EFFICIENT NETWORK PROTECTION GAMES AGAINST MULTIPLE TYPES OF STRATEGIC ATTACKERS

Zhifan Xu, Melike Baykal-Gürsoy

Industrial and Systems Engineering, Rutgers University

ABSTRACT

This paper considers network protection games against different types of attackers for a heterogeneous network system with N units. A defender, by applying resources to networked units, can decrease the units' vulnerabilities. At the same time, the defender needs to take into account the cost of using defense resources. Two non-zero sum Nash games against two different types of attackers are studied. The first type tries to maximize damage based on the value of security assets related to networked units, while the second type aims at infiltrating the network. The analyses show that there exists a cut-off index determining the set of units that will be protected in the equilibrium strategies of the first game, while either all units or none will be covered in the equilibria of the second game. Numerical examples detail an application for wireless communication networks.

***Index Terms*—** Network protection, non-zero sum game, wireless networks security

1. INTRODUCTION

Cyber attacks have become a major threat to networked systems such as computer networks and wireless communication networks. Game-theoretic models have been used to investigate optimal defense strategies against intelligent attackers to enhance network security addressing various aspects [1, 2], including intrusion detection systems [3, 4] and physical layer security for wireless communication networks [5, 6, 7, 8].

In intrusion detection problems, the defender needs to monitor a set of subsystems in preparation for upcoming intrusion attacks. Alpcan and Basar [4] introduced the fundamental game-theoretic framework in which an intrusion detection system (IDS) strategically decides the probability of setting an alarm for a subsystem. Agah *et al.* [3, 9] studied an intrusion detection game for a sensor network and showed that the defender should monitor clusters with lower defense cost. Chen and Leneutre [10] proposed a game-theoretic model to find the optimal target selection strategy for intrusion detection in heterogeneous networks with each network unit containing security assets of different values. Garnaev et al. [11] considered a scenario in which the level of protection effort and intrusion effort can affect the probability of successful intrusion detection. Comprehensive surveys of game-theoretic models applied to intrusion detection systems can be found in [12] and [13].

Game-theoretic models have also been used to find optimal resource allocation plans to protect parallel communication networks. Altman *et al.* [5] presented a game-theoretic transmission power allocation strategy over parallel channels against a hostile jammer. Garnaev and Trappe [7] proposed a type of active eavesdropper who strategically attacks a limited number of wireless channels and solved for the optimal transmission power control plan using an anti-eavesdropping game. A review of other related works can be found in Chapter 10 through 12 of the book [14].

Most of the work mentioned above assume that the attacker differentiates the networked units based on some value. For instance, a network intruder prefers to attack a unit that contains more valuable assets, and an eavesdropper tends to attack wireless channels with higher eavesdropping capacity. However, some attackers may treat all networked units equally, such as the infiltration type attacker discussed in [13, 15]. Therefore, a key point to successfully applying game-theoretic models for security is to correctly evaluate the adversary's intentions. Garnaev *et al.* [16] discussed protection strategies when the attacker may be of maximal damage or infiltration type, or when the attacker's type is uncertain. Zhang *et al.* [17] defined a security game where the defender has ambiguous information about the attackers' types. Recently, Chen *et al.* [18] applied the principle of Pareto optimality in repeated security games in which the defender can handle different types of attackers simultaneously.

This paper presents a game-theoretic approach to protect a heterogeneous network from intelligent attackers. Particularly, we focus on the case in which the attacker's payoff varies according to its type while also taking into account the cost of defense. As shown in [5, 9], the defense cost has significant effect on the equilibrium strategies. To the best of our knowledge, the research that is most relevant to this paper is [16], which ignores the cost of defense. We introduce two Nash games corresponding to different attacker types. The analysis demonstrates the optimality of threshold type equilibrium policies for the first game and the opti-

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

mality of an All-or-Nothing type equilibrium policies for the second game. The equilibrium of each game are derived in closed form. Furthermore, numerical examples of the proposed game-theoretic models applied to cooperative jamming problems exhibit various insights.

2. FORMULATION OF THE PROBLEM

Consider a heterogeneous networked system with N units, of which the assets that need to be protected are valued as $C_1, C_2, \ldots, C_i, \ldots, C_N$, respectively. A cyber attacker is targeting some of the units. To minimize the effect of these cyber attacks, an agent works as the defender.

This paper considers the situation in which both the attacker and the defender have limited resources, so the units to be attacked and protected must be picked strategically. For the sake of simplicity, assume that $C_1 > C_2 > \cdots > C_N$. The attacker's mixed strategy is a normalized vector $\boldsymbol{y} = (y_1, ..., y_N)$ such that $y_i \geq 0,\ \forall i = 1, ..., N$, where y_i is the attack resource applied at unit i. Assume the attacker is aggressive and she will always use up all resources on hand such that $\sum_{i=1}^{N} y_i = 1$. The defender's mixed strategy is a normalized vector $\boldsymbol{x} = (x_1, ..., x_N)$ such that $x_i \geq 0,\ \forall i = 1, ..., N$, where x_i is the defense resource applied at unit i. Unlike the attacker, the defender needs to consider the cost related to the usage of defense resources and may not allocate all resources into defense when it is not economic. Thus, the constraint for $\boldsymbol{x}$ is $\sum_{i=1}^{N} x_i \leq 1$. Moreover, let $G_i(x_i) = g_i x_i$ be the cost of defending unit i, where $g_i > 0$ denotes the unit cost of applying defense resources at unit i [11, 19].

Let $p_i(x_i, y_i)$ be the vulnerability of unit i when x_i defense resources and y_i attack resources are applied. Let $R_i(x_i, y_i) = p_i(x_i, y_i)C_i$ denote the expected damage at unit i which is proportional to the vulnerability and security assets' value at unit i. Note that the vulnerability function $p_i(x_i, y_i)$ should have the following properties: (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 unit i is not attacked, that is, $p_i(x_i, 0) = 0$. In this paper, a linear representation for the vulnerability function is adopted as suggested in [16], 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 defense resources at unit i.

Below are two application scenarios of the network protection problem described above.

1. *Intrusion detection against DDoS attack*. Let the networked system be a cluster of distributed cache servers. y_i denotes the proportion of attack packets used to attack server i. x_i denotes the proportion of monitoring time assigned by the defender to server i. C_i represents the volume of network traffic assigned to server i. d_i stands for the maximal detection probability at server i, and g_i stands for the cost per unit time when the monitoring device is turned on.
2. *Cooperative jamming against eavesdropper*. Let the networked system be an OFDM wireless network with N sub-carriers. y_i denotes the proportion of time an eavesdropper spending on attacking sub-carrier i. x_i denotes the proportion of time to initiate cooperative jamming on sub-carrier i. Let C_i be the eavesdropping capacity of sub-carrier i and d_i be the percentage of reduction of C_i if cooperative jamming is activated at channel i. Moreover, let g_i stands for the cost per unit time to send cooperative jamming signal.

This paper considers the situation in which the defender and the attacker take actions simultaneously and can not observe their opponent's decisions ahead of time. The defender wants to minimize the total expected damage to the whole network caused by a cyber attack while maintaining a reasonable level of defense expenditure. Thus, the defender's utility function is

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

which needs to be maximized. Meanwhile, the attacker wants to maximize $u_h^A(\boldsymbol{x}, \boldsymbol{y_h})$, which is the total expected damage to the whole network based on C_{h_i}'s, where $h \in \{\mathrm{I}, \mathrm{II}\}$ stands for the type of the attacker, and C_{h_i} is type h attacker's evaluation for her benefit of attacking unit i. Next two sections discuss the defense strategies against two types of attackers, namely, the maximal damage type attacker and the infiltration type attacker. This paper looks for the Nash Equilibrium (NE) strategy $\boldsymbol{y_h^*}$ for each type of attackers, together with the corresponding defense strategy $\boldsymbol{x}^*$, under complete information. That is, the strategy pair $(\boldsymbol{x}^*, \boldsymbol{y_h^*})$ satisfies

$$\begin{aligned} u^D(\boldsymbol{x}^*, \boldsymbol{y_h^*}) &\geq u^D(\boldsymbol{x}, \boldsymbol{y_h^*}),\ \ \forall \boldsymbol{x} \in X, \\ u_h^A(\boldsymbol{x}^*, \boldsymbol{y_h^*}) &\geq u_h^A(\boldsymbol{x}^*, \boldsymbol{y_h}),\ \ \forall \boldsymbol{y_h} \in Y, \end{aligned}$$

where X and Y denote the sets of strategies of the defender and the attacker, respectively.

3. THE MAXIMAL DAMAGE TYPE ATTACKER

This section considers the scenario in which the attacker, called the Type I attacker, tries to inflict the maximal damage to the system.Type I attacker will use the security assets' value to represent the damage on unit i, that is, $C_{\mathrm{I}_i} = C_i, \quad \forall i = 1, ..., N$. So the utility function for Type I attacker under arbitrary strategy pair, $(\boldsymbol{x}, \boldsymbol{y_\mathrm{I}})$, is

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

Notice that this is a bimatrix non-zero sum game with two players, namely the defender and the Type I attacker. Since this is a finite game, there is at least one mixed NE pair as proved by Nash [20]. The following theorem demonstrates an explicit threshold type structure of the equilibrium strategy pair, $(\boldsymbol{x}^*, \boldsymbol{y_\mathrm{I}^*})$, for this non-zero sum game.

Theorem 1. *Consider the non-zero sum game against a Type I attacker, let k be a positive integer such that $\phi_k < 1 < \phi_{k+1}$ where ϕ_i is a strictly increasing sequence defined as $\phi_i = \sum_{j=1}^{i} \frac{C_j - C_i}{d_j C_j}, \quad \forall i = 1, .., N$, and $\phi_{N+1} = \infty$. Let m be a non-negative integer such that $\psi_m < 1 < \psi_{m+1}$ where ψ_i is a strictly increasing sequence defined as $\psi_i = \sum_{j=1}^{i} \frac{g_j}{d_j C_j}, \quad \forall i = 1, .., N$, and $\psi_{N+1} = \infty$.*

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

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

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

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

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

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

Proof. We provide a proof in the appendix. □

Remark. We assume that $\phi_k \neq 1$ and $\psi_m \neq 1$. In case $\phi_k = 1$ and $\psi_m \neq 1$, the defender, in case $\phi_k \neq 1$ and $\psi_m = 1$, the attacker may have infinitely many solutions, depending on $k \leq m$ or $m < k$, respectively.

Notice that the value of m will be smaller if g_j is close to $d_j C_{E_j}$. That means, when the cost of defense is high, the number of network units that will be protected by the defender is smaller, and the defender will not utilize all resources as opposed to the case $m < k$.

4. THE INFILTRATION TYPE ATTACKER

In this scenario, the attacker tries to infiltrate the network without being detected, ignoring the marginal benefit of attacking unit i, that is, $C_{\mathrm{II}_i} = C, \quad \forall i = 1, ..., N$, where $C > 0$ is constant. We call the infiltration type attacker as the Type II attacker for convenience. Thus, the utility function of the Type II attacker is

$$u_{\mathrm{II}}^A(\boldsymbol{x}, \boldsymbol{y}_{\mathbf{II}}) = C \sum_{i=1}^{N} (1 - d_i x_i) y_{\mathrm{II}_i}. \tag{3}$$

Apparently, the defense levels are more important to the Type II attacker. We assume the defender still evaluates the importance of each unit i based on his own valuation of the security assets, C_i, so his utility function stays the same.

In the Nash game between the defender and the Type II attacker, the NE strategies are no longer of threshold type. The following theorem shows that the defender either covers all channels or chooses to protect none at all, and the choice depends on the value of $\xi_N = \sum_{j=1}^{N} \frac{g_j}{d_j C_j}$. If $\xi_N < 1$, the defender protects all channels.

Theorem 2. *Consider the game against Type II Eve.*

(a) If $\xi_N < 1$, then the game has a unique equilibrium strategy for both players such that for all $j = 1, ..., N$,

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

(b) If $\xi_N > 1$, then the game has a unique NE strategy for the defender but a continuum of NE strategies for the Type II attacker such that for all $j = 1, ..., N$,

$$x_j^* = 0, \quad y_{\mathrm{II}_j}^* \leq \frac{g_j}{d_j C_j}.$$

Proof. We provide a proof in Appendix. □

Remark. Here we assume $\xi_N \neq 1$ to focus on the cases in which the defender has unique equilibrium strategies.

Note that when the defender decides to cover the whole network, he tends to put more defense resources to units with smaller d_j values. That is intuitive since Type II attacker will infiltrate to units that are more difficult to defend.

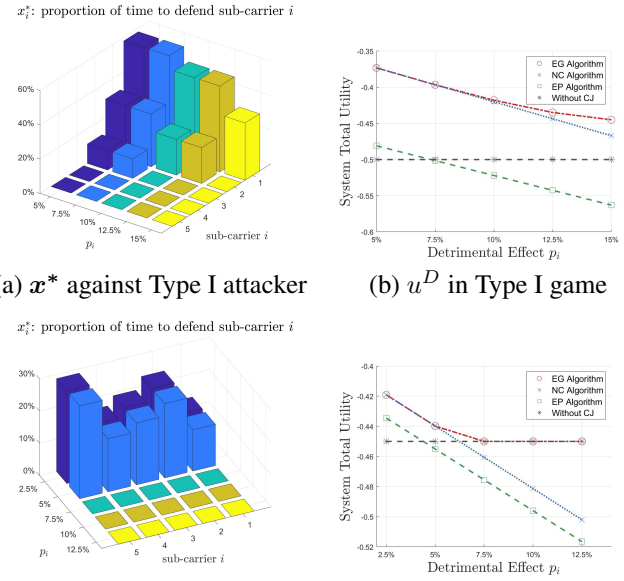
5. NUMERICAL ILLUSTRATIONS

This section focuses on the cooperative jamming against eavesdropping interpretation of our model. An OFDM network with $N = 5$ sub-carriers is being protected, where both the defender and the attacker can only pick one sub-carrier as target probabilistically. Consider the scenario that legitimate users will also be interfered, so $g_i = p_i C_{L_i}$ where C_{L_i} is the communication capacity at channel i and p_i is the percentage of decreasing caused by cooperative jamming. Let $\{C_{L_i}\}$=$\{0.9, 1.1, 0.7, 0.6, 0.8\}$.

For the game against Type I attacker, let eavesdropping capacity of each sub-carrier be $\{C_i\}$=$\{0.5, 0.4, 0.35, 0.3, 0.2\}$. Also, let $d_i = 60\%$ and $p_i = p, \ \forall i = 1, ..., 5$, where p is a constant. When p increases from 5% to 15%, the number of protected sub-carriers decreases from 3 to 1, as shown in Fig.1(a). Also, when p increases, the defender uses less and less time for protection.

For the game against Type II attacker, let $C_i = 0.45$ and still $p_i = p, \ \forall i = 1, ..., 5$. Let $\{d_i\}$ = {90%, 50%, 60%, 70%, 40%} such that it is easier to eavesdrop on some sub-carriers under defense. As shown in Fig.1(c), all sub-carriers are under protection when $p \leq 5\%$, but it is not worthy for the defender to protect any channel when $p > 5\%$.

Fig. 1(b) and 1(d) compares the system's total utility when the defender uses the proposed efficient game-theoretic algorithm (EG Algorithm), uses EG Algorithm but ignores defense cost (NC Algorithm), uses an Equal Probability algorithm (EP Algorithm), and does nothing (Without CJ), respectively. As p increases, the EG Algorithm always outperform the others.



(a) $\boldsymbol{x}^*$ against Type I attacker (b) u^D in Type I game

(c) $\boldsymbol{x}^*$ against Type II attacker (d) u^D in Type II game

Fig. 1. Optimal proportion of time spent on each sub-carrier.

6. CONCLUSIONS AND FUTURE RESEARCH

This paper discusses defending against two types of cyber attackers for a heterogeneous networked system consisted of N units, while taking the cost of defense into consideration. The attacker could be of two types, I or II; I) either she tries to inflict maximal damage based on the value of security assets, or II) she tries to infiltrate the networked system from any unit. The non-zero sum games modeling the problem against each attacker type demonstrate that the cost of defense is critical in deciding how to allocate defense resources.

Of interest for future research is an extension of this model to a Bayesian game when the eavesdropper's type is not known with certainty. Another possible extension is to consider a repeated game in which the defender can learn the attacker's true intention.

Appendix

Proof of Theorem 1

By Karuhn-Kush-Tucker (KKT) conditions, $(\boldsymbol{x}^*, \boldsymbol{y}_\mathbf{I}^*)$ are NE strategies if there exists Lagrange multipliers $w_D \geq 0$ and $w_A \geq 0$ such that, for all $i = 1, ..., N$,

$$\frac{\partial u^D(\boldsymbol{x}^*, \boldsymbol{y}_\mathbf{I}^*)}{\partial x_i} = y_{\mathrm{I}_i}^* d_i C_i - g_i \begin{cases} = w_D, & for\ \ x_i^* > 0, \\ \leq w_D, & for\ \ x_i^* = 0, \end{cases} \tag{4}$$

$$\frac{\partial u_\mathrm{I}^A(\boldsymbol{x}^*, \boldsymbol{y}_\mathbf{I}^*)}{\partial y_{\mathrm{I}_i}} = (1 - d_i x_i^*) C_i \begin{cases} = w_A, & for\ \ y_{\mathrm{I}_i}^* > 0, \\ \leq w_A, & for\ \ y_{\mathrm{I}_i}^* = 0, \end{cases} \tag{5}$$

and $w_D(\sum_{i=1}^N x_i^* - 1) = 0$. Equations system (4) implies that, if $x_i^* > 0$, then $y_{\mathrm{I}_i}^* = \frac{w_D + g_i}{d_i C_i} > 0$. Equations system (5) implies that, if $y_{\mathrm{I}_i}^* > 0$, then $C_i \geq w_A$. Also, since $C_j > C_i,\ \forall j < i$ by assumption, then $x_j^* = \frac{C_j - w_A}{d_j C_j},\ \forall j \leq i$ if $y_{\mathrm{I}_i}^* > 0$. Also notice that, if $y_{\mathrm{I}_i}^* > 0$, then $y_{\mathrm{I}_j}^* > 0,\ \forall j < i$. Thus, threshold k decided by $\phi_k < 1 < \phi_{k+1}$ actually points out the largest possible k such that $\sum_{j=1}^k x_j^* = \sum_{j=1}^k \frac{C_j - w_A}{d_j C_j} \leq 1$ and $C_k \geq w_A > C_{k+1}$. Similarly, threshold m decided by $\psi_m < 1 < \psi_{m+1}$ shows the largest possible m such that $\sum_{j=1}^m y_{\mathrm{I}_j}^* = \sum_{j=1}^m \frac{w_D + g_j}{d_j C_j} \leq 1$ when $w_D = 0$.

Notice that we must have $x_i^* = 0$ and $w_A > C_i,\ \forall i > k$, which leads to $y_{\mathrm{I}_i}^* = 0,\ \forall i > k$. Thus, when $k \leq m$, it must be true that $w_D > 0$. Otherwise, if $w_D = 0$, then $\sum_{i=1}^N y_{\mathrm{I}_i}^* = \sum_{i=1}^k y_{\mathrm{I}_i}^* \leq \sum_{i=1}^k \frac{g_i}{d_i C_i} \leq \sum_{i=1}^m \frac{g_i}{d_i C_i} < 1$, which is not possible. Therefore, $w_D > 0$, which requires $\sum_{i=1}^k x_i^* = 1$. So w_A is the solution of $\sum_{j=1}^k \frac{C_j - w_A}{d_j C_j} = 1$, and $x_i^* = \frac{C_j - w_A}{d_j C_j},\ \forall i = 1, ..., k$. Under the assumption that $\phi_k > 1$, we must have $x_i^* > 0,\ \forall i = 1, ..., k$, then $y_{\mathrm{I}_i}^* = \frac{w_D + g_i}{d_i C_i},\ \forall i = 1, ..., k$ where w_D is the solution of $\sum_{i=1}^k \frac{w_D + g_i}{d_i C_i} = 1$.

When $k > m$, then $w_D = 0$. Otherwise, if $w_D > 0$, it follows that $x_k^* > 0$ as shown before, then $y_{\mathrm{I}_i}^* > \frac{g_i}{d_i C_i},\ \forall i = 1, ..., k$ and $\sum_{i=1}^k y_{\mathrm{I}_i}^* \geq \sum_{i=1}^{m+1} \frac{g_i}{d_i C_i} > 1$, which is impossible. Therefore, $w_D = 0$. Now to satisfy the constraint $\sum_{i=1}^N y_{\mathrm{I}_i}^* = 1$, we must have $y_{\mathrm{I}_i}^* = \frac{g_i}{d_i C_i}\ \forall i = 1, ..., m$ and $y_{\mathrm{I}_{m+1}}^* = 1 - \sum_{i=1}^m y_{\mathrm{I}_i}^*$. Under the assumption that $\psi_m < 1$, it must be true that $y_{\mathrm{I}_{m+1}}^* > 0$ but $\frac{\partial u^D(\boldsymbol{x}^*, \boldsymbol{y}_\mathbf{I}^*)}{\partial x_i} < 0$. Thus, $x_{m+1}^* = 0$. It follows that $w_A = C_{m+1}$ and $x_i^* = \frac{C_j - w_A}{d_j C_j},\ \forall i = 1, ..., m$.

Proof of Theorem 2

In this situation, KKT condition (5) changes to

$$\frac{\partial u_{\mathrm{II}}^A(\boldsymbol{x}^*, \boldsymbol{y}_{\mathbf{II}}^*)}{\partial y_{\mathrm{II}_i}} = (1 - d_i x_i^*) C \begin{cases} = w_A, & for\ \ y_{\mathrm{II}_i}^* > 0, \\ \leq w_A, & for\ \ y_{\mathrm{II}_i}^* = 0, \end{cases} \tag{6}$$

for all $i = 1, ..., N$. Thus, if $w_A < C$, then $x_i^* > 0,\ \forall i = 1, ..., N$, which implies an All-or-Nothing defending strategy, and we must have $\frac{\partial u^D(\boldsymbol{x}^*, \boldsymbol{y}_{\mathbf{II}}^*)}{\partial x_i} = w_D,\ \forall i = 1, ..., N$.

When $\xi_N < 1$, there exists an $y_{\mathrm{II}_i}^*$ such that $\frac{\partial u^D(\boldsymbol{x}^*, \boldsymbol{y}_{\mathbf{II}}^*)}{\partial x_i} = y_{\mathrm{II}_i}^* d_i C_i - g_i > 0$. Thus, $w_D > 0$ and $y_{\mathrm{II}_i}^* = \frac{w_D + g_i}{d_i C_i} > 0,\ \forall i = 1, ..., N$, where w_D is the solution of $\sum_{i=1}^N \frac{w_D + g_i}{d_i C_i} = 1$. Recall that $w_D > 0$ requires $\sum_{i=1}^N x_i^* = 1$, therefore, $x_i^* = \frac{C - w_A}{d_i C},\ \forall i = 1, ..., N$, where w_A is the solution of $\sum_{i=1}^N \frac{C - w_A}{d_i C} = 1$.

When $\xi_N > 1$, there must be some $y_{\mathrm{II}_i}^*$ such that $\frac{\partial u^D(\boldsymbol{x}^*, \boldsymbol{y}_{\mathbf{II}}^*)}{\partial x_i} = y_{\mathrm{II}_i}^* d_i C_i - g_i < 0$. So $w_D = 0$ is the only solution and $x_i^* = 0,\ \forall i = 1, .., N$, since it is not beneficial to protect any target. The attacker can use any policy as long as $\frac{\partial u^D(\boldsymbol{x}^*, \boldsymbol{y}_{\mathbf{II}}^*)}{\partial x_i} \leq 0,\ \forall i = 1, ..., N$.

7. 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] A. Garnaev, M. Baykal-Gürsoy, and H. V. Poor, "A Game Theoretic Analysis of Secret and Reliable Communication With Active and Passive Adversarial Modes," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2155–2163, 2016.

[7] 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.

[8] 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.

[9] Afrand Agah, Sajal K Das, and Kalyan Basu, "A non-cooperative game approach for intrusion detection in sensor networks," in *IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004*. IEEE, 2004, vol. 4, pp. 2902–2906.

[10] 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.

[11] 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.

[12] Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya, and Qishi Wu, "A survey of game theory as applied to network security," in *2010 43rd Hawaii International Conference on System Sciences*. IEEE, 2010, pp. 1–10.

[13] 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.

[14] Xiangyun Zhou, Lingyang Song, and Yan Zhang, *Physical layer security in wireless communications*, Crc Press, 2013.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] John F Nash, "Equilibrium points in n-person games," *Proceedings of the National Academy of Sciences*, vol. 36, no. 1, pp. 48–49, 1950.