\frac{C_i}{C_j}(1 - x^*_i d_i), \\ &< C(1 - x^*_i d_i) = u^A_{\mathrm{II}}(\boldsymbol{x}^*, S^A_i), \quad \forall j < i \end{aligned}$$

since $C_j > C_i, \ \forall j < i$. It means that S^A_j's are not Type II attacker's best responses for all $j < i$ under $\boldsymbol{x}^*$. ☐

By lemma 4, there must exist an integer n such that

$$\begin{cases} y^{\mathrm{I}}_i > 0, y^{\mathrm{II}}_i = 0 & \forall 1 \le i < n \\ y^{\mathrm{I}}_n > 0, y^{\mathrm{II}}_n \ge 0 \\ y^{\mathrm{I}}_i = 0, y^{\mathrm{II}}_i \ge 0 & \forall n < i \le N \end{cases} \quad (12)$$

That is, the defender will confront only Type I attacker from nodes 1 to $n-1$, only Type II attacker from nodes $n+1$ to N, and a mix of Type I attacker and Type II attacker at nodes n in the Bayesian equilibrium. Let S^D_i be a pure policy of defender such that all defensive resources are allocated to node i, and let S^D_{N+1} represent defender's choice of not allocating any defensive resource. Then the payoff of action S^D_{N+1} is

$$u^D(S^D_{N+1}, \boldsymbol{y}^*_{\mathbf{I}}, \boldsymbol{y}^*_{\mathbf{II}}) = -\sum_{i=1}^N \Big(\alpha y_{\mathrm{I}_i} + (1-\alpha) y_{\mathrm{II}_i}\Big) C_i. \quad (13)$$

Let $\bar{\mu}^D_{B_i} = u^D(S^D_i, \boldsymbol{y^*_{\mathrm{I}}}, \boldsymbol{y^*_{\mathrm{II}}}) - u^D(S^D_{N+1}, \boldsymbol{y^*_{\mathrm{I}}}, \boldsymbol{y^*_{\mathrm{II}}})$ be the benefit of defending nodes i as opposed to not defending at all. It is equal to

$$\bar{\mu}^D_{B_i} = \begin{cases} -g_i + \alpha y^*_{\mathrm{I}_i} d_i C_i, \quad \forall i = 1, ..., n-1, \\ -g_i + \alpha y^*_{\mathrm{I}_i} d_i C_i + (1-\alpha) y^*_{\mathrm{II}_i} d_i C_i, \;\; i = n, \\ -g_i + (1-\alpha) y^*_{\mathrm{II}_i} d_i C_i, \quad \forall i = n+1, ..., N, \\ 0, \quad i = N+1. \end{cases}$$

By the structure of $\bar{\mu}^D_{B_i}$, we can interpret the Bayesian game in the following way: the defender is playing against Type I attacker from node 1 to node n and is playing against Type II attacker from node n to node N where the two games entangle at node n. The Bayesian game should have similar properties of the previous 2 games including:

- Lemma 1 and 2 should still hold here for the defender and Type I attacker between $i = 1$ to n.
- Lemma 3 should still hold here for the defender and Type II attacker between $i = n$ to N. That is, either $x_i > 0$ or $x_i = 0 \;\; \forall i = n, ..., N$ will be true.

If the defender confronts both Type I and Type II defender in the Bayesian equilibrium, he will allocate resources to every node i. It follows that $\bar{\mu}^D_{B_i} = \bar{\mu}^D_{B_j}, \; \forall i, j$. We can then get the value of $\bar{\mu}^D_{B_i}$s by solving

$$\begin{cases} \tilde{v}^D_B = \bar{\mu}^D_{B_1} = \cdots = \bar{\mu}^D_{B_N}, \\ \sum_{i=1}^N y^*_{\mathrm{I}_i} = 1, \\ \sum_{i=n}^N y^*_{\mathrm{II}_i} = 1. \end{cases} \tag{14}$$

And a cut-off index n can be found.

However, the defender may not chose to counter both Type I and Type II attacker in the Bayesian equilibrium. The next theorem presents the conditions for the Bayesian equilibrium to be in different cases and provides analytical solutions.

Theorem 1. *Consider the Bayesian game described above. Let $\tilde{v}^D_B$ be the solution of 14, that is,*

$$\tilde{v}^D_B = \frac{1 - \sum_{i=1}^N \frac{g_i}{d_i C_i}}{\sum_{i=1}^N \frac{1}{d_i C_i}} \tag{15}$$

Let k and ϕ_k be defined in the same way as before. Let m be a non-negative integer such that $\zeta_m < 1 < \zeta_{m+1}$ where ζ_i is a strictly increasing sequence defined as

$$\zeta_i = \frac{1}{\alpha} \sum_{j=1}^{i} \frac{g_j + \max\left\{\tilde{v}^D_B, 0\right\}}{d_j C_j}, \quad \forall i = 1, ..., N, \tag{16}$$

and $\zeta_{N+1} = \infty$.

(a) If $k \leq m$, the game has unique equilibrium strategies for the defender and Type I attacker, and a continuum of equilibrium strategies for Type II attacker, given as

$$x^*_j = \begin{cases} \frac{\frac{1}{d_j C_i}}{\sum_{i=1}^k \frac{1}{d_i C_j}} (1 - \sum_{i=1}^k \frac{C_i - C_j}{d_i C_i}), & \forall j \leq k, \\ 0, & \forall j > k, \end{cases}$$

$$y^*_{\mathrm{I}_j} = \begin{cases} \frac{\frac{1}{d_j C_j}}{\sum_{i=1}^k \frac{1}{d_i C_i}} \left(1 - \frac{1}{\alpha} \sum_{i=1}^k \frac{g_i - g_j}{d_i C_i}\right), & \forall j \leq k, \\ 0, & \forall j > k, \end{cases}$$

$$y^*_{\mathrm{II}_j} = \begin{cases} 0, & \forall j \leq k, \\ \leq \frac{\alpha}{1-\alpha} \frac{\frac{1}{d_j C_j}}{\sum_{i=1}^k \frac{1}{d_i C_i}} (1 - \frac{1}{\alpha} \sum_{i=1}^k \frac{g_i - g_j}{d_i C_i}), & \forall j > k. \end{cases}$$

(b) If $k > m$, and

(b - 1) $\tilde{v}^D_B < 0$, the game again has unique equilibrium strategies for the defender and for Type I attacker, and a continuum of equilibrium strategies for Type II attacker, given as

$$x^*_j = \begin{cases} \frac{C_j - C_{m+1}}{d_j C_j}, & \forall j \leq m, \\ 0, & \forall m < j \leq N, \\ 1 - \sum_{i=1}^m \frac{C_i - C_{m+1}}{d_i C_i}, & j = N+1, \end{cases}$$

$$y^*_{\mathrm{I}_j} = \begin{cases} \frac{1}{\alpha} \cdot \frac{g_j}{d_j C_j}, & \forall j \leq m, \\ 1 - \frac{1}{\alpha} \sum_{i=1}^m \frac{g_i}{d_i C_i}, & j = m+1, \\ 0, & \forall j > m+1, \end{cases}$$

$$y^*_{\mathrm{II}_j} = \begin{cases} 0, \quad \forall j < m, \\ \leq \frac{1}{1-\alpha} \cdot \frac{g_j}{d_j C_j} - \frac{\alpha}{(1-\alpha)} (1 - \frac{1}{\alpha} \sum_{i=1}^m \frac{g_j}{d_i C_i}), j = m+1, \\ \leq \frac{1}{1-\alpha} \cdot \frac{g_j}{d_j C_j}, \quad \forall j > m+1. \end{cases}$$

(b - 2) $\tilde{v}^D_B > 0$, then all players have unique equilibrium strategies. The attackers' equilibrium strategies are

$$y^*_{\mathrm{I}_j} = \begin{cases} \frac{1}{\alpha} \cdot \frac{g_j + \tilde{v}^D_B}{d_j C_j}, & \forall j \leq m, \\ 1 - \frac{1}{\alpha} \sum_{i=1}^m \frac{g_i + \tilde{v}^D_B}{d_i C_i}, & j = m+1, \\ 0, & \forall j > m+1, \end{cases}$$

$$y^*_{\mathrm{II}_j} = \begin{cases} 0, & \forall j < m, \\ 1 - \frac{1}{1-\alpha} \sum_{i=m+1}^N \frac{g_i + \tilde{v}^D_B}{d_i C_i}, & j = m+1, \\ \frac{1}{1-\alpha} \cdot \frac{g_j + \tilde{v}^D_B}{d_j C_j}, & \forall j > m+1. \end{cases}$$

The defender's equilibrium strategy is

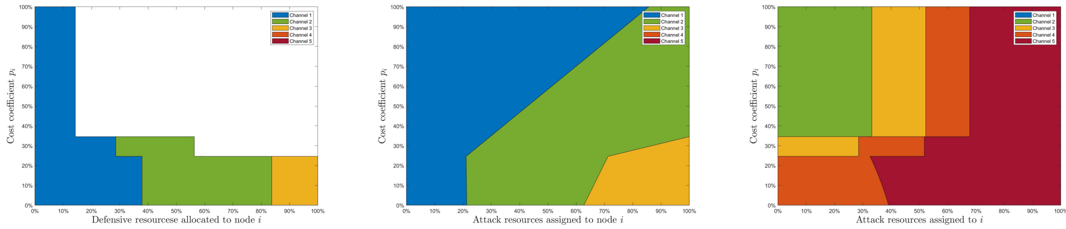
$$x^*_j = \begin{cases} \frac{C_j - v^A_{\mathrm{I}}}{d_j C_j}, & \forall j \leq m_I, \\ \frac{1 - v^A_{\mathrm{II}}}{d_j}, & \forall m_I < j \leq N, \\ 0, & j = N+1, \end{cases}$$

where

$$v^A_{\mathrm{I}} = \frac{\sum_{i=1}^N \frac{1}{d_i} - 1}{\sum_{i=1}^m \frac{1}{d_i C_i} + \sum_{i=m+1}^N \frac{1}{d_i C_{m+1}}}, v^A_{\mathrm{II}} = \frac{v^A_{\mathrm{I}}}{C_{m+1}}.$$

Proof. We provided a proof in Appendix. □

Remark. Here we assume that $\tilde{v}^D_B \neq 0, \phi_k \neq 1$ and $\zeta_m \neq 1$ to focus on the cases in which most players have unique equilibrium strategies.



(a) Optimal defense strategies (b) Type I attacker's strategies (c) Type II attacker's strategies

Fig. 1: Bayesian equilibrium strategies against uncertain types of attackers

The value of $\tilde{v}_B^D$ indicates whether it is cost-efficient for the defender to intercept Type II attacker. The case of $k \leq m$ implies that the defender has no additional resources to intercept Type II attacker. When $k > m$ and $\tilde{v}_B^D > 0$, it is cost-effective for the defender to protect all nodes. If $k > m$ and $\tilde{v}_B^D < 0$, then the defender will not allocate defensive resources to any nodes targeted by a Type II attacker.

4. NUMERICAL ILLUSTRATION

Consider a network consisted of $N = 5$ nodes with indices $I = \{1, ..., 5\}$. Let $\{C_i, i \in I\} = (0.5, 0.45, 0.40, 0.35, 0.30)$ and $\{d_i, i \in I\} = \{70\%, 40\%, 50\%, 60\%, 45\%\}$. Let $\{\tilde{g}_i, i \in I\} = \{0.18, 0.22, 0.14, 0.12, 0.16\}$ be the cost of defense, and $\alpha = 60\%$ be the probability of a Type I attack.

We introduce a cost coefficient $p \in [0\%, 100\%]$ and let $g_i = p \cdot \tilde{g}_i$ to observe the effect of cost on NE defense strategy. Fig. 1 demonstrates the equilibrium strategies as p increases. When $p \leq 24.63\%$, Theorem 1 gives $k = 3$ and $m = 3$. So the Bayesian equilibrium falls in Theorem 3 case (a), and only nodes 1 to 3 will be protected. As $p \geq 24.63\%$, k becomes larger than m but $\tilde{v}_B^D < 0$. Hence, the Bayesian equilibrium falls in the Theorem 3 case (b - 1), and the defender will protect fewer nodes. Also, the defender will not put his full effort into defending the network since it is not cost-effective.

5. CONCLUSIONS

This paper discusses defending against two types of cyber attackers for a heterogeneous networked system consisting of N nodes while taking the cost of defense into consideration. The attacker could be of two types, I or II; I) either he tries to inflict maximal damage based on the value of security assets, or II) he tries to infiltrate the networked system and treat all nodes the same. Considered is the case that the attacker's type is not known with certainty, a Bayesian game model provides the best policies for the defender, and Type I and Type II attackers. The attackers' best policy reveals a somewhat target-sharing structure, in which Type I attacker will focus on a few channels, while Type II attacker attacks the rest. However, one node may be attacked by both types of attackers.

Of interest for future research is to extend consider a dynamic game against multiple types of attackers. Instead of using a one-shot Bayesian game to model the case when the attacker's type is not known with certainty, we would like to investigate how the defender can learn the attacker's type from historical attack events.

6. REFERENCES

[1] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Bacşar, and Jean-Pierre Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys (CSUR)*, vol. 45, no. 3, pp. 1–39, 2013.

[2] Quanyan Zhu and Stefan Rass, "Game theory meets network security: A tutorial," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 2163–2165.

[3] Afrand Agah, Sajal K Das, Kalyan Basu, and Mehran Asadi, "Intrusion detection in sensor networks: A non-cooperative game approach," in *Third IEEE International Symposium on Network Computing and Applications, 2004.(NCA 2004). Proceedings.* IEEE, 2004, pp. 343–346.

[4] Tansu Alpcan and Tamer Basar, "A game theoretic approach to decision and analysis in network intrusion detection," in *42nd IEEE International Conference on Decision and Control (IEEE Cat. No. 03CH37475)*. IEEE, 2003, vol. 3, pp. 2595–2600.

[5] Eitan Altman, Konstantin Avrachenkov, and Andrey Garnaev, "A jamming game in wireless networks with transmission cost," in *International Conference on Network Control and Optimization*. Springer, 2007, pp. 1–12.

[6] Andrey Garnaev and Wade Trappe, "Secret communication when the eavesdropper might be an active adversary," in *International Workshop on Multiple Access Communications*. Springer, 2014, pp. 121–136.

[7] Zhu Han, Ninoslav Marina, Mérouane Debbah, and Are Hjorungnes, "Physical layer security game: How to date a girl with her boyfriend on the same table," in *2009 International Conference on Game Theory for Networks*. IEEE, 2009, pp. 287–294.

[8] Lin Chen and Jean Leneutre, "A game theoretical framework on intrusion detection in heterogeneous networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 2, pp. 165–178, 2009.

[9] Hao Wu, Wei Wang, Changyun Wen, and Zhengguo Li, "Game theoretical security detection strategy for networked systems," *Information Sciences*, vol. 453, pp. 346–363, 2018.

[10] Christophe Kiennert, Ziad Ismail, Herve Debar, and Jean Leneutre, "A survey on game-theoretic approaches for intrusion detection and response optimization," *ACM Computing Surveys (CSUR)*, vol. 51, no. 5, pp. 1–31, 2018.

[11] Andrey Garnaev, Melike Baykal-Gursoy, and H Vincent Poor, "How to deal with an intelligent adversary," *Computers & Industrial Engineering*, vol. 90, pp. 352–360, 2015.

[12] Andrey Garnaev, Melike Baykal-Gürsoy, and H Vincent Poor, "Incorporating attack-type uncertainty into network protection," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 8, pp. 1278–1287, 2014.

[13] Zhifan Xu and Melike Baykal-Gürsoy, "Efficient network protection games against multiple types of strategic attackers," in *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2021, pp. 2620–2624.

[14] Youzhi Zhang, Xudong Luo, and Wenjun Ma, "Security games with ambiguous information about attacker types," in *Australasian Joint Conference on Artificial Intelligence*. Springer, 2013, pp. 14–25.

[15] Ling Chen, Mingchu Li, and Yingmo Jie, "Playing repeated security games with multiple attacker types: a q-iteration on a linear programming approach," *Journal of Control and Decision*, vol. 0, no. 0, pp. 1–15, 2020.

[16] Andrey Garnaev, Melike Baykal-Gursoy, and H Vincent Poor, "Security games with unknown adversarial strategies," *IEEE transactions on cybernetics*, vol. 46, no. 10, pp. 2291–2299, 2015.

[17] Sankar Kumar Roy and Prasanta Mula, "Solving matrix game with rough payoffs using genetic algorithm," *Operational Research*, vol. 16, no. 1, pp. 117–130, 2016.

[18] Amirhossein Feizi Ashtiani and Samuel Pierre, "Power allocation and resource assignment for secure d2d communication underlaying cellular networks: A tabu search approach," *Computer Networks*, vol. 178, pp. 107350, 2020.

[19] Shan Jiang, Yilun Zhang, Ran Liu, Mohsen Jafari, and Mohamed Kharbeche, "Data-driven optimization for dynamic shortest path problem considering traffic safety," *IEEE Transactions on Intelligent Transportation Systems*, 2022.

Appendix

Proof of Theorem 1

Denote v_{I}^A to be the game value of Type I attacker, v_{II}^A to be the game value of Type II attacker, v_B^D be the game value of the defender in the Bayesian equilibrium. Define $\bar{v}_B^D = v_B^D - \mu^D(S_{N+1}^D, \boldsymbol{y_{\mathrm{I}}^*}, \boldsymbol{y_{\mathrm{II}}^*})$, the next proposition will be essential to construct an upper bound for n.

Proposition. $\bar{v}_B^D \geq \tilde{v}_B^D$.

Proof. If $\tilde{v}_B^D \leq 0$, then $\bar{v}_B^D \geq \tilde{v}_B^D$ since $\bar{v}_B^D \geq 0$ by definition. If $\tilde{v}_B^D > 0$, consider the following optimization problem

$$\begin{aligned} \min_{\bar{v}_B^D, \boldsymbol{y_{\mathrm{I}}^*}, \boldsymbol{y_{\mathrm{II}}^*}} \quad & \bar{v}_B^D \\ \text{s.t.} \quad & \bar{v}_B^D \geq \bar{\mu}_{B_i}^D \quad \forall i = 1, ..., N \\ & \sum_{i=1}^{n} y_{\mathrm{I}_i}^* = 1, \quad \sum_{i=n}^{N} y_{\mathrm{II}_i}^* = 1. \end{aligned}$$

It is easy to show that the optimal value of this minimization problem is $\tilde{v}_B^D$. □

Hence, it holds that $\bar{v}_B^D \geq \max\left\{\tilde{v}_B^D, 0\right\}$. This in turn suggests an upper bound for the cut-off index n, given the indices m and k defined in Theorem 1.

Proposition. $n \leq \min\{k, m+1\}$.

Proof. By the definition of n, $y_{\mathrm{I}_n}^* > 0$. Then, lemma 1 implies that $x_j^* \geq \frac{C_j - C_n}{d_j C_j} \geq 0$, $\forall j = 1, ..., n$. Thus, $n \leq k$ since $\sum_{j=1}^{n} x_j^* \leq 1$.

By lemmas 1 and 2, clearly, $x_i^* > 0$, $y_{\mathrm{I}_i}^* > 0$, $\forall i \leq n-1$, and $\bar{\mu}_{B_i}^D = \bar{v}_B^D$, $\forall i \leq n-1$, giving

$$y_{\mathrm{I}_i}^* = \frac{\bar{v}_B^D + g_i}{\alpha d_i C_i} > 0, \quad \forall i = 1, ..., n-1.$$

Since it is also true that $y_{\mathrm{I}_n}^* > 0$ and $\bar{v}_B^D \geq \max\left\{\tilde{v}_B^D, 0\right\}$, the following holds

$$\sum_{i=1}^{n-1} \frac{\tilde{v}_B^D + g_i}{\alpha d_i C_i} \leq \sum_{i=1}^{n-1} \frac{\bar{v}_B^D + g_i}{\alpha d_i C_i} \leq 1,$$

hence, by definition, $n \leq m+1$. □

The final value of n and the explicit solution of $(\boldsymbol{x^*}, \boldsymbol{y^*_{\mathrm{I}}}, \boldsymbol{y^*_{\mathrm{II}}})$ depends on the relationship between k, m and $\tilde{v}_B^D$ as defined in Theorem 3. There are three possible cases: (a) $k \leq m$, (b - 1) $m < k$ and $\tilde{v}_B^D < 0$, (b - 2) $m < k$ and $\tilde{v}_B^D > 0$.

(a) The case $k \leq m$ is similar to case (a) in sectione 2.1, where the defender will use up all his attention to intercept Type I Eve at the first k channels. Thus $n = k$ follows. The defender will not interfere Type II Eve, with $x_i^* = 0, \ \forall i = k+1, ..., N, N+1$. Meanwhile, Type I attacker will also focus on channels 1 through k. The equilibrium strategies for the defender and Type I attacker are the solution to

$$\begin{cases} v_{\mathrm{I}}^A = \mu_{\mathrm{I}}^A(\boldsymbol{x^*}, S_1^A) = \cdots = \mu_{\mathrm{I}}^A(\boldsymbol{x^*}, S_k^A), \\ \bar{v}_B^D = \bar{\mu}_{B_1}^D = \cdots = \bar{\mu}_{B_k}^D, \\ \sum_{i=1}^k x_i^* = 1, \quad \sum_{i=1}^k y_{\mathrm{I}_i}^* = 1, \end{cases} \tag{17}$$

which gives $C_{k+1} < v_{\mathrm{I}}^A < C_k$, $\bar{v}_B^D > \max\left\{\tilde{v}_B^D, 0\right\}$ and $x_i^* > 0, \ \forall i = 1, ..., k$. Since $x_i = 0, \ \forall i = k+1, ..., N$, it holds that

$$\begin{aligned} v_{\mathrm{II}}^A = \mu_{\mathrm{II}}^A(\boldsymbol{x^*}, S_{k+1}^A) = \cdots = \mu_{\mathrm{I}}^A(\boldsymbol{x^*}, S_N^A) = C \\ > \mu_{\mathrm{II}}^A(\boldsymbol{x^*}, S_i^A), \quad \forall i = 1, ..., k. \end{aligned}$$

So in equilibrium, Type II attacker attacks channels $k+1$ to N and makes sure that it is always more beneficial for the defender to intercept Type I attacker. Any strategy that satisfies

$$\begin{cases} \bar{\mu}_{B_i}^D \leq \bar{v}_B^D, \quad \forall i = k+1, ..., N, \\ \sum_{i=k+1}^N y_{\mathrm{II}_i}^* = 1 \end{cases} \tag{18}$$

is a NE strategy of Type II attacker.

(b) The case $k > m$ can be imagined as case (b) of section 2.1 combined with Type II game. The defender has extra resources to fight against Type II attacker, but whether the defender will interfere Type II attacker depends on the value of an indicator, $\tilde{v}_B^D$.

Lemma 5. *Given $k > m$, if $\tilde{v}_B^D < 0$, then $x_i^* = 0, \ \forall i = n, ..., N$; but, if $\tilde{v}_B^D > 0$, then $x_i^* > 0, \ \forall i = n, ..., N$.*

Proof. In order to prove the first statement by contradiction, assume $x_i^* \neq 0$ for some $i = n, ..., N$ given $\tilde{v}_D^B < 0$. By lemma 4, $x_i^* > 0, \ \forall i = n, ..., N$. Moreover, by lemmas 1 and 2, it is also true that $x_i^* > 0, \ \forall i = 1, ..., n-1$. That requires,

$$\bar{\mu}_{B_i}^D = \bar{v}_B^D \geq 0, \quad \forall i = 1, ..., N.$$

However, it is impossible to find such $\bar{\mu}_{B_i}^D \ \forall i = 1, ..., N$, since $\tilde{v}_D^B < 0$. Hence, the assumption cannot be true.
To prove the second statement again by contradiction, assume $x_i^* = 0$ for some $i = n, ..., N$, under the constraint $\tilde{v}_D^B > 0$. Then, lemma 4 implies $x_i^* = 0, \ \forall i = n, ..., N$, furthermore, $x_{N+1}^* = 0$ since $\bar{v}_B^D \geq \tilde{v}_B^D > 0 = \bar{\mu}_{B_{N+1}}^D$. That will lead to $\sum_{i=1}^{n-1} x_i^* = 1$. Meanwhile, if $x_i^* > 0$ for an integer $i = 1, ..., n$, then $y_i^* > 0$ by lemma 2 and $\mu_{\mathrm{I}}^A(\boldsymbol{x^*}, S_i^A) = v_{\mathrm{I}}^A$. Moreover, $v_{\mathrm{I}}^A \geq C_{E_n}$ since $x_n^* = 0$.
It can be seen that it is impossible to find a solution of $\sum_{i=1}^{n-1} x_i^* = 1$ given $n-1 \leq m$, $k > m$ and the constraint $\mu_{\mathrm{I}}^A(\boldsymbol{x^*}, S_i^A) \geq C_n \ i = 1, ..., n-1$. Hence, the assumption cannot be true. □

(b - 1) If $k > m$ and $\tilde{v}_B^D < 0$, this case is similar to case (b) of section 2.1 combined with case (b) of section 2.2. Thus, $n = m+1$ follows. Type I attacker will focus on channels 1 to $m+1$, while the defender can protect more than m channels but it is beneficial not to protect the remaining channels so that $x_i^* = 0, \ \forall i = m+1, ..., N$ by lemma 5 and has $x_{N+1}^* > 0$. Thus, the equilibrium strategies of the defender and Type I attacker are solutions to

$$\begin{cases} v_{\mathrm{I}}^A = \mu_{\mathrm{I}}^A(\boldsymbol{x^*}, S_1^A) = \cdots = \mu_{\mathrm{I}}^A(\boldsymbol{x^*}, S_m^A) = C_{m+1}, \\ \bar{v}_B^D = \bar{\mu}_{B_1}^D = \cdots = \bar{\mu}_{B_m}^D = 0, \\ x_{N+1}^* = 1 - \sum_{i=1}^m x_i^*, \quad y_{\mathrm{I}_{m+1}}^* = 1 - \sum_{i=1}^m y_{\mathrm{I}_i}^*. \end{cases}$$

Note that $x_i^* > 0, \ \forall i = 1, ..., m$ and $x_i = 0, \ \forall i = m+1, ..., N$. Thus, any strategy that satisfies

$$\begin{cases} \bar{\mu}_{B_i}^D \leq 0, \quad \forall i = m+1, ..., N, \\ \sum_{i=m+1}^N y_{\mathrm{II}_i}^* = 1, \end{cases}$$

can be a NE strategy of Type II attacker.

(b - 2) If $k > m$ and $\tilde{v}_B^D > 0$, this case can be regarded as case (b) of Theorem 1 combined with case (a) of Theorem 2. By lemma 5 $x_i^* > 0, \ \forall i = 1, ..., N$, so the attackers' equilibrium strategies $(\boldsymbol{y^*_{\mathrm{I}}}, \boldsymbol{y^*_{\mathrm{II}}})$ are solutions to the system of equations 14, which gives $\bar{v}_B^D = \tilde{v}_B^D$ and $n = m+1$. Thus, $(\boldsymbol{y^*_{\mathrm{I}}}, \boldsymbol{y^*_{\mathrm{II}}})$ must satisfy

$$\begin{cases} y_{\mathrm{I}_i}^* > 0, y_{\mathrm{II}_i}^* = 0, \quad \forall 1 \leq i < n, \\ y_{\mathrm{I}_n}^* > 0, y_{\mathrm{II}_n}^* > 0, \\ y_{\mathrm{I}_i}^* = 0, y_{\mathrm{II}_i}^* > 0, \quad \forall n < i \leq N. \end{cases}$$

Hence, the defender's equilibrium strategy $\boldsymbol{x^*}$ is the solution to

$$\begin{cases} v_{\mathrm{I}}^A = \mu_{\mathrm{I}}^A(\boldsymbol{x^*}, S_1^A) = \cdots = \mu_{\mathrm{I}}^A(\boldsymbol{x^*}, S_{m+1}^A), \\ v_{\mathrm{II}}^A = \mu_{\mathrm{II}}^A(\boldsymbol{x^*}, S_{m+1}^A) = \cdots = \mu_{\mathrm{II}}^A(\boldsymbol{x^*}, S_N^A), \\ \sum_{i=1}^N x_i^* = 1, \end{cases}$$

which is unique.